

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

เนาวรัตน์ ปิ่นอำนาจ

ดุษฎีนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ปีการศึกษา 2569

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

เนาวรัตน์ ปิ่นอำนาจ

ดุษฎีนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร

สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ปีการศึกษา 2569

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ใบรับรองดุษฎีนิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

โดย เนาวรัตน์ ปิ่นอำนาจ

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา

คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

คณะกรรมการสอบดุษฎีนิพนธ์

..... ประธาน

(ศาสตราจารย์ ดร.ปิยะ โควินท์ทวีวัฒน์)

..... อาจารย์ที่ปรึกษา

(ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข)

..... อาจารย์ที่ปรึกษาร่วม

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)

..... กรรมการ

(ศาสตราจารย์ ดร.พัลลภ พิริยะสุรวงศ์)

..... กรรมการ

(รองศาสตราจารย์ ดร.ลวัณกร มุกดาสนิท)

ชื่อ : **เนาวรัตน์ ปิ่นอำนาจ**

ชื่อดุษฎีนิพนธ์ : **สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา**

สาขาวิชา : **เทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา**
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

อาจารย์ที่ปรึกษาดุษฎีนิพนธ์หลัก : **ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข**

อาจารย์ที่ปรึกษาดุษฎีนิพนธ์ร่วม : **ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ**

ปีการศึกษา : **2569**

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ (1) วิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา (2) สร้างแบบจำลองสมการโครงสร้างของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัล (3) พัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อสนับสนุนการจัดการภูมิคุ้มกันดิจิทัล และ (4) ประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ที่พัฒนาขึ้น การวิจัยเป็นการวิจัยแบบผสานวิธี แบ่งการดำเนินการวิจัยออกเป็น 4 ระยะ ได้แก่ การวิเคราะห์ปัจจัย การสร้างแบบจำลองสมการโครงสร้าง การพัฒนาสถาปัตยกรรม และการประเมินความเหมาะสมของสถาปัตยกรรม การวิจัยเชิงปริมาณเก็บข้อมูลจากบุคลากรในสถาบันอุดมศึกษา จำนวน 500 คน โดยใช้แบบสอบถามมาตรประมาณค่า 5 ระดับ และวิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนาและการวิเคราะห์แบบจำลองสมการโครงสร้าง (Structural Equation Modeling: SEM) ส่วนการวิจัยเชิงคุณภาพใช้การสัมภาษณ์ผู้เชี่ยวชาญเพื่อยืนยันและปรับปรุงรูปแบบและสถาปัตยกรรมที่พัฒนาขึ้น

ผลการวิจัยพบว่า ปัจจัยด้านโครงสร้างองค์กร (EAC) เทคโนโลยีอัจฉริยะ (AIT) ระบบภูมิคุ้มกันดิจิทัล (DIS) และการจัดการองค์กรดิจิทัล (DEM) มีความสัมพันธ์และมีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) และการจัดการภูมิคุ้มกันดิจิทัล (DIM) ตามแบบจำลองที่พัฒนาขึ้น โดยแบบจำลองมีความสอดคล้องกับข้อมูลเชิงประจักษ์ในระดับดีมาก มีค่า Chi-square = 517.17, df = 499, p-value = 0.27784 และ RMSEA = 0.012 ผลการวิเคราะห์อิทธิพลพบว่า การจัดการองค์กรดิจิทัล (DEM) มีอิทธิพลทางบวกต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) สูงที่สุด มีค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.83 รองลงมาคือ ระบบภูมิคุ้มกันดิจิทัล (DIS) มีอิทธิพลทางบวกต่อการจัดการภูมิคุ้มกันดิจิทัล (DIM) มีค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.72 ขณะที่พบอิทธิพลทางตรงในทิศทางลบของ DIS ต่อ AIA และ DEM ต่อ DIM โดยมีค่า

สัมประสิทธิ์อิทธิพลเท่ากับ -0.28 และ -0.10 ตามลำดับ ทั้งนี้ แบบจำลองสามารถอธิบายความแปรปรวนของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) ได้ร้อยละ 70 และสามารถอธิบายความแปรปรวนของการจัดการภูมิคุ้มกันดิจิทัล (DIM) ได้ร้อยละ 81

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ประกอบด้วยองค์ประกอบสำคัญ ได้แก่ โครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัล โดยมีการบูรณาการสถาปัตยกรรมธุรกิจ ข้อมูล ระบบแอปพลิเคชัน เทคโนโลยี ความมั่นคงปลอดภัย การบูรณาการ และการกำกับดูแล ร่วมกับเทคโนโลยีปัญญาประดิษฐ์และกลไกการจัดการภูมิคุ้มกันดิจิทัล เพื่อสนับสนุนความสามารถของสถาบันอุดมศึกษาในการตรวจจับภัยคุกคาม การตอบสนองต่อเหตุการณ์ การประเมินและจัดการความเสี่ยง การปกป้องข้อมูลและความเป็นส่วนตัว การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย และการปฏิบัติตามนโยบายและกฎระเบียบ

ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยผู้เชี่ยวชาญ จำนวน 9 ท่าน พบว่า โดยภาพรวมมีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.89, S.D. = 0.31) โดยด้านระบบภูมิคุ้มกันดิจิทัลและด้านการจัดการภูมิคุ้มกันดิจิทัลมีความเหมาะสมในระดับมาก รองลงมาคือ ด้านเทคโนโลยีอัจฉริยะ ด้านการจัดการองค์กรดิจิทัล ด้านโครงสร้างองค์กร และด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ซึ่งทุกด้านมีความเหมาะสมอยู่ในระดับมาก ผลการวิจัยแสดงให้เห็นว่า สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ที่พัฒนาขึ้นสามารถใช้เป็นกรอบสถาปัตยกรรมสำหรับบูรณาการปัญญาประดิษฐ์เข้ากับการบริหารจัดการองค์กรและการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา เพื่อเพิ่มความสามารถในการป้องกัน ตรวจจับ ตอบสนอง และจัดการความเสี่ยงจากภัยคุกคามทางดิจิทัล

(มีจำนวนทั้งสิ้น 398 หน้า)

คำสำคัญ : สถาปัตยกรรมองค์กร, ปัญญาประดิษฐ์, ระบบภูมิคุ้มกันดิจิทัล, การจัดการองค์กรดิจิทัล, สถาปัตยกรรมองค์กรปัญญาประดิษฐ์, การจัดการภูมิคุ้มกันดิจิทัล, สถาบันอุดมศึกษา

อาจารย์ที่ปรึกษาดุษฎีนิพนธ์หลัก

Name : Nawarat Pinamnaj

Dissertation Title : Artificial Intelligence Enterprise Architecture for Digital Immunity Management in Higher Education Institution

Major Field : Information and Communication Technology for Educational
King Mongkut's University of Technology North Bangkok

Dissertation Advisor : Professor Dr. Prachyanun Nilsook

Co-Advisor : Professor Dr. Panita Wannapiroon

Academic Year : 2026

ABSTRACT

This research aimed to (1) analyze the factors influencing Artificial Intelligence Enterprise Architecture and Digital Immunity Management for higher education institutions; (2) develop a structural equation model of Artificial Intelligence Enterprise Architecture and Digital Immunity Management; (3) develop an Artificial Intelligence Enterprise Architecture to support Digital Immunity Management; and (4) evaluate the appropriateness of the developed architecture. The study employed a mixed-methodology research design conducted in four phases: factor and component analysis, structural equation model development, architecture development, and architecture evaluation. The quantitative research collected data from 500 personnel in higher education institutions using a five-point Likert-scale questionnaire. The data were analyzed using descriptive statistics and Structural Equation Modeling (SEM). The qualitative research employed expert interviews to validate and refine the proposed architecture.

The findings revealed that Organizational Structure (EAC), Artificial Intelligence Technology (AIT), Digital Immune System (DIS), and Digital Enterprise Management (DEM) were associated with and exerted influences on Artificial Intelligence Enterprise Architecture (AIA) and Digital Immunity Management (DIM)

within the proposed structural model. The structural equation model demonstrated a good fit with the empirical data, with Chi-square = 517.17, df = 499, p-value = 0.27784, and RMSEA = 0.012. The path analysis indicated that Digital Enterprise Management (DEM) had the strongest positive influence on Artificial Intelligence Enterprise Architecture (AIA), with a standardized path coefficient of 0.83. Digital Immune System (DIS) had a positive influence on Digital Immunity Management (DIM), with a standardized path coefficient of 0.72. The structural model explained 70% of the variance in Artificial Intelligence Enterprise Architecture (AIA) and 81% of the variance in Digital Immunity Management (DIM).

The developed Artificial Intelligence Enterprise Architecture for Digital Immunity Management in higher education institutions consisted of key components including Organizational Structure, Intelligent Technology, Digital Immune System, Digital Enterprise Management, Artificial Intelligence Enterprise Architecture, and Digital Immunity Management. The architecture integrates business, data, application, technology, security, integration, and governance architectures with artificial intelligence technologies and digital immunity mechanisms to support systematic threat detection, incident response, risk assessment and management, data and privacy protection, security awareness, and policy and regulatory compliance.

The proposed architecture was evaluated by nine experts and achieved an overall mean appropriateness score of 4.89 (S.D. = 0.31), indicating the highest level of appropriateness. All six major components were rated at a high level of appropriateness. The findings demonstrate that the proposed Artificial Intelligence Enterprise Architecture can serve as an architectural framework for integrating artificial intelligence into organizational management and digital immunity management in higher education institutions, thereby enhancing their capabilities to prevent, detect, respond to, and manage digital threats and risks.

(Total 398 Pages)

Keywords: Enterprise Architecture, Artificial Intelligence, Digital Immunity, Digital Enterprise Management, AI Enterprise Architecture, Digital Immunity Management, Higher Education Institution

_____ **Advisor**



กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างสมบูรณ์ด้วยความกรุณา ความเมตตา และความเอาใจใส่อย่างดียิ่งจาก ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ อาจารย์ที่ปรึกษาร่วม ซึ่งได้กรุณาให้คำปรึกษา แนวคิด ข้อเสนอแนะ ตลอดจนถ่ายทอดองค์ความรู้ที่เป็นประโยชน์อย่างยิ่งต่อการดำเนินงานวิจัย ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูงในความเมตตาและความทุ่มเทที่มีให้เสมอมา

ขอกราบขอบพระคุณ ศาสตราจารย์ ดร.ปิยะ โควินท์ทวีวัฒน์ ศาสตราจารย์ ดร.พัลลภ พิริยะสุรวงศ์ รองศาสตราจารย์ ดร.ลวัณกร มุกดาสนิท และ อาจารย์ ดร.จันทร์จิราพร ทองประสิทธิ์ ที่กรุณาเสียสละเวลาอันมีค่าในการเป็นคณะกรรมการสอบป้องกันวิทยานิพนธ์ พร้อมทั้งให้ข้อเสนอแนะและคำแนะนำที่เป็นประโยชน์อย่างยิ่ง ซึ่งช่วยให้งานวิจัยฉบับนี้มีความสมบูรณ์และชัดเจนมากยิ่งขึ้น

ขอขอบพระคุณ ดร.ดารัตน์ ศิริวิริยะกุล วิภาตะกลัศ อธิการบดีมหาวิทยาลัยเจ้าพระยา ตลอดจนผู้เชี่ยวชาญและผู้ทรงคุณวุฒิทุกท่าน ที่กรุณาให้ความอนุเคราะห์ในการตรวจสอบและประเมินคุณภาพเครื่องมือวิจัย พร้อมทั้งให้ข้อเสนอแนะอันทรงคุณค่า ซึ่งมีส่วนสำคัญอย่างยิ่งต่อความน่าเชื่อถือของงานวิจัยครั้งนี้

ขอขอบพระคุณมหาวิทยาลัยเจ้าพระยา ที่กรุณาอนุมัติให้ผู้วิจัยลาศึกษาต่อในระดับปริญญาเอก และให้การสนับสนุนทุนการศึกษาตลอดระยะเวลาการศึกษา รวมทั้งคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเจ้าพระยา ที่ให้การสนับสนุนและอำนวยความสะดวกในการดำเนินงานวิจัยจนสำเร็จลุล่วงด้วยดี นอกจากนี้ ขอขอบคุณเพื่อนร่วมงาน เพื่อนร่วมศึกษา และผู้ที่มิได้กล่าวนามทุกท่าน ที่ให้ความช่วยเหลือ สนับสนุน และเป็นกำลังใจตลอดระยะเวลาการศึกษา

เหนือสิ่งอื่นใด ผู้วิจัยขอกราบขอบพระคุณครอบครัวและญาติพี่น้องทุกท่าน ที่เป็นพลังใจสำคัญ เป็นแรงสนับสนุนและแรงผลักดันให้ผู้วิจัยสามารถก้าวผ่านอุปสรรคต่าง ๆ และประสบความสำเร็จในการศึกษาครั้งนี้

สุดท้ายนี้ ขอขอบพระคุณบัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ที่ได้ให้โอกาสทางการศึกษา ให้การสนับสนุนด้านวิชาการ และสร้างสภาพแวดล้อมทางการเรียนรู้ที่เอื้อต่อการพัฒนาศักยภาพทางวิชาการของผู้วิจัย จนทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยดี

ผู้วิจัยขอกราบขอบพระคุณทุกท่านมา ณ โอกาสนี้อย่างสุดซึ้ง

เนาวรัตน์ ปิ่นอำนาจ

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... ฉ

กิตติกรรมประกาศ ..... ฌ

สารบัญ ..... ญ

สารบัญตาราง ..... ฏ

สารบัญรูปภาพ ..... ณ

บทที่ 1 บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์การวิจัย 6
1.3 ขอบเขตของการวิจัย 6
1.4 คำถามวิจัย 7
1.5 สมมติฐานการวิจัย 7
1.6 กรอบแนวคิดการวิจัย 8
1.7 ประโยชน์ที่คาดว่าจะได้รับ 10
1.8 นิยามศัพท์เฉพาะ 10

บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง 13

2.1 โครงสร้างองค์กร (Organizational Structure) 13
2.2 เทคโนโลยีอัจฉริยะ (Intelligent Technology) 51
2.3 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) 58
2.4 ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity System) 63
2.5 การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) 68
2.6 การจัดการองค์กรดิจิทัล (Digital Enterprise Management) 73
2.7 สถาบันอุดมศึกษา (Higher Education Institution) 80
2.8 สรุปเอกสารและงานวิจัยที่เกี่ยวข้อง 90

บทที่ 3 วิธีดำเนินการวิจัย 93

3.1 การวิจัยระยะที่ 1 การวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 97
3.2 การวิจัยระยะที่ 2 การสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 98
3.3 การวิจัยระยะที่ 3 การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาตามแบบจำลองสมการโครงสร้าง 108
3.4 การวิจัยระยะที่ 4 การประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 111
บทที่ 4 ผลการสร้างแบบจำลองสมการโครงสร้าง 114
4.1 ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล 114
4.2 ผลการสร้างแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษ 164
บทที่ 5 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 175
5.1 แผนและนโยบายที่เกี่ยวข้อง 175
5.2 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 186
5.3 การออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 253
5.4 ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 275
บทที่ 6 สรุปผล อภิปรายผล และข้อเสนอแนะ 282
6.1 สรุปผลการวิจัย 282
6.2 อภิปรายผล 292
6.3 ข้อเสนอแนะ 295
บรรณานุกรม 298
ภาคผนวก 336
ประวัติผู้เขียน 397

สารบัญตาราง

หน้า

ตารางที่ 2-1 การสังเคราะห์กรอบของโครงสร้างองค์กร 49
ตารางที่ 2-2 การสังเคราะห์เทคโนโลยีอัจฉริยะ 56
ตารางที่ 2-3 การสังเคราะห์องค์ประกอบของการจัดการภูมิคุ้มกันดิจิทัล 63
ตารางที่ 2-4 การสังเคราะห์องค์ประกอบของการจัดการองค์กรดิจิทัล 70
ตารางที่ 2-5 วิเคราะห์คำสำคัญ 78
ตารางที่ 3-1 ขั้นตอนการดำเนินการวิจัย 93
ตารางที่ 3-2 ขั้นตอนการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 97
ตารางที่ 3-3 ขั้นตอนการสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 99
ตารางที่ 3-4 ขนาดกลุ่มตัวอย่างในการวิเคราะห์โมเดลแบบจำลอง 100
ตารางที่ 3-5 ผลการตรวจสอบอำนาจจำแนกและความเชื่อมั่นของแบบสอบถาม 102
ตารางที่ 3-6 จำนวนกลุ่มตัวอย่างที่ได้จาการเก็บข้อมูลเชิงปริมาณ 105
ตารางที่ 3-7 เกณฑ์การประเมินความสอดคล้องของโมเดลแบบจำลองสมการโครงสร้าง 107
ตารางที่ 3-8 ขั้นตอนการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 109
ตารางที่ 3-9 ขั้นตอนการประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 111
ตารางที่ 4-1 แสดงจำนวนและร้อยละข้อมูลทั่วไปของผู้ตอบแบบสอบถาม 115
ตารางที่ 4-2 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านโครงสร้างองค์กร 124
ตารางที่ 4-3 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านโครงสร้างองค์กร 125
ตารางที่ 4-4 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านเทคโนโลยีอัจฉริยะ 129
ตารางที่ 4-5 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านเทคโนโลยีอัจฉริยะ 129
ตารางที่ 4-6 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านระบบภูมิคุ้มกันดิจิทัล 131
ตารางที่ 4-7 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านระบบภูมิคุ้มกันดิจิทัล 132

ตารางที่ 4-8 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล 136
ตารางที่ 4-9 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านการจัดการองค์กรดิจิทัล..... 136
ตารางที่ 4-10 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ 139
ตารางที่ 4-11 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์..... 140
ตารางที่ 4-12 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการภูมิคุ้มกันดิจิทัล 144
ตารางที่ 4-13 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านการจัดการภูมิคุ้มกันดิจิทัล ... 145
ตารางที่ 4-14 ผลการวิเคราะห์อิทธิพลทางตรง (Direct Effect) อิทธิพลทางอ้อม (Indirect Effect) และอิทธิพลรวม (Total Effect) ตามแบบจำลองสมการโครงสร้าง..... 149
ตารางที่ 4-15 สรุปอิทธิพลทางตรง (Direct Effect) อิทธิพลทางอ้อม (Indirect Effect) และอิทธิพลรวม (Total Effect) ระหว่างตัวแปรในแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 155
ตารางที่ 4-16 ผลวิเคราะห์ค่าสถิติองค์ประกอบเชิงยืนยันที่มีอิทธิพบต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิททัลสำหรับสถาบันอุดมศึกษา..... 149
ตารางที่ 4-17 วิเคราะห์สหสัมพันธ์แบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 155
ตารางที่ 4-18 วิวิเคราะห์ตครวจสอบข้อมูลตัวแปรปัจจัยที่มีดิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 149
ตารางที่ 4-19 ค่าสถิติประเมินความกลมกลืนของสมการเชิงโครงสร้างแบบจำลอง..... 155
ตารางที่ 4-20 วิเคราะห์สมการเชิงโครงสร้างแบบจำลองผลปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 155
ตารางที่ 4-21 ผลการวิเคราะห์เส้นอิทธิพลสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 149
ตารางที่ 4-22 สรุปผลการทดสอบสมมติฐานปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 155
ตารางที่ 5-1 การวิเคราะห์ช่องว่างด้านธุรกิจ..... 191
ตารางที่ 5-2 การวิเคราะห์ช่องว่างด้านข้อมูล..... 199
ตารางที่ 5-3 การวิเคราะห์ช่องว่างด้านแอปพลิเคชัน 203

ตารางที่ 5-4 ความสัมพันธ์ระหว่างเทคโนโลยีกับกระบวนการธุรกิจของสถาบันอุดมศึกษา 205
ตารางที่ 5-5 การวิเคราะห์ช่องว่างด้านเทคโนโลยี 207
ตารางที่ 5-6 สรุปผลการวิเคราะห์ด้านเทคโนโลยี 210
ตารางที่ 5-7 ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยกับกระบวนการธุรกิจ 212
ตารางที่ 5-8 การวิเคราะห์ช่องว่างด้านความมั่นคงปลอดภัย 213
ตารางที่ 5-9 สรุปผลการวิเคราะห์ด้านความมั่นคงปลอดภัย 215
ตารางที่ 5-10 ความสัมพันธ์ระหว่างการบูรณาการกับกระบวนการธุรกิจ 217
ตารางที่ 5-11 การวิเคราะห์ช่องว่างด้านการบูรณาการ 219
ตารางที่ 5-12 สรุปผลการวิเคราะห์ด้านการบูรณาการ 221
ตารางที่ 5-13 ความสัมพันธ์ระหว่างการกำกับดูแลกับกระบวนการธุรกิจ 223
ตารางที่ 5-14 การวิเคราะห์ช่องว่างด้านการกำกับดูแล 224
ตารางที่ 5-15 สรุปผลการวิเคราะห์ด้านการกำกับดูแล 226
ตารางที่ 5-16 ความสัมพันธ์ระหว่างเทคโนโลยีอัจฉริยะกับกระบวนการธุรกิจ 229
ตารางที่ 5-17 การวิเคราะห์ช่องว่างด้านเทคโนโลยีอัจฉริยะ 230
ตารางที่ 5-18 สรุปสำหรับเชื่อมไปสู่ Target Architecture 231
ตารางที่ 5-19 ความสัมพันธ์ระหว่างระบบภูมิคุ้มกันดิจิทัลกับกระบวนการธุรกิจ 234
ตารางที่ 5-20 การวิเคราะห์ช่องว่างด้านระบบภูมิคุ้มกันดิจิทัล 235
ตารางที่ 5-21 สรุปสำหรับเชื่อม Current Architecture ⟶ Target Architecture 236
ตารางที่ 5-22 ความสัมพันธ์ระหว่างการจัดการองค์กรดิจิทัลกับกระบวนการธุรกิจ 239
ตารางที่ 5-23 การวิเคราะห์ช่องว่างด้านการจัดการองค์กรดิจิทัล 240
ตารางที่ 5-24 สรุปผลการวิเคราะห์สถาปัตยกรรมปัจจุบัน ช่องว่าง และสถาปัตยกรรมเป้าหมาย 242
ตารางที่ 5-25 ความสัมพันธ์ระหว่าง AI Enterprise Architecture กับกระบวนการธุรกิจ 245
ตารางที่ 5-26 การวิเคราะห์ช่องว่าง AI Enterprise Architecture Gap 245
ตารางที่ 5-27 ความสัมพันธ์กับกระบวนการธุรกิจ 247
ตารางที่ 5-28 Digital Immunity Management Gap 248
ตารางที่ 5-29 การวิเคราะห์ปัจจัยภายในตามกรอบ 7-S Model 249
ตารางที่ 5-30 การวิเคราะห์ปัจจัยภายนอกตาม PEST Model 249
ตารางที่ 5-31 การวิเคราะห์ SWOT 250
ตารางที่ 5-32 TOWS Matrix สำหรับสถาบันอุดมศึกษา 250
ตารางที่ 5-33 การเชื่อมโยงผลการวิเคราะห์กับข้อกำหนดสถาปัตยกรรม 251
ตารางที่ 5-34 สรุปสำหรับเชื่อมเข้าสู่การออกแบบ Target Architecture 252

ตารางที่ 5-35 ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 275
ตารางที่ 6-1 ผลการวิเคราะห์อิทธิพลแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 289

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

สารบัญรูปภาพ

หน้า

ภาพที่ 1-1 กรอบแนวคิดการวิจัยของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 8
ภาพที่ 2-1 กรอบแนวคิดการออกแบบสถาปัตยกรรมองค์กรแบบ TOGAF 18
ภาพที่ 2-2 The Zachman Framework of enterprise architecture 24
ภาพที่ 2-3 Federal Enterprise Architecture Framework (FEAF) 26
ภาพที่ 2-4 SABSA Architecture 42
ภาพที่ 2-5 องค์ประกอบของโครงสร้างองค์กร 44
ภาพที่ 2-6 องค์ประกอบของเทคโนโลยีอัจฉริยะ 50
ภาพที่ 2-7 องค์ประกอบของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ 56
ภาพที่ 2-8 องค์ประกอบของระบบภูมิคุ้มกันดิจิทัล 59
ภาพที่ 2-9 Six Prerequisites for a Strong Digital Immune System 61
ภาพที่ 2-10 องค์ประกอบของการจัดการภูมิคุ้มกันดิจิทัล 64
ภาพที่ 2-11 องค์ประกอบของการจัดการองค์กรดิจิทัล 71
ภาพที่ 3-1 วิธีการสุ่มกลุ่มตัวอย่าง 101
ภาพที่ 4-1 Full Path Model ความสัมพันธ์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 150
ภาพที่ 4-2 องค์ประกอบสำคัญด้านโครงสร้างองค์กร 151
ภาพที่ 4-3 องค์ประกอบสำคัญด้านเทคโนโลยีอัจฉริยะ 152
ภาพที่ 4-4 องค์ประกอบสำคัญด้านระบบภูมิคุ้มกันดิจิทัล 152
ภาพที่ 4-5 องค์ประกอบสำคัญด้านการจัดการองค์กรดิจิทัล 153
ภาพที่ 4-6 องค์ประกอบสำคัญด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ 153
ภาพที่ 4-7 องค์ประกอบสำคัญด้านการจัดการภูมิคุ้มกันดิจิทัล 154
ภาพที่ 4-8 Over-identified Model ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 156
ภาพที่ 4-9 แบบจำลองสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 165
ภาพที่ 5-1 แสดงความสัมพันธ์เชิงสถาปัตยกรรม 168
ภาพที่ 5-2 โครงสร้างการทำงานของระบบภูมิคุ้มกันดิจิทัล 207

ภาพที่ 5-3 องค์ประกอบกลไกสนับสนุนการบริหารจัดการและการตัดสินใจสถาปัตยกรรมเป้าหมาย 212
ภาพที่ 5-4 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 222
ภาพที่ 5-5 ธรรมาภิบาลองค์กร 222
ภาพที่ 5-6 โครงสร้างองค์กร 225
ภาพที่ 5-7 เทคโนโลยีปัญญาประดิษฐ์ และระบบอัจฉริยะ 229
ภาพที่ 5-8 การจัดการองค์กรดิจิทัล 230
ภาพที่ 5-9 สถาปัตยกรรมภูมิคุ้มกันดิจิทัลและความเสี่ยง 231
ภาพที่ 5-10 การจัดการภูมิคุ้มกันดิจิทัล 235
ภาพที่ 5-11 แหล่งข้อมูล 237
ภาพที่ 5-12 ผู้ใช้งาน 239

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคดิจิทัลที่เทคโนโลยีมีบทบาทสำคัญในทุกภาคส่วน การรักษาความปลอดภัยทางไซเบอร์กลายเป็นเรื่องที่มีความสำคัญอย่างยิ่ง โดยเฉพาะในสถาบันการศึกษา เช่น สถาบันอุดมศึกษา ซึ่งมีข้อมูลที่สำคัญและเป็นความลับมากมาย เช่น ข้อมูลนักศึกษา ข้อมูลการวิจัย และข้อมูลทางการเงิน การโจมตีทางไซเบอร์ที่เกิดขึ้นสามารถก่อให้เกิดความเสียหายทั้งทางการเงินและชื่อเสียงของสถาบันได้ การใช้ปัญญาประดิษฐ์ (AI) และสถาปัตยกรรมองค์กรเพื่อการจัดการภูมิคุ้มกันดิจิทัล ได้กลายเป็นแนวทางที่สำคัญในการป้องกันความเสี่ยงทางเทคโนโลยีและเสริมสร้างความยืดหยุ่นของระบบดิจิทัลในสถาบันอุดมศึกษา ซึ่งต้องการการปกป้องข้อมูลและการบริหารจัดการความปลอดภัยอย่างรัดกุม ในช่วงหลายปีที่ผ่านมาการโจมตีทางไซเบอร์มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ทั้งในรูปแบบของการโจมตี แบบฟิชชิ่ง (phishing), มัลแวร์ (malware), และการโจมตีแบบ DDoS (Distributed Denial of Service) สถาบันอุดมศึกษาเป็นหนึ่งในเป้าหมายหลักของการโจมตีเหล่านี้ เนื่องจากมีข้อมูลที่มีมูลค่าสูงและระบบความปลอดภัยที่อาจไม่แข็งแกร่งเท่าที่ควร

การเปลี่ยนแปลงที่รวดเร็วในแนวทางการศึกษาในศตวรรษที่ 21 ซึ่งเกิดจากความก้าวหน้าทางเทคโนโลยี โดยเฉพาะอย่างยิ่งในด้าน AI ที่มีการพัฒนาอย่างรวดเร็วในช่วงไม่กี่ปีที่ผ่านมา AI เป็นเทคโนโลยีที่สามารถสร้างเนื้อหาหรือข้อมูลใหม่ได้ โดยใช้โมเดลการเรียนรู้ที่ไม่ต้องมีการควบคุมหรือมีการควบคุมบางส่วน (unsupervised or partially supervised learning) ซึ่งช่วยให้สามารถสร้างสิ่งที่มีความหมายจากข้อมูลที่มีอยู่ได้ (Baidoo-Anu & Owusu Ansah, 2023)

ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) ของประเทศไทยถูกวางแผนขึ้นเพื่อให้ประเทศมีการพัฒนาอย่างยั่งยืนในทุกมิติ โดยมีวิสัยทัศน์ที่จะทำให้ประเทศไทยเป็นประเทศที่มีความมั่นคง และยั่งยืนในระยะยาว โดยเฉพาะด้านเศรษฐกิจและสังคม หนึ่งในเป้าหมายสำคัญของยุทธศาสตร์นี้ คือ การเสริมสร้างขีดความสามารถทางเทคโนโลยีและนวัตกรรม เพื่อผลักดันให้ประเทศสามารถแข่งขันในเวทีโลกได้อย่างมีประสิทธิภาพ โดยเฉพาะการส่งเสริมการใช้ ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ที่เป็นหนึ่งในเทคโนโลยีสำคัญในการสนับสนุนการเติบโตทางเศรษฐกิจดิจิทัล (Digital Economy) ของประเทศ ในบริบทของสถาบันอุดมศึกษา การจัดการภูมิคุ้มกันดิจิทัลเป็นสิ่งสำคัญ เนื่องจากมหาวิทยาลัยเป็นศูนย์กลางของการผลิตความรู้และนวัตกรรมที่สำคัญ ยุทธศาสตร์ชาติยังชี้ให้เห็นถึงความจำเป็นในการพัฒนาระบบการศึกษาที่มุ่งเน้นการสร้างคนไทยที่มีทักษะและความรู้ที่ทันสมัย สอดคล้องกับโลกที่เปลี่ยนแปลงอย่างรวดเร็ว การใช้สถาปัตยกรรมองค์กร

ปัญญาประดิษฐ์เพื่อสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลจะเป็นกลไกสำคัญที่ช่วยให้สถาบันอุดมศึกษาสามารถรักษาความปลอดภัยของข้อมูลและทรัพยากรดิจิทัล ตลอดจนเตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้น (สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2567)

นอกจากนี้แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติของประเทศไทย ซึ่งเป็นกรอบนโยบายที่ใช้ในการพัฒนาประเทศมาตั้งแต่ปี พ.ศ. 2504 ได้มุ่งเน้นการสร้างความมั่นคงและยั่งยืนทางเศรษฐกิจและสังคม ผ่านการพัฒนาทางเทคโนโลยีและนวัตกรรมเพื่อเพิ่มศักยภาพการแข่งขันของประเทศในเวทีโลก ในแผนพัฒนาฉบับที่ 13 (พ.ศ. 2566-2570) ให้ความสำคัญอย่างยิ่งกับการพัฒนาระบบเศรษฐกิจดิจิทัล (Digital Economy) และการนำเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้ในการยกระดับภาคการศึกษาและการจัดการข้อมูล เพื่อให้สอดคล้องกับเป้าหมายการพัฒนาที่ยั่งยืน (Sustainable Development Goals: SDGs) และการสร้างเศรษฐกิจที่ยั่งยืน ในบริบทของสถาบันอุดมศึกษา ซึ่งเป็นศูนย์กลางการผลิตบุคลากรที่มีความรู้ความสามารถในยุคดิจิทัล แผนพัฒนาฯ ได้มุ่งเน้นการสนับสนุนการสร้างระบบภูมิคุ้มกันทางดิจิทัล (Digital Immunity) เพื่อรักษาความปลอดภัยของข้อมูลและระบบเทคโนโลยีที่เกี่ยวข้อง การจัดการภูมิคุ้มกันดิจิทัลกลายเป็นประเด็นสำคัญในการปกป้องทรัพยากรข้อมูลที่มีค่าและสำคัญของมหาวิทยาลัยจากภัยคุกคามไซเบอร์ที่เพิ่มมากขึ้นในยุคดิจิทัล (สำนักงานปลัดกระทรวงศึกษาธิการ, 2567)

ปัญญาประดิษฐ์ (AI) เริ่มต้นขึ้นในช่วงกลางศตวรรษที่ 20 เมื่อมีการพัฒนาเครื่องจักรที่สามารถคำนวณและแก้ปัญหาทางคณิตศาสตร์ได้อย่างมีประสิทธิภาพ การวิจัยเกี่ยวกับ AI เริ่มต้นอย่างจริงจังในปี 1956 ในการประชุม Dartmouth Conference ซึ่งเป็นการรวมกลุ่มของนักวิทยาศาสตร์ที่เชื่อว่าเครื่องจักรสามารถถูกออกแบบให้ "คิด" ได้เหมือนมนุษย์ ต่อมา AI ได้รับการพัฒนาอย่างต่อเนื่อง โดยมีการสร้างเทคโนโลยีและเครื่องมือที่สามารถเรียนรู้และปรับปรุงประสิทธิภาพได้ด้วยตนเอง เช่น Machine Learning และ Deep Learning ซึ่งเป็นการนำเอาข้อมูลจำนวนมากมาใช้เพื่อให้ AI เรียนรู้และพัฒนาตนเอง (Xiao et al., 2022) นอกจากนี้ ปัญญาประดิษฐ์ยังเป็นเทคโนโลยีที่พัฒนาขึ้นเพื่อให้เครื่องจักรหรือคอมพิวเตอร์สามารถทำงานที่ซับซ้อน ซึ่งโดยปกติแล้วต้องอาศัยความคิดเชิงวิเคราะห์และการตัดสินใจของมนุษย์ AI มีความสามารถในการเลียนแบบกระบวนการคิดของมนุษย์ เช่น การเรียนรู้ การวิเคราะห์ข้อมูล การแก้ปัญหา และการตัดสินใจ ได้กลายเป็นเทคโนโลยีสำคัญในการจัดการกับปัญหาภัยคุกคามทางดิจิทัล โดยมีความสามารถในการตรวจจับและตอบสนองต่อพฤติกรรมที่เป็นอันตรายในเครือข่ายได้อย่างรวดเร็วและมีประสิทธิภาพ (Mkhwanazi & Beharry-Ramraj, 2023) และยังมีการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) เพื่อเสริมสร้างความปลอดภัยในระบบคลาวด์ โดยเน้นถึงความสำคัญของการรักษาความปลอดภัยและความเป็นส่วนตัวในสภาพแวดล้อมของ IoT (Internet of Things) ที่กำลังเติบโตอย่างรวดเร็ว ปัญหา

หลักที่เกี่ยวข้องกับความปลอดภัยในคลาวด์ เช่น การเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต การโจมตีจากภายนอก และความเสี่ยงจากการสูญหายของข้อมูล ซึ่งเป็นปัญหาที่ไม่สามารถหลีกเลี่ยงได้เมื่อมีการใช้บริการคลาวด์ นอกจากนี้ยังมีการพูดถึงการใช้เทคนิค AI เช่น การเรียนรู้เชิงลึก (Deep Learning) และอัลกอริธึมการจำแนกประเภท (Classification Algorithms) เพื่อช่วยในการตรวจจับและตอบสนองต่อภัยคุกคามใหม่ ๆ ที่เกิดขึ้น (Saleh Alrubayyi, 2023a; Sneesl et al., 2022)

สถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นกรอบแนวทางในการออกแบบพิมพ์เขียวแบบจำลองอนาคตภาพขององค์กร รวมถึงเป็นเครื่องมือในการพัฒนาโครงสร้างองค์กรที่ใช้ในการออกแบบและจัดการองค์กร เพื่อให้สามารถตอบสนองต่อการดำเนินงานและการเปลี่ยนแปลงที่รวดเร็วของเทคโนโลยีได้อย่างเหมาะสม (Srisawat et al., 2023) นอกจากนี้ สถาปัตยกรรมองค์กร (Enterprise Architecture) ยังเป็นกรอบการทำงานที่สำคัญในการจัดการและวางแผนระบบไอทีให้มีประสิทธิภาพ ซึ่งสามารถนำมาผสานกับ AI เพื่อพัฒนากลยุทธ์การป้องกันภัยคุกคามในระดับองค์กร (Krauze & Grabis, 2024a) และยังกล่าวได้ว่าสถาปัตยกรรมองค์กร ยังหมายถึงการออกแบบโครงสร้างและกระบวนการบริหารจัดการขององค์กรในลักษณะที่ใช้เทคโนโลยีดิจิทัลเป็นแกนกลาง สถาปัตยกรรมองค์กรมีบทบาทในการเชื่อมโยงทรัพยากร เทคโนโลยี และกระบวนการทำงานขององค์กร เพื่อให้เกิดประสิทธิภาพสูงสุดในการดำเนินงาน ซึ่งในบริบทของสถาปัตยกรรมองค์กรดิจิทัลจะรวมถึงการจัดการระบบสารสนเทศ ระบบการสอนผ่านออนไลน์ และเทคโนโลยีการเรียนรู้ที่สามารถปรับตัวให้เข้ากับความต้องการของผู้เรียนและการจัดการทรัพยากรการศึกษา โดยมีเป้าหมายหลักคือการเพิ่มประสิทธิภาพในการจัดการและการส่งมอบการศึกษาอย่างมีคุณภาพผ่านระบบดิจิทัล (Srisawat et al., 2023) นอกจากนี้สถาปัตยกรรมองค์กรยังหมายถึงกรอบการทำงานที่ช่วยในการจัดการ และวางแผนโครงสร้างขององค์กร ที่มีการเชื่อมโยงระหว่างกลยุทธ์ทางธุรกิจและเทคโนโลยีสารสนเทศ (IT) เพื่อให้สามารถตอบสนองต่อการเปลี่ยนแปลงและความต้องการของตลาดได้อย่างมีประสิทธิภาพ โดยเฉพาะในบริบทของสถาปัตยกรรมองค์กรแบบ Agile (Agile Enterprise Architecture - AEA) จะเน้นที่ความยืดหยุ่น การปรับตัว และการพัฒนาอย่างต่อเนื่อง ซึ่งช่วยให้องค์กรสามารถจัดการกับความซับซ้อน และการเปลี่ยนแปลงทางดิจิทัลได้ดีขึ้น AEA ใช้หลักการของ Agile เช่น การพัฒนาแบบวนรอบ (iterative development) การตอบรับอย่างรวดเร็ว (rapid feedback) และการทำงานร่วมกัน (collaboration) เพื่อสร้างและจัดการเอกสารสถาปัตยกรรมองค์กรที่สามารถสร้างคุณค่าให้กับองค์กรได้อย่างรวดเร็วและมีประสิทธิภาพ (Sararuch et al., 2023a)

สถาปัตยกรรมองค์กร (Enterprise Architecture) ยังถือเป็นเรื่องการเข้าใจองค์ประกอบต่าง ๆ ที่ทำให้ธุรกิจดำเนินไปและความสัมพันธ์ระหว่างองค์ประกอบเหล่านั้น สถาปัตยกรรมองค์กรเป็นแผนที่ครอบคลุมซึ่งทำหน้าที่เป็นแรงขับเคลื่อนความร่วมมือระหว่างวัตถุประสงค์ วิสัยทัศน์ กล

ยุทธ์ และหลักการกำกับดูแล นอกจากนี้ยังเชื่อมโยงกับด้านต่าง ๆ ของการดำเนินธุรกิจ เช่น โครงสร้างองค์กร กระบวนการ และข้อมูล รวมถึงด้านการทำงานอัตโนมัติ เช่น ระบบสารสนเทศและฐานข้อมูล รวมถึงโครงสร้างพื้นฐานทางเทคโนโลยีที่สนับสนุนธุรกิจ เช่น คอมพิวเตอร์ ระบบปฏิบัติการ และเครือข่าย (Dumitriu & Popescu, 2020a)

สถาปัตยกรรมองค์กรจะช่วยในการวางแผนและจัดการโครงสร้างขององค์กรทั้งหมด รวมถึงกระบวนการทางธุรกิจ ระบบเทคโนโลยี และข้อมูล เพื่อให้สอดคล้องกับกลยุทธ์และเป้าหมายขององค์กร สถาปัตยกรรมองค์กร (Enterprise Architecture, EA) มีประโยชน์มากมายต่อองค์กรในหลายด้าน เช่น การเชื่อมโยงกลยุทธ์และการปฏิบัติ การเพิ่มประสิทธิภาพและลดความซ้ำซ้อน การปรับตัวและความยืดหยุ่น การปรับปรุงคุณภาพและการควบคุม การสนับสนุนการตัดสินใจ การเสริมสร้างการสื่อสารและความร่วมมือ และการจัดการความเสี่ยง (Karande & Joshi, 2022a)

การนำสถาปัตยกรรมองค์กรมาใช้ประโยชน์นั้นมีความสำคัญอย่างยิ่งในการเพิ่มประสิทธิภาพและความสามารถในการปรับตัวขององค์กร สถาปัตยกรรมองค์กรช่วยเชื่อมโยงกลยุทธ์ทางธุรกิจและการดำเนินงานในระดับปฏิบัติการ โดยทำหน้าที่เป็นแผนที่ที่แสดงถึงความสัมพันธ์และการทำงานร่วมกันระหว่างระบบ เทคโนโลยี และกระบวนการต่าง ๆ ภายในองค์กร การนำสถาปัตยกรรมองค์กรมาใช้ช่วยในการบูรณาการระบบและกระบวนการต่าง ๆ ทำให้การทำงานร่วมกันเป็นไปอย่างมีประสิทธิภาพ ลดความซ้ำซ้อน และลดค่าใช้จ่ายที่ไม่จำเป็น นอกจากนี้ สถาปัตยกรรมองค์กรยังสนับสนุนองค์กรในการปรับตัวและตอบสนองต่อการเปลี่ยนแปลงในตลาดหรือเทคโนโลยีอย่างรวดเร็ว โดยช่วยในการพัฒนาระบบใหม่ที่ไม่ส่งผลกระทบต่อระบบที่มีอยู่ นอกจากนี้ สถาปัตยกรรมองค์กรยังเสริมสร้างการควบคุมและการจัดการคุณภาพของข้อมูลและระบบ ทำให้สามารถติดตามและปรับปรุงคุณภาพได้อย่างมีประสิทธิภาพ รวมถึงช่วยในการตัดสินใจเชิงกลยุทธ์โดยให้ข้อมูลเชิงลึกและการวิเคราะห์ที่มีประโยชน์ การใช้สถาปัตยกรรมองค์กรยังช่วยในการสื่อสารและสร้างความเข้าใจร่วมกันภายในองค์กร ทำให้การดำเนินงานเป็นไปอย่างราบรื่นและสอดคล้องกัน (Kotusev & Kurnia, 2021)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) เป็นกรอบแนวคิดที่ออกแบบและจัดการโครงสร้างพื้นฐานขององค์กรร่วมกับเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) เข้าไว้ในกระบวนการทางธุรกิจ ระบบเทคโนโลยี และข้อมูล การนำปัญญาประดิษฐ์ (Artificial Intelligence) มาใช้ในองค์กรมีเป้าหมายเพื่อเพิ่มประสิทธิภาพในการดำเนินงานและสร้างคุณค่าใหม่ ๆ จากข้อมูลและการวิเคราะห์เชิงลึก เพื่อให้เกิดกรอบการทำงานที่สามารถออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ รวมถึงการจัดการทรัพยากรต่าง ๆ

ภายในองค์กรในลักษณะที่สามารถตอบสนองต่อการเปลี่ยนแปลงและภัยคุกคามต่าง ๆ ได้อย่างรวดเร็วและแม่นยำ (X. Han et al., 2021) องค์ประกอบหลักของ สถาปัตยกรรมองค์กร

ปัญญาประดิษฐ์ ประกอบด้วยการกำหนดกลยุทธ์ปัญญาประดิษฐ์ ที่สอดคล้องกับเป้าหมายขององค์กร การจัดการข้อมูลที่จำเป็นสำหรับการฝึกสอนและการใช้งานปัญญาประดิษฐ์ รวมถึงการออกแบบและพัฒนาโมเดลปัญญาประดิษฐ์ และแพลตฟอร์มที่ใช้ในการสร้างและจัดการโมเดลเหล่านั้น การรวมปัญญาประดิษฐ์เข้ากับระบบที่มีอยู่ การควบคุมและการจัดการคุณภาพของโมเดลปัญญาประดิษฐ์ และการจัดการความเสี่ยงที่เกี่ยวข้อง นอกจากนี้ยังรวมถึงการใช้ปัญญาประดิษฐ์ เพื่อสนับสนุนการตัดสินใจเชิงกลยุทธ์ การสร้างรายงาน และการปรับปรุงอย่างต่อเนื่องเพื่อให้แน่ใจว่าระบบปัญญาประดิษฐ์ทำงานได้ตามความต้องการขององค์กร การรวมองค์ประกอบเหล่านี้เข้าด้วยกันช่วยให้สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ สามารถเพิ่มประสิทธิภาพในการดำเนินงานและสร้างคุณค่าใหม่ ๆ ให้กับองค์กรอย่างมีประสิทธิภาพ การรวมระหว่างปัญญาประดิษฐ์กับสถาปัตยกรรมองค์กรจึงเป็นการสร้างความสามารถในการตอบสนองต่อความเปลี่ยนแปลงและภัยคุกคามในโลกดิจิทัลได้อย่างรวดเร็ว ช่วยเสริมสร้างภูมิคุ้มกันดิจิทัล (Digital Immunity) เพื่อป้องกันและบริหารจัดการความเสี่ยงทางไซเบอร์ที่อาจเกิดขึ้นกับสถาบันอุดมศึกษา (Krauze & Grabis, 2024a)

จากภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นและมีความซับซ้อนซึ่งก่อให้เกิดความเสียหายหลายด้าน เช่น ทางการเงินและข้อมูลสำหรับสถาบันอุดมศึกษา ความเสี่ยงเหล่านี้เกิดจากการขาดการป้องกันที่มีประสิทธิภาพและความสามารถในการตอบสนองต่อการโจมตีที่รวดเร็วและรุนแรง การจัดการภูมิคุ้มกันดิจิทัลที่ไม่เพียงพออาจทำให้ข้อมูลสำคัญรั่วไหล เกิดการเสียหายของระบบ และผลกระทบต่อความเชื่อมั่นของนักศึกษาและผู้มีส่วนเกี่ยวข้อง เพื่อให้สถาบันอุดมศึกษามีการจัดการภูมิคุ้มกันดิจิทัลอย่างมีประสิทธิภาพ

จากที่กล่าวมาข้างต้นผู้วิจัยจึงมีแนวคิดในการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) ขึ้นมาเป็นเครื่องมือหลักในการพัฒนาและเสริมสร้างระบบความปลอดภัยทางไซเบอร์ การรวมปัญญาประดิษฐ์เข้ากับโครงสร้างพื้นฐานของมหาวิทยาลัยช่วยให้สามารถตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ ปัญญาประดิษฐ์สามารถใช้ในการวิเคราะห์ข้อมูลเชิงลึกเพื่อคาดการณ์และป้องกันการโจมตี การเรียนรู้ของเครื่องช่วยในการพัฒนาระบบที่สามารถเรียนรู้จากพฤติกรรมของภัยคุกคามและปรับกลยุทธ์การป้องกันให้ทันสมัยอยู่เสมอ นอกจากนี้ การนำสถาปัตยกรรมองค์กรมาใช้ยังช่วยในการออกแบบและจัดการระบบความปลอดภัยที่สอดคล้องกับกลยุทธ์ของมหาวิทยาลัย เพื่อให้การจัดการภูมิคุ้มกันดิจิทัลเป็นไปอย่างมีระเบียบและสามารถตอบสนองต่อการเปลี่ยนแปลงของสภาพแวดล้อมทางไซเบอร์ได้อย่างมีประสิทธิภาพ โดยการเสริมสร้างการป้องกันและการตอบสนองที่มีประสิทธิภาพจะช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และปกป้องข้อมูลสำคัญของมหาวิทยาลัยได้อย่างยั่งยืน

1.2 วัตถุประสงค์การวิจัย

1.2.1 เพื่อวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.2.2 เพื่อสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.2.3 เพื่อพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.2.4 เพื่อประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.3 ขอบเขตของการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยแบบผสมผสาน (Mixed-Methodology Research) ประกอบไปด้วย การวิจัยเชิงปริมาณ (Quantitative Research) และการวิจัยเชิงคุณภาพ (Qualitative Research)

1.3.1 ประชากรและกลุ่มตัวอย่าง

1.3.1.1 การวิจัยเชิงปริมาณ (Quantitative Research) ประชากรที่ใช้ในการวิจัย ได้แก่ บุคลากรในสถาบันอุดมศึกษา สังกัดสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) จำนวนทั้งสิ้น 500 คน

1.3.1.2 การวิจัยเชิงคุณภาพ (Qualitative Research) ผู้ให้ข้อมูลหลัก ประกอบด้วย 1. ผู้บริหารระดับสูง 2. ผู้เชี่ยวชาญด้านโครงสร้างองค์กร 3. ผู้เชี่ยวชาญด้านเทคโนโลยีอัจฉริยะ 4. ผู้เชี่ยวชาญด้านระบบภูมิคุ้มกันดิจิทัล 5.ผู้เชี่ยวชาญด้านการจัดการองค์กรดิจิทัล 6. ผู้เชี่ยวชาญด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และ 7. ผู้เชี่ยวชาญด้านการจัดการภูมิคุ้มกันดิจิทัล

1.3.2 ตัวแปรที่ใช้ในการศึกษาจากการวิจัยเชิงปริมาณ (Quantitative Research) แบ่งเป็น 2 ประเภท

1.3.2.1 ตัวแปรอิสระ (Independent Variable) ได้แก่ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.3.2.1 ตัวแปรตาม (Dependent Variable) ได้แก่ ระดับปัจจัยที่มีอิทธิพลต่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ซึ่งวัดเป็นแบบมาตราส่วนประมาณค่า (Rating Scale) ตัวแปรจำแนกเป็น 2 ลักษณะ ได้แก่

1.3.2.2.1 ตัวแปรเชิงสังเกต (Observed Variable) ได้แก่ ตัวแปรที่ได้จากการรวบรวม ประมวลเนื้อหาของปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

1.3.2.2.2 ตัวแปรแฝง (Latent Variable) ได้แก่ ตัวแปรที่ได้จากการรวบรวมข้อมูลจากตัวแปรเชิงสังเกตเป็นตัวแปรแฝงภายใน (Endogenous Latent Variable) ประกอบด้วย สถาปัตยกรรมองค์กร เทคโนโลยีปัญญาประดิษฐ์ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.3.3 ขอบเขตพื้นที่เชิงปริมาณ เก็บตัวอย่างจากบุคลากรในสถาบันอุดมศึกษา

1.3.4 ระยะเวลาในการเก็บรวบรวมข้อมูลโดยการส่งแบบสอบถามเก็บข้อมูลในรูปแบบออนไลน์ ดำเนินการในระหว่างเดือน เมษายน - มิถุนายน 2568

1.4 คำถามวิจัย

1.4.1 ปัจจัยใดบ้างที่มีอิทธิพลต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

1.4.2 แบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สามารถอธิบายความสัมพันธ์ระหว่างปัจจัยต่างๆในการจัดการความปลอดภัยดิจิทัลได้อย่างมีนัยสำคัญ

1.4.3 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์สามารถสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.4.4 ผลการประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาอยู่ในระดับใด

1.5 สมมติฐานการวิจัย

1.5.1 H1: โครงสร้างองค์กรมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สำหรับสถาบันอุดมศึกษา

1.5.2 H2: โครงสร้างองค์กรมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.5.3 H3: เทคโนโลยีอัจฉริยะมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สำหรับสถาบันอุดมศึกษา

1.5.4 H4: เทคโนโลยีอัจฉริยะมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.5.5 H5: ระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สำหรับสถาบันอุดมศึกษา

1.5.6 H6: ระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.5.7 H7: การจัดการองค์กรดิจิทัลมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สำหรับสถาบันอุดมศึกษา

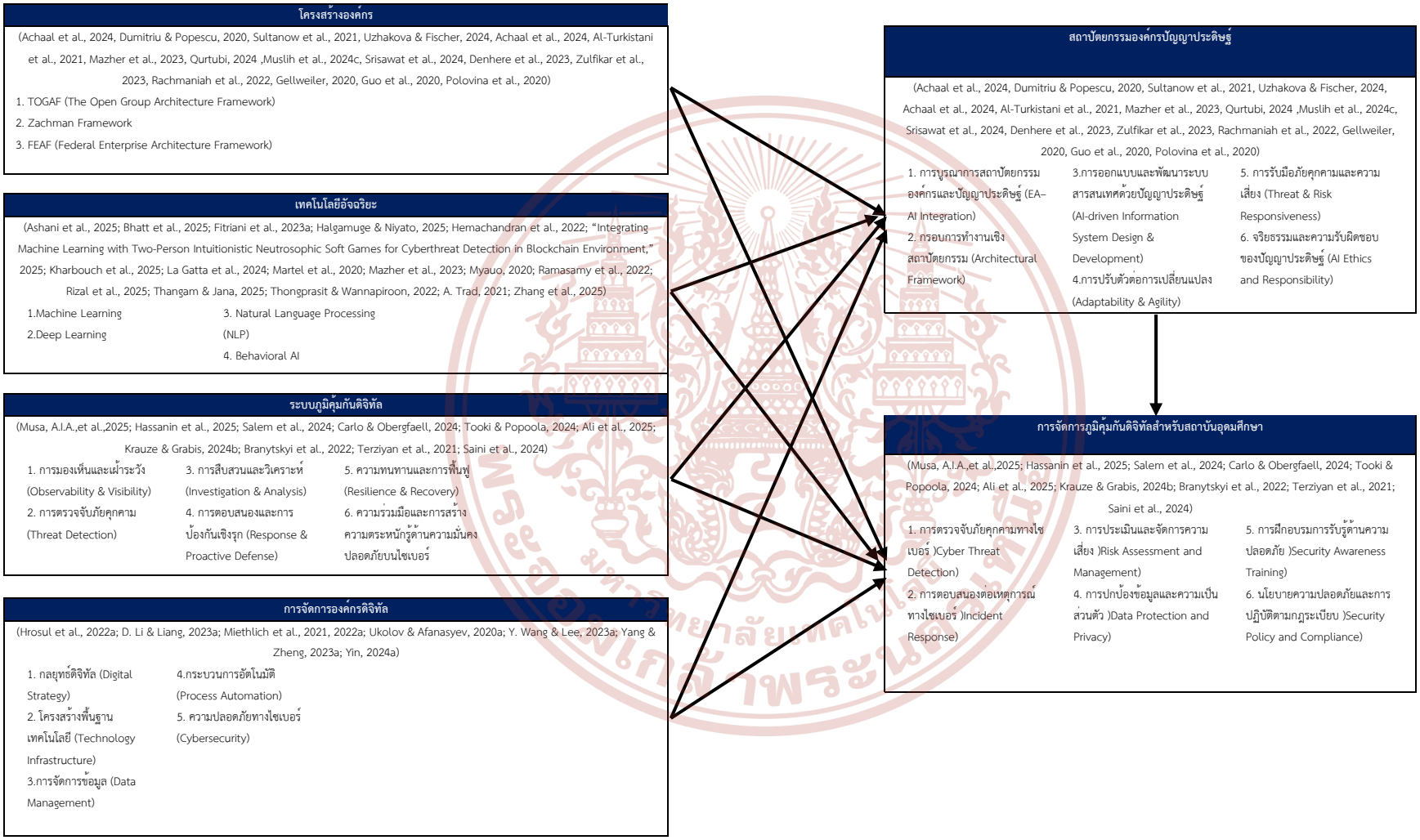
1.5.8 H8: การจัดการองค์กรดิจิทัลมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.5.9 H9: การจัดการภูมิคุ้มกันดิจิทัลได้รับอิทธิพลทั้งทางตรงและทางอ้อมจากโครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล และการจัดการองค์กรดิจิทัล โดยมีสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เป็นตัวแปรส่งผ่านอิทธิพล

1.6 กรอบแนวคิดการวิจัย

การศึกษาและสังเคราะห์กรอบแนวคิดการวิจัยของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยแบ่งเป็นองค์ประกอบหลัก แสดงดังภาพที่ 1

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ภาพที่ 1-1 กรอบแนวคิดการวิจัยของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

จากภาพที่ 1-1 แสดงถึงแนวคิดทฤษฎีที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ประกอบด้วย โครงสร้างองค์กร (Organizational Structure) เทคโนโลยีอัจฉริยะ (Intelligent Technology) ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity) การจัดการองค์กรดิจิทัล (Digital Enterprise Management) สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) จากนั้นทำการวิเคราะห์สังเคราะห์เพื่อหาปัจจัยที่มีอิทธิพลต่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา เพื่อสร้างแบบจำลองสมการโครงสร้างการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาและผลลัพธ์ที่ได้นำไปพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1.7.1 สถาบันอุดมศึกษามีสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

1.7.2 สถาบันอุดมศึกษาสามารถตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

1.7.3 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสามารถนำไปเป็นต้นแบบในการพัฒนาระบบรักษาความปลอดภัยให้กับสถาบันการศึกษาทุกระดับได้

1.8 นิยามศัพท์เฉพาะ

1.8.1 โครงสร้างองค์กร (Organizational Structure) หมายถึง กรอบแนวคิดที่ใช้ในการออกแบบ พัฒนา และจัดการระบบและกระบวนการภายในองค์กรอย่างเป็นระบบ โดยมีการบูรณาการด้านต่าง ๆ ทั้งด้านธุรกิจ ข้อมูล เทคโนโลยี และการจัดการทรัพยากรที่สำคัญ โดยสถาปัตยกรรมองค์กรมีบทบาทในการสร้างความเข้าใจที่ชัดเจนเกี่ยวกับการดำเนินงานในปัจจุบันและวิสัยทัศน์ในอนาคตขององค์กร ช่วยให้ผู้บริหารสามารถวางแผนและตัดสินใจเกี่ยวกับการนำเทคโนโลยีไปใช้อย่างมีประสิทธิภาพ นอกจากนี้สถาปัตยกรรมองค์กรยังครอบคลุมถึงการจัดการเปลี่ยนแปลง การกำกับดูแล และการกำหนดกลยุทธ์ที่สามารถปรับตัวให้สอดคล้องกับสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงอย่างรวดเร็ว เช่นเดียวกับการรับมือกับความต้องการและความท้าทายใหม่ ๆ ซึ่งช่วยให้องค์กรสามารถตอบสนองต่อโอกาสทางธุรกิจและการพัฒนานวัตกรรมได้อย่างมีประสิทธิภาพและยั่งยืน

1.8.2 เทคโนโลยีอัจฉริยะ (Intelligent Technology) หมายถึง เทคโนโลยีที่พัฒนาให้ระบบคอมพิวเตอร์หรือเครื่องจักรสามารถทำงานที่ต้องใช้ความสามารถทางสติปัญญาของมนุษย์ เช่น การ

เรียนรู้ การคิดวิเคราะห์ และการตัดสินใจ ปัญญาประดิษฐ์ถูกแบ่งออกเป็นหลายประเภท เช่น การเรียนรู้ของเครื่อง (Machine Learning) และการเรียนรู้เชิงลึก (Deep Learning) โดยมีบทบาทสำคัญในการเพิ่มประสิทธิภาพในการทำงาน ช่วยในการวิเคราะห์ข้อมูลจำนวนมาก และทำให้กระบวนการต่าง ๆ เป็นอัตโนมัติ การนำปัญญาประดิษฐ์มาใช้ในองค์กรช่วยให้การจัดการและดำเนินงานในหลายด้านเป็นไปอย่างมีประสิทธิภาพ ลดข้อผิดพลาด และปรับปรุงการตัดสินใจ

1.8.3 ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity) หมายถึง ระบบและกลไกเชิงรุกที่ใช้เทคโนโลยีอัจฉริยะและมาตรการด้านความปลอดภัย เพื่อเสริมสร้างความปลอดภัย ความทนทาน และความสามารถในการฟื้นฟูของระบบดิจิทัล ให้สามารถตรวจจับ ป้องกัน ตอบสนอง และฟื้นตัวจากภัยคุกคามได้อย่างมีประสิทธิภาพ โดยมีเป้าหมายเพื่อรักษาความต่อเนื่อง ความมั่นคง และความยั่งยืนในการดำเนินงานขององค์กร

1.8.4 การจัดการองค์กรดิจิทัล (Digital Enterprise Management) หมายถึง การบริหารจัดการองค์กรแบบบูรณาการ โดยใช้เทคโนโลยีดิจิทัลและระบบสารสนเทศเพื่อเพิ่มประสิทธิภาพในการดำเนินงาน พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีและนวัตกรรมให้รองรับการเติบโตขององค์กรในยุคดิจิทัล รวมถึงการปรับตัวให้เข้ากับการเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็ว

1.8.5 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) หมายถึง การบูรณาการสถาปัตยกรรมองค์กร กับปัญญาประดิษฐ์ เพื่อให้เกิดกรอบการทำงานที่สามารถออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ รวมถึงการจัดการทรัพยากรต่าง ๆ ภายในองค์กรในลักษณะที่สามารถตอบสนองต่อการเปลี่ยนแปลงและภัยคุกคามต่างๆ ได้อย่างรวดเร็วและแม่นยำ

1.8.6 การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) หมายถึง แนวทางการสร้างและพัฒนาระบบที่มีความสามารถในการตอบสนองต่อภัยคุกคามไซเบอร์ โดยมุ่งเน้นการใช้เทคโนโลยีและวิธีการที่ช่วยเสริมสร้างภูมิคุ้มกันให้กับข้อมูลและโครงสร้างพื้นฐานดิจิทัล เพื่อป้องกันและลดความเสี่ยงจากการโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต โดยการจัดการภูมิคุ้มกันดิจิทัลมักใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และการเรียนรู้ของเครื่อง (Machine Learning) ในวิเคราะห์และตรวจจับพฤติกรรมที่อาจเป็นภัยคุกคาม รวมถึงการพัฒนาแบบจำลองที่สามารถคาดการณ์การโจมตีในอนาคตได้อย่างมีประสิทธิภาพ การจัดการภูมิคุ้มกันดิจิทัลนี้ถือเป็นกลยุทธ์ที่สำคัญในการสร้างความมั่นคงและเสริมสร้างความปลอดภัยให้กับองค์กรหรือสถาบันในยุคที่เทคโนโลยีและการสื่อสารมีความซับซ้อนและพัฒนาอย่างรวดเร็ว

1.8.7 สถาบันอุดมศึกษา (Higher Education Institution) หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาในระดับปริญญาตรีและสูงกว่า โดยมีเป้าหมายในการพัฒนาความรู้ ทักษะ และคุณสมบัติของนักศึกษา เพื่อเตรียมความพร้อมให้กับนักศึกษาสำหรับการทำงานในตลาดแรงงาน รวมถึงการมีส่วนร่วมในสังคมและการพัฒนาทางเศรษฐกิจและวัฒนธรรม

พระจอมเกล้าพระนครเหนือ มหาวิทยาลัยเทคโนโลยี

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่อง สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ผู้วิจัยได้ศึกษา แนวคิด ทฤษฎี เอกสาร ตำรา และงานวิจัยต่างๆ เพื่อนำข้อมูลที่ได้มาประกอบการจัดทำโดยแยกเป็นหัวข้อดังนี้

2.1. โครงสร้างองค์กร (Organizational Structure)
2.2. เทคโนโลยีอัจฉริยะ (Intelligent Technology)
2.3. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture)
2.4. ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity)
2.5. การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)
2.6. การจัดการองค์กรดิจิทัล (Digital Enterprise Management)
2.7. สถาบันอุดมศึกษา (Higher Education Institution)
2.8. สรุปเอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 โครงสร้างองค์กร (Organizational Structure)

2.1.1 ความหมาย

โครงสร้างองค์กร (Organizational Structure) หมายถึง แนวคิดและกระบวนการในการกำหนดโครงสร้าง รูปแบบการดำเนินงาน และการจัดวางองค์ประกอบภายในองค์กร เพื่อให้สามารถบริหารจัดการทรัพยากร บุคลากร กระบวนการ และเทคโนโลยีได้อย่างมีประสิทธิภาพ โดยมีจุดมุ่งหมายเพื่อให้เกิดความสอดคล้องระหว่างกลยุทธ์ทางธุรกิจและการดำเนินงานขององค์กร การออกแบบองค์กรช่วยให้องค์กรมองเห็นภาพรวมของโครงสร้างและบทบาทหน้าที่ต่าง ๆ อย่างเป็นระบบ มีการเชื่อมโยงระหว่างหน่วยงาน กระบวนการทำงาน และการใช้เทคโนโลยีอย่างชัดเจน ส่งผลให้องค์กรสามารถกำหนดความสัมพันธ์ระหว่างองค์ประกอบต่าง ๆ ได้อย่างเหมาะสม นอกจากนี้ยังสนับสนุนการตัดสินใจเชิงกลยุทธ์ การเพิ่มประสิทธิภาพการดำเนินงาน และการจัดสรรทรัพยากรให้สอดคล้องกับเป้าหมายระยะยาวขององค์กร อีกทั้งยังเป็นกลไกสำคัญในการรองรับการเปลี่ยนแปลงและการพัฒนาองค์กรในบริบทของยุคดิจิทัลที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว (Takeuchi et al., 2024a)

โครงสร้างองค์กร หมายถึง กรอบการทำงานที่ครอบคลุม และมุ่งเน้นการจัดการและออกแบบโครงสร้างขององค์กรในหลากหลายมิติ มีการเชื่อมโยงกับเทคโนโลยีสารสนเทศ ข้อมูล กระบวนการทำงาน และบุคลากร โดยมีเป้าหมายหลักเพื่อเสริมสร้างความสามารถในการบรรลุเป้าหมายทางธุรกิจและการดำเนินงานอย่างมีประสิทธิภาพ ผ่านการวางแผนและการดำเนินการที่มีความเชื่อมโยงกันในทุกระดับ สถาปัตยกรรมองค์กรช่วยให้องค์กรสามารถรวมกลยุทธ์ทางธุรกิจกับเทคโนโลยีดิจิทัลได้อย่างลงตัว ส่งผลให้เกิดการพัฒนาประสิทธิภาพการทำงาน การลดต้นทุน และการเพิ่มศักยภาพในการแข่งขันในตลาด โดยเฉพาะในยุคดิจิทัลที่องค์กรต้องการปรับตัวและสร้างความได้เปรียบทางการแข่งขันอย่างต่อเนื่อง กรอบการทำงานนี้ยังช่วยสนับสนุนการตัดสินใจอย่างรอบคอบ การบริหารทรัพยากรอย่างมีประสิทธิผล และการสร้างนวัตกรรมที่ตอบสนองต่อความต้องการของตลาดที่เปลี่ยนแปลงอย่างรวดเร็ว (Srisawat et al., 2023)

โครงสร้างองค์กร หรือสถาปัตยกรรมองค์กร (Enterprise Architecture) หมายถึง เครื่องมือเชิงกลยุทธ์ที่ช่วยองค์กรในการจัดการและออกแบบระบบสารสนเทศอย่างมีประสิทธิภาพ โดยมุ่งเน้นการวางแผนโครงสร้างและการจัดการองค์ประกอบต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อให้สามารถตอบสนองและสนับสนุนวัตถุประสงค์ทางธุรกิจและกลยุทธ์โดยรวมขององค์กรได้อย่างเหมาะสม การนำสถาปัตยกรรมองค์กรมาใช้ช่วยให้องค์กรสามารถวิเคราะห์และจัดลำดับความสำคัญของทรัพยากร IT เพื่อเพิ่มคุณค่าและประสิทธิภาพในการดำเนินงาน นอกจากนี้ยังช่วยสร้างความสอดคล้องระหว่างระบบสารสนเทศกับกระบวนการทางธุรกิจ ทำให้องค์กรสามารถรับมือกับความเปลี่ยนแปลงได้อย่างมีประสิทธิภาพและรวดเร็ว ทั้งนี้ สถาปัตยกรรมองค์กรยังเป็นพื้นฐานสำคัญในการสร้างนวัตกรรมทางเทคโนโลยีและการปรับตัวให้เข้ากับสภาพแวดล้อมทางธุรกิจที่มีการเปลี่ยนแปลงอย่างต่อเนื่องในยุคดิจิทัล (Muslih et al., 2024a)

โครงสร้างองค์กร หมายถึง แนวทางที่มุ่งเน้นการออกแบบและจัดโครงสร้างองค์กรในทุกแง่มุมอย่างครอบคลุม ตั้งแต่กระบวนการทำงาน ระบบเทคโนโลยีสารสนเทศ ไปจนถึงการจัดการข้อมูล เพื่อให้ทุกองค์ประกอบภายในองค์กรทำงานร่วมกันอย่างเป็นระบบและสอดคล้องกับเป้าหมายและกลยุทธ์ระยะยาว การจัดการดังกล่าวช่วยให้องค์กรสามารถบูรณาการทรัพยากรและความสามารถต่าง ๆ ได้อย่างมีประสิทธิภาพ และตอบสนองต่อความเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจได้อย่างรวดเร็ว นอกจากนี้ สถาปัตยกรรมองค์กรยังช่วยสร้างความเชื่อมโยงระหว่างกลยุทธ์และการปฏิบัติงานในระดับปฏิบัติการ ช่วยลดความซ้ำซ้อนและข้อผิดพลาดในกระบวนการทำงาน ขณะเดียวกันยังส่งเสริมการตัดสินใจที่อิงข้อมูลเชิงลึกเพื่อการพัฒนาและนวัตกรรมในระยะยาวขององค์กร (Atencio et al., 2024a)

โครงสร้างองค์กร หมายถึง กรอบการทำงานที่ออกแบบมาเพื่อจัดการและปรับโครงสร้างของธุรกิจให้สามารถรับมือกับสถานการณ์วิกฤต เช่น การระบาดของ COVID-19 ได้อย่างมีประสิทธิภาพ โดยมุ่งเน้นการบูรณาการเทคโนโลยีดิจิทัลและกระบวนการทางธุรกิจให้ทำงานร่วมกันอย่างสอดคล้อง เพื่อสร้างความยืดหยุ่นในการดำเนินงานและความต่อเนื่องของธุรกิจ ช่วยให้ธุรกิจสามารถปรับตัวกับความเปลี่ยนแปลงในสภาพแวดล้อมภายนอก เช่น การเปลี่ยนพฤติกรรมผู้บริโภคหรือข้อจำกัดทางกฎหมาย พร้อมทั้งสนับสนุนการนำโซลูชันดิจิทัล เช่น ระบบสั่งอาหารออนไลน์หรือการจัดการคลังสินค้าอัตโนมัติ มาช่วยเพิ่มประสิทธิภาพ กระตุ้นการสร้างรายได้ และลดความสูญเสีย การวางแผนและการดำเนินการที่ยึดตามหลักการของสถาปัตยกรรมองค์กรในลักษณะนี้จึงเป็นรากฐานสำคัญสำหรับธุรกิจร้านอาหารที่ต้องการเติบโตและดำรงอยู่ในสถานการณ์ที่มีความไม่แน่นอนสูง (Rave-Gómez et al., 2024)

โครงสร้างองค์กร หมายถึง กรอบการทำงานที่มุ่งเน้นการออกแบบโครงสร้างและระบบที่ครอบคลุมทุกภาคส่วนภายในองค์กรด้านสุขภาพ ตั้งแต่กระบวนการทำงาน ระบบข้อมูล ไปจนถึงการบริหารจัดการทรัพยากรต่าง ๆ ทั้งด้านบุคลากร งบประมาณ และเทคโนโลยี โดยมีเป้าหมายเพื่อสนับสนุนการดูแลผู้ป่วยอย่างมีประสิทธิภาพ การออกแบบนี้ช่วยให้เกิดการเชื่อมโยงที่ชัดเจนและสอดคล้องระหว่างผู้มีส่วนได้ส่วนเสีย ไม่ว่าจะเป็นบุคลากรทางการแพทย์ หน่วยงานที่เกี่ยวข้อง หรือระบบเทคโนโลยีสารสนเทศที่นำมาใช้ในการจัดการข้อมูลผู้ป่วย การประสานงานที่ดีระหว่างภาคส่วนต่าง ๆ จะช่วยลดความซับซ้อน เพิ่มความรวดเร็วในการบริการ และยกระดับคุณภาพการดูแลสุขภาพ และยังเป็นเครื่องมือสำคัญที่ช่วยให้หน่วยงานด้านสุขภาพสามารถปรับตัวต่อการเปลี่ยนแปลง เช่น การนำระบบดิจิทัลมาใช้หรือการตอบสนองต่อสถานการณ์ฉุกเฉิน เช่น โรคระบาดหรือวิกฤตสุขภาพ (Nakakawa et al., 2024)

โครงสร้างองค์กร หมายถึง กรอบการทำงานที่มุ่งเน้นการออกแบบโครงสร้างองค์กรและระบบสารสนเทศ เพื่อสนับสนุนการวิเคราะห์ การจัดการ และการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะในโครงสร้างพื้นฐานที่มีความสำคัญ เช่น ระบบไฟฟ้า การสื่อสาร และการขนส่ง การใช้สถาปัตยกรรมองค์กรในด้านนี้เน้นการสร้างแบบจำลอง (EA Modeling) ที่ครอบคลุมทุกมิติของการจัดการความปลอดภัย ไม่ว่าจะเป็นการวางแผนเชิงกลยุทธ์ การประเมินและจัดลำดับความเสี่ยง การระบุช่องโหว่ และการพัฒนามาตรการป้องกันภัยคุกคามอย่างมีระบบ สถาปัตยกรรมนี้ช่วยให้องค์กรสามารถบูรณาการข้อมูล เทคโนโลยี และกระบวนการปฏิบัติงานเข้าด้วยกัน เพื่อสร้างความพร้อมในการตอบสนองต่อเหตุการณ์ทางไซเบอร์ที่อาจเกิดขึ้น อีกทั้งยังช่วยในการปรับปรุงมาตรการป้องกันอย่างต่อเนื่อง เพื่อให้มั่นใจว่าระบบโครงสร้างพื้นฐานสำคัญขององค์กรยังคงดำเนินการได้อย่างมั่นคง ปลอดภัย และมีประสิทธิภาพในทุกสถานการณ์ (Y. Jiang et al., 2024a)

โครงสร้างองค์กร หมายถึง กรอบการทำงานที่มุ่งเน้นการออกแบบและจัดการโครงสร้างที่ช่วยสนับสนุนการพัฒนาแพลตฟอร์มดิจิทัลและบริการที่เกี่ยวข้อง เพื่อให้เมืองสามารถเปลี่ยนผ่านไปสู่ความเป็นเมืองอัจฉริยะได้อย่างมีประสิทธิภาพ โดยกรอบการทำงานนี้ทำหน้าที่เป็นตัวกลางที่เชื่อมโยงและบูรณาการองค์ประกอบต่าง ๆ ทั้งในเชิงดิจิทัล เช่น ระบบข้อมูล การสื่อสาร เทคโนโลยี IoT และในเชิงกายภาพ เช่น โครงสร้างพื้นฐาน พื้นที่เมือง และทรัพยากรต่าง ๆ เพื่อสร้างความสอดคล้องและประสิทธิภาพในกระบวนการจัดการทรัพยากรของเมือง ช่วยให้เกิดความโปร่งใสในระบบข้อมูล การปรับปรุงกระบวนการทำงาน และการจัดการทรัพยากรของเมืองอย่างเหมาะสม เพื่อรองรับการดำรงชีวิตของประชากรในยุคดิจิทัล นอกจากนี้ยังช่วยพัฒนาโซลูชันที่ยืดหยุ่นและตอบสนองต่อความต้องการของประชาชน รวมถึงการจัดการปัญหาทางสังคมและสิ่งแวดล้อมอย่างมีประสิทธิภาพ (Anthony Jnr et al., 2021)

โครงสร้างองค์กร หมายถึง กรอบการทำงานที่มีบทบาทสำคัญในการออกแบบและจัดโครงสร้างองค์ประกอบต่าง ๆ ขององค์กร ไม่ว่าจะเป็นกระบวนการทางธุรกิจ ระบบเทคโนโลยีสารสนเทศ ข้อมูล และบุคลากร โดยมีเป้าหมายเพื่อสร้างความบูรณาการและการทำงานร่วมกันอย่างเป็นระบบและมีประสิทธิภาพ สถาปัตยกรรมองค์กรถูกออกแบบให้สอดคล้องกับเป้าหมายทางกลยุทธ์ขององค์กร ช่วยให้องค์กรสามารถดำเนินการตามเป้าหมายได้อย่างมีประสิทธิผล พร้อมทั้งสามารถปรับตัวให้เข้ากับความเปลี่ยนแปลงที่เกิดขึ้นในสภาพแวดล้อมทางธุรกิจและเทคโนโลยีได้อย่างเหมาะสม กรอบการทำงานนี้ยังช่วยสนับสนุนการวางแผนและการตัดสินใจในระดับยุทธศาสตร์ โดยมุ่งเน้นการรักษาความสอดคล้องระหว่างกลยุทธ์ กระบวนการ และเทคโนโลยีที่ใช้ในองค์กร นอกจากนี้โครงสร้างองค์กรอย่างต่อเนื่องยังช่วยให้องค์กรสามารถตอบสนองต่อความต้องการใหม่ ๆ ของตลาดและผู้มีส่วนได้ส่วนเสียได้อย่างรวดเร็วและยืดหยุ่น ส่งผลให้สามารถสร้างความได้เปรียบในการแข่งขันในระยะยาว (Costa & Brito, 2022)

โครงสร้างองค์กร หมายถึง กระบวนการที่มีเป้าหมายในการจัดระเบียบและเชื่อมโยงทรัพยากรต่าง ๆ ขององค์กร เช่น เทคโนโลยีสารสนเทศ ข้อมูล และกระบวนการทางธุรกิจ เพื่อให้สามารถสร้างความเข้าใจที่ชัดเจนเกี่ยวกับโครงสร้างการทำงานขององค์กร ซึ่งช่วยในการกำหนดแนวทางในการวางแผนและจัดการการเปลี่ยนแปลงในองค์กรได้อย่างมีประสิทธิภาพ โดยการใช้โครงสร้างองค์กรช่วยให้สามารถระบุและปรับปรุงจุดอ่อนในระบบต่าง ๆ ขององค์กร เช่น การลดความซ้ำซ้อนในกระบวนการทางธุรกิจ การเพิ่มประสิทธิภาพการทำงาน และการพัฒนาระบบการทำงานที่สามารถตอบสนองได้ดีในสภาพแวดล้อมที่เปลี่ยนแปลง นอกจากนี้ สถาปัตยกรรมองค์กรยังช่วยในการลดความเสี่ยงด้านความปลอดภัยไซเบอร์ ด้วยการกำหนดกรอบในการจัดการความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในระบบองค์กร และยังเสริมสร้างความสามารถในการฟื้นตัวของ

องค์กรจากสถานการณ์วิกฤตต่าง ๆ โดยการออกแบบที่ยืดหยุ่นและสามารถปรับตัวให้เหมาะสมกับการเปลี่ยนแปลงได้อย่างรวดเร็ว (Al-Turkistani et al., 2021a)

2.1.2 กรอบแนวคิดของโครงสร้างองค์กร

2.1.2.1 TOGAF (The Open Group Architecture Framework) หมายถึง กรอบแนวคิดที่ใช้ในการพัฒนาสถาปัตยกรรมองค์กร โดยเน้นการกำหนดวิธีการและเครื่องมือที่จำเป็นในการออกแบบ พัฒนา และจัดการสถาปัตยกรรมองค์กรอย่างเป็นระบบ ซึ่งช่วยให้องค์กรสามารถสร้างโครงสร้างที่ชัดเจนและเหมาะสมกับเป้าหมายทางธุรกิจ TOGAF ประกอบด้วย Architecture Development Method (ADM) ซึ่งเป็นกระบวนการที่มีลำดับขั้นตอนชัดเจนในการพัฒนาสถาปัตยกรรมองค์กร (Rujira et al., 2021) โดยเริ่มตั้งแต่การวิเคราะห์และการกำหนดขอบเขต ไปจนถึงการออกแบบและการนำไปใช้จริงในองค์กร กระบวนการ ADM ของ TOGAF จะช่วยให้สามารถจัดการและพัฒนาสถาปัตยกรรมได้อย่างมีประสิทธิภาพ โดยการทำงานร่วมกันระหว่างทีมต่าง ๆ ภายในองค์กร เช่น ทีมไอที ทีมธุรกิจ และทีมการจัดการ เพื่อให้สถาปัตยกรรมที่สร้างขึ้นสามารถสนับสนุนการดำเนินงานและการบรรลุเป้าหมายทางธุรกิจได้อย่างยั่งยืน นอกจากนี้ TOGAF ยังช่วยให้สามารถปรับเปลี่ยนและพัฒนาสถาปัตยกรรมองค์กรให้สามารถตอบสนองต่อการเปลี่ยนแปลงของเทคโนโลยีและความต้องการทางธุรกิจได้อย่างมีความยืดหยุ่น (Camatti et al., 2020b; Chandra & Legowo, 2022b; Fitriani et al., 2023b; Jumansyah et al., 2022b; Noranita et al., 2021b)

กรอบสถาปัตยกรรมองค์กร TOGAF (The Open Group Architecture Framework) เป็นหนึ่งในกรอบแนวทางที่ได้รับการยอมรับอย่างแพร่หลายในการออกแบบและจัดการโครงสร้างองค์กร โดยมีการกำหนดองค์ประกอบหลักที่สำคัญ 5 ด้าน ดังนี้

1. ด้านธุรกิจ (Business Architecture) มุ่งเน้นการกำหนดยุทธศาสตร์และกลยุทธ์ขององค์กร (Business Strategy and Tactic) การออกแบบกระบวนการทางธุรกิจ (Business Processes) รวมถึงการบริหารจัดการด้านธรรมาภิบาล (Governance) เพื่อให้การดำเนินงานขององค์กรสอดคล้องกับเป้าหมายเชิงกลยุทธ์

2. ด้านข้อมูล (Data Architecture) อธิบายถึงโครงสร้างของข้อมูลทั้งในระดับตรรกะ (Logical) และระดับกายภาพ (Physical) รวมถึงการใช้เครื่องมือและกระบวนการบริหารจัดการข้อมูลอย่างเป็นระบบ เพื่อสนับสนุนการจัดเก็บ การเข้าถึง และการใช้ประโยชน์จากข้อมูลได้อย่างมีประสิทธิภาพ

3. ด้านแอปพลิเคชัน (Application Architecture) แสดงความสัมพันธ์ระหว่างแอปพลิเคชันกับกระบวนการทางธุรกิจ และการเชื่อมโยงระหว่างแอปพลิเคชันต่าง ๆ ภายในองค์กร เพื่อสร้างการทำงานร่วมกันอย่างเป็นเอกภาพและลดความซ้ำซ้อนของระบบ

4. เทคโนโลยี (Technology Architecture) มุ่งเน้นการนำซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) มาใช้สนับสนุนการจัดการข้อมูล แอปพลิเคชัน และธุรกิจ รวมถึงการวางโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ (IT Infrastructure) เครือข่าย (Network) กระบวนการ (Process) และมาตรฐาน (Standard) ที่เกี่ยวข้อง เพื่อรองรับความต้องการด้านการประมวลผลและการสื่อสาร

5. ด้านความปลอดภัย (Security Architecture) ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของระบบในทุกมิติ ไม่ว่าจะเป็นด้านธุรกิจ แอปพลิเคชัน ข้อมูล หรือโครงสร้างพื้นฐาน โดยอ้างอิงหลักการ GRC ได้แก่ การกำกับดูแล (Governance) การบริหารความเสี่ยง (Risk Management) และความสอดคล้องกับกฎระเบียบ (Compliance) เพื่อสร้างความเชื่อมั่นและความปลอดภัยขององค์กรในภาพรวม



ภาพที่ 2-1 กรอบแนวคิดการออกแบบสถาปัตยกรรมองค์กรแบบ TOGAF (Camatti et al., 2020b)

จากภาพที่ 2-1 แสดงให้เห็นถึงวงจร Architecture Development Method (ADM) ของ The Open Group Architecture Framework (TOGAF) ซึ่งประกอบด้วย 9 ขั้นตอน ดังนี้

1. ระยะเตรียมความพร้อม (Preliminary Phase) เป็นขั้นตอนแรกของกระบวนการพัฒนาสถาปัตยกรรมองค์กรที่มีความสำคัญอย่างยิ่ง เนื่องจากเป็นช่วงที่กำหนดทิศทางและแนวทางการดำเนินงานของโครงการ โดยมีเป้าหมายหลักเพื่อทบทวนบริบทขององค์กร วิเคราะห์ความต้องการและประเมินผลกระทบที่อาจเกิดขึ้นจากการดำเนินโครงการ นอกจากนี้ยังเป็นระยะที่กำหนดบทบาท

และความรับผิดชอบของผู้ที่เกี่ยวข้อง รวมถึงสร้างความเข้าใจร่วมกันระหว่างผู้มีส่วนได้ส่วนเสียเกี่ยวกับวัตถุประสงค์ของโครงการ อีกทั้งยังต้องตรวจสอบการสนับสนุนจากผู้บริหารและความพร้อมของทรัพยากรที่จำเป็น เช่น บุคลากร เทคโนโลยี และเครื่องมือที่ใช้ในการพัฒนา การกำหนดหลักเกณฑ์และแนวทางการดำเนินงาน เพื่อให้มั่นใจว่ากระบวนการพัฒนาสถาปัตยกรรมองค์กรเป็นไปในทิศทางที่เหมาะสมกับโครงสร้างและกลยุทธ์ขององค์กร นอกจากนี้ยังต้องวางแผนเกี่ยวกับเครื่องมือที่จะใช้และกำหนดเกณฑ์สำหรับการประเมินผลสำเร็จของโครงการ ซึ่งทั้งหมดนี้ช่วยให้การดำเนินงานในระยะถัดไปสามารถดำเนินไปได้อย่างมีประสิทธิภาพและบรรลุเป้าหมายที่ตั้งไว้

2. ระยะ A การกำหนดวิสัยทัศน์ต่อสถาปัตยกรรม (Phase A: Architecture Vision) เป็นกระบวนการที่สำคัญในการพัฒนาสถาปัตยกรรมองค์กร โดยมุ่งเน้นให้สอดคล้องกับเป้าหมายทางธุรกิจ ยุทธศาสตร์องค์กร และตัวชี้วัดที่สำคัญ กระบวนการนี้ครอบคลุมการกำหนดแนวทางและวงจรการพัฒนาสถาปัตยกรรมให้เหมาะสมกับบริบทขององค์กร รวมถึงการระบุขอบเขตและบรรทัดฐานของสถาปัตยกรรม ตลอดจนการกำหนดผู้มีส่วนได้เสียและความสัมพันธ์ของพวกเขาต่อการพัฒนาองค์กร นอกจากนี้ ยังต้องวิเคราะห์ความต้องการหลักทางธุรกิจที่มีอิทธิพลต่อการพัฒนาสถาปัตยกรรม และพิจารณาปัจจัยที่ส่งผลต่อแนวทางการดำเนินงาน เพื่อให้สามารถเสริมสร้างมูลค่าให้กับองค์กรได้อย่างมีประสิทธิภาพ ในกระบวนการนี้ยังต้องมีการวางแผนด้านการใช้ทรัพยากร การกำหนดขั้นตอนการดำเนินโครงการ การประเมินและจัดการความเสี่ยง รวมถึงการกำหนดกรอบงบประมาณ เพื่อให้การดำเนินงานมีระบบและมีเสถียรภาพ นอกจากนี้ การกำหนดวิสัยทัศน์ยังช่วยให้เกิดความเข้าใจในผลกระทบที่อาจเกิดขึ้นจากการพัฒนาสถาปัตยกรรมองค์กร โดยมีขั้นตอนสำคัญได้แก่ การจัดตั้งโครงการพัฒนาสถาปัตยกรรมองค์กร การกำหนดผู้มีส่วนได้เสียและความต้องการทางธุรกิจ การตรวจสอบเป้าหมายและปัจจัยสู่ความสำเร็จ การประเมินประสิทธิภาพของกิจกรรมทางธุรกิจ และการตรวจสอบความพร้อมขององค์กรในการปรับเปลี่ยน รวมถึงการกำหนดขอบเขตการดำเนินงาน การกำหนดสถาปัตยกรรมเป้าหมาย ตัวชี้วัด และแนวทางจัดการความเสี่ยง ทั้งหมดนี้มีเป้าหมายเพื่อสร้างกรอบการพัฒนาสถาปัตยกรรมองค์กรที่มั่นคง และสามารถตอบโจทย์เชิงกลยุทธ์ขององค์กรได้อย่างมีประสิทธิภาพ

3. ระยะ B สถาปัตยกรรมธุรกิจ (Phase B: Business Architecture) เป็นกระบวนการกำหนดรายละเอียดของสถาปัตยกรรมธุรกิจเพื่อให้มีโครงสร้างที่ชัดเจนและสอดคล้องกับเป้าหมายทางธุรกิจขององค์กร โดยเริ่มจากการกำหนด สถาปัตยกรรมธุรกิจพื้นฐาน (Base Line Business Architecture) ซึ่งเป็นโครงสร้างปัจจุบันขององค์กร และพัฒนาสู่ สถาปัตยกรรมธุรกิจเป้าหมาย ที่ประกอบไปด้วยผลิตภัณฑ์ ยุทธศาสตร์ และบริการที่สอดคล้องกับทิศทางทางธุรกิจและปัจจัยขับเคลื่อนทางยุทธศาสตร์ กระบวนการนี้ยังครอบคลุมการประเมินช่องว่างระหว่างสถาปัตยกรรมธุรกิจพื้นฐานกับสถาปัตยกรรมเป้าหมาย เพื่อวิเคราะห์ความแตกต่างและวางแนวทางในการปรับปรุง

นอกจากนี้ ยังต้องมีการคัดเลือกและพัฒนามุมมองที่เป็นประโยชน์ต่อผู้มีส่วนได้เสีย รวมถึงการเลือกใช้เครื่องมือและเทคนิคที่เหมาะสมในการพัฒนา มุมมองด้านสถาปัตยกรรมธุรกิจ ขั้นตอนดำเนินการประกอบไปด้วยการคัดเลือกกรอบแนวคิดและเครื่องมือที่ใช้พัฒนา การสร้างรายละเอียดของ สถาปัตยกรรมธุรกิจพื้นฐานและเป้าหมาย การตรวจประเมินช่องว่าง การกำหนดองค์ประกอบสำคัญในการพัฒนาและประเมินผลกระทบที่อาจเกิดขึ้น ตลอดจนการจัดทำข้อเสนอแนะแก่ผู้มีส่วนได้เสีย ทั้งนี้ ยังรวมถึงการจัดทำสรุปสถาปัตยกรรมธุรกิจและการจัดทำเอกสารนิยามเพื่อให้เกิดความเข้าใจและสามารถนำไปใช้ได้อย่างเป็นระบบและมีประสิทธิภาพ

4. ระยะ C ระบบเทคโนโลยีสารสนเทศ (Phase C: Information Systems Architectures) เป็นกระบวนการกำหนดสถาปัตยกรรมด้านโปรแกรมประยุกต์ เพื่อรองรับกระบวนการทางธุรกิจขององค์กร โดยครอบคลุมการออกแบบโครงสร้างและมาตรฐานของโปรแกรมประยุกต์ รวมถึงการเชื่อมต่อระหว่างระบบต่าง ๆ ให้ทำงานร่วมกันได้อย่างมีประสิทธิภาพ วัตถุประสงค์หลักของการพัฒนาสถาปัตยกรรมโปรแกรมประยุกต์ คือการกำหนดหลักการออกแบบและแนวทางการพัฒนา เพื่อให้สามารถรองรับกระบวนการทางธุรกิจได้อย่างเหมาะสม โดยคำนึงถึงตรรกะของกระบวนการทำงาน และความสามารถในการบูรณาการกับระบบอื่น ๆ กระบวนการพัฒนาสถาปัตยกรรมโปรแกรมประยุกต์ประกอบด้วยหลายขั้นตอน เริ่มจากการคัดเลือกมุมมองและเครื่องมือที่เหมาะสมสำหรับการออกแบบสถาปัตยกรรม จากนั้นดำเนินการพัฒนาสถาปัตยกรรมโปรแกรมประยุกต์พื้นฐานและเป้าหมาย รวมถึงการกำหนดรายละเอียดที่เกี่ยวข้อง มีการตรวจประเมินช่องว่างระหว่างสถานะปัจจุบันกับสถาปัตยกรรมเป้าหมายเพื่อนำไปสู่การกำหนดแนวทางพัฒนาและการประเมินผลกระทบของการดำเนินงาน อีกทั้งยังต้องมีการให้คำแนะนำและจัดทำการทบทวนร่วมกับผู้มีส่วนได้เสีย เพื่อให้แน่ใจว่าสถาปัตยกรรมที่พัฒนาขึ้นตอบสนองต่อความต้องการขององค์กรได้อย่างแท้จริง ขั้นสุดท้ายคือการจัดทำสรุปสถาปัตยกรรมโปรแกรมประยุกต์ และการจัดทำเอกสารนิยามเพื่อให้สามารถนำไปใช้งานและพัฒนาต่อยอดได้อย่างมีประสิทธิภาพ

5. ระยะ D สถาปัตยกรรมเทคโนโลยี (Phase D: Technology Architecture) เป็นกระบวนการกำหนดรายละเอียดของเทคโนโลยีที่ใช้ในการสนับสนุนโครงสร้างพื้นฐานของระบบสารสนเทศในองค์กร โดยครอบคลุมทั้งเทคโนโลยีโครงข่ายสื่อสาร ฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่ายข้อมูล วัตถุประสงค์หลักของการพัฒนาสถาปัตยกรรมเทคโนโลยีคือการกำหนดแนวทางการเชื่อมโยงเทคโนโลยีให้สามารถรองรับสถาปัตยกรรมข้อมูล สถาปัตยกรรมระบบสารสนเทศ และโปรแกรมประยุกต์ ได้อย่างมีประสิทธิภาพ เพื่อสร้างความสอดคล้องระหว่างองค์ประกอบทางเทคโนโลยีและความต้องการทางธุรกิจ กระบวนการพัฒนาสถาปัตยกรรมเทคโนโลยีเริ่มต้นจากการคัดเลือกมุมมองที่ใช้อ้างอิงและเครื่องมือที่เหมาะสมสำหรับการออกแบบ จากนั้นดำเนินการพัฒนาสถาปัตยกรรมเทคโนโลยีพื้นฐานและเป้าหมาย รวมถึงรายละเอียดของเทคโนโลยีที่ใช้ในการ

ดำเนินงาน มีการตรวจประเมินช่องว่างระหว่างเทคโนโลยีที่มีอยู่และเทคโนโลยีที่ต้องการในอนาคต เพื่อนำไปสู่ การกำหนดแนวทางการพัฒนาและการประเมินผลกระทบ ที่อาจเกิดขึ้น นอกจากนี้ ยังมีการให้คำแนะนำและจัดทำการทบทวนร่วมกับผู้มีส่วนได้เสีย เพื่อให้แน่ใจว่าสถาปัตยกรรมเทคโนโลยีสามารถตอบสนองความต้องการขององค์กรได้อย่างเหมาะสม ขั้นตอนสุดท้ายคือการจัดทำสรุปสถาปัตยกรรมเทคโนโลยีและการจัดทำเอกสารนิยาม เพื่อเป็นแนวทางในการนำไปใช้งานจริงและพัฒนาต่อยอดในอนาคต

6. ระยะ E โอกาสและแนวทาง (Phase E: Opportunities and Solutions) เป็นกระบวนการกำหนดแนวทางและจัดทำกลยุทธ์เพื่อรองรับโอกาสในการพัฒนาสถาปัตยกรรมองค์กร โดยมีเป้าหมายในการทบทวนวัตถุประสงค์ของสถาปัตยกรรมเป้าหมาย และรวบรวมผลการประเมินช่องว่าง เพื่อเตรียมแผนการพัฒนา นอกจากนี้ ยังมุ่งเน้นการรวบรวมปัจจัยที่ส่งผลต่อการปรับเปลี่ยนและกำหนดกลยุทธ์และรายละเอียดสำหรับการเปลี่ยนแปลง เพื่อให้การดำเนินงานเป็นไปอย่างต่อเนื่องและสอดคล้องกับเป้าหมายทางธุรกิจขององค์กร กระบวนการดำเนินงานของระยะนี้ประกอบด้วย การกำหนดรายละเอียดหลักและองค์ประกอบที่เกี่ยวข้องกับการปรับเปลี่ยนการ ระบุเงื่อนไขและปัจจัยที่มีผลกระทบต่อการดำเนินงาน รวมถึงการทบทวนผลการประเมินช่องว่างจากขั้นตอนที่ผ่านมาเพื่อให้สามารถวิเคราะห์แนวทางแก้ไขได้อย่างมีประสิทธิภาพ นอกจากนี้ มีการทบทวนความต้องการจากหน่วยงานต่าง ๆ เพื่อให้มั่นใจว่าสถาปัตยกรรมที่พัฒนาขึ้นสามารถรองรับการทำงานร่วมกันระหว่างหน่วยงาน อีกขั้นตอนสำคัญคือ การรวบรวมและพิจารณาความต้องการในการเชื่อมต่อของแต่ละหน่วยงาน เพื่อให้มั่นใจว่าโซลูชันที่ออกแบบสามารถรองรับการทำงานแบบบูรณาการได้อย่างสมบูรณ์ จากนั้นดำเนินการตรวจสอบความพร้อมต่อการปรับเปลี่ยน และกำหนดแผนและกลยุทธ์ในการเปลี่ยนแปลง ซึ่งรวมถึงการกำหนดงานหลักที่ต้องดำเนินการ และออกแบบสถาปัตยกรรมที่รองรับการเปลี่ยนแปลง ขั้นตอนสุดท้ายคือการกำหนดรายละเอียดของโครงการให้สอดคล้องกับสถาปัตยกรรมที่ออกแบบไว้ เพื่อให้การดำเนินงานเป็นไปตามแผนที่วางไว้และรองรับการเติบโตขององค์กรในอนาคต

7. ระย F การจัดทำแผนการปรับย้าย (Phase F: Migration Planning) เป็นกระบวนการกำหนดแผนงานเพื่อปรับเปลี่ยนจากสถาปัตยกรรมปัจจุบันไปสู่สถาปัตยกรรมเป้าหมาย โดยมีวัตถุประสงค์หลักเพื่อสร้างความสอดคล้องของแผนงานกับการออกแบบสถาปัตยกรรมองค์กร รวมถึงกำหนดลำดับความสำคัญของแผนงานโครงการ และรวบรวมสรุปวิสัยทัศน์ของการพัฒนาสถาปัตยกรรม พร้อมกับเอกสารที่เกี่ยวข้อง เพื่อให้สามารถดำเนินการได้อย่างเป็นระบบและรองรับการเปลี่ยนแปลงได้อย่างมีประสิทธิภาพ อีกหนึ่งเป้าหมายสำคัญคือ การสร้างแผนงานที่ตอบสนองต่อความต้องการของผู้มีส่วนได้เสีย รวมถึงการกำหนดแนวทางการควบคุมและตรวจสอบที่สอดคล้องกับแผนงานโครงการ เพื่อให้มั่นใจว่าการดำเนินงานเป็นไปในทิศทางที่ถูกต้อง กระบวนการดำเนินงานใน

ระยะนี้ประกอบด้วยการสอบทานและยืนยันความมีส่วนร่วมของผู้บริหารต่อการปรับเปลี่ยน เพื่อให้มั่นใจว่ามีการสนับสนุนจากระดับองค์กร รวมถึงการกำหนดมูลค่าทางธุรกิจของโครงการตามแผนที่วางไว้ นอกจากนี้ยังต้องมีการประเมินทรัพยากรที่ต้องใช้ ไม่ว่าจะเป็นงบประมาณ ระยะเวลา และกำลังคน ขั้นตอนสำคัญอีกประการคือการกำหนดลำดับความสำคัญของแผนงาน โดยพิจารณาทั้ง ต้นทุนและประโยชน์ที่ได้รับ พร้อมกับตรวจสอบความสอดคล้องของแผนงานโครงการกับสถาปัตยกรรมที่ออกแบบ เพื่อให้การดำเนินการเป็นไปอย่างมีทิศทางและสามารถบรรลุเป้าหมายได้ สุดท้ายคือการกำหนดแผนงานพัฒนาสถาปัตยกรรมในรายละเอียดด้านเวลาและการดำเนินงาน รวมถึง การสร้างองค์ความรู้ใหม่เพื่อเป็นนวัตกรรมที่ช่วยให้การเปลี่ยนผ่านสู่สถาปัตยกรรมเป้าหมายเป็นไปอย่างราบรื่นและมีประสิทธิภาพสูงสุด

8. ระยะ G การจัดการต่อการพัฒนาสถาปัตยกรรม (Phase G: Implementation Governance) เป็นกระบวนการกำกับดูแลและบริหารจัดการการพัฒนาสถาปัตยกรรมขององค์กรให้เป็นไปตามแนวทางและเป้าหมายที่กำหนด โดยมีวัตถุประสงค์หลักเพื่อสร้างแนวทางการบริหารจัดการที่ดี และกำหนดบทบาทของผู้เกี่ยวข้องในแต่ละโครงการ เพื่อให้มั่นใจว่าการดำเนินงานสอดคล้องกับกรอบสถาปัตยกรรมขององค์กร รวมถึงสามารถปรับเปลี่ยนแผนงานให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงได้ กระบวนการในระยะนี้ประกอบไปด้วยการกำกับดูแลโครงการ การทบทวนขอบเขตและแผนดำเนินงาน การกำหนดทรัพยากรและทักษะที่จำเป็น การวางแนวทางการพัฒนาและการดำเนินงาน รวมถึงการตรวจสอบความสอดคล้องของแผนงานกับเป้าหมายขององค์กร นอกจากนี้ยังให้ความสำคัญกับการดำเนินกระบวนการทั้งในด้านปฏิบัติงานและด้านธุรกิจ ตลอดจนการเตรียมความพร้อมหลังสิ้นสุดโครงการเพื่อให้มั่นใจว่าการพัฒนาสถาปัตยกรรมสามารถรองรับการดำเนินงานขององค์กรได้อย่างต่อเนื่องและมีประสิทธิภาพ การดำเนินงานในระยะนี้ช่วยลดความเสี่ยงในการเบี่ยงเบนจากแนวทางที่กำหนด และทำให้การพัฒนาสถาปัตยกรรมมีความยืดหยุ่น สามารถปรับตัวให้เหมาะสมกับความต้องการขององค์กรในระยะยาว

9. ระยะ H การบริหารการเปลี่ยนแปลง (Phase H: Architecture Change Management) เป็นกระบวนการบริหารจัดการการเปลี่ยนแปลงของสถาปัตยกรรมองค์กร เพื่อให้มั่นใจว่าสถาปัตยกรรมพื้นฐานยังคงเหมาะสมและสามารถรองรับความต้องการขององค์กรในอนาคตได้ โดยมุ่งเน้นไปที่การตรวจประเมินและเสนอแนะการเปลี่ยนแปลง การกำหนดกรอบแนวทางปฏิบัติสำหรับการปรับปรุงสถาปัตยกรรม และการจัดตั้งกระบวนการบริหารจัดการการเปลี่ยนแปลงให้เป็นระบบ ทั้งนี้เพื่อให้เกิดประโยชน์สูงสุดต่อองค์กรในระยะยาว ขั้นตอนหลักในระยะนี้ประกอบด้วย การสร้างกระบวนการทำงานที่ช่วยเพิ่มมูลค่าในการพัฒนาสถาปัตยกรรม การใช้เครื่องมือเพื่อสนับสนุนการพัฒนา การบริหารความเสี่ยง การวิเคราะห์และตรวจประเมินเพื่อนำไปสู่การพัฒนาสถาปัตยกรรมให้สอดคล้องกับเป้าหมายขององค์กร รวมถึงการกำกับดูแลกระบวนการดำเนินงานให้

เกิดความต่อเนื่องและมีประสิทธิภาพ การบริหารจัดการการเปลี่ยนแปลงในระยะนี้ช่วยให้องค์กรสามารถปรับตัวได้อย่างคล่องตัว รองรับการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจ และสร้างความมั่นคงให้กับโครงสร้างสถาปัตยกรรมองค์กรในระยะยาว

สรุปได้ว่า TOGAF (The Open Group Architecture Framework) ซึ่งพัฒนาโดย Open Group Architecture Forum เป็นกรอบแนวทางสำหรับการออกแบบ วางแผน นำไปใช้ และควบคุมสถาปัตยกรรมเทคโนโลยีสารสนเทศขององค์กร โดยสถาปัตยกรรมองค์กรถูกแบ่งออกเป็น 5 ด้านหลัก ได้แก่ ด้านธุรกิจ (Business Architecture) ด้านข้อมูล (Data Architecture) ด้านแอปพลิเคชัน (Application Architecture) ด้านเทคโนโลยี (Technology Architecture) และด้านความปลอดภัยข้อมูล (Security Architecture)

2.1.2.2 Zachman Framework หมายถึง กรอบแนวคิดที่ใช้ในการจัดการและวิเคราะห์สถาปัตยกรรมองค์กร โดยการแบ่งออกเป็น 6 มุมมอง (perspectives) และ 6 มิติ (dimensions) เพื่อให้สามารถมองเห็นภาพรวมขององค์กรได้อย่างชัดเจนและครบถ้วน มุมมองทั้ง 6 ได้แก่ Planner, Owner, Designer, Builder, Subcontractor, และ User ซึ่งแต่ละมุมมองแสดงถึงมุมมองที่แตกต่างกันในแต่ละระดับการจัดการและการดำเนินงานขององค์กร เช่น มุมมองของ Planner จะมุ่งเน้นในระดับกลยุทธ์และการวางแผนเชิงธุรกิจ ขณะที่มุมมองของ Owner จะเน้นการจัดการองค์กรและการตัดสินใจในระดับสูงสุด ส่วนมุมมองอื่น ๆ เช่น Designer, Builder, Subcontractor, และ User จะมุ่งเน้นในกระบวนการออกแบบ การสร้าง การดำเนินการ และการใช้งานจริงของระบบตามลำดับ มิติทั้ง 6 ได้แก่ Data, Function, Network, People, Time, และ Motivation จะช่วยให้สามารถวิเคราะห์และออกแบบส่วนต่าง ๆ ขององค์กรได้อย่างครอบคลุม ไม่ว่าจะเป็นการจัดการข้อมูล ฟังก์ชันการทำงาน การเชื่อมโยงเครือข่าย การจัดการทรัพยากรมนุษย์ การวางแผนเวลา หรือการสร้างแรงจูงใจในการดำเนินงานผ่านการใช้เทคโนโลยีและกระบวนการทางธุรกิจที่เหมาะสม การผสานมุมมองและมิติทั้งสองจะช่วยให้องค์กรสามารถจัดการและวิเคราะห์สถาปัตยกรรมองค์กรได้อย่างมีประสิทธิภาพและตอบสนองต่อความต้องการที่หลากหลายของผู้มีส่วนได้ส่วนเสียต่าง ๆ (Andry et al., 2021; Ghahremani-Nahr et al., 2023; Madyatmadja et al., 2021; Saoud & Bellabdaoui, 2023; Sharma & Sarkar, 2023)

	Why	How	What	Who	Where	When
Contextual	Goal List	Process List	Material List	Organisational Unit & Role List	Geographical Locations List	Event List
Conceptual	Goal Relationship	Process Model	Entity Relationship Model	Organisational Unit & Role Relationship Model	Locations Model	Event Model
Logical	Rules Diagram	Process Diagram	Data Model Diagram	Role Relationship Diagram	Locations Diagram	Event Diagram
Physical	Rules Specification	Process Function Specification	Data Entity Specification	Role Specification	Location Specification	Event Specification
Detailed	Rules Details	Process Details	Data Details	Role Details	Location Details	Event Details

ภาพที่ 2-2 The Zachman Framework of enterprise architecture

By Ideasintegration (image) + SunSw0rd(text) - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=20113287

2.1.2.3 FEAF (Federal Enterprise Architecture Framework) หมายถึง กรอบแนวคิดที่ถูกพัฒนาขึ้นเพื่อใช้ในการออกแบบและพัฒนาสถาปัตยกรรมองค์กรสำหรับหน่วยงานภาครัฐของสหรัฐอเมริกา โดยมีเป้าหมายในการสร้างมาตรฐานและแนวทางที่ช่วยให้หน่วยงานต่าง ๆ สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพและสอดคล้องกัน เพื่อเสริมสร้างการบูรณาการและประสิทธิภาพในการให้บริการภาครัฐ FEAF มุ่งเน้นการพัฒนาโครงสร้างที่สามารถรองรับการทำงานข้ามหน่วยงานและการแชร์ข้อมูล รวมถึงการลดความซ้ำซ้อนของทรัพยากรและการปรับปรุงกระบวนการทางธุรกิจในระดับรัฐบาล การนำ FEAF มาใช้ในหน่วยงานรัฐบาลจะช่วยให้สามารถสร้างความเชื่อมโยงระหว่างกระบวนการทำงานและเทคโนโลยีสารสนเทศต่าง ๆ ได้อย่างมีระเบียบ โดยการใช้มาตรฐานที่ชัดเจนในทุกด้านของสถาปัตยกรรมองค์กร ซึ่งจะช่วยเพิ่มความคล่องตัวและลดความซับซ้อนในการบริหารจัดการทรัพยากรและข้อมูล อีกทั้งยังสามารถปรับปรุงการให้บริการที่ตอบสนองได้รวดเร็วและมีประสิทธิภาพมากขึ้น (Muslih et al., 2024b)

องค์ประกอบหลักของ FEAF ประกอบด้วย

1. แบบจำลองอ้างอิง (Reference Models) ใน FEAF (Federal Enterprise Architecture Framework) เป็นแนวทางที่ใช้ในการจัดการและวิเคราะห์สถาปัตยกรรมองค์กรโดยแบ่งออกเป็น 5

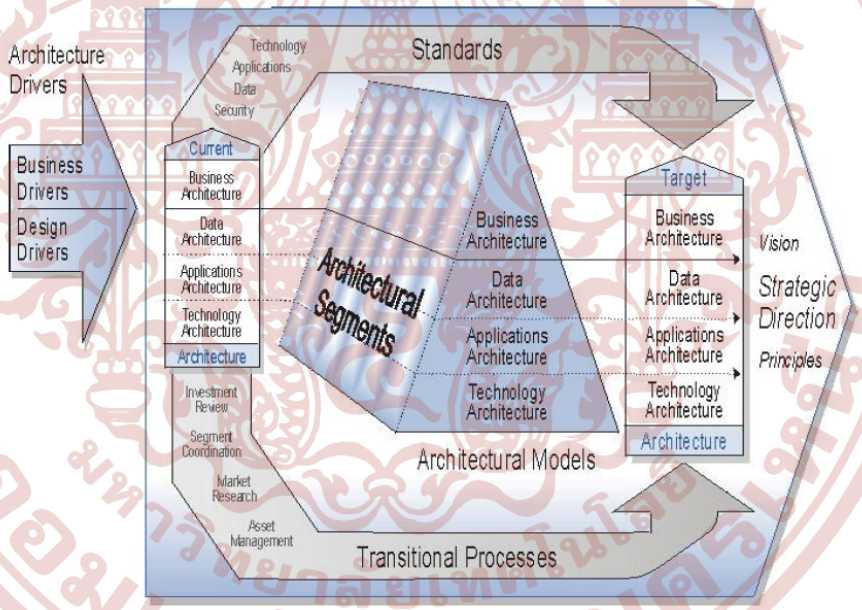
มิติหลัก ได้แก่ แบบจำลองด้านประสิทธิภาพ (Performance Reference Model - PRM) ซึ่งช่วยในการวัดผลและปรับปรุงประสิทธิภาพขององค์กรผ่านตัวชี้วัดและการวิเคราะห์ผลการดำเนินงาน , แบบจำลองด้านธุรกิจ (Business Reference Model - BRM) ที่กำหนดโครงสร้างและองค์ประกอบของกระบวนการธุรกิจหลัก เพื่อให้เข้าใจแนวทางการดำเนินงานขององค์กรได้อย่างเป็นระบบ , แบบจำลองด้านบริการ (Service Reference Model - SRM) ซึ่งใช้จัดหมวดหมู่บริการทางธุรกิจและบริการด้านไอที เพื่อเพิ่มความสามารถในการใช้งานซ้ำและการบูรณาการข้ามหน่วยงาน , แบบจำลองด้านข้อมูล (Data Reference Model - DRM) ที่กำหนดแนวทางมาตรฐานสำหรับการจัดการและแลกเปลี่ยนข้อมูล เพื่อให้เกิดความสอดคล้องและสามารถนำข้อมูลมาใช้ร่วมกันได้อย่างมีประสิทธิภาพ และสุดท้ายคือ แบบจำลองด้านเทคนิค (Technical Reference Model - TRM) ซึ่งกำหนดมาตรฐานทางเทคนิคและโครงสร้างพื้นฐานด้านไอที เช่น แพลตฟอร์ม ซอฟต์แวร์ และโปรโตคอลที่องค์กรใช้ในการดำเนินงาน ทั้งหมดนี้ช่วยให้การออกแบบและบริหารจัดการสถาปัตยกรรมองค์กรเป็นไปในทิศทางเดียวกันและสามารถรองรับการเปลี่ยนแปลงในอนาคตได้อย่างมีประสิทธิภาพ

2. การกำกับดูแล (Governance) ใน FEAF (Federal Enterprise Architecture Framework) เป็นกระบวนการสำคัญที่ช่วยให้การบริหารจัดการทรัพยากรด้าน IT เป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับกลยุทธ์และเป้าหมายขององค์กร โดย FEAF เน้นให้มีโครงสร้างการกำกับดูแลที่ชัดเจน เพื่อให้แน่ใจว่าการลงทุนด้านเทคโนโลยีสารสนเทศสามารถสนับสนุนภารกิจขององค์กรได้อย่างเหมาะสม การกำกับดูแลใน FEAF ครอบคลุมถึงการวางนโยบาย กฎระเบียบ กระบวนการตัดสินใจ และกลไกในการตรวจสอบและประเมินผล เพื่อให้มั่นใจว่าโครงการด้านไอทีมีการดำเนินงานตามมาตรฐานและแนวปฏิบัติที่กำหนดไว้ รวมถึงการบริหารความเสี่ยงและการควบคุมต้นทุน เพื่อเพิ่มประสิทธิภาพและความคุ้มค่าของการใช้ทรัพยากร นอกจากนี้ FEAF ยังส่งเสริมการมีส่วนร่วมของผู้มีส่วนได้เสียภายในองค์กร เพื่อให้เกิดความร่วมมือและการบูรณาการที่ดีขึ้นในการดำเนินงานด้านสถาปัตยกรรมองค์กร

3. การมาตรฐานและการบูรณาการ (Standardization and Integration) ใน FEAF (Federal Enterprise Architecture Framework) มุ่งเน้นการส่งเสริมการใช้มาตรฐานที่สอดคล้องกันและการทำงานร่วมกันระหว่างระบบต่าง ๆ ภายในหน่วยงานของรัฐบาล ซึ่งช่วยเพิ่มประสิทธิภาพในการประสานงานและการแบ่งปันข้อมูลอย่างมีประสิทธิภาพ การใช้มาตรฐานช่วยให้ระบบต่าง ๆ ที่พัฒนาขึ้นในแต่ละหน่วยงานสามารถเชื่อมโยงและทำงานร่วมกันได้อย่างราบรื่น โดยไม่เกิดความซ้ำซ้อนหรือข้อผิดพลาดในข้อมูล การบูรณาการของระบบต่าง ๆ ทำให้การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นไปอย่างมีประสิทธิภาพ ลดการทำงานซ้ำซ้อนและการจัดการข้อมูลที่ไม่ตรงกัน ซึ่งในที่สุดจะช่วยให้กระบวนการทางธุรกิจภาครัฐทำงานได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

นอกจากนี้ การบูรณาการยังช่วยในการตัดสินใจที่ดีกว่า เนื่องจากข้อมูลที่ใช้ในการวิเคราะห์และการวางแผนมีความถูกต้องและสอดคล้องกันทุกหน่วยงาน

4. การจัดการวงจรชีวิต (Lifecycle Management) ใน FEAF (Federal Enterprise Architecture Framework) สนับสนุนกระบวนการจัดการวงจรชีวิตที่เป็นระบบสำหรับการพัฒนา การใช้งาน และการบำรุงรักษาโซลูชัน IT โดยมีการวางแผนและดำเนินการในทุกขั้นตอนของวงจรชีวิตของโซลูชัน IT ตั้งแต่เริ่มต้นการพัฒนา จนถึงการบำรุงรักษาหลังจากการใช้งาน เพื่อให้ระบบ IT สามารถทำงานได้อย่างมีประสิทธิภาพและตอบสนองต่อความต้องการขององค์กรได้อย่างต่อเนื่อง การจัดการวงจรชีวิตใน FEAF ช่วยให้การพัฒนาโซลูชัน IT มีความยืดหยุ่น ปรับเปลี่ยนได้ตามความต้องการของธุรกิจ และสามารถรักษาความเสถียรของระบบได้ในระยะยาว นอกจากนี้ ยังช่วยให้การบำรุงรักษาระบบเป็นไปอย่างมีประสิทธิภาพ ลดการใช้ทรัพยากรและเพิ่มอายุการใช้งานของโซลูชัน IT โดยรวม



ภาพที่ 2-3 Federal Enterprise Architecture Framework" (FEAF)

By Chief Information Officer Council - A Practical Guide to Federal Enterprise Architecture, Public Domain, https://commons.wikimedia.org/w/index.php?curid=5394291

2.1.3 กรอบของโครงสร้างองค์กร

โครงสร้างองค์กร หรือการพัฒนาสถาปัตยกรรมองค์กร สามารถแบ่งองค์ประกอบย่อยออกเป็น 7 ส่วนตามลักษณะขององค์กร คือ สถาปัตยกรรมธุรกิจ (Business Architecture) สถาปัตยกรรมข้อมูล

(Data Architecture) สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture) สถาปัตยกรรมเทคโนโลยี (Technology Architecture) สถาปัตยกรรมด้านความปลอดภัย (Security Architecture) สถาปัตยกรรมการบูรณาการ (Integration Architecture) และ สถาปัตยกรรมการกำกับดูแล (Governance Architecture) (Atencio et al., 2024b; Dumitriu & Popescu, 2020a; Muslih et al., 2024c; Qurtubi, 2024; Srisawat et al., 2024; Sultanow et al., 2021; Uzhakova & Fischer, 2024a)

2.1.3.1 สถาปัตยกรรมธุรกิจ (Business Architecture)

2.1.3.1.1 ความหมาย

สถาปัตยกรรมธุรกิจ (Business Architecture) หมายถึง การออกแบบโครงสร้างและกลยุทธ์ขององค์กรที่มีเป้าหมายในการกำหนดและจัดการความสามารถหลัก)core capabilities) ของธุรกิจ ซึ่งช่วยให้สามารถเชื่อมโยงและประสานงานระหว่างฟังก์ชันธุรกิจต่าง ๆ ได้อย่างมีประสิทธิภาพ โดยการกำหนดกระบวนการที่สำคัญและโครงสร้างที่เหมาะสมกับวัตถุประสงค์ทางธุรกิจ สถาปัตยกรรมธุรกิจจะพิจารณาถึงองค์ประกอบสำคัญของธุรกิจ เช่น เป้าหมาย บริการ และโครงสร้างองค์กร พร้อมทั้งเชื่อมโยงกับกลยุทธ์โดยรวมขององค์กร เพื่อให้การดำเนินธุรกิจสามารถตอบสนองต่อความท้าทายในตลาดและการเปลี่ยนแปลงของสภาพแวดล้อมได้อย่างมีประสิทธิภาพมากขึ้น การใช้ Business Architecture จึงไม่เพียงแต่ช่วยในการพัฒนากระบวนการและความสามารถขององค์กร แต่ยังช่วยให้สามารถสร้างความยืดหยุ่นในการปรับกลยุทธ์และกระบวนการตัดสินใจในแต่ละระดับการดำเนินงานได้ เพื่อให้องค์กรสามารถแข่งขันและเติบโตได้มีประสิทธิภาพในระยะยาว (Sutton, 2024)

สถาปัตยกรรมธุรกิจ หมายถึง โครงสร้างการดำเนินงานหลัก กลยุทธ์ และทรัพยากรขององค์กรที่ได้รับการออกแบบให้สอดคล้องกับสถานการณ์ใหม่ ๆ โดยเฉพาะในช่วงเวลาที่มีการเปลี่ยนแปลงอย่างรวดเร็วหรือเกิดวิกฤต (Meepung, Wannapiroon, et al., 2021) สถาปัตยกรรมธุรกิจนี้เน้นการปรับรูปแบบการติดต่อกับลูกค้า การใช้เทคโนโลยีดิจิทัล การบริหารจัดการห่วงโซ่อุปทาน และการจัดการวิกฤต เพื่อให้ธุรกิจสามารถรับมือกับความท้าทายและความไม่แน่นอนในตลาดได้อย่างมีประสิทธิภาพ นอกจากนี้ยังมุ่งเน้นไปที่การเสริมสร้างความยืดหยุ่นในกระบวนการทางธุรกิจ โดยการออกแบบและกำหนดบทบาทในองค์กรและกลไกการตัดสินใจที่ช่วยให้สามารถปรับตัวและเปลี่ยนแปลงได้ทันทีเมื่อเกิดวิกฤต การใช้ Business Architecture ช่วยให้ธุรกิจสามารถตอบสนองต่อสถานการณ์ที่ไม่คาดคิดและรักษาความสามารถในการแข่งขันได้อย่างต่อเนื่อง โดยเฉพาะในสภาวะที่ต้องการความคล่องตัวและประสิทธิภาพสูงสุด (Rave-Gómez et al., 2024)

สถาปัตยกรรมธุรกิจ หมายถึง กรอบการออกแบบและจัดระบบที่มีการกำหนดวิธีการดำเนินงานขององค์กรให้สอดคล้องกับเป้าหมายเชิงกลยุทธ์ขององค์กรและกระบวนการทำงานต่าง ๆ ที่เกี่ยวข้อง รวมถึงหน้าที่และโครงสร้างภายในองค์กร การออกแบบ Business Architecture จึงมีบทบาทสำคัญในการสร้างความมั่นใจว่าเป้าหมายทางธุรกิจจะได้รับการสนับสนุนอย่างมีประสิทธิภาพจากการดำเนินงานที่ดำเนินไปและทรัพยากรที่มีอยู่ ซึ่งโดยทั่วไปจะเกี่ยวข้องกับการสร้างแบบจำลองความสามารถขององค์กร กระบวนการทางธุรกิจ ข้อมูล และคุณค่าที่องค์กรต้องการส่งมอบให้แก่ลูกค้าและผู้มีส่วนได้ส่วนเสีย การมี Business Architecture ที่ชัดเจนช่วยให้สามารถเข้าใจและปรับปรุงกระบวนการทำงานได้ดีขึ้น ทำให้สามารถเพิ่มประสิทธิภาพการดำเนินงานได้อย่างมีระบบ นอกจากนี้ยังช่วยในการวางแผนเชิงกลยุทธ์และการตัดสินใจที่สำคัญในการพัฒนาธุรกิจ โดยการให้ภาพที่ชัดเจนเกี่ยวกับวิธีที่แต่ละส่วนขององค์กรเชื่อมโยงและทำงานร่วมกัน เพื่อให้สามารถตอบสนองต่อความท้าทายต่าง ๆ และบรรลุเป้าหมายขององค์กรได้อย่างมีประสิทธิภาพ (Uzhakova & Fischer, 2024a)

สถาปัตยกรรมธุรกิจ หมายถึง สำหรับศูนย์ออกกำลังกายหมายถึงกรอบพื้นฐานที่ช่วยให้การดำเนินงานและโครงสร้างของศูนย์ออกกำลังกายสอดคล้องกับเป้าหมายเชิงกลยุทธ์ขององค์กร โดยการออกแบบและจัดระเบียบทุกส่วนของศูนย์ให้สามารถทำงานร่วมกันอย่างมีประสิทธิภาพ เช่น การบริหารจัดการบริการลูกค้า การจัดการทรัพยากรบุคคล และการดำเนินการทางการเงิน ซึ่งจะช่วยให้การทำงานภายในศูนย์ออกกำลังกายสามารถตอบสนองความต้องการของลูกค้าได้อย่างเหมาะสมและตรงตามเป้าหมายทางธุรกิจ (Srisawat et al., 2024) การวิจัยนี้ใช้กรอบการทำงานของ The Open Group Architecture Framework (TOGAF) ซึ่งเป็นเครื่องมือที่ช่วยในการสร้างโมเดลความสามารถ กระบวนการ และโครงสร้างองค์กรของศูนย์ออกกำลังกาย โดยการใช้ TOGAF ทำให้สามารถวางแผนและออกแบบสถาปัตยกรรมธุรกิจได้อย่างเป็นระบบ ซึ่งไม่เพียงแต่ช่วยให้ทุกภาคส่วนของศูนย์ออกกำลังกายทำงานร่วมกันอย่างมีประสิทธิภาพเท่านั้น แต่ยังช่วยให้สามารถบรรลุเป้าหมายที่ตั้งไว้ได้อย่างเหมาะสม ด้วยการเชื่อมโยงกลยุทธ์ทางธุรกิจและการดำเนินงานที่เกี่ยวข้อง (Jonathan & Andry, 2024)

สถาปัตยกรรมธุรกิจ หมายถึง สำหรับธุรกิจขนาดกลางและขนาดเล็ก (SMEs) ในอุตสาหกรรมร้านอาหารฟาสต์ฟู้ดเป็นกรอบการออกแบบที่เชื่อมโยงกลยุทธ์ทางธุรกิจกับกระบวนการดำเนินงานต่าง ๆ ภายในองค์กร โดยใช้กรอบการทำงานสถาปัตยกรรมองค์กร (TOGAF) ซึ่งช่วยในการวางแผนและออกแบบโครงสร้างธุรกิจให้สอดคล้องกับเป้าหมายและกลยุทธ์ขององค์กร โดยเน้นการเชื่อมโยงระหว่างกระบวนการทำงานต่าง ๆ เช่น การจัดการการขาย การจัดสรรทรัพยากร และการบริหารจัดการโครงสร้างองค์กรที่เกี่ยวข้อง เพื่อให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพและตอบสนองความต้องการของตลาด การใช้ TOGAF จะช่วยให้สามารถปรับปรุงกลยุทธ์การขายและ

การจัดการทรัพยากรในองค์กรได้อย่างต่อเนื่อง ทั้งยังช่วยเสริมสร้างความสามารถในการแข่งขันของธุรกิจและเพิ่มความคล่องตัวในการปรับตัวต่อสถานการณ์ต่าง ๆ ที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ ด้วยการเชื่อมโยงทุกภาคส่วนของธุรกิจให้ทำงานร่วมกันอย่างมีระบบและประสิทธิผล (Ovalle et al., 2024)

สถาปัตยกรรมธุรกิจ หมายถึง กรอบโครงสร้างที่ออกแบบมาเพื่อเชื่อมโยงและจัดการกลยุทธ์ทางธุรกิจกับกระบวนการดำเนินงานต่าง ๆ ภายในองค์กร โดยใช้วิธีการจากกรอบการทำงาน TOGAF ซึ่งเน้นการจัดระเบียบฟังก์ชันหลักของธุรกิจ เช่น การขาย การตลาด และการให้บริการ เพื่อเพิ่มประสิทธิภาพในการดำเนินงานและเสริมความสามารถในการปรับตัวให้ทันกับการเปลี่ยนแปลงของตลาด การใช้ TOGAF ช่วยให้สามารถระบุและจัดลำดับขั้นตอนทางธุรกิจที่สำคัญได้อย่างมีระเบียบ พร้อมทั้งตรวจสอบและประเมินความต้องการทางเทคโนโลยีที่จำเป็นเพื่อสนับสนุนการให้บริการและการมีปฏิสัมพันธ์กับลูกค้าได้อย่างมีประสิทธิผล โครงสร้างพื้นฐาน IT ที่ถูกกำหนดโดย TOGAF จะช่วยสนับสนุนการดำเนินงานขององค์กรให้สอดคล้องกับกลยุทธ์ธุรกิจอย่างมีประสิทธิภาพและยั่งยืน นอกจากนี้ยังช่วยเสริมสร้างความเติบโตและเพิ่มขีดความสามารถในการแข่งขันในตลาด โดยให้ความสำคัญกับการเชื่อมโยงระหว่างเทคโนโลยีและการดำเนินงานทางธุรกิจ ซึ่งส่งผลต่อการพัฒนาองค์กรให้ก้าวหน้าต่อไป (Teodoro Ramírez Guija et al., 2024)

สถาปัตยกรรมธุรกิจ หมายถึง เครื่องมือที่มีบทบาทสำคัญในการจัดระเบียบและวิเคราะห์กระบวนการทางธุรกิจขององค์กร โดยเฉพาะในภาคสิ่งทอ ซึ่งเป็นภาคธุรกิจขนาดเล็กที่ต้องการการจัดการที่มีประสิทธิภาพ สถาปัตยกรรมนี้ช่วยเชื่อมโยงทรัพยากร เทคโนโลยี และข้อมูลต่าง ๆ ภายในองค์กรให้ทำงานร่วมกันอย่างเป็นระบบ เพื่อเพิ่มประสิทธิภาพในการดำเนินงานในแต่ละขั้นตอนของธุรกิจ เช่น การผลิต การจัดการทรัพยากร และการจัดจำหน่ายสินค้า โดยการใช้โครงสร้างพื้นฐานที่เหมาะสมกับขนาดของธุรกิจ สถาปัตยกรรมธุรกิจนี้ยังช่วยให้ผู้ประกอบการสามารถระบุจุดที่ต้องปรับปรุงในกระบวนการทางธุรกิจและสามารถปรับเปลี่ยนกลยุทธ์ให้สอดคล้องกับความต้องการของตลาดและผู้บริโภคได้อย่างมีประสิทธิภาพ นอกจากนี้ ยังช่วยสร้างการเติบโตและความสามารถในการแข่งขันในตลาดได้อย่างยั่งยืน โดยการพัฒนาและปรับปรุงกระบวนการทำงานที่เกี่ยวข้องกับการผลิตและการจัดจำหน่ายสินค้าเพื่อให้สามารถตอบสนองต่อความต้องการที่เปลี่ยนแปลงไปได้ดีขึ้น (Lizby Suarez Torres et al., 2024)

สถาปัตยกรรมธุรกิจ หมายถึง โครงสร้างที่สำคัญในการวิเคราะห์และออกแบบระบบสารสนเทศทางธุรกิจ โดยเน้นการสร้างกรอบการทำงานที่ช่วยสนับสนุนการจัดการข้อมูลและกระบวนการทำงานขององค์กรให้มีประสิทธิภาพยิ่งขึ้น สถาปัตยกรรมนี้มุ่งเน้นไปที่การเพิ่มประสิทธิภาพในการตัดสินใจทางธุรกิจ โดยการใช้เครื่องมือและวิธีการที่สามารถช่วยในการวิเคราะห์

ข้อมูลที่มีอยู่ได้อย่างมีประสิทธิภาพ การนำเสนอเทคนิคการวิเคราะห์ในสถาปัตยกรรมธุรกิจจึงเป็นกุญแจสำคัญที่ช่วยให้ผู้ประกอบการสามารถระบุความต้องการทางธุรกิจได้อย่างชัดเจนและแม่นยำยิ่งขึ้น นอกจากนี้ยังสามารถช่วยในการพัฒนาเครื่องมือที่จะใช้ในการปรับปรุงกลยุทธ์ธุรกิจได้อย่างมีประสิทธิภาพ โดยการนำข้อมูลที่มีอยู่ไปใช้ในการวางแผนเชิงกลยุทธ์และการปรับปรุงกระบวนการทำงานในองค์กรให้สอดคล้องกับเป้าหมายทางธุรกิจที่ต้องการการพัฒนาอย่างต่อเนื่องเพื่อความสำเร็จในระยะยาว (Pankowski, 2023)

สถาปัตยกรรมธุรกิจ หมายถึง โครงสร้างเชิงกลยุทธ์ที่เชื่อมโยงกระบวนการธุรกิจหลักกับเทคโนโลยีที่ใช้สนับสนุนการดำเนินงานขององค์กร โดยมุ่งเน้นการสร้างการเชื่อมโยงที่มีประสิทธิภาพระหว่างกระบวนการเหล่านี้ เพื่อให้การเปลี่ยนผ่านจากระบบการศึกษาดั้งเดิมไปสู่ระบบ e-Learning เป็นไปอย่างราบรื่นและมีประสิทธิผล การใช้กรอบการทำงาน TOGAF ร่วมกับเทคโนโลยีอย่าง Google Classroom และ DLPCA ช่วยให้สถาบันการศึกษาสามารถพัฒนาและปรับปรุงกระบวนการเรียนการสอนทางดิจิทัลได้อย่างมีประสิทธิภาพ ทั้งยังสามารถตอบสนองต่อความต้องการของผู้เรียนในยุคปัจจุบันที่ต้องการความสะดวกและยืดหยุ่นในการเรียนรู้ โดยสถาปัตยกรรมธุรกิจนี้มีบทบาทในการจัดการความเปลี่ยนแปลงที่เกิดขึ้นในระบบการศึกษา เพื่อให้สามารถปรับตัวและตอบสนองต่อความท้าทายใหม่ ๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ ทำให้ระบบการศึกษาสามารถรักษาคุณภาพการเรียนการสอนได้ในสภาพแวดล้อมที่เปลี่ยนแปลงไปในทิศทางดิจิทัลอย่างยั่งยืน (Puntillo et al., 2022)

สรุปได้ว่า สถาปัตยกรรมธุรกิจ หมายถึง การออกแบบและจัดโครงสร้างกระบวนการทางธุรกิจ เป้าหมาย กลยุทธ์ และความสัมพันธ์ระหว่างหน่วยงานต่างๆ ภายในองค์กร เพื่อให้การทำงานเป็นไปอย่างมีประสิทธิภาพและตอบสนองต่อความต้องการของตลาด โดยเน้นการเชื่อมโยงระหว่างกระบวนการและทรัพยากรต่าง ๆ ภายในองค์กร เช่น โมเดลธุรกิจ (business models), กระบวนการทางธุรกิจ (business processes), และการจัดการทรัพยากรบุคคล (HR management) เพื่อให้มั่นใจว่าองค์กรสามารถบรรลุเป้าหมายทางธุรกิจได้อย่างมีประสิทธิภาพและสอดคล้องกับทิศทางกลยุทธ์ที่กำหนด นอกจากนี้ยังช่วยให้การดำเนินงานขององค์กรสามารถปรับตัวและตอบสนองต่อการเปลี่ยนแปลงในตลาดและสภาพแวดล้อมธุรกิจได้อย่างยืดหยุ่นและยั่งยืน

2.1.3.2. สถาปัตยกรรมข้อมูล (Data Architecture)

2.1.3.2.1 ความหมาย

สถาปัตยกรรมข้อมูล (Data Architecture) ในองค์กรการศึกษาหมายถึงการออกแบบและจัดการโครงสร้างข้อมูลที่ใช้ในการสนับสนุนการดำเนินงานและการตัดสินใจในระบบดิจิทัล โดยการ

จัดระเบียบการจัดเก็บและการไหลเวียนของข้อมูลจากแหล่งต่าง ๆ อย่างมีระบบ เพื่อให้ข้อมูลสามารถเข้าถึงได้อย่างรวดเร็วและมีประสิทธิภาพ โครงสร้างนี้ยังครอบคลุมถึงการจัดการคุณภาพข้อมูล ความปลอดภัยของข้อมูล และการเชื่อมโยงข้อมูลที่เกี่ยวข้องจากภายในและภายนอกองค์กร เพื่อให้สามารถนำข้อมูลไปใช้ในการพัฒนาและปรับปรุงกระบวนการทางการศึกษาต่าง ๆ รวมถึงการบริหารจัดการและการกำหนดกลยุทธ์ที่ตอบสนองต่อความต้องการของการศึกษาในยุคดิจิทัล (Srisawat et al., 2024)

สถาปัตยกรรมข้อมูล ในบริบทของการประมวลผลข้อมูลหลากหลาย (multi-omics data) เน้นการจัดการและรวมข้อมูลขนาดใหญ่ที่มีแหล่งที่มาหลายประเภท โดยใช้เทคโนโลยีปัญญาประดิษฐ์เพื่อพัฒนากระบวนการประมวลผลข้อมูลและสร้างตัวอย่างจำลองที่มีความแม่นยำสูง การออกแบบสถาปัตยกรรมนี้รวมถึงการใช้โมเดลเชิงลึก เช่น Transformer ที่ได้รับการฝึกฝนล่วงหน้าเพื่อเพิ่มประสิทธิภาพในการเรียนรู้จากข้อมูลจำนวนมาก นอกจากนี้ยังใช้เทคนิคการกระจายข้อมูลแบบมีเงื่อนไข (conditional diffusion) เพื่อช่วยในการจำลองข้อมูลที่มีความซับซ้อนและความสัมพันธ์ที่ไม่ชัดเจน ซึ่งทั้งหมดนี้ทำให้สามารถใช้ข้อมูลที่ประมวลผลแล้วในการพัฒนาระบบที่สามารถสนับสนุนการตัดสินใจในงานวิจัยหรือการพัฒนาแอปพลิเคชันที่เกี่ยวข้องกับการวิเคราะห์ข้อมูลเชิงลึก (Sidorenko et al., 2024)

สถาปัตยกรรมข้อมูล ในบริบทของการเรียนรู้เมตา (Meta-Learning) มีความสำคัญในการออกแบบและจัดโครงสร้างข้อมูลที่สามารถรองรับกระบวนการเรียนรู้จากข้อมูลที่มีลักษณะซับซ้อนและหลากหลาย โดยมุ่งเน้นการจัดการข้อมูลในรูปแบบเชิงโครงสร้าง ซึ่งทำให้ระบบสามารถเรียนรู้และปรับตัวได้อย่างมีประสิทธิภาพ ในสถาปัตยกรรมนี้ ข้อมูลจะถูกเก็บรวบรวมและจัดระเบียบอย่างมีระบบเพื่อรองรับการเรียนรู้ในระดับที่สูงขึ้น โดยที่ข้อมูลสามารถนำมาใช้ในหลายโดเมนหรือปัญหาที่แตกต่างกันได้อย่างยืดหยุ่นและมีประสิทธิภาพ สถาปัตยกรรมนี้ช่วยให้ระบบสามารถสร้างแบบจำลองที่ไม่เพียงแค่แก้ไขปัญหาหนึ่งๆ แต่ยังสามารถปรับตัวและเรียนรู้จากประสบการณ์ในหลากหลายสถานการณ์ ทำให้ระบบมีความสามารถในการปรับตัวให้เข้ากับปัญหาหรือข้อมูลใหม่ๆ ได้อย่างรวดเร็วและแม่นยำ (Binz et al., 2024)

สถาปัตยกรรมข้อมูล หมายถึง การออกแบบโครงสร้างพื้นฐานสำหรับรองรับการประมวลผลข้อมูลขนาดใหญ่ (Big Data) และเชื่อมโยงกับปัญญาประดิษฐ์ที่สามารถอธิบายได้ (Explainable AI) เป็นโครงสร้างที่มีการออกแบบเพื่อจัดการกับข้อมูลเชิงโครงสร้างในปริมาณมหาศาล พร้อมรองรับการประมวลผลและวิเคราะห์ข้อมูลที่มีความซับซ้อนสูง โครงสร้างนี้ช่วยให้การตัดสินใจของระบบปัญญาประดิษฐ์ (AI) สามารถอธิบายได้อย่างชัดเจนและโปร่งใส โดยไม่เพียงแค่ให้ผลลัพธ์ที่ถูกต้อง แต่ยังสามารถให้คำอธิบายที่เข้าใจได้เกี่ยวกับการตัดสินใจของ AI ซึ่งเป็นการลดความไม่แน่นอนและ

เสริมสร้างความเชื่อมั่นในการใช้งาน AI ในหลายๆ ด้าน การจัดการข้อมูลในลักษณะนี้ช่วยให้การเรียนรู้ของระบบ AI มีประสิทธิภาพมากขึ้น และการตัดสินใจที่เกิดจาก AI สามารถเข้าถึงและตรวจสอบได้อย่างโปร่งใส ทำให้การใช้งาน AI ในองค์กรหรือในบริบทต่างๆ เป็นไปอย่างมั่นใจและเชื่อถือได้ (La Gatta et al., 2024)

สถาปัตยกรรมข้อมูล หมายถึง การออกแบบโครงสร้างพื้นฐานสำหรับรองรับการประมวลผลและวิเคราะห์ข้อมูลขนาดใหญ่ ในการตรวจจับกิจกรรมผิดกฎหมายบนเครือข่ายมืด (Dark Web) มีบทบาทสำคัญในการออกแบบโครงสร้างพื้นฐานที่สามารถจัดการกับข้อมูลจำนวนมหาศาลที่มาจากแหล่งที่ไม่เป็นที่รู้จักหรือเข้าถึงยาก โดยการใช้เทคนิคการวิเคราะห์ข้อมูลที่ทันสมัย เช่น การประมวลผลข้อมูลขนาดใหญ่ (Big Data Analytics) และ Machine Learning เพื่อช่วยในการระบุ จัดประเภท และติดตามเว็บไซต์ที่อาจมีความเกี่ยวข้องกับกิจกรรมผิดกฎหมายหรือการกระทำที่เป็นอันตราย ระบบนี้เน้นการเก็บรวบรวมข้อมูลจากแหล่งข้อมูลที่มีลักษณะลึกลับและไม่สามารถเข้าถึงได้ง่าย พร้อมทั้งการจัดเก็บข้อมูลในโครงสร้างที่สามารถประมวลผลและวิเคราะห์ได้อย่างมีประสิทธิภาพ การใช้งานในลักษณะนี้ทำให้สามารถตรวจจับและตอบสนองต่อเหตุการณ์หรือกิจกรรมผิดกฎหมายในเครือข่ายมืดได้อย่างรวดเร็วและแม่นยำ ส่งผลให้การรักษาความปลอดภัยทางไซเบอร์มีความแข็งแกร่งยิ่งขึ้น (Pastor-Galindo et al., 2024)

สถาปัตยกรรมข้อมูล หมายถึง การออกแบบโครงสร้างข้อมูลที่มีประสิทธิภาพสำหรับใช้ในการพัฒนาเมืองสมัยใหม่มีบทบาทสำคัญในการออกแบบโครงสร้างข้อมูลที่มีประสิทธิภาพเพื่อจัดเก็บประมวลผล และวิเคราะห์ข้อมูลจากแหล่งต่าง ๆ ภายในโครงสร้างพื้นฐานอัจฉริยะของเมือง โดยเฉพาะการใช้เทคนิคการเรียนรู้ของเครื่อง (Machine Learning) เพื่อประเมินความเสี่ยงด้านความปลอดภัย การออกแบบสถาปัตยกรรมข้อมูลนี้มุ่งเน้นที่การจัดการข้อมูลที่ซับซ้อนในระบบเมือง เช่น การตรวจจับภัยคุกคามที่อาจเกิดขึ้นจากการวิเคราะห์ข้อมูลที่ได้จากกล้องวงจรปิด ระบบ IoT หรือเซ็นเซอร์ต่าง ๆ ในเมือง ด้วยการประมวลผลข้อมูลแบบเรียลไทม์ เทคโนโลยีนี้ช่วยให้สามารถระบุและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยในเมืองได้ทันที เช่น การตรวจจับการเคลื่อนไหวที่ผิดปกติหรือพฤติกรรมที่อาจเป็นภัยคุกคาม พร้อมทั้งทำให้ระบบเมืองสามารถปรับตัวและดำเนินการแก้ไขปัญหาความปลอดภัยได้อย่างมีประสิทธิภาพ จึงสามารถสร้างสภาพแวดล้อมที่ปลอดภัยและตอบสนองต่อความต้องการของประชาชนได้ดีขึ้น (Shuhan et al., 2024)

สถาปัตยกรรมข้อมูล หมายถึง โครงสร้างพื้นฐานสำหรับรองรับข้อมูลหลายรูปแบบ (Multimodal Data) ในการโต้ตอบระหว่างหุ่นยนต์ทางการศึกษาและผู้เรียน มีการออกแบบโครงสร้างพื้นฐานเพื่อจัดการและประมวลผลข้อมูลที่มาจากหลายแหล่งและช่องทาง เช่น การมองเห็น การได้ยิน การสัมผัส และการพูด โดยข้อมูลเหล่านี้ถูกจัดเก็บและนำมาประมวลผลอย่างมีระบบใน

ระบบการเรียนรู้ของหุ่นยนต์อัจฉริยะ ระบบนี้ถูกพัฒนาเพื่อรองรับการเรียนรู้ที่หลากหลายตามทฤษฎีพหุปัญญา (Multiple Intelligences) ซึ่งเป็นการสร้างการเรียนรู้ที่สามารถตอบสนองต่อความสามารถและลักษณะการเรียนรู้ที่แตกต่างของแต่ละบุคคล โดยใช้หุ่นยนต์เป็นตัวกลางในการช่วยกระตุ้นและสนับสนุนผู้เรียนให้มีส่วนร่วมในกระบวนการเรียนรู้ได้อย่างมีประสิทธิภาพ สถาปัตยกรรมข้อมูลนี้ไม่เพียงแต่ช่วยให้หุ่นยนต์สามารถตอบสนองต่อคำสั่งและคำถามของผู้เรียนได้ดีขึ้น แต่ยังช่วยพัฒนาการเรียนรู้ในรูปแบบที่เป็นองค์รวมและหลากหลายตามวิธีการและช่องทางที่ผู้เรียนแต่ละคนถนัด (X. Wang et al., 2024)

สถาปัตยกรรมข้อมูล หมายถึง โครงสร้างและการออกแบบระบบที่จัดการกับข้อมูลทั่วโลกที่เกี่ยวข้องกับปัญญาประดิษฐ์ เป็นการออกแบบและกำหนดโครงสร้างระบบที่มีความรับผิดชอบในการจัดการข้อมูลทั่วโลก โดยมุ่งเน้นที่การรวบรวม การจัดเก็บ การประมวลผล และการใช้ข้อมูลในลักษณะที่สอดคล้องกับจริยธรรม ซึ่งจะช่วยให้การพัฒนาระบบขององค์กรเป็นไปอย่างยั่งยืนและมีประสิทธิภาพ การออกแบบนี้ไม่เพียงแต่ต้องคำนึงถึงการใช้ข้อมูลเพื่อเพิ่มความสามารถในการประมวลผลของ AI แต่ยังต้องคำนึงถึงการปกป้องข้อมูลส่วนบุคคลและรักษาความเป็นส่วนตัวของข้อมูลอย่างเคร่งครัด โดยจะต้องมีการจัดการความเสี่ยงที่อาจเกิดจากการใช้ AI เช่น การตัดสินใจที่ไม่โปร่งใส หรือการใช้งานที่อาจละเมิดสิทธิของบุคคล การสร้างสถาปัตยกรรมข้อมูลในลักษณะนี้จะช่วยให้เกิดความเชื่อมั่นในระบบขององค์กรและสร้างความไว้วางใจจากผู้ใช้ข้อมูล โดยองค์กรสามารถดำเนินการในลักษณะที่มีความรับผิดชอบ และสอดคล้องกับมาตรฐานทางจริยธรรมเพื่อปกป้องข้อมูลและผลประโยชน์ของทุกฝ่าย (Monlezun, 2024)

สถาปัตยกรรมข้อมูล หมายถึง โครงสร้างที่ออกแบบมาเพื่อจัดการและประมวลผลข้อมูลขนาดใหญ่แบบ มีบทบาทสำคัญในการจัดการข้อมูลดิจิทัลและข้อมูลจากสื่อสังคมออนไลน์ ซึ่งต้องมีการประมวลผลข้อมูลที่เปลี่ยนแปลงอย่างรวดเร็ว ระบบนี้ใช้เทคนิคการจัดกลุ่มข้อมูล (clustering) โดยเฉพาะวิธี k-means ซึ่งเป็นหนึ่งในเทคนิคการวิเคราะห์ข้อมูลที่มีประสิทธิภาพในการจำแนกและจัดหมวดหมู่ข้อมูลที่มีความซับซ้อน วิธีนี้ช่วยให้สามารถระบุและจัดกลุ่มข้อมูลที่มีลักษณะคล้ายกันอย่างแม่นยำ เพื่อให้การวิเคราะห์ข้อมูลเป็นไปอย่างมีประสิทธิภาพมากขึ้น โดยเฉพาะในการจัดการข้อมูลที่ต้องมีการตอบสนองในเวลาจริง (real-time) ในโลกดิจิทัลที่มีการเปลี่ยนแปลงข้อมูลอย่างรวดเร็ว การใช้เทคนิค k-means จึงช่วยให้สามารถเข้าถึงและใช้ประโยชน์จากข้อมูลได้อย่างมีประสิทธิภาพมากขึ้น ในการตัดสินใจหรือวางแผนธุรกิจที่เกี่ยวข้องกับข้อมูล (Barradas et al., 2022)

สถาปัตยกรรมข้อมูล หมายถึง การจัดการโครงสร้างข้อมูลสำหรับระบบโครงข่ายดิจิทัล (Digital Grid) เน้นการจัดการโครงสร้างข้อมูลที่สามารถรองรับและประมวลผลข้อมูลจำนวนมหาศาลอย่างมีประสิทธิภาพ โดยใช้เทคโนโลยีบล็อกเชน (Blockchain) และเทคโนโลยีนาโน (Nanomaterial

Technology) เพื่อเสริมสร้างความมั่นคงและความน่าเชื่อถือของข้อมูลในระบบดิจิทัล บล็อกเชนมีบทบาทสำคัญในการตรวจสอบและรักษาความปลอดภัยของข้อมูล โดยการใช้การเข้ารหัสและการกระจายข้อมูลในรูปแบบที่ไม่สามารถเปลี่ยนแปลงได้ ซึ่งทำให้ข้อมูลมีความปลอดภัยและสามารถตรวจสอบได้ในทุกขั้นตอน เทคโนโลยีนาโนมุ่งเน้นไปที่การพัฒนาวัสดุที่มีคุณสมบัติพิเศษในการช่วยเพิ่มประสิทธิภาพในการประมวลผลข้อมูลและการจัดเก็บข้อมูล โดยใช้วัสดุนาโนที่มีความสามารถในการรองรับการประมวลผลข้อมูลที่รวดเร็วและมีประสิทธิภาพสูง ซึ่งทั้งสองเทคโนโลยีนี้ร่วมกันสร้างโครงสร้างข้อมูลที่สามารถรองรับความต้องการของระบบโครงข่ายดิจิทัลได้อย่างครบถ้วนและปลอดภัย (Long et al., 2022)

สรุปได้ว่า สถาปัตยกรรมข้อมูล หมายถึง การออกแบบและการจัดโครงสร้างข้อมูลภายในองค์กรหรือระบบต่าง ๆ เพื่อรองรับการจัดการและประมวลผลข้อมูลอย่างมีประสิทธิภาพ โดยการใช้เทคโนโลยีและเครื่องมือที่ทันสมัย เช่น บล็อกเชน, การเรียนรู้ของเครื่อง, และการประมวลผลข้อมูลขนาดใหญ่ เพื่อเสริมสร้างความมั่นคง ความปลอดภัย และประสิทธิภาพในการใช้งานข้อมูลในด้านต่าง ๆ เช่น การวิเคราะห์ข้อมูล, การประมวลผลข้อมูลในโลกดิจิทัล, การป้องกันข้อมูลจากภัยคุกคาม, และการรองรับการประมวลผลแบบเรียลไทม์ โดยการออกแบบสถาปัตยกรรมข้อมูลนี้สามารถรองรับข้อมูลที่หลากหลายรูปแบบ เช่น ข้อมูลจากเครือข่ายสังคมออนไลน์, ข้อมูลที่เกี่ยวข้องกับปัญญาประดิษฐ์, หรือข้อมูลจากแหล่งข้อมูลที่ซับซ้อน เพื่อสนับสนุนการตัดสินใจและการพัฒนาระบบที่มีประสิทธิภาพสูงและปลอดภัย

2.1.3.3. สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture)

2.1.3.3.1 ความหมาย

สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture) หมายถึง โครงสร้างและการออกแบบระบบแอปพลิเคชันที่มุ่งเน้นการสนับสนุนเป้าหมายเชิงกลยุทธ์ขององค์กร โดยเน้นการบูรณาการและการจัดการแอปพลิเคชันต่าง ๆ ให้ทำงานร่วมกันได้อย่างมีประสิทธิภาพ สถาปัตยกรรมนี้เป็นส่วนสำคัญในกรอบของสถาปัตยกรรมองค์กร (Enterprise Architecture) ที่ช่วยสร้างความเชื่อมโยงระหว่างสถาปัตยกรรมข้อมูล (Data Architecture), สถาปัตยกรรมเทคโนโลยี (Technology Architecture) และสถาปัตยกรรมธุรกิจ (Business Architecture) ทำให้กระบวนการทางธุรกิจและการจัดการข้อมูลสามารถทำงานได้อย่างราบรื่นและตอบสนองต่อความต้องการขององค์กรได้อย่างยืดหยุ่น บทความยังชี้ให้เห็นว่า การวางโครงสร้างระบบแอปพลิเคชันอย่างเหมาะสมจะช่วยลดความซับซ้อนของระบบ IT และเพิ่มประสิทธิภาพในการจัดการทรัพยากร โดยการออกแบบจะต้องคำนึงถึงคุณภาพที่สำคัญ เช่น ความสามารถในการทำงานร่วมกัน (Interoperability), ความ

เสถียร (Reliability), และความยืดหยุ่น (Adaptability) เพื่อรองรับการเปลี่ยนแปลงในอนาคตและเพิ่มความคล่องตัวให้กับองค์กรในการแข่งขันทางธุรกิจ (Karande & Joshi, 2022b)

สถาปัตยกรรมระบบแอปพลิเคชัน หมายถึง การออกแบบและโครงสร้างระบบแอปพลิเคชันที่สนับสนุนการวิจัยและพัฒนา ในอุตสาหกรรมเภสัชกรรม โดยเน้นการเชื่อมโยงและการบูรณาการระบบแอปพลิเคชันต่าง ๆ เข้าด้วยกัน เพื่อจัดการข้อมูลที่มีความซับซ้อนและมีปริมาณมากที่เกิดจากกระบวนการ R&D บทความชี้ให้เห็นว่าสถาปัตยกรรมนี้ช่วยให้การไหลเวียนข้อมูลเป็นไปอย่างราบรื่น ลดความซ้ำซ้อนของระบบ และเพิ่มประสิทธิภาพการทำงานร่วมกันระหว่างทีมวิจัย ระบบแอปพลิเคชันยังถูกออกแบบให้รองรับการวิเคราะห์ข้อมูลเชิงลึก (Data Analytics) และการประมวลผลข้อมูลแบบเรียลไทม์ เพื่อช่วยในกระบวนการตัดสินใจและการพัฒนานวัตกรรมใหม่ ๆ อย่างรวดเร็วและแม่นยำ นอกจากนี้ ยังมีการนำแนวคิดการขับเคลื่อนด้วยข้อมูล (Data-Driven Approach) มาใช้ในการออกแบบสถาปัตยกรรม เพื่อสร้างความยืดหยุ่นและความสามารถในการปรับตัวต่อความท้าทายที่เปลี่ยนแปลงอย่างรวดเร็วในอุตสาหกรรมเภสัชกรรม (Uzhakova & Fischer, 2024b)

สถาปัตยกรรมระบบแอปพลิเคชัน หมายถึง โครงสร้างเชิงตรรกะและการออกแบบระบบแอปพลิเคชันที่ใช้ในองค์กร โดยมีจุดมุ่งหมายเพื่อสร้างความสอดคล้องระหว่างฟังก์ชันการทำงานของแอปพลิเคชันและกระบวนการทางธุรกิจ สถาปัตยกรรมนี้มีบทบาทสำคัญในการบูรณาการระบบแอปพลิเคชันต่าง ๆ ภายในองค์กรให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ โดยบทความได้เน้นถึงการใช้ออนโทโลยี (Ontology) เป็นเครื่องมือในการสร้างแบบจำลองและปรับปรุงคุณภาพของสถาปัตยกรรมระบบแอปพลิเคชัน เพื่อช่วยให้ผู้ใช้งานสามารถเข้าใจความสัมพันธ์ระหว่างส่วนประกอบต่าง ๆ ภายในระบบได้อย่างชัดเจน สถาปัตยกรรมนี้ยังช่วยเพิ่มความสามารถในการวิเคราะห์และปรับปรุงกระบวนการทำงาน โดยรองรับการเปลี่ยนแปลงและความซับซ้อนขององค์กรในระยะยาว นอกจากนี้ การใช้แนวทางออนโทโลยียังช่วยเสริมสร้างความถูกต้อง ความสมบูรณ์ และความสอดคล้องของโมเดลสถาปัตยกรรม ซึ่งเป็นปัจจัยสำคัญในการสร้างมูลค่าและประสิทธิภาพของระบบแอปพลิเคชันในภาพรวม (Schoonderbeek & Proper, 2024)

สถาปัตยกรรมระบบแอปพลิเคชัน หมายถึง การออกแบบและจัดโครงสร้างของระบบแอปพลิเคชันที่รองรับการพัฒนาระบบเว็บสำหรับการจับคู่ความเข้ากันได้ของงานและอาชีพ โดยใช้วิธีการจากกรอบสถาปัตยกรรมองค์กรของรัฐบาลกลาง (Federal Enterprise Architecture Framework: FEAF) สถาปัตยกรรมนี้มุ่งเน้นการเชื่อมโยงระหว่างการทำงานของแอปพลิเคชันและกระบวนการสนับสนุนที่จำเป็น เช่น การรวบรวมข้อมูลจากผู้ใช้ การประมวลผลข้อมูลเพื่อสร้างคำแนะนำที่เหมาะสม และการแสดงผลในรูปแบบที่ใช้งานง่าย นอกจากนี้ บทความยังเน้นว่าการใช้ FEAF ช่วยกำหนดโครงสร้างและโมเดลที่มีความชัดเจนและเป็นมาตรฐานสำหรับการพัฒนาแอปพลิเคชัน ทำให้

ระบบสามารถตอบสนองต่อความต้องการของผู้ใช้ในมหาวิทยาลัยได้อย่างมีประสิทธิภาพและปรับเปลี่ยนได้ตามความต้องการในอนาคต (Muslih et al., 2024d)

สถาปัตยกรรมระบบแอปพลิเคชัน หมายถึง การออกแบบโครงสร้างของแอปพลิเคชันที่รองรับการพัฒนาและการจัดการโครงการด้านการเรียนรู้ของเครื่อง(Machine Learning) โดยใช้กรอบสถาปัตยกรรมองค์กรเป็นฐาน ในที่นี้ สถาปัตยกรรมระบบแอปพลิเคชันจะเน้นการออกแบบที่เชื่อมโยงและจัดการส่วนประกอบต่างๆ ของระบบ เช่น การเตรียมข้อมูล การสร้างและฝึกโมเดล การประมวลผลข้อมูล และการประเมินผลแอปพลิเคชันให้สามารถทำงานได้อย่างมีประสิทธิภาพ นอกจากนี้ยังคำนึงถึงการจัดการและการวางแผนโครงการในมุมมองเชิงกลยุทธ์ โดยการใช้เมตาโมเดลจากสถาปัตยกรรมองค์กร (Enterprise Architecture) เพื่อจัดการกับความซับซ้อนและสร้างความโปร่งใสในการพัฒนาและจัดการโครงการ Machine Learning ซึ่งจะช่วยเพิ่มความยั่งยืนและประสิทธิภาพในกระบวนการทางธุรกิจและเทคโนโลยี (Takeuchi et al., 2024c)

สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture) หมายถึง การออกแบบและพัฒนาโครงสร้างของแอปพลิเคชันที่รองรับความต้องการทางธุรกิจของธุรกิจที่พักในพื้นที่ชนบท โดยเฉพาะในภูมิภาคที่มีปัญหาการยุบตัวของประชากร ในบริบทนี้ สถาปัตยกรรมระบบแอปพลิเคชันจะเชื่อมโยงการทำงานของแอปพลิเคชันต่างๆ ที่เกี่ยวข้องกับการจัดการทรัพยากรธุรกิจ การจองห้องพัก การจัดการลูกค้า และการให้บริการ เพื่อสนับสนุนการดำเนินงานของธุรกิจในพื้นที่ที่ขาดแคลนทรัพยากรและการสนับสนุนทางเทคโนโลยี สถาปัตยกรรมนี้มุ่งเน้นที่การพัฒนาระบบที่มีความยืดหยุ่นและสามารถปรับตัวได้ดีในสภาวะที่เปลี่ยนแปลง เพื่อเสริมสร้างความยั่งยืนและความสามารถในการแข่งขันในตลาดที่พักของพื้นที่ชนบท (Anes Silveira & Mamede, 2024)

สถาปัตยกรรมระบบแอปพลิเคชัน หมายถึง การออกแบบและกำหนดโครงสร้างที่รองรับการพัฒนาและการดำเนินการของแอปพลิเคชันในองค์กร ซึ่งรวมถึงการกำหนดวิธีการเชื่อมต่อ การจัดการข้อมูล และฟังก์ชันการทำงานต่างๆ ของระบบที่สนับสนุนการทำงานของธุรกิจให้มีประสิทธิภาพสูงสุด สถาปัตยกรรมนี้ช่วยให้การพัฒนาแอปพลิเคชันสามารถตอบสนองต่อความต้องการขององค์กรได้อย่างมีประสิทธิภาพ โดยพิจารณาจากคุณภาพและมาตรฐานต่างๆ เช่น ความยืดหยุ่น ความปลอดภัย และการบำรุงรักษาที่ง่ายขึ้น การจัดการแอปพลิเคชันต้องคำนึงถึงการใช้งานที่สอดคล้องกับกลยุทธ์ทางธุรกิจ และสามารถปรับตัวได้ตามการเปลี่ยนแปลงของเทคโนโลยีและความต้องการของตลาด (Karande & Joshi, 2022b)

สถาปัตยกรรมระบบแอปพลิเคชัน หมายถึง การออกแบบโครงสร้างของแอปพลิเคชันในองค์กร โดยเน้นที่การกำหนดวิธีการที่แอปพลิเคชันจะเชื่อมต่อและทำงานร่วมกันกับระบบต่างๆ ในองค์กร เพื่อสนับสนุนกระบวนการทางธุรกิจและการจัดการด้านไอทีอย่างมีประสิทธิภาพ

สถาปัตยกรรมนี้ไม่เพียงแต่รวมถึงการออกแบบฟังก์ชันการทำงานของแอปพลิเคชันเท่านั้น แต่ยังรวมถึงการวางแผนเกี่ยวกับการบำรุงรักษา ความยืดหยุ่นในการปรับขนาด และความปลอดภัยของระบบ การออกแบบสถาปัตยกรรมระบบแอปพลิเคชันในบทความนี้จึงมุ่งหวังที่จะสร้างกรอบการทำงานที่สามารถรองรับการเปลี่ยนแปลงทางเทคโนโลยีและการขยายตัวขององค์กรในระยะยาว ขณะเดียวกันยังคำนึงถึงการเชื่อมต่อระหว่างระบบต่างๆ ในลักษณะที่มีประสิทธิภาพและเป็นมิตรกับการจัดการทรัพยากรไอที (Dumitriu & Popescu, 2020b)

สรุปได้ว่า สถาปัตยกรรมระบบแอปพลิเคชัน คือ การออกแบบโครงสร้างและการจัดระเบียบของแอปพลิเคชันในองค์กร โดยมุ่งเน้นการกำหนดวิธีการที่แอปพลิเคชันต่างๆ จะเชื่อมโยงและทำงานร่วมกับระบบอื่นๆ ในองค์กร เพื่อสนับสนุนกระบวนการทางธุรกิจและการจัดการด้านไอทีอย่างมีประสิทธิภาพ การออกแบบนี้รวมถึงการพิจารณาฟังก์ชันการทำงาน การบำรุงรักษา การปรับขนาด ความปลอดภัย และความยืดหยุ่นของระบบ เพื่อให้สามารถรองรับการเปลี่ยนแปลงทางเทคโนโลยีและการขยายตัวขององค์กรในระยะยาว นอกจากนี้ยังเน้นการเชื่อมต่อระหว่างแอปพลิเคชันและระบบต่างๆ อย่างมีประสิทธิภาพ เพื่อให้สามารถบริหารจัดการทรัพยากรไอทีได้อย่างเหมาะสมและสนับสนุนการเติบโตขององค์กร

2.1.3.4. สถาปัตยกรรมเทคโนโลยี (Technology Architecture)

2.1.3.4.1 ความหมาย

สถาปัตยกรรมเทคโนโลยี (Technology Architecture) หมายถึง การสร้างโครงสร้างพื้นฐานทางเทคโนโลยีที่รองรับการดำเนินงานของโครงการ Machine Learning (ML) โดยรวมถึงการออกแบบเทคโนโลยีที่ใช้ในการรวบรวมข้อมูล การฝึกโมเดล การจัดการการประมวลผลที่มีประสิทธิภาพ รวมถึงการบูรณาการระบบต่างๆ เช่น ฮาร์ดแวร์และซอฟต์แวร์ที่เหมาะสมกับการพัฒนาโครงการ ML เพื่อเพิ่มประสิทธิภาพและความยืดหยุ่นในกระบวนการวิจัยและพัฒนา (Takeuchi et al., 2024c)

สถาปัตยกรรมเทคโนโลยี หมายถึง การใช้เทคโนโลยีที่ช่วยปรับปรุงความยืดหยุ่นและการตอบสนองของธุรกิจที่พักในพื้นที่ชนบท โดยเน้นการใช้ IoT, ระบบการจัดการข้อมูลและเทคโนโลยีคลาวด์เพื่อช่วยในการจัดการกระบวนการต่างๆ ในธุรกิจ เช่น การตรวจสอบสภาพแวดล้อม การจัดการการบริการ และการเพิ่มขีดความสามารถในการแข่งขันในตลาดที่มีความเปลี่ยนแปลง (Anes Silveira & Mamede, 2024)

สถาปัตยกรรมเทคโนโลยี หมายถึง การออกแบบเทคโนโลยีที่รองรับการประเมินและการวัดคุณภาพของ Enterprise Architecture โดยใช้มาตรฐานเทคโนโลยีที่ได้รับการยอมรับเพื่อประเมินประสิทธิภาพในการดำเนินงาน การจัดการข้อมูล และการรองรับการใช้งานที่สามารถขยายตัวและพัฒนาได้ในอนาคต เช่น การใช้ระบบที่สามารถวัดผลลัพธ์และปรับปรุงได้ (Karande & Joshi, 2022b)

สถาปัตยกรรมเทคโนโลยี หมายถึง โครงสร้างพื้นฐานทางเทคโนโลยีที่ออกแบบเพื่อรองรับการจัดการระบบ IT ภายในองค์กร โดยมีการใช้เทคโนโลยีการจัดการข้อมูล (Data Management) การจัดการเครือข่าย (Network Management) และการวางแผนระบบ (System Planning) เพื่อให้ระบบ IT ภายในองค์กรทำงานได้อย่างมีประสิทธิภาพและมีความยืดหยุ่นในการตอบสนองความต้องการของธุรกิจ (Dumitriu & Popescu, 2020b)

สถาปัตยกรรมเทคโนโลยี หมายถึง การออกแบบระบบเทคโนโลยีที่ใช้ Big Data, AI, และ Cloud Computing เพื่อสนับสนุนการวิจัยและพัฒนาในอุตสาหกรรมเภสัชกรรม โดยมุ่งเน้นการใช้เทคโนโลยีในการรวบรวมและประมวลผลข้อมูลขนาดใหญ่จากแหล่งข้อมูลต่างๆ เช่น ผลการทดลองการวิจัยคลินิก และการศึกษาเชิงลึก เพื่อช่วยในการตัดสินใจและการพัฒนาเทคโนโลยีใหม่ๆ (Uzhakova & Fischer, 2024b)

สถาปัตยกรรมเทคโนโลยี หมายถึง การออกแบบโครงสร้างทางเทคโนโลยีที่ให้ความสำคัญกับความมั่นคงปลอดภัยทางไซเบอร์และความสามารถในการฟื้นตัวจากเหตุการณ์ที่ไม่คาดคิด โดยการใช้เทคโนโลยีในการป้องกันข้อมูลและตรวจจับภัยคุกคาม เช่น การเข้ารหัสข้อมูล ระบบป้องกันการโจมตี และเทคโนโลยีเครือข่ายที่ปลอดภัย (Al-Turkistani et al., 2021b)

สถาปัตยกรรมเทคโนโลยี หมายถึง การใช้โครงสร้างทางเทคโนโลยีที่ออกแบบตามกรอบของ Zachman Framework เพื่อสนับสนุนการออกแบบและการจัดการระบบ IT ภายในโรงเรียน โดยใช้เทคโนโลยีต่างๆ เช่น ระบบการจัดการการเรียนการสอน (LMS) และการจัดการทรัพยากรองค์กร (ERP) เพื่อรองรับการดำเนินงานและการศึกษา (Aprilia et al., 2024b)

สถาปัตยกรรมเทคโนโลยี หมายถึง การใช้เทคโนโลยีเพื่อสนับสนุนการเปลี่ยนแปลงทางดิจิทัลขององค์กร โดยการใช้เทคโนโลยีที่รองรับการเปลี่ยนแปลง เช่น Cloud Computing, API, และ Microservices ที่ช่วยเพิ่มความยืดหยุ่นในการพัฒนาและรองรับการขยายตัวขององค์กรในยุคดิจิทัล (Alghamdi, 2024)

สถาปัตยกรรมเทคโนโลยี หมายถึง การปรับใช้เทคโนโลยีที่ทันสมัย เช่น ระบบอัตโนมัติ (Automation), แพลตฟอร์มการเรียนรู้ (Learning Platforms) และเทคโนโลยีคลาวด์ (Cloud

Technology) เพื่อเสริมสร้างการพัฒนาองค์กรการศึกษาในยุคดิจิทัล โดยมีเป้าหมายในการพัฒนากระบวนการเรียนการสอนและการบริหารจัดการที่มีประสิทธิภาพมากยิ่งขึ้น (Amin et al., 2024)

สถาปัตยกรรมเทคโนโลยี หมายถึง การพัฒนาเทคโนโลยีที่ยืดหยุ่น เช่น Microservices, API และ Cloud Computing เพื่อรองรับการเปลี่ยนแปลงทางดิจิทัลในสถาบันการศึกษา โดยมีเป้าหมายในการเพิ่มประสิทธิภาพในการดำเนินงานและการให้บริการแก่ผู้เรียน (Sararuch et al., 2023b)

สถาปัตยกรรมเทคโนโลยี หมายถึง การใช้เทคโนโลยีในการออกแบบและวิเคราะห์ความปลอดภัยของโครงสร้างพื้นฐานที่สำคัญ เช่น การใช้ระบบป้องกันภัยคุกคาม (Cybersecurity Systems), การตรวจจับช่องโหว่และการวิเคราะห์ความเสี่ยงของระบบ IT เพื่อปกป้องข้อมูลที่สำคัญ (Y. Jiang et al., 2024b)

สรุปได้ว่า สถาปัตยกรรมเทคโนโลยี หมายถึง โครงสร้างและการออกแบบระบบทางเทคโนโลยีที่รองรับการทำงานขององค์กรและโครงการต่างๆ โดยใช้เทคโนโลยีที่เหมาะสมในการสนับสนุนกระบวนการต่างๆ เช่น การจัดการข้อมูล, การประมวลผล, การสื่อสาร, การรักษาความปลอดภัย, และการทำงานร่วมกันในระบบที่ซับซ้อน ซึ่งในบริบทต่างๆ สถาปัตยกรรมเทคโนโลยีจะเน้นการเลือกใช้เทคโนโลยีที่ช่วยเพิ่มประสิทธิภาพ, ความยืดหยุ่น, และความปลอดภัย โดยเทคโนโลยีต่างๆ เช่น Cloud Computing, IoT, Microservices, AI, และ Cybersecurity Systems ถูกนำมาใช้เพื่อรองรับการดำเนินงานในสภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ทั้งนี้เพื่อให้ระบบสามารถปรับตัวและรองรับการขยายตัวในอนาคตได้อย่างมีประสิทธิภาพ

2.1.3.5. สถาปัตยกรรมด้านความปลอดภัย (Security Architecture)

2.1.3.5.1 ความหมาย

สถาปัตยกรรมด้านความปลอดภัย (Security Architecture) หมายถึง การออกแบบโครงสร้างเครือข่ายที่มุ่งเน้นการป้องกันภัยคุกคามและลดช่องโหว่ของระบบ โดยใช้หลักการรักษาความปลอดภัยแบบบูรณาการที่ครอบคลุมตั้งแต่การควบคุมการเข้าถึงข้อมูล การตรวจสอบกิจกรรมในเครือข่าย ไปจนถึงการตอบสนองต่อเหตุการณ์ที่อาจเป็นอันตราย ระบบดังกล่าวต้องพึ่งพากระบวนการเชิงรุก เช่น การวิเคราะห์พฤติกรรมการใช้งานที่ผิดปกติ การติดตั้งระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection and Prevention Systems: IDPS) และการใช้เทคโนโลยีเข้ารหัสขั้นสูง เพื่อรับประกันความปลอดภัยในทุกระดับของการดำเนินงาน นอกจากนี้ สถาปัตยกรรมด้านความปลอดภัยยังถูกออกแบบให้มีความสามารถในการปรับตัวต่อภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็วในสภาพแวดล้อมดิจิทัล เช่น การโจมตีไซเบอร์รูปแบบใหม่ การแอบแฝงในระบบ และการ

โจมตีแบบปฏิเสธการให้บริการ (DDoS) งานวิจัยนี้ชี้ให้เห็นถึงความสำคัญของการนำแนวทาง Zero Trust Architecture ซึ่งมุ่งเน้นการตรวจสอบและยืนยันความปลอดภัยทุกครั้งที่มีการเข้าถึงระบบมาใช้ในการพัฒนาเครือข่ายที่ปลอดภัยมากขึ้น (W. Jiang et al., 2021)

สถาปัตยกรรมด้านความปลอดภัย หมายถึง การกำหนดข้อจำกัดด้านการออกแบบเชิงโครงสร้างที่เน้นให้ระบบและแอปพลิเคชันมีความปลอดภัยตั้งแต่ขั้นตอนการออกแบบเบื้องต้น โดยการรักษาความปลอดภัยไม่ได้ถูกมองว่าเป็นคุณสมบัติที่เพิ่มเข้ามาภายหลัง แต่เป็นส่วนหนึ่งของกระบวนการออกแบบสถาปัตยกรรมที่ครอบคลุมการวิเคราะห์ความเสี่ยง การวางแผนการจัดการภัยคุกคาม และการกำหนดมาตรการป้องกันล่วงหน้า ในมุมมองของงานวิจัยนี้ สถาปัตยกรรมด้านความปลอดภัยต้องพิจารณาข้อกำหนดเชิงโครงสร้าง เช่น การกำหนดบทบาทและสิทธิ์การเข้าถึงข้อมูล (Access Control) การปกป้องความลับและความสมบูรณ์ของข้อมูล (Confidentiality and Integrity) และการออกแบบระบบที่สามารถตรวจสอบและฟื้นฟูได้ในกรณีเกิดเหตุการณ์ไม่พึงประสงค์ แนวทางนี้สอดคล้องกับหลักการ Secure by Design ที่เน้นการป้องกันภัยคุกคามที่อาจเกิดขึ้นในทุกขั้นตอนของการพัฒนาระบบ (Ravi et al., 2019)

สถาปัตยกรรมด้านความปลอดภัย หมายถึง การออกแบบระบบที่ให้ความสำคัญกับความปลอดภัยเป็นอันดับแรก โดยเน้นการใช้ตัวประมวลผลความปลอดภัยแบบแยกส่วนทางกายภาพ (Physically Isolated Active Security Processors - PASPs) เพื่อปกป้องข้อมูลและระบบจากภัยคุกคามที่มีความซับซ้อนในอนาคต โครงสร้างนี้ถูกพัฒนาเพื่อแยกกระบวนการที่เกี่ยวข้องกับความปลอดภัยออกจากการประมวลผลทั่วไป ช่วยลดโอกาสที่ภัยคุกคามจะเข้าถึงหรือโจมตีระบบหลัก (Meng et al., 2018)

สถาปัตยกรรมด้านความปลอดภัย หมายถึง การกำหนดมาตรฐานและโครงสร้างเพื่อป้องกันความเสี่ยงด้านความปลอดภัยในระบบสารสนเทศขององค์กร โดยการใช้แนวคิดเชิงออนโทโลยี (Ontology) เพื่อสร้างแบบจำลองที่ช่วยให้สามารถกำหนดคุณลักษณะด้านความปลอดภัยได้อย่างเป็นระบบและชัดเจน งานวิจัยนี้ชี้ให้เห็นว่าสถาปัตยกรรมด้านความปลอดภัยต้องผสานรวมกับมิติอื่นๆ ของสถาปัตยกรรมองค์กร เช่น แอปพลิเคชัน ข้อมูล และเทคโนโลยี เพื่อให้เกิดความสอดคล้องในระดับโครงสร้างทั้งหมด การออกแบบเน้นการวิเคราะห์ความเสี่ยง การกำหนดกลไกควบคุม (Control Mechanisms) และการบูรณาการความปลอดภัยเข้ากับกระบวนการธุรกิจและระบบสารสนเทศขององค์กร นอกจากนี้ยังเน้นความสำคัญของการพัฒนาคุณภาพโมเดลความปลอดภัยเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพและตอบสนองความต้องการขององค์กรในยุคดิจิทัล (Schoonderbeek & Proper, 2024)

สถาปัตยกรรมด้านความปลอดภัย หมายถึง โครงสร้างเชิงกลยุทธ์ที่เน้นการออกแบบระบบเพื่อสร้างภูมิคุ้มกันดิจิทัล (Digital Immune Systems) โดยมีวัตถุประสงค์เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในยุคที่การโจมตีมีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว โดยประกอบด้วยองค์ประกอบหลัก คือ การใช้เทคโนโลยีปัญญาประดิษฐ์ ในการตรวจจับและตอบสนองต่อภัยคุกคาม การออกแบบระบบให้มีความยืดหยุ่น (Resilience) เพื่อรับมือกับการโจมตีที่ไม่คาดคิด และการสร้างระบบป้องกันแบบองค์รวมที่ครอบคลุมทั้งเครือข่าย แอปพลิเคชัน และข้อมูล งานวิจัยยังเน้นย้ำถึงความสำคัญของการบูรณาการกลยุทธ์ด้านความปลอดภัยเข้ากับโครงสร้างพื้นฐานดิจิทัลขององค์กรอย่างเป็นระบบ เพื่อเพิ่มประสิทธิภาพในการป้องกันและฟื้นฟูระบบหลังเกิดการโจมตี (George et al., 2023b)

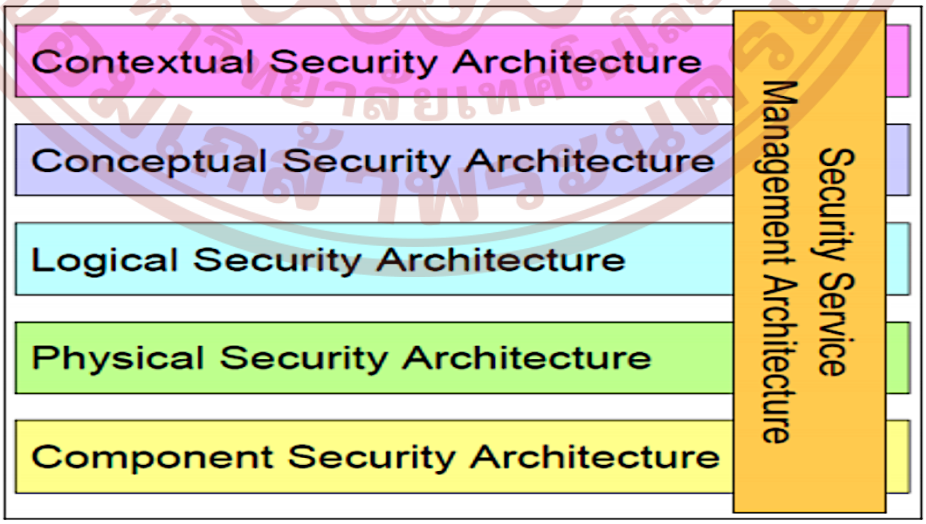
สถาปัตยกรรมด้านความปลอดภัย หมายถึง กรอบโครงสร้างที่ออกแบบมาเพื่อรับมือกับการโจมตีทางไซเบอร์ที่ไม่เคยรู้จักมาก่อน (Unknown Cyberattacks) โดยใช้แนวคิดจากระบบภูมิคุ้มกันของมนุษย์เป็นต้นแบบ การออกแบบสถาปัตยกรรมนี้มุ่งเน้นการสร้างระบบตรวจจับการบุกรุก (Intrusion Detection System หรือ IDS) ที่สามารถตอบสนองและป้องกันการโจมตีได้อย่างอัตโนมัติ องค์ประกอบหลัก คือ 1) การเรียนรู้จากภัยคุกคามใหม่ๆ ระบบใช้ปัญญาประดิษฐ์และเทคนิคการจำลองการตอบสนองของระบบภูมิคุ้มกัน (Artificial Immunity) เพื่อเรียนรู้พฤติกรรมของภัยคุกคามและสร้าง เพื่อรับมือกับการโจมตีในอนาคต "แอนติบอดีดิจิทัล" 2) การตรวจจับที่หลากหลายและแม่นยำ ระบบสามารถวิเคราะห์รูปแบบของข้อมูลที่แปลกปลอมและไม่เคยพบเจอมาก่อน พร้อมแจ้งเตือนเมื่อพบกิจกรรมที่น่าสงสัย และ 3) การตอบสนองแบบปรับตัว เมื่อระบบตรวจจับการโจมตี มันสามารถปรับกลยุทธ์ป้องกันโดยอัตโนมัติ เช่น การจำกัดการเข้าถึงหรือการกักกันเครือข่าย (Huang et al., 2023a)

สถาปัตยกรรมด้านความปลอดภัย หมายถึง กรอบแนวคิดและการออกแบบโครงสร้างที่ใช้เทคโนโลยีปัญญาประดิษฐ์ เพื่อสนับสนุนการตรวจจับความผิดปกติ (Anomaly Detection) และเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ โดยเน้นบทบาทของสถาปัตยกรรมด้านความปลอดภัยในการเรียนรู้และป้องกันภัยคุกคามในสภาพแวดล้อมการศึกษา องค์ประกอบสำคัญ คือ การตรวจจับความผิดปกติด้วย AI ใช้โมเดล AI เช่น การเรียนรู้เชิงลึก (Deep Learning) ในการวิเคราะห์พฤติกรรมที่ไม่ปกติในเครือข่าย เพื่อระบุภัยคุกคาม เช่น 1) การบุกรุก (Intrusion) หรือมัลแวร์ 2) แพลตฟอร์มเพื่อการศึกษา ระบบถูกออกแบบให้เป็นเครื่องมือการเรียนรู้เพื่อช่วยผู้ใช้งาน โดยเฉพาะนักศึกษาและบุคลากรในสถาบันการศึกษา ให้สามารถเข้าใจและจัดการภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ 3) การสร้างความตระหนักรู้ด้านความปลอดภัย นอกจากการตรวจจับและตอบสนองต่อภัยคุกคาม แพลตฟอร์มนี้ยังสนับสนุนการเรียนรู้เกี่ยวกับแนวทางการป้องกันและลดความเสี่ยงจาก

การโจมตี 4) ความยืดหยุ่นและการปรับตัว สถาปัตยกรรมถูกออกแบบให้สามารถปรับตัวเข้ากับรูปแบบการโจมตีใหม่ๆ และพฤติกรรมที่เปลี่ยนแปลงของผู้โจมตี (Ortiz-Garcés et al., 2024a)

สถาปัตยกรรมด้านความปลอดภัย หมายถึง โครงสร้างที่เน้นการป้องกันและตรวจจับการโจมตีทางไซเบอร์ในระบบอินเทอร์เน็ตของสรรพสิ่ง (IoT) โดยใช้เทคนิคปัญญาประดิษฐ์ เช่น การเรียนรู้ของเครื่อง (Machine Learning) และการเรียนรู้เชิงลึก (Deep Learning) เพื่อวิเคราะห์ข้อมูลจากอุปกรณ์ IoT และตรวจหาภัยคุกคามที่อาจเกิดขึ้น ระบบนี้ต้องสามารถจัดการกับปริมาณข้อมูลที่มีความหลากหลายและมาจากแหล่งที่ต่างกันในเครือข่าย IoT ที่มักมีข้อจำกัดในด้านการประมวลผลและความปลอดภัย การใช้ AI ในการตรวจจับภัยคุกคามที่ไม่เคยพบมาก่อนหรือที่ไม่สามารถระบุได้ในระบบ IoT จึงเป็นสิ่งสำคัญในการรักษาความปลอดภัย โดยสถาปัตยกรรมนี้ออกแบบมาเพื่อให้สามารถปรับตัวและตอบสนองต่อภัยคุกคามใหม่ๆ ได้อย่างมีประสิทธิภาพ ช่วยให้ระบบ IoT สามารถทำงานได้อย่างปลอดภัยและต่อเนื่องแม้จะมีภัยคุกคามที่มีความซับซ้อนและไม่รู้จัก (Abdullahi et al., 2022a)

สถาปัตยกรรมด้านความปลอดภัย หมายถึง กรอบการทำงานที่ช่วยในการออกแบบและจัดการโครงสร้างพื้นฐานด้านความปลอดภัยขององค์กร โดยมุ่งเน้นการสร้างสภาพแวดล้อมที่ปลอดภัยสำหรับข้อมูลและระบบต่างๆ ภายในองค์กร ซึ่งรวมถึงการกำหนดนโยบาย ความเสี่ยง และมาตรการที่จำเป็นในการป้องกันภัยคุกคามทางไซเบอร์ นอกจากนี้ สถาปัตยกรรมด้านความปลอดภัยยังมีบทบาทในการสนับสนุนการตัดสินใจทางธุรกิจ โดยการพิจารณาความต้องการด้านความปลอดภัยของผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร เพื่อให้แน่ใจว่ามีการจัดการความเสี่ยงอย่างมีประสิทธิภาพและสอดคล้องกับกลยุทธ์ทางธุรกิจ (Al-Turkistani et al., 2021a)



ภาพที่ 2-4 SABSA Architecture (Al-Turkistani et al., 2021a)

จากภาพที่ 2-4 SABSA (Sherwood Applied Business Security Architecture) เป็นกรอบการทำงานที่มุ่งเน้นการสร้างสถาปัตยกรรมความปลอดภัยขององค์กร โดยมีการจัดระเบียบในรูปแบบของชั้นต่าง ๆ ซึ่งแต่ละชั้นจะนำเสนอวิสัยทัศน์ที่สำคัญของผู้มีส่วนได้ส่วนเสียในกระบวนการขององค์กร โดยมีรายละเอียดดังนี้

1. Contextual Security Architecture - วิสัยทัศน์ทางธุรกิจ
2. Conceptual Security Architecture - วิสัยทัศน์ของสถาปนิก
3. Logical Security Architecture - วิสัยทัศน์ของนักออกแบบ
4. Physical Security Architecture - วิสัยทัศน์ของผู้สร้าง
5. Component Security Architecture - วิสัยทัศน์ของช่างเทคนิค
6. Operational Security Architecture – วิสัยทัศน์ของผู้จัดการสิ่งอำนวยความสะดวก

ชั้นการทำงานที่สำคัญที่สุดคือ Operational Security Architecture ซึ่งมีบทบาทในการเชื่อมโยงกับชั้นอื่น ๆ และมีการจัดการด้านการตอบสนองต่อเหตุการณ์ การฟื้นฟูจากภัยพิบัติ และการควบคุมการเปลี่ยนแปลง โดย SABSA จะไม่ใช้มาตรฐานหรือวิธีการของตนเอง แต่จะปฏิบัติตามมาตรฐานความปลอดภัยที่มีอยู่ เช่น ISO 2700x และ ITIL จะเห็นได้ว่า SABSA ถูกนำมาใช้บ่อยในองค์กรที่มีความสำคัญทางธุรกิจ โดยมีเป้าหมายในการพัฒนาการจัดการความเสี่ยงด้านความปลอดภัยขององค์กรและการรับประกันความปลอดภัยที่เกี่ยวข้องกับโครงสร้างพื้นฐาน (Al-Turkistani et al., 2021a)

สรุปได้ว่า สถาปัตยกรรมด้านความปลอดภัย หมายถึง การออกแบบโครงสร้างและกลไกที่ใช้ในการปกป้องระบบคอมพิวเตอร์และเครือข่ายจากภัยคุกคามและการโจมตีทางไซเบอร์ โดยการจัดการความเสี่ยงที่อาจเกิดขึ้นจากการเข้าถึงข้อมูลและทรัพยากรที่ไม่ถูกต้องและไม่พึงประสงค์ รวมทั้งการตรวจจับภัยคุกคามที่อาจเกิดขึ้นในระบบที่มีความซับซ้อนและหลากหลาย เช่น อินเทอร์เน็ตของสรรพสิ่ง (IoT) โดยสถาปัตยกรรมนี้จะรวมถึงการใช้เทคนิคและเครื่องมือที่สามารถตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ เช่น การใช้ปัญญาประดิษฐ์ ในการตรวจสอบพฤติกรรมที่ผิดปกติ การออกแบบเพื่อให้มั่นใจในความปลอดภัยของข้อมูลและการป้องกันการโจมตีแบบไม่รู้จัก รวมไปถึงการสร้างระบบที่สามารถปรับตัวและทำงานต่อเนื่องแม้ในสถานการณ์ที่เสี่ยงสูง ความมั่นคงและการป้องกันที่แข็งแกร่งในสถาปัตยกรรมความปลอดภัยจึงเป็นกุญแจสำคัญในการคงความปลอดภัยของข้อมูลและโครงสร้างพื้นฐานในโลกดิจิทัลที่ซับซ้อน

2.1.3.6. สถาปัตยกรรมการบูรณาการ (Integration Architecture)

2.1.3.6.1 ความหมาย

สถาปัตยกรรมการบูรณาการ (Integration Architecture) หมายถึง โครงสร้างที่ออกแบบมาเพื่อเชื่อมโยงระบบต่างๆ ภายในองค์กรเข้าด้วยกัน ทำให้ข้อมูลและกระบวนการทำงานสามารถแลกเปลี่ยนและใช้งานร่วมกันได้อย่างราบรื่น เป็นเสมือน ระหว่างระบบต่างๆ ที่ "สะพานเชื่อม" แตกต่างกัน ทั้งระบบเก่าและระบบใหม่ ระบบภายในและระบบภายนอก (Qurtubi, 2024)

สถาปัตยกรรมการบูรณาการ หมายถึง โครงสร้างที่มีบทบาทสำคัญในการเชื่อมโยงเครื่องมือ ระบบ และโมเดลต่าง ๆ ที่เกี่ยวข้องกับโครงการ Machine Learning ให้สามารถทำงานร่วมกันได้อย่างราบรื่น โดยมุ่งเน้นการจัดการข้อมูลและกระบวนการที่เกี่ยวข้องในทุกขั้นตอน ตั้งแต่การรวบรวมข้อมูล การเตรียมข้อมูล การพัฒนาโมเดล การทดสอบ และการนำไปใช้จริง (deployment) ซึ่งสถาปัตยกรรมการบูรณาการช่วยลดความซับซ้อนของการเชื่อมต่อระหว่างระบบ Machine Learning กับโครงสร้างพื้นฐาน (infrastructure) ขององค์กร ผ่านมาตรฐานและเครื่องมือที่ออกแบบมาเฉพาะสำหรับโครงการ Machine Learning นอกจากนี้ โครงสร้างนี้ยังช่วยสนับสนุนการทำงานร่วมกันระหว่างทีมงานในหลากหลายบทบาท เช่น นักวิจัยด้าน AI ผู้พัฒนาระบบ และผู้บริหาร โดยให้ความสำคัญกับการจัดการข้อมูลแบบครบวงจรและการปรับปรุงประสิทธิภาพของโครงการให้สอดคล้องกับเป้าหมายขององค์กรอย่างต่อเนื่อง (Takeuchi et al., 2024c)

สถาปัตยกรรมการบูรณาการ หมายถึง ครงสร้างสำคัญที่สนับสนุนการเชื่อมโยงและการบูรณาการระบบต่าง ๆ ภายในและภายนอกองค์กร โดยเฉพาะในบริบทของธุรกิจที่พักในชนบทที่ต้องเผชิญกับความท้าทายจากการลดลงของประชากรในพื้นที่ชนบท โครงสร้าง Integration Architecture ทำหน้าที่ประสานงานระหว่างแพลตฟอร์มการจองออนไลน์ ระบบการจัดการทรัพยากร (Resource Management Systems) และช่องทางการสื่อสารดิจิทัลต่าง ๆ เพื่อช่วยให้ธุรกิจเหล่านี้สามารถเพิ่มประสิทธิภาพการดำเนินงานและตอบสนองความต้องการของลูกค้าได้อย่างรวดเร็ว (Anes Silveira & Mamede, 2024)

สถาปัตยกรรมการบูรณาการ หมายถึง องค์ประกอบที่สำคัญในการเชื่อมโยงระบบและบริการต่าง ๆ ภายในองค์กร โดยมีเป้าหมายเพื่อสนับสนุนความสอดคล้องและประสิทธิภาพของโครงสร้างสถาปัตยกรรมองค์รวม (Enterprise Architecture) ในการเชื่อมโยงระบบ แอปพลิเคชัน และกระบวนการต่าง ๆ ภายในองค์กร เพื่อให้การทำงานเป็นไปอย่างไร้รอยต่อและสอดคล้องกับเป้าหมายเชิงกลยุทธ์ขององค์กร โครงสร้างนี้ช่วยลดความซับซ้อนในการจัดการระบบที่มีความหลากหลายผ่านการกำหนดมาตรฐานสำหรับการแลกเปลี่ยนข้อมูลระหว่างแพลตฟอร์มและหน่วยงานต่าง ๆ ภายใต้กรอบการดำเนินงานที่ชัดเจน นอกจากนี้ Integration Architecture ยังช่วยเพิ่มความ

ยืดหยุ่นในการปรับตัวของระบบและส่งเสริมคุณภาพโดยรวมของสถาปัตยกรรมองค์กร เช่น ความสามารถในการตรวจสอบ ความโปร่งใส และความสอดคล้องกับกลยุทธ์องค์กร ซึ่งมีผลทำให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพและตอบสนองต่อความเปลี่ยนแปลงในระยะยาวได้ดียิ่งขึ้น (Karande & Joshi, 2022b)

สถาปัตยกรรมการบูรณาการ หมายถึง โครงสร้างสำคัญที่ช่วยสนับสนุนการทำงานร่วมกันระหว่างโมดูลและระบบต่าง ๆ ของแพลตฟอร์มเว็บเพื่อการจับคู่สายอาชีพและความเข้ากันได้ของงาน ระบบนี้พัฒนาขึ้นโดยอิงกับกรอบงานสถาปัตยกรรมองค์กร (Federal Enterprise Architecture Framework - FEAF) ซึ่งช่วยให้การเชื่อมโยงระหว่างฐานข้อมูล การประมวลผลข้อมูล และฟังก์ชันต่าง ๆ ภายในระบบทำงานอย่างราบรื่น Integration Architecture ในบริบทนี้ยังช่วยสร้างมาตรฐานสำหรับการแลกเปลี่ยนข้อมูลระหว่างส่วนประกอบของระบบ เช่น การประมวลผลข้อมูลของผู้ใช้ การจับคู่สายอาชีพ และการวิเคราะห์ความเหมาะสมของผู้สมัครงาน นอกจากนี้ยังช่วยให้ระบบมีความยืดหยุ่นและสามารถปรับตัวให้เข้ากับข้อมูลและความต้องการที่เปลี่ยนแปลงได้อย่างมีประสิทธิภาพ ซึ่งเป็นส่วนสำคัญที่ทำให้ระบบสามารถตอบสนองต่อเป้าหมายของมหาวิทยาลัยในการพัฒนาบริการที่เน้นผู้ใช้เป็นศูนย์กลาง (Muslih et al., 2024d)

สถาปัตยกรรมการบูรณาการ หมายถึง การออกแบบโครงสร้างสำหรับการเชื่อมโยงและบูรณาการระบบที่เกี่ยวข้องกับอินเทอร์เน็ตสรรพสิ่ง (IoT) ในสภาพแวดล้อมใต้น้ำ โดยอาศัยกรอบแนวคิดของสถาปัตยกรรมองค์กร (Enterprise Architecture) Integration Architecture ในบริบทนี้มีบทบาทสำคัญในการประสานงานระหว่างอุปกรณ์ IoT อัจฉริยะในสภาพแวดล้อมใต้น้ำ เช่น เซ็นเซอร์ กล้อง และอุปกรณ์สื่อสาร เพื่อให้สามารถเก็บรวบรวมข้อมูล วิเคราะห์ และส่งต่อข้อมูลในเครือข่ายที่มีข้อจำกัดด้านทรัพยากร เช่น พลังงาน การส่งข้อมูลระยะไกล และสัญญาณรบกวนใต้น้ำ โครงสร้างนี้ยังช่วยให้การทำงานระหว่างระบบบนพื้นผิวและใต้น้ำเป็นไปอย่างราบรื่น เช่น การเชื่อมโยงข้อมูลระหว่างศูนย์ควบคุมบนบกและอุปกรณ์ใต้น้ำ โดยการออกแบบที่เน้นความสามารถในการทำงานร่วมกันและการปรับตัวต่อข้อจำกัดในสภาพแวดล้อมเฉพาะ Integration Architecture ยังช่วยสนับสนุนการสร้างความน่าเชื่อถือและความยั่งยืนของระบบ IoT ใต้น้ำ เพื่อตอบสนองความต้องการในด้านการวิจัยและการพัฒนาในพื้นที่ที่ซับซ้อน (Aoun et al., 2024a)

สถาปัตยกรรมการบูรณาการ หมายถึง โครงสร้างที่สนับสนุนการบูรณาการระบบต่าง ๆ ในโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructures) เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) สถาปัตยกรรมการบูรณาการมีบทบาทสำคัญในการรวมศูนย์ข้อมูล กระบวนการ และเทคโนโลยีจากหลากหลายแหล่งในระบบที่มีความซับซ้อน เช่น ระบบพลังงาน การคมนาคม หรือระบบสาธารณสุข โครงสร้างนี้มุ่งเน้นการประสานงานระหว่างองค์ประกอบที่แตกต่างกัน เพื่อให้

สามารถตรวจจับภัยคุกคาม วิเคราะห์ข้อมูลด้านความปลอดภัย และตอบสนองต่อเหตุการณ์ในเวลาจริง นอกจากนี้ยังช่วยในการออกแบบและใช้งานกรอบความปลอดภัยที่สอดคล้องกับความต้องการเฉพาะของแต่ละองค์กร โดยใช้มาตรฐานและแนวทางปฏิบัติที่ยอมรับในระดับสากล Integration Architecture จึงทำหน้าที่เป็นตัวกลางที่ช่วยให้ระบบต่าง ๆ สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ ลดช่องว่างด้านความปลอดภัย และเพิ่มความยืดหยุ่นของระบบต่อภัยคุกคามในสภาพแวดล้อมที่เปลี่ยนแปลงอย่างรวดเร็ว (Y. Jiang et al., 2024b)

สรุปได้ว่า สถาปัตยกรรมการบูรณาการ หมายถึง โครงสร้างและกรอบแนวทางในการเชื่อมโยงและประสานงานระหว่างระบบ เทคโนโลยี ข้อมูล กระบวนการ และบริการที่หลากหลาย เพื่อสร้างการทำงานร่วมกันอย่างมีประสิทธิภาพและลดความซับซ้อนในองค์กรหรือระบบที่เกี่ยวข้อง โดยมีวัตถุประสงค์หลักในการเพิ่มความสามารถในการแลกเปลี่ยนข้อมูล การตอบสนองต่อความต้องการเชิงธุรกิจและเทคโนโลยี และสร้างความยืดหยุ่นในการปรับตัวต่อการเปลี่ยนแปลง

สถาปัตยกรรมการบูรณาการ มีบทบาทสำคัญต่อการดำเนินงานขององค์กรในหลายมิติ ประการแรก คือ การสนับสนุนโครงการเทคโนโลยี โดยช่วยจัดการข้อมูลและเทคโนโลยีให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ เช่น โครงการที่เกี่ยวข้องกับปัญญาประดิษฐ์ การเรียนรู้ของเครื่อง (Machine Learning) หรือระบบอินเทอร์เน็ตของสรรพสิ่ง (IoT) ประการที่สอง คือ การบูรณาการข้อมูลและระบบในโครงสร้างพื้นฐานที่สำคัญ เช่น ระบบรักษาความปลอดภัยของพลังงาน การควบคุม หรือเครือข่ายใต้น้ำ เพื่อให้การดำเนินงานมีความต่อเนื่องและมั่นคง ประการที่สาม คือ การเพิ่มประสิทธิภาพในธุรกิจและองค์กร โดยช่วยให้องค์กรสามารถใช้ทรัพยากรและข้อมูลร่วมกันได้อย่างคุ้มค่า เช่น การออกแบบโครงสร้างที่ตอบสนองต่อความต้องการดิจิทัลและการพัฒนาแอปพลิเคชันเฉพาะด้าน และประการสุดท้าย คือ การปรับตัวเชิงกลยุทธ์ ช่วยให้องค์กรสามารถเชื่อมโยงกับระบบภายนอกและรองรับการเติบโตในระยะยาวได้อย่างยั่งยืน

2.1.3.7. สถาปัตยกรรมการกำกับดูแล (Governance Architecture)

2.1.3.7.1 ความหมาย

สถาปัตยกรรมการกำกับดูแล (Governance Architecture) หมายถึง กรอบแนวคิดที่ใช้ในการกำกับดูแลและบริหารจัดการองค์กรโดยรวม โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศ (IT) เพื่อให้แน่ใจว่าการดำเนินงานต่างๆ สอดคล้องกับกลยุทธ์และเป้าหมายขององค์กร (Srisawat et al., 2024)

สถาปัตยกรรมการกำกับดูแล หมายถึง การจัดการและควบคุมโครงการที่เกี่ยวกับ Machine Learning โดยเน้นการกำหนดกรอบการกำกับดูแลเพื่อให้มั่นใจว่าโครงการและกระบวนการพัฒนา

ระบบ Machine Learning สอดคล้องกับเป้าหมายขององค์กร รวมถึงการบริหารความเสี่ยงและการจัดการทรัพยากรอย่างเหมาะสม สถาปัตยกรรมการกำกับดูแลในบริบทนี้มีบทบาทสำคัญในการจัดการทรัพยากร, การจัดการความเสี่ยง, และการประเมินความคืบหน้าของโครงการ โดยการกำหนดกรอบการทำงานที่ชัดเจนและการควบคุมที่มีประสิทธิภาพ ซึ่งช่วยให้สามารถตรวจสอบและติดตามการพัฒนาโครงการ Machine Learning ได้ โดยไม่ละเลยข้อกำหนดด้านความปลอดภัย, ความเป็นส่วนตัวของข้อมูล, และการปฏิบัติตามกฎระเบียบทางกฎหมายที่เกี่ยวข้อง (Takeuchi et al., 2024c)

สถาปัตยกรรมการกำกับดูแล หมายถึง โครงสร้างและกรอบการกำกับดูแลที่ใช้ในการสนับสนุนการพัฒนาและการดำเนินงานขององค์กรที่มีจุดมุ่งหมายในการเสริมสร้างความยืดหยุ่นและความสามารถในการต่อสู้ของธุรกิจที่พักในพื้นที่ชนบทที่มีการลดจำนวนประชากร โดยมีการใช้สถาปัตยกรรมองค์กร (Enterprise Architecture) เพื่อให้การบริหารจัดการระบบต่างๆ ภายในองค์กรเป็นไปอย่างมีประสิทธิภาพ สถาปัตยกรรมการกำกับดูแลในงานวิจัยนี้มุ่งเน้นที่การกำหนดกรอบการกำกับดูแลที่สามารถช่วยให้ธุรกิจที่พักในพื้นที่ชนบทมีการปรับตัวที่ดีขึ้นในสภาพแวดล้อมที่ท้าทาย โดยการกำหนดบทบาทและหน้าที่ของผู้มีส่วนเกี่ยวข้อง เช่น ผู้จัดการ, พนักงาน, และเจ้าของกิจการ รวมถึงการจัดการทรัพยากรอย่างมีประสิทธิภาพ เพื่อเสริมสร้างการเติบโตและความยั่งยืนของธุรกิจ การกำกับดูแลนี้ยังมีบทบาทในการสร้างความเชื่อมโยงระหว่างธุรกิจที่พักและชุมชนท้องถิ่น, การพัฒนาความสามารถในการต้านทานต่อการเปลี่ยนแปลงทางเศรษฐกิจและสังคม และการพัฒนากลยุทธ์ที่เหมาะสม (Anes Silveira & Mamede, 2024)

สถาปัตยกรรมการกำกับดูแล หมายถึง กรอบการกำกับดูแลที่มีการออกแบบอย่างเป็นระบบเพื่อให้การดำเนินงานของสถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นไปตามมาตรฐานและวิธีการที่กำหนด โดยมุ่งเน้นการตรวจสอบและควบคุมการดำเนินงานของระบบต่างๆ ในองค์กรเพื่อให้สอดคล้องกับกลยุทธ์และวัตถุประสงค์ขององค์กร การกำกับดูแลนี้มีบทบาทในการกำหนดแนวทางที่ชัดเจนในการดำเนินการ, การตรวจสอบคุณภาพ, และการประเมินผลเพื่อให้สามารถบรรลุผลสำเร็จตามที่ตั้งเป้าหมายไว้ (Karande & Joshi, 2022b)

สถาปัตยกรรมการกำกับดูแล หมายถึง กระบวนการและโครงสร้างที่ช่วยในการควบคุมและตรวจสอบการดำเนินงานของสถาปัตยกรรมองค์กร (Enterprise Architecture) ภายในองค์กร โดยมุ่งเน้นที่การกำหนดนโยบายและแนวทางที่ชัดเจนในการบริหารจัดการทรัพยากรและกระบวนการทางเทคโนโลยีสารสนเทศ (IT) เพื่อให้สามารถบรรลุผลตามเป้าหมายทางธุรกิจได้อย่างมีประสิทธิภาพและยั่งยืน สถาปัตยกรรมการกำกับดูแลในการออกแบบกรอบสถาปัตยกรรมองค์กรในงานวิจัยนี้จะรวมถึงการกำหนดวิธีการในการควบคุมการใช้ทรัพยากรต่างๆ ภายใน IT, การจัดการการเปลี่ยนแปลง, การประเมินผลกระทบจากการดำเนินงาน, และการดูแลให้การตัดสินใจในระดับต่างๆ ภายในองค์กรเป็นไปอย่างโปร่งใสและสอดคล้องกับกลยุทธ์ทางธุรกิจ โดยการออกแบบกรอบการกำกับดูแลนี้จะ

ช่วยให้สามารถสร้างความมั่นคงในกระบวนการ IT ต่างๆ และรองรับการเปลี่ยนแปลงในอนาคตได้อย่างมีประสิทธิภาพ (Dumitriu & Popescu, 2020b)

สถาปัตยกรรมการกำกับดูแล หมายถึง กรอบการทำงานที่เน้นการควบคุมและบริหารจัดการกระบวนการต่างๆ ภายในองค์กรเพื่อให้สถาปัตยกรรมองค์กร (Enterprise Architecture) ดำเนินไปอย่างมีประสิทธิภาพและสอดคล้องกับกลยุทธ์ทางธุรกิจ ซึ่งในบริบทนี้จะมุ่งเน้นที่การออกแบบโครงสร้างการกำกับดูแลที่สามารถตรวจสอบและประเมินผลการดำเนินงานขององค์กรได้อย่างต่อเนื่อง โดยมีการกำหนดนโยบาย แนวทาง และกระบวนการในการตัดสินใจเพื่อสนับสนุนการบริหารทรัพยากรและการจัดการความเสี่ยง (Khairina et al., 2024a)

สถาปัตยกรรมการกำกับดูแล หมายถึง โครงสร้างและกระบวนการที่ใช้ในการควบคุมและจัดการการดำเนินงานของสถาปัตยกรรมองค์กร เพื่อให้มั่นใจว่าทุกกิจกรรมที่เกี่ยวข้องกับการเปลี่ยนแปลงทางดิจิทัลจะสามารถบรรลุผลสำเร็จตามเป้าหมายที่กำหนดไว้ การกำกับดูแลนี้ครอบคลุมถึงการตั้งนโยบาย, การตรวจสอบความสอดคล้องของการดำเนินงาน, และการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการนำสถาปัตยกรรมองค์กรมาปรับใช้ในกระบวนการเปลี่ยนแปลงทางดิจิทัล การกำกับดูแลในที่นี้ยังหมายถึงการสร้างกรอบการทำงานที่สามารถช่วยให้องค์กรตรวจสอบและประเมินผลของการใช้สถาปัตยกรรมองค์กรในระหว่างการเปลี่ยนแปลงดิจิทัล ซึ่งจะสนับสนุนการตัดสินใจทางธุรกิจที่ถูกต้อง, ลดความซับซ้อน, และเสริมสร้างความยืดหยุ่นในการปรับตัวต่อการเปลี่ยนแปลงในโลกดิจิทัลได้อย่างมีประสิทธิภาพ นอกจากนี้ยังมีบทบาทสำคัญในการประเมินความสำเร็จของการเปลี่ยนแปลงทางดิจิทัลผ่านกระบวนการควบคุมที่ชัดเจนและเชื่อมโยงกับเป้าหมายทางธุรกิจขององค์กร (Alghamdi, 2024)

สถาปัตยกรรมการกำกับดูแล หมายถึง โครงสร้างและกระบวนการที่ออกแบบมาเพื่อควบคุมและดูแลการดำเนินงานของสถาปัตยกรรมองค์กรในภาคการศึกษา โดยมุ่งเน้นที่การเสริมสร้างความเป็นเลิศในกระบวนการเปลี่ยนแปลงขององค์กร การกำกับดูแลนี้มีบทบาทสำคัญในการกำหนดนโยบาย, แนวทางการดำเนินงาน, และการตรวจสอบให้แน่ใจว่าการใช้สถาปัตยกรรมองค์กรสอดคล้องกับวิสัยทัศน์และพันธกิจของสถาบันการศึกษา ในกรณีศึกษานี้ สถาปัตยกรรมการกำกับดูแลช่วยสร้างกรอบการทำงานที่สนับสนุนการปรับตัวให้ทันสมัยในสภาพแวดล้อมทางการศึกษาที่เปลี่ยนแปลงอย่างรวดเร็ว การควบคุมนี้ยังเกี่ยวข้องกับการบริหารจัดการความเสี่ยง, การตรวจสอบผลลัพธ์จากการดำเนินการของสถาปัตยกรรมองค์กร, และการสร้างความมั่นใจว่าองค์กรสามารถบรรลุผลสำเร็จตามเป้าหมายการพัฒนาในระยะยาว ผ่านการออกแบบที่โปร่งใสและการมีส่วนร่วมของผู้มีส่วนได้เสียในทุกระดับ (Amin et al., 2024)

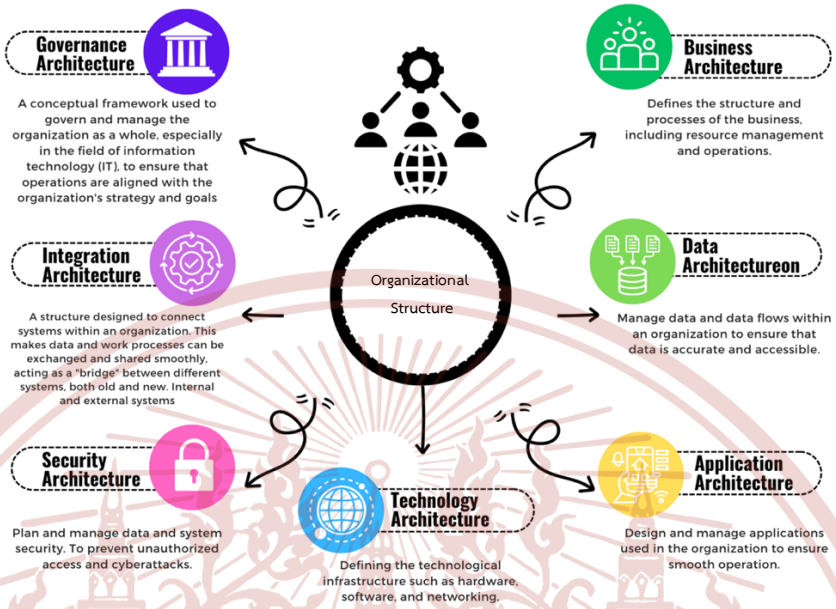
สรุปได้ว่า สถาปัตยกรรมการกำกับดูแล หมายถึง โครงสร้างที่ช่วยกำกับดูแลและควบคุมการดำเนินงานของสถาปัตยกรรมองค์รวมในระดับองค์กรหรือโครงการ โดยครอบคลุมการกำหนด

นโยบาย การจัดการทรัพยากร และการประเมินผล เพื่อให้มั่นใจว่าสถาปัตยกรรมดังกล่าวสอดคล้องกับเป้าหมายและกลยุทธ์ขององค์กร รวมถึงสามารถรองรับการเปลี่ยนแปลงในอนาคตได้อย่างยั่งยืน

ตารางที่ 2-1 การสังเคราะห์กรอบของโครงสร้างองค์กร (Organizational Structure)

ลำดับ	การโครงสร้างองค์กร	(Achaal et al., 2024)	(Dumitriu & Popescu, 2020a)	(Sultanow et al., 2021)	(Uzhakova & Fischer, 2024a)	(Al-Turkistani et al., 2021a)	(Mazher et al., 2023)	(Qurtubi, 2024)	(Muslih et al., 2024c)	(Srisawat et al., 2024)	(Denhere et al., 2023)	(Zulfikar et al., 2023)	(Rachmaniah et al., 2022)	(Gellweiler, 2020)	(Guo et al., 2020)	(Polovina et al., 2020)	ผู้วิจัย
1	Business Architecture	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	Data Architecture	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	Application Architecture	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓
4	Technology Architecture	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
5	Security Architecture	✓		✓	✓	✓		✓	✓	✓			✓				✓
6	Integration Architecture	✓			✓		✓	✓		✓			✓	✓	✓	✓	✓
7	Governance Architecture	✓	✓	✓	✓		✓			✓		✓		✓	✓		✓

จากตารางที่ 2-1 การสังเคราะห์กรอบโครงสร้างองค์กรจากงานวิจัยที่เกี่ยวข้องจำนวน 15 เรื่อง พบว่ามี 7 ด้านที่มีความสอดคล้องกันมากเกินเกณฑ์ 60% ได้แก่ 1) สถาปัตยกรรมธุรกิจ (Business Architecture) 2) สถาปัตยกรรมข้อมูล (Data Architecture) 3) สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture) 4) สถาปัตยกรรมเทคโนโลยี (Technology Architecture) 5) สถาปัตยกรรมด้านความปลอดภัย (Security Architecture) 6) สถาปัตยกรรมการบูรณาการ (Integration Architecture) และ 7) สถาปัตยกรรมการกำกับดูแล (Governance Architecture)



ภาพที่ 2-5 องค์ประกอบของโครงสร้างองค์กร (Organizational Structure)

2.1.4 ประโยชน์ของโครงสร้างองค์ แบ่งออกเป็นด้าน ๆ ได้แก่

2.1.4.1 ด้านการปรับปรุงโครงสร้างองค์กร ช่วยให้การจัดการโครงสร้างองค์กรเป็นระบบระเบียบมากขึ้น ทำให้สามารถกระจายงานและทรัพยากรได้อย่างมีประสิทธิภาพ

2.1.4.2 ด้านการเชื่อมโยงข้อมูล ช่วยแก้ปัญหาด้านการเชื่อมโยงข้อมูลภายในองค์กร ทำให้การสื่อสารและการทำงานร่วมกันระหว่างแผนกต่าง ๆ เป็นไปอย่างราบรื่น

2.1.4.3 ด้านการจัดการความเสี่ยง ช่วยระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับระบบไอที ซึ่งสามารถนำไปสู่มาตรการป้องกัน เพื่อลดความเสี่ยงและป้องกันการหยุดชะงักของระบบและการสูญเสียข้อมูล

2.1.4.4 ด้านการปรับตัวต่อการเปลี่ยนแปลง ช่วยให้องค์กรสามารถปรับตัวเข้ากับการเปลี่ยนแปลงทางธุรกิจได้อย่างรวดเร็ว โดยไม่ต้องเปลี่ยนแปลงโครงสร้างระบบไอทีทั้งหมด

2.1.4.5 ด้านการมองเห็นภาพรวมขององค์กร ช่วยให้มองเห็นภาพรวมขององค์กรทั้งระบบ ซึ่งช่วยในการตัดสินใจเกี่ยวกับการลงทุนในเทคโนโลยีสารสนเทศได้อย่างชาญฉลาด

2.1.4.6 ด้านการเพิ่มประสิทธิภาพการดำเนินงาน ช่วยระบุขั้นตอนที่ซ้ำซ้อนและกระบวนการที่ไม่มีประสิทธิภาพ ซึ่งสามารถนำไปสู่การปรับปรุงประสิทธิภาพการดำเนินงานและประหยัดค่าใช้จ่าย

สรุปได้ว่าโครงสร้างองค์ เป็นกรอบแนวคิดที่ใช้ในการออกแบบ พัฒนา และจัดการระบบและกระบวนการภายในองค์กรอย่างเป็นระบบ โดยมีการบูรณาการด้านต่าง ๆ ทั้งด้านธุรกิจ ข้อมูล เทคโนโลยี และการจัดการทรัพยากรที่สำคัญ โดยสถาปัตยกรรมองค์กรมีบทบาทในการสร้างความ

เข้าใจที่ชัดเจนเกี่ยวกับการดำเนินงานในปัจจุบันและวิสัยทัศน์ในอนาคตขององค์กร ช่วยให้ผู้บริหารสามารถวางแผนและตัดสินใจเกี่ยวกับการนำเทคโนโลยีไปใช้อย่างมีประสิทธิภาพ นอกจากนี้ สถาปัตยกรรมองค์กรยังครอบคลุมถึงการจัดการเปลี่ยนแปลง การกำกับดูแล และการกำหนดกลยุทธ์ที่สามารถปรับตัวให้สอดคล้องกับสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงอย่างรวดเร็ว เช่นเดียวกับการรับมือกับความต้องการและความท้าทายใหม่ ๆ ซึ่งช่วยให้องค์กรสามารถตอบสนองต่อโอกาสทางธุรกิจและการพัฒนานวัตกรรมได้อย่างมีประสิทธิภาพและยั่งยืน

2.2 เทคโนโลยีอัจฉริยะ (Intelligent Technology)

2.2.1 ความหมาย

เทคโนโลยีอัจฉริยะ (Intelligent Technology) หมายถึง การพัฒนาระบบคอมพิวเตอร์ที่สามารถทำงานที่ต้องการความฉลาดของมนุษย์ เช่น การเรียนรู้ การคิดวิเคราะห์ การแก้ปัญหา การรับรู้ และการเข้าใจภาษา AI ถูกออกแบบมาเพื่อเลียนแบบกระบวนการทางปัญญาของมนุษย์ โดยสามารถแบ่งออกเป็น 2 ประเภทหลัก คือ Narrow AI (Weak AI) เป็น AI ที่ถูกออกแบบมาเพื่อทำงานเฉพาะเจาะจงในขอบเขตที่จำกัด ซึ่ง Narrow AI มีความสามารถในการทำงานที่เฉพาะเจาะจง แต่ไม่สามารถทำงานที่อยู่นอกเหนือจากขอบเขตที่กำหนดได้ และ General AI (Strong AI) เป็น AI ที่มีความสามารถในการเข้าใจและเรียนรู้ในหลาย ๆ ด้าน คล้ายกับความสามารถของมนุษย์ ซึ่งยังเป็นแนวคิดที่อยู่ในระหว่างการวิจัยและพัฒนา (Pan & Zhang, 2021)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีและวิธีการที่ใช้ในการสร้างระบบที่สามารถทำงานหรือคิดได้เหมือนมนุษย์ โดยเฉพาะในบริบทของการจัดการกับซอฟต์แวร์และการแก้ไขบั๊ก (bug triaging) AI ถูกนำมาใช้เพื่อปรับปรุงและอัตโนมัติขั้นตอนการจัดการบั๊กในซอฟต์แวร์ ซึ่งช่วยให้การพัฒนาซอฟต์แวร์มีประสิทธิภาพมากขึ้น การใช้ AI ในการวิเคราะห์ข้อมูลและการตัดสินใจที่เกี่ยวข้องกับการจัดการบั๊ก โดยมีการสำรวจเทคนิคต่าง ๆ ที่เกี่ยวข้องกับ AI เช่น การเรียนรู้ของเครื่อง (machine learning) และการเรียนรู้เชิงลึก (deep learning) ที่ช่วยในการคัดกรองและจัดลำดับความสำคัญของบั๊กที่ต้องแก้ไข (Nagwani & Suri, 2023)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีที่สามารถทำงานหรือกระทำการที่ต้องการความฉลาดของมนุษย์ เช่น การเรียนรู้ การวิเคราะห์ข้อมูล และการตัดสินใจ โดย AI สามารถแบ่งออกเป็นหลายประเภท เช่น Machine Learning และ Generative AI ซึ่ง Generative AI เป็นรูปแบบหนึ่งที่สามารถสร้างเนื้อหาหรือข้อมูลใหม่จากข้อมูลที่มีอยู่ โดยใช้สถิติและความน่าจะเป็นในการสร้างผลลัพธ์ที่มีความหมาย โดยสามารถช่วยในการปรับปรุงวิธีการสอนและการเรียนรู้ เช่น การสร้างเนื้อหาการเรียนการสอนที่เหมาะสมกับผู้เรียนแต่ละคน และการให้คำแนะนำที่เป็นส่วนตัว (Baidoo-Anu & Owusu Ansah, 2023)

เทคโนโลยีอัจฉริยะ หมายถึง ความสามารถของเครื่องจักรหรือระบบคอมพิวเตอร์ในการทำงานที่ต้องใช้ความฉลาดเชิงมนุษย์ เช่น การวิเคราะห์ข้อมูล, การตัดสินใจ, และการแก้ปัญหา โดยในงานนี้ AI ถูกนำมาใช้ในรูปแบบของ Generative Pre-trained Transformers (GPT) ซึ่งเป็นรูปแบบของการเรียนรู้ของเครื่องที่สามารถให้คำแนะนำและช่วยในการจัดการกระบวนการธุรกิจได้อย่างมีประสิทธิภาพ (Beheshti et al., 2023)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีที่ใช้ระบบประมวลผลเพื่อช่วยในการตรวจจับและวิเคราะห์สัญญาณชีพ เช่น อัตราการเต้นของหัวใจและการหายใจในทารกแรกเกิด โดยไม่ต้องสัมผัสตัวผู้ป่วยโดยตรง เทคโนโลยีนี้ใช้การประมวลผลภาพจากกล้องวิดีโอที่ติดตั้งไว้ในตู้บ่มเด็ก (incubator) เพื่อวิเคราะห์สัญญาณ photoplethysmography (PPG) ซึ่งช่วยลดการใช้พลังงานและเพิ่มประสิทธิภาพในการตรวจจับอัตราการเต้นของหัวใจและการหายใจในลักษณะที่ไม่สร้างความรำคาญให้กับทารกและผู้ดูแล (Chen et al., 2023)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีที่พัฒนาขึ้นเพื่อให้เครื่องจักรสามารถจำลองหรือเลียนแบบความสามารถในการคิดและการตัดสินใจของมนุษย์ได้ AI ใช้การเรียนรู้จากข้อมูลและสร้างผลลัพธ์หรือการกระทำที่มีความชาญฉลาดและเป็นอัตโนมัติ ซึ่งสามารถแยกประเภทออกเป็นหลายประเภท เช่น การเรียนรู้ของเครื่อง (Machine Learning) และการเรียนรู้เชิงลึก (Deep Learning) เป็นต้น ในกรณีของ Generative Artificial Intelligence คือ การใช้ AI เพื่อสร้างเนื้อหาหรือข้อมูลใหม่ที่มีความเหมือนหรือคล้ายคลึงกับข้อมูลต้นฉบับ เช่น การสร้างข้อความ รูปภาพ หรือเสียง (Chiu & Chen, 2023)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีที่มีจุดมุ่งหมายเพื่อให้เครื่องจักรหรือระบบคอมพิวเตอร์สามารถดำเนินการที่ต้องใช้ความสามารถของมนุษย์ เช่น การเรียนรู้ การคิด และการตัดสินใจ AI ประกอบด้วยหลายสาขาย่อย เช่น การเรียนรู้ของเครื่อง (Machine Learning) การเรียนรู้เชิงลึก (Deep Learning) และการประมวลผลภาษาธรรมชาติ (Natural Language Processing) ซึ่ง AI สามารถใช้ในการวิเคราะห์ข้อมูลจำนวนมากและสร้างการคาดการณ์หรือการตัดสินใจที่มีความแม่นยำสูง (Kuzlu et al., 2023)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีที่พัฒนาขึ้นเพื่อให้ระบบคอมพิวเตอร์สามารถดำเนินการและคิดเหมือนมนุษย์ได้ เช่น การเรียนรู้ การวิเคราะห์ และการตัดสินใจ AI ใช้เทคนิคที่หลากหลายในการจำลองความสามารถของมนุษย์ เช่น การเรียนรู้ของเครื่อง (Machine Learning), การเรียนรู้เชิงลึก (Deep Learning), และการประมวลผลภาษาธรรมชาติ (Natural Language Processing) (Kshetri & Schordan, 2023)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีที่พัฒนาขึ้นเพื่อให้ระบบคอมพิวเตอร์สามารถดำเนินการที่ต้องใช้ความสามารถของมนุษย์ เช่น การเรียนรู้ การคิด และการตัดสินใจ AI ใช้เทคนิคที่

หลากหลายเพื่อจำลองความสามารถเหล่านี้ รวมถึงการเรียนรู้ของเครื่อง (Machine Learning), การเรียนรู้เชิงลึก (Deep Learning), และการประมวลผลภาษาธรรมชาติ (Natural Language Processing) การพัฒนาและการเรียนรู้ของมนุษย์, AI สามารถช่วยในการศึกษาและการพัฒนาทักษะใหม่ ๆ โดยการสร้างเครื่องมือหรือแพลตฟอร์มที่ช่วยในการเรียนรู้และฝึกฝนทักษะที่จำเป็นในสภาพแวดล้อมการศึกษา (Benvenuti et al., 2023)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีที่ออกแบบมาเพื่อให้ระบบคอมพิวเตอร์สามารถทำงานที่ต้องใช้ความสามารถทางสติปัญญาของมนุษย์ เช่น การเรียนรู้ การวิเคราะห์ และการตัดสินใจ AI ใช้เทคนิคต่าง ๆ เช่น การเรียนรู้ของเครื่อง (Machine Learning) และการเรียนรู้เชิงลึก (Deep Learning) เพื่อจำลองความสามารถ Anomaly Detection หรือ การตรวจจับความผิดปกติ เป็นหนึ่งในแอปพลิเคชันของ AI ที่มุ่งเน้นการระบุหรือจับความผิดปกติที่อาจเป็นสัญญาณของภัยคุกคามหรือปัญหาในระบบ เช่น การโจมตีทางไซเบอร์ หรือพฤติกรรมที่ไม่ปกติในระบบเครือข่าย (Ortiz-Garcés et al., 2024b)

เทคโนโลยีอัจฉริยะ หมายถึง เป็นเครื่องมือสำคัญในการสนับสนุนการเรียนรู้และการวิจัยสหวิทยาการ โดยเฉพาะในด้านดิจิทัลมนุษยศาสตร์ (Digital Humanities) งานวิจัยนี้มุ่งเน้นการใช้ AI ในการถอดความตัวอักษรและข้อมูลจากเอกสารทางประวัติศาสตร์ที่มีความซับซ้อน เช่น ตัวอักษรที่หายไปหรืออ่านยาก เพื่อนำมาประยุกต์ใช้ในการศึกษาวิจัยข้ามสาขาวิชา AI ในบริบทนี้ช่วยในการแก้ปัญหาเกี่ยวกับเอกสารเก่า โดยสามารถทำการถอดรหัสและประมวลผลข้อมูลได้รวดเร็วกว่าวิธีการแบบดั้งเดิม อีกทั้งยังช่วยเพิ่มความแม่นยำในการวิเคราะห์และการแปลเอกสาร ทำให้นักวิจัยสามารถเข้าถึงข้อมูลได้ง่ายขึ้นและเชื่อมโยงความรู้จากหลาย ๆ สาขาวิชาได้ดีขึ้น (Frincu & Frincu, 2025)

เทคโนโลยีอัจฉริยะ หมายถึง เทคโนโลยีที่จำลองความสามารถของมนุษย์ผ่านเครื่องจักร ซึ่งสามารถทำงานที่ต้องใช้การคิดวิเคราะห์ การตัดสินใจ การเรียนรู้ และการปรับตัวได้ โดยสามารถนำไปประยุกต์ในงานด้านต่างๆ เช่น การแพทย์ AI ช่วยในด้านการวินิจฉัยที่แม่นยำมากขึ้น การพัฒนายา และการรักษาผู้ป่วยแบบเฉพาะบุคคล การเงิน AI ช่วยตรวจจับการทุจริต การประเมินความเสี่ยง และการซื้อขายอัตโนมัติในตลาดหุ้น การผลิต AI ช่วยเพิ่มประสิทธิภาพในกระบวนการผลิต การบำรุงรักษาเครื่องจักรเชิงพยากรณ์ และการบริหารจัดการห่วงโซ่อุปทาน ค้าปลีก AI ช่วยในการคาดการณ์ความต้องการสินค้า การจัดการสต็อก และการมอบประสบการณ์ที่เป็นส่วนตัวให้กับลูกค้า การขนส่ง AI สนับสนุนระบบยานยนต์อัตโนมัติและการจัดการโลจิสติกส์ และการศึกษา AI นำมาใช้ในแพลตฟอร์มการเรียนรู้ที่ปรับตามความต้องการของผู้เรียน (Rashid & Kausik, 2024)

เทคโนโลยีอัจฉริยะ หมายถึง การนำอัลกอริทึมการคำนวณขั้นสูงมาใช้เพื่อให้เครื่องจักรสามารถเลียนแบบความฉลาดของมนุษย์ รวมถึงความสามารถในการเรียนรู้ การให้เหตุผล และการ

แก้ปัญหา AI มีบทบาทสำคัญในการส่งเสริมการจัดการการศึกษาด้วยการนำเสนอระบบอัจฉริยะที่สนับสนุนการเรียนรู้แบบเฉพาะบุคคล การตัดสินใจบนพื้นฐานข้อมูล และการจัดการทรัพยากรอย่างมีประสิทธิภาพ (L. Han et al., 2024)

เทคโนโลยีอัจฉริยะ หมายถึง ระบบที่ช่วยให้กระบวนการตัดสินใจและการทำงานของเทคโนโลยีใต้น้ำ (Internet of Underwater Things: IoUT) มีความชาญฉลาดขึ้น โดย AI มีบทบาทในการปรับปรุงความสามารถในการประมวลผลข้อมูลและการตอบสนองต่อสิ่งแวดล้อมใต้น้ำซึ่งมีข้อจำกัดด้านสิ่งแวดล้อมหลายประการ เช่น ความดันสูง การสื่อสารยาก และความหลากหลายของอุณหภูมิ AI ทำหน้าที่ช่วยให้ระบบสามารถเรียนรู้และปรับตัวได้อย่างอัตโนมัติ ทำให้การดำเนินงานมีความต่อเนื่องและมีประสิทธิภาพมากขึ้นโดยไม่ต้องพึ่งพามนุษย์ (Aoun et al., 2024b)

เทคโนโลยีอัจฉริยะ หมายถึง เครื่องมือที่ช่วยเสริมสร้างกระบวนการเรียนรู้และการเปลี่ยนแปลงองค์กร โดย AI จะมีบทบาทสำคัญในการวิเคราะห์ข้อมูลและให้ข้อมูลเชิงลึกที่ช่วยในการตัดสินใจในโครงการเปลี่ยนแปลงองค์กรที่ซับซ้อน นอกจากนี้ AI ยังสามารถสร้างความเข้าใจที่หลากหลายในการปรับเปลี่ยนโครงสร้างองค์กรให้เข้ากับการเปลี่ยนแปลงทางเทคโนโลยีและตลาด ซึ่งส่งผลให้เกิดการสร้างนวัตกรรมและความยืดหยุ่นในองค์กร (A. T. Trad, 2024)

2.2.2 องค์ประกอบของเทคโนโลยีอัจฉริยะ ประกอบไปด้วยหลายส่วนสำคัญที่ทำให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพดังนี้

2.2.2.1 การเรียนรู้ของเครื่อง (Machine Learning) คือ สาขาหนึ่งของปัญญาประดิษฐ์ที่มุ่งเน้นการพัฒนาอัลกอริทึมและโมเดลที่สามารถเรียนรู้จากข้อมูลและปรับปรุงความสามารถในการทำนายหรือการตัดสินใจโดยอัตโนมัติ โดยไม่จำเป็นต้องตั้งโปรแกรมที่ชัดเจนจากมนุษย์ ระบบจะสามารถจดจำรูปแบบและสร้างข้อสรุปจากข้อมูลที่ได้รับ การเรียนรู้ของเครื่องสามารถแบ่งออกเป็น 3 หมวดหลัก ได้แก่ การเรียนรู้ที่มีการควบคุม (Supervised Learning) ซึ่งใช้ข้อมูลที่มีป้ายกำกับเพื่อฝึกฝนโมเดลให้สามารถทำนายหรือจำแนกข้อมูลใหม่ได้อย่างถูกต้อง, การเรียนรู้ที่ไม่มีการควบคุม (Unsupervised Learning) ซึ่งใช้ข้อมูลที่ไม่มีป้ายกำกับในการหาความสัมพันธ์หรือรูปแบบที่ซ่อนอยู่ในข้อมูล และการเรียนรู้เชิงลึก (Deep Learning) ซึ่งใช้โครงข่ายประสาทเทียมหลายชั้นในการเรียนรู้คุณสมบัติที่ซับซ้อนจากข้อมูลปริมาณมาก การเรียนรู้ของเครื่องมีการประยุกต์ใช้อย่างกว้างขวางในหลายแอปพลิเคชัน

2.2.2.2 การเรียนรู้เชิงลึก (Deep Learning) คือ สาขาย่อยของการเรียนรู้ของเครื่องที่ใช้โครงข่ายประสาทเทียมหลายชั้นในการจำลองกระบวนการคิดและการเรียนรู้ของสมองมนุษย์ ซึ่งสามารถประมวลผลข้อมูลที่มีความซับซ้อนและมีมิติสูง เช่น ภาพ เสียง และข้อความ การเรียนรู้เชิงลึกมักใช้ในงานที่ต้องการการจดจำหรือการแยกแยะรูปแบบที่ซับซ้อน เช่น การจดจำใบหน้าจากภาพถ่าย, การแปลภาษาด้วยระบบอัตโนมัติ, หรือการจำแนกประเภทของเสียง โดยโครงข่ายประสาท

เทียมในรูปแบบของเครือข่ายหลายชั้น (เช่น Convolutional Neural Networks หรือ CNNs และ Recurrent Neural Networks หรือ RNNs) ทำให้สามารถเรียนรู้คุณสมบัติจากข้อมูลดิบได้อย่างมีประสิทธิภาพและแม่นยำมากขึ้น การเรียนรู้เชิงลึกจึงมีการประยุกต์ใช้อย่างแพร่หลายในการพัฒนาเทคโนโลยีขั้นสูง เช่น การขับขี่รถยนต์อัตโนมัติ, การแพทย์, และการวิเคราะห์ข้อมูลขนาดใหญ่

2.2.2.3 การประมวลผลภาษาธรรมชาติ (Natural Language Processing - NLP) คือ เทคโนโลยีที่ช่วยให้ปัญญาประดิษฐ์สามารถเข้าใจและประมวลผลภาษาที่มนุษย์ใช้ในการสื่อสารกันในชีวิตประจำวัน โดยใช้เทคนิคและอัลกอริทึมต่างๆ ในการแยกแยะและวิเคราะห์ข้อความที่เป็นภาษาธรรมชาติ เช่น การแปลภาษา การวิเคราะห์ความหมายของข้อความ การจำแนกประเภทข้อความ หรือการสร้างข้อความอัตโนมัติ เทคโนโลยีนี้มีความสำคัญในการพัฒนาแอปพลิเคชันต่างๆ เช่น ผู้ช่วยส่วนตัว (Virtual Assistants), การค้นหาข้อมูล, และการวิเคราะห์ความคิดเห็นในสื่อสังคมออนไลน์ เป็นต้น

2.2.2.4 ระบบหุ่นยนต์ (Robotics) คือ การประยุกต์ใช้ปัญญาประดิษฐ์ในหุ่นยนต์เพื่อให้สามารถทำงานอัตโนมัติหรือโต้ตอบกับสภาพแวดล้อมได้อย่างมีประสิทธิภาพ โดยใช้เซ็นเซอร์, ระบบควบคุม, และอัลกอริทึมในการประมวลผลข้อมูลเพื่อให้หุ่นยนต์สามารถตัดสินใจและปฏิบัติงานได้อย่างเหมาะสม ระบบหุ่นยนต์ถูกนำมาใช้ในหลากหลายสาขา เช่น อุตสาหกรรมการผลิต, การแพทย์, การให้บริการ, และการสำรวจ ซึ่งช่วยเพิ่มประสิทธิภาพและลดความเสี่ยงจากการทำงานในสภาพแวดล้อมที่ยากลำบากหรืออันตราย

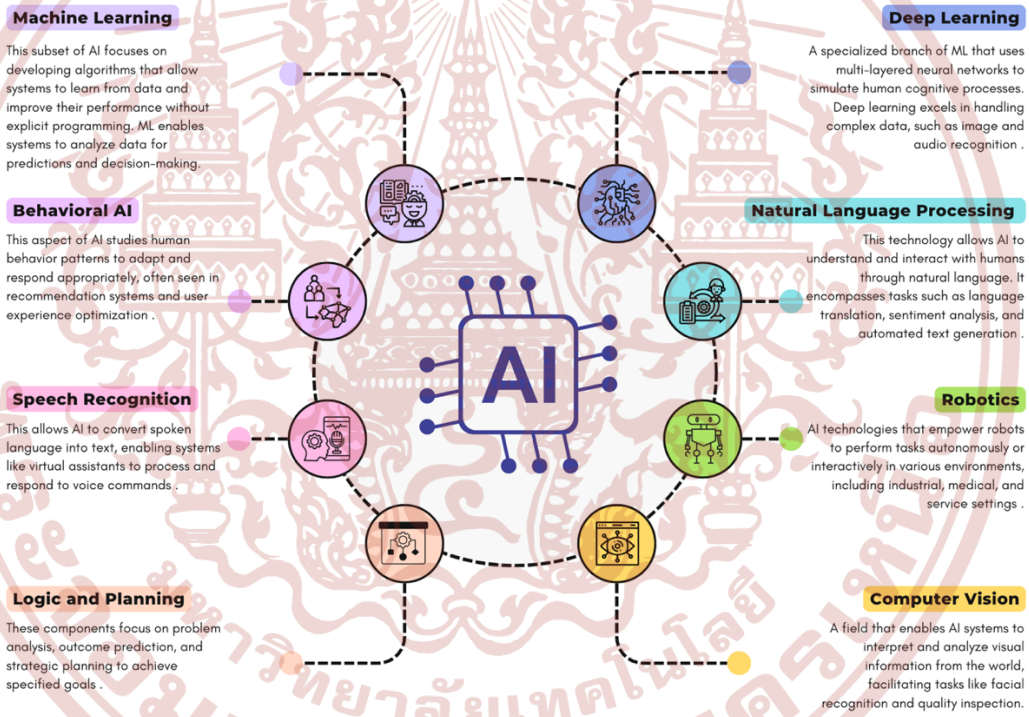
2.2.2.5 การมองเห็นด้วยคอมพิวเตอร์ (Computer Vision) คือ การใช้เทคโนโลยีและอัลกอริธึมในปัญญาประดิษฐ์เพื่อให้คอมพิวเตอร์หรือหุ่นยนต์สามารถรับรู้และตีความภาพหรือวิดีโอได้เหมือนกับมนุษย์ โดยการประมวลผลข้อมูลภาพเพื่อให้สามารถทำการวิเคราะห์หรือตัดสินใจเกี่ยวกับสิ่งที่เห็น เช่น การจดจำใบหน้า, การตรวจสอบคุณภาพสินค้าในสายการผลิต, หรือการวิเคราะห์ภาพทางการแพทย์เพื่อช่วยในการวินิจฉัยโรค ระบบนี้ใช้ในหลากหลายอุตสาหกรรมเพื่อปรับปรุงประสิทธิภาพการทำงานและการให้บริการ

2.2.2.6 การคิดเชิงตรรกะและการวางแผน (Logic and Planning) คือ กระบวนการที่ทำให้ปัญญาประดิษฐ์ (AI) สามารถใช้การคิดเชิงตรรกะในการวิเคราะห์ปัญหาและตัดสินใจ โดย AI จะพิจารณาผลลัพธ์ที่เป็นไปได้จากสถานการณ์ต่าง ๆ และวางแผนขั้นตอนในการดำเนินการเพื่อให้บรรลุเป้าหมายที่ตั้งไว้ ระบบนี้มีบทบาทสำคัญในการแก้ไขปัญหาที่ยากซับซ้อน เช่น การวางแผนเส้นทางในการเดินทางของหุ่นยนต์ การตัดสินใจทางธุรกิจ หรือการสร้างกลยุทธ์ในการเล่นเกม เป็นต้น

2.2.2.7 การรู้จำเสียง (Speech Recognition) คือ เทคโนโลยีที่ช่วยให้ปัญญาประดิษฐ์ (AI) สามารถแปลงเสียงพูดของมนุษย์ให้เป็นข้อความที่สามารถเข้าใจและประมวลผล

ได้ โดยใช้เทคนิคการวิเคราะห์และแยกแยะลักษณะเสียง เช่น การแปลงคำพูดของผู้ใช้ให้เป็นคำสั่ง หรือการตอบคำถามผ่านผู้ช่วยเสมือน เช่น Siri หรือ Google Assistant ซึ่งช่วยให้การสื่อสารระหว่างมนุษย์กับเครื่องจักรมีความสะดวกและเป็นธรรมชาติมากขึ้น

2.2.2.8 ความรู้เชิงพฤติกรรม (Behavioral AI) คือ การใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ในการวิเคราะห์และทำความเข้าใจพฤติกรรมของมนุษย์ เพื่อให้ AI สามารถปรับตัวและตอบสนองต่อการเปลี่ยนแปลงที่เกิดขึ้นในพฤติกรรมของผู้ใช้ เช่น ระบบแนะนำสินค้าในอีคอมเมิร์ซที่สามารถเสนอสินค้าที่ตรงกับความสนใจหรือพฤติกรรมการซื้อของลูกค้า หรือระบบติดตามพฤติกรรมผู้ใช้ที่ช่วยให้บริการตอบสนองตามการกระทำหรือความชอบส่วนบุคคล



ภาพที่ 2-6 องค์ประกอบของเทคโนโลยีอัจฉริยะ (Intelligent Technology)

ตารางที่ 2-2 การสังเคราะห์เทคโนโลยีอัจฉริยะ (Intelligent Technology)

ลำดับ	เทคโนโลยีอัจฉริยะ	(Rizal et al., 2025)	(Zhang et al., 2025)	(Khalbouch et al., 2025)	(Ashani et al., 2025)	(Halgamuge & Nyato, 2025)	(Thangam & Jana, 2025)	(Bhatt et al., 2025)	(Musa, A.I.A.et al., 2025)	(Hemachandran et al., 2022)	(Ramasamy et al., 2022)	(Martel et al., 2020)	(Nyauo, 2020)	(La Gatta et al., 2024)	(Nazher et al., 2023)	(Fritsani et al., 2023a)	ผู้แต่ง
1	Machine Learning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	Deep Learning	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓
3	Natural Language Processing (NLP)	✓	✓	✓		✓				✓	✓	✓	✓	✓	✓	✓	✓
4	Robotics					✓						✓					
5	Computer Vision	✓			✓												

ลำดับ	เทคโนโลยีอัจฉริยะ	(Rizal et al., 2025)	(Zhang et al., 2025)	(Kharbouch et al., 2025)	(Ashani et al., 2025)	(Hatgamuge & Niyato, 2025)	(Thangam & Jana, 2025)	(Bhatt et al., 2025)	(Musa, A.I.A et al., 2025)	(Hemachandran et al., 2022)	(Ramasamy et al., 2022)	(Martel et al., 2020)	(Miyauo, 2020)	(La Gatta et al., 2024)	(Mazher et al., 2023)	(Fitriani et al., 2023a)	ผู้แต่ง
6	Logic and Planning	✓	✓	✓		✓			✓								
7	Speech Recognition									✓							
8	Behavioral AI	✓	✓	✓	✓	✓	✓	✓	✓				✓				✓

จากตารางที่ 2-2 การสังเคราะห์องค์ประกอบของเทคโนโลยีอัจฉริยะจากงานวิจัยที่เกี่ยวข้อง จำนวน 15 เรื่อง พบว่ามีเทคโนโลยี 4 ด้านที่มีความสอดคล้องกันมากเกินเกณฑ์ 60% ได้แก่ 1) การเรียนรู้ของเครื่อง (Machine Learning) 2) การเรียนรู้เชิงลึก (Deep Learning) 3) การประมวลผลภาษาธรรมชาติ (Natural Language Processing - NLP) และ 4) ความรู้เชิงพฤติกรรม (Behavioral AI)

2.2.3 ประโยชน์ของเทคโนโลยีอัจฉริยะ

เทคโนโลยีอัจฉริยะ มีบทบาทสำคัญในการเพิ่มประสิทธิภาพและประสิทธิผลขององค์กรในหลายด้าน ดังนี้

2.2.3.1 การเพิ่มประสิทธิภาพการทำงาน เทคโนโลยีอัจฉริยะช่วยลดความซ้ำซ้อนและความผิดพลาดในการทำงาน เช่น ระบบอัตโนมัติในสายการผลิตหรือการประมวลผลข้อมูล ทำให้องค์กรสามารถดำเนินงานได้รวดเร็วและแม่นยำมากขึ้น

2.2.3.2 การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) เทคโนโลยีอัจฉริยะสามารถประมวลผลและวิเคราะห์ข้อมูลขนาดใหญ่ได้อย่างรวดเร็วและละเอียด ส่งผลให้การตัดสินใจเชิงกลยุทธ์มีความแม่นยำและสามารถคาดการณ์แนวโน้มในอนาคตได้อย่างมีประสิทธิผล

2.2.3.3 การพัฒนานวัตกรรม เทคโนโลยีอัจฉริยะช่วยสร้างนวัตกรรมใหม่ ๆ เช่น การพัฒนาแอปพลิเคชันเพื่อการตรวจจับโรคผ่านภาพทางการแพทย์ หรือเทคโนโลยีการสื่อสารอัจฉริยะ

2.2.3.4 การปรับปรุงประสบการณ์ผู้ใช้ เทคโนโลยีอัจฉริยะสามารถพัฒนา Chatbot และผู้ช่วยดิจิทัล (Digital Assistant) ที่ตอบสนองต่อความต้องการของผู้ใช้ได้อย่างรวดเร็วและเป็นธรรมชาติ

2.2.3.5 การใช้ในด้านความปลอดภัย เทคโนโลยีอัจฉริยะสามารถตรวจสอบและตอบสนองต่อความผิดปกติหรือภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ส่งผลให้การป้องกันภัยคุกคามทางดิจิทัลมีความทันสมัยและรวดเร็วมากขึ้น

2.2.3.6 การเรียนรู้และการศึกษา เทคโนโลยีอัจฉริยะสามารถช่วยสร้างเนื้อหาและวางแผนการเรียนรู้ที่เหมาะสมกับผู้เรียนแต่ละคน ทำให้การเรียนการสอนมีความเฉพาะตัวและมีประสิทธิภาพมากขึ้น

2.2.3.7 การแพทย์และสุขภาพ เทคโนโลยีอัจฉริยะถูกนำมาใช้ในการวินิจฉัยโรค การวางแผนการรักษา และการติดตามสุขภาพของผู้ป่วยอย่างแม่นยำ เช่น การใช้ปัญญาประดิษฐ์ในการวิเคราะห์ภาพถ่ายจากเครื่องมือทางการแพทย์

สรุปได้ว่าเทคโนโลยีอัจฉริยะ คือเทคโนโลยีที่พัฒนาให้ระบบคอมพิวเตอร์หรือเครื่องจักรสามารถทำงานที่ต้องใช้ความสามารถทางสติปัญญาของมนุษย์ เช่น การเรียนรู้ การคิดวิเคราะห์ และการตัดสินใจ ปัญญาประดิษฐ์ถูกแบ่งออกเป็นหลายประเภท เช่น การเรียนรู้ของเครื่อง (Machine Learning) และการเรียนรู้เชิงลึก (Deep Learning) โดยมีบทบาทสำคัญในการเพิ่มประสิทธิภาพในการทำงาน ช่วยในการวิเคราะห์ข้อมูลจำนวนมาก และทำให้กระบวนการต่าง ๆ เป็นอัตโนมัติ การนำปัญญาประดิษฐ์มาใช้ในองค์กรช่วยให้การจัดการและดำเนินงานในหลายด้านเป็นไปอย่างมีประสิทธิภาพ ลดข้อผิดพลาด และปรับปรุงการตัดสินใจ

2.3 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture)

2.3.1 ความหมาย

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) หมายถึง โครงสร้างและแนวทางการออกแบบที่ใช้เพื่อจัดการและรวมเทคโนโลยีปัญญาประดิษฐ์ เข้ากับการดำเนินงานและกลยุทธ์ขององค์กรอย่างเป็นระบบและมีประสิทธิภาพ โดยเน้นที่การใช้ AI เพื่อสนับสนุนการตัดสินใจ, การปรับปรุงกระบวนการธุรกิจ, และการสร้างคุณค่าให้กับองค์กร (Rittelmeyer & Sandkuhl, 2021)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง กรอบการทำงานเชิงกลยุทธ์ที่ออกแบบมาเพื่อผสานรวมเทคโนโลยีปัญญาประดิษฐ์เข้ากับส่วนประกอบโครงสร้างและการดำเนินงานขององค์กรกริดไฟฟ้า โดยใช้หลักการของสถาปัตยกรรมองค์กร (Enterprise Architecture - EA) เพื่อจัดระเบียบการประยุกต์ใช้และความสามารถของ AI ภายในองค์กรให้สอดคล้องและเพิ่มประสิทธิภาพในการปฏิบัติงาน (X. Han et al., 2021)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง การนำปัญญาประดิษฐ์ เป็นแรงขับเคลื่อนการเปลี่ยนแปลงที่สำคัญภายในสถาปัตยกรรมองค์กร โดยการศึกษาชี้ให้เห็นถึงความสามารถของ AI ในการสนับสนุนการตัดสินใจอย่างชาญฉลาดด้วยการให้ข้อมูลเชิงลึกผ่านการวิเคราะห์ข้อมูล ซึ่งช่วยปรับปรุงกระบวนการวางแผนกลยุทธ์ นอกจากนี้ AI ยังมีบทบาทในการส่งเสริมนวัตกรรมและการพัฒนาบริการใหม่ ๆ ที่ตอบสนองความต้องการของตลาดได้อย่างมีประสิทธิภาพ การปรับปรุง

ประสิทธิภาพการดำเนินงานโดยการทำให้งานอัตโนมัติและการวิเคราะห์ข้อมูลยังส่งผลให้ค่าใช้จ่ายลดลงและเพิ่มผลผลิตได้อีกด้วย การบูรณาการ AI ที่ประสบความสำเร็จในสถาปัตยกรรมองค์กรต้องมีการวางแผนอย่างรอบคอบ โดยเน้นความสำคัญของวัฒนธรรมองค์กรและการพัฒนาทักษะของพนักงาน สุดท้ายงานวิจัยนี้ยังเน้นถึงศักยภาพของ AI ในการกำหนดกลยุทธ์ในอนาคต เพื่อให้มั่นใจในความยั่งยืนและความสามารถในการปรับตัวต่อสภาวะตลาดที่เปลี่ยนแปลงไป (Denni-Fiberesima, 2024)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง เป็นกรอบการทำงานที่มุ่งเน้นการบูรณาการปัญญาประดิษฐ์ เข้ากับโครงสร้างและกระบวนการขององค์กร เพื่อสร้างสภาพแวดล้อมที่เอื้อต่อการใช้งาน AI อย่างมีประสิทธิภาพและยั่งยืน โดยสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ไม่เพียงแค่เกี่ยวข้องกับเทคโนโลยีและเครื่องมือ แต่ยังรวมถึงการวางแผนเชิงกลยุทธ์ การจัดการข้อมูล และการกำกับดูแลระบบที่สนับสนุนการพัฒนา AI ในองค์กร การบูรณาการ AI เข้ากับสถาปัตยกรรมองค์กรทำให้สามารถใช้ AI ในการตัดสินใจและการวิเคราะห์ข้อมูลได้อย่างมีประสิทธิภาพ โดยที่สถาปัตยกรรมองค์กรต้องมีความยืดหยุ่นเพื่อรองรับการเปลี่ยนแปลงที่รวดเร็วในเทคโนโลยีและความต้องการของตลาด นอกจากนี้ ยังมีการเน้นถึงความสำคัญของความยั่งยืนในการออกแบบสถาปัตยกรรมองค์กร ซึ่งต้องคำนึงถึงผลกระทบต่อสิ่งแวดล้อมและสังคม โดยรวมแล้ว AI Enterprise Architecture จึงมีบทบาทสำคัญในการสร้างสรรค์นวัตกรรมและเพิ่มประสิทธิภาพในการทำงานขององค์กรในยุคดิจิทัล (Kamalabai et al., 2024)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง โครงสร้างที่สนับสนุนการใช้ปัญญาประดิษฐ์ภายในองค์กร โดยมีเป้าหมายในการส่งเสริมการเปลี่ยนแปลงทางดิจิทัลและการปรับใช้สถาปัตยกรรมองค์กร สถาปัตยกรรมองค์กรปัญญาประดิษฐ์มีองค์ประกอบสำคัญที่ช่วยให้การจัดการข้อมูลและกระบวนการทำงานสามารถใช้ AI ในการวิเคราะห์และการตัดสินใจได้อย่างมีประสิทธิภาพ โดยจะมุ่งเน้นไปที่การสร้างกรอบการทำงานที่ยืดหยุ่นและสามารถปรับตัวได้ตามความต้องการขององค์กร การบูรณาการ AI กับสถาปัตยกรรมองค์กรไม่เพียงแต่ช่วยเพิ่มประสิทธิภาพในการดำเนินงาน แต่ยังสามารถสนับสนุนการพัฒนานวัตกรรมและการปรับตัวเข้ากับสภาพแวดล้อมที่เปลี่ยนแปลงอย่างรวดเร็ว (Tshuma et al., 2024)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง โครงสร้างและรูปแบบการจัดการที่เน้นการใช้ปัญญาประดิษฐ์เพื่อสนับสนุนการเปลี่ยนแปลงทางดิจิทัลในองค์กร โดยมีจุดมุ่งหมายเพื่อเพิ่มประสิทธิภาพในการดำเนินงานและการตัดสินใจภายในอุตสาหกรรมพลังงานไฟฟ้า เป็นเครื่องมือที่สำคัญในการวิเคราะห์ข้อมูลและการพัฒนาอัลกอริธึมที่ช่วยให้การจัดการระบบพลังงานมีความยืดหยุ่นและปรับตัวได้ตามความต้องการ โดยเฉพาะในการเพิ่มความสามารถในการคาดการณ์และ

การจัดการทรัพยากรอย่างมีประสิทธิภาพ นอกจากนี้ AI ยังช่วยในการเพิ่มความสามารถในการวิเคราะห์ข้อมูลจากแหล่งต่างๆ เพื่อสนับสนุนการตัดสินใจที่มีข้อมูลเป็นพื้นฐาน (X. Li & Zhang, 2024)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง กรอบการทำงานที่ใช้ TOGAF เพื่อสร้างและพัฒนาโครงสร้างขององค์กรที่สามารถบูรณาการปัญญาประดิษฐ์ได้อย่างมีประสิทธิภาพ โดยมุ่งเน้นที่การปรับปรุงการดำเนินงาน การตัดสินใจ และการจัดการทรัพยากรในองค์กร ผ่านการใช้เทคโนโลยี AI ในด้านต่าง ๆ เช่น การวิเคราะห์ข้อมูล การปรับปรุงกระบวนการธุรกิจ และการเสริมสร้างนวัตกรรมทางธุรกิจ (Fitriani et al., 2023a)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง กรอบการทำงานที่จัดการรวมเอาความสามารถของปัญญาประดิษฐ์เข้ากับสถาปัตยกรรมโดยรวมขององค์กร กรอบนี้เน้นความสำคัญของการออกแบบระบบที่ให้ความสำคัญกับความต้องการและประสบการณ์ของมนุษย์ ในขณะที่ใช้เทคโนโลยี AI เพื่อเพิ่มประสิทธิภาพในการตัดสินใจ การทำงาน และนวัตกรรม สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ประกอบด้วยหลายส่วน เช่น การจัดการข้อมูล การทำงานอัตโนมัติของกระบวนการ และการออกแบบการมีปฏิสัมพันธ์กับผู้ใช้ ซึ่งทั้งหมดมีเป้าหมายเพื่อสร้างระบบอัจฉริยะที่ตอบสนองต่อความต้องการของผู้ใช้ กรอบนี้ช่วยให้สามารถจัดตำแหน่งเป้าหมายทางธุรกิจกับโครงการ AI ได้อย่างมีประสิทธิภาพ ทำให้การใช้งานโซลูชัน AI สนับสนุนเป้าหมายเชิงกลยุทธ์ขององค์กร (Zimmermann et al., 2023)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง กรอบแนวคิดที่รวมเทคโนโลยีปัญญาประดิษฐ์เข้ากับสถาปัตยกรรมขององค์กรโดยรวม เน้นการสร้างดิจิทัลทวิน (digital twin) การแทนค่าของวัตถุจริงในรูปแบบเสมือน ซึ่งช่วยให้องค์กรสามารถจำลอง วิเคราะห์ และปรับปรุงการดำเนินงานได้แบบเรียลไทม์ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ถูกออกแบบมาเพื่ออำนวยความสะดวกในการทำงานร่วมกันระหว่างดิจิทัลทวินและกระบวนการต่างๆ ขององค์กร ซึ่งส่งผลให้การตัดสินใจและประสิทธิภาพในการดำเนินงานดีขึ้น รวมถึงการบูรณาการข้อมูล อัลกอริธึมการเรียนรู้ของเครื่อง และการวิเคราะห์แบบเรียลไทม์ เพื่อให้มั่นใจว่าดิจิทัลทวินสามารถแสดงและคาดการณ์พฤติกรรมของระบบจริงได้อย่างถูกต้อง การรวมกันนี้สนับสนุนการมองเห็นที่ครอบคลุมเกี่ยวกับองค์กร ซึ่งช่วยในการจัดการทรัพยากรอย่างมีประสิทธิภาพและการวางแผนเชิงกลยุทธ์ (Crespi et al., 2023)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง การบูรณาการเทคโนโลยีปัญญาประดิษฐ์ในองค์กร โดยเฉพาะในบริบทของการผลิตที่มุ่งเน้นมนุษย์และการสร้างคุณค่าใหม่ องค์ประกอบสำคัญของ AI Enterprise Architecture รวมถึงการบูรณาการข้อมูล การใช้ AI ในกระบวนการทำงาน และ

การสร้างระบบอัจฉริยะ เพื่อเพิ่มประสิทธิภาพและลดข้อผิดพลาดในการดำเนินงาน กรอบนี้ช่วยให้องค์กรสามารถตอบสนองต่อความต้องการที่เปลี่ยนแปลงไปอย่างรวดเร็วในสังคมและตลาดยุคใหม่ ซึ่งมีความสำคัญต่อความยั่งยืนและการเติบโตในยุคการแข่งขันที่สูงขึ้น (Bhatia et al., 2023)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง การบูรณาการการเรียนรู้ของเครื่อง (Machine Learning) ในการเปลี่ยนแปลงธุรกิจและการพัฒนาโครงการ โดยมุ่งเน้นการสร้างสภาพแวดล้อมที่เหมาะสมสำหรับการดำเนินงานของ AI เพื่อเพิ่มประสิทธิภาพและการปรับตัวขององค์กร สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ช่วยให้ธุรกิจสามารถรวบรวมข้อมูล วิเคราะห์ และทำการตัดสินใจอย่างชาญฉลาด ซึ่งมีความสำคัญต่อการพัฒนาโครงการที่สามารถตอบสนองความต้องการและแนวโน้มของตลาดที่เปลี่ยนแปลงอย่างรวดเร็ว โดยการนำเสนอข้อมูลเชิงลึกและการคาดการณ์ที่ถูกต้องในการตัดสินใจทางธุรกิจ (A. Trad, 2022)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง การทำงานที่มุ่งเน้นการใช้เทคโนโลยีปัญญาประดิษฐ์เพื่อปรับปรุงการบริการของรัฐบาลอย่างมีประสิทธิภาพ โดยมีจุดประสงค์หลักในการสร้างความสามารถในการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) เพื่อสนับสนุนการตัดสินใจและการดำเนินงานในองค์กรภาครัฐ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์จึงเป็นการบูรณาการระหว่างสถาปัตยกรรมองค์กรทั่วไปกับการใช้ AI เพื่อพัฒนาบริการสาธารณะ ให้มีความทันสมัยและตอบสนองต่อความต้องการของประชาชนได้ดียิ่งขึ้น (Mukherjee, 2022)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง การบูรณาการเทคโนโลยีปัญญาประดิษฐ์เพื่อเพิ่มประสิทธิภาพในการให้บริการสาธารณะและการดำเนินงานของเมือง การสร้างสถาปัตยกรรมที่มีความยืดหยุ่นและสามารถปรับตัวได้ตามความต้องการของประชาชน โดยใช้ข้อมูลจากเซนเซอร์และการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) เพื่อทำความเข้าใจพฤติกรรมและความต้องการของประชาชน นอกจากนี้ยังช่วยในการปรับปรุงการสื่อสารระหว่างหน่วยงานรัฐและประชาชน เพื่อให้บริการที่รวดเร็วและตอบสนองต่อความต้องการในระดับที่สูงขึ้น (Prasetyo & Habibie, 2022)

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ หมายถึง การทำงานที่บูรณาการเทคโนโลยีปัญญาประดิษฐ์ การวิเคราะห์ข้อมูล และข้อมูลขนาดใหญ่ เพื่อสร้างความเชื่อมโยงระหว่างกลยุทธ์ทางธุรกิจ สังคม และโครงสร้างองค์กร (A. Trad, 2021)

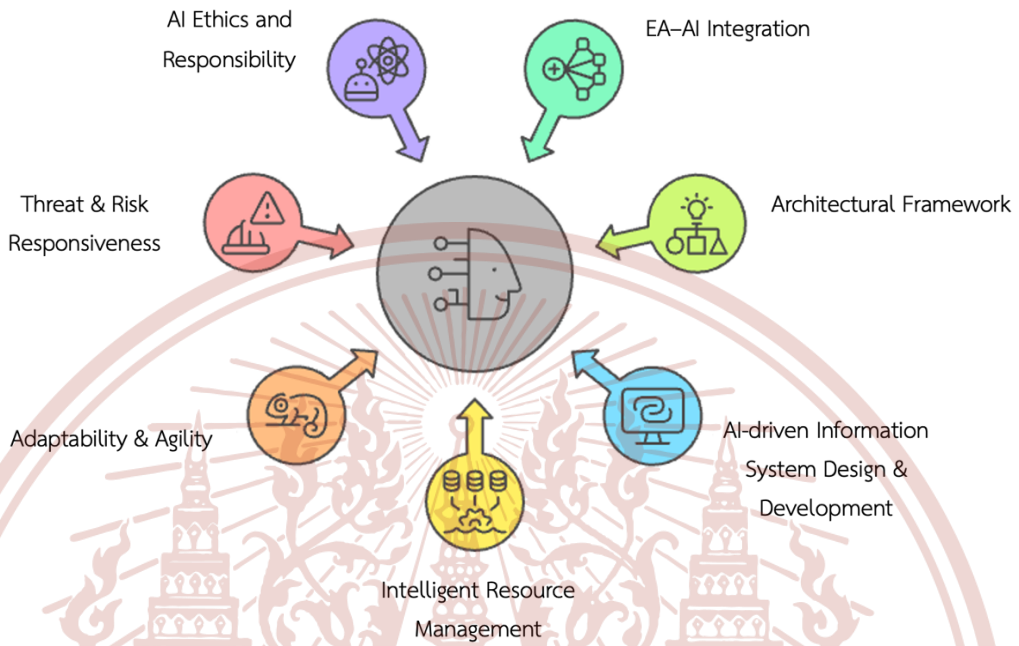
2.3.2 องค์ประกอบของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

จากการวิเคราะห์วรรณกรรมและงานวิจัยที่เกี่ยวข้องในปัจจุบัน พบว่ายังคงมีช่องว่างทางวิชาการที่สำคัญเกี่ยวกับการกำหนดนิยามหรือคำจำกัดความมาตรฐานที่เป็นสากล (Universal Definition) ของแนวคิด สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ไว้อย่างชัดเจน แต่การนิยามมักอยู่ในลักษณะของการประยุกต์หรือบูรณาการร่วมกับแนวคิดพื้นฐานด้าน สถาปัตยกรรมองค์กร

(Enterprise Architecture) และ สถาปัตยกรรมข้อมูล (Data Architecture) มากกว่าการกำหนดเป็นกรอบแนวคิดที่มีนิยามเฉพาะ

ทั้งนี้การที่ยังไม่มีนิยามที่เป็นมาตรฐานเดียวกันอาจเกิดจากลักษณะการพัฒนาอย่างรวดเร็วของเทคโนโลยีปัญญาประดิษฐ์ ซึ่งมีความเป็นสหวิทยาการ (Interdisciplinary) และเกี่ยวข้องกับหลายมิติ ทั้งด้านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ การบริหารจัดการวงจรชีวิตของแบบจำลองการเรียนรู้ของเครื่อง (Machine Learning Operations: MLOps) ตลอดจนประเด็นด้านธรรมาภิบาลข้อมูลและจริยธรรมของปัญญาประดิษฐ์ ส่งผลให้งานวิจัยจำนวนมากมักมุ่งเน้นการอธิบายแนวคิดผ่าน คุณลักษณะเชิงสมรรถนะ (Functional Capabilities) หรือ กรอบการบริหารจัดการความเสี่ยง (Risk Management Frameworks) มากกว่าการกำหนดนิยามเชิงทฤษฎีที่มีความชัดเจนและเป็นมาตรฐาน

สรุปได้ว่า สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ คือการบูรณาการสถาปัตยกรรมองค์กร (Enterprise Architecture) กับปัญญาประดิษฐ์ (Artificial Intelligence) เพื่อให้เกิดกรอบการทำงานที่สามารถออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ รวมถึงการจัดการทรัพยากรต่าง ๆ ภายในองค์กรในลักษณะที่สามารถตอบสนองต่อการเปลี่ยนแปลงและภัยคุกคามต่างๆ ได้อย่างรวดเร็วและแม่นยำ โดยประกอบด้วย 7 ด้าน ได้แก่ 1. การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ (EA–AI Integration) 2.กรอบการทำงานเชิงสถาปัตยกรรม (Architectural Framework) 3.การออกแบบและพัฒนาระบบสารสนเทศด้วย AI (AI-driven Information System Design & Development) 4.การจัดการทรัพยากรอย่างชาญฉลาด (Intelligent Resource Management) 5.การปรับตัวต่อการเปลี่ยนแปลง (Adaptability & Agility) 6.การรับมือภัยคุกคามและความเสี่ยง (Threat & Risk Responsiveness) และ7. จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ (AI Ethics and Responsibility)



ภาพที่ 2-7 องค์ประกอบของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture)

2.4 ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity System)

2.4.1 ความหมาย

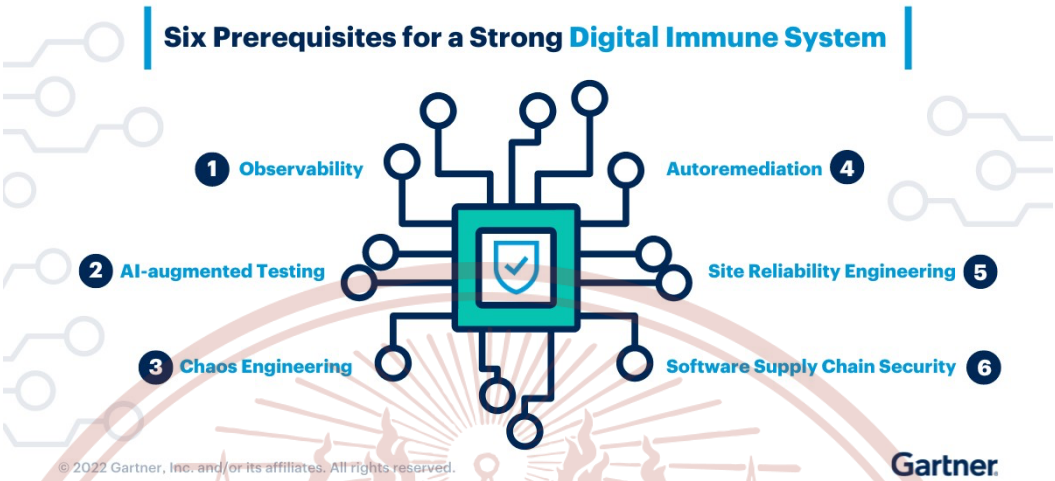
ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity System) หมายถึง กลไกเชิงระบบที่ทำหน้าที่ในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยเฉพาะในบริบทของเมืองอัจฉริยะ (Smart City) ซึ่งระบบดังกล่าวถูกเปรียบเทียบกับภูมิคุ้มกันของร่างกายมนุษย์ที่สามารถตรวจจับ ป้องกัน และกำจัดภัยคุกคามได้อย่างทันท่วงทีก่อนที่จะก่อให้เกิดความเสียหายร้ายแรง ทั้งนี้ Digital Immunity มีบทบาทสำคัญในการป้องกันความเสี่ยงที่เกิดจากการโจมตีทางไซเบอร์ (Cyberattacks) และมัลแวร์ (Cyber Malware) ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล โครงสร้างพื้นฐาน และการให้บริการดิจิทัลในระดับองค์กรและสังคมโดยรวม (Termanini, 2020)

ระบบภูมิคุ้มกันดิจิทัล หมายถึง ความสามารถขององค์กรในการป้องกัน ตรวจจับ วิเคราะห์ ฟื้นฟู และตอบสนองต่อเหตุการณ์ที่อาจก่อให้เกิดความเสียหายหรือการหยุดชะงักทางดิจิทัลได้อย่างมีประสิทธิภาพ โดยเปรียบเสมือนระบบภูมิคุ้มกันของร่างกายมนุษย์ที่สามารถรับมือกับภัยคุกคามได้อย่างทันท่วงที องค์ประกอบสำคัญของ Digital Immunity ประกอบด้วย (1) Visibility การมองเห็นและเข้าใจภาพรวมของระบบดิจิทัลและเทคโนโลยี (2) Detection การตรวจจับภัยคุกคามหรือ

เหตุการณ์ผิดปกติอย่างรวดเร็ว (3) Investigation การสืบสวนและวิเคราะห์หาสาเหตุของปัญหา (4) Response การตอบสนองต่อภัยคุกคามอย่างมีประสิทธิภาพ และ (5) Collaboration การประสานงานและทำงานร่วมกันระหว่างหน่วยงานหรือทีมที่เกี่ยวข้องเพื่อแก้ไขและฟื้นฟูสถานการณ์ได้อย่างเหมาะสม (Splunk, 2023)

ระบบภูมิคุ้มกันดิจิทัล หมายถึง แนวทางหรือกลไกเชิงรุกที่ออกแบบมาเพื่อเสริมสร้างความปลอดภัย ความทนทาน และความสามารถในการฟื้นฟูของระบบดิจิทัลต่อภัยคุกคามทั้งทางไซเบอร์และทางกายภาพ โดยมีเป้าหมายเพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ ลดความเสี่ยง และฟื้นฟูสภาพกลับคืนได้อย่างรวดเร็วเมื่อเกิดเหตุไม่คาดคิด องค์ประกอบสำคัญของ Digital Immunity ได้แก่ ความน่าเชื่อถือ (Reliability), ความทนทาน (Robustness), และ ความยืดหยุ่นพร้อมการฟื้นฟู (Resilience) ซึ่งทั้งหมดทำให้ระบบดิจิทัลสามารถป้องกัน ตรวจจับ และตอบสนองต่อการโจมตีได้อย่างมีประสิทธิผล อีกทั้งยังอาศัยเทคนิคเสริม เช่น การเรียนรู้เชิงป้องกัน (adversarial pre-training) เพื่อสร้างภูมิคุ้มกันเชิงดิจิทัลที่เปรียบเสมือน “วัคซีน” สำหรับระบบและองค์กรในยุค Industry 4.0 และ 5.0 ที่มีการเชื่อมต่อและความอัจฉริยะเพิ่มมากขึ้นอย่างต่อเนื่อง (Terziyan & Kaikova, 2025)

ระบบภูมิคุ้มกันดิจิทัล หมายถึง ระบบเฝ้าระวังและป้องกันด้านดิจิทัลที่อาศัยเทคโนโลยีอัจฉริยะ เช่น ปัญญาประดิษฐ์ (AI), การตรวจจับภัยคุกคาม, การเข้ารหัสข้อมูล และมาตรการความปลอดภัยเชิงรุก เพื่อเสริมสร้างความมั่นคง ความทนทาน และความสามารถในการฟื้นฟูของระบบดิจิทัลต่อการโจมตีหรือความผิดพลาด องค์ประกอบสำคัญของ Digital Immunity ได้แก่ การมอนิเตอร์และเฝ้าระวัง (Observability), การตรวจจับภัยคุกคาม (Threat Detection), การฟื้นฟูระบบ (Resilience and Recovery), การป้องกันเชิงรุก (Proactive Defense) และ การสร้างความรู้และความตระหนักด้านความปลอดภัย (Cybersecurity Awareness) ทั้งนี้ Digital Immunity จึงเป็นแนวคิดเชิงรุกที่มุ่งสร้างความปลอดภัย ความต่อเนื่อง และความเชื่อมั่นในการดำเนินงานขององค์กร โดยเฉพาะในบริบทของสถาบันการศึกษา ซึ่งต้องปกป้องข้อมูลสำคัญ ระบบการเรียนการสอน และเครือข่ายดิจิทัลให้มีความมั่นคงและยั่งยืน (Pikulhom, 2025)



ภาพที่ 2-9 Six Prerequisites for a Strong Digital Immune System

https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter

จากภาพที่ 2-9 องค์ประกอบหลัก 6 ประการที่สำคัญสำหรับระบบภูมิคุ้มกันดิจิทัล (Digital Immune System) โดย Gartner ระบุไว้ว่าระบบภูมิคุ้มกันดิจิทัล นั้นเปรียบเสมือนระบบป้องกันที่ช่วยปกป้องระบบคอมพิวเตอร์และเครือข่ายจากภัยคุกคามทางไซเบอร์ต่างๆ เช่น ไวรัส แรนซัมแวร์ และการโจมตีทางไซเบอร์อื่นๆ

องค์ประกอบหลักทั้ง 6 ประการ ได้แก่

1. Observability หมายถึงความสามารถในการมองเห็นและติดตามระบบได้อย่างครอบคลุม รวมถึงการตรวจสอบและวิเคราะห์ข้อมูลต่างๆ ที่เกี่ยวข้องกับระบบ เพื่อให้รู้ว่าระบบกำลังทำงานเป็นปกติหรือไม่ มีอะไรผิดปกติเกิดขึ้น และหาสาเหตุของปัญหาและภัยคุกคามได้อย่างรวดเร็ว

2. AI-augmented Testing หมายถึงการใช้ปัญญาประดิษฐ์ (AI) มาช่วยในการทดสอบระบบ เพื่อค้นหาข้อบกพร่องและช่องโหว่ที่อาจเกิดขึ้นได้

3. Chaos Engineering หมายถึงการสร้างสถานการณ์จำลองที่อาจเกิดขึ้นในระบบ เพื่อทดสอบความแข็งแกร่งและความสามารถในการฟื้นตัวของระบบ ว่าสามารถรับมือกับสถานการณ์ที่ไม่คาดคิดได้หรือไม่

4. Autoremediation หมายถึงการใช้ระบบอัตโนมัติในการแก้ไขปัญหาที่เกิดขึ้นในระบบโดยไม่ต้องอาศัยการแทรกแซงของมนุษย์ ทำให้สามารถแก้ไขปัญหาได้อย่างรวดเร็ว

5. Site Reliability Engineering หมายถึงวิธีการทำงานที่เน้นความน่าเชื่อถือของระบบโดยให้ความสำคัญกับการออกแบบระบบ การทดสอบ และการติดตาม เพื่อให้ระบบมีความเสถียรและสามารถให้บริการได้อย่างต่อเนื่อง

6. Software Supply Chain Security หมายถึงการรักษาความปลอดภัยของซอฟต์แวร์ที่ใช้ในระบบ ตั้งแต่ขั้นตอนการพัฒนาจนถึงการใช้งาน เพื่อป้องกันไม่ให้มีช่องโหว่ที่ผู้โจมตีสามารถใช้ประโยชน์ได้

องค์ประกอบสำคัญของระบบภูมิคุ้มกันดิจิทัล ประกอบด้วย

1. การมองเห็นและเฝ้าระวัง (Observability & Visibility) การติดตามและวิเคราะห์พฤติกรรมของระบบและผู้ใช้งานเพื่อคาดการณ์และป้องกันภัยคุกคาม ถือเป็นรากฐานสำคัญของการสร้างภูมิคุ้มกันดิจิทัล เพราะเป็นกลไกที่ช่วยให้องค์กรสามารถติดตาม ตรวจสอบ และเก็บข้อมูลจากระบบ แอปพลิเคชัน และเครือข่ายได้อย่างต่อเนื่อง ความสามารถนี้ทำให้องค์กรสามารถตรวจพบพฤติกรรมที่ผิดปกติ คาดการณ์ความเสี่ยงล่วงหน้า และกำหนดมาตรการรับมือที่เหมาะสมได้ทันเวลา เครื่องมือที่นิยมใช้ เช่น ระบบ Security Information and Event Management (SIEM) ระบบ Dashboard Monitoring รวมถึงเครื่องมือที่ใช้ปัญญาประดิษฐ์ (AI-based Monitoring) ซึ่งช่วยเพิ่มประสิทธิภาพในการมองเห็นภัยคุกคามเชิงรุกได้ดียิ่งขึ้น

2. การตรวจจับภัยคุกคาม (Threat Detection) เป็นองค์ประกอบที่ช่วยให้องค์กรสามารถรับมือกับการโจมตีในเชิงป้องกันและตอบสนองอย่างรวดเร็ว โดยใช้เทคโนโลยีสมัยใหม่ เช่น ปัญญาประดิษฐ์ (AI) การเรียนรู้ของเครื่อง (Machine Learning) และระบบตรวจจับการบุกรุก (IDS/IPS) เพื่อระบุและแจ้งเตือนภัยคุกคามที่เกิดขึ้นแบบเรียลไทม์ ซึ่งรวมถึงการตรวจจับมัลแวร์ การโจมตีแบบฟิชชิ่ง หรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต การมีระบบตรวจจับที่มีประสิทธิภาพทำให้องค์กรสามารถลดโอกาสความเสียหายและเพิ่มความมั่นคงปลอดภัยทางดิจิทัลได้อย่างมีนัยสำคัญ

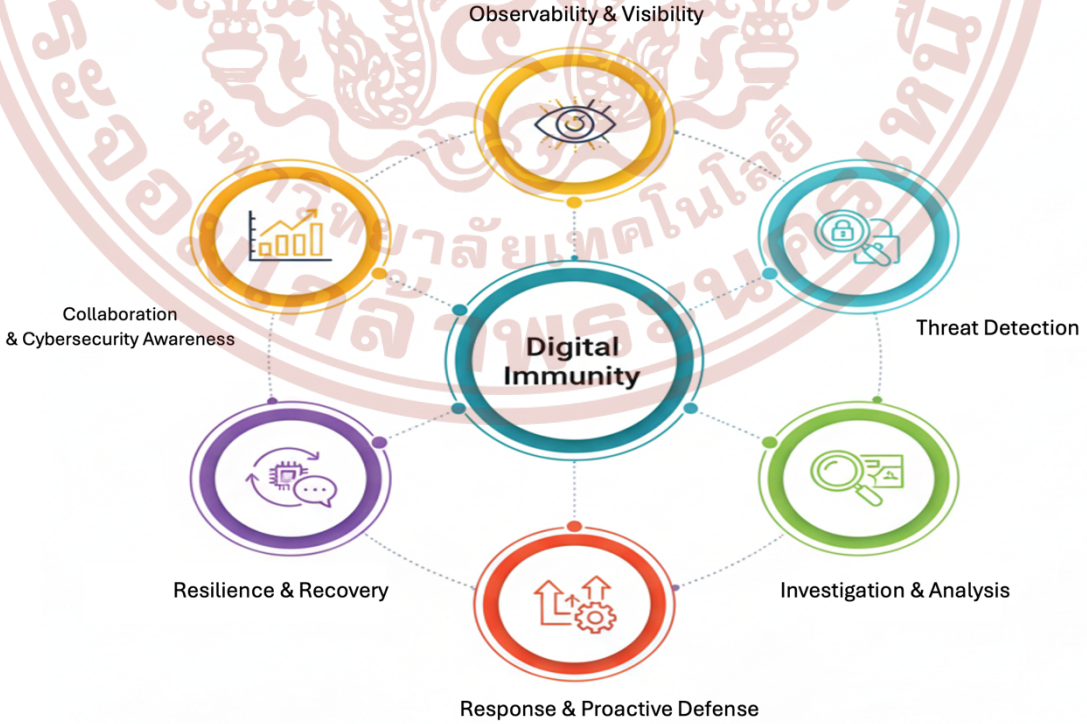
3. การสืบสวนและวิเคราะห์ (Investigation & Analysis) การระบุสาเหตุและผลกระทบเพื่อวางแผนรับมือได้อย่างเหมาะสม เมื่อเกิดเหตุการณ์ด้านความปลอดภัยขึ้น องค์กรจำเป็นต้องมีความสามารถในการสืบสวนและวิเคราะห์เพื่อทำความเข้าใจถึงสาเหตุและผลกระทบที่เกิดขึ้น องค์ประกอบนี้ช่วยให้องค์กรสามารถระบุช่องโหว่ที่ถูกโจมตี วิเคราะห์รูปแบบการโจมตี และใช้ข้อมูลดังกล่าวเพื่อปรับปรุงระบบในอนาคต กระบวนการนี้มักเกี่ยวข้องกับเทคนิคด้าน Threat Intelligence การวิเคราะห์นิติวิทยาศาสตร์ดิจิทัล (Digital Forensics) และการหาสาเหตุราก (Root Cause Analysis) ซึ่งมีบทบาทสำคัญในการสร้างภูมิคุ้มกันเชิงรุกและลดความเสี่ยงจากการโจมตีซ้ำ

4. การตอบสนองและการป้องกันเชิงรุก (Response & Proactive Defense) เป็นกลไกสำคัญที่ช่วยให้องค์กรสามารถจัดการกับภัยคุกคามได้อย่างทันท่วงที โดยรวมถึงการกักกันระบบที่ถูกโจมตี (Isolation) การปิดกั้นการเข้าถึง (Blocking) และการอัปเดตแพตช์ด้านความปลอดภัย (Patch Management) นอกจากนี้ยังรวมถึงมาตรการป้องกันล่วงหน้า เช่น Firewall การเข้ารหัสข้อมูล (Encryption) การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) และสถาปัตยกรรม

แบบ Zero Trust ที่เน้นไม่เชื่อถือการเข้าถึงใด ๆ โดยอัตโนมัติ การมีระบบตอบสนองและป้องกันเชิงรุกช่วยลดผลกระทบจากภัยคุกคามและสร้างความมั่นใจในความปลอดภัยของระบบ

5. ความทนทานและการฟื้นฟู (Resilience & Recovery) เป็นองค์ประกอบที่ช่วยให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่องแม้เผชิญกับการโจมตีหรือความผิดพลาดที่ไม่คาดคิด ระบบที่มีความทนทานสูงสามารถรักษาการทำงานหลักไว้ได้ และเมื่อเกิดการหยุดชะงักสามารถฟื้นฟูการทำงานกลับสู่สภาวะปกติได้อย่างรวดเร็ว แนวทางที่นิยมใช้ เช่น การสำรองข้อมูลและการกู้คืนระบบ (Backup & Disaster Recovery) การสร้างความซ้ำซ้อน (Redundancy Systems) และการใช้โครงสร้างพื้นฐานแบบ Cloud-based Recovery ที่ช่วยลดระยะเวลาในการฟื้นตัวและลดผลกระทบต่อการดำเนินงาน

6. ความร่วมมือและการสร้างความตระหนักรู้ (Collaboration & Cybersecurity Awareness) การสร้างจิตสำนึกด้านความปลอดภัยไซเบอร์และความร่วมมือของบุคลากรในองค์กรเพื่อป้องกันและลดความเสี่ยง นอกจากเทคโนโลยีแล้ว ปัจจัยด้านคนยังมีความสำคัญไม่แพ้กัน ความร่วมมือระหว่างทีมด้านความปลอดภัยไซเบอร์ทั้งภายในและภายนอกองค์กรช่วยเสริมความแข็งแกร่งในการรับมือภัยคุกคาม อีกทั้งการสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ให้กับผู้ใช้งานทุกระดับ โดยเฉพาะในสถาบันอุดมศึกษา ซึ่งมีผู้ใช้งานที่หลากหลาย ตั้งแต่ผู้บริหาร คณาจารย์ บุคลากร ไปจนถึงนักศึกษา ถือเป็นหัวใจสำคัญ การอบรมและสร้างวัฒนธรรมด้านความปลอดภัยดิจิทัลจะช่วยลดความเสี่ยงจากพฤติกรรมที่อาจนำไปสู่การโจมตีและสร้างภูมิคุ้มกันดิจิทัลในเชิงสังคมได้อย่างยั่งยืน



ภาพที่ 2-8 องค์ประกอบของระบบภูมิคุ้มกันดิจิทัล (Digital Immunity System)

สรุปได้ว่า ระบบภูมิคุ้มกันดิจิทัล หมายถึงระบบและกลไกเชิงรุกที่ใช้เทคโนโลยีอัจฉริยะและมาตรการด้านความปลอดภัย เพื่อเสริมสร้างความปลอดภัย ความทนทาน และความสามารถในการฟื้นฟูของระบบดิจิทัล ให้สามารถตรวจจับ ป้องกัน ตอบสนอง และฟื้นตัวจากภัยคุกคามได้อย่างมีประสิทธิภาพ โดยมีเป้าหมายเพื่อรักษาความต่อเนื่อง ความมั่นคง และความยั่งยืนในการดำเนินงานขององค์กร

2.5 การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)

2.5.1 ความหมาย

การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) หมายถึง กระบวนการและระบบที่ใช้ในการป้องกัน ควบคุม และตอบสนองต่อภัยคุกคามทางไซเบอร์หรือช่องโหว่ที่อาจเกิดขึ้นในระบบดิจิทัล โดยใช้เทคโนโลยีและแนวคิดที่คล้ายกับระบบภูมิคุ้มกันในร่างกายมนุษย์เพื่อสร้างความมั่นคงปลอดภัยทางดิจิทัล โดยการใช้เทคนิคการเรียนรู้แบบปรปักษ์ (Adversarial Learning) เพื่อเพิ่มความปลอดภัยและความสามารถในการต้านทานภัยคุกคามทางไซเบอร์ของระบบดิจิทัล โดยแนวคิดนี้ได้รับแรงบันดาลใจจากระบบภูมิคุ้มกันทางชีวภาพ ซึ่งระบบจะพัฒนาตัวเองให้มีประสิทธิภาพมากขึ้นในการป้องกันภัยคุกคามหลังจากที่ได้เจอกับภัยนั้น ๆ แล้ว (Branytskyi et al., 2022)

การจัดการภูมิคุ้มกันดิจิทัล หมายถึง การสร้างโครงสร้างสถาปัตยกรรมความปลอดภัยที่ปรับตัวได้ ระบบจะเรียนรู้จากการโจมตีจำลองเพื่อเพิ่มขีดความสามารถในการปกป้องตนเองจากภัยคุกคามที่เกิดขึ้นจริง จุดมุ่งหมายคือเพื่อเพิ่มความแข็งแกร่งและความปลอดภัยของระบบดิจิทัล กรอบแนวคิดหรือวิธีการที่ใช้ Generative Adversarial Networks (GANs) เพื่อเสริมสร้างความแข็งแกร่งและความยืดหยุ่นทางไซเบอร์ของระบบในยุคอุตสาหกรรม 4.0 แนวคิดนี้เกี่ยวข้องกับการใช้เทคนิคปัญญาประดิษฐ์แบบปรปักษ์ (adversarial machine learning) โดยเฉพาะ GANs เพื่อจำลองการโจมตีทางไซเบอร์และตรวจหาช่องโหว่ภายในระบบอุตสาหกรรม ช่วยให้ระบบสามารถพัฒนากลไกการป้องกันที่ดีขึ้น (Terziyan et al., 2021)

การจัดการภูมิคุ้มกันดิจิทัล หมายถึง กระบวนการและแนวทางในการสร้างความปลอดภัยและการป้องกันให้กับแพลตฟอร์มดิจิทัล การจัดการภูมิคุ้มกันดิจิทัลมุ่งเน้นที่การปกป้องผู้ใช้จากการปฏิบัติที่ไม่เป็นธรรมและการละเมิดความโปร่งใสในแพลตฟอร์มออนไลน์ การจัดการภูมิคุ้มกันดิจิทัลไม่เพียงแต่เกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคลของผู้ใช้ แต่ยังรวมถึงการตรวจสอบความเป็นธรรมในเงื่อนไขการให้บริการและการทำให้กระบวนการที่เกี่ยวข้องมีความโปร่งใสมากขึ้น ทั้งนี้เพื่อสร้างความมั่นใจให้กับผู้ใช้และเพิ่มความเชื่อมั่นในระบบดิจิทัล การจัดการภูมิคุ้มกันดิจิทัลจึงเป็น

เครื่องมือที่สำคัญในการรักษาสมดุลระหว่างการพัฒนาเทคโนโลยีดิจิทัลและการปกป้องสิทธิของผู้บริโภค โดยเฉพาะในยุคที่การทำธุรกรรมออนไลน์เป็นสิ่งที่แพร่หลายและสำคัญต่อเศรษฐกิจดิจิทัล (Prasetyo & Habibie, 2022)

การจัดการภูมิคุ้มกันดิจิทัล หมายถึง การสร้างระบบที่สามารถตรวจจับการโจมตีไซเบอร์ที่ไม่รู้จัก โดยอิงจากแนวคิดการสร้างภูมิคุ้มกันเทียม (artificial immunity) เพื่อป้องกันและตอบสนองต่อภัยคุกคามไซเบอร์ ระบบนี้มีการพัฒนาอัลกอริทึมที่ช่วยให้สามารถระบุและจำแนกประเภทของการโจมตีที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ โดยมีจุดมุ่งหมายเพื่อลดความเสี่ยงและปกป้องข้อมูลที่สำคัญจากการถูกโจมตีหรือเข้าถึงโดยไม่ได้รับอนุญาต ระบบการจัดการภูมิคุ้มกันนี้ไม่เพียงแต่ตรวจจับและตอบสนองต่อภัยคุกคาม แต่ยังสามารถเรียนรู้จากเหตุการณ์ที่ผ่านมาเพื่อนำไปสู่การพัฒนากลยุทธ์ที่ดียิ่งขึ้นในการป้องกันการโจมตีในอนาคต ซึ่งเป็นการนำแนวคิดของปัญญาประดิษฐ์ (AI) มาใช้ในการสร้างความปลอดภัยในระบบดิจิทัลที่มีความซับซ้อนมากขึ้น (Huang et al., 2023b)

การจัดการภูมิคุ้มกันดิจิทัล หมายถึง แนวทางการสร้างระบบป้องกันที่มีความสามารถในการตอบสนองและปรับตัวต่อภัยคุกคามไซเบอร์ที่เกิดขึ้นในยุคดิจิทัล โดยมุ่งเน้นที่การพัฒนาภูมิคุ้มกันให้แข็งแกร่งในระดับระบบ เพื่อปกป้องข้อมูลและโครงสร้างพื้นฐานดิจิทัลจากการถูกโจมตีหรือเข้าถึงโดยไม่ถูกต้อง การจัดการภูมิคุ้มกันดิจิทัลนี้จะใช้เทคโนโลยีต่างๆ เช่น ปัญญาประดิษฐ์ (AI) และอัลกอริทึมการเรียนรู้ของเครื่อง (Machine Learning) เพื่อช่วยในการวิเคราะห์และตรวจจับพฤติกรรมที่อาจเป็นภัยคุกคาม โดยมีการสร้างแบบจำลองที่สามารถคาดการณ์การโจมตีที่อาจเกิดขึ้นในอนาคต ซึ่งเป็นการทำให้ระบบสามารถรักษาความปลอดภัยและความสมบูรณ์ของข้อมูลได้อย่างมีประสิทธิภาพและรวดเร็วในโลกที่มีการเปลี่ยนแปลงตลอดเวลา (George et al., 2023c)

การจัดการภูมิคุ้มกันดิจิทัล หมายถึง กลยุทธ์และกระบวนการที่มุ่งหวังจะสร้างความสามารถในการตอบสนองต่อภัยคุกคามและการโจมตีในระบบเทคโนโลยี โดยเฉพาะอย่างยิ่งในสภาพแวดล้อมที่มีความซับซ้อนและหลากหลาย การจัดการภูมิคุ้มกันดิจิทัลนี้เน้นการใช้เทคโนโลยีที่ช่วยเพิ่มความสามารถในการป้องกันและฟื้นตัวจากภัยคุกคามต่างๆ โดยการสร้างแบบจำลองภูมิคุ้มกันดิจิทัลที่มีประสิทธิภาพ ซึ่งสามารถปรับตัวได้ตามการเปลี่ยนแปลงในภัยคุกคามและสภาพแวดล้อมต่างๆ ได้ (Krauze & Grabis, 2024b)

2.4.2 องค์ประกอบสำคัญของการจัดการภูมิคุ้มกันดิจิทัล

องค์ประกอบของการจัดการภูมิคุ้มกันดิจิทัล ประกอบไปด้วยหลายด้านที่สำคัญเพื่อสร้างความมั่นคงและป้องกันภัยคุกคามในระบบดิจิทัล องค์ประกอบเหล่านี้สามารถสรุปได้ดังนี้

2.4.2.1 การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection) คือระบบที่สามารถระบุและตรวจจับภัยคุกคามที่เกิดขึ้นในเวลาจริง เช่น การโจมตีจากไวรัสหรือมัลแวร์ โดยใช้เทคนิคการวิเคราะห์ข้อมูลและ AI เพื่อปรับปรุงประสิทธิภาพในการตรวจจับภัยคุกคาม

2.4.2.2 การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response) คือแนวทางและแผนการที่ช่วยให้องค์กรสามารถตอบสนองต่อเหตุการณ์ทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ เช่น การกู้คืนระบบหลังจากเกิดการโจมตี

2.4.2.3 การประเมินและจัดการความเสี่ยง (Risk Assessment and Management) คือการระบุความเสี่ยงที่อาจเกิดขึ้นต่อองค์กรและพัฒนากลยุทธ์เพื่อจัดการและลดความเสี่ยงเหล่านั้น

2.4.2.4 การจัดการช่องโหว่ (Vulnerability Management) คือการค้นหาและจัดการช่องโหว่ในระบบ เช่น การอัปเดตซอฟต์แวร์ที่มีอยู่ เพื่อป้องกันไม่ให้ถูกโจมตี

2.4.2.5 การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy) คือการใช้มาตรการเพื่อป้องกันข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต และรักษาความเป็นส่วนตัวของข้อมูล

2.4.2.6 การฝึกอบรมการรับรู้ด้านความปลอดภัย (Security Awareness Training) คือการให้ความรู้และการฝึกอบรมแก่พนักงานเกี่ยวกับการรักษาความปลอดภัยและการป้องกันภัยคุกคามทางไซเบอร์

2.4.2.7 นโยบายความปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance) คือการจัดตั้งนโยบายที่ชัดเจนเกี่ยวกับความปลอดภัยและการตรวจสอบให้มั่นใจว่าองค์กรปฏิบัติตามกฎระเบียบที่เกี่ยวข้อง

2.4.2.8 การป้องกันอุปกรณ์ปลายทาง (Endpoint Security) คือการใช้เทคโนโลยีและซอฟต์แวร์เพื่อปกป้องอุปกรณ์ที่เชื่อมต่อกับเครือข่าย เช่น คอมพิวเตอร์และโทรศัพท์มือถือ

2.4.2.9 การสำรองข้อมูลและการฟื้นฟูระบบ (Backup and Recovery) คือการสร้างระบบสำรองข้อมูลเพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีที่เกิดการโจมตีหรือสูญหายของข้อมูล

2.4.2.10 ความปลอดภัยของเครือข่าย (Network Security) คือการใช้เทคโนโลยีเพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต เช่น การใช้ไฟร์วอลล์ และ VPN

2.4.2.11 โซลูชันความปลอดภัยที่ขับเคลื่อนด้วย AI (AI-driven Security Solutions) คือการใช้ AI ในการวิเคราะห์ข้อมูลและค้นหาภัยคุกคามทางไซเบอร์ เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัย

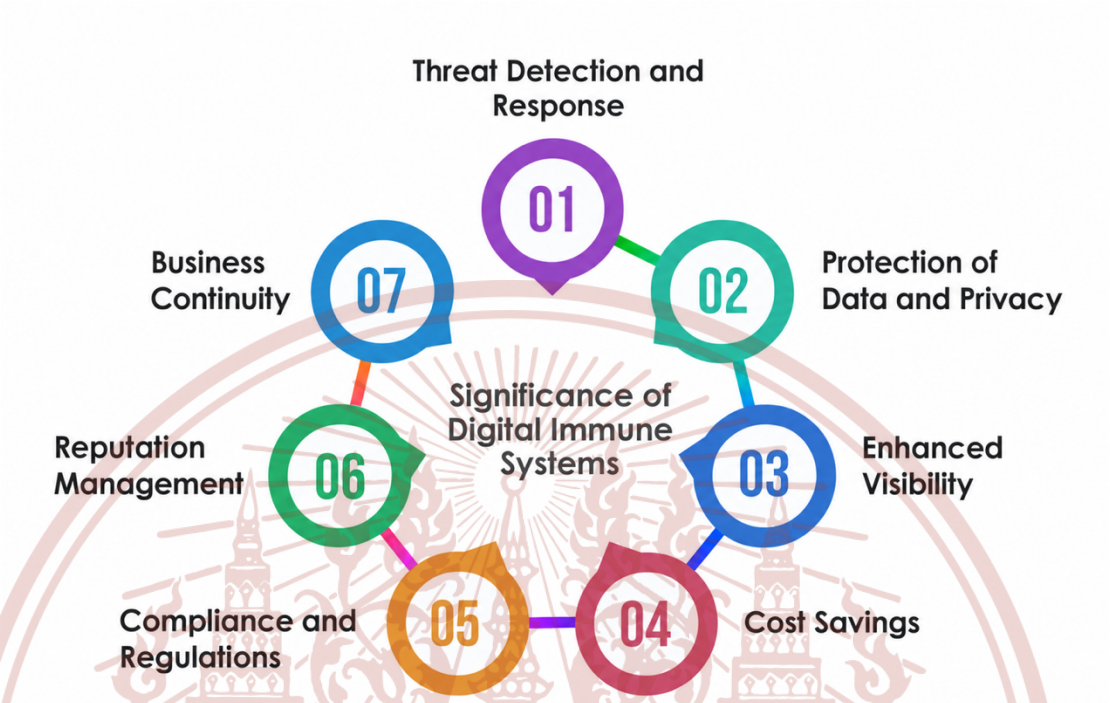
2.4.2.12 ความปลอดภัยบนคลาวด์ (Cloud Security) คือการปกป้องข้อมูลและแอปพลิเคชันที่อยู่บนบริการคลาวด์ เช่น การเข้ารหัสข้อมูลและการควบคุมการเข้าถึง

ตารางที่ 2-3 การสังเคราะห์องค์ประกอบของการจัดการภูมิคุ้มกันดิจิทัล

ลำดับ	องค์ประกอบ	(Musa, A.I.A.,et al.,2025)	(Hassanin et al., 2025)	(Salem et al., 2024)	(Carlo & Obergfaell, 2024)	(Tooki & Popoola, 2024)	(Ali et al., 2025)	(Krauze & Grabis, 2024b)	(Branytskyi et al., 2022)	(Terziyan et al., 2021)	(Saini et al., 2024)	ผู้แต่ง
1	Cyber Threat Detection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	Incident Response	✓	✓	✓	✓			✓		✓		✓
3	Risk Assessment and Management	✓	✓	✓	✓	✓	✓	✓			✓	✓
4	Vulnerability Management			✓						✓		
5	Data Protection and Privacy	✓	✓	✓	✓	✓	✓		✓			✓
6	Security Awareness Training		✓	✓	✓	✓	✓	✓		✓		✓
7	Security Policy and Compliance		✓	✓		✓	✓		✓	✓		✓
8	Endpoint Security								✓	✓		
9	Backup and Recovery											
10	Network Security	✓	✓	✓		✓				✓		
11	AI-driven Security Solutions	✓		✓		✓			✓			
12	Cloud Security						✓				✓	

จากตารางที่ 2-3 การสังเคราะห์องค์ประกอบของการจัดการภูมิคุ้มกันดิจิทัลจากงานวิจัยที่เกี่ยวข้องจำนวน 10 เรื่อง พบว่ามี 6 ด้าน ที่มีความสอดคล้องกันมากเกินเกณฑ์ 60% ได้แก่ 1) การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection) 2) การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response) 3) การประเมินและจัดการความเสี่ยง (Risk Assessment and Management) 4) การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy) 5) การฝึกอบรมการรับรู้ด้านความปลอดภัย (Security Awareness Training) และ 6) นโยบายความปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance)

ผลการวิเคราะห์ดังกล่าวแสดงให้เห็นถึงองค์ประกอบหลักที่ควรพิจารณาในการพัมนาระบบภูมิคุ้มกันดิจิทัลสำหรับบริบทของสถาบันอุดมศึกษา และเป็นแนวทางในการออกแบบโมเดลที่ตอบสนองต่อภัยคุกคามและความเสี่ยงในสภาพแวดล้อมดิจิทัลได้อย่างครอบคลุม



ภาพที่ 2-10 องค์ประกอบของการจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)

https://www.testingxperts.com

สรุปได้ว่าการจัดการภูมิคุ้มกันดิจิทัล หมายถึงแนวทางการสร้างและพัฒนาระบบที่มีความสามารถในการตอบสนองต่อภัยคุกคามไซเบอร์ โดยมุ่งเน้นการใช้เทคโนโลยีและวิธีการที่ช่วยเสริมสร้างภูมิคุ้มกันให้กับข้อมูลและโครงสร้างพื้นฐานดิจิทัล เพื่อป้องกันและลดความเสี่ยงจากการโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต โดยการจัดการภูมิคุ้มกันดิจิทัลมักใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และการเรียนรู้ของเครื่อง (Machine Learning) ในวิเคราะห์และตรวจจับพฤติกรรมที่อาจเป็นภัยคุกคาม รวมถึงการพัฒนาแบบจำลองที่สามารถคาดการณ์การโจมตีในอนาคตได้อย่างมีประสิทธิภาพ การจัดการภูมิคุ้มกันดิจิทัลนี้ถือเป็นกลยุทธ์ที่สำคัญในการสร้างความมั่นคงและเสริมสร้างความปลอดภัยให้กับองค์กรหรือสถาบันในยุคที่เทคโนโลยีและการสื่อสารมีความซับซ้อนและพัฒนาอย่างรวดเร็ว

2.5 การจัดการองค์กรดิจิทัล (Digital Enterprise Management)

2.5.1 ความหมาย

การจัดการองค์กรดิจิทัล (Digital Enterprise Management) หมายถึง กระบวนการและแนวทางในการบริหารจัดการองค์กรที่ใช้เทคโนโลยีดิจิทัลในการปรับปรุงประสิทธิภาพและการดำเนินงานขององค์กร โดยมุ่งเน้นการสร้างนวัตกรรมและการใช้เทคนิคที่ทันสมัย เช่น อัลกอริธึมฝูงอนุภาค (Particle Swarm Algorithm) เพื่อเพิ่มประสิทธิภาพในการจัดการ การตัดสินใจ และการตอบสนองต่อความต้องการของตลาดในยุคดิจิทัล การจัดการองค์กรดิจิทัลนี้ยังรวมถึงการใช้ข้อมูลและการวิเคราะห์ข้อมูลในการตัดสินใจเชิงกลยุทธ์ เพื่อให้สามารถดำเนินการอย่างรวดเร็วและมีประสิทธิภาพในสภาพแวดล้อมที่เปลี่ยนแปลงอย่างรวดเร็ว (Yin, 2024b)

การจัดการองค์กรดิจิทัล หมายถึง การใช้เทคโนโลยีดิจิทัลและข้อมูลเพื่อปรับปรุงการดำเนินงานและการจัดการทรัพยากรภายในองค์กร โดยเฉพาะการนำเสนอนวัตกรรมในกระบวนการจัดการผ่านการใช้เทคนิคการเรียนรู้เชิงลึก (Deep Learning) ซึ่งสามารถวิเคราะห์และจัดการข้อมูลที่หลากหลายรูปแบบได้อย่างมีประสิทธิภาพ การสร้างและใช้โมเดลข้อมูลที่สามารถนำไปใช้ในการตัดสินใจเชิงกลยุทธ์และการปรับปรุงกระบวนการทำงานขององค์กรได้ นอกจากนี้ การพัฒนาระบบการจัดการที่สามารถประมวลผลข้อมูลจากแหล่งต่าง ๆ ได้อย่างรวดเร็วยังเป็นส่วนสำคัญในการเพิ่มประสิทธิภาพขององค์กรในยุคดิจิทัลอีกด้วย (Yang & Zheng, 2023b)

การจัดการองค์กรดิจิทัล หมายถึง การใช้เทคโนโลยีบล็อกเชนร่วมกับระบบประมวลผลฝังตัว (Embedded Processing System) เพื่อเพิ่มประสิทธิภาพและความโปร่งใสในการดำเนินงานขององค์กรในยุคดิจิทัล โดยมุ่งเน้นการปรับปรุงการจัดการข้อมูลและการสื่อสารภายในองค์กรการจัดการองค์กรดิจิทัลในบริบทนี้เน้นการใช้บล็อกเชนเพื่อสร้างความมั่นคงและความน่าเชื่อถือในข้อมูลที่องค์กรใช้ โดยช่วยให้สามารถติดตามและจัดการข้อมูลได้อย่างมีประสิทธิภาพ รวมถึงการนำเสนอข้อมูลที่ชัดเจนและปลอดภัยสำหรับการตัดสินใจเชิงกลยุทธ์ (D. Li & Liang, 2023a)

การจัดการองค์กรดิจิทัล หมายถึง กระบวนการที่องค์กรใช้เทคโนโลยีดิจิทัลและนวัตกรรมเพื่อปรับปรุงการดำเนินงาน การจัดการทรัพยากร และการตัดสินใจเชิงกลยุทธ์ โดยมุ่งหวังที่จะสร้างคุณค่าและความได้เปรียบในการแข่งขันในตลาดที่เปลี่ยนแปลงอย่างรวดเร็ว การจัดการองค์กรดิจิทัลในบริบทนี้เน้นการบูรณาการเครื่องมือและเทคโนโลยีใหม่ ๆ เช่น ระบบคลาวด์, ปัญญาประดิษฐ์, และการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) เพื่อเพิ่มประสิทธิภาพในการทำงานและส่งเสริมการตัดสินใจที่ดีขึ้น นอกจากนี้ยังเกี่ยวข้องกับการสร้างวัฒนธรรมองค์กรที่เปิดรับการเปลี่ยนแปลงและนวัตกรรม (Y. Wang & Lee, 2023a)

การจัดการองค์กรดิจิทัล หมายถึง การปรับเปลี่ยนโครงสร้างและการดำเนินงานของสถาบันหรือองค์กรด้วยการใช้เทคโนโลยีดิจิทัล เพื่อให้เกิดประสิทธิภาพสูงสุดในการจัดการทรัพยากรและ

ข้อมูล วิจัยนี้เน้นถึงความสำคัญของการพัฒนาโครงสร้างพื้นฐานดิจิทัลและทรัพยากรการศึกษาขั้นสูง เพื่อสร้างความเชื่อมโยงระหว่างการศึกษาและเทคโนโลยีสมัยใหม่ (Xie & Zhang, 2024)

การจัดการองค์กรดิจิทัล หมายถึง กระบวนการที่องค์กรปรับตัวให้สอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยีและดิจิทัล โดยเน้นการพัฒนาและบริหารจัดการในรูปแบบดิจิทัล เพื่อให้เกิดความยืดหยุ่น ความรวดเร็ว และความสามารถในการปรับตัวกับการเปลี่ยนแปลง เพื่อพัฒนาความสามารถของนักศึกษาในการปรับตัวให้เข้ากับการเปลี่ยนแปลงด้านเทคโนโลยีในรูปแบบของการเรียนรู้ดิจิทัล การจัดการองค์กรดิจิทัลจึงเกี่ยวข้องกับการสร้างสภาพแวดล้อมที่พร้อมรองรับการเปลี่ยนแปลงอย่างรวดเร็ว และการพัฒนาทักษะทางสังคมเพื่อให้สอดคล้องกับการใช้งานเทคโนโลยี (E. Hossain et al., 2024)

การจัดการองค์กรดิจิทัล หมายถึง การจัดการโครงสร้าง การดำเนินการ และการใช้ทรัพยากรด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในภาคการศึกษาในยุคหลัง COVID-19 องค์ประกอบสำคัญของการจัดการองค์กรดิจิทัลในการศึกษาระดับสูงเน้นไปที่การพัฒนาระบบการเรียนการสอนผ่านช่องทางดิจิทัล การสร้างแพลตฟอร์มที่สนับสนุนการเรียนรู้ทางไกล และการสร้างความร่วมมือระหว่างนักศึกษาและผู้สอนผ่านเครื่องมือดิจิทัลอย่างต่อเนื่อง ความสำเร็จของการจัดการในองค์กรดิจิทัลในยุคนี้มักมุ่งเน้นไปที่ปัจจัยความสำเร็จที่สำคัญ เช่น ความพร้อมของโครงสร้างพื้นฐานดิจิทัล การฝึกอบรมผู้สอนในเทคโนโลยีใหม่ ๆ และการสนับสนุนจากทั้งผู้บริหารและหน่วยงานภายนอกในการพัฒนานวัตกรรมการเรียนรู้ (Draxler-Weber et al., 2024)

การจัดการองค์กรดิจิทัล หมายถึง การสร้างระบบการบริหารจัดการดิจิทัลที่มีคุณภาพและมีประสิทธิภาพสูง โดยเฉพาะในสถาบันการศึกษาระดับสูงในแอฟริกา งานวิจัยนี้ชี้ให้เห็นถึงความสำคัญของการพัฒนากรอบการประกันคุณภาพสำหรับการเรียนรู้ผ่านระบบดิจิทัล ซึ่งเป็นการผสมผสานระหว่างนโยบาย การกำกับดูแล และการสนับสนุนการใช้เทคโนโลยีดิจิทัลอย่างยั่งยืนในกระบวนการเรียนการสอน โดยมีองค์ประกอบสำคัญของการจัดการองค์กรดิจิทัลในงานวิจัยนี้ได้แก่ โครงสร้างการกำกับดูแล (Governance Structure) การสนับสนุนโครงสร้างพื้นฐานดิจิทัล (Digital Infrastructure Support) การพัฒนาขีดความสามารถของบุคลากร (Capacity Building) และการประเมินและปรับปรุง (Evaluation and Continuous Improvement) (Haipinge & Kadhila, 2024)

การจัดการองค์กรดิจิทัล หมายถึง การดำเนินการและบริหารจัดการโครงสร้างพื้นฐานด้านข้อมูลและการดำเนินธุรกิจโดยใช้เทคโนโลยีดิจิทัลเป็นตัวขับเคลื่อนหลัก เพื่อเพิ่มประสิทธิภาพ ความยืดหยุ่น และความสามารถในการตอบสนองต่อการเปลี่ยนแปลงอย่างรวดเร็วในสภาพแวดล้อมการทำงานที่เป็นดิจิทัล การจัดการองค์กรดิจิทัลภายใต้แนวคิด Industry 4.0 มุ่งเน้นการบูรณาการเทคโนโลยีดิจิทัลและเทคโนโลยีอัตโนมัติในกระบวนการธุรกิจ โดยมีองค์ประกอบ ถ องค์ประกอบ

ได้แก่ 1) โครงสร้างพื้นฐานด้านข้อมูล (Information Infrastructure) การจัดการข้อมูล การรวบรวม วิเคราะห์ และการใช้ข้อมูลในระบบดิจิทัลอย่างมีประสิทธิภาพ 2) เทคโนโลยีอัจฉริยะ (Smart Technologies) เช่น ปัญญาประดิษฐ์ (AI), อินเทอร์เน็ตของสรรพสิ่ง (IoT), และการวิเคราะห์ข้อมูล (Data Analytics) ที่สามารถนำมาใช้ในกระบวนการผลิตและการบริหารจัดการธุรกิจ 3) การบูรณาการระบบ (System Integration) การเชื่อมต่อและบูรณาการระบบดิจิทัลต่าง ๆ ทั้งภายในและภายนอกองค์กรเพื่อเพิ่มความคล่องตัวและประสิทธิภาพในการทำงาน 4) การทำงานอัตโนมัติ (Automation) การใช้ระบบอัตโนมัติในกระบวนการทางธุรกิจเพื่อลดข้อผิดพลาด เพิ่มความแม่นยำ และปรับปรุงการดำเนินงาน และ 5) ความปลอดภัยทางไซเบอร์ (Cybersecurity) การรักษาความปลอดภัยของข้อมูลและโครงสร้างพื้นฐานดิจิทัลเพื่อตอบสนองต่อความเสี่ยงและภัยคุกคามทางไซเบอร์ (Andriushchenko et al., 2019)

การจัดการองค์กรดิจิทัล หมายถึง กระบวนการที่ใช้เทคโนโลยีดิจิทัลในการบริหารจัดการข้อมูลและทรัพยากรขององค์กร เพื่อเพิ่มประสิทธิภาพ ความคล่องตัว และความสามารถในการแข่งขัน โดยการนำเทคโนโลยีที่ทันสมัย เช่น ฐานข้อมูลอิงวัตถุในเชิงประวัติศาสตร์ (Historical Object Base) มาใช้ในการจัดการและวิเคราะห์ข้อมูลที่ซับซ้อนภายในองค์กร โดยมีองค์ประกอบหลักของการจัดการองค์กรดิจิทัลจากงานวิจัยนี้ 5 องค์ประกอบ ได้แก่ 1) ฐานข้อมูลอิงวัตถุในเชิงประวัติศาสตร์ (Historical Object Base) 2) การบูรณาการข้อมูล (Data Integration) 3) การวิเคราะห์ข้อมูลเชิงลึก (Data Analytics) 4) ความปลอดภัยของข้อมูล (Data Security) และ 5) ความยืดหยุ่นในการปรับตัว (Flexibility and Adaptability) (Shvartsman, 1993)

การจัดการองค์กรดิจิทัล หมายถึง การจัดการทรัพยากรดิจิทัลและการใช้เทคโนโลยีขั้นสูง เช่น ปัญญาประดิษฐ์ การวิเคราะห์ข้อมูลขนาดใหญ่ และการเรียนรู้เชิงลึก เพื่อเพิ่มประสิทธิภาพการดำเนินงานองค์กร และปรับปรุงกระบวนการภายในองค์กรอย่างต่อเนื่อง (Yang & Zheng, 2023c)

การจัดการองค์กรดิจิทัล หมายถึง การประยุกต์ใช้เทคโนโลยีดิจิทัลในการจัดการองค์กรอย่างมีประสิทธิภาพ เพื่อรับมือกับการเปลี่ยนแปลงที่เกิดขึ้นในช่วงวิกฤติโรคระบาด โดยใช้เทคโนโลยีเช่น คลาวด์คอมพิวติ้ง ปัญญาประดิษฐ์ และระบบอัตโนมัติเพื่อเพิ่มประสิทธิภาพการดำเนินงานและลดผลกระทบจากปัจจัยภายนอก องค์ประกอบหลักได้แก่ การใช้เทคโนโลยีดิจิทัล การวางแผนและการตัดสินใจโดยใช้ข้อมูล และการเพิ่มประสิทธิภาพและความคล่องตัวในกระบวนการ (Miethlich et al., 2022b)

การจัดการองค์กรดิจิทัล หมายถึง การใช้เทคโนโลยีดิจิทัลในการปรับตัวขององค์กรให้สอดคล้องกับการเปลี่ยนแปลงในเศรษฐกิจดิจิทัล โดยมุ่งเน้นที่การสร้างความยืดหยุ่น ความคล่องตัว และการใช้ข้อมูลเชิงลึกเพื่อสนับสนุนการตัดสินใจ องค์ประกอบสำคัญ ได้แก่ การใช้เทคโนโลยี

สารสนเทศ การปรับตัวเชิงกลยุทธ์ขององค์กร การบริหารจัดการที่ขับเคลื่อนด้วยข้อมูล และการสร้างความยั่งยืนในการดำเนินงาน (Hrosul et al., 2022b)

การจัดการองค์กรดิจิทัล หมายถึง การใช้เทคโนโลยีดิจิทัลในการบริหารจัดการองค์กร รวมถึงกระบวนการจัดการซัพพลายเชนที่ผสมผสานกับการวิเคราะห์พฤติกรรมและการปรับตัวของบุคลากรในองค์กรเพื่อให้การดำเนินงานมีประสิทธิภาพมากขึ้น องค์ประกอบสำคัญได้แก่ การบริหารซัพพลายเชนดิจิทัล การปรับตัวทางจิตวิทยาและพฤติกรรมของบุคลากร และการวิเคราะห์ข้อมูลเพื่อตัดสินใจ (Ukolov & Afanasyev, 2020b)

การจัดการองค์กรดิจิทัล หมายถึง การใช้เทคโนโลยีดิจิทัลและระบบอัตโนมัติในการบริหารจัดการทรัพยากรและกระบวนการต่างๆ ภายในองค์กรเพื่อเพิ่มประสิทธิภาพการดำเนินงาน โดยเฉพาะการใช้เทคโนโลยีเช่น อัลกอริธึมฝูงอนุภาค (Particle Swarm Algorithm) เพื่อปรับปรุงกระบวนการตัดสินใจและการจัดการข้อมูลเชิงกลยุทธ์ องค์ประกอบหลักได้แก่ การวิเคราะห์และการจัดการข้อมูล การเพิ่มประสิทธิภาพการทำงานผ่านอัลกอริธึม และระบบอัตโนมัติและการใช้เทคโนโลยีดิจิทัลในกระบวนการ (Yin, 2024c)

การจัดการองค์กรดิจิทัล หมายถึง กระบวนการจัดการที่ใช้เทคโนโลยีบล็อกเชนและระบบฝังตัว (embedded systems) เพื่อเสริมสร้างความปลอดภัย ความโปร่งใส และประสิทธิภาพในการดำเนินงานขององค์กรในยุคดิจิทัล โดยการบูรณาการระบบต่างๆ ให้สามารถทำงานได้อย่างมีประสิทธิภาพสูงสุด องค์ประกอบหลักได้แก่ การใช้บล็อกเชนในการจัดการข้อมูล ระบบฝังตัวเพื่อการประมวลผล การจัดการความปลอดภัยและความโปร่งใส และการเพิ่มประสิทธิภาพการดำเนินงาน (D. Li & Liang, 2023b)

การจัดการองค์กรดิจิทัล หมายถึง การนำเทคโนโลยีดิจิทัลเข้ามาปรับปรุงกระบวนการบริหารจัดการองค์กรเพื่อสร้างความเป็นเลิศในการดำเนินธุรกิจ โดยการใช้เทคโนโลยีดิจิทัลเพื่อปรับปรุงประสิทธิภาพและขับเคลื่อนนวัตกรรมทางธุรกิจ องค์ประกอบได้แก่ นวัตกรรมดิจิทัลเพื่อเพิ่มประสิทธิภาพการดำเนินงาน การใช้เทคโนโลยีเพื่อปรับปรุงกระบวนการธุรกิจ การบริหารจัดการข้อมูลและเทคโนโลยี และการเสริมสร้างความสามารถทางการแข่งขันผ่านดิจิทัล (Y. Wang & Lee, 2023b)

การจัดการองค์กรดิจิทัล หมายถึง กระบวนการที่ใช้เทคโนโลยีดิจิทัลเพื่อปรับปรุงการดำเนินงานและการบริหารจัดการข้อมูลในองค์กร โดยเน้นการใช้มาตรการด้านความปลอดภัยและกลยุทธ์ที่เชื่อถือได้เพื่อปกป้องข้อมูลและเพิ่มประสิทธิภาพในการทำงานในสภาพแวดล้อมคลาวด์ (Rujira et al., 2020) มีองค์ประกอบหลักได้แก่ การจัดการข้อมูล คือการจัดเก็บและการวิเคราะห์ข้อมูลเพื่อปรับปรุงการตัดสินใจ ความปลอดภัยของข้อมูล คือการใช้มาตรการความปลอดภัยเพื่อปกป้องข้อมูล

ในระบบคลาวด์ กลยุทธ์ด้านความเชื่อถือ คือการสร้างกลไกการให้บริการที่เชื่อถือได้ และการใช้เทคโนโลยี AI คือการนำการเรียนรู้ของเครื่องมาช่วยในการตรวจสอบและป้องกันภัยคุกคาม (Saini et al., 2024)

องค์กรดิจิทัล (Digital Organization) คือ องค์กรที่ใช้เทคโนโลยีดิจิทัลเป็นศูนย์กลางในการดำเนินธุรกิจและกระบวนการทำงานทั้งหมด ตั้งแต่การบริหารจัดการภายใน การประมวลผลข้อมูลไปจนถึงการให้บริการลูกค้า องค์กรดิจิทัลมุ่งเน้นการนำเทคโนโลยีมาช่วยเสริมประสิทธิภาพของงานในทุกระดับ เช่น การใช้ระบบคลาวด์ ปัญญาประดิษฐ์ (AI) บล็อกเชน และการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) เพื่อตัดสินใจเชิงกลยุทธ์ นอกจากนี้ องค์กรยังต้องมีความยืดหยุ่นสูงในการปรับตัวให้สอดคล้องกับความเปลี่ยนแปลงทางเทคโนโลยีและความต้องการของตลาด โดยส่งเสริมวัฒนธรรมดิจิทัลที่เน้นการทำงานร่วมกัน การปรับตัวอย่างรวดเร็ว และการสร้างนวัตกรรมใหม่ๆ เพื่อสร้างความได้เปรียบทางธุรกิจ อีกทั้งการใช้ข้อมูลเป็นฐานในการดำเนินการช่วยเพิ่มความแม่นยำในการตัดสินใจและการพัฒนาผลิตภัณฑ์หรือบริการที่ตอบโจทย์ความต้องการของผู้บริโภค (Meepung, Nilsook, et al., 2021)

องค์ประกอบขององค์กรดิจิทัล (Digital Organization) เพื่อให้องค์กรก้าวไปสู่องค์กรแบบใหม่ที่ได้ชื่อว่า เป็นองค์กรดิจิทัล (Digital Organization) มีองค์ประกอบสำคัญ 4 ประการดังนี้

1. Digital Mindset
2. Digital Skills
3. Digital Culture
4. Digital Proces

McKinsey (2020) กล่าวถึง กรอบการเป็นองค์กรดิจิทัล (Digital Organization Framework) ประกอบด้วย

1. Structure
2. Leadership
3. Culture
4. Operating model
5. Taltent and Skills
6. Sequencing the Journey

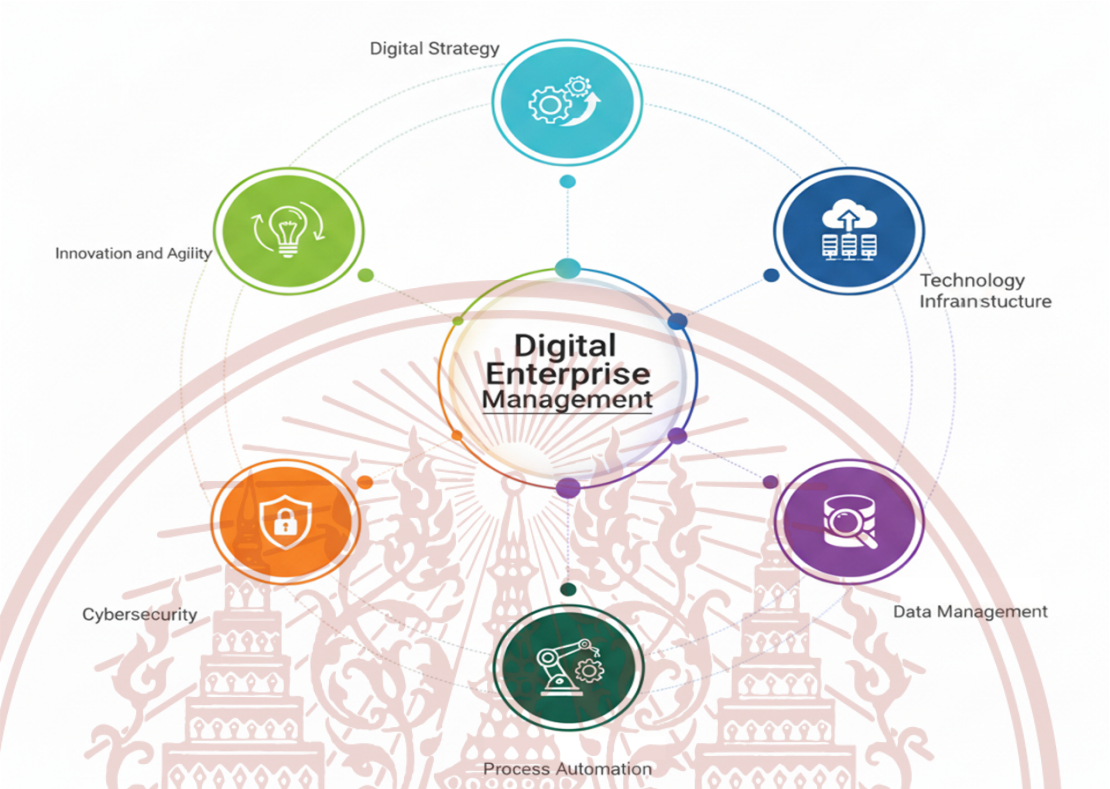
2.5.2 องค์ประกอบของ Digital Enterprise Management ประกอบไปด้วยหลายส่วนที่สำคัญเพื่อให้การจัดการองค์กรในยุคดิจิทัลมีประสิทธิภาพและตอบสนองต่อความเปลี่ยนแปลงของเทคโนโลยีสมัยใหม่ โดยองค์ประกอบหลักของการจัดการองค์กรดิจิทัล ได้แก่

1. กลยุทธ์ดิจิทัล (Digital Strategy) องค์กรต้องมีกลยุทธ์ที่ชัดเจนเกี่ยวกับการใช้เทคโนโลยีดิจิทัล เพื่อให้เกิดประโยชน์สูงสุด ทั้งในการเพิ่มประสิทธิภาพและความสามารถในการแข่งขันในตลาด
2. โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure) โครงสร้างพื้นฐานทางเทคโนโลยี เช่น ระบบคลาวด์, บิ๊กดาต้า, อินเทอร์เน็ตของสรรพสิ่ง (IoT), และเครือข่ายความปลอดภัยไซเบอร์ ถือเป็นรากฐานสำคัญที่สนับสนุนการดำเนินงานขององค์กร
3. การจัดการข้อมูล (Data Management) การเก็บรวบรวม จัดการ และวิเคราะห์ข้อมูลถือเป็นหัวใจสำคัญในการสนับสนุนการตัดสินใจที่มีข้อมูลสนับสนุน การจัดการข้อมูลที่ดีช่วยสร้างมูลค่าและเพิ่มความสามารถในการคาดการณ์และตอบสนองต่อความต้องการของลูกค้า
4. การทำงานอัตโนมัติของกระบวนการ (Process Automation) เทคโนโลยีดิจิทัลสามารถนำมาปรับปรุงและทำให้งานภายในองค์กรดำเนินไปโดยอัตโนมัติ (Automation) เพื่อลดความซับซ้อน เพิ่มประสิทธิภาพ และลดต้นทุนในการดำเนินงาน
5. การพัฒนาแรงงานดิจิทัล (Workforce Transformation) การพัฒนาและเพิ่มพูนทักษะของพนักงานให้สามารถใช้เทคโนโลยีดิจิทัลได้อย่างมีประสิทธิภาพ พร้อมปรับเปลี่ยนรูปแบบการทำงานให้ทันสมัยและตอบสนองต่อการเปลี่ยนแปลงอย่างรวดเร็ว
6. ประสบการณ์ลูกค้า/ผู้รับบริการ (Customer Experience) การใช้เทคโนโลยีดิจิทัลเพื่อสร้างประสบการณ์ที่ดีให้กับลูกค้า เช่น การใช้ปัญญาประดิษฐ์ (AI) และเครื่องมือวิเคราะห์ข้อมูลเพื่อปรับปรุงการบริการและเข้าใจพฤติกรรมของลูกค้า
7. ความปลอดภัยทางไซเบอร์ (Cybersecurity) ความปลอดภัยของข้อมูลและระบบดิจิทัลเป็นสิ่งสำคัญอย่างยิ่ง โดยองค์กรต้องมีระบบการป้องกันที่เข้มแข็งเพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์
8. นวัตกรรมและความคล่องตัว (Innovation and Agility) การสร้างสรรค์นวัตกรรมและความสามารถในการปรับตัวอย่างรวดเร็วต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ ถือเป็นหัวใจสำคัญในการสร้างความยั่งยืนให้กับองค์กรดิจิทัล

ตารางที่ 2-4 การสังเคราะห์องค์ประกอบของการจัดการองค์กรดิจิทัล

ลำดับ	การจัดการองค์กรดิจิทัล	(Saini et al., 2024)	(D. Li & Liang, 2023b)	(Yin, 2024c)	(Ukolov & Afanasyev, 2020b)	(Hrosul et al., 2022b)	(Y. Wang & Lee, 2023a)	(Miethlich et al., 2022b)	(Yang & Zheng, 2023c)	(Andriushchenko et al., 2019)	(Shvartsman, 1993)	ผู้วิจัย
1	Digital Strategy	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
2	Technology Infrastructure	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
3	Data Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	Process Automation		✓	✓			✓	✓	✓	✓		✓
5	Workforce Transformation											
6	Customer Experience				✓	✓						
7	Cybersecurity	✓	✓	✓				✓		✓	✓	✓
8	Innovation and Agility	✓		✓			✓	✓		✓		

จากตาราง 2-4 การสังเคราะห์องค์ประกอบของการจัดการองค์กรดิจิทัล (Digital Enterprise Management) จากงานวิจัยที่เกี่ยวข้องจำนวน 10 เรื่อง พบว่ามี 5 ด้านที่มีความสอดคล้องกันมากเกินเกณฑ์ 60% ได้แก่ 1) กลยุทธ์ดิจิทัล (Digital Strategy) 2) โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure) 3) การจัดการข้อมูล (Data Management) 4) กระบวนการอัตโนมัติ (Process Automation) และ 5) ความปลอดภัยทางไซเบอร์ (Cybersecurity)



ภาพที่ 2-11 องค์ประกอบของการจัดการองค์กรดิจิทัล (Digital Enterprise Management)

สรุปได้ว่า การจัดการองค์กรดิจิทัล (Digital Enterprise Management) คือการบริหารจัดการองค์กรแบบบูรณาการ โดยใช้เทคโนโลยีดิจิทัลและระบบสารสนเทศเพื่อเพิ่มประสิทธิภาพในการดำเนินงาน พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีและนวัตกรรมให้รองรับการเติบโตขององค์กรในยุคดิจิทัล รวมถึงการปรับตัวให้เข้ากับการเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็ว การจัดการองค์กรดิจิทัลประกอบด้วย 6 องค์ประกอบสำคัญ คือ กลยุทธ์ดิจิทัล (Digital Strategy) โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure) การจัดการข้อมูล (Data Management) กระบวนการอัตโนมัติ (Process Automation) ความปลอดภัยทางไซเบอร์ (Cybersecurity) และนวัตกรรมและความคล่องตัว (Innovation and Agility)

2.6 สถาบันอุดมศึกษา (Higher Education Institution)

2.6.1 ความหมาย

สถาบันอุดมศึกษา (Higher Education Institution) หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาและพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษานี้ จะเน้นการสำรวจแนวทางและข้อมูลเชิงลึกเกี่ยวกับการเปลี่ยนแปลงดิจิทัลในด้านการศึกษาการจัดการการเงินที่

เกิดขึ้นใน สถาบันการศึกษาของเอกชน การศึกษาอาจวิเคราะห์ถึงแนวทางปฏิบัติที่ใช้ในการนำเทคโนโลยีดิจิทัลมาใช้ในการสอนและการเรียนรู้ รวมถึงผลกระทบที่มีต่อการพัฒนาทักษะและความรู้ของนักศึกษาในสาขาการจัดการการเงิน นอกจากนี้ ยังอาจตรวจสอบถึงความท้าทายและโอกาสที่เกิดขึ้นจากการนำการเปลี่ยนแปลงดิจิทัลมาใช้ในระบบการศึกษาที่มีเป้าหมายเพื่อเตรียมความพร้อมให้กับนักศึกษาในตลาดแรงงาน (Chenchen et al., 2023)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาและพัฒนาทักษะในระดับปริญญาตรีและสูงกว่าในบริบทของการศึกษานี้จะมุ่งเน้นการสำรวจผลกระทบของความหลากหลาย (Diversity) ต่อผลการทำงาน (Job Performance) โดยเฉพาะในมหาวิทยาลัยเอกชนในประเทศอียิปต์ การศึกษาอาจวิเคราะห์ถึงปัจจัยต่าง ๆ เช่น ความหลากหลายทางวัฒนธรรม เพศ อายุ และประสบการณ์ ที่อาจส่งผลต่อการทำงานร่วมกันและประสิทธิภาพของบุคลากรในสถาบันการศึกษา นอกจากนี้ยังอาจพิจารณาถึงความท้าทายและโอกาสที่เกิดจากความหลากหลายในการสร้างสภาพแวดล้อมการทำงานที่มีประสิทธิภาพและสร้างสรรค์ (Said et al., 2023)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่นๆ ที่มุ่งเน้นการให้การศึกษาและพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษานี้จะมุ่งเน้นการสำรวจผลกระทบของการนำเทคโนโลยีที่เป็นการเปลี่ยนแปลง (Disruptive Technology) มาใช้ต่อการเปลี่ยนแปลงองค์กร (Organizational Change) โดยเฉพาะในมหาวิทยาลัยเอกชนในประเทศจอร์แดน การศึกษาอาจวิเคราะห์ถึงวิธีการที่เทคโนโลยีใหม่สามารถเปลี่ยนแปลงโครงสร้าง วิธีการทำงาน และวัฒนธรรมภายในองค์กร รวมถึงผลกระทบที่มีต่อการเรียนการสอน การบริหารจัดการ และประสิทธิภาพโดยรวมของสถาบันการศึกษา (Al-Fugaha et al., 2024)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาในระดับปริญญาโทและระดับสูงกว่า ในบริบทของการศึกษานี้จะมุ่งเน้นการสำรวจและวิเคราะห์ ทักษศตวรรษที่ 21 (21st Century Skills) ที่นักศึกษาปริญญาโทใน สาขาศิลปศาสตร์ (Liberal Arts) ของมหาวิทยาลัยเอกชนได้รับ การศึกษาอาจพิจารณาถึงทักษะที่จำเป็นในยุคปัจจุบัน เช่น การคิดอย่างมีวิจารณญาณ การสื่อสารที่มีประสิทธิภาพ การทำงานร่วมกัน การใช้เทคโนโลยีดิจิทัล และการมีจริยธรรมและความรับผิดชอบทางสังคม (Watcharinrat et al., 2024)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษานี้จะมุ่งเน้นการสำรวจผลกระทบของ การเป็นผู้ประกอบการเชิงกล

ยุทธ์และนวัตกรรม (Strategic and Innovative Entrepreneurship) และทุนทางสังคม (Social Capital) ต่อผลการดำเนินงานโดยรวมของธุรกิจ (Business Overall Performance) ผ่านการสร้าง การจัดการซัพพลายเชนที่ยั่งยืน (Sustainable Supply Chain Management) ในมหาวิทยาลัยเอกชนในจอร์แดน การศึกษาอาจวิเคราะห์ถึงความสัมพันธ์ระหว่างองค์ประกอบเหล่านี้และผลกระทบที่มีต่อประสิทธิภาพทางธุรกิจภายในสถาบันการศึกษา (Al-Tarawneh et al., 2024)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษานี้จะมุ่งเน้นการสำรวจผลกระทบของ แนวคิดเกี่ยวกับการเป็นผู้ประกอบการ (Entrepreneurship Self-Concept), แรงจูงใจในการทำงาน (Work Motivation), และ การรับความเสี่ยง (Risk Taking) ต่อ ประสิทธิภาพของฝ่ายทรัพยากรมนุษย์ (Human Resource Department Performance) และ ผลการดำเนินงานโดยรวมของธุรกิจ (Business Overall Performance) ในมหาวิทยาลัยเอกชนในจอร์แดน การศึกษาอาจวิเคราะห์ถึงปัจจัยที่มีผลต่อการดำเนินงานของฝ่ายทรัพยากรมนุษย์และวิธีการที่สามารถปรับปรุงประสิทธิภาพทางธุรกิจได้ (Hanandeh et al., 2024)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันอื่น ๆ ที่มุ่งเน้นการให้ความรู้และการฝึกอบรมในระดับปริญญาตรีและสูงกว่านั้น โดยมักมีการดำเนินการวิจัยและพัฒนานวัตกรรมในหลากหลายสาขา ทั้งในด้านวิทยาศาสตร์ สังคมศาสตร์ และมนุษยศาสตร์ สถาบันอุดมศึกษามีบทบาทสำคัญในการพัฒนาความสามารถทางการศึกษาและทักษะของบุคลากรในอนาคต รวมถึงการเตรียมความพร้อมให้กับนักเรียนในการเผชิญกับความท้าทายใหม่ ๆ ในโลกที่มีการเปลี่ยนแปลงอย่างรวดเร็ว (Cheng & Wang, 2022)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูงให้แก่ผู้เรียน ซึ่งรวมถึงมหาวิทยาลัยและวิทยาลัยที่มีการเสนอหลักสูตรที่มุ่งเน้นการศึกษาที่มีคุณภาพและการพัฒนาทักษะที่จำเป็นสำหรับการทำงานในอนาคต โดยสถาบันอุดมศึกษาจะมีลักษณะเฉพาะที่แตกต่างจากสถาบันการศึกษาระดับต่ำกว่า เช่น การนำเทคโนโลยีใหม่ๆ มาใช้ในกระบวนการเรียนการสอน การให้บริการที่สนับสนุนการเรียนรู้ รวมถึงการมีความมุ่งมั่นในการสร้างสภาพแวดล้อมการเรียนรู้ที่ทันสมัยและตอบสนองความต้องการของนักศึกษา ซึ่งในกรณีนี้เกี่ยวข้องกับแนวคิดของ "Smart Campus" ที่ใช้เทคโนโลยีและนวัตกรรมในการพัฒนาสภาพแวดล้อมการเรียนรู้และการใช้ชีวิตในมหาวิทยาลัย (Mustafa et al., 2021)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง เช่น มหาวิทยาลัย วิทยาลัย หรือสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการพัฒนาความรู้และทักษะให้กับนักศึกษาในระดับ

ปริญญาตรีและสูงกว่านั้น โดยเฉพาะในบริบทของการนำ Blockchain Technology มาใช้ สถาบันอุดมศึกษาจะมีบทบาทในการศึกษาความพร้อมทางด้านเทคโนโลยี การพัฒนาหลักสูตรที่เกี่ยวข้อง การสร้างโครงสร้างพื้นฐาน และการส่งเสริมการวิจัยและนวัตกรรมที่ใช้เทคโนโลยีนี้ เพื่อปรับปรุงระบบการจัดการข้อมูล การลงทะเบียน และการรับรองคุณวุฒิของนักศึกษา รวมถึงการสนับสนุนการทำธุรกรรมที่มีความปลอดภัยและโปร่งใส (Dwivedi & Vig, 2023)

สถาบันอุดมศึกษา หมายถึง ถาบันการศึกษาที่มอบการศึกษาระดับสูง โดยรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาที่มุ่งเน้นการให้ความรู้และพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษาเกี่ยวกับเทคโนโลยี Metaverse และการใช้เทคโนโลยีเสมือนจริงใน สถาบันอุดมศึกษาจะเน้นถึงการศึกษาและการทำความเข้าใจเกี่ยวกับผลกระทบทางสังคมและความยั่งยืนของการนำเทคโนโลยีเหล่านี้มาใช้ การสำรวจความคิดเห็นของนักศึกษาเกี่ยวกับประสบการณ์และการมีส่วนร่วมในสภาพแวดล้อมการเรียนรู้ที่ใช้เทคโนโลยีเสมือนจริง และการพิจารณาว่าเทคโนโลยีนี้สามารถสนับสนุนการพัฒนาและการยั่งยืนในด้านการศึกษาของสถาบันได้ (Alkhwaldi, 2024)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาที่มีคุณภาพในระดับปริญญาตรีและสูงกว่านั้น ในบริบทของการศึกษาเกี่ยวกับ Cloud Computing ในสถาบันอุดมศึกษาจะเน้นถึงการใช้บริการคลาวด์ในการสนับสนุนการเรียนการสอน การบริหารจัดการข้อมูล และการให้บริการต่าง ๆ แก่นักศึกษาและบุคลากร การวิจัยนี้อาจสำรวจปัจจัยที่มีผลต่อการใช้บริการคลาวด์อย่างต่อเนื่อง เช่น ความสะดวกสบาย ความปลอดภัยของข้อมูล และประสิทธิภาพของการบริการ รวมถึงการวิเคราะห์ว่าเทคโนโลยีคลาวด์สามารถช่วยพัฒนาสถาบันการศึกษาให้ทันสมัยและมีประสิทธิภาพมากขึ้นได้ (Qasem et al., 2020)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง เช่น มหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการเรียนการสอนในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษาเกี่ยวกับ Enterprise Architecture (EA) และการเปลี่ยนแปลงดิจิทัลในสถาบันอุดมศึกษา จะมุ่งเน้นถึงการนำกรอบการทำงานทางสถาปัตยกรรมองค์กรมาใช้เพื่อสนับสนุนการเปลี่ยนแปลงทางดิจิทัลในสถาบันการศึกษา การศึกษานี้อาจสำรวจว่า EA สามารถช่วยในการปรับปรุงกระบวนการทำงาน การจัดการข้อมูล และการให้บริการทางการศึกษาที่มีประสิทธิภาพมากขึ้นได้อย่างไร รวมถึงการสร้างความยั่งยืนในระบบการศึกษาที่ใช้เทคโนโลยีดิจิทัล (Gomes et al., 2020)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้ความรู้ในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษาเกี่ยวกับ Internet of Things (IoT) และการนำไปใช้ในสถาบันอุดมศึกษา จะมุ่งเน้นถึงการสำรวจปัจจัยที่มีผลต่อการยอมรับและการนำ IoT มาใช้ในสถาบันการศึกษาภายในประเทศซาอุดีอาระเบีย โดยใช้ Technology Acceptance Model (TAM) ที่ปรับปรุงใหม่เพื่อวิเคราะห์พฤติกรรมและทัศนคติของบุคลากรและนักศึกษาในด้านการใช้เทคโนโลยี IoT ในกระบวนการเรียนการสอน การบริหารจัดการ และการสร้างสภาพแวดล้อมการเรียนรู้ที่ดีขึ้น (Masadeh & El-Haggar, 2023)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง เช่น มหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการพัฒนาความรู้และทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษาเกี่ยวกับปัญญาประดิษฐ์ (AI) ในสถาบันอุดมศึกษา จะมุ่งเน้นถึงการสำรวจโอกาสและอุปสรรคในการใช้ AI เพื่อสนับสนุนการเรียนรู้และผลลัพธ์การศึกษาของนักศึกษาในสถาบันการศึกษาในซาอุดีอาระเบีย การศึกษาอาจวิเคราะห์ถึงความเป็นไปได้ของการนำปัญญาประดิษฐ์ มาใช้ในการพัฒนาหลักสูตร การประเมินผลการเรียนรู้ และการปรับปรุงประสบการณ์การเรียนการสอน เพื่อเสริมสร้างผลลัพธ์การเรียนรู้ที่มีคุณภาพและสอดคล้องกับความต้องการของนักศึกษาในยุคดิจิทัล (Alotaibi & Alshehri, 2023)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้ความรู้และพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษาเกี่ยวกับสถาปัตยกรรมองค์กรในสถาบันอุดมศึกษา จะมุ่งเน้นการวิเคราะห์ปัจจัยที่มีผลต่อการออกแบบและการจัดการสถาปัตยกรรมองค์กรในสถาบันการศึกษา การศึกษานี้อาจใช้วิธีการ Confirmatory Factor Analysis (CFA) เพื่อตรวจสอบและยืนยันโครงสร้างปัจจัยที่เกี่ยวข้องกับ EA และประเมินความสัมพันธ์ระหว่างปัจจัยต่าง ๆ ที่มีผลต่อประสิทธิภาพในการบริหารจัดการและการดำเนินงานของสถาบันการศึกษา (Tungpantong et al., 2022)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้ความรู้และการพัฒนาทักษะในระดับปริญญาตรีและสูงกว่านั้น ในบริบทของการพัฒนา Agile Enterprise Architecture สำหรับการเปลี่ยนแปลงดิจิทัลในสถาบันอุดมศึกษา จะมุ่งเน้นไปที่การสร้างกรอบการทำงานที่มีความยืดหยุ่นและตอบสนองได้เร็วเพื่อตอบสนองต่อความต้องการและความท้าทายของการศึกษาในยุคดิจิทัล การศึกษาอาจสำรวจวิธีการที่ Agile EA สามารถสนับสนุนกระบวนการเปลี่ยนแปลงใน

สถาบันการศึกษา เช่น การปรับปรุงการเรียนการสอน การบริหารจัดการข้อมูล และการให้บริการทางการศึกษา รวมถึงการสร้างวัฒนธรรมที่เปิดกว้างต่อการใช้เทคโนโลยีใหม่ ๆ และการเรียนรู้ที่ยั่งยืน (Sararuch et al., 2023a)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้ความรู้และพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการพัฒนา ICT Strategic Framework สำหรับสถาบันอุดมศึกษา จะมุ่งเน้นไปที่การสร้างกรอบการทำงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ที่มีประสิทธิภาพ เพื่อสนับสนุนการดำเนินงาน การเรียนการสอน และการบริหารจัดการภายในสถาบัน โดยเฉพาะในกรณีของมหาวิทยาลัยมะตารัม การศึกษาอาจเน้นที่การประเมินความต้องการทาง ICT การพัฒนานโยบาย และการสร้างแผนกลยุทธ์ที่ตอบสนองต่อเป้าหมายทางการศึกษา รวมถึงการสนับสนุนการเปลี่ยนแปลงและนวัตกรรมในสถาบันการศึกษา (Hussein et al., 2023)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มีการให้การศึกษาที่มุ่งเน้นการพัฒนาความรู้และทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษานี้จะเน้นไปที่การสำรวจและวิเคราะห์การนำ EdTech (เทคโนโลยีการศึกษาใหม่ ๆ มาใช้ใน (สถาบันอุดมศึกษา ในช่วงวิกฤติการระบาดของ COVID-19 เพื่อสนับสนุนการเรียนการสอนออนไลน์และการปรับตัวของสถาบันการศึกษา การศึกษานี้อาจพิจารณาถึงวิธีที่สถาบันอุดมศึกษา ปรับใช้เทคโนโลยีใหม่ ๆ เพื่อรับมือกับความท้าทายที่เกิดขึ้นในช่วงการระบาด รวมถึงผลกระทบที่มีต่อการเรียนรู้ของนักศึกษา การสื่อสารระหว่างบุคลากร และการบริหารจัดการภายในสถาบัน (Wood-Harper, 2020)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาและพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษาเกี่ยวกับ IoT-based Smart Campus จะเน้นการพัฒนาและนำเสนอโมเดลการนำ IoT มาใช้ในสถาบันการศึกษาเพื่อสร้างสภาพแวดล้อมการเรียนรู้ที่ทันสมัยและมีประสิทธิภาพ การศึกษาอาจตรวจสอบแนวทางที่สถาบันอุดมศึกษา สามารถนำ IoT มาปรับใช้เพื่อปรับปรุงการบริหารจัดการพื้นที่การเรียนรู้ การบริการสำหรับนักศึกษา และการใช้ทรัพยากรอย่างมีประสิทธิภาพ นอกจากนี้ ยังอาจวิเคราะห์ปัจจัยที่มีผลต่อการนำโมเดลนี้มาใช้และความท้าทายที่สถาบันการศึกษาอาจเผชิญในการทำให้เกิด Smart Campus (Sneesl et al., 2022)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาและการพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษานี้ จะเน้นถึงการเพิ่มขึ้นของการใช้ทรัพยากร

ดิจิทัลในสถาบันอุดมศึกษา และบทบาทของ Artificial Intelligence (AI) ในการช่วยในการตัดสินใจที่เกี่ยวข้องกับผลการเรียนของนักศึกษา การศึกษาอาจสำรวจถึงวิธีที่ AI สามารถวิเคราะห์ข้อมูลการเรียนรู้และพฤติกรรมของนักศึกษาเพื่อให้ข้อมูลเชิงลึกที่ช่วยในการปรับปรุงผลสัมฤทธิ์ทางการศึกษา รวมถึงการใช้ข้อมูลเหล่านี้ในการพัฒนานโยบายและกลยุทธ์ในการสนับสนุนการเรียนรู้ของนักศึกษา (Jokhan et al., 2022)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่มอบการศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้ความรู้และการพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษานี้ จะมุ่งเน้นการสำรวจผลกระทบของการใช้ เทคโนโลยีอัจฉริยะ (Smart Technologies) เพื่อสนับสนุนการพัฒนาที่ยั่งยืนในสถาบันอุดมศึกษา การศึกษาอาจวิเคราะห์ถึงวิธีที่เทคโนโลยีเหล่านี้สามารถนำมาใช้เพื่อปรับปรุงกระบวนการเรียนการสอน การบริหารจัดการภายในสถาบัน และการใช้ทรัพยากรอย่างมีประสิทธิภาพ นอกจากนี้ ยังอาจสำรวจถึงความท้าทายและโอกาสที่เกิดขึ้นจากการนำเทคโนโลยีอัจฉริยะมาใช้ในการพัฒนาที่ยั่งยืน ซึ่งเป็นปัจจัยสำคัญในการสร้างสภาพแวดล้อมการเรียนรู้ที่ตอบสนองต่อความต้องการในอนาคต (Shishakly et al., 2024)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้ความรู้และการพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษาเกี่ยวกับการออกแบบและวิเคราะห์ ระบบ IoT (Internet of Things) ที่อัตโนมัติเพื่อเพิ่มประสิทธิภาพการไหลของข้อมูลในสถาบันอุดมศึกษา การศึกษานี้จะเน้นการพัฒนาวิธีการและเทคโนโลยีที่สามารถช่วยในการจัดการและปรับปรุงการไหลของข้อมูลภายในสถาบันการศึกษา โดยเฉพาะในด้านการบริหารจัดการข้อมูล การสื่อสารระหว่างระบบต่าง ๆ และการสนับสนุนการตัดสินใจอย่างมีประสิทธิภาพ การศึกษาอาจตรวจสอบถึงการประยุกต์ใช้ IoT ในการพัฒนาโครงสร้างพื้นฐานที่ทำให้การแลกเปลี่ยนข้อมูลระหว่างผู้เรียน ผู้สอน และระบบการศึกษาอื่น ๆ เป็นไปได้อย่างราบรื่นและมีประสิทธิภาพ (Adegbenjo et al., 2023)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง เช่น มหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้ความรู้และการพัฒนาทักษะในระดับปริญญาตรีและสูงกว่า ในบริบทของการศึกษานี้ จะมุ่งเน้นการสำรวจปัจจัยที่มีผลต่อการนำ Cloud Computing มาใช้ในสถาบันอุดมศึกษาในประเทศที่พัฒนาไม่มาก เช่น สาธารณรัฐเยเมน การศึกษาอาจวิเคราะห์ถึงความท้าทายและโอกาสที่เกี่ยวข้องกับการนำเทคโนโลยีคลาวด์มาใช้ในสถาบันการศึกษา รวมถึงปัจจัยทางด้านเทคนิค การเงิน นโยบาย และวัฒนธรรมองค์กรที่มีผลต่อการ

ตัดสินใจในการใช้บริการคลาวด์ เพื่อสนับสนุนการเรียนการสอนและการบริหารจัดการข้อมูลภายในสถาบัน (Alghushami et al., 2020)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาในระดับอุดมศึกษา เช่น มหาวิทยาลัย หรือวิทยาลัยต่าง ๆ ในประเทศกำลังพัฒนา ซึ่งเป็นกลุ่มเป้าหมายในการศึกษาพฤติกรรมและเจตนาของนักศึกษาในการใช้เทคโนโลยี Metaverse เพื่อนำไปพัฒนาการเรียนการสอนและการบริหารจัดการในสถาบันอุดมศึกษาให้มีประสิทธิภาพยิ่งขึ้น (Alkhwaldi, 2023)

สถาบันอุดมศึกษา หมายถึง สถาบันการศึกษาที่ให้การศึกษาระดับสูง มีบทบามสำคัญในการพัฒนาทักษะและความรู้ที่สนับสนุนการเติมโตทางเศรษฐกิจ และสังคม โดยเฉพาะในบริบทของการใช้เทคโนโลยีใหม่ๆ (Hiran & Dadhich, 2024)

สรุปได้ว่า สถาบันอุดมศึกษา คือสถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาในระดับปริญญาตรีและสูงกว่า โดยมีเป้าหมายในการพัฒนาความรู้ ทักษะ และคุณสมบัติของนักศึกษา เพื่อเตรียมความพร้อมให้กับนักศึกษาสำหรับการทำงานในตลาดแรงงาน รวมถึงการมีส่วนร่วมในสังคมและการพัฒนาทางเศรษฐกิจและวัฒนธรรม

ตารางที่ 2-5 วิเคราะห์คำสำคัญ

Theme	Definition	Ref.
โครงสร้างองค์กร (Organizational Structure)	กรอบแนวคิดที่ใช้ในในการออกแบบ พัฒนาและจัดการระบบและกระบวนการภายในองค์กรอย่างเป็นระบบ โดยมีการบูรณาการด้านต่าง ๆ ทั้งด้านธุรกิจ ข้อมูล เทคโนโลยี และการจัดการทรัพยากรที่สำคัญ โดยสถาปัตยกรรมองค์กรมีบทบาทในการสร้างความเข้าใจที่ชัดเจนเกี่ยวกับการดำเนินงานในปัจจุบันและวิสัยทัศน์ในอนาคตขององค์กร ช่วยให้ผู้บริหารสามารถวางแผนและตัดสินใจเกี่ยวกับการนำเทคโนโลยีไปใช้อย่างมีประสิทธิภาพ นอกจากนี้สถาปัตยกรรมองค์กรยังครอบคลุมถึงการจัดการเปลี่ยนแปลง การกำกับดูแล และการกำหนดกลยุทธ์ที่สามารถปรับตัวให้สอดคล้องกับสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงอย่างรวดเร็ว เช่นเดียวกับการรับมือกับความต้องการและความท้าทายใหม่ ๆ ซึ่งช่วยให้องค์กรสามารถ	(Y. Jiang et al., 2024c; Khairina et al., 2024b; Muslih et al., 2024a; Takeuchi et al., 2024a; Uzhakova & Fischer, 2024a)

Theme	Definition	Ref.
	ตอบสนองต่อโอกาสทางธุรกิจและการพัฒนานวัตกรรมได้อย่างมีประสิทธิภาพและยั่งยืน	
เทคโนโลยีอัจฉริยะ (Intelligent Technology)	เทคโนโลยีที่พัฒนาให้ระบบคอมพิวเตอร์หรือเครื่องจักรสามารถทำงานที่ต้องใช้ความสามารถทางสติปัญญาของมนุษย์ เช่น การเรียนรู้ การคิดวิเคราะห์ และการตัดสินใจ ปัญญาประดิษฐ์ถูกแบ่งออกเป็นหลายประเภท เช่น การเรียนรู้ของเครื่อง (Machine Learning) และการเรียนรู้เชิงลึก (Deep Learning) โดยมีบทบาทสำคัญในการเพิ่มประสิทธิภาพในการทำงาน ช่วยในการวิเคราะห์ข้อมูลจำนวนมาก และทำให้กระบวนการต่าง ๆ เป็นอัตโนมัติ การนำปัญญาประดิษฐ์มาใช้ในองค์กรช่วยให้การจัดการและดำเนินงานในหลายด้านเป็นไปอย่างมีประสิทธิภาพ ลดข้อผิดพลาด และปรับปรุงการตัดสินใจ	(Abdullahi et al., 2022b; Homaei et al., 2024b; Ortiz-Garcés et al., 2024c; Pexyean et al., 2022; Ramasamy et al., 2022; Vial et al., 2023)
สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture)	การบูรณาการสถาปัตยกรรมองค์กร (Enterprise Architecture) กับปัญญาประดิษฐ์ (Artificial Intelligence) เพื่อให้เกิดกรอบการทำงานที่สามารถออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ รวมถึงการจัดการทรัพยากรต่าง ๆ ภายในองค์กรในลักษณะที่สามารถตอบสนองต่อการเปลี่ยนแปลงและภัยคุกคามต่างๆ ได้อย่างรวดเร็วและแม่นยำ	(X. Han et al., 2021; Krauze & Grabis, 2024a; Mazher et al., 2023)
ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity)	ระบบและกลไกเชิงรุกที่ใช้เทคโนโลยีอัจฉริยะและมาตรการด้านความปลอดภัย เพื่อเสริมสร้างความปลอดภัย ความทนทาน และความสามารถในการฟื้นฟูของระบบดิจิทัล ให้สามารถตรวจจับ ป้องกัน ตอบสนอง และฟื้นตัวจากภัยคุกคามได้อย่างมีประสิทธิภาพ โดยมีเป้าหมายเพื่อรักษาความต่อเนื่อง ความมั่นคง และความยั่งยืนในการดำเนินงานขององค์กร	(George et al., 2023d; Le Blond et al., 2018; Splunk, 2023; Termanini, 2020; Terziyan & Kaikova, 2025)

Theme	Definition	Ref.
การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)	แนวทางการสร้างและพัฒนาระบบที่มีความสามารถในการตอบสนองต่อภัยคุกคามไซเบอร์ โดยมุ่งเน้นการใช้เทคโนโลยีและวิธีการที่ช่วยเสริมสร้างภูมิคุ้มกันให้กับข้อมูลและโครงสร้างพื้นฐานดิจิทัล เพื่อป้องกันและลดความเสี่ยงจากการโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต โดยการจัดการภูมิคุ้มกันดิจิทัลมักใช้เทคโนโลยีปัญญาประดิษฐ์ และการเรียนรู้ของเครื่อง (Machine Learning) ในวิเคราะห์และตรวจจับพฤติกรรมที่อาจเป็นภัยคุกคาม รวมถึงการพัฒนาแบบจำลองที่สามารถคาดการณ์การโจมตีในอนาคตได้อย่างมีประสิทธิภาพ การจัดการภูมิคุ้มกันดิจิทัลนี้ถือเป็นกลยุทธ์ที่สำคัญในการสร้างความมั่นคงและเสริมสร้างความปลอดภัยให้กับองค์กรหรือสถาบันในยุคที่เทคโนโลยีและการสื่อสารมีความซับซ้อนและพัฒนาอย่างรวดเร็ว	(George et al., 2023c; Krauze & Grabis, 2024c, 2024b; Saleh Alrubayyi, 2023a)
การจัดการองค์กรดิจิทัล (Digital Enterprise Management)	การบริหารจัดการองค์กรที่ใช้เทคโนโลยีดิจิทัลและระบบสารสนเทศเพื่อเพิ่มประสิทธิภาพในการดำเนินงาน พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีและนวัตกรรมให้รองรับการเติบโตขององค์กรในยุคดิจิทัล รวมถึงการปรับตัวให้เข้ากับการเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็ว	(Hrosul et al., 2022a; D. Li & Liang, 2023a; Miethlich et al., 2021, 2022a; Ukolov & Afanasyev, 2020a; Y. Wang & Lee, 2023a; Yang & Zheng, 2023a; Yin, 2024a)
สถาบันอุดมศึกษา (Private Universities)	สถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่น ๆ ที่มุ่งเน้นการให้การศึกษาในระดับปริญญาตรีและสูงกว่า โดยมีเป้าหมายในการพัฒนาความรู้ ทักษะ และคุณสมบัติของนักศึกษา เพื่อเตรียมความพร้อมให้กับนักศึกษาสำหรับการทำงานในตลาดแรงงาน รวมถึงการมีส่วนร่วมในสังคมและการพัฒนาทางเศรษฐกิจและวัฒนธรรม	(Al-Fugaha et al., 2024; Muslih et al., 2024a; Roslan et al., 2025b; Safiah et al., 2024; Said et al., 2023; Uruntie et al., 2024)

2.7 สรุปเอกสารและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา พบว่าในปัจจุบัน สถาบันอุดมศึกษากำลังเผชิญกับความท้าทายจากการเปลี่ยนแปลงทางด้านดิจิทัล (Digital Transformation) ที่เกิดขึ้นอย่างรวดเร็ว ทั้งในด้านการจัดการเรียนการสอน การบริหารจัดการองค์กร และการวิจัยเชิงนวัตกรรม ข้อมูลจำนวนมหาศาลจากระบบสารสนเทศเพื่อการศึกษา งานวิจัย และกิจกรรมการเรียนรู้ถูกรวบรวมและนำมาใช้ประโยชน์ แต่ในขณะเดียวกันกลับกลายเป็นเป้าหมายของภัยคุกคามทางไซเบอร์ที่ซับซ้อนและรุนแรงมากขึ้น เช่น การโจมตีข้อมูลผู้เรียน การรั่วไหลของงานวิจัยเชิงลึก ตลอดจนความเสี่ยงจากการใช้แพลตฟอร์มดิจิทัลต่าง ๆ

โครงสร้างองค์กร (Organizational Structure) คือกรอบแนวทางในการวางแผน ออกแบบและบริหารจัดการระบบต่าง ๆ ภายในองค์กรอย่างเป็นระบบ โดยเชื่อมโยงระหว่างการดำเนินงาน การบริหารจัดการ และเทคโนโลยีสารสนเทศ เพื่อให้การทำงานภายในองค์กรสอดคล้องและสามารถปรับตัวได้อย่างรวดเร็วตามการเปลี่ยนแปลง โดยมีองค์ประกอบหลัก เช่น สถาปัตยกรรมด้านธุรกิจ ข้อมูล แอปพลิเคชัน เทคโนโลยี และความปลอดภัย ซึ่งช่วยให้องค์กรสามารถเชื่อมโยงกลยุทธ์ วิสัยทัศน์ และพันธกิจ เข้ากับการใช้ทรัพยากรและเทคโนโลยีได้อย่างเป็นระบบ (TOGAF, Zachman Framework, FEAF)

เทคโนโลยีอัจฉริยะ (Intelligent Technology) คือเทคโนโลยีที่พัฒนาให้ระบบคอมพิวเตอร์หรือเครื่องจักรสามารถทำงานที่ต้องใช้ความสามารถทางสติปัญญาของมนุษย์ เช่น การเรียนรู้ การคิดวิเคราะห์ และการตัดสินใจ ปัญญาประดิษฐ์ถูกแบ่งออกเป็น 4 ประเภท ได้แก่ 1) การเรียนรู้ของเครื่อง (Machine Learning) 2) การเรียนรู้เชิงลึก (Deep Learning) 3) การประมวลผลภาษาธรรมชาติ (Natural Language Processing - NLP) และ 4) ความรู้เชิงพฤติกรรม (Behavioral AI) โดยมีบทบาทสำคัญในการเพิ่มประสิทธิภาพในการทำงาน ช่วยในการวิเคราะห์ข้อมูลจำนวนมาก และทำให้กระบวนการต่าง ๆ เป็นอัตโนมัติ การนำปัญญาประดิษฐ์มาใช้ในองค์กรช่วยให้การจัดการและดำเนินงานในหลายด้านเป็นไปอย่างมีประสิทธิภาพ ลดข้อผิดพลาด และปรับปรุงการตัดสินใจ

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) คือการบูรณาการสถาปัตยกรรมองค์กร (Enterprise Architecture) กับปัญญาประดิษฐ์ (Artificial Intelligence) เพื่อให้เกิดกรอบการทำงานที่สามารถออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ รวมถึงการจัดการทรัพยากรต่าง ๆ ภายในองค์กรในลักษณะที่สามารถตอบสนองต่อการเปลี่ยนแปลงและภัยคุกคามต่างๆ ได้อย่างรวดเร็วและแม่นยำ โดยประกอบด้วย 7 ด้าน ได้แก่ 1.การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ (EA–AI Integration) 2.กรอบการทำงาน

เชิงสถาปัตยกรรม (Architectural Framework) 3.การออกแบบและพัฒนาระบบสารสนเทศด้วย AI (AI-driven Information System Design & Development) 4.การจัดการทรัพยากรอย่างชาญฉลาด (Intelligent Resource Management) 5.การปรับตัวต่อการเปลี่ยนแปลง (Adaptability & Agility) 6.การรับมือภัยคุกคามและความเสี่ยง (Threat & Risk Responsiveness) และ7. จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ (AI Ethics and Responsibility)

ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity) คือระบบและกลไกเชิงรุกที่ใช้เทคโนโลยีอัจฉริยะและมาตรการด้านความปลอดภัย เพื่อเสริมสร้างความปลอดภัย ความทนทาน และความสามารถในการฟื้นฟูของระบบดิจิทัล ให้สามารถตรวจจับ ป้องกัน ตอบสนอง และฟื้นตัวจากภัยคุกคามได้อย่างมีประสิทธิภาพ โดยมีเป้าหมายเพื่อรักษาความต่อเนื่อง ความมั่นคง และความยั่งยืนในการดำเนินงานขององค์กร โดยประกอบด้วย 6 ด้าน ได้แก่ 1) การมองเห็นและเฝ้าระวัง (Observability & Visibility) 2) การตรวจจับภัยคุกคาม (Threat Detection) 3) การสืบสวนและวิเคราะห์ (Investigation & Analysis) 4) การตอบสนองและการป้องกันเชิงรุก (Response & Proactive Defense) 5) ความทนทานและการฟื้นฟู (Resilience & Recovery) และ 6) ความร่วมมือและการสร้างความตระหนักรู้ (Collaboration & Cybersecurity Awareness)

การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) คือแนวทางการสร้างและพัฒนาระบบที่มีความสามารถในการตอบสนองต่อภัยคุกคามไซเบอร์ โดยมุ่งเน้นการใช้เทคโนโลยีและวิธีการที่ช่วยเสริมสร้างภูมิคุ้มกันให้กับข้อมูลและโครงสร้างพื้นฐานดิจิทัล เพื่อป้องกันและลดความเสี่ยงจากการโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต โดยการจัดการภูมิคุ้มกันดิจิทัลมักใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และการเรียนรู้ของเครื่อง (Machine Learning) ในวิเคราะห์และตรวจจับพฤติกรรมที่อาจเป็นภัยคุกคาม รวมถึงการพัฒนาแบบจำลองที่สามารถคาดการณ์การโจมตีในอนาคตได้อย่างมีประสิทธิภาพ การจัดการภูมิคุ้มกันดิจิทัลนี้ถือเป็นกลยุทธ์ที่สำคัญในการสร้างความมั่นคงและเสริมสร้างความปลอดภัยให้กับองค์กรหรือสถาบันในยุคที่เทคโนโลยีและการสื่อสารมีความซับซ้อนและพัฒนาอย่างรวดเร็ว โดยประกอบด้วย 9 ด้าน ได้แก่ 1) การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection) 2) การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response) 3) การประเมินและจัดการความเสี่ยง (Risk Assessment and Management) 4) การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy) 5) การฝึกอบรมการรับรู้ด้านความปลอดภัย (Security Awareness Training) 6) นโยบายความปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance) 7) ความปลอดภัยของเครือข่าย (Network Security) 8) โซลูชันความปลอดภัยที่ขับเคลื่อนด้วย AI (AI-driven Security Solutions) และ 9) ความปลอดภัยบนคลาวด์ (Cloud Security)

การจัดการองค์กรดิจิทัล (Digital Enterprise Management) คือการบริหารจัดการองค์กรแบบบูรณาการ โดยใช้เทคโนโลยีดิจิทัลและระบบสารสนเทศเพื่อเพิ่มประสิทธิภาพในการดำเนินงาน พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีและนวัตกรรมให้รองรับการเติบโตขององค์กรในยุคดิจิทัล รวมถึงการปรับตัวให้เข้ากับการเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็ว การจัดการองค์กรดิจิทัลประกอบด้วย 6 องค์ประกอบสำคัญ คือ กลยุทธ์ดิจิทัล (Digital Strategy) โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure) การจัดการข้อมูล (Data Management) กระบวนการอัตโนมัติ (Process Automation) ความปลอดภัยทางไซเบอร์ (Cybersecurity) และนวัตกรรมและความคล่องตัว (Innovation and Agility)

สถาบันอุดมศึกษา (Higher Education Institution) คือสถาบันการศึกษาที่ให้การศึกษาระดับสูง ซึ่งรวมถึงมหาวิทยาลัย วิทยาลัย และสถาบันการศึกษาอื่นๆ ที่มุ่งเน้นการให้การศึกษาในระดับปริญญาตรีและสูงกว่า โดยมีเป้าหมายในการพัฒนาความรู้ ทักษะ และคุณสมบัติของนักศึกษาเพื่อเตรียมความพร้อมให้กับนักศึกษาสำหรับการทำงานในตลาดแรงงาน รวมถึงการมีส่วนร่วมในสังคมและการพัฒนาทางเศรษฐกิจและวัฒนธรรม

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยเรื่อง สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา การวิจัยครั้งนี้เป็นการวิจัยแบบผสมผสาน (Mixed-Methodology Research) ประกอบไปด้วยการวิจัยเชิงปริมาณ (Quantitative Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีวัตถุประสงค์ดังนี้ 1) เพื่อวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ 2) เพื่อสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 3) เพื่อพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา และ 4) เพื่อประเมินรูปแบบการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา เพื่อให้สอดคล้องกับงานวิจัย จึงได้แบ่งวิธีการดำเนินการวิจัยออกเป็น 4 ระยะ ดังนี้

ระยะที่ 1 การวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ระยะที่ 2 การสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ระยะที่ 3 การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ระยะที่ 4 การประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผู้วิจัยขอนำเสนอขั้นตอนดำเนินการวิจัย ดังแสดงในตารางที่ 3-1 และนำเสนอรายละเอียดในแต่ละขั้นตอนในหัวข้อต่อไปนี้

ตารางที่ 3-1 ขั้นตอนการดำเนินการวิจัย

ระยะที่ 1 การวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา		
วัตถุประสงค์การวิจัย	**ขั้นตอน/กระบวนการ**	**ผลลัพธ์**
1. วิเคราะห์ปัจจัยที่มีอิทธิพลต่อ	1. ศึกษาค้นคว้าข้อมูล เอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับ	1. ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อ

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. สังเคราะห์เอกสารและงานวิจัยที่เกี่ยวข้องกับ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 3. นำผลการสังเคราะห์ปัจจัยเสนออาจารย์ที่ปรึกษาเพื่อพิจารณาปรับปรุง	สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ระยะที่ 2 การสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

วัตถุประสงค์การวิจัย	**ขั้นตอน/กระบวนการ**	**ผลลัพธ์**
1. สร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. ตรวจสอบยืนยันสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	1. นำผลการสังเคราะห์จากระยะที่ 1 มาสร้างแบบสอบถามเกี่ยวกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. นำแบบสอบถามที่ปรับปรุงเรียบร้อยแล้วไปเก็บข้อมูลกับกลุ่มตัวอย่างจำนวน 500 คน 3. วิเคราะห์ข้อมูลโดยตรวจสอบวิเคราะห์องค์ประกอบเชิงยืนยัน (CFA) สถิติที่ใช้ได้แก่ การวิเคราะห์เส้นทาง (Path Analysis) โดยใช้โปรแกรม LISREL Version 8.72 แบบ Basic Model 4. สร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	1. แบบสอบถามเพื่อนำไปใช้ในการเก็บข้อมูล 2. ผลวิเคราะห์ข้อมูลโดยการวิเคราะห์เชิงยืนยัน 3. แบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

	เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 5. ตรวจสอบยืนยันแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	
ระยะที่ 3 การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา		
วัตถุประสงค์การวิจัย	**ขั้นตอน/กระบวนการ**	**ผลลัพธ์**
1. พัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	1. นำผลในระยะที่ 2 มาเป็นข้อมูลสำหรับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. ศึกษา ทบทวนวิธีการ แนวคิดเกี่ยวข้องกับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 3. ออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 4. ประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาโดยผู้เชียวชาญ	1. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ระยะที่ 4 การประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา		
วัตถุประสงค์การวิจัย	**ขั้นตอน/กระบวนการ**	**ผลลัพธ์**
1. การประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	1. นำผลจากการดำเนินการในระยะที่ 3 ต้นแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา มาเป็นข้อมูลในการสร้างแบบประเมิน 2. สร้างแบบประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 3. ประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาโดยผู้เชี่ยวชาญ 4. วิเคราะห์ข้อมูลจากการประเมินรูปแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	1. ผลการประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 5. ข้อเสนอแนะเชิงนโยบายสำหรับสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.1 การวิจัยระยะที่ 1 การวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

มีขั้นตอนการดำเนินการดังตารางที่ 3-2

ตารางที่ 3-2 ขั้นตอนการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ขั้นตอน/กระบวนการ	ผลลัพธ์
1. ศึกษาค้นคว้าข้อมูล เอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. สังเคราะห์เอกสารและงานวิจัยที่เกี่ยวข้องกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาได้แก่ - โครงสร้างองค์กร - เทคโนโลยีอัจฉริยะ - ระบบภูมิคุ้มกันดิจิทัล - การจัดการองค์กรดิจิทัล - สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ - การจัดการภูมิคุ้มกันดิจิทัล 3. นำผลการสังเคราะห์ปัจจัยเสนออาจารย์ที่ปรึกษาเพื่อพิจารณาปรับปรุง	1. ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

การดำเนินงานตามขั้นตอนการวิจัยในระยะที่ 1 เป็นการสังเคราะห์เอกสารและงานวิจัยเกี่ยวข้องกับกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ได้แก่ โครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัล โดยมีรายละเอียด ดังนี้

3.1.1 วัตถุประสงค์การวิจัย ระยะที่ 1

เพื่อวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.1.2 ตัวแปรที่ใช้ในการวิจัย ระยะที่ 1

ตัวแปรต้น คือ ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตัวแปรตาม คือ ผลการสังเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.1.3 ขั้นตอนวิธีการดำเนินการวิจัย ระยะที่ 1

3.1.3.1 ศึกษาค้นคว้าข้อมูล เอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

3.1.3.1.1 โครงสร้างองค์กร (Organizational Structure)

3.1.3.1.2 เทคโนโลยีอัจฉริยะ (Intelligent Technology)

3.1.3.1.3 การจัดการองค์กรดิจิทัล (Digital Enterprise Management)

3.1.3.1.4 ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity System)

3.1.3.1.5 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture)

3.1.3.1.6 การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)

3.1.3.1.7 สถาบันอุดมศึกษา (Higher Education Institution)

3.1.3.2 สังเคราะห์เอกสาร และงานวิจัยที่เกี่ยวข้องกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

3.1.3.3 สังเคราะห์เอกสารและงานวิจัยที่เกี่ยวข้องกับปัจจัยที่มีอิทธิพลต่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.1.3.4 นำผลการสังเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาเสนอต่ออาจารย์ที่ปรึกษาเพื่อพิจารณาและปรับปรุงตามคำแนะนำ

3.2 การวิจัยระยะที่ 2 การสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

จากการวิจัยในระยะที่ 1 ผู้วิจัยได้ทำการสังเคราะห์เอกสารและงานวิจัยที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรปัญญาประดิษฐ์แล้วเสร็จ หลังจากนั้นได้นำปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาที่ได้จากการ

สังเคราะห์นั้นมาสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาซึ่งมีขั้นตอนการดำเนินการดังตารางที่ 3-3

ตารางที่ 3-3 ขั้นตอนการสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ขั้นตอน/กระบวนการ	ผลลัพธ์
1. นำผลการสังเคราะห์จากระยะที่ 1 มาสร้างแบบสอบถามเกี่ยวกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. นำแบบสอบถามที่ปรับปรุงเรียบร้อยแล้วไปเก็บข้อมูลกับกลุ่มตัวอย่าง จำนวน 500 คน 3. วิเคราะห์ข้อมูลโดยตรวจสอบวิเคราะห์องค์ประกอบเชิงยืนยัน (CFA) สถิติที่ใช้ได้แก่ การวิเคราะห์เส้นทาง (Path Analysis) โดยใช้โปรแกรม LISREL Version 8.72 แบบ Basic Model 4. สร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 5. ตรวจสอบยืนยันแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	1. แบบสอบถามเพื่อนำไปใช้ในการเก็บข้อมูล 2. ผลวิเคราะห์ข้อมูลโดยการวิเคราะห์เชิงยืนยัน 3. แบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

การดำเนินงานตามขั้นตอนการวิจัยในระยะที่ 2 เป็นการนำข้อมูลจากระยะที่ 1 มาสร้างแบบสอบถามเกี่ยวกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา และนำผลที่ได้จากแบบสอบถามมาตรวจสอบโดยการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis) และการสร้างและตรวจสอบยืนยันโมเดลแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา (Structural Equation Model) โดยมีรายละเอียด ดังนี้

3.1.1 วัตถุประสงค์การวิจัย ระยที่ 2

เพื่อสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.1.2 ประชากรและกลุ่มตัวอย่างการวิจัย ระยะที่ 2

ประชากร คือ ผู้บริหารและบุคลากรในสถาบันอุดมศึกษาสังกัดสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) จำนวน 500 คน

กลุ่มตัวอย่าง คือ คือ สำหรับการวิจัยครั้งนี้อ้างอิงเกณฑ์การใช้ขนาดตัวอย่างสำหรับการใช้สถิติวิเคราะห์ปัจจัยองค์ประกอบของ Comrey & Lee อ้างถึงใน (White, 2022) ได้ขนาดกลุ่มตัวอย่างจำนวน 500 ราย

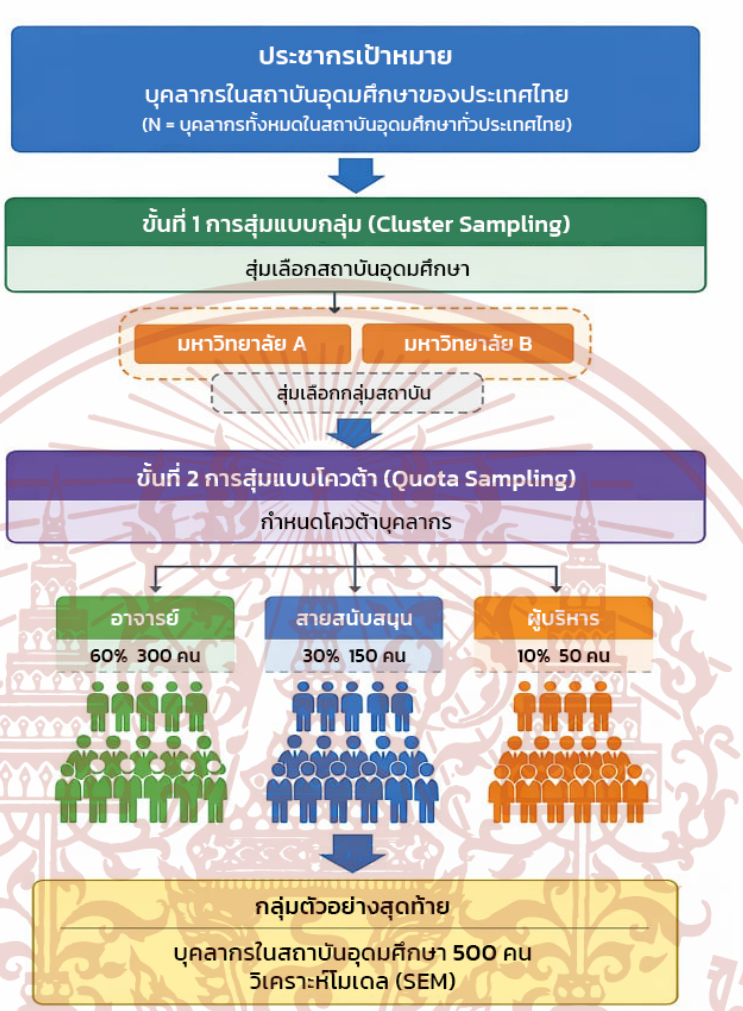
ตารางที่ 3-4 ขนาดกลุ่มตัวอย่างในการวิเคราะห์โมเดลแบบจำลอง

ขนาดตัวอย่าง	ความเหมาะสมของการวิเคราะห์
≤ 50	แย่มาก (Very weak)
100	แย่ (weak)
200	พอใช้ (Adequate)
300	ดี (Good)
500	ดีมาก (Very good)
≥1,000	ดีเยี่ยม (Excellent)

การสุ่มกลุ่มตัวอย่างในการศึกษาครั้งนี้ใช้วิธีการสุ่มแบบหลายขั้นตอน มีรายละเอียดดังต่อไปนี้ แสดงดังภาพที่ 3-1

ขั้นที่ 1 ใช้วิธีการสุ่มแบบกลุ่ม (Cluster Sampling) โดยแบ่งประชากรตามโครงสร้างการแบ่งส่วนราชการ/การจัดกลุ่มของสถาบันอุดมศึกษา ที่กำหนดไว้ จากนั้นสุ่มเลือกสถาบันอุดมศึกษาจากแต่ละกลุ่มเพื่อให้ได้สถาบันที่เป็นตัวแทนสำหรับการเก็บรวบรวมข้อมูลในขั้นตอนต่อไป

ขั้นที่ 2 ใช้วิธีการสุ่มแบบโควต้า (Quota Sampling) โดยแบ่งตามจำนวนสัดส่วนที่เท่าๆ กัน เพื่อคำนึงถึงการกระจายตัวของข้อมูลอย่างเหมาะสม



ภาพที่ 3-1 วิธีการสุ่มกลุ่มตัวอย่าง

3.1.3 ตัวแปรที่ใช้ในการวิจัย ระยะที่ 2

ตัวแปรต้น คือ แบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตัวแปรตาม คือ ผลการตรวจสอบยืนยันแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาขั้นตอนวีการดำเนินการวิจัย ระยะที่ 2

3.1.3.1 นำผลการสังเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์จากระยะที่ 1 มาสร้างแบบสอบถามเกี่ยวกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

3.1.3.2 นำแบบสอบถามฉบับร่างไปให้ผู้เชี่ยวชาญที่มีความรู้และประสบการณ์ทางด้านจะทำการศึกษาวิจัยพิจารณา จำนวน 9 ท่าน เพื่อหาคุณภาพเครื่องมือ ด้วยการตรวจสอบดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของการวิจัย (Index of Item-Objective Congruence: IOC) โดยได้กำหนดเกณฑ์ในการประเมิน ดังนี้

+1 หมายถึง ข้อคำถามนั้นมีความสอดคล้องกับวัตถุประสงค์ของการวิจัย

0 หมายถึง ไม่แน่ใจว่าข้อคำถามนั้นมีความสอดคล้องกับวัตถุประสงค์ของการวิจัย

-1 หมายถึง ข้อคำถามนั้นไม่มีความสอดคล้องกับวัตถุประสงค์ของการวิจัย

โดยมีเกณฑ์การพิจารณาคัดเลือกความสอดคล้องของข้อคำถามกับวัตถุประสงค์ของการวิจัยดังนี้

1. ถ้าค่า IOC > 0.50 เลือกใช้ ข้อคำถามมีความสอดคล้องกับวัตถุประสงค์ของการวิจัย
2. ถ้าค่า IOC < 0.50 ตัดทิ้ง ข้อคำถามไม่สอดคล้องกับวัตถุประสงค์ของการวิจัย

ผลการตรวจสอบดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของการวิจัย (Index of Item-Objective Congruence: IOC) สำหรับงานวิจัยนี้มีค่าอยู่ระหว่าง 0.80 – 1.00

3.1.3.3 นำแบบสอบถามฉบับที่ผ่านการประเมินของผู้เชี่ยวชาญแล้วนำไปทดลองใช้ (Pilot study) กับกลุ่มประชากรที่มีลักษณะคล้ายคลึงกับประชากรที่ต้องการศึกษา จำนวน 30 คน เพื่อหาค่าอำนาจจำแนก (Discrimination) โดยค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) และค่าสัมประสิทธิ์สหสัมพันธ์ (Correlation) และหาค่าความเชื่อมั่น (Reliability) โดยวิเคราะห์ค่าครอนบัคแอลฟ่า (Cronbach Alpha)

ตารางที่ 3-5 ผลการตรวจสอบอำนาจจำแนกและความเชื่อมั่นของแบบสอบถาม (Pilot Study)

ลำดับ	รายการ	Cronbach's Alpha	สรุปผล
ด้านโครงสร้างองค์กร (Organizational Structure)			
1	สถาปัตยกรรมธุรกิจ (Business Architecture)	.810	เหมาะสม
2	สถาปัตยกรรมข้อมูล (Data Architecture)	.790	ผ่านเกณฑ์
3	สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture)	.885	เหมาะสม
4	สถาปัตยกรรมเทคโนโลยี (Technology Architecture)	.758	ผ่านเกณฑ์
5	สถาปัตยกรรมด้านความมั่งคงปลอดภัย (Security Architecture)	.854	เหมาะสม
6	สถาปัตยกรรมการบูรณาการ (Integration Architecture)	.834	เหมาะสม

ลำดับ	รายการ	Cronbach's Alpha	สรุปผล
7	สถาปัตยกรรมการกำกับดูแล (Governance Architecture)	.888	เหมาะสม
ด้านเทคโนโลยีอัจฉริยะ (Intelligent Technology)			
1	การเรียนรู้ของเครื่อง (Machine Learning)	.897	เหมาะสม
2	การเรียนรู้เชิงลึก (Deep Learning)	.848	เหมาะสม
3	การประมวลผลภาษาธรรมชาติ (Natural Language Processing - NLP)	.872	เหมาะสม
4	ความรู้เชิงพฤติกรรม (Behavioral AI)	.748	ผ่านเกณฑ์
ด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity)			
1	การมองเห็นและเฝ้าระวัง (Observability & Visibility)	.881	เหมาะสม
2	การตรวจจับภัยคุกคาม (Threat Detection)	.930	เหมาะสมมาก
3	การสืบสวนและวิเคราะห์ (Investigation & Analysis)	.883	เหมาะสม
4	การตอบสนองและการป้องกันเชิงรุก (Response & Proactive Defense)	.928	เหมาะสมมาก
5	ความทนทานและการฟื้นฟู (Resilience & Recovery)	.823	เหมาะสม
6	ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ (Collaboration & Cybersecurity Awareness)	.910	เหมาะสมมาก
ด้านการจัดการองค์กรดิจิทัล (Digital Enterprise Management)			
1	กลยุทธ์ดิจิทัล (Digital Strategy)	.881	เหมาะสม
2	โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure)	.848	เหมาะสม
3	การจัดการข้อมูล (Data Management)	.930	เหมาะสมมาก
4	กระบวนการอัตโนมัติ (Process Automation)	.857	เหมาะสม
5	ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)	.962	เหมาะสมมาก
ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (Artificial Intelligence Enterprise Architecture)			

ลำดับ	รายการ	Cronbach's Alpha	สรุปผล
1	การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ (EA–AI Integration)	.908	เหมาะสมมาก
2	กรอบการทำงานเชิงสถาปัตยกรรม (Architectural Framework)	.885	เหมาะสม
3	การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ (AI-driven Information System Design & Development)	.897	เหมาะสม
4	การปรับตัวต่อการเปลี่ยนแปลง (Adaptability & Agility)	.793	ผ่านเกณฑ์
5	การรับมือภัยคุกคามและความเสี่ยง (Threat & Risk Responsiveness)	.928	เหมาะสมมาก
6	จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ (AI Ethics and Responsibility)	.872	เหมาะสม
ด้านการจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)			
1	การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection)	.905	เหมาะสมมาก
2	การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response)	.870	เหมาะสม
3	การประเมินและจัดการความเสี่ยง (Risk Assessment and Management)	.796	ผ่านเกณฑ์
4	การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy)	.908	เหมาะสมมาก
5	การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย (Security Awareness Training)	.748	ผ่านเกณฑ์
6	นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance)	.897	เหมาะสม

3.1.3.4 ปรับปรุงแก้ไขแบบสอบถามตามผลการวิเคราะห์ค่าอำนาจจำแนกและค่าความเชื่อมั่นของแบบสอบถามก่อนนำไปใช้จริง

3.1.3.5 นำแบบสอบถามที่ปรับปรุงเรียบร้อยแล้วไปเก็บข้อมูลกับกลุ่มตัวอย่างจำนวน 500 ราย

ตารางที่ 3-6 จำนวนกลุ่มตัวอย่างที่ได้จากการเก็บข้อมูลเชิงปริมาณ

กลุ่มตัวอย่าง	ร้อยละ	จำนวนตัวอย่าง (คน)
แบ่งตามประเภทสถาบันอุดมศึกษา		
มหาวิทยาลัยภาครัฐ	40%	200
มหาวิทยาลัยราชภัฏ	35%	175
มหาวิทยาลัยเอกชน	25%	125
รวม	**100%**	**500**
แบ่งตามประเภทบุคลากรภายในแต่ละสถาบัน		
มหาวิทยาลัยภาครัฐ (200 คน)		
อาจารย์	60%	120
บุคลากรสายสนับสนุน	30%	60
ผู้บริหาร	10%	20
มหาวิทยาลัยราชภัฏ (175 คน)		
อาจารย์	65%	114
บุคลากรสายสนับสนุน	25%	44
ผู้บริหาร	10%	17
มหาวิทยาลัยเอกชน (125 คน)		
อาจารย์	55%	69
บุคลากรสายสนับสนุน	35%	44
ผู้บริหาร	10%	12

3.1.3.6 นำข้อมูลที่ได้จากแบบสอบถามมาตรวจสอบโดยการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis)

3.1.3.7 นำข้อมูลที่ผ่านการวิเคราะห์องค์ประกอบเชิงยืนยันมาสร้างโมเดลแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ แบ่งขั้นตอนการดำเนินงานออกเป็น 5 ขั้นตอน ดังนี้

3.2.4.7.1 การกำหนดข้อมูลเฉพาะของโมเดล

3.2.4.7.2 การระบุค่าความเป็นไปได้ค่าเดียวของโมเดล

3.2.4.7.3 การประมาณค่าพารามิเตอร์ของโมเดล

3.2.4.7.4 การตรวจสอบความสอดคล้องของโมเดล

3.2.4.7.5 การปรับโมเดล

3.1.3.8 ตรวจสอบยืนยันโมเดลแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ โดยใช้เกณฑ์การประเมินความสอดคล้องของโมเดลแบบจำลอง ดังแสดงในตารางที่ 3-5

3.1.4 เครื่องมือที่ใช้ในการวิจัย ระยะที่ 2

3.2.5.1 แบบสอบถามเกี่ยวกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ซึ่งเป็นแบบมาตรส่วนประเมินค่า (Rating Scale) ตามวิธีของลิเคิร์ท (Likert Scale) โดยมีเกณฑ์ในการให้ค่าของน้ำหนักการประเมินเป็น 5 ระดับ ดังนี้

5 คะแนน หมายถึง มีความเหมาะสมมากที่สุด

4 คะแนน หมายถึง มีความเหมาะสมมาก

3 คะแนน หมายถึง มีความเหมาะสมปานกลาง

2 คะแนน หมายถึง มีความเหมาะสมน้อย

1 คะแนน หมายถึง มีความเหมาะสมน้อยที่สุด

การใช้สถิติเชิงพรรณนา คือ ค่าเฉลี่ยสูงสุดและต่ำสุด ค่าร้อยละ และส่วนเบี่ยงเบนมาตรฐาน สำหรับการแปลผลระดับของความคิดเห็นพิจารณาจากค่าเฉลี่ยโดยใช้เกณฑ์ของเบสท์ (Louis Cohen, 2002) ซึ่งในการวิจัยครั้งนี้ใช้การแปรผล 3 ระดับ มีรายละเอียดดังนี้

ค่าเฉลี่ย 4.34 - 6.00 หมายถึง ระดับสูง

ค่าเฉลี่ย 2.67 - 4.33 หมายถึง ระดับปานกลาง

ค่าเฉลี่ย 1.00 - 2.66 หมายถึง ระดับต่ำ

การใช้สถิติเชิงอนุมาน คือ การวิเคราะห์สหสัมพันธ์ (Correlation Analysis) สำหรับระดับหรือขนาดของความสัมพันธ์ จะใช้ตัวเลขของค่าสัมประสิทธิ์สหสัมพันธ์ หากค่าสัมประสิทธิ์สหสัมพันธ์มีค่าเข้าใกล้ -1 หรือ 1 แสดงถึงการมีความสัมพันธ์กันในระดับสูง แต่หากมีค่าเข้าใกล้ 0 แสดงถึงการมีความสัมพันธ์กันในระดับน้อยหรือไม่มีเลย สำหรับการพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ ในการวิจัยครั้งนี้ใช้เกณฑ์ดังนี้ (Golby & Wood, 2016)

ค่า *r* 0.90 - 1.00 หมายถึง ระดับความสัมพันธ์กันสูงมาก

ค่า *r* 0.70 - 0.90 หมายถึง ระดับความสัมพันธ์กันสูง

ค่า *r* 0.50 - 0.70 หมายถึง ระดับความสัมพันธ์ปานกลาง

ค่า *r* 0.30 - 0.50 หมายถึง ระดับความสัมพันธ์กันต่ำ

ค่า *r* 0.00 - 0.30 หมายถึง ระดับความสัมพันธ์กันต่ำมาก

เกณฑ์การแปลความหมายเพื่อจัดระดับช่วงคะแนนเฉลี่ยค่าความสำคัญของปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เป็นช่วงดังต่อไปนี้

คะแนนเฉลี่ย 4.50-5.00 หมายถึง มีความสำคัญมากที่สุด

คะแนนเฉลี่ย 3.50-4.49 หมายถึง มีความสำคัญมาก

คะแนนเฉลี่ย 2.50-3.49 หมายถึง มีความสำคัญปานกลาง

คะแนนเฉลี่ย 1.50-2.49 หมายถึง มีความสำคัญน้อย

คะแนนเฉลี่ย 1.00-1.49 หมายถึง มีความสำคัญน้อยที่สุด

3.1.5 สถิติที่ใช้ในการวิจัย ระยะที่ 2

3.2.6.1 ร้อยละ

3.2.6.2 ค่าเฉลี่ยเลขคณิต ($\bar{x}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.)

3.2.6.3 วิเคราะห์ตัวแปรเชิงพหุด้วยโปรแกรมสำเร็จรูป

3.2.6.4 เกณ์การประเมินโมเดลแบบจำลองสมการโครงสร้าง (SEM)

ตารางที่ 3-7 เกณฑ์การประเมินความสอดคล้องของโมเดลแบบจำลองสมการโครงสร้าง

ดัชนีความสอดคล้อง	เกณฑ์การยอมรับ
Sig.	> 0.05
CMIN/df.	< 2.0
Goodness of Fit Index: GFI	> 0.90
Adjusted Goodness of Fit: AGFI	> 0.80
Normed Fit Index: NFI	> 0.90
Incremental Fit Index: IFI	> 0.90
Comparative Fit Index: CFI	> 0.90
Root of Mean Square Residual: RMR	< 0.05
Root Mean Square error of Approximation: RMSEA	< 0.05

จากตารางที่ 3-7 แสดงเกณฑ์การประเมินความสอดคล้องของโมเดลแบบจำลองสมการโครงสร้างระหว่างตัวแบบที่ได้พัฒนาขึ้นกับข้อมูลเชิงประจักษ์ที่นิยมใช้กันในการพิจารณาความกลมกลืนสอดคล้องระหว่างตัวแบบเชิงทฤษฎีกับข้อมูลเชิงประจักษ์

1. ค่าไค-สแควร์สัมพัทธ์ (Relative Chi-Square) เป็นอัตราส่วนระหว่างจำนวนองศาอิสระกับค่าสถิติไค-สแควร์ ควรมีค่าน้อยกว่า < 2.0 แสดงว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ในระดับดี

2. ดัชนีวัดระดับความสอดคล้อง (Goodness of Fit Index: GFI) เป็นค่าที่แสดงสัดส่วนของค่าความแปรปรวนร่วมของข้อมูลเชิงประจักษ์ที่สามารถอธิบายได้โดยค่าความแปรปรวนร่วมของโมเดล ควรมีค่ามากกว่า > 0.90 แสดงว่า โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์

3. ดัชนีวัดความสอดคล้องที่ปรับแก้แล้ว (Adjusted Goodness of Fit: AGFI) เป็นค่าที่แสดงถึงปริมาณความแปรปรวนและความแปรปรวนร่วมที่อธิบายได้ด้วยโมเดลที่ปรับแก้ด้วยองศาอิสระ ควรมีค่ามากกว่า > 0.80 แสดงว่า โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์

4. ดัชนีความกลมกลืนเปรียบเทียบกับรูปแบบอิสระ (Normed Fit Index: NFI) เป็นค่าที่แสดงให้เห็นว่าโมเดลที่นำมาตรวจสอบดีกว่าโมเดลที่ตัวแปรไม่สัมพันธ์กันเลย ซึ่งควรมีค่าอยู่ระหว่าง 0 ถึง 1โดยค่าดัชนี NFI ที่ยอมรับได้ควรมีค่ามากกว่า > 0.90 แสดงว่า โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์

5. ดัชนีความกลมกลืนเชิงเปรียบเทียบกับรูปแบบฐาน (Incremental Fit Index: IFI) เป็นค่าดัชนีที่ใช้เปรียบเทียบโมเดลพื้นฐานกับโมเดลเชิงทฤษฎีที่ตัวแปรทุกตัวไม่มีความสัมพันธ์กัน ควรมีค่ามากกว่า > 0.90 แสดงว่า โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์

6. ดัชนีวัดความสอดคล้องกลมกลืนสัมพัทธ์ (Comparative Fit Index: CFI) เป็นค่าดัชนีที่ใช้เปรียบเทียบความสอดคล้องระหว่างโมเดลเชิงสมมติฐานกับข้อมูลเชิงประจักษ์ ควรมีค่ามากกว่า > 0.90แสดงว่า โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ในระดับดี

7. ดัชนีรากของกำลังสองเฉลี่ยของเศษเหลือ (Root of Mean Square Residual: RMR) เป็นค่าดัชนีที่ใช้เปรียบเทียบระดับความกลมกลืนของโมเดลกับข้อมูลเชิงประจักษ์ ควรมีค่าน้อยกว่า < 0.05 หรือมีค่าเข้าใกล้ศูนย์ แสดงว่า โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์

8. ดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนกำลังสองของการประมาณค่า (Root Mean Square error of Approximation: RMSEA) เป็นค่าดัชนีที่แสดงถึงค่าเฉลี่ยความแตกต่าง (ความไม่กลมกลืน) ควรมีค่าน้อยกว่า < 0.05 หรือมีค่าเข้าใกล้ศูนย์ แสดงว่าโมเดลมีความสอดคล้องหรือกลมกลืนกับข้อมูลเชิงประจักษ์ในระดับดี

3.3 การวิจัยระยะที่ 3 การพัฒนาการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาตามแบบจำลองสมการโครงสร้าง

จากการวิจัยในระยะที่ 2 ผู้วิจัยได้ทำการตรวจสอบโดยการวิเคราะห์องค์ประกอบเชิงยืนยันของปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการสร้างและตรวจสอบยืนยันแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา หลังจากนั้นนำผลที่ได้มาพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา ซึ่งมีขั้นตอนการดำเนินการดังตารางที่ 3-8

ตารางที่ 3-8 ขั้นตอนการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ขั้นตอน/กระบวนการ	ผลลัพธ์
1. นำผลในระยะที่ 2 มาเป็นข้อมูลสำรับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. ศึกษา วิเคราะห์และทบทวนวิธีการ แนวคิด จากเอกสารและงานวิจัยที่เกี่ยวข้องกับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 3. พัฒนาร่างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 4. สนทนากลุ่ม (Focus Group Discussion) เพื่อวิพากษ์และเสนอแนะสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	1. องค์ประกอบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

การดำเนินงานตามขั้นตอนการวิจัยในระยะที่ 3 เป็นการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาตามแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยมีรายละเอียด ดังนี้

3.1.6 วัตถุประสงค์การวิจัย ระยะที่ 3

เพื่อพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.1.7 ประชาชนและกลุ่มตัวอย่างการวิจัย ระยะที่ 2

ประชากร คือ ผู้เชี่ยวชาญที่เป็นบุคลากรในสถาบันอุดมศึกษา

กลุ่มตัวอย่าง คือ ผู้เชี่ยวชาญด้านสถาปัตยกรรมองค์กร ผู้เชี่ยวชาญด้านปัญญาประดิษฐ์ ผู้เชี่ยวชาญด้านระบบภูมิคุ้มกันดิจิทัล ผู้เชี่ยวชาญด้านการจัดการองค์กรดิจิทัล และผู้เชี่ยวชาญด้าน

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ จำนวน 11 คน โดยใช้วิธีการเลือกกลุ่มตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling) ประกอบด้วย

กลุ่มที่ 1 ผู้เชี่ยวชาญด้านสถาปัตยกรรมองค์กร เป็นผู้บริหารระดับสูง มีประสบการณ์ไม่น้อยกว่า 5 ปี สังกัดสถาบันอุดมศึกษา

กลุ่มที่ 2 ผู้เชี่ยวชาญด้านปัญญาประดิษฐ์ มีประสบการณ์ไม่น้อยกว่า 5 ปี สังกัดสถาบันอุดมศึกษา

กลุ่มที่ 3 ผู้เชี่ยวชาญด้านการจัดการภูมิคุ้มกันดิจิทัล มีประสบการณ์ไม่น้อยกว่า 5 ปี สังกัดสถาบันอุดมศึกษา

กลุ่มที่ 4 ผู้เชียวชาญด้านการจัดการองค์กรดิจิทัล มีประสบการณ์ไม่น้อยกว่า 5 ปี สังกัดสถาบันอุดมศึกษา

กลุ่มที่ 5 ผู้เชียวชาญด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีประสบการณ์ไม่น้อยกว่า 5 ปี สังกัดสถาบันอุดมศึกษา

3.1.8 ตัวแปรที่ใช้ในการวิจัย ระยะที่ 3

ตัวแปรต้น คือ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตัวแปรตาม คือ ผลการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษาตามแบบจำลองสมการโครงสร้างการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา

3.1.9 ขั้นตอนวิธีการดำเนินการวิจัย ระยะที่ 3

3.3.4.1 นำผลจากการดำเนินการในระยะที่ 2 มาเป็นข้อมูลสำหรับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา

3.3.4.2 ศึกษา วิเคราะห์และทบทวนวิธีการ แนวคิด จากเอกสารและงานวิจัยที่เกี่ยวข้องกับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.3.4.2.1 กรอบและแนวคิดการพัฒนาสถาปัตยกรรมองค์กร ประกอบด้วย 3 แบบดังนี้

1. TOGAF Framework
2. The Zachman Framework
3. Federal Enterprise Framework

3.3.4.3 พัฒนาร่างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.3.4.4 การประชุมสนทนากลุ่ม (Focus Group Discussion) เพื่อวิพากษ์และเสนอแนะสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ในรูปแบบออนไลน์ โดยผู้เชี่ยวชาญเข้าร่วมประชุมพิจารณาประเมิน อภิปรายและแสดงความคิดเห็นเกี่ยวกับร่างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา รวมถึงให้ข้อเสนอแนะและความคิดเห็นเพิ่มเติม เพื่อการปรับปรุงร่างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาให้ครบถ้วน ถูกต้องและครอบคลุมในทุกประเด็น

3.1.10 เครื่องมือที่ใช้ในการวิจัย ระยะที่ 3

3.3.5.1 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.4 การวิจัยระยะที่ 4 การประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

จากการวิจัยในระยะที่ 3 ผู้วิจัยได้ทำการพัฒนาร่างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาแล้วเสร็จ หลังจากนั้นนำร่างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาดังกล่าวมาประเมินการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาโดยผู้เชี่ยวชาญ ซึ่งแบ่งออกเป็น 3 กลุ่ม ซึ่งมีขั้นตอนการดำเนินการดังตารางที่ 3-9

ตารางที่ 3-9 ขั้นตอนการประเมินรสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ขั้นตอน/กระบวนการ	ผลลัพธ์
1. นำผลจากการดำเนินการในระยะที่ 3 ต้นแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 2. สร้างแบบประเมินรูปแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา 3. ประเมินรูปแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาโดยผู้เชี่ยวชาญ 4. วิเคราะห์ข้อมูลจากการประเมินรูปแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา	ผลการประเมินรูปแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

การดำเนินงานตามขั้นตอนการวิจัยในระยะที่ 4 เป็นการประเมินรูปแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยมีรายละเอียดดังนี้

3.4.1 วัตถุประสงค์การวิจัย ระยะที่ 4

เพื่อการประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.4.2 ประชากรและกลุ่มตัวอย่างการวิจัย ระยะที่ 4

ประชากร คือ ผู้เชี่ยวชาญที่อยู่ในสถาบันอุดมศึกษา

กลุ่มตัวอย่าง คือ ผู้เชี่ยวชาญด้านโครงสร้างองค์กร ด้านเทคโนโลยีอัจฉริยะ ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัล จำนวน 9 คน โดยใช้วิธีการเลือกกลุ่มตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling) ประกอบด้วย

กลุ่มที่ 1 ผู้เชี่ยวชาญด้านโครงสร้างองค์กร ด้านเทคโนโลยีอัจฉริยะ ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัล มีประสบการณ์ไม่น้อยกว่า 5 ปี ที่อยู่ในสถาบันอุดมศึกษา

3.4.3 ตัวแปรที่ใช้ในการวิจัย ระยะที่ 4

ตัวแปรต้น คือ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตัวแปรตาม คือ ผลการประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.4.4 ขั้นตอนวิธีการดำเนินการวิจัย ระยะที่ 4

3.4.4.1 นำผลจากการดำเนินการในระยะที่ 3 ร่างต้นแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษามาเป็นข้อมูลในการดำเนินการ

3.4.4.2 สร้างแบบประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.4.4.3 ประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยผู้เชี่ยวชาญ

3.4.4.4 สรุปผลข้อมูลที่ได้รับจากการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.4.5 เครื่องมือที่ใช้ในการวิจัย ระยะที่ 4

3.4.5.1 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

3.4.5.2 แบบประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ซึ่งเป็นแบบมาตรส่วนประเมินค่า (Rating Scale) ตามวิธีของลิเคิร์ท (Likert Scale) โดยมีเกณฑ์ในการให้ค่าของน้ำหนักของการประเมินเป็น 5 ระดับดังนี้ (ละเอียด และ กันฑิมาลย์, 2562)

5 คะแนน หมายถึง มีความเหมาะสมอยู่ในระดับมากที่สุด

4 คะแนน หมายถึง มีความเหมาะสมอยู่ในระดับมาก

3 คะแนน หมายถึง มีความเหมาะสมอยู่ในระดับปานกลาง

2 คะแนน หมายถึง มีความเหมาะสมอยู่ในระดับน้อย

1 คะแนน หมายถึง มีความเหมาะสมอยู่ในระดับน้อยที่สุด

เกณฑ์การแปลความหมายเพื่อจัดระดับช่วงคะแนนเฉลี่ยค่าของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา เป็นช่วงดังต่อไปนี้

คะแนนเฉลี่ย 4.50-5.00 หมายถึง มีความเหมาะสมอยู่ในระดับมากที่สุด

คะแนนเฉลี่ย 3.50-4.49 หมายถึง มีความเหมาะสมอยู่ในระดับมาก

คะแนนเฉลี่ย 2.50-3.49 หมายถึง มีความเหมาะสมอยู่ในระดับปานกลาง

คะแนนเฉลี่ย 1.50-2.49 หมายถึง มีความเหมาะสมอยู่ในระดับน้อย

คะแนนเฉลี่ย 1.00-1.49 หมายถึง มีความเหมาะสมอยู่ในระดับน้อยที่สุด

3.4.6 สถิติที่ใช้ในการวิจัย ระยะที่ 4

3.4.6.1 ค่าเฉลี่ยเลขคณิต ($\bar{x}$)

3.4.6.2 ส่วนเบี่ยงเบนมาตรฐาน (S.D.)

บทที่ 4
ผลการสร้างแบบจำลองสมการโครงสร้าง

การวิจัยเรื่อง สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยใช้ระเบียบวิธีวิจัยแบบผสมผสาน (Mixed-Methodology Research) ประกอบไปด้วย การวิจัยเชิงปริมาณ (Quantitative Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) จากการเก็บข้อมูลจากกลุ่มตัวอย่าง 500 คน นำมาวิเคราะห์ข้อมูลโดยใช้สถิติเชิงบรรยาย (Descriptive Statistics) การแจกแจงความถี่ของข้อมูล ร้อยละ ค่าเฉลี่ยเลขคณิต ค่าเบี่ยงเบนมาตรฐาน โดยใช้สถิติการวิเคราะห์ได้แก่ การวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis) และการวิเคราะห์สมการเชิงโครงสร้าง (System Equation Model: SEM) ตรวจสอบความสอดคล้องของโมเดลกับข้อมูลเชิงประจักษ์ (Assessment of Model Fit) โดยเกณฑ์และดัชนีการตรวจสอบความสอดคล้องกลมกลืนของโมเดลกับข้อมูลเชิงประจักษ์ และใช้โปรแกรมคอมพิวเตอร์สำเร็จรูปทางสถิติในการประมวลผลข้อมูล ผู้วิจัยขอนำเสนอผลงานวิจัยตามกระบวนการวิจัย โดยแบ่งออกเป็น 4 ระยะ ตามวัตถุประสงค์ของการวิจัย รายละเอียดดังนี้

4.1 ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

4.2 ผลการสร้างแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

4.3 ผลการตรวจสอบยืนยันแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สามารถสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

4.4 ผลการประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาอยู่ในระดับใด

4.1 ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

4.1.1 ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ส่วนนี้เป็นการแสดงผลการวิเคราะห์ข้อมูลทั่วไป ได้แก่ เพศ สถานภาพ ตำแหน่งวิชาการ สถาบันอุดมศึกษาที่สังกัด และภูมิภาค สรุปผลการวิเคราะห์ได้ดังตารางที่ 4-1 ดังนี้

ตารางที่ 4-1 แสดงจำนวนและร้อยละข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม		จำนวน	ร้อยละ
เพศ	ชาย	230	46.00
	หญิง	270	54.00
	รวม	500	100
วุฒิการศึกษา	ต่ำกว่าปริญญาตรี	-	-
	ปริญญาตรี	120	24.00
	ปริญญาโท	230	46.00
	ปริญญาเอก	150	30.00
	รวม	500	100
สถานภาพ	ผู้บริหาร	50	10.00
	อาจารย์	300	60.00
	บุคลากรสายสนับสนุน	150	30.00
	รวม	500	100
สถาบันอุดมศึกษาที่สังกัด	มหาวิทยาลัยภาครัฐ	200	40.00
	มหาวิทยาลัยราชภัฏ	175	35.00
	มหาวิทยาลัยเอกชน	125	25.00
	รวม	500	100

จากตารางที่ 4-1 ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถามจำนวน 500 กลุ่มตัวอย่างในด้านเพศ ส่วนมากเป็นเพศหญิง จำนวน 270 คน คิดเป็นร้อยละ 54.00 และเพศชาย จำนวน 230 คน คิดเป็นร้อยละ 46.00 แสดงให้เห็นว่ากลุ่มตัวอย่างมีสัดส่วนเพศหญิงมากกว่าเพศชาย ส่วนใหญ่มีวุฒิการศึกษาระดับปริญญาโท จำนวน 230 คน คิดเป็นร้อยละ 46.00 รองลงมาคือระดับปริญญาเอก จำนวน 150 คน คิดเป็นร้อยละ 30.00 และระดับปริญญาตรี จำนวน 120 คน คิดเป็นร้อยละ 24.00 ทั้งนี้ไม่พบผู้ตอบแบบสอบถามที่มีวุฒการศึกษาต่ำกว่าปริญญาตรี แสดงให้เห็นว่ากลุ่มตัวอย่างมีระดับการศึกษาค่อนข้างสูง ซึ่งเหมาะสมกับบริบทของบุคลากรในสถาบันอุดมศึกษา เมื่อพิจารณาสถานภาพของผู้ตอบแบบสอบถาม พบว่า ส่วนใหญ่เป็นอาจารย์ จำนวน 300 คน คิดเป็นร้อยละ 60.00 รองลงมาคือ บุคลากรสายสนับสนุน จำนวน 150 คน คิดเป็นร้อยละ 30.00 และ ผู้บริหาร จำนวน 50 คน คิดเป็นร้อยละ 10.00 แสดงให้เห็นว่ากลุ่มตัวอย่างครอบคลุมบุคลากรหลักในสถาบันอุดมศึกษาอย่างครบถ้วน ผู้ตอบแบบสอบถามส่วนใหญ่สังกัด

มหาวิทยาลัยภาครัฐ จำนวน 200 คน คิดเป็นร้อยละ 40.00 รองลงมาคือ มหาวิทยาลัยราชภัฏ จำนวน 175 คน คิดเป็นร้อยละ 35.00 และ มหาวิทยาลัยเอกชน จำนวน 125 คน คิดเป็นร้อยละ 25.00 แสดงให้เห็นว่ากลุ่มตัวอย่างมีความหลากหลายตามประเภทของสถาบันอุดมศึกษา ซึ่งช่วยเพิ่มความครอบคลุมและความน่าเชื่อถือของผลการวิจัย

4.1.2 ผลการศึกษาปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล

ผลการศึกษาปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาด้วยเทคนิคการวิเคราะห์เนื้อหา (Content Analysis) และการสัมภาษณ์เชิงลึก (In-depth Interviewing) สามารถจำแนกได้เป็น 6 ปัจจัย ได้แก่ ด้านโครงสร้างองค์กร (Organizational Structure) ด้านเทคโนโลยีอัจฉริยะ (Intelligent Technology) ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และด้านการจัดการภูมิคุ้มกันดิจิทัล รวมทั้งสิ้น 156 ข้อ ดังนี้

4.1.2.1 ด้านโครงสร้างองค์กร (Organizational Structure) ประกอบด้วย

1. กำหนดวิสัยทัศน์และกลยุทธ์ด้านปัญญาประดิษฐ์ที่สอดคล้องกับพันธกิจขององค์กร
2. บูรณาการการใช้ปัญญาประดิษฐ์เข้ากับกระบวนการหลักของมหาวิทยาลัย
3. ประเมินความพร้อมและศักยภาพของหน่วยงานในการใช้เทคโนโลยีปัญญาประดิษฐ์อย่างต่อเนื่อง
4. ผู้บริหารระดับสูงสนับสนุนและส่งเสริมการใช้เทคโนโลยีปัญญาประดิษฐ์เพื่อพัฒนาองค์กร
5. มีกลยุทธ์ข้อมูลที่สนับสนุนการใช้งานปัญญาประดิษฐ์อย่างชัดเจน
6. มีมาตรการควบคุมคุณภาพและความมั่นคงปลอดภัยของข้อมูลอย่างเป็นระบบ
7. โครงสร้างข้อมูลรองรับการจัดเก็บและประมวลผล Big Data และข้อมูลแบบ Unstructured
8. มีระบบติดป้ายกำกับและจัดการข้อมูลเพื่อสนับสนุนการเรียนรู้ของโมเดลปัญญาประดิษฐ์
9. มีการพัฒนาแอปพลิเคชันหรือระบบสารสนเทศที่เชื่อมโยงกับปัญญาประดิษฐ์
10. ระบบแอปพลิเคชันได้รับการออกแบบให้สามารถปรับขนาดและเชื่อมต่อได้ง่าย
11. มีมาตรฐานกลางในการพัฒนาและบูรณาการแอปพลิเคชัน
12. มีการปรับปรุงระบบงานอย่างต่อเนื่องเพื่อรองรับเทคโนโลยีปัญญาประดิษฐ์ใหม่ๆ
13. มีโครงสร้างพื้นฐานด้านเทคโนโลยีที่รองรับการประมวลผลของปัญญาประดิษฐ์

14. ใช้แพลตฟอร์มคลาวด์ในการพัฒนาปัญญาประดิษฐ์
15. มีแผนการบำรุงรักษาและอัปเดตเทคโนโลยีอย่างต่อเนื่อง
16. มีการนำเทคโนโลยี Edge AI หรือระบบประมวลผลแบบกระจายมาใช้เพื่อเพิ่มประสิทธิภาพ
17. มีกลยุทธ์และนโยบายความปลอดภัยทางไซเบอร์ที่ชัดเจน
18. มีการประเมินและป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์
19. มีการเข้ารหัสและจำกัดสิทธิ์การเข้าถึงข้อมูลอย่างเหมาะสม
20. มีแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลและระบบปัญญาประดิษฐ์
21. มีสถาปัตยกรรมเชื่อมต่อโมเดลปัญญาประดิษฐ์กับระบบหลักขององค์กร
22. มีมาตรฐานหรือ API กลางสำหรับการแลกเปลี่ยนข้อมูลระหว่างระบบ
23. มีการตรวจสอบและทดสอบการเชื่อมต่อระหว่างระบบอย่างสม่ำเสมอ
24. ระบบบูรณาการมีความยืดหยุ่นรองรับการเปลี่ยนแปลงของเทคโนโลยี
25. มีกรอบการกำกับดูแล (Governance Framework) ด้านปัญญาประดิษฐ์ที่ชัดเจน
26. มีการติดตามและประเมินผลการใช้ปัญญาประดิษฐ์อย่างต่อเนื่อง
27. มีการกำหนดบทบาทและความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับปัญญาประดิษฐ์
28. กำหนดตัวชี้วัดความสำเร็จของโครงการปัญญาประดิษฐ์สอดคล้องกับเป้าหมายองค์กร

4.1.2.2 ด้านเทคโนโลยีอัจฉริยะ (Intelligent Technology) ประกอบด้วย

1. มีการนำเทคโนโลยีการเรียนรู้ของเครื่องมาใช้ในการวิเคราะห์ข้อมูล
2. โมเดลการเรียนรู้ของเครื่องช่วยสนับสนุนการตัดสินใจของผู้บริหารและบุคลากร
3. มีการปรับปรุงและพัฒนาโมเดลอย่างต่อเนื่องตามข้อมูลใหม่
4. ผลลัพธ์จากการเรียนรู้ของเครื่องมีความแม่นยำและเชื่อถือได้
5. มีการประยุกต์ใช้การเรียนรู้เชิงลึกกับข้อมูลขนาดใหญ่หรือข้อมูลซับซ้อน
6. ระบบการเรียนรู้เชิงลึกช่วยเพิ่มประสิทธิภาพในการคาดการณ์หรือจำแนกข้อมูล
7. โครงสร้างพื้นฐานรองรับการประมวลผลของโมเดลเชิงลึกได้อย่างเหมาะสม
8. มีการประเมินประสิทธิภาพของโมเดลการเรียนรู้เชิงลึกอย่างสม่ำเสมอ
9. มีการใช้เทคโนโลยี NLP ในการวิเคราะห์ข้อมูลข้อความหรือภาษา

10. ระบบ NLP ช่วยเพิ่มประสิทธิภาพในการให้บริการหรือการสื่อสารกับผู้ใช้

11. การประมวลผลภาษามีความถูกต้องและสอดคล้องกับบริบทของสถาบัน

12. มีการพัฒนาและปรับปรุงระบบ NLP อย่างต่อเนื่อง

13. มีการใช้ปัญญาประดิษฐ์ในการวิเคราะห์พฤติกรรมของผู้ใช้หรือผู้เรียน

14. ผลการวิเคราะห์พฤติกรรมช่วยสนับสนุนการวางแผนและปรับปรุงบริการ

15. ระบบสามารถเรียนรู้และปรับตัวตามพฤติกรรมที่เปลี่ยนแปลงได้

16. การใช้ Behavioral AI คำนึงถึงจริยธรรมและความเป็นส่วนตัวของผู้ใช้

4.1.2.3 ด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity) ประกอบด้วย

1. ติดตั้งเครื่องมือสำหรับการมองเห็นและเฝ้าระวังที่ครอบคลุมเครือข่ายแอปพลิเคชัน และโครงสร้างพื้นฐาน

2. มีมาตรการสร้างความโปร่งใสและตรวจสอบการทำงานของระบบปัญญาประดิษฐ์

3. มีการเข้ารหัสข้อมูลทั้งขณะส่งและจัดเก็บ

4. ระบบสามารถแสดงภาพรวมสถานะการทำงานและแจ้งเตือนเหตุการณ์ผิดปกติได้แบบเรียลไทม์

5. ระบบสามารถตรวจจับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ

6. มีการใช้เทคโนโลยีปัญญาประดิษฐ์วิเคราะห์ Log และ Traffic เพื่อระบุพฤติกรรมที่ผิดปกติ

7. มีการจำลองและทดสอบสถานการณ์โจมตีทางไซเบอร์เพื่อประเมินความแข็งแกร่งของระบบอย่างสม่ำเสมอ

8. มีการตรวจสอบช่องโหว่ของระบบแอปพลิเคชัน และโครงสร้างพื้นฐานเป็นประจำ

9. มีระบบสนับสนุนการรวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่งได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

10. มีทีมผู้เชี่ยวชาญวิเคราะห์เชิงลึกระบุแหล่งและขอบเขตความเสียหาย

11. มีการใช้เครื่องมือวิเคราะห์เหตุการณ์ เพื่อสืบหาต้นตอของภัยคุกคามอย่างเป็นระบบ

12. ผลการวิเคราะห์ถูกนำมาใช้ปรับปรุงมาตรการความปลอดภัยและเพิ่มประสิทธิภาพการป้องกันในอนาคต

13. มีแผนตอบสนองเหตุการณ์ไซเบอร์ที่ชัดเจนและเป็นปัจจุบัน

14. ระบบสามารถตอบสนองและป้องกันภัยคุกคามเชิงรุกได้โดยอัตโนมัติ

15. มีการดำเนินกิจกรรม Threat Hunting เพื่อตรวจหาภัยคุกคามที่อาจแฝงอยู่ในระบบอย่างต่อเนื่อง

16. มีการบังคับใช้มาตรการ Zero Trust เพื่อควบคุมสิทธิ์การเข้าถึงข้อมูลและทรัพยากรภายในองค์กร

17. ระบบได้รับการออกแบบให้สามารถดำเนินงานต่อได้แม้บางส่วนได้รับความเสียหาย

18. มีการทดสอบแผนกู้คืนระบบหลังภัยพิบัติอย่างสม่ำเสมอ

19. มีการจัดเก็บข้อมูลสำรองในพื้นที่แยกหรือระบบคลาวด์ เพื่อป้องกันการสูญหายจาก Ransomware

20. มีมาตรการในการฟื้นฟูระบบและบริการให้กลับมาทำงานได้อย่างรวดเร็วหลังเหตุการณ์โจมตี

21. มีทีมปฏิบัติการด้านความมั่นคงปลอดภัยหรือใช้บริการภายนอกในการเฝ้าระวังระบบอย่างมีประสิทธิภาพ

22. มีการแลกเปลี่ยนและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอกอย่างต่อเนื่อง

23. มีการจัดฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรเป็นประจำ

24. องค์กรปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยสากล

4.1.2.4 ด้านการจัดการองค์กรดิจิทัล (Digital Enterprise Management) ประกอบด้วย

1. มีการกำหนดและสื่อสารกลยุทธ์ดิจิทัลไปยังทุกหน่วยงานในองค์กรอย่างชัดเจน

2. มีกระบวนการวัดผลความสำเร็จของกลยุทธ์ผ่านตัวชี้วัดที่เชื่อมโยงกับพันธกิจองค์กร

3. มีคณะกรรมการกำกับดูแลดิจิทัล (Digital Governance Committee)

4. มีการจัดสรรคงบประมาณและประเมินผลตอบแทนการลงทุนของโครงการ AI และโครงสร้างพื้นฐานดิจิทัลอย่างเป็นระบบ

5. มีการลงทุนในโครงสร้างพื้นฐานเทคโนโลยีเพื่อรองรับการเติบโตในระยะ 3–5 ปีข้างหน้า

6. มีแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อให้ระบบ AI ทำงานต่อได้ในภาวะวิกฤต

7. มีระบบสำรองข้อมูลและศูนย์ข้อมูลสำรอง (Disaster Recovery Site) เพื่อป้องกันการสูญเสียข้อมูล

8. มีการปรับปรุงและอัปเกรดเทคโนโลยีให้สอดคล้องกับนวัตกรรมดิจิทัลสมัยใหม่อย่างต่อเนื่อง

9. มีการบริหารจัดการข้อมูลให้เป็นสินทรัพย์หลักขององค์กร

10. มีการพัฒนาและบำรุงรักษาคลังข้อมูลเพื่อรองรับการทำงานของปัญญาประดิษฐ์

11. ใช้เทคโนโลยีดิจิทัลเพิ่มประสิทธิภาพการทำงานร่วมกันระหว่างหน่วยงาน

12. มีมาตรการควบคุมคุณภาพและความถูกต้องของข้อมูล (Data Quality & Integrity) เพื่อการตัดสินใจที่แม่นยำ

13. มีการใช้ระบบอัตโนมัติในกระบวนการภายในเพื่อลดภาระงานบริหาร

14. มีการประเมินและปรับปรุงประสบการณ์ดิจิทัลของนักศึกษาและบุคลากรอย่างต่อเนื่อง

15. มีการบูรณาการระบบอัตโนมัติเข้ากับระบบสารสนเทศหลักขององค์กร

16. มีการติดตามผลลัพธ์จากการปรับใช้กระบวนการอัตโนมัติเพื่อเพิ่มประสิทธิภาพการดำเนินงาน

17. มีการรวมความปลอดภัยตั้งแต่ต้นทางของทุกโครงการดิจิทัล

18. มีการสื่อสารความเสี่ยงไซเบอร์ต่อผู้บริหารในรูปผลกระทบทางธุรกิจ

19. มีการประเมินช่องโหว่และทดสอบการเจาะระบบ (Vulnerability Assessment & Penetration Test) อย่างต่อเนื่อง

20. มีการจัดทำรายงานสถานะความปลอดภัยไซเบอร์และแผนการปรับปรุงอย่างเป็นระบบ

21. ส่งเสริมวัฒนธรรมนวัตกรรมให้บุคลากรทดลองและเรียนรู้เทคโนโลยีใหม่ ๆ

22. มีการจัดตั้งห้องปฏิบัติการนวัตกรรมหรือกลไกนำร่องเพื่อพัฒนาโซลูชันใหม่

23. มีความคล่องตัวในการปรับเปลี่ยนหรือปรับขนาดโครงการดิจิทัลให้สอดคล้องกับการเปลี่ยนแปลงของตลาด

24. ใช้แนวทางการพัฒนาแบบ Agile/Scrum เพื่อเพิ่มความเร็วและความยืดหยุ่นในการดำเนินงาน

4.1.2.5 ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (Artificial Intelligence Enterprise Architecture) ประกอบด้วย

1. มีการบูรณาการการใช้ปัญญาประดิษฐ์เข้ากับสถาปัตยกรรมองค์กรอย่างเป็นระบบ

2. โครงสร้างสถาปัตยกรรมองค์กรของสถาบันสนับสนุนการนำปัญญาประดิษฐ์ไปใช้ในกระบวนการหลักได้อย่างเหมาะสม

3. การพัฒนาปัญญาประดิษฐ์ของสถาบันสอดคล้องกับแผนสถาปัตยกรรมองค์กรในภาพรวม

4. การบูรณาการสถาปัตยกรรมองค์กร และปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพและความยืดหยุ่นในการดำเนินงานของสถาบัน

5. มีกรอบการทำงานเชิงสถาปัตยกรรมที่ชัดเจนสำหรับการพัฒนาและใช้งานปัญญาประดิษฐ์

6. สามารถกำหนดทิศทางและมาตรฐานของระบบปัญญาประดิษฐ์ได้อย่างเหมาะสม

7. ช่วยลดความซ้ำซ้อนและความซับซ้อนของระบบสารสนเทศ

8. สามารถปรับปรุงและพัฒนาให้สอดคล้องกับเทคโนโลยีปัญญาประดิษฐ์ที่เปลี่ยนแปลงได้

9. ระบบสารสนเทศของสถาบันถูกออกแบบให้ใช้ปัญญาประดิษฐ์ เพื่อเพิ่มประสิทธิภาพการทำงาน

10. การพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ช่วยสนับสนุนการตัดสินใจของผู้บริหารและผู้ปฏิบัติงาน

11. ระบบปัญญาประดิษฐ์สามารถเชื่อมโยงและทำงานร่วมกับระบบสารสนเทศเดิมได้อย่างราบรื่น

12. การออกแบบระบบสารสนเทศด้วยปัญญาประดิษฐ์ ที่คำนึงถึงความปลอดภัยและความน่าเชื่อถือของข้อมูล

13. ใช้ปัญญาประดิษฐ์ในการบริหารจัดการทรัพยากรด้านเทคโนโลยีอย่างมีประสิทธิภาพ

14. ระบบปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพในการใช้ทรัพยากรบุคคลและงบประมาณของสถาบัน

15. การจัดการทรัพยากรด้วยปัญญาประดิษฐ์ช่วยลดต้นทุนและเพิ่มความคุ้มค่าในการดำเนินงาน

16. สามารถติดตามและประเมินการใช้ทรัพยากรผ่านระบบอัจฉริยะได้อย่างเหมาะสม

17. สามารถปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยีได้รวดเร็ว

18. ระบบปัญญาประดิษฐ์สนับสนุนการปรับปรุงกระบวนการทำงานให้มีความคล่องตัวมากขึ้น

19. สามารถปรับเปลี่ยนหรือขยายระบบปัญญาประดิษฐ์ได้ตามความต้องการในอนาคต

20. ตอบสนองต่อการเปลี่ยนแปลงด้านนโยบายและสภาพแวดล้อมได้อย่างมีประสิทธิภาพ

21. สนับสนุนการตรวจจับภัยคุกคามทางดิจิทัลได้อย่างรวดเร็ว

22. ระบบปัญญาประดิษฐ์มีบทบาทในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ

23. สามารถตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ

24. การใช้ปัญญาประดิษฐ์ช่วยเพิ่มความสามารถในการป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์

25. มีการกำหนดหลักจริยธรรมในการพัฒนาและใช้ปัญญาประดิษฐ์อย่างชัดเจน

26. มีระบบปัญญาประดิษฐ์ถูกออกแบบให้โปร่งใสและสามารถอธิบายผลลัพธ์ได้

27. มีมาตรการลดอคติในข้อมูลและโมเดลปัญญาประดิษฐ์

28. มีการอบรมและส่งเสริมความรู้เรื่องจริยธรรมและความรับผิดชอบในการใช้ปัญญาประดิษฐ์

4.1.2.6 ด้านการจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) ประกอบด้วย

1. มีการทดสอบเจาะระบบ และตรวจสอบโค้ดของแอปพลิเคชันเพื่อค้นหาช่องโหว่อย่างสม่ำเสมอ

2. มีการประเมินประสิทธิภาพของมาตรการป้องกันภัยไซเบอร์อย่างต่อเนื่องเพื่อลดความเสี่ยง

3. ใช้เทคโนโลยี AI หรือ Machine Learning ในการตรวจจับพฤติกรรมที่ผิดปกติในระบบเครือข่าย

4. มีระบบแจ้งเตือนภัยคุกคามแบบเรียลไทม์ เพื่อให้ทีมสามารถตอบสนองได้อย่างรวดเร็ว

5. มีแผนขั้นตอนการตอบสนองเหตุการณ์ทางไซเบอร์ที่ครอบคลุมทุกระบบ

6. มีแนวทางเฉพาะในการจัดการเหตุการณ์ที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์

7. มีการกำหนดบทบาทและความรับผิดชอบของทีม IR (Incident Response Team) อย่างชัดเจน

8. มีการทดสอบจำลองเหตุการณ์โจมตี (Cyber Drill) เพื่อประเมินความพร้อมของบุคลากรและระบบ

9. มีการประเมินและจัดการความเสี่ยงทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง

10. มีระบบบริหารจัดการการเปลี่ยนแปลงของ IT และ AI อย่างเป็นระบบ

11. มีการบริหารจัดการแพตช์ (Patch Management) และอัปเดตซอฟต์แวร์อย่างรวดเร็วและมีประสิทธิภาพ

12. มีการจัดทำรายงานความเสี่ยงและความปลอดภัยทางไซเบอร์ที่ชัดเจนสำหรับผู้บริหาร

13. มีนโยบายและมาตรการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย PDPA

14. มีการเข้ารหัสและควบคุมการเข้าถึงข้อมูลเพื่อป้องกันการรั่วไหลหรือการโจมตี

15. มีการบริหารจัดการความเสี่ยงของข้อมูลที่ใช้โดยระบบ AI อย่างเป็นระบบ

16. มีการตรวจสอบและประเมินการจัดการข้อมูลอย่างสม่ำเสมอเพื่อรักษาความเป็นส่วนตัวของผู้ใช้

17. มีการจัดฝึกอบรมภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับสถาบันอุดมศึกษาอย่างสม่ำเสมอ

18. บุคลากรได้รับการอบรมและอัปเดตความรู้ด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง

19. มีการจัดกิจกรรมหรือการรณรงค์สร้างจิตสำนึกด้านความปลอดภัยดิจิทัลภายในองค์กร

20. มีระบบประเมินผลหลังการฝึกอบรมเพื่อวัดผลการเรียนรู้และการนำไปใช้จริงของผู้เข้าร่วม

21. มีนโยบายและข้อบังคับด้านความปลอดภัยสำหรับ AI และ Cloud

22. ผู้บริหารมีการทบทวนและประเมินสถานะความปลอดภัยของระบบอย่างสม่ำเสมอ

23. จัดทำสัญญากับผู้ให้บริการภายนอก พร้อมข้อกำหนดด้านความปลอดภัย

24. ใช้เครื่องมืออัตโนมัติในการตรวจสอบและบังคับใช้ข้อกำหนดด้านความปลอดภัย

25. มีมาตรการความปลอดภัยเครือข่ายเข้มงวดโดยเฉพาะ IoT และอุปกรณ์นักศึกษา

26. มีการกำหนดสิทธิ์การเข้าถึงตามหลัก “Least Privilege” อย่างชัดเจน

27. ระบบเครือข่ายได้รับการตรวจสอบและอัปเดตการป้องกันภัยอย่างต่อเนื่อง

28. มีการใช้ไฟร์วอลล์ ระบบ IDS/IPS และระบบตรวจสอบการจราจรเครือข่ายเพื่อป้องกันภัยคุกคาม

29. ใช้โซลูชัน AI เพื่อช่วยตรวจจับและตอบสนองต่อภัยคุกคามโดยอัตโนมัติ

30. ระบบ AI ถูกฝึกด้วยข้อมูลภัยคุกคามจริงเพื่อเพิ่มความแม่นยำในการวิเคราะห์

31. มีการประเมินและปรับปรุงโมเดล AI ด้านความปลอดภัยอย่างต่อเนื่อง

32. มีการผสานระบบ AI Security เข้ากับระบบปฏิบัติการด้านความปลอดภัยขององค์กรอย่างเป็นเอกภาพ

33. มีมาตรการจัดการการตั้งค่าที่ผิดพลาด (Misconfiguration) ในระบบคลาวด์อย่างเข้มงวด

34. มีการควบคุมสิทธิ์การเข้าถึงข้อมูลบนคลาวด์ตามระดับผู้ใช้งานอย่างเหมาะสม

35. มีการเข้ารหัสและตรวจสอบการรับส่งข้อมูลระหว่างคลาวด์และระบบภายใน

36. มีการสำรองข้อมูลและแผนฟื้นฟูข้อมูลบนคลาวด์เพื่อรองรับเหตุการณ์ไม่คาดคิด

4.1.3 ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

4.1.3.1 ด้านโครงสร้างองค์กร

ผลการวิเคราะห์ความคิดเห็นต่อปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ด้านโครงสร้างองค์กร ประกอบด้วย สถาปัตยกรรมธุรกิจ สถาปัตยกรรมข้อมูล สถาปัตยกรรมระบบแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยี สถาปัตยกรรมด้านความปลอดภัย สถาปัตยกรรมการบูรณาการ และสถาปัตยกรรมการกำกับดูแล

ตารางที่ 4-2 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านโครงสร้างองค์กร (Organizational Structure) โดยรวม

ตัวย่อ	ด้านโครงสร้างองค์กร	$\bar{X}$	S.D.	แปลค่า
EAC	โครงสร้างองค์กร (Organizational Structure)			
BA	สถาปัตยกรรมธุรกิจ	3.77	0.93	มาก
DA	สถาปัตยกรรมข้อมูล	3.79	0.94	มาก
AA	สถาปัตยกรรมระบบแอปพลิเคชัน	3.86	0.94	มาก
TA	สถาปัตยกรรมเทคโนโลยี	3.86	0.95	มาก
SA	สถาปัตยกรรมด้านความปลอดภัย	3.95	0.86	มาก
IA	สถาปัตยกรรมการบูรณาการ	3.83	0.92	มาก

GA	สถาปัตยกรรมการกำกับดูแล	3.91	0.90	มาก
ค่าเฉลี่ยรวม		3.85	0.92	มาก

จากตารางที่ 4-2 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านโครงสร้างองค์กร โดยรวม พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมาก โดยมีค่าเฉลี่ยรวมเท่ากับ 3.85 และมีค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.92 แสดงให้เห็นว่าผู้ตอบแบบสอบถามมีความคิดเห็นสอดคล้องกันในระดับค่อนข้างสูง เมื่อพิจารณาเป็นรายด้าน พบว่า สถาปัตยกรรมด้านความปลอดภัย มีค่าเฉลี่ยสูงที่สุด ($\bar{x}$ = 3.95, S.D. = 0.86) อยู่ในระดับมาก รองลงมา คือ สถาปัตยกรรมการกำกับดูแล มีค่าเฉลี่ยเท่ากับ ($\bar{x}$ =3.91, S.D. = 0.90) อยู่ในระดับมาก สถาปัตยกรรมเทคโนโลยี และสถาปัตยกรรมระบบแอปพลิเคชัน มีค่าเฉลี่ยเท่ากัน ($\bar{x}$=3.86,S.D. = 0.95, 0.94 ตามลำดับ) อยู่ในระดับมาก สถาปัตยกรรมการบูรณาการ มีค่าเฉลี่ยเท่ากับ ($\bar{x}$ =3.83, S.D. = 0.92) อยู่ในระดับมาก สถาปัตยกรรมข้อมูล ($\bar{x}$ =3.79, S.D. = 0.55) และ สถาปัตยกรรมธุรกิจ ($\bar{x}$ =3.77, S.D. = 0.93) ตามลำดับ

ตารางที่ 4-3 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลโครงสร้างองค์กร

ตัวย่อ	ด้านโครงสร้างองค์กร	$\bar{x}$	S.D.	แปลค่า
สถาปัตยกรรมธุรกิจ (Business Architecture)				
BA1	กำหนดวิสัยทัศน์และกลยุทธ์ด้านปัญญาประดิษฐ์ที่สอดคล้องกับพันธกิจ	3.67	0.93	มาก
BA2	บูรณาการการใช้ปัญญาประดิษฐ์เข้ากับกระบวนการหลัก	4.01	0.90	มาก
BA3	ประเมินความพร้อมและศักยภาพของหน่วยงานในการใช้เทคโนโลยีปัญญาประดิษฐ์อย่างต่อเนื่อง	3.61	1.03	มาก
BA4	ผู้บริหารระดับสูงสนับสนุนและส่งเสริมการใช้เทคโนโลยีปัญญาประดิษฐ์	3.79	0.88	มาก
ค่าเฉลี่ย		3.77	0.93	มาก
สถาปัตยกรรมข้อมูล (Data Architecture)				
DA1	กลยุทธ์ข้อมูลที่สนับสนุนการใช้งานปัญญาประดิษฐ์อย่างชัดเจน	3.70	0.90	มาก
DA2	มาตรการควบคุมคุณภาพและความมั่นคงปลอดภัยของข้อมูลอย่างเป็นระบบ	3.75	0.93	มาก
DA3	โครงสร้างข้อมูลรองรับการจัดเก็บและประมวลผล Big Data และข้อมูลแบบ Unstructured	4.06	0.91	มาก
DA4	ระบบติดป้ายกำกับและจัดการข้อมูลเพื่อสนับสนุนการเรียนรู้ของโมเดลปัญญาประดิษฐ์	3.64	1.03	มาก

ตัวย่อ	ด้านโครงสร้างองค์กร	$\bar{x}$	S.D.	แปลค่า
ค่าเฉลี่ย		3.79	0.94	มาก
สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture)				
AA1	การพัฒนาแอปพลิเคชันหรือระบบสารสนเทศที่เชื่อมโยงกับปัญญาประดิษฐ์	3.93	0.88	มาก
AA2	ระบบแอปพลิเคชันได้รับการออกแบบให้สามารถปรับขนาดและเชื่อมต่อได้ง่าย	3.93	0.87	มาก
AA3	มาตรฐานกลางในการพัฒนาและบูรณาการแอปพลิเคชัน	3.85	0.97	มาก
AA4	การปรับปรุงระบบงานอย่างต่อเนื่องเพื่อรองรับเทคโนโลยีปัญญาประดิษฐ์ใหม่ๆ	3.72	1.07	มาก
ค่าเฉลี่ย		3.86	0.94	มาก
สถาปัตยกรรมเทคโนโลยี (Technology Architecture)				
TA1	โครงสร้างพื้นฐานด้านเทคโนโลยีที่รองรับการประมวลผลของปัญญาประดิษฐ์	4.02	0.88	มาก
TA2	ใช้แพลตฟอร์มคลาวด์ในการพัฒนาปัญญาประดิษฐ์	3.61	1.11	มาก
TA3	แผนการบำรุงรักษาและอัปเดตเทคโนโลยีอย่างต่อเนื่อง	3.99	0.87	มาก
TA4	การนำเทคโนโลยี Edge AI หรือระบบประมวลผลแบบกระจายมาใช้เพื่อเพิ่มประสิทธิภาพ	3.81	0.94	มาก
ค่าเฉลี่ย		3.86	0.95	มาก
สถาปัตยกรรมด้านความมั่งคงปลอดภัย (Security Architecture)				
SA1	กลยุทธ์และนโยบายความปลอดภัยทางไซเบอร์ที่ชัดเจน	4.08	0.87	มาก
SA2	การประเมินและป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์	3.91	0.87	มาก
SA3	การเข้ารหัสและจำกัดสิทธิ์การเข้าถึงข้อมูลอย่างเหมาะสม	3.95	0.85	มาก
SA4	แผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลและระบบปัญญาประดิษฐ์	3.84	0.86	มาก
ค่าเฉลี่ย		3.95	0.86	มาก
สถาปัตยกรรมการบูรณาการ (Integration Architecture)				
IA1	สถาปัตยกรรมเชื่อมต่อโมเดลปัญญาประดิษฐ์กับระบบหลักขององค์กร	3.78	0.96	มาก
IA2	มาตรฐานหรือ API กลางสำหรับการแลกเปลี่ยนข้อมูลระหว่างระบบ	3.93	0.88	มาก
IA3	การตรวจสอบและทดสอบการเชื่อมต่อระหว่างระบบอย่างสม่ำเสมอ	3.93	0.82	มาก
IA4	ระบบบูรณาการมีความยืดหยุ่นรองรับการเปลี่ยนแปลงของเทคโนโลยี	3.67	1.04	มาก
ค่าเฉลี่ย		3.83	0.92	มาก
สถาปัตยกรรมการกำกับดูแล (Governance Architecture)				
GA1	กรอบการกำกับดูแลด้านปัญญาประดิษฐ์ที่ชัดเจน	4.07	0.89	มาก

ตัวย่อ	ด้านโครงสร้างองค์กร	$\bar{x}$	S.D.	แปลค่า
GA2	การติดตามและประเมินผลการใช้ปัญญาประดิษฐ์อย่างต่อเนื่อง	3.78	0.94	มาก
GA3	การกำหนดบทบาทและความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับปัญญาประดิษฐ์	3.99	0.90	มาก
GA4	กำหนดตัวชี้วัดความสำเร็จของโครงการปัญญาประดิษฐ์สอดคล้องกับเป้าหมายองค์กร	3.81	0.89	มาก
ค่าเฉลี่ย		3.91	0.90	มาก
ค่าเฉลี่ยรวม		3.85	0.92	มาก

จากตารางที่ 4-3 ผลการวิเคราะห์ความคิดเห็นต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านโครงสร้างองค์กร มีค่าเฉลี่ยอยู่ในระดับ มาก ($\bar{x}$=3.85, S.D. = 0.92) โดยสถาปัตยกรรมด้านความปลอดภัย มีค่าเฉลี่ยสูงที่สุด รองลงมา คือ สถาปัตยกรรมการกำกับดูแล สถาปัตยกรรมเทคโนโลยี สถาปัตยกรรมการบูรณาการ สถาปัตยกรรมข้อมูล และ สถาปัตยกรรมธุรกิจ ตามลำดับ สรุปผลรายด้านดังนี้

สถาปัตยกรรมธุรกิจ โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.77, S.D. = 0.93) เมื่อพิจารณารายข้อ พบว่า การบูรณาการการใช้ปัญญาประดิษฐ์เข้ากับกระบวนการหลักขององค์กรมีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.01, S.D. = 0.90) รองลงมา คือ ผู้บริหารระดับสูงสนับสนุนและส่งเสริมการใช้เทคโนโลยีปัญญาประดิษฐ์ ($\bar{x}$ = 3.79, S.D. = 0.88) การกำหนดวิสัยทัศน์และกลยุทธ์ด้านปัญญาประดิษฐ์ที่สอดคล้องกับพันธกิจขององค์กร ($\bar{x}$ = 3.67, S.D. = 0.93) การประเมินความพร้อมและศักยภาพของหน่วยงานในการใช้เทคโนโลยีปัญญาประดิษฐ์อย่างต่อเนื่อง ($\bar{x}$ = 3.61, S.D. = 1.03) ตามลำดับ

สถาปัตยกรรมข้อมูล โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.79, S.D. = 0.94) เมื่อพิจารณารายข้อ พบว่า โครงสร้างข้อมูลรองรับการจัดเก็บและประมวลผล Big Data และข้อมูลแบบไม่มีโครงสร้างมีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.06, S.D. = 0.91) รองลงมา คือ มาตรการควบคุมคุณภาพและความมั่นคงปลอดภัยของข้อมูล ($\bar{x}$ = 3.75, S.D. = 0.93) กลยุทธ์ข้อมูลที่สนับสนุนการใช้งานปัญญาประดิษฐ์ ($\bar{x}$ = 3.70, S.D. = 0.90) และระบบติดป้ายกำกับและจัดการข้อมูลเพื่อสนับสนุนการเรียนรู้ของโมเดลปัญญาประดิษฐ์ ($\bar{x}$ = 3.64, S.D. = 1.03) ตามลำดับ

สถาปัตยกรรมระบบแอปพลิเคชัน โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.86, S.D. = 0.94) เมื่อพิจารณารายข้อ พบว่า การพัฒนาแอปพลิเคชันหรือระบบสารสนเทศที่เชื่อมโยงกับปัญญาประดิษฐ์และการออกแบบระบบให้สามารถปรับขนาดและเชื่อมต่อได้ง่าย มีค่าเฉลี่ยเท่ากันและสูงสุด ($\bar{x}$ = 3.93, S.D. = 0.88 และ 0.87 ตามลำดับ) รองลงมา คือ การกำหนดมาตรฐานกลางในการพัฒนาและ

บูรณาการแอปพลิเคชัน ($\bar{X}$ = 3.85, S.D. = 0.97) และการปรับปรุงระบบงานอย่างต่อเนื่องเพื่อรองรับเทคโนโลยี AI ใหม่ๆ ($\bar{X}$ = 3.72, S.D. = 1.07) ตามลำดับ

สถาปัตยกรรมเทคโนโลยี โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.86, S.D. = 0.95) เมื่อพิจารณารายข้อ พบว่า โครงสร้างพื้นฐานด้านเทคโนโลยีที่รองรับการประมวลผล AI มีค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.02, S.D. = 0.88) รองลงมา คือ แผนการบำรุงรักษาและอัปเดตเทคโนโลยีอย่างต่อเนื่อง ($\bar{X}$ = 3.99, S.D. = 0.87) การนำเทคโนโลยี Edge AI มาใช้เพื่อเพิ่มประสิทธิภาพ ($\bar{X}$ = 3.81, S.D. = 0.94) และการใช้แพลตฟอร์มคลาวด์ในการพัฒนา AI ($\bar{X}$ = 3.61, S.D. = 1.11) ตามลำดับ

สถาปัตยกรรมด้านความมั่งคงปลอดภัย โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.95, S.D. = 0.86) เมื่อพิจารณารายข้อ พบว่า กลยุทธ์และนโยบายความปลอดภัยทางไซเบอร์มีค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.08, S.D. = 0.87) รองลงมา คือ การเข้ารหัสและจำกัดสิทธิ์การเข้าถึงข้อมูล ($\bar{X}$ = 3.95, S.D. = 0.85) การประเมินและป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของระบบ AI ($\bar{X}$ = 3.91, S.D. = 0.87) และแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยมีค่าเฉลี่ยต่ำสุด ($\bar{X}$ = 3.84, S.D. = 0.86) ตามลำดับ

สถาปัตยกรรมการบูรณาการโดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.83, S.D. = 0.92) เมื่อพิจารณารายข้อ พบว่า มาตรฐานหรือ API กลางสำหรับการแลกเปลี่ยนข้อมูล และการตรวจสอบการเชื่อมต่อระบบอย่างสม่ำเสมอ มีค่าเฉลี่ยสูงสุดเท่ากัน ($\bar{X}$ = 3.93, S.D. = 0.88 และ 0.82 ตามลำดับ) รองลงมา คือ สถาปัตยกรรมการเชื่อมต่อโมเดล AI กับระบบหลักขององค์กร ($\bar{X}$ = 3.78, S.D. = 0.96) และส่วนความยืดหยุ่นของระบบบูรณาการ ($\bar{X}$ = 3.67, S.D. = 1.04) ตามลำดับ

สถาปัตยกรรมการกำกับดูแลโดรวมอยู่ในระดับมาก ($\bar{X}$ = 3.91, S.D. = 0.90) เมื่อพิจารณารายข้อ พบว่า กรอบการกำกับดูแลด้านปัญญาประดิษฐ์มีค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.07, S.D. = 0.89) รองลงมา คือ การกำหนดบทบาทและความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับ AI ($\bar{X}$ = 3.99, S.D. = 0.90) การกำหนดตัวชี้วัดความสำเร็จของโครงการ AI ($\bar{X}$ = 3.81, S.D. = 0.89) และการติดตามและประเมินผลการใช้ AI อย่างต่อเนื่อง ($\bar{X}$ = 3.78 , S.D. = 0.94) ตามลำดับ

4.1.3.2 ด้านเทคโนโลยีอัจฉริยะ

ผลการวิเคราะห์ความคิดเห็นต่อปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ด้านเทคโนโลยีอัจฉริยะ ประกอบด้วย การเรียนรู้ของเครื่อง การเรียนรู้เชิงลึก การประมวลผลภาษาธรรมชาติ และความรู้เชิงพฤติกรรม มีผลการวิเคราะห์ดังนี้

ตารางที่ 4-4 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านเทคโนโลยีอัจฉริยะ โดยรวม

ตัวย่อ	ด้านเทคโนโลยีอัจฉริยะ	$\bar{X}$	S.D.	แปลค่า
AIT	ด้านเทคโนโลยีอัจฉริยะ (Intelligent Technology)			
ML	การเรียนรู้ของเครื่อง	3.95	0.88	มาก
DL	การเรียนรู้เชิงลึก	3.93	0.80	มาก
NL	การประมวลผลภาษาธรรมชาติ	3.90	0.87	มาก
BI	ความรู้เชิงพฤติกรรม	3.91	0.84	มาก
ค่าเฉลี่ยรวม		3.92	0.85	มาก

จากตารางที่ 4-4 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านเทคโนโลยีอัจฉริยะ โดยรวม พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมาก โดยมีค่าเฉลี่ยเท่ากับ 3.92 และมีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.85 แสดงให้เห็นว่าผู้ตอบแบบสอบถามมีความคิดเห็นสอดคล้องกันในระดับค่อนข้างสูง เมื่อพิจารณาเป็นรายด้าน พบว่า การเรียนรู้ของเครื่อง มีค่าเฉลี่ยสูงที่สุด ($\bar{x}$ = 3.95, S.D. = 0.88) อยู่ในระดับมาก รองลงมาคือ การเรียนรู้เชิงลึก มีค่าเฉลี่ย ($\bar{x}$ = 3.93, S.D. = 0.80) อยู่ในระดับมาก ความรู้เชิงพฤติกรรม มีค่าเฉลี่ย ($\bar{x}$ = 3.91, S.D. = 0.87) อยู่ในระดับมาก และ การประมวลผลภาษาธรรมชาติ มีค่าเฉลี่ย ($\bar{x}$ = 3.90, S.D. = 0.84) อยู่ในระดับมาก ตามลำดับ

ตารางที่ 4-5 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านเทคโนโลยีอัจฉริยะ

ตัวย่อ	ด้านเทคโนโลยีอัจฉริยะ	$\bar{X}$	S.D.	แปลค่า
การเรียนรู้ของเครื่อง (Machine Learning)				
ML1	การนำเทคโนโลยีการเรียนรู้ของเครื่องมาใช้ในการวิเคราะห์ข้อมูล	4.04	0.83	มาก
ML2	สนับสนุนการตัดสินใจของผู้บริหารและบุคลากร	3.96	0.90	มาก
ML3	การปรับปรุงและพัฒนาโมเดลอย่างต่อเนื่องตามข้อมูลใหม่	4.04	0.83	มาก
ML4	ความแม่นยำและเชื่อถือได้	3.75	0.95	มาก
ค่าเฉลี่ย		3.95	0.88	มาก
การเรียนรู้เชิงลึก (Deep Learning)				
DL1	การประยุกต์ใช้การเรียนรู้เชิงลึกกับข้อมูลขนาดใหญ่หรือข้อมูลซับซ้อน	4.02	0.78	มาก
DL2	เพิ่มประสิทธิภาพในการคาดการณ์หรือจำแนกข้อมูล	3.83	0.84	มาก
DL3	โครงสร้างพื้นฐานรองรับการประมวลผลของโมเดลเชิงลึกได้อย่างเหมาะสม	3.90	0.77	มาก

ตัวย่อ	ด้านเทคโนโลยีอัจฉริยะ	$\bar{X}$	S.D.	แปลค่า
DL4	การประเมินประสิทธิภาพของโมเดลการเรียนรู้เชิงลึกอย่างสม่ำเสมอ	3.95	0.80	มาก
ค่าเฉลี่ย		3.93	0.80	มาก
การประมวลผลภาษาธรรมชาติ (Natural Language Processing - NLP)				
NL1	การวิเคราะห์ข้อมูลข้อความหรือภาษา	3.78	0.87	มาก
NL2	เพิ่มประสิทธิภาพในการให้บริการหรือการสื่อสารกับผู้ใช้	4.02	0.85	มาก
NL3	ความถูกต้องและสอดคล้องกับบริบทของสถาบัน	3.79	0.92	มาก
NL4	การพัฒนาและปรับปรุงระบบ NLP อย่างต่อเนื่อง	4.02	0.85	มาก
ค่าเฉลี่ย		3.90	0.87	มาก
ความรู้เชิงพฤติกรรม (Behavioral AI)				
BI1	การใช้ปัญญาประดิษฐ์ในการวิเคราะห์พฤติกรรมของผู้ใช้หรือผู้เรียน	3.89	0.82	มาก
BI2	สนับสนุนการวางแผนและปรับปรุงบริการ	3.83	0.85	มาก
BI3	ระบบสามารถเรียนรู้และปรับตัวตามพฤติกรรมที่เปลี่ยนแปลงได้	4.02	0.87	มาก
BI4	การคำนึงถึงจริยธรรมและความเป็นส่วนตัวของผู้ใช้	3.92	0.82	มาก
ค่าเฉลี่ย		3.91	0.85	มาก
ค่าเฉลี่ยรวม		3.92	0.85	มาก

จากตารางที่ 4-5 ผลการวิเคราะห์ความคิดเห็นต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านเทคโนโลยีอัจฉริยะ มีค่าเฉลี่ยอยู่ในระดับ มาก ($\bar{X}$ = 3.92, S.D. = 0.85) โดยการเรียนรู้ของเครื่อง มีค่าเฉลี่ยสูงที่สุด รองลงมาคือ การเรียนรู้เชิงลึก ความรู้เชิงพฤติกรรม และ การประมวลผลภาษาธรรมชาติ ตามลำดับ สรุปผลรายด้านดังนี้

การเรียนรู้ของเครื่อง โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.95, S.D. = 0.88) เมื่อพิจารณารายข้อ พบว่า การนำเทคโนโลยีการเรียนรู้ของเครื่องมาใช้ในการวิเคราะห์ข้อมูล มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.04, S.D. = 0.83) และการปรับปรุงและพัฒนาโมเดลอย่างต่อเนื่องตามข้อมูลใหม่ ($\bar{x}$ = 4.04, S.D. = 0.83) รองลงมา คือ สนับสนุนการตัดสินใจของผู้บริหารและบุคลากร ($\bar{x}$ = 3.96, S.D. = 0.90) และความแม่นยำและความเชื่อถือได้ของระบบ ($\bar{x}$ = 3.75, S.D. = 0.95) ตามลำดับ

การเรียนรู้เชิงลึก โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.93, S.D. = 0.80) เมื่อพิจารณารายข้อ พบว่า การประยุกต์ใช้การเรียนรู้เชิงลึกกับข้อมูลขนาดใหญ่หรือข้อมูลซับซ้อน มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.02, S.D. = 0.78) รองลงมา คือ การประเมินประสิทธิภาพของโมเดลอย่างสม่ำเสมอ ($\bar{x}$ = 3.95, S.D. = 0.80) โครงสร้างพื้นฐานรองรับการประมวลผลของโมเดลเชิงลึก ($\bar{x}$ = 3.90, S.D. = 0.77) และการเพิ่มประสิทธิภาพในการคาดการณ์หรือจำแนกข้อมูล ($\bar{x}$ = 3.83, S.D. = 0.84) ตามลำดับ

การประมวลผลภาษาธรรมชาติ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.90, S.D. = 0.87) เมื่อพิจารณารายข้อ พบว่า การเพิ่มประสิทธิภาพในการให้บริการหรือการสื่อสารกับผู้ใช้ และการพัฒนาและปรับปรุงระบบ NLP อย่างต่อเนื่อง มีค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.02, S.D. = 0.85) รองลงมา คือ ความถูกต้องและสอดคล้องกับบริบทของสถาบัน ($\bar{X}$ = 3.79, S.D. = 0.92) และการวิเคราะห์ข้อมูลข้อความหรือภาษา ($\bar{X}$ = 3.78, S.D. = 0.87) ตามลำดับ

ความรู้เชิงพฤติกรรม โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.91, S.D. = 0.84) เมื่อพิจารณารายข้อ พบว่า ระบบสามารถเรียนรู้และปรับตัวตามพฤติกรรมที่เปลี่ยนแปลง มีค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.02, S.D. = 0.87) รองลงมา คือ การคำนึงถึงจริยธรรมและความเป็นส่วนตัวของผู้ใช้ ($\bar{X}$ = 3.92, S.D. = 0.82) การใช้ AI วิเคราะห์พฤติกรรมของผู้ใช้หรือผู้เรียน ($\bar{X}$ = 3.89, S.D. = 0.82) และสนับสนุนการวางแผนและปรับปรุงบริการ ($\bar{X}$ = 3.83, S.D. = 0.85) ตามลำดับ

4.1.3.3 ด้านระบบภูมิคุ้มกันดิจิทัล

ผลการวิเคราะห์ความคิดเห็นต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านระบบภูมิคุ้มกันดิจิทัล ประกอบด้วย การมองเห็นและเฝ้าระวัง การตรวจจับภัยคุกคาม การสืบสวนและวิเคราะห์ การตอบสนองและการป้องกันเชิงรุก ความทนทานและการฟื้นฟู และความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ มีผลวิเคราะห์ ดังนี้

ตารางที่ 4-6 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านระบบภูมิคุ้มกันดิจิทัล โดยรวม

ตัวย่อ	ด้านระบบภูมิคุ้มกันดิจิทัล	$\bar{X}$	S.D.	แปลค่า
DIS	ด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity)			
OV	การมองเห็นและเฝ้าระวัง	3.97	0.81	มาก
TD	การตรวจจับภัยคุกคาม	3.95	0.80	มาก
AN	การสืบสวนและวิเคราะห์	3.95	0.79	มาก
RP	การตอบสนองและการป้องกันเชิงรุก	3.89	0.79	มาก
RR	ความทนทานและการฟื้นฟู	3.91	0.80	มาก
CC	ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์	3.92	0.80	มาก
ค่าเฉลี่ยรวม		3.93	0.80	มาก

จากตารางที่ 4-6 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านระบบภูมิคุ้มกันดิจิทัล โดยรวม พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมาก โดยมีค่าเฉลี่ยเท่ากับ 3.93 และมีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.80 แสดงให้เห็นว่าผู้ตอบแบบสอบถามมีความคิดเห็นสอดคล้องกันในระดับค่อนข้างสูง เมื่อพิจารณาเป็นรายด้าน พบว่า การมองเห็นและเฝ้าระวัง มีค่าเฉลี่ยสูงที่สุด ($\bar{X}$ = 3.97, S.D. = 0.81) อยู่ในระดับมาก รองลงมาคือ การตรวจจับภัยคุกคาม และการสืบสวนและวิเคราะห์ มีค่าเฉลี่ย ($\bar{X}$ = 3.95, S.D. = 0.79) อยู่ในระดับมาก ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ มีค่าเฉลี่ย ($\bar{X}$ = 3.92, S.D. = 0.80) อยู่ในระดับมาก ความทนทานและการฟื้นฟู มีค่าเฉลี่ย ($\bar{X}$ = 3.91, S.D. = 0.80) และการตอบสนองและการป้องกันเชิงรุก มีค่าเฉลี่ย ($\bar{X}$ = 3.89, S.D. = 0.79) อยู่ในระดับมาก ตามลำดับ

ตารางที่ 4-7 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านระบบภูมิคุ้มกันดิจิทัลโดยรวม

ตัวย่อ	ด้านระบบภูมิคุ้มกันดิจิทัล	$\bar{X}$	S.D.	แปลค่า
การมองเห็นและเฝ้าระวัง (Observability & Visibility)				
OV1	ติดตั้งเครื่องมือสำหรับการมองเห็นและเฝ้าระวังที่ครอบคลุมเครือข่ายแอปพลิเคชัน และโครงสร้างพื้นฐาน	4.04	0.79	มาก
OV2	มาตรการสร้างความโปร่งใสและตรวจสอบการทำงานของระบบปัญญาประดิษฐ์	3.87	0.82	มาก
OV3	การเข้ารหัสข้อมูลทั้งขณะส่งและจัดเก็บ	4.05	0.82	มาก
OV4	แสดงภาพรวมสถานะการทำงานและแจ้งเตือนเหตุการณ์ผิดปกติได้แบบเรียลไทม์	3.91	0.80	มาก
ค่าเฉลี่ย		3.97	0.81	มาก
การตรวจจับภัยคุกคาม (Threat Detection)				
TD1	ระบบสามารถตรวจจับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ	4.03	0.81	มาก
TD2	การใช้เทคโนโลยีปัญญาประดิษฐ์วิเคราะห์ Log และ Traffic เพื่อระบุพฤติกรรมที่ผิดปกติ	3.95	0.82	มาก
TD3	การจำลองและทดสอบสถานการณ์โจมตีทางไซเบอร์เพื่อประเมินความแข็งแกร่งของระบบอย่างสม่ำเสมอ	3.82	0.84	มาก
TD4	การตรวจสอบช่องโหว่ของระบบแอปพลิเคชัน และโครงสร้างพื้นฐานเป็นประจำ	3.99	0.75	มาก
ค่าเฉลี่ย		3.95	0.80	มาก

ตัวย่อ	ด้านระบบภูมิคุ้มกันดิจิทัล	$\bar{X}$	S.D.	แปลค่า
การสืบสวนและวิเคราะห์ (Investigation & Analysis)				
AN1	สนับสนุนการรวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่งได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย	3.88	0.78	มาก
AN2	ผู้เชี่ยวชาญวิเคราะห์เชิงลึกระบุแหล่งและขอบเขตความเสียหาย	4.09	0.78	มาก
AN3	การใช้เครื่องมือวิเคราะห์เหตุการณ์ เพื่อสืบหาต้นตอของภัยคุกคามอย่างเป็นระบบ	3.92	0.79	มาก
AN4	การวิเคราะห์ถูกนำมาใช้ปรับปรุงมาตรการความปลอดภัยและเพิ่มประสิทธิภาพการป้องกันในอนาคต	3.91	0.80	มาก
	ค่าเฉลี่ย	3.95	0.79	มาก
การตอบสนองและการป้องกันเชิงรุก (Response & Proactive Defense)				
RP1	แผนตอบสนองเหตุการณ์ไซเบอร์ที่ชัดเจนและเป็นปัจจุบัน	3.92	0.80	มาก
RP2	ตอบสนองและป้องกันภัยคุกคามเชิงรุกได้โดยอัตโนมัติ	3.81	0.80	มาก
RP3	การดำเนินกิจกรรม Threat Hunting เพื่อตรวจหาภัยคุกคามที่อาจแฝงอยู่ในระบบอย่างต่อเนื่อง	3.87	0.80	มาก
RP4	การบังคับใช้มาตรการ Zero Trust เพื่อควบคุมสิทธิ์การเข้าถึงข้อมูลและทรัพยากรภายในองค์กร	3.97	0.78	มาก
	ค่าเฉลี่ย	3.89	0.79	มาก
ความทนทานและการฟื้นฟู (Resilience & Recovery)				
RR1	การออกแบบให้สามารถดำเนินงานต่อได้แม้บางส่วนได้รับความเสียหาย	3.87	0.81	มาก
RR2	การทดสอบแผนกู้คืนระบบหลังภัยพิบัติอย่างสม่ำเสมอ	4.07	0.80	มาก
RR3	การจัดเก็บข้อมูลสำรองในพื้นที่แยกหรือระบบคลาวด์ เพื่อป้องกันการสูญหายจาก Ransomware	3.76	0.80	มาก
RR4	มาตรการในการฟื้นฟูระบบและบริการให้กลับมาทำงานได้อย่างรวดเร็วหลังเหตุการณ์โจมตี	3.93	0.79	มาก
	ค่าเฉลี่ย	3.91	0.80	มาก
ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ (Collaboration & Cybersecurity Awareness)				
CC1	ทีมปฏิบัติการด้านความมั่นคงปลอดภัยหรือใช้บริการภายนอกในการเฝ้าระวังระบบอย่างมีประสิทธิภาพ	3.98	0.80	มาก
CC2	การแลกเปลี่ยนและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอกอย่างต่อเนื่อง	3.84	0.82	มาก
CC3	การจัดฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรเป็นประจำ	3.99	0.76	มาก

ตัวย่อ	ด้านระบบภูมิคุ้มกันดิจิทัล	$\bar{X}$	S.D.	แปลค่า
CC4	มาตรฐานความมั่นคงปลอดภัยสากล	3.88	0.82	มาก
ค่าเฉลี่ย		3.92	0.80	มาก
ค่าเฉลี่ยรวม		3.93	0.80	มาก

จากตารางที่ 4-7 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านระบบภูมิคุ้มกันดิจิทัล โดยรวม มีค่าเฉลี่ยอยู่ในระดับมาก ($\bar{X}$ = 3.93, S.D. = 0.80) โดยการมองเห็นและเฝ้าระวัง มีค่าเฉลี่ยสูงที่สุด รองลงมาคือ การตรวจจับภัยคุกคาม การสืบสวนและวิเคราะห์ ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ ความทนทานและการฟื้นฟู และการตอบสนองและการป้องกันเชิงรุก ตามลำดับ สรุปผลรายด้านดังนี้

การมองเห็นและเฝ้าระวัง โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.97, S.D. = 0.81) เมื่อพิจารณารายข้อ พบว่า การเข้ารหัสข้อมูลทั้งขณะส่งและจัดเก็บ มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.05, S.D. = 0.82) รองลงมา คือ การติดตั้งเครื่องมือสำหรับการมองเห็นและเฝ้าระวังที่ครอบคลุมเครือข่ายแอปพลิเคชันและโครงสร้างพื้นฐาน ($\bar{x}$ = 4.04, S.D. = 0.79) แสดงภาพรวมสถานะการทำงานและแจ้งเตือนเหตุการณ์ผิดปกติได้แบบเรียลไทม์ ($\bar{x}$ = 3.91, S.D. = 0.80) และมาตรการสร้างความโปร่งใสและตรวจสอบการทำงานของระบบปัญญาประดิษฐ์ ($\bar{x}$ = 3.87, S.D. = 0.82) ตามลำดับ

การตรวจจับภัยคุกคาม โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.95, S.D. = 0.80) เมื่อพิจารณารายข้อ พบว่า ระบบสามารถตรวจจับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.03, S.D. = 0.81) รองลงมา คือ การตรวจสอบช่องโหว่ของระบบแอปพลิเคชัน และโครงสร้างพื้นฐานเป็นประจำ ($\bar{x}$ = 3.99, S.D. = 0.75) การใช้เทคโนโลยีปัญญาประดิษฐ์วิเคราะห์ Log และ Traffic เพื่อระบุพฤติกรรมที่ผิดปกติ ($\bar{x}$ = 3.95, S.D. = 0.82) และการจำลองและทดสอบสถานการณ์โจมตีทางไซเบอร์เพื่อประเมินความแข็งแกร่งของระบบอย่างสม่ำเสมอ ($\bar{x}$ = 3.82, S.D. = 0.84) ตามลำดับ

การสืบสวนและวิเคราะห์ โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.95, S.D. = 0.79) เมื่อพิจารณารายข้อ พบว่า ผู้เชี่ยวชาญวิเคราะห์เชิงลึกระบุแหล่งและขอบเขตความเสียหาย มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.09, S.D. = 0.78) รองลงมา คือ การใช้เครื่องมือวิเคราะห์เหตุการณ์ เพื่อสืบหาต้นตอของภัยคุกคามอย่างเป็นระบบ ($\bar{x}$ = 3.92, S.D. = 0.79) การวิเคราะห์ถูกนำมาใช้ปรับปรุงมาตรการความปลอดภัยและเพิ่มประสิทธิภาพการป้องกันในอนาคต ($\bar{x}$ = 3.91, S.D. = 0.80) และสนับสนุนการรวบรวมและ

วิเคราะห์ข้อมูลจากหลายแหล่งได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย ($\bar{x}$ = 3.88, S.D. = 0.78) ตามลำดับ

การตอบสนองและการป้องกันเชิงรุก โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.89, S.D. = 0.79) เมื่อพิจารณารายข้อ พบว่า การบังคับใช้มาตรการ Zero Trust เพื่อควบคุมสิทธิ์การเข้าถึงข้อมูลและทรัพยากรภายในองค์กร มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 3.97, S.D. = 0.78) รองลงมา คือ แผนตอบสนองเหตุการณ์ไซเบอร์ที่ชัดเจนและเป็นปัจจุบัน ($\bar{x}$ = 3.92, S.D. = 0.80) การดำเนินกิจกรรม Threat Hunting เพื่อตรวจหาภัยคุกคามที่อาจแฝงอยู่ในระบบอย่างต่อเนื่อง ($\bar{x}$ = 3.87, S.D. = 0.80) และตอบสนองและป้องกันภัยคุกคามเชิงรุกได้โดยอัตโนมัติ ($\bar{x}$ = 3.81, S.D. = 0.80) ตามลำดับ

ความทนทานและการฟื้นฟู โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.91, S.D. = 0.80) เมื่อพิจารณารายข้อ พบว่า การทดสอบแผนกู้คืนระบบหลังภัยพิบัติอย่างสม่ำเสมอ มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.07, S.D. = 0.80) รองลงมา คือ มาตรการในการฟื้นฟูระบบและบริการให้กลับมาทำงานได้อย่างรวดเร็วหลังเหตุการณ์โจมตี ($\bar{x}$ = 3.93, S.D. = 0.79) การออกแบบให้สามารถดำเนินงานต่อได้แม้บางส่วนได้รับความเสียหาย ($\bar{x}$ = 3.87, S.D. = 0.81) และการจัดเก็บข้อมูลสำรองในพื้นที่แยกหรือระบบคลาวด์ เพื่อป้องกันการสูญหายจาก Ransomware ($\bar{x}$ = 3.76, S.D. = 0.80) ตามลำดับ

ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.92, S.D. = 0.80) เมื่อพิจารณารายข้อ พบว่า การจัดฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรเป็นประจำ มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 3.99, S.D. = 0.76) รองลงมา คือ ทีมปฏิบัติการด้านความมั่นคงปลอดภัยหรือใช้บริการภายนอกในการเฝ้าระวังระบบอย่างมีประสิทธิภาพ ($\bar{x}$ = 3.98, S.D. = 0.80) มาตรฐานความมั่นคงปลอดภัยสากล ($\bar{x}$ = 3.88, S.D. = 0.82) และการแลกเปลี่ยนและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอกอย่างต่อเนื่อง ($\bar{x}$ = 3.84, S.D. = 0.82) ตามลำดับ

4.1.3.4 ด้านการจัดการองค์กรดิจิทัล

ผลการวิเคราะห์ความคิดเห็นต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ประกอบด้วย กลยุทธ์ดิจิทัล โครงสร้างพื้นฐานเทคโนโลยี การจัดการข้อมูล กระบวนการอัตโนมัติ ความมั่นคงปลอดภัยทางไซเบอร์ มีผลวิเคราะห์ ดังนี้

ตารางที่ 4-8 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล โดยรวม

ตัวย่อ	ด้านการจัดการองค์กรดิจิทัล	$\bar{X}$	S.D.	แปลค่า
DEM	การจัดการองค์กรดิจิทัล (Digital Enterprise Management)			
DS	กลยุทธ์ดิจิทัล	3.92	0.80	มาก
TI	โครงสร้างพื้นฐานเทคโนโลยี	3.94	0.80	มาก
DM	การจัดการข้อมูล	3.92	0.80	มาก
PA	กระบวนการอัตโนมัติ	3.82	0.81	มาก
CB	ความมั่นคงปลอดภัยทางไซเบอร์	3.88	0.79	มาก
ค่าเฉลี่ยรวม		3.90	0.80	มาก

จากตารางที่ 4-8 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล โดยรวม พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมาก โดยมีค่าเฉลี่ยเท่ากับ 3.90 และมีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.80 แสดงให้เห็นว่าผู้ตอบแบบสอบถามมีความคิดเห็นสอดคล้องกันในระดับค่อนข้างสูง เมื่อพิจารณาเป็นรายด้าน พบว่า โครงสร้างพื้นฐานเทคโนโลยี มีค่าเฉลี่ยสูงที่สุด ($\bar{x}$ = 3.94, S.D. = 0.80) อยู่ในระดับมาก รองลงมาคือ กลยุทธ์ดิจิทัล และการจัดการข้อมูล มีค่าเฉลี่ย ($\bar{x}$ = 3.92, S.D. = 0.80) อยู่ในระดับมาก ความมั่นคงปลอดภัยทางไซเบอร์ มีค่าเฉลี่ย ($\bar{x}$ = 3.88, S.D. = 0.79) อยู่ในระดับมาก และกระบวนการอัตโนมัติ มีค่าเฉลี่ย ($\bar{x}$ = 3.82, S.D. = 0.81) อยู่ในระดับมาก ตามลำดับ

ตารางที่ 4-9 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านการจัดการองค์กรดิจิทัลโดยรวม

ตัวย่อ	ด้านการจัดการองค์กรดิจิทัล	$\bar{X}$	S.D.	แปลค่า
กลยุทธ์ดิจิทัล (Digital Strategy)				
OV1	การกำหนดและสื่อสารกลยุทธ์ดิจิทัลไปยังทุกหน่วยงานในองค์กรอย่างชัดเจน	3.97	0.78	มาก
OV2	กระบวนการวัดผลความสำเร็จของกลยุทธ์ผ่านตัวชี้วัดที่เชื่อมโยงกับพันธกิจองค์กร	3.88	0.82	มาก
OV3	คณะกรรมการกำกับดูแลดิจิทัล	3.89	0.80	มาก
OV4	การจัดสรรคงบประมาณและประเมินผลตอบแทนการลงทุนของโครงการ AI และโครงสร้างพื้นฐานดิจิทัลอย่างเป็นระบบ	3.93	0.83	มาก

ตัวย่อ	ด้านการจัดการองค์กรดิจิทัล	$\bar{X}$	S.D.	แปลค่า
ค่าเฉลี่ย		3.92	0.80	มาก
โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure)				
TI1	การลงทุนในโครงสร้างพื้นฐานเทคโนโลยีเพื่อรองรับการเติบโตในระยะ 3–5 ปีข้างหน้า	4.01	0.81	มาก
TI2	แผนบริหารความต่อเนื่องทางธุรกิจ เพื่อให้ระบบ AI ทำงานต่อได้ในภาวะวิกฤต	3.87	0.81	มาก
TI3	ระบบสำรองข้อมูลและศูนย์ข้อมูล เพื่อป้องกันการสูญเสียข้อมูล	3.76	0.79	มาก
TI4	การปรับปรุงและอัปเกรดเทคโนโลยีให้สอดคล้องกับนวัตกรรมดิจิทัลสมัยใหม่อย่างต่อเนื่อง	4.13	0.78	มาก
ค่าเฉลี่ย		3.94	0.80	มาก
การจัดการข้อมูล (Data Management)				
DM1	การบริหารจัดการข้อมูลให้เป็นสินทรัพย์หลักขององค์กร	3.89	0.81	มาก
DM2	การพัฒนาและบำรุงรักษาคลังข้อมูลเพื่อรองรับการทำงานของปัญญาประดิษฐ์	3.87	0.80	มาก
DM3	ใช้เทคโนโลยีดิจิทัลเพิ่มประสิทธิภาพการทำงานร่วมกันระหว่างหน่วยงาน	3.84	0.77	มาก
DM4	มาตรการควบคุมคุณภาพและความถูกต้องของข้อมูล เพื่อการตัดสินใจที่แม่นยำ	4.07	0.80	มาก
ค่าเฉลี่ย		3.92	0.80	มาก
กระบวนการอัตโนมัติ (Process Automation)				
PA1	การใช้ระบบอัตโนมัติในกระบวนการภายในเพื่อลดภาระงานบริหาร	3.71	0.81	มาก
PA2	การประเมินและปรับปรุงประสบการณ์ดิจิทัลของนักศึกษาและบุคลากรอย่างต่อเนื่อง	3.90	0.81	มาก
PA3	การบูรณาการระบบอัตโนมัติเข้ากับระบบสารสนเทศหลักขององค์กร	3.77	0.77	มาก
PA4	การติดตามผลลัพธ์จากการปรับใช้กระบวนการอัตโนมัติเพื่อเพิ่มประสิทธิภาพการดำเนินงาน	3.88	0.85	มาก
ค่าเฉลี่ย		3.82	0.81	มาก
ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)				
CB1	การรวมความปลอดภัยตั้งแต่ต้นทางของทุกโครงการดิจิทัล	3.90	0.77	มาก
CB2	การสื่อสารความเสี่ยงไซเบอร์ต่อผู้บริหารในรูปผลกระทบทางธุรกิจ	3.79	0.80	มาก
CB3	การประเมินช่องโหว่และทดสอบการเจาะระบบอย่างต่อเนื่อง	3.95	0.82	มาก
CB4	การจัดทำรายงานสถานะความปลอดภัยไซเบอร์และแผนการปรับปรุงอย่างเป็นระบบ	3.89	0.78	มาก

ตัวย่อ	ด้านการจัดการองค์กรดิจิทัล	$\bar{X}$	S.D.	แปลค่า
ค่าเฉลี่ย		3.88	0.79	มาก
ค่าเฉลี่ยรวม		3.90	0.80	มาก

จากตารางที่ 4-9 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล โดยรวม มีค่าเฉลี่ยอยู่ในระดับมาก ($\bar{X}$ = 3.90, S.D. = 0.80) โดยโครงสร้างพื้นฐานเทคโนโลยี มีค่าเฉลี่ยสูงที่สุด รองลงมา คือ กลยุทธ์ดิจิทัล การจัดการข้อมูล ความมั่นคงปลอดภัยทางไซเบอร์ และกระบวนการอัตโนมัติ ตามลำดับ สรุปผลรายด้านดังนี้

กลยุทธ์ดิจิทัล โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.92, S.D. = 0.80) เมื่อพิจารณารายข้อ พบว่า การกำหนดและสื่อสารกลยุทธ์ดิจิทัลไปยังทุกหน่วยงานในองค์กรอย่างชัดเจน มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 3.97, S.D. = 0.78) รองลงมา คือ การจัดสรรคงบประมาณและประเมินผลตอบแทนการลงทุนของโครงการ AI และโครงสร้างพื้นฐานดิจิทัลอย่างเป็นระบบ ($\bar{x}$ = 3.93, S.D. = 0.83) คณะกรรมการกำกับดูแลดิจิทัล ($\bar{x}$ = 3.89, S.D. = 0.80) และกระบวนการวัดผลความสำเร็จของกลยุทธ์ผ่านตัวชี้วัดที่เชื่อมโยงกับพันธกิจองค์กร ($\bar{x}$ = 3.88, S.D. = 0.82) ตามลำดับ

โครงสร้างพื้นฐานเทคโนโลยี โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.94, S.D. = 0.80) เมื่อพิจารณารายข้อ พบว่า การปรับปรุงและอัปเกรดเทคโนโลยีให้สอดคล้องกับนวัตกรรมดิจิทัลสมัยใหม่อย่างต่อเนื่อง มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.13, S.D. = 0.78) รองลงมา คือ การลงทุนในโครงสร้างพื้นฐานเทคโนโลยีเพื่อรองรับการเติบโตในระยะ 3–5 ปีข้างหน้า ($\bar{x}$ = 4.01, S.D. = 0.81) แผนบริหารความต่อเนื่องทางธุรกิจ เพื่อให้ระบบ AI ทำงานต่อได้ในภาวะวิกฤต ($\bar{x}$ = 3.87, S.D. = 0.81) และระบบสำรองข้อมูลและศูนย์ข้อมูล เพื่อป้องกันการสูญเสียข้อมูล ($\bar{x}$ = 3.76, S.D. = 0.79) ตามลำดับ

การจัดการข้อมูล โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.92, S.D. = 0.80) เมื่อพิจารณารายข้อ พบว่า มาตรการควบคุมคุณภาพและความถูกต้องของข้อมูล เพื่อการตัดสินใจที่แม่นยำ มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.07, S.D. = 0.80) รองลงมา คือ การบริหารจัดการข้อมูลให้เป็นสินทรัพย์หลักขององค์กร ($\bar{x}$ = 3.89, S.D. = 0.81) การพัฒนาและบำรุงรักษาคลังข้อมูลเพื่อรองรับการทำงานของปัญญาประดิษฐ์ ($\bar{x}$ = 3.87, S.D. = 0.80) และการใช้เทคโนโลยีดิจิทัลเพิ่มประสิทธิภาพการทำงานร่วมกันระหว่างหน่วยงาน ($\bar{x}$ = 3.84, S.D. = 0.77) ตามลำดับ

กระบวนการอัตโนมัติ โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.82, S.D. = 0.81) เมื่อพิจารณารายข้อ พบว่า การประเมินและปรับปรุงประสบการณ์ดิจิทัลของนักศึกษาและบุคลากรอย่างต่อเนื่อง มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 3.90, S.D. = 0.81) รองลงมา คือ การติดตามผลลัพธ์จากการปรับใช้กระบวนการ

อัตโนมัติเพื่อเพิ่มประสิทธิภาพการดำเนินงาน ($\bar{X}$ = 3.88, S.D. = 0.85) การบูรณาการระบบอัตโนมัติเข้ากับระบบสารสนเทศหลักขององค์กร ($\bar{X}$ = 3.77, S.D. = 0.77) และการใช้ระบบอัตโนมัติในกระบวนการภายในเพื่อลดภาระงานบริหาร ($\bar{X}$ = 3.71, S.D. = 0.81) ตามลำดับ

ความมั่นคงปลอดภัยทางไซเบอร์ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.88, S.D. = 0.79) เมื่อพิจารณารายข้อ พบว่า การประเมินช่องโหว่และทดสอบการเจาะระบบอย่างต่อเนื่อง มีค่าเฉลี่ยสูงสุด ($\bar{X}$ = 3.95, S.D. = 0.82) รองลงมา คือ การรวมความปลอดภัยตั้งแต่ต้นทางของทุกโครงการดิจิทัล ($\bar{X}$ = 3.90, S.D. = 0.77) การจัดทำรายงานสถานะความปลอดภัยไซเบอร์และแผนการปรับปรุงอย่างเป็นระบบ ($\bar{X}$ = 3.89, S.D. = 0.78) และการสื่อสารความเสี่ยงไซเบอร์ต่อผู้บริหารในรูปผลกระทบทางธุรกิจ ($\bar{X}$ = 3.79, S.D. = 0.80) ตามลำดับ

4.1.3.5 ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการวิเคราะห์ความคิดเห็นต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ประกอบด้วย การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ กรอบการทำงานเชิงสถาปัตยกรรมการออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ความสามารถในการปรับตัวต่อการเปลี่ยนแปลง ความสามารถในการรับมือภัยคุกคามและความเสี่ยง และจริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ มีผลวิเคราะห์ ดังนี้

ตารางที่ 4-10 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ โดยรวม

ตัวย่อ	ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	$\bar{X}$	S.D.	แปลค่า
AIA	สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (Artificial Intelligence Enterprise Architecture)			
EI	การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์	3.83	0.90	มาก
AF	กรอบการทำงานเชิงสถาปัตยกรรม	3.84	0.94	มาก
AS	การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์	3.84	0.98	มาก
AD	การปรับตัวต่อการเปลี่ยนแปลง	3.87	0.88	มาก
TR	การรับมือภัยคุกคามและความเสี่ยง	3.88	0.94	มาก
ER	จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์	3.96	0.86	มาก
ค่าเฉลี่ยรวม		3.87	0.92	มาก

จากตารางที่ 4-10 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

โดยรวม พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมาก โดยมีค่าเฉลี่ยเท่ากับ 3.87 และมีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.92 แสดงให้เห็นว่าผู้ตอบแบบสอบถามมีความคิดเห็นสอดคล้องกันในระดับค่อนข้างสูง เมื่อพิจารณาเป็นรายด้าน พบว่า จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ มีค่าเฉลี่ยสูงที่สุด ($\bar{X}$ = 3.96, S.D. = 0.86) อยู่ในระดับมาก รองลงมา คือ ความสามารถในการรับมือภัยคุกคามและความเสี่ยง มีค่าเฉลี่ย ($\bar{X}$ = 3.88, S.D. = 0.94) อยู่ในระดับมาก ความสามารถในการปรับตัวต่อการเปลี่ยนแปลง มีค่าเฉลี่ย ($\bar{X}$ = 3.87, S.D. = 0.88) อยู่ในระดับมาก กรอบการทำงานเชิงสถาปัตยกรรม และการออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ มีค่าเฉลี่ย ($\bar{X}$ = 3.84, S.D. = 0.94, 0.98) อยู่ในระดับมาก และการบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ ค่าเฉลี่ย ($\bar{X}$ = 3.83, S.D. = 0.90) อยู่ในระดับมาก ตามลำดับ

ตารางที่ 4-11 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ โดยรวม

ตัวย่อ	ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	$\bar{X}$	S.D.	แปลค่า
การบูรณาการสถาปัตยกรรมองค์กร และปัญญาประดิษฐ์ (EA–AI Integration)				
EI1	การบูรณาการการใช้ปัญญาประดิษฐ์เข้ากับสถาปัตยกรรมองค์กรอย่างเป็นระบบ	3.79	0.88	มาก
EI2	โครงสร้างสถาปัตยกรรมองค์กรของสถาบันสนับสนุนการนำปัญญาประดิษฐ์ไปใช้ในกระบวนการหลักได้อย่างเหมาะสม	3.70	0.90	มาก
EI3	การพัฒนาปัญญาประดิษฐ์ของสถาบันสอดคล้องกับแผนสถาปัตยกรรมองค์กรในภาพรวม	3.75	0.93	มาก
EI4	การบูรณาการสถาปัตยกรรมองค์กร และปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพและความยืดหยุ่นในการดำเนินงานของสถาบัน	4.06	0.91	มาก
ค่าเฉลี่ย		3.83	0.90	มาก
กรอบการทำงานเชิงสถาปัตยกรรม (Architectural Framework)				
AF1	กรอบการทำงานเชิงสถาปัตยกรรมที่ชัดเจนสำหรับการพัฒนาและใช้งานปัญญาประดิษฐ์	3.64	1.03	มาก
AF2	สามารถกำหนดทิศทางและมาตรฐานของระบบปัญญาประดิษฐ์ได้อย่างเหมาะสม	3.93	0.88	มาก
AF3	ลดความซ้ำซ้อนและความซับซ้อนของระบบสารสนเทศ	3.93	0.87	มาก
AF4	สามารถปรับปรุงและพัฒนาให้สอดคล้องกับเทคโนโลยีปัญญาประดิษฐ์ที่เปลี่ยนแปลงได้	3.85	0.97	มาก

ตัวย่อ	ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	$\bar{X}$	S.D.	แปลค่า
ค่าเฉลี่ย		3.84	0.94	มาก
การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ (AI-driven Information System Design & Development)				
AS1	ระบบสารสนเทศของสถาบันถูกออกแบบให้ใช้ปัญญาประดิษฐ์ เพื่อเพิ่มประสิทธิภาพการทำงาน	3.72	1.07	มาก
AS2	การพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ช่วยสนับสนุนการตัดสินใจของผู้บริหารและผู้ปฏิบัติงาน	4.02	0.88	มาก
AS3	ระบบปัญญาประดิษฐ์สามารถเชื่อมโยงและทำงานร่วมกับระบบสารสนเทศเดิมได้อย่างราบรื่น	3.61	1.11	มาก
AS4	การออกแบบระบบสารสนเทศด้วยปัญญาประดิษฐ์ ที่คำนึงถึงความปลอดภัยและความน่าเชื่อถือของข้อมูล	3.99	0.87	มาก
ค่าเฉลี่ย		3.84	0.98	มาก
การปรับตัวต่อการเปลี่ยนแปลง (Adaptability & Agility)				
AD1	สามารถปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยีได้รวดเร็ว	3.84	0.86	มาก
AD2	ระบบปัญญาประดิษฐ์สนับสนุนการปรับปรุงกระบวนการทำงานให้มีความคล่องตัวมากขึ้น	3.78	0.96	มาก
AD3	สามารถปรับเปลี่ยนหรือขยายระบบปัญญาประดิษฐ์ได้ตามความต้องการในอนาคต	3.93	0.88	มาก
AD4	ตอบสนองต่อการเปลี่ยนแปลงด้านนโยบายและสภาพแวดล้อมได้อย่างมีประสิทธิภาพ	3.93	0.82	มาก
ค่าเฉลี่ย		3.87	0.88	มาก
การรับมือภัยคุกคามและความเสี่ยง (Threat & Risk Responsiveness)				
TR1	สนับสนุนการตรวจจับภัยคุกคามทางดิจิทัลได้อย่างรวดเร็ว	3.67	1.04	มาก
TR2	ระบบปัญญาประดิษฐ์มีบทบาทในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ	4.07	0.89	มาก
TR3	สามารถตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ	3.78	0.94	มาก
TR4	การใช้ปัญญาประดิษฐ์ช่วยเพิ่มความสามารถในการป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์	3.99	0.90	มาก
ค่าเฉลี่ย		3.88	0.94	มาก
จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ (AI Ethics and Responsibility)				
ER1	การกำหนดหลักจริยธรรมในการพัฒนาและใช้ปัญญาประดิษฐ์อย่างชัดเจน	3.81	0.89	มาก

ตัวย่อ	ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	$\bar{X}$	S.D.	แปลค่า
ER2	ระบบปัญญาประดิษฐ์ถูกออกแบบให้โปร่งใสและสามารถอธิบายผลลัพธ์ได้	4.04	0.83	มาก
ER3	มาตรการลดอคติในข้อมูลและโมเดลปัญญาประดิษฐ์	3.96	0.90	มาก
ER4	การอบรมและส่งเสริมความรู้เรื่องจริยธรรมและความรับผิดชอบในการใช้ปัญญาประดิษฐ์	4.04	0.83	มาก
ค่าเฉลี่ย		3.96	0.86	มาก
ค่าเฉลี่ยรวม		3.87	0.92	มาก

จากตารางที่ 4-11 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์โดยรวม มีค่าเฉลี่ยอยู่ในระดับมาก ($\bar{X}$ = 3.87, S.D. = 0.92) โดยการบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ กรอบการทำงานเชิงสถาปัตยกรรม การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ความสามารถในการปรับตัวต่อการเปลี่ยนแปลง ความสามารถในการรับมือภัยคุกคามและความเสี่ยง และจริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ ตามลำดับ สรุปผลรายด้านดังนี้

การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.83, S.D. = 0.90) เมื่อพิจารณารายข้อ พบว่า การบูรณาการสถาปัตยกรรมองค์กร และปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพและความยืดหยุ่นในการดำเนินงานของสถาบัน มีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.06, S.D. = 0.91) รองลงมา คือ การบูรณาการการใช้ปัญญาประดิษฐ์เข้ากับสถาปัตยกรรมองค์กรอย่างเป็นระบบ ($\bar{x}$ = 3.79, S.D. = 0.88) การพัฒนาปัญญาประดิษฐ์ของสถาบันสอดคล้องกับแผนสถาปัตยกรรมองค์กรในภาพรวม ($\bar{x}$ = 3.75, S.D. = 0.93) และโครงสร้างสถาปัตยกรรมองค์กรของสถาบันสนับสนุนการนำปัญญาประดิษฐ์ไปใช้ในกระบวนการหลักได้อย่างเหมาะสม ($\bar{x}$ = 3.70, S.D. = 0.90) ตามลำดับ

กรอบการทำงานเชิงสถาปัตยกรรม โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.84, S.D. = 0.94) เมื่อพิจารณารายข้อ พบว่า สามารถกำหนดทิศทางและมาตรฐานของระบบปัญญาประดิษฐ์ได้อย่างเหมาะสม และลดความซ้ำซ้อนและความซับซ้อนของระบบสารสนเทศ ค่าเฉลี่ยสูงสุด ($\bar{x}$ = 3.93, S.D. = 0.88, 0.87) รองลงมา คือ สามารถปรับปรุงและพัฒนาให้สอดคล้องกับเทคโนโลยีปัญญาประดิษฐ์ที่เปลี่ยนแปลงได้ ($\bar{x}$ = 3.85, S.D. = 0.97) และกรอบการทำงานเชิงสถาปัตยกรรมที่ชัดเจนสำหรับการพัฒนาและใช้งานปัญญาประดิษฐ์ ($\bar{x}$ = 3.64, S.D. = 1.03) ตามลำดับ

การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.84, S.D. = 0.98) เมื่อพิจารณารายข้อ พบว่า การพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ช่วยสนับสนุนการตัดสินใจของผู้บริหารและผู้ปฏิบัติงาน ค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.02, S.D. = 0.88) รองลงมา คือ การออกแบบระบบสารสนเทศด้วยปัญญาประดิษฐ์ที่คำนึงถึงความปลอดภัยและความน่าเชื่อถือของข้อมูล ($\bar{X}$ = 3.99, S.D. = 0.87) ระบบสารสนเทศของสถาบันถูกออกแบบให้ใช้ปัญญาประดิษฐ์ เพื่อเพิ่มประสิทธิภาพการทำงาน ($\bar{X}$ = 3.72, S.D. = 1.07) และระบบปัญญาประดิษฐ์สามารถเชื่อมโยงและทำงานร่วมกับระบบสารสนเทศเดิมได้อย่างราบรื่น ($\bar{X}$ = 3.61, S.D. = 1.11) ตามลำดับ

การปรับตัวต่อการเปลี่ยนแปลง โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.87, S.D. = 0.88) เมื่อพิจารณารายข้อ พบว่า สามารถปรับเปลี่ยนหรือขยายระบบปัญญาประดิษฐ์ได้ตามความต้องการในอนาคต และตอบสนองต่อการเปลี่ยนแปลงด้านนโยบายและสภาพแวดล้อมได้อย่างมีประสิทธิภาพ ค่าเฉลี่ยสูงสุด ($\bar{X}$ = 3.93, S.D. = 0.88, 0.82) รองลงมา คือ สามารถปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยีได้รวดเร็ว ($\bar{X}$ = 3.84, S.D. = 0.86) และระบบปัญญาประดิษฐ์สนับสนุนการปรับปรุงกระบวนการทำงานให้มีความคล่องตัวมากขึ้น ($\bar{X}$ = 3.78, S.D. = 0.96) ตามลำดับ

การรับมือภัยคุกคามและความเสี่ยง โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.88, S.D. = 0.94) เมื่อพิจารณารายข้อ พบว่า ระบบปัญญาประดิษฐ์มีบทบาทในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ ค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.07, S.D. = 0.89) รองลงมา คือ การใช้ปัญญาประดิษฐ์ช่วยเพิ่มความสามารถในการป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์ ($\bar{X}$ = 3.99, S.D. = 0.90) สามารถตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.78, S.D. = 0.94) และสนับสนุนการตรวจจับภัยคุกคามทางดิจิทัลได้อย่างรวดเร็ว ($\bar{X}$ = 3.67, S.D. = 1.04) ตามลำดับ

จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.96, S.D. = 0.86) เมื่อพิจารณารายข้อ พบว่า ระบบปัญญาประดิษฐ์ถูกออกแบบให้โปร่งใสและสามารถอธิบายผลลัพธ์ได้ และการอบรมและส่งเสริมความรู้เรื่องจริยธรรมและความรับผิดชอบในการใช้ปัญญาประดิษฐ์ ค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.04, S.D. = 0.83) รองลงมา มาตรการลดอคติในข้อมูลและโมเดลปัญญาประดิษฐ์ ($\bar{X}$ = 3.96, S.D. = 0.90) และการกำหนดหลักจริยธรรมในการพัฒนาและใช้ปัญญาประดิษฐ์อย่างชัดเจน ($\bar{X}$ = 3.81, S.D. = 0.89) ตามลำดับ

4.1.3.5 ด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการวิเคราะห์ความคิดเห็นต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการภูมิคุ้มกันดิจิทัล ประกอบด้วย การตรวจจับภัยคุกคามทาง

ไซเบอร์ การตอบสนองต่อเหตุการณ์ทางไซเบอร์ การประเมินและจัดการความเสี่ยง การปกป้องข้อมูลและความเป็นส่วนตัว การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย และนโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ มีผลวิเคราะห์ ดังนี้

ตารางที่ 4-12 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการภูมิคุ้มกันดิจิทัล โดยรวม

ตัวย่อ	ด้านการจัดการภูมิคุ้มกันดิจิทัล	$\bar{X}$	S.D.	แปลค่า
DIM	การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)			
CD	การตรวจจับภัยคุกคามทางไซเบอร์	3.88	0.83	มาก
IR	การตอบสนองต่อเหตุการณ์ทางไซเบอร์	3.89	0.86	มาก
RA	การประเมินและจัดการความเสี่ยง	3.94	0.84	มาก
DP	การปกป้องข้อมูลและความเป็นส่วนตัว	3.97	0.81	มาก
ST	การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย	3.93	0.82	มาก
SC	นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ	3.97	0.77	มาก
	ค่าเฉลี่ยรวม	3.93	0.82	มาก

จากตารางที่ 4-12 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการภูมิคุ้มกันดิจิทัล โดยรวม พบว่าผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมาก โดยมีค่าเฉลี่ยเท่ากับ 3.93 และมีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.82 แสดงให้เห็นว่าผู้ตอบแบบสอบถามมีความคิดเห็นสอดคล้องกันในระดับค่อนข้างสูง เมื่อพิจารณาเป็นรายด้าน พบว่า การปกป้องข้อมูลและความเป็นส่วนตัว และนโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ มีค่าเฉลี่ยสูงที่สุด ($\bar{x}$ = 3.97, S.D. = 0.81, 0.77) อยู่ในระดับมาก รองลงมาคือ การประเมินและจัดการความเสี่ยง มีค่าเฉลี่ย ($\bar{x}$ = 3.94, S.D. = 0.84) อยู่ในระดับมาก การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย มีค่าเฉลี่ย ($\bar{x}$ = 3.93, S.D. = 0.82) อยู่ในระดับมาก การตอบสนองต่อเหตุการณ์ทางไซเบอร์ มีค่าเฉลี่ย ($\bar{x}$ = 3.89, S.D. = 0.86) อยู่ในระดับมาก และการตรวจจับภัยคุกคามทางไซเบอร์ ค่าเฉลี่ย ($\bar{x}$ = 3.88, S.D. = 0.83) อยู่ในระดับมาก ตามลำดับ

ตารางที่ 4-13 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐานปัจจัยที่มีอิทธิพลด้านการจัดการภูมิคุ้มกันดิจิทัลโดยรวม

ตัวย่อ	ด้านการจัดการภูมิคุ้มกันดิจิทัล	$\bar{X}$	S.D.	แปลค่า
การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection)				
CD1	การทดสอบเจาะระบบ และตรวจสอบโค้ดของแอปพลิเคชันเพื่อค้นหาช่องโหว่อย่างสม่ำเสมอ	3.75	0.95	มาก
CD2	การประเมินประสิทธิภาพของมาตรการป้องกันภัยไซเบอร์อย่างต่อเนื่องเพื่อลดความเสี่ยง	4.02	0.78	มาก
CD3	ใช้เทคโนโลยี AI หรือ Machine Learning ในการตรวจจับพฤติกรรมที่ผิดปกติในระบบเครือข่าย	3.83	0.84	มาก
CD4	ระบบแจ้งเตือนภัยคุกคามแบบเรียลไทม์ เพื่อให้ทีมสามารถตอบสนองได้อย่างรวดเร็ว	3.90	0.77	มาก
ค่าเฉลี่ย		3.88	0.83	มาก
การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response)				
IR1	แผนขั้นตอนการตอบสนองเหตุการณ์ทางไซเบอร์ที่ครอบคลุมทุกระบบ	3.95	0.80	มาก
IR2	แนวทางเฉพาะในการจัดการเหตุการณ์ที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์	3.78	0.87	มาก
IR3	การกำหนดบทบาทและความรับผิดชอบของทีม IR อย่างชัดเจน	4.02	0.85	มาก
IR4	การทดสอบจำลองเหตุการณ์โจมตีเพื่อประเมินความพร้อมของบุคลากรและระบบ	3.79	0.92	มาก
ค่าเฉลี่ย		3.89	0.86	มาก
การประเมินและจัดการความเสี่ยง (Risk Assessment and Management)				
RA1	การประเมินและจัดการความเสี่ยงทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง	4.02	0.85	มาก
RA2	ระบบบริหารจัดการการเปลี่ยนแปลงของ IT และ AI อย่างเป็นระบบ	3.89	0.82	มาก
RA3	การบริหารจัดการแพตช์ (Patch Management) และอัปเดตซอฟต์แวร์อย่างรวดเร็วและมีประสิทธิภาพ	3.83	0.85	มาก
RA4	การจัดทำรายงานความเสี่ยงและความปลอดภัยทางไซเบอร์ที่ชัดเจนสำหรับผู้บริหาร	4.02	0.87	มาก
ค่าเฉลี่ย		3.94	0.84	มาก
การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy)				

ตัวย่อ	ด้านการจัดการภูมิคุ้มกันดิจิทัล	$\bar{X}$	S.D.	แปลค่า
DP1	นโยบายและมาตรการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย PDPA	3.92	0.82	มาก
DP2	การเข้ารหัสและควบคุมการเข้าถึงข้อมูลเพื่อป้องกันการรั่วไหลหรือการโจมตี	4.04	0.79	มาก
DP3	การบริหารจัดการความเสี่ยงของข้อมูลที่ใช้โดยระบบปัญญาประดิษฐ์อย่างเป็นระบบ	3.87	0.82	มาก
DP4	การตรวจสอบและประเมินการจัดการข้อมูลอย่างสม่ำเสมอเพื่อรักษาความเป็นส่วนตัวของผู้ใช้	4.05	0.82	มาก
	ค่าเฉลี่ย	3.97	0.81	มาก
การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย (Security Awareness Training)				
ST1	การจัดฝึกอบรมภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับสถาบันอุดมศึกษาอย่างสม่ำเสมอ	3.91	0.80	มาก
ST2	บุคลากรได้รับการอบรมและอัปเดตความรู้ด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง	4.03	0.81	มาก
ST3	การจัดกิจกรรมหรือการรณรงค์สร้างจิตสำนึกด้านความปลอดภัยดิจิทัลภายในองค์กร	3.95	0.82	มาก
ST4	ระบบประเมินผลหลังการฝึกอบรมเพื่อวัดผลการเรียนรู้และการนำไปใช้จริงของผู้เข้าร่วม	3.82	0.84	มาก
	ค่าเฉลี่ย	3.93	0.82	มาก
นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance)				
SC1	นโยบายและข้อบังคับด้านความปลอดภัยสำหรับ AI และ Cloud	3.99	0.75	มาก
SC2	ผู้บริหารมีการทบทวนและประเมินสถานะความปลอดภัยของระบบอย่างสม่ำเสมอ	3.88	0.78	มาก
SC3	จัดทำสัญญากับผู้ให้บริการภายนอก พร้อมข้อกำหนดด้านความปลอดภัย	4.09	0.78	มาก
SC4	ใช้เครื่องมืออัตโนมัติในการตรวจสอบและบังคับใช้ข้อกำหนดด้านความปลอดภัย	3.92	0.79	มาก
	ค่าเฉลี่ย	3.97	0.77	มาก
	ค่าเฉลี่ยรวม	3.93	0.82	มาก

จากตารางที่ 4-13 ผลการวิเคราะห์ความคิดเห็นที่มีต่อปัจจัยที่มีอิทธิพลสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ด้านการจัดการภูมิคุ้มกันดิจิทัล โดยรวม มีค่าเฉลี่ยอยู่ในระดับมาก ($\bar{X}$ = 3.93, S.D. = 0.82) โดยการตรวจจับภัยคุกคามทางไซเบอร์ การ

ตอบสนองต่อเหตุการณ์ทางไซเบอร์ การประเมินและจัดการความเสี่ยง การปกป้องข้อมูลและความเป็นส่วนตัว การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัยและนโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ ตามลำดับ สรุปผลรายด้านดังนี้

การตรวจจับภัยคุกคามทางไซเบอร์ โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.88, S.D. = 0.83) เมื่อพิจารณารายข้อ พบว่า การประเมินประสิทธิภาพของมาตรการป้องกันภัยไซเบอร์อย่างต่อเนื่องเพื่อลดความเสี่ยง ค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.02, S.D. = 0.78) รองลงมา คือ ระบบแจ้งเตือนภัยคุกคามแบบเรียลไทม์ เพื่อให้ทีมสามารถตอบสนองได้อย่างรวดเร็ว ($\bar{x}$ = 3.90, S.D. = 0.77) ใช้เทคโนโลยี AI หรือ Machine Learning ในการตรวจจับพฤติกรรมที่ผิดปกติในระบบเครือข่าย ($\bar{x}$ = 3.83, S.D. = 0.84) และการทดสอบเจาะระบบ และตรวจสอบโค้ดของแอปพลิเคชันเพื่อค้นหาช่องโหว่อย่างสม่ำเสมอ ($\bar{x}$ = 3.75, S.D. = 0.95) ตามลำดับ

การตอบสนองต่อเหตุการณ์ทางไซเบอร์ โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.89, S.D. = 0.86) เมื่อพิจารณารายข้อ พบว่า การกำหนดบทบาทและความรับผิดชอบของทีม IR อย่างชัดเจน ค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.02, S.D. = 0.85) รองลงมา คือ แผนขั้นตอนการตอบสนองเหตุการณ์ทางไซเบอร์ที่ครอบคลุมทุกระบบ ($\bar{x}$ = 3.95, S.D. = 0.80) การทดสอบจำลองเหตุการณ์โจมตีเพื่อประเมินความพร้อมของบุคลากรและระบบ ($\bar{x}$ = 3.79, S.D. = 0.92) และแนวทางเฉพาะในการจัดการเหตุการณ์ที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์ ($\bar{x}$ = 3.78, S.D. = 0.87) ตามลำดับ

การประเมินและจัดการความเสี่ยง โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.94, S.D. = 0.84) เมื่อพิจารณารายข้อ พบว่า การประเมินและจัดการความเสี่ยงทางไซเบอร์อย่างเป็นระบบและต่อเนื่องและการจัดทำรายงานความเสี่ยงและความปลอดภัยทางไซเบอร์ที่ชัดเจนสำหรับผู้บริหาร ค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.02, S.D. = 0.85, 0.87) รองลงมา คือ ระบบบริหารจัดการการเปลี่ยนแปลงของ IT และ AI อย่างเป็นระบบ ($\bar{x}$ = 3.89, S.D. = 0.82) และการบริหารจัดการแพตช์ (Patch Management) และอัปเดตซอฟต์แวร์อย่างรวดเร็วและมีประสิทธิภาพ ($\bar{x}$ = 3.83, S.D. = 0.85) ตามลำดับ

การปกป้องข้อมูลและความเป็นส่วนตัว โดยรวมอยู่ในระดับมาก ($\bar{x}$ = 3.97, S.D. = 0.81) เมื่อพิจารณารายข้อ พบว่า การตรวจสอบและประเมินการจัดการข้อมูลอย่างสม่ำเสมอเพื่อรักษาความเป็นส่วนตัวของผู้ใช้ ค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.05, S.D. = 0.82) รองลงมา คือ การเข้ารหัสและควบคุมการเข้าถึงข้อมูลเพื่อป้องกันการรั่วไหลหรือการโจมตี ($\bar{x}$ = 4.04, S.D. = 0.79) นโยบายและมาตรการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย PDPA ($\bar{x}$ = 3.92, S.D. = 0.82) และการบริหารจัดการความเสี่ยงของข้อมูลที่ใช้โดยระบบปัญญาประดิษฐ์อย่างเป็นระบบ ($\bar{x}$ = 3.87, S.D. = 0.82) ตามลำดับ

การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.93, S.D. = 0.82) เมื่อพิจารณารายข้อ พบว่า บุคลากรได้รับการอบรมและอัปเดตความรู้ด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง ค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.03, S.D. = 0.81) รองลงมา คือ การจัดกิจกรรมหรือการรณรงค์สร้างจิตสำนึกด้านความปลอดภัยดิจิทัลภายในองค์กร ($\bar{X}$ = 3.95, S.D. = 0.82) การจัดฝึกอบรมภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับสถาบันอุดมศึกษาอย่างสม่ำเสมอ ($\bar{X}$ = 3.91, S.D. = 0.80) และระบบประเมินผลหลังการฝึกอบรมเพื่อวัดผลการเรียนรู้และการนำไปใช้จริงของผู้เข้าร่วม ($\bar{X}$ = 3.82, S.D. = 0.84) ตามลำดับ

นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.97, S.D. = 0.77) เมื่อพิจารณารายข้อ พบว่า จัดทำสัญญากับผู้ให้บริการภายนอกพร้อมข้อกำหนดด้านความปลอดภัย ค่าเฉลี่ยสูงสุด ($\bar{X}$ = 4.09, S.D. = 0.78) รองลงมา คือ นโยบายและข้อบังคับด้านความปลอดภัยสำหรับ AI และ Cloud ($\bar{X}$ = 3.99, S.D. = 0.75) ใช้เครื่องมืออัตโนมัติในการตรวจสอบและบังคับใช้ข้อกำหนดด้านความปลอดภัย ($\bar{X}$ = 3.92, S.D. = 0.79) และผู้บริหารมีการทบทวนและประเมินสถานะความปลอดภัยของระบบอย่างสม่ำเสมอ ($\bar{X}$ = 3.88, S.D. = 0.78) ตามลำดับ

4.1.4 ผลการวิเคราะห์องค์ประกอบเชิงยืนยันแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

การวิเคราะห์องค์ประกอบเชิงยืนยันของปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ตามแบบจำลองสมการโครงสร้าง (Structural Equation Model) โดยแบบจำลองโครงสร้างเต็มรูปแบบ (Full Path Mode) ประกอบด้วย ตัวแปรแฝง (Latent Variable) และตัวแปรเชิงสังเกต (Observed Variable) ดังนี้

ตัวแปรแฝงที่ 1 โครงสร้างองค์กร ประกอบด้วยตัวแปรสังเกต จำนวน 7 ตัว คือ 1) สถาปัตยกรรมธุรกิจ 2) สถาปัตยกรรมข้อมูล 3) สถาปัตยกรรมระบบแอปพลิเคชัน 4) สถาปัตยกรรมเทคโนโลยี 5) สถาปัตยกรรมด้านความมั่งคงปลอดภัย 6) สถาปัตยกรรมการบูรณาการ และ 7) สถาปัตยกรรมการกำกับดูแล

ตัวแปรแฝงที่ 2 เทคโนโลยีอัจฉริยะ ประกอบด้วยตัวแปรสังเกต จำนวน 4 ตัว คือ 1) การเรียนรู้ของเครื่อง 2) การเรียนรู้เชิงลึก 3) การประมวลผลภาษาธรรมชาติ และ 4) ความรู้เชิงพฤติกรรม

ตัวแปรแฝงที่ 3 ระบบภูมิคุ้มกันดิจิทัล ประกอบด้วยตัวแปรสังเกต จำนวน 6 ตัว คือ 1) การมองเห็นและเฝ้าระวัง 2) การตรวจจับภัยคุกคาม 3) การสืบสวนและวิเคราะห์ 4) การตอบสนองและ

การป้องกันเชิงรุก 5) ความทนทานและการฟื้นฟู และ 6) ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์

ตัวแปรแฝงที่ 4 การจัดการองค์กรดิจิทัล ประกอบด้วยตัวแปรสังเกต จำนวน 5 ตัว คือ 1) กลยุทธ์ดิจิทัล 2) โครงสร้างพื้นฐานเทคโนโลยี 3) การจัดการข้อมูล 4) กระบวนการอัตโนมัติ และ 5) ความมั่นคงปลอดภัยทางไซเบอร์

ตัวแปรแฝงที่ 5 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ประกอบด้วยตัวแปรสังเกต จำนวน 6 ตัว คือ 1. การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ 2 กรอบการทำงานเชิงสถาปัตยกรรม 3) การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ 4) การปรับตัวต่อการเปลี่ยนแปลง 5) การรับมือภัยคุกคามและความเสี่ยง และ6) จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์

ตัวแปรแฝงที่ 6 การจัดการภูมิคุ้มกันดิจิทัล ประกอบด้วยตัวแปรสังเกต จำนวน 6 ตัว คือ 1) การตรวจจับภัยคุกคามทางไซเบอร์ 2) การตอบสนองต่อเหตุการณ์ทางไซเบอร์ 3) การประเมินและจัดการความเสี่ยง 4) การปกป้องข้อมูลและความเป็นส่วนตัว 5) การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย และ 6) นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ

โดยผลลัพธ์ที่ได้จะต้องเป็นไปตามข้อตกลงทางสถิติ ดังนี้ 1) ค่าไคสแควร์ (Chi-square Value) ต้องไม่มีนัยสำคัญทางสถิติที่ระดับ .05 หรือ P > .05 2) ค่าไคสแควร์ (Chi-square Value) หารด้วย ระดับชั้นแห่งความเป็นอิสระ (Degree of freedom หรือ df) ต้องไม่เกิน 3 และ 3) ค่า Root Mean Square Error of Approximation หรือ RMSEA ต้องมีค่าน้อยกว่า 0.05 หรือไม่เกิน 0.08 (Avkiran, 2018)

สำหรับผลการวิเคราะห์องค์ประกอบและการศึกษาความสัมพันธ์เชิงเหตุผลตามแบบจำลองสมการโครงสร้างประสิทธิผลการดำเนินงานของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ปรากฏดังนี้

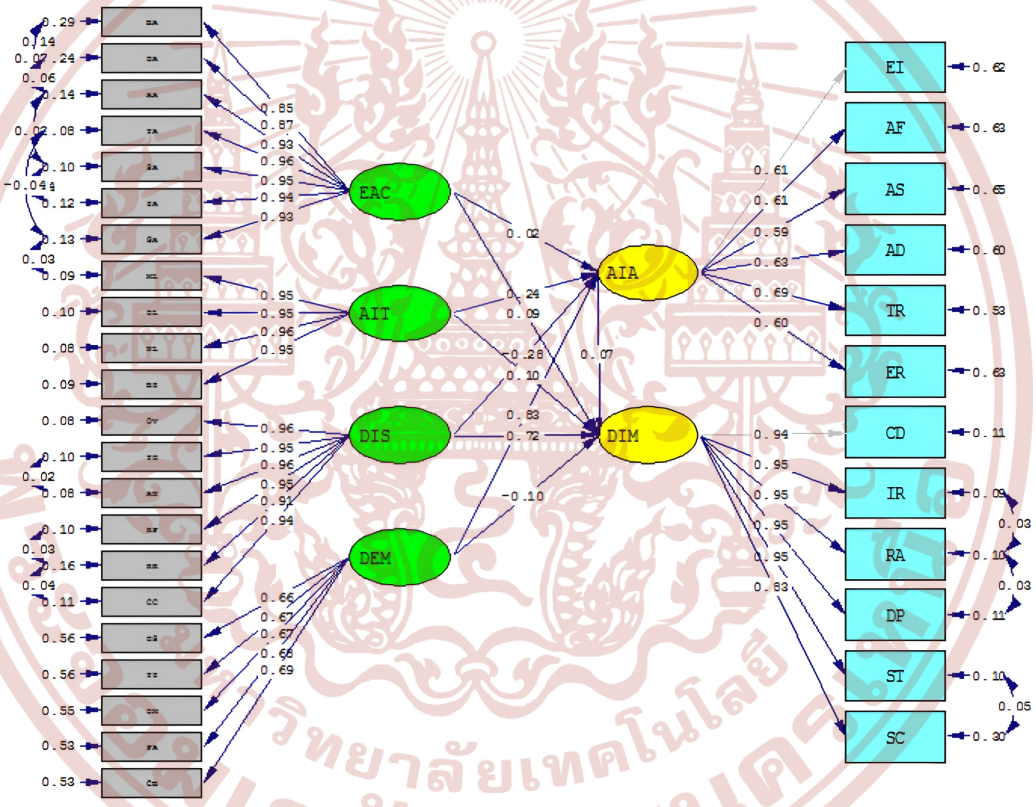
ตารางที่ 4-14 ผลการวิเคราะห์อิทธิพลทางตรง (Direct Effect) อิทธิพลทางอ้อม (Indirect Effect) และอิทธิพลรวม (Total Effect) ตามแบบจำลองสมการโครงสร้าง

Dep.V.	Indep.V	R-square	F	Path Coefficients		
				DE	IE	TT
AIA – สถาปัตยกรรมองค์กรปัญญาประดิษฐ์	EAC – โครงสร้างองค์กร	0.70	0.096	0.02	0.00	0.02
	AIT – เทคโนโลยีอัจฉริยะ			0.24	0.00	0.24
	DIS – ระบบภูมิคุ้มกันดิจิทัล			-0.28	0.00	-0.28
	DEM – การจัดการองค์กรดิจิทัล			0.83	0.00	0.83
DIM – การจัดการภูมิคุ้มกันดิจิทัล	EAC –โครงสร้างองค์กร	0.81	0.850	0.09	0.09	0.18

Dep.V.	Indep.V	R-square	F	Path Coefficients		
				DE	IE	TT
	AIT – เทคโนโลยีอัจฉริยะ			0.10	0.02	0.12
	DIS – ระบบภูมิคุ้มกันดิจิทัล			0.72	-0.02	0.70
	DEM – การจัดการองค์กรดิจิทัล			-0.10	0.06	-0.04
	AIA – สถาปัตยกรรมองค์กรปัญญาประดิษฐ์			0.07	0.00	0.07

* P < .05

Remark: Dep.V. = Dependent Variable, Indep.V. = Independent Variable, DE = Direct Effect, IE =Indirect Effect, and TT = Total Effect



Chi-Square = 517.17, df = 499, p-value = 0.27784, RMSEA = 0.012

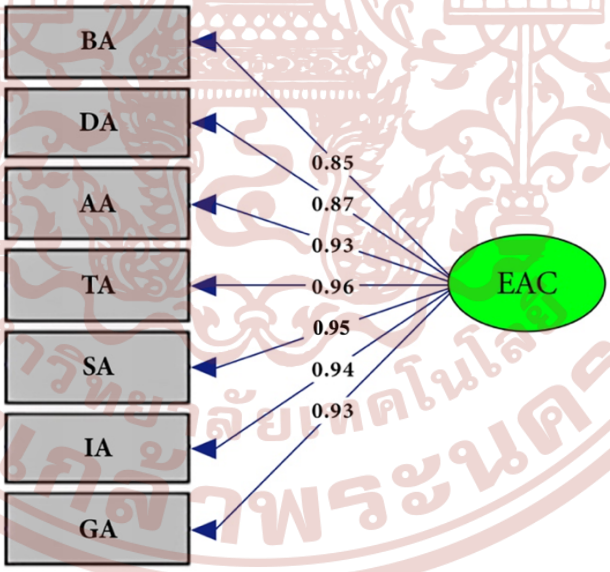
ภาพที่ 4-1 Full Path Model ความสัมพันธ์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

จากตารางที่ 4-14 และภาพที่ 4-1 ซึ่งเป็นแบบจำลองเต็มรูปแบบ Full Path Model ผลลัพธ์ที่ได้จากการวิเคราะห์ พบว่าแบบจำลองมีความสอดคล้องกับข้อมูลเชิงประจักษ์ในระดับดีมาก โดยมีค่า Chi-square เท่ากับ 517.17 ที่ระดับองศาอิสระ 499 (χ^2/df = 1.04) และมีค่า p-value เท่ากับ 0.27784 ซึ่งไม่มีนัยสำคัญทางสถิติ แสดงให้เห็นว่าแบบจำลองไม่แตกต่างจากข้อมูลเชิง

ประจักษ์ นอกจากนี้ ค่า RMSEA เท่ากับ 0.012 แสดงถึงความสอดคล้องในระดับยอดเยี่ยม สำหรับผลการวิจัยตามวัตถุประสงค์ข้อที่ 2 สรุปได้ดังนี้

การวิเคราะห์องค์ประกอบเชิงยืนยันของปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ตามแบบจำลองสมการโครงสร้าง (Structural Equation Model) โดยพิจารณาน้ำหนักองค์ประกอบ Completely Standardized Solution ตามเกณฑ์ที่ตั้งไว้ตั้งแต่ .50 ขึ้นไป เป็นองค์ประกอบสำคัญ (Crucial Component) พบว่า

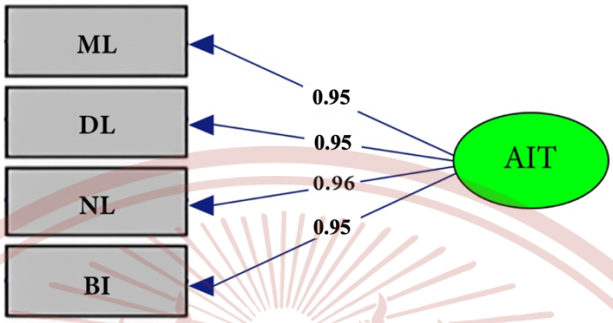
1. ตัวแปรแฝงด้านโครสร้างองค์กร พบว่าทั้ง 7 องค์ประกอบที่ใช้ในการศึกษาครั้งนี้เป็นองค์ประกอบสำคัญเชิงยืนยัน ได้แก่ 1) สถาปัตยกรรมธุรกิจ 2) สถาปัตยกรรมข้อมูล 3) สถาปัตยกรรมระบบแอปพลิเคชัน 4) สถาปัตยกรรมเทคโนโลยี 5) สถาปัตยกรรมด้านความมั่งคงปลอดภัย 6) สถาปัตยกรรมการบูรณาการ และ 7) สถาปัตยกรรมการกำกับดูแล โดยมีค่าน้ำหนักองค์ประกอบแบบ Completely Standardized Solution เป็น 0.85, 0.87, 0.93, 0.96, 0.95, 0.94 และ 0.93 ตามลำดับ ซึ่งเป็นไปตามสมมติฐานการวิจัยที่ตั้งไว้ ดังภาพที่ 4-2



ภาพที่ 4-2 องค์ประกอบสำคัญด้านโครงสร้างองค์กร

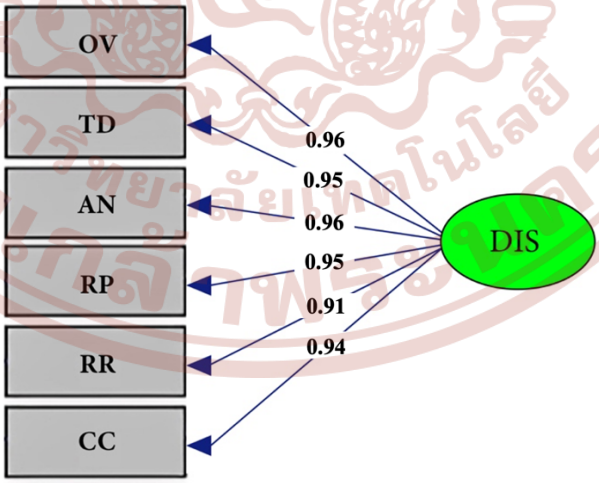
2. ตัวแปรแฝงด้านเทคโนโลยีอัจฉริยะ พบว่าทั้ง 4 องค์ประกอบที่ใช้ในการศึกษาครั้งนี้เป็นองค์ประกอบสำคัญเชิงยืนยัน ได้แก่ 1) การเรียนรู้ของเครื่อง 2) การเรียนรู้เชิงลึก 3) การประมวลผลภาษาธรรมชาติ และ 4) ความรู้เชิงพฤติกรรม โดยมีค่าน้ำหนักองค์ประกอบแบบ Completely

Standardized Solution เป็น 0.95, 0.95, 0.96 และ 0.95 ตามลำดับ ซึ่งเป็นไปตามสมมติฐานการวิจัยที่ตั้งไว้ ดังภาพที่ 4-3



ภาพที่ 4-3 องค์ประกอบสำคัญด้านเทคโนโลยีอัจฉริยะ

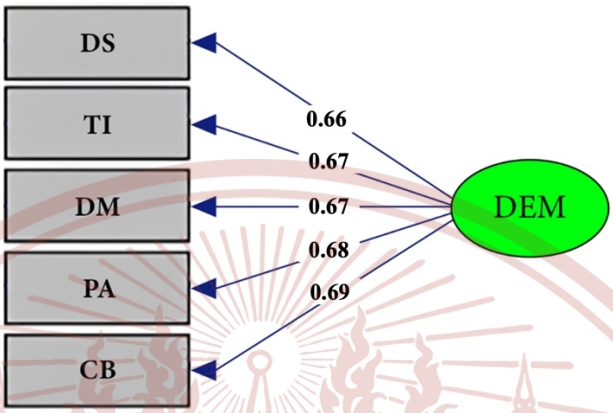
3. ตัวแปรแฝงด้านระบบภูมิคุ้มกันดิจิทัล พบว่าทั้ง 6 องค์ประกอบที่ใช้ในการศึกษาครั้งนี้เป็นองค์ประกอบสำคัญเชิงยืนยัน ได้แก่ 1) การมองเห็นและเฝ้าระวัง 2) การตรวจจับภัยคุกคาม 3) การสืบสวนและวิเคราะห์ 4) การตอบสนองและการป้องกันเชิงรุก 5) ความทนทานและการฟื้นฟู และ 6) ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ โดยมีค่าน้ำหนักองค์ประกอบแบบ Completely Standardized Solution เป็น 0.96, 0.95, 0.96, 0.95, 0.91 และ 0.94 ตามลำดับ ซึ่งเป็นไปตามสมมติฐานการวิจัยที่ตั้งไว้ ดังภาพที่ 4-4



ภาพที่ 4-4 องค์ประกอบสำคัญด้านระบบภูมิคุ้มกันดิจิทัล

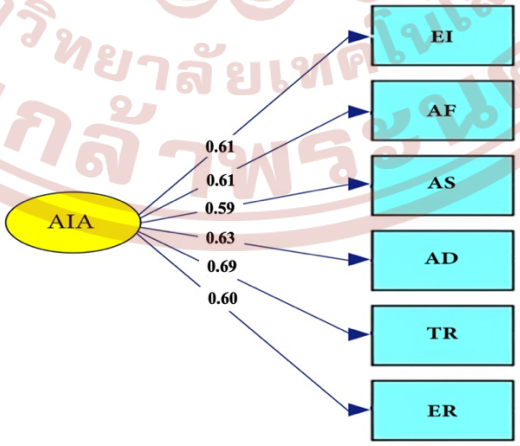
4. ตัวแปรแฝงด้านการจัดการองค์กรดิจิทัล พบว่าทั้ง 5 องค์ประกอบที่ใช้ในการศึกษาครั้งนี้เป็นองค์ประกอบสำคัญเชิงยืนยัน ได้แก่ 1) กลยุทธ์ดิจิทัล 2) โครงสร้างพื้นฐานเทคโนโลยี 3) การจัดการข้อมูล 4) กระบวนการอัตโนมัติ และ 5) ความมั่นคงปลอดภัยทางไซเบอร์ โดยมีค่าน้ำหนัก

องค์ประกอบแบบ Completely Standardized Solution เป็น 0.66, 0.67, 0.67, 0.68 และ 0.69 ตามลำดับ ซึ่งเป็นไปตามสมมติฐานการวิจัยที่ตั้งไว้ ดังภาพที่ 4-5



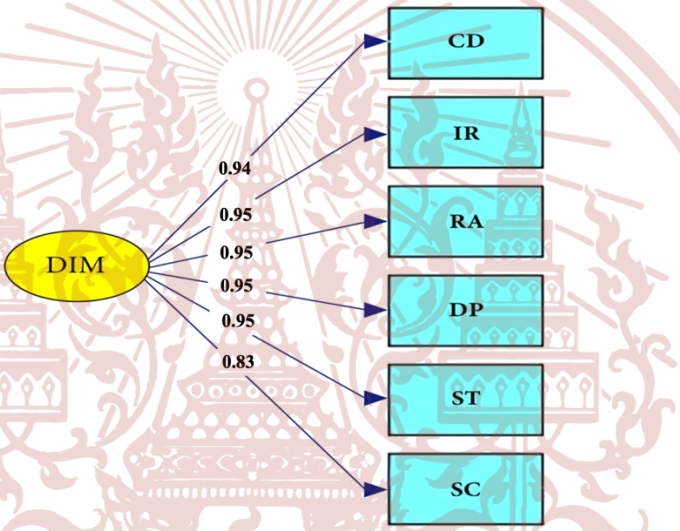
ภาพที่ 4-5 องค์ประกอบสำคัญด้านการจัดการองค์กรดิจิทัล

5. ตัวแปรแฝงด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ พบว่าทั้ง 6 องค์ประกอบที่ใช้ในการศึกษาครั้งนี้เป็นองค์ประกอบสำคัญเชิงยืนยัน ได้แก่ 1. การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ 2 กรอบการทำงานเชิงสถาปัตยกรรม 3) การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ 4) การปรับตัวต่อการเปลี่ยนแปลง 5) การรับมือภัยคุกคามและความเสี่ยง และ 6) จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ โดยมีค่าน้ำหนักองค์ประกอบแบบ Completely Standardized Solution เป็น 0.61, 0.61, 0.59, 0.63, 0.69 และ 0.60 ตามลำดับ ซึ่งเป็นไปตามสมมติฐานการวิจัยที่ตั้งไว้ ดังภาพที่ 4-6



ภาพที่ 4-6 องค์ประกอบสำคัญด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

6. ตัวแปรแฝงด้านการจัดการภูมิคุ้มกันดิจิทัล พบว่าทั้ง 6 องค์ประกอบที่ใช้ในการศึกษาครั้งนี้เป็นองค์ประกอบสำคัญเชิงยืนยัน ได้แก่ 1) การตรวจจับภัยคุกคามทางไซเบอร์ 2) การตอบสนองต่อเหตุการณ์ทางไซเบอร์ 3) การประเมินและจัดการความเสี่ยง 4) การปกป้องข้อมูลและความเป็นส่วนตัว 5) การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย และ 6) นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ โดยมีค่าน้ำหนักองค์ประกอบแบบ Completely Standardized Solution เป็น 0.94, 0.95, 0.95, 0.95, 0.95 และ 0.83 ตามลำดับ ซึ่งเป็นไปตามสมมติฐานการวิจัยที่ตั้งไว้ ดังภาพที่ 4-7



ภาพที่ 4-7 องค์ประกอบสำคัญด้านการจัดการภูมิคุ้มกันดิจิทัล

4.1.5 ความสัมพันธ์เชิงเหตุผล ตามแบบจำลองสมการโครงสร้าง (Structural Equation Model) สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผลสรุปความสัมพันธ์เชิงเหตุผลตามแบบจำลองสมการโครงสร้าง (Structural Equation Model: SEM) เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” ตามที่ผู้วิจัยได้พัฒนาขึ้น พบว่าแบบจำลองมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยมีค่าสถิติต่าง ๆ เป็นไปตามเกณฑ์ที่ยอมรับทางสถิติ กล่าวคือ ค่า Chi-Square เท่ากับ 517.17 ที่องศาอิสระ 499 ค่า p-value เท่ากับ 0.27784 ซึ่งไม่มีนัยสำคัญทางสถิติ และค่า RMSEA เท่ากับ 0.012 แสดงถึงความสอดคล้องในระดับดีมาก ทั้งนี้ผลการวิเคราะห์ดังกล่าวยืนยันว่าแบบจำลองมีความเหมาะสมและสามารถอธิบายความสัมพันธ์ระหว่างตัวแปรได้อย่างมีประสิทธิภาพ โดยพบว่าโครงสร้างองค์กรมีอิทธิพลทางตรงเชิงบวกในระดับสูงต่อสถาปัตยกรรมองค์กร

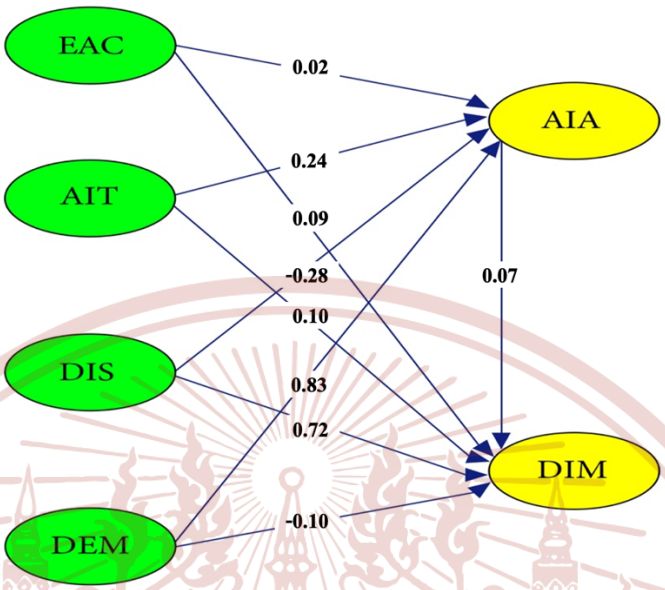
ปัญญาประดิษฐ์ ขณะที่เทคโนโลยีอัจฉริยะมีอิทธิพลเชิงบวกทั้งต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัล โดยเฉพาะอย่างยิ่งมีอิทธิพลต่อการจัดการภูมิคุ้มกันดิจิทัลในระดับสูง นอกจากนี้ ระบบภูมิคุ้มกันดิจิทัลยังมีอิทธิพลทางตรงเชิงบวกต่อการจัดการภูมิคุ้มกันดิจิทัลอย่างมีนัยสำคัญ ในขณะที่สถาปัตยกรรมองค์กรปัญญาประดิษฐ์มีอิทธิพลต่อการจัดการภูมิคุ้มกันดิจิทัลในระดับต่ำ แสดงถึงบทบาทในลักษณะของกลไกสนับสนุนเชิงโครงสร้างมากกว่าปัจจัยขับเคลื่อนหลัก อีกทั้งยังพบว่าการจัดการองค์กรดิจิทัลมีอิทธิพลเชิงลบต่อทั้งสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัล ซึ่งอาจแสดงถึงความไม่สอดคล้องหรือข้อจำกัดในการบูรณาการการบริหารจัดการดิจิทัลภายในองค์กรโดยรวม ดังนั้นสามารถสรุปได้ว่าแบบจำลองนี้มีลักษณะเป็นการขับเคลื่อนด้วยเทคโนโลยีอัจฉริยะเป็นหลัก โดยมีโครงสร้างองค์กรและสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ทำหน้าที่เป็นกลไกสนับสนุนเพื่อเสริมสร้างประสิทธิภาพของการจัดการภูมิคุ้มกันดิจิทัลในสถาบันอุดมศึกษาอย่างเป็นระบบและยั่งยืน จากแบบจำลองสมการโครงสร้างดังกล่าวสามารถสรุปผลการวิจัยได้ดังตารางที่ 4-15 และภาพที่ 4-8 ดังนี้

ตารางที่ 4-15 สรุปอิทธิพลทางตรง (Direct Effect) อิทธิพลทางอ้อม (Indirect Effect) และอิทธิพลรวม (Total Effect) ระหว่างตัวแปรในแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

Dep.V.	Indep.V	R-square	F	Path Coefficients		
				DE	IE	TT
AIA – สถาปัตยกรรมองค์กรปัญญาประดิษฐ์	EAC – โครงสร้างองค์กร	0.70	0.096	0.02	0.00	0.02
	AIT – เทคโนโลยีอัจฉริยะ			0.24	0.00	0.24
	DIS – ระบบภูมิคุ้มกันดิจิทัล			-0.28	0.00	-0.28
	DEM – การจัดการองค์กรดิจิทัล			0.83	0.00	0.83
DIM – การจัดการภูมิคุ้มกันดิจิทัล	EAC – โครงสร้างองค์กร	0.81	0.850	0.09	0.09	0.18
	AIT – เทคโนโลยีอัจฉริยะ			0.10	0.02	0.12
	DIS – ระบบภูมิคุ้มกันดิจิทัล			0.72	-0.02	0.70
	DEM – การจัดการองค์กรดิจิทัล			-0.10	0.06	-0.04
	AIA – สถาปัตยกรรมองค์กรปัญญาประดิษฐ์			0.07	0.00	0.07

* P < .05

Remark: Dep.V. = Dependent Variable, Indep.V. = Independent Variable, DE = Direct Effect, IE = Indirect Effect, and TT = Total Effect



Chi-Square = 517.17, df = 499, P-value = 0. 27784, RMSEA = 0.012

ภาพที่ 4-8 Over-identified Model ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

แบบจำลองที่ 1 ซึ่งมีตัวแปรตามคือ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) ได้รับอิทธิพลจากปัจจัยโครงสร้างองค์กร (EAC) เทคโนโลยีอัจฉริยะ (AIT) ระบบภูมิคุ้มกันดิจิทัล (DIS) และการจัดการองค์กรดิจิทัล (DEM) โดยแบบจำลองสามารถอธิบายความแปรปรวนของ AIA ได้ร้อยละ 70 (R^2 = 0.70) ซึ่งแสดงถึงความสามารถในการอธิบายของแบบจำลองในระดับสูง และมีความเหมาะสมเชิงสถิติในภาพรวม เมื่อพิจารณาค่าสัมประสิทธิ์อิทธิพลทางตรง (Direct Effects: DE) พบว่า ปัจจัยที่มีอิทธิพลสูงที่สุดต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์คือ การจัดการองค์กรดิจิทัล (DEM = 0.83) รองลงมาคือ เทคโนโลยีอัจฉริยะ (AIT = 0.24) ซึ่งมีอิทธิพลในระดับปานกลาง ขณะที่โครงสร้างองค์กร (EAC = 0.02) มีอิทธิพลในระดับต่ำมาก และระบบภูมิคุ้มกันดิจิทัล (DIS = -0.28) มีอิทธิพลเชิงลบในระดับต่ำ นอกจากนี้ ไม่พบอิทธิพลทางอ้อม (Indirect Effects: IE = 0.00) ของตัวแปรอิสระต่อ AIA ในแบบจำลองนี้ ส่งผลให้ค่าอิทธิพลรวม (Total Effects: TT) มีค่าเท่ากับอิทธิพลทางตรง ผลการวิเคราะห์ดังกล่าวแสดงให้เห็นว่า การจัดการองค์กรดิจิทัลเป็นปัจจัยเชิงกลยุทธ์ที่มีบทบาทสำคัญที่สุดในการขับเคลื่อนการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ในสถาบันอุดมศึกษา ขณะที่เทคโนโลยีอัจฉริยะมีบทบาทสนับสนุน และโครงสร้างองค์กรมีบทบาทค่อนข้างจำกัดในบริบทของแบบจำลองนี้ ส่วนอิทธิพลเชิงลบของระบบภูมิคุ้มกันดิจิทัลอาจแสดงถึง

ความไม่สอดคล้องหรือความซ้ำซ้อนของกลไกการดำเนินงานที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ในเชิงปฏิบัติ

แบบจำลองที่ 2 ซึ่งมีตัวแปรตามคือ การจัดการภูมิคุ้มกันดิจิทัล (DIM) พบว่าสามารถอธิบายความแปรปรวนของ DIM ได้ร้อยละ 81 (R^2 = 0.81) ซึ่งแสดงถึงความสามารถในการพยากรณ์ของแบบจำลองในระดับสูงมาก และมีความเหมาะสมเชิงสถิติในภาพรวม เมื่อพิจารณาอิทธิพลทางตรง (Direct Effects: DE) พบว่า ระบบภูมิคุ้มกันดิจิทัล (DIS = 0.72) มีอิทธิพลเชิงบวกในระดับสูงที่สุด รองลงมาคือ เทคโนโลยีอัจฉริยะ (AIT = 0.10) และโครงสร้างองค์กร (EAC = 0.09) ซึ่งมีอิทธิพลในระดับต่ำ ขณะที่สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA = 0.07) มีอิทธิพลในระดับต่ำมาก และการจัดการองค์กรดิจิทัล (DEM = -0.10) มีอิทธิพลเชิงลบในระดับต่ำ เมื่อพิจารณาอิทธิพลทางอ้อม (Indirect Effects: IE) พบว่า โครงสร้างองค์กรมีอิทธิพลทางอ้อมต่อการจัดการภูมิคุ้มกันดิจิทัล (IE = 0.09) ขณะที่เทคโนโลยีอัจฉริยะ (IE = 0.02) และการจัดการองค์กรดิจิทัล (IE = 0.06) มีอิทธิพลทางอ้อมในระดับต่ำ และระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางอ้อมเชิงลบเล็กน้อย (IE = -0.02) สำหรับอิทธิพลรวม (Total Effects: TT) พบว่า ระบบภูมิคุ้มกันดิจิทัลยังคงเป็นปัจจัยที่มีอิทธิพลสูงสุด (TT = 0.70) รองลงมาคือ โครงสร้างองค์กร (TT = 0.18) เทคโนโลยีอัจฉริยะ (TT = 0.12) และสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (TT = 0.07) ขณะที่การจัดการองค์กรดิจิทัลมีอิทธิพลรวมเชิงลบเล็กน้อย (TT = -0.04) ผลการวิเคราะห์ดังกล่าวชี้ให้เห็นว่า ความเข้มแข็งของระบบภูมิคุ้มกันดิจิทัลเป็นปัจจัยหลักที่ส่งผลต่อความสำเร็จของการจัดการภูมิคุ้มกันดิจิทัลโดยรวม ขณะที่ปัจจัยด้านโครงสร้างองค์กรและเทคโนโลยีอัจฉริยะมีบทบาทสนับสนุนทั้งทางตรงและทางอ้อมผ่านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ นอกจากนี้ อิทธิพลเชิงลบของการจัดการองค์กรดิจิทัลอาจแสดงถึงความท้าทายในการบูรณาการระบบดิจิทัลภายในองค์กร ดังนั้น การพัฒนาและเสริมสร้างระบบภูมิคุ้มกันดิจิทัลควบคู่กับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์อย่างเป็นระบบ จะเป็นปัจจัยสำคัญต่อการยกระดับความมั่นคงปลอดภัยและความยั่งยืนทางดิจิทัลของสถาบันอุดมศึกษาได้อย่างมีประสิทธิภาพ

ตารางที่ 4-16 ผลวิเคราะห์ค่าสถิติองค์ประกอบเชิงยืนยันที่มีอิทธิพบต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิททัลสำหรับสถาบันอุดมศึกษา

ตัวชี้วัดโดยรวม	λ	SE.	t-value	R^2	AVE	CR.
ด้านโครงสร้างองค์กร					0.87	0.97
BA (ค่าคงที่พารามิเตอร์)	0.85	0.04	21.25	0.72		
DA	0.87	0.04	21.75	0.77		

ตัวชี้วัดโดยรวม	λ	SE.	t-value	R^2	AVE	CR.
AA	0.93	0.03	31.00	0.87		
TA	0.96	0.03	32.00	0.92		
SA	0.95	0.03	31.67	0.90		
IA	0.94	0.03	31.33	0.88		
GA	0.93	0.03	31.00	0.86		
ด้านเทคโนโลยีอัจฉริยะ					0.91	0.98
ML (ค่าคงที่พารามิเตอร์)	0.95	0.03	31.67	0.91		
DL	0.95	0.03	31.67	0.90		
NL	0.96	0.03	32.00	0.92		
BI	0.95	0.03	31.67	0.91		
ด้านระบบภูมิคุ้มกันดิจิทัล					0.89	0.97
OV (ค่าคงที่พารามิเตอร์)	0.96	0.03	32.00	0.92		
TD	0.95	0.03	31.67	0.90		
AN	0.96	0.03	32.00	0.92		
RP	0.95	0.03	31.67	0.90		
RR	0.91	0.04	22.75	0.84		
CC	0.94	0.03	31.33	0.89		
ด้านการจัดการองค์กรดิจิทัล					0.45	0.81
DS (ค่าคงที่พารามิเตอร์)	0.66	0.05	13.20	0.44		
TI	0.67	0.05	13.40	0.44		
DM	0.67	0.05	13.40	0.45		
PA	0.68	0.05	13.60	0.47		
CB	0.69	0.05	13.80	0.47		
ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์					0.39	0.79
EI (ค่าคงที่พารามิเตอร์)	0.61	0.05	12.20	0.38		
AF	0.61	0.05	12.20	0.37		
AS	0.59	0.05	11.80	0.35		
AD	0.63	0.05	12.60	0.40		
TR	0.69	0.05	13.80	0.47		

ตัวชี้วัดโดยรวม	λ	SE.	t-value	R^2	AVE	CR.
ER	0.60	0.05	12.00	0.36		
ด้านการจัดการภูมิคุ้มกันดิจิทัล					0.87	0.97
CD (ค่าคงที่พารามิเตอร์)	0.94	0.03	31.33	0.89		
IR	0.95	0.03	31.67	0.91		
RA	0.95	0.03	31.67	0.90		
DP	0.95	0.03	31.67	0.89		
ST	0.95	0.03	31.67	0.90		
SC	0.83	0.04	20.75	0.70		

** อย่างมีนัยสำคัญทางสถิติที่ 0.001

ผลการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis: CFA) ของปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา พบว่า แบบจำลองประกอบด้วยตัวแปรแฝงจำนวน 6 ตัว ได้แก่ ด้านโครงสร้างองค์กร (EAC) ด้านเทคโนโลยีอัจฉริยะ (AIT) ด้านระบบภูมิคุ้มกันดิจิทัล (DIS) ด้านการจัดการองค์กรดิจิทัล (DEM) ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) และด้านการจัดการภูมิคุ้มกันดิจิทัล (DIM) รวมทั้งสิ้น 34 ตัวแปรสังเกตได้ ผลการวิเคราะห์พบว่า ค่าน้ำหนักองค์ประกอบมาตรฐาน (Factor Loadings: λ) มีค่าอยู่ระหว่าง 0.66 – 0.96 ซึ่งสูงกว่าเกณฑ์ขั้นต่ำที่กำหนดไว้ที่ 0.40 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.001 แสดงให้เห็นว่าตัวแปรสังเกตได้สามารถอธิบายตัวแปรแฝงได้เป็นอย่างดี ในส่วนของค่าความคลาดเคลื่อน (Error Variance) พบว่ามีค่าอยู่ในช่วงต่ำประมาณ **0**.02 – 0.10 แสดงถึงความแม่นยำของเครื่องมือวัดในระดับที่ยอมรับได้ สำหรับค่าสัมประสิทธิ์สหสัมพันธ์เชิงพหุ (R^2) ของตัวแปรสังเกตได้ พบว่ามีค่าอยู่ระหว่างประมาณ 0.41 – 0.95 แสดงถึงความสามารถของตัวแปรแฝงในการอธิบายความแปรปรวนของตัวแปรสังเกตได้ในระดับปานกลางถึงสูง เมื่อพิจารณาค่าเฉลี่ยความแปรปรวนที่ถูกสกัดได้ (Average Variance Extracted: AVE) พบว่ามีค่าอยู่ระหว่าง 0.61 – 0.87 ซึ่งสูงกว่าเกณฑ์ 0.50 บ่งชี้ว่าโมเดลมีความตรงเชิงลู่เข้า (Convergent Validity) ที่ดี นอกจากนี้ ค่าความเชื่อมั่นรวม (Composite Reliability: CR) มีค่าอยู่ระหว่าง 0.86 – 0.96 ซึ่งสูงกว่าเกณฑ์ 0.60 แสดงให้เห็นว่าตัวแปรมีความเชื่อมั่นในระดับสูง โดยสรุป โมเดลการวัดมีทั้งความตรงเชิงลู่เข้าและความเชื่อมั่นที่ดี รวมถึงมีความตรงเชิงจำแนก (Discriminant Validity) ที่เหมาะสม แสดงถึงความเป็นเอกภาพของตัวแปรแฝงในแต่ละมิติ ดังนั้นจึงสามารถนำโมเดลการวัดนี้ไปใช้ในการวิเคราะห์แบบจำลองสมการเชิงโครงสร้าง (Structural Equation Modeling: SEM) ได้อย่างเหมาะสมและมีนัยสำคัญทางสถิติที่ระดับ 0.001

4.1.6 การวิเคราะห์ตรวจสอบสหสัมพันธ์ตัวแปรแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ในส่วนนี้วิเคราะห์ตรวจสอบปัญหาสหสัมพันธ์ระหว่างตัวแปรแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา เพื่อทดสอบว่าเกิดปัญหาภาวะร่วมเส้นตรงพหุ (Multi Collinearrity) ประมวลผลข้อมูลโปรแกรมคอมพิวเตอร์สำเร็จรูปทางสถิติ สรุปผลได้ดังนี้

4.1.6.1 การตรวจสอบปัญหาสหสัมพันธ์ของตัวแปร

ในส่วนนี้ทำการวิเคราะห์เพื่อทำการตรวจสอบปัญหาสหสัมพันธ์ตัวแปรแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ด้านโครงสร้างองค์กร ด้านเทคโนโลยีอัจฉริยะ ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์สหสัมพันธ์ระหว่าง 0.30 – 0.85 ซึ่งมีค่าสัมประสิทธิ์สหสัมพันธ์ในเชิงบวกและไม่เกิน 0.90 (TomassMHultt, 2021) ผลดังกล่าวแสดงให้เห็นว่า ตัวแปรอิสระแต่ละตัวมีความสัมพันธ์กันในระดับที่เหมาะสม แต่ยังคงมีความเป็นอิสระต่อกัน ไม่เกิดปัญหาความซ้ำซ้อนของตัวแปร (Redundancy) หรือความสัมพันธ์เชิงเส้นสูงเกินไป ซึ่งอาจส่งผลกระทบต่อความแม่นยำของการประมาณค่าในแบบจำลอง ดังนั้น จึงสามารถสรุปได้ว่า ตัวแปรในแบบจำลองมีคุณสมบัติผ่านเกณฑ์ด้านความเป็นอิสระของตัวแปร มีความเที่ยงตรงเชิงโครงสร้าง และมีความเป็นเอกภาพของตัวแปรแฝงในระดับที่เหมาะสม สามารถนำไปใช้ในการวิเคราะห์แบบจำลองสมการเชิงโครงสร้าง (Structural Equation Modeling: SEM) ของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาได้อย่างมีประสิทธิภาพและเชื่อถือได้ แสดงผลดังตารางที่ 4-17

ตารางที่ 4-17 วิเคราะห์สหสัมพันธ์แบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตัวแปร	ด้านโครงสร้างองค์กร							ด้านเทคโนโลยีอัจฉริยะ				ด้านระบบภูมิคุ้มกันดิจิทัล						ด้านการจัดการองค์กรดิจิทัล					ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์						ด้านการจัดการภูมิคุ้มกันดิจิทัล					
	BA	DA	AA	TA	SA	IA	GA	ML	DL	NL	BI	OV	TD	AN	RP	RR	CC	DS	TI	DM	PA	CB	EI	AF	AS	AD	TR	ER	CD	IR	RA	DP	ST	SC
BA	1.00																																	
DA	0.72	1.00																																
AA	0.69	0.74	1.00																															
TA	0.71	0.76	0.73	1.00																														
SA	0.67	0.71	0.70	0.75	1.00																													
IA	0.70	0.73	0.72	0.77	0.74	1.00																												
GA	0.66	0.70	0.68	0.74	0.72	0.76	1.00																											
ML	0.63	0.67	0.65	0.71	0.68	0.72	0.70	1.00																										
DL	0.65	0.69	0.67	0.73	0.71	0.74	0.72	0.81	1.00																									
NL	0.62	0.66	0.64	0.70	0.68	0.71	0.69	0.78	0.82	1.00																								
BI	0.61	0.65	0.63	0.68	0.66	0.70	0.68	0.75	0.79	0.77	1.00																							
OV	0.59	0.63	0.61	0.66	0.64	0.68	0.66	0.72	0.75	0.73	0.71	1.00																						
TD	0.60	0.64	0.62	0.67	0.65	0.69	0.67	0.73	0.76	0.74	0.72	0.81	1.00																					
AN	0.58	0.62	0.60	0.65	0.63	0.67	0.65	0.71	0.74	0.72	0.70	0.79	0.82	1.00																				
RP	0.57	0.61	0.59	0.64	0.62	0.66	0.64	0.70	0.73	0.71	0.69	0.77	0.80	0.83	1.00																			
RR	0.56	0.60	0.58	0.63	0.61	0.65	0.63	0.69	0.72	0.70	0.68	0.76	0.79	0.81	0.84	1.00																		
CC	0.55	0.59	0.57	0.62	0.60	0.64	0.62	0.68	0.71	0.69	0.67	0.75	0.78	0.80	0.82	0.85	1.00																	
DS	0.64	0.68	0.66	0.72	0.70	0.73	0.71	0.76	0.79	0.77	0.75	0.72	0.73	0.71	0.69	0.68	0.66	1.00																
TI	0.63	0.67	0.65	0.71	0.69	0.72	0.70	0.75	0.78	0.76	0.74	0.71	0.72	0.70	0.68	0.67	0.65	0.82	1.00															
DM	0.62	0.66	0.64	0.70	0.68	0.71	0.69	0.74	0.77	0.75	0.73	0.70	0.71	0.69	0.67	0.66	0.64	0.80	0.84	1.00														
PA	0.61	0.65	0.63	0.69	0.67	0.70	0.68	0.73	0.76	0.74	0.72	0.69	0.70	0.68	0.66	0.65	0.63	0.78	0.82	0.85	1.00													
CB	0.60	0.64	0.62	0.68	0.66	0.69	0.67	0.72	0.75	0.73	0.71	0.68	0.69	0.67	0.65	0.64	0.62	0.77	0.81	0.83	0.84	1.00												
EI	0.68	0.72	0.70	0.75	0.73	0.76	0.74	0.71	0.73	0.70	0.69	0.66	0.67	0.65	0.64	0.63	0.62	0.78	0.80	0.82	0.81	0.79	1.00											
AF	0.67	0.71	0.69	0.74	0.72	0.75	0.73	0.70	0.72	0.69	0.68	0.65	0.66	0.64	0.63	0.62	0.61	0.77	0.79	0.81	0.80	0.78	0.84	1.00										
AS	0.66	0.70	0.68	0.73	0.71	0.74	0.72	0.69	0.71	0.68	0.67	0.64	0.65	0.63	0.62	0.61	0.60	0.76	0.78	0.80	0.79	0.77	0.83	0.85	1.00									
AD	0.65	0.69	0.67	0.72	0.70	0.73	0.71	0.68	0.70	0.67	0.66	0.63	0.64	0.62	0.61	0.60	0.59	0.75	0.77	0.79	0.78	0.76	0.82	0.84	0.86	1.00								
TR	0.64	0.68	0.66	0.71	0.69	0.72	0.70	0.67	0.69	0.66	0.65	0.62	0.63	0.61	0.60	0.59	0.58	0.74	0.76	0.78	0.77	0.75	0.81	0.83	0.85	0.84	1.00							
ER	0.63	0.67	0.65	0.70	0.68	0.71	0.69	0.66	0.68	0.65	0.64	0.61	0.62	0.60	0.59	0.58	0.57	0.73	0.75	0.77	0.76	0.74	0.80	0.82	0.84	0.83	0.82	1.00						
CD	0.62	0.66	0.64	0.69	0.67	0.70	0.68	0.65	0.67	0.64	0.63	0.60	0.61	0.59	0.58	0.57	0.56	0.72	0.74	0.76	0.75	0.73	0.79	0.81	0.83	0.82	0.81	0.80	1.00					
IR	0.61	0.65	0.63	0.68	0.66	0.69	0.67	0.64	0.66	0.63	0.62	0.59	0.60	0.58	0.57	0.56	0.55	0.71	0.73	0.75	0.74	0.72	0.78	0.80	0.82	0.81	0.80	0.79	0.78	1.00				
RA	0.60	0.64	0.62	0.67	0.65	0.68	0.66	0.63	0.65	0.62	0.61	0.58	0.59	0.57	0.56	0.55	0.54	0.70	0.72	0.74	0.73	0.71	0.77	0.79	0.81	0.80	0.79	0.78	0.77	0.76	1.00			
DP	0.59	0.63	0.61	0.66	0.64	0.67	0.65	0.62	0.64	0.61	0.60	0.57	0.58	0.56	0.55	0.54	0.53	0.69	0.71	0.73	0.72	0.70	0.76	0.78	0.80	0.79	0.78	0.77	0.76	0.75	0.74	1.00		
ST	0.58	0.62	0.60	0.65	0.63	0.66	0.64	0.61	0.63	0.60	0.59	0.56	0.57	0.55	0.54	0.53	0.52	0.68	0.70	0.72	0.71	0.69	0.75	0.77	0.79	0.78	0.77	0.76	0.75	0.74	0.73	0.72	1.00	
SC	0.57	0.61	0.59	0.64	0.62	0.65	0.63	0.60	0.62	0.59	0.58	0.55	0.56	0.54	0.53	0.52	0.51	0.67	0.69	0.71	0.70	0.68	0.74	0.76	0.78	0.77	0.76	0.75	0.74	0.73	0.72	0.71	0.70	1.00

** อย่างมีนัยสำคัญทางสถิติที่ 0.001

4.1.6.2 การตรวจสอบการแจกแจงค่าสถิติเชิงพรรณา

ผลการวิเคราะห์การตรวจสอบค่าสถิติตัวแปรแบบจำลองผลปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ทั้งจำนวน 6 ตัวแปรแฝง ด้านโครงสร้างองค์กร ด้านเทคโนโลยีอัจฉริยะ ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และด้านการจัดการภูมิคุ้มกันดิจิทัล รวมทั้งหมด 34 ตัวแปรสังเกตได้ พบว่าค่าเฉลี่ยอยู่ในช่วง 3.82 ถึง 4.39 ซึ่งแสดงให้เห็นว่ากลุ่มตัวอย่างมีความคิดเห็นอยู่ในระดับมากถึงมากที่สุดต่อองค์ประกอบของแบบจำลอง โดยมีค่าความเบี่ยงเบนมาตรฐานอยู่ระหว่าง 0.47 ถึง 0.77 แสดงถึงการกระจายตัวของข้อมูลในระดับต่ำถึงปานกลางและมีความสม่ำเสมอของคำตอบค่อนข้างดี เมื่อพิจารณาค่าความเบ้ (Skewness) พบว่าส่วนใหญ่มีค่าเป็นลบ อยู่ในช่วง -1.27 ถึง 0.36 แสดงให้เห็นว่าข้อมูลมีแนวโน้มกระจุกตัวอยู่ทางด้านคะแนนสูง ขณะที่ค่าความโด่ง (Kurtosis) อยู่ระหว่าง -0.33 ถึง 1.79 ซึ่งอยู่ในเกณฑ์ที่ยอมรับได้และบ่งชี้ว่าการแจกแจงของข้อมูลมีลักษณะใกล้เคียงการแจกแจงแบบปกติ นอกจากนี้ ค่าต่ำสุดและค่าสูงสุดอยู่ระหว่าง 1.00 ถึง 5.00 และค่าพิสัยอยู่ในช่วง 2.00 ถึง 4.00 แสดงให้เห็นว่าผู้ตอบแบบสอบถามมีการใช้ช่วงคะแนนอย่างครอบคลุมและเหมาะสม โดยสรุป ข้อมูลมีคุณสมบัติด้านการกระจายและรูปแบบการแจกแจงที่เหมาะสม สามารถนำไปใช้ในการวิเคราะห์แบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาได้แสดงผลดังตารางที่ 4 - 18

ตารางที่ 4-18 วิเคราะห์ตครวจสอบข้อมูลตัวแปรปัจจัยที่มีทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

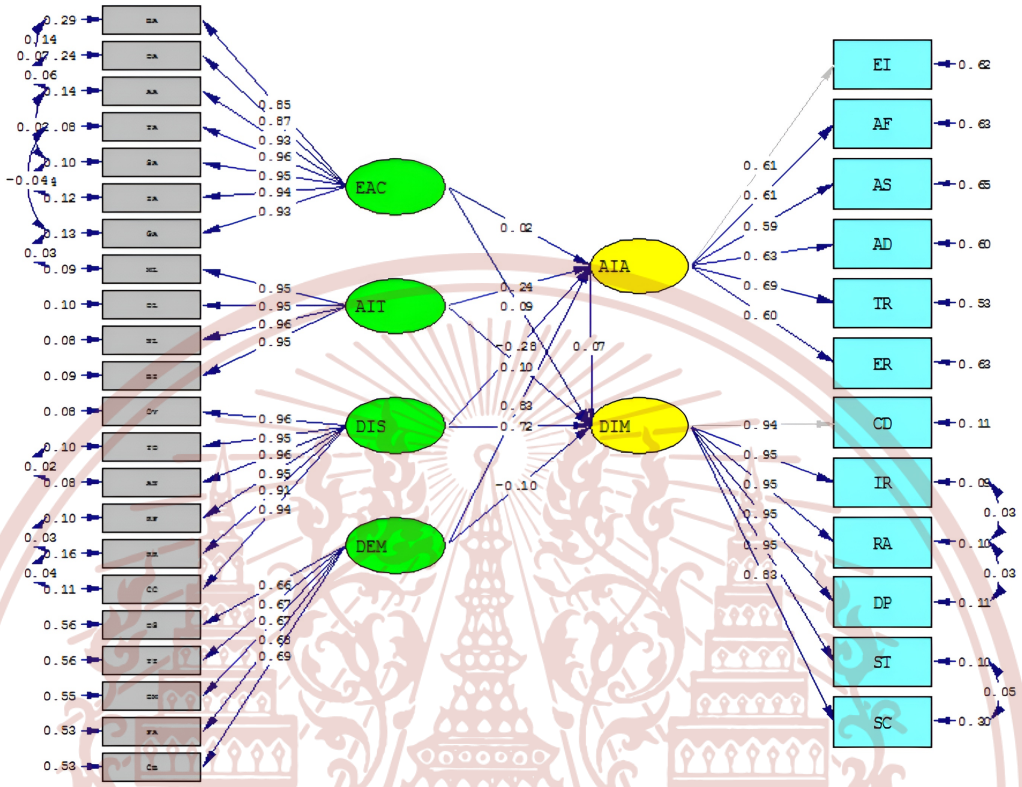
ตัวแปร	พิสัย	ต่ำสุด	สูงสุด	$\bar{X}$	S.D.	ความแปรปรวน	ความเบ้	ความโด่ง
ด้านโครงสร้างองค์กร								
BA	4.00	1.00	5.00	4.36	0.74	0.54	-1.22	1.38
DA	3.25	1.75	5.00	4.31	0.75	0.56	-1.05	0.56
AA	3.75	1.25	5.00	4.39	0.72	0.52	-1.22	1.18
TA	3.50	1.50	5.00	4.31	0.73	0.53	-1.07	0.84
SA	3.50	1.50	5.00	4.36	0.73	0.54	-1.09	0.63
IA	4.00	1.00	5.00	4.36	0.74	0.55	-1.20	1.25
GA	3.75	1.25	5.00	4.34	0.73	0.54	-1.17	1.13
ด้านเทคโนโลยีอัจฉริยะ								
ML	3.50	1.50	5.00	4.37	0.73	0.53	-1.13	0.77
DL	3.00	2.00	5.00	4.35	0.71	0.50	-0.95	0.30

ตัวแปร	พิสัย	ต่ำสุด	สูงสุด	$\bar{x}$	S.D.	ความแปรปรวน	ความเบ้	ความโด่ง
NL	4.00	1.00	5.00	4.34	0.75	0.56	-1.15	0.97
BI	3.50	1.50	5.00	4.38	0.73	0.54	-1.08	0.66
ด้านระบบภูมิคุ้มกันดิจิทัล								
OV	3.75	1.25	5.00	4.36	0.76	0.57	-1.27	1.54
TD	4.00	1.00	5.00	4.34	0.77	0.59	-1.18	1.24
AN	4.00	1.00	5.00	4.35	0.75	0.56	-1.22	1.37
RP	3.75	1.25	5.00	4.35	0.73	0.53	-1.05	0.72
RR	3.50	1.50	5.00	4.39	0.72	0.52	-1.15	0.91
CC	3.75	1.25	5.00	4.37	0.73	0.54	-1.08	0.68
ด้านการจัดการองค์กรดิจิทัล								
DS	2.25	2.75	5.00	3.92	0.48	0.23	0.12	-0.23
TI	2.25	2.75	5.00	3.94	0.47	0.22	0.18	-0.13
DM	2.00	3.00	5.00	3.92	0.49	0.24	0.36	-0.21
PA	2.50	2.50	5.00	3.82	0.51	0.26	0.34	-0.01
CB	2.50	2.50	5.00	3.88	0.50	0.25	0.23	-0.12
ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์								
EI	3.00	2.00	5.00	3.82	0.55	0.30	0.12	-0.03
AF	2.75	2.25	5.00	3.84	0.54	0.29	0.10	-0.12
AS	2.75	2.25	5.00	3.84	0.54	0.29	0.06	-0.33
AD	3.25	1.75	5.00	3.87	0.53	0.28	-0.35	1.26
TR	3.00	2.00	5.00	3.88	0.55	0.31	0.06	0.01
ER	3.25	1.75	5.00	3.96	0.52	0.27	-0.36	1.30
ด้านการจัดการภูมิคุ้มกันดิจิทัล								
CD	4.00	1.00	5.00	4.34	0.74	0.54	-1.17	1.24
IR	4.00	1.00	5.00	4.37	0.72	0.52	-1.25	1.79
RA	4.00	1.00	5.00	4.36	0.72	0.51	-1.21	1.76
DP	4.00	1.00	5.00	4.37	0.70	0.50	-1.21	1.53
ST	4.00	1.00	5.00	4.33	0.74	0.55	-1.10	1.01
SC	3.25	1.75	5.00	4.19	0.62	0.38	-1.00	1.03

4.2 ผลการสร้างแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

การสร้างแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา เป็นการนำผลจากการศึกษาค้นคว้า และสังเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาจากข้อมูล เอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับโครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัล ในการดำเนินงานในระยะที่ 1 ผ่านการตรวจสอบโดยการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis) พบว่าตัวแปรทั้งหมดมีความสอดคล้องตามเกณฑ์ สามารถนำไปสร้างโมเดลแบบจำลองสมการเชิงโครงนร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

แบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ประกอบด้วย ตัวแปรแฝง จำนวน 6 ตัว ได้แก่ ด้านโครงสร้างองค์กร (EAC), ด้านเทคโนโลยีอัจฉริยะ (AIT), ด้านระบบภูมิคุ้มกันดิจิทัล (DIS), ด้านการจัดการองค์กรดิจิทัล (DEM), ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) และ ด้านการจัดการภูมิคุ้มกันดิจิทัล (DIM) โดยตัวแปร EAC, AIT, DIS และ DEM จัดเป็นตัวแปรแฝงภายนอก (Exogenous Latent Variables) ที่ทำหน้าที่เป็นปัจจัยเชิงสาเหตุ ขณะที่ AIA (สถาปัตยกรรมองค์กรปัญญาประดิษฐ์) และ DIM (การจัดการภูมิคุ้มกันดิจิทัล) เป็นตัวแปรแฝงภายใน (Endogenous Latent Variables) ซึ่งทำหน้าที่เป็นตัวแปรตามในแบบจำลอง ในส่วนของตัวแปรเชิงสังเกต (Observed Variables) พบว่ามีจำนวนทั้งสิ้น 34 ตัว โดยตัวแปร EAC วัดด้วยตัวชี้วัด BA, DA, AA, TA, SA, IA และ GA ส่วน AIT วัดด้วย ML, DL, NL และ BI ขณะที่ DIS วัดด้วย OV, TD, AN, RP, RR และ CC และ DEM วัดด้วย DS, TI, DM, PA และ CB สำหรับตัวแปร AIA วัดด้วย EI, AF, AS, AD, TR และ ER และตัวแปร DIM วัดด้วย CD, IR, RA, DP, SI และ SC สรุปได้ดังนั้น แบบจำลองนี้จึงแสดงให้เห็นโครงสร้างความสัมพันธ์ระหว่างปัจจัยเชิงสาเหตุด้านสถาปัตยกรรมองค์กร เทคโนโลยีปัญญาประดิษฐ์ ระบบดิจิทัล และการบริหารจัดการดิจิทัล ที่ส่งผลต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และนำไปสู่การเสริมสร้างการจัดการภูมิคุ้มกันดิจิทัลในสถาบันอุดมศึกษาอย่างเป็นระบบ โดยมีตัวแปรแฝงและตัวแปรสังเกตรองรับโครงสร้างเชิงทฤษฎีของงานวิจัยอย่างครบถ้วนและชัดเจน สรุปผลดังภาพที่ 4-9



Chi-Square = 517.17, df = 499, P-value = 0. 27784, RMSEA = 0.012

ภาพที่ 4-9 แบบจำลองสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตารางที่ 4-19 ค่าสถิติประเมินความกลมกลืนของสมการเชิงโครงสร้างแบบจำลอง

ดัชนี	เกณฑ์วัด	ผลลัพธ์	ผลสรุป	แนวคิดในการอ้างอิง
Chi-Square = 517.17, df = 499				
Sig.	> 0.05	0. 278	ตรงเกณฑ์	(Hair et al., 2021), (Arbuckle, 2019), Bollen(1989) and Sorbon (1996)
CMIN/df.	< 2.0	1.036	ตรงเกณฑ์	Bollen (1993) (Corrêa Ferraz, 2020)
GFI	> 0.90	0.890	ยอมรับได้	Hair et al. (2006), Browne and Cudeck (1993)
AGFI	> 0.80	0.870	ตรงเกณฑ์	Durande-Moreau an Usunier(1999), Harrison walker (3001)
NFI	> 0.90	0.990	ตรงเกณฑ์	(Hair et al., 2021), (Arbuckle, 2019)
IFI	> 0.90	1.000	ตรงเกณฑ์	(Hair et al., 2021), (Arbuckle, 2019)
CFI	> 0.90	1.000	ตรงเกณฑ์	(Hair et al., 2021), (Arbuckle, 2019)

RMR	< 0.05	0.010	ตรงเกณฑ์	Diamantopoulos, Siguaw (2000)
RMSEA	< 0.05	0.012	ตรงเกณฑ์	(Hair et al., 2021), Browne and Cudeck (1993)

จากภาพโมเดลสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา พบว่าผลการวิเคราะห์แบบจำลอง มีความสอดคล้องกับข้อมูลเชิงประจักษ์อยู่ในเกณฑ์ดี โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ มีค่า Chi-Square = 517.17, df = 499, P-value (Sig.) = 0. 27784 > 0.05 และ CMIN/df. = 1.036 < 2.0 สอดคล้องกับแนวคิดของ Hair et al. (2021), Bollen (1993) and Sorbon (1996) ผลการวิเคราะห์พบว่าดัชนีมีความสอดคล้องและค่าสถิติเหล่านี้ผ่านเกณฑ์ที่กำหนดไว้ ทั้ง 7 ดัชนี สรุปดังนี้

1. ดัชนีวัดความสอดคล้องกลมกลืนเชิงสัมพัทธ์ (Comparative Fit Index: CFI) ซึ่งผลการวิเคราะห์พบว่าค่า CFI มีค่าเท่ากับ 1.00 > 0.90 แสดงให้เห็นว่ารูปแบบมีความสอดคล้องกับข้อมูลเชิงประจักษ์ในระดับดีเยี่ยมที่สุด

2. ดัชนีวัดความกลมกลืน (Goodness of Fit Index: GFI) ซึ่งผลการวิเคราะห์พบว่าค่า GFI ค่าเท่ากับ 0.890 แม้จะต่ำกว่าเกณฑ์ 0.90 เล็กน้อย แต่ยังอยู่ในระดับที่ยอมรับได้ (Marginal Fit) แสดงว่าแบบจำลองมีความกลมกลืนกับข้อมูลในระดับที่เหมาะสม

3. ดัชนีวัดความกลมกลืนที่ปรับแก้ไขแล้ว (Adjusted Goodness of Fit Index: AGFI) ซึ่งผลการวิเคราะห์พบว่าค่า AGFI มีค่าเท่ากับ 0.870 > 0.80 แสดงว่าแบบจำลองมีความเหมาะสม

4. ดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนกำลังสองของการประมาณค่า (Root Mean Square Error of Approximation: RMSEA) ซึ่งผลการวิเคราะห์พบว่าค่า RMSEA มีค่าเท่ากับ 0.012 < 0.05 มีค่า RMSEA ที่ดีมาก ผลของค่าดัชนีเป็นไปตามแนวคิด แสดงว่าแบบจำลองมีความสอดคล้องกลมกลืนเชิงสัมพัทธ์ และมีความสอดคล้องกับข้อมูลในระดับดีมาก

5. ดัชนีความกลมกลืนประเภทเปรียบเทียบกับรูปแบบอิสระ (Normed Fit Index: NFI) ซึ่งผลการวิเคราะห์พบว่าค่า NFI เท่ากับ 0.990 > 0.90 แสดงว่าแบบจำลองมีความสอดคล้องกับข้อมูลในระดับสูงมาก

6. ดัชนีความกลมกลืนเชิงเปรียบเทียบกับรูปแบบฐาน (Incremental Fit Index: IFI) ซึ่งผลการวิเคราะห์พบว่าค่า IFI เท่ากับ 1.000 > 0.90 แสดงว่าแบบจำลองมีความเหมาะสมในระดับดีเยี่ยม

7. ดัชนีรากของค่าเฉลี่ยกำลังสองของส่วนเหลือ (Root Mean Square Residual: RMR) ซึ่งผลการวิเคราะห์พบว่าค่า RMR เท่ากับ 0.010 < 0.05 ซึ่งเป็นค่า RMR ที่ดีมาก แสดงว่าแบบจำลองมีความสอดคล้องกลมกลืนเชิงสัมพัทธ์

จากผลการวิเคราะห์ค่าดัชนีทั้ง 7 ตัว มีความสอดคล้องกลมกลืนกับข้อมูลเชิงเชิงประจักษ์ ชี้ให้เห็นว่าสมการเชิงโครงสร้างแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ตามเงื่อนไขในระดับการยอมรับทางสถิติ ประกอบด้วย ด้านโครงสร้างองค์กร ด้านเทคโนโลยีอัจฉริยะ ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ตัวแปรผล คือ ด้านการจัดการภูมิคุ้มกันดิจิทัล ทุกตัวแปรนั้นมีความสอดคล้องเป็นไปตามเกณฑ์การกำหนดค่าซึ่งแสดงว่าโมเดลในการวัดนี้มีความเที่ยงตรง (Validity) หรือ OK Fit Confirm สรุปผลทดสอบอิทธิพลได้ดังตารางที่ 4 - 20

ตารางที่ 4-20 วิเคราะห์สมการเชิงโครงสร้างแบบจำลองผลปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตัวแปรตาม	ตัวแปรอิสระ (เส้นทาง)	λ	Sig.	R^2
สถาปัตยกรรมองค์กรปัญญาประดิษฐ์	EAC ⟶ AIA	0.02	*	0.70
	AIT ⟶ AIA	0.24	*	
	DIS ⟶ AIA	-0.28	*	
	DEM ⟶ AIA	0.83	*	
การจัดการภูมิคุ้มกันดิจิทัล	EAC ⟶ DIM	0.09	*	0.81
	AIT ⟶ DIM	0.10	*	
	DIS ⟶ DIM	0.72	*	
	DEM ⟶ DIM	-0.10	*	
	AIA ⟶ DIM	0.07	*	

***** อย่างมีนัยสำคัญทางสถิติที่ 0.05

ผลการวิเคราะห์ทดสอบสมการเชิงโครงสร้างแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ประกอบด้วย ด้านโครงสร้างองค์กร ด้านเทคโนโลยีอัจฉริยะ ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และด้านการจัดการภูมิคุ้มกันดิจิทัล โดยพิจารณาจากค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระในรูปคะแนนมาตรฐาน (Standardized Regression Coefficients) ซึ่งเป็นค่าที่แสดงถึงระดับอิทธิพลของตัวแปรที่มีต่อกันในแบบจำลองสมการโครงสร้าง สามารถสรุปผลการทดสอบเป็นรายด้านได้ดังนี้

4.2.1 ด้านโครงสร้างองค์กร

ผลการวิเคราะห์พบว่า ด้านโครงสร้างองค์กร (EAC) มีผลต่อสมการเชิงโครงสร้างแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยเป็นอิทธิพลทางตรงจำนวน 2 เส้นทาง และอิทธิพลทางอ้อมจำนวน 1 เส้นทาง สรุปได้ดังนี้

4.2.1.1 ด้านโครงสร้างองค์กรมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) เท่ากับ 0.02 แสดงให้เห็นว่า การกำหนดโครงสร้างองค์กร การกำกับดูแล และการบริหารจัดการภายในองค์กร มีส่วนสนับสนุนต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ แม้อิทธิพลจะอยู่ในระดับต่ำ แต่ยังสะท้อนถึงความสำคัญของโครงสร้างพื้นฐานเชิงบริหารในการขับเคลื่อนองค์กรดิจิทัล

4.2.1.2 ด้านโครงสร้างองค์กรมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัล (DIM) เท่ากับ 0.09 แสดงให้เห็นว่า องค์กรที่มีโครงสร้างการบริหารจัดการที่ชัดเจน มีนโยบายและกระบวนการดำเนินงานที่เป็นระบบ จะช่วยส่งเสริมการบริหารจัดการด้านความมั่นคงปลอดภัยทางดิจิทัลได้อย่างมีประสิทธิภาพ

4.2.1.3 ด้านโครงสร้างองค์กรมีอิทธิพลทางอ้อมต่อการจัดการภูมิคุ้มกันดิจิทัลผ่านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เท่ากับ 0.09 และมีอิทธิพลรวมเท่ากับ 0.18 แสดงให้เห็นว่าการพัฒนาโครงสร้างองค์กรที่เหมาะสมสามารถสนับสนุนการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ซึ่งจะส่งผลต่อประสิทธิภาพของการจัดการภูมิคุ้มกันดิจิทัลในสถาบันอุดมศึกษา

4.2.2 ด้านเทคโนโลยีอัจฉริยะ

ผลการวิเคราะห์พบว่า ด้านเทคโนโลยีอัจฉริยะ (AIT) มีผลต่อสมการเชิงโครงสร้างแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยเป็นอิทธิพลทางตรงจำนวน 2 เส้นทาง และอิทธิพลทางอ้อมจำนวน 1 เส้นทาง สรุปได้ดังนี้

4.2.2.1 ด้านเทคโนโลยีอัจฉริยะมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) เท่ากับ 0.24 แสดงให้เห็นว่า การประยุกต์ใช้เทคโนโลยีอัจฉริยะ เช่น Machine Learning, Deep Learning และ Natural Language Processing มีส่วนสำคัญในการสนับสนุนการออกแบบและพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

4.2.2.2 ด้านเทคโนโลยีอัจฉริยะมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัล (DIM) เท่ากับ 0.10 แสดงให้เห็นว่า เทคโนโลยีอัจฉริยะช่วยเพิ่มศักยภาพในการเฝ้าระวัง การวิเคราะห์ และการตอบสนองต่อภัยคุกคามทางไซเบอร์ของสถาบันอุดมศึกษา

4.2.2.3 ด้านเทคโนโลยีอัจฉริยะมีอิทธิพลทางอ้อมต่อการจัดการภูมิคุ้มกันดิจิทัลผ่านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เท่ากับ 0.02 และมีอิทธิพลรวมเท่ากับ 0.12 แสดงให้เห็นว่าการพัฒนาเทคโนโลยีอัจฉริยะสามารถเสริมสร้างประสิทธิภาพของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และส่งผลต่อการบริหารจัดการภูมิคุ้มกันดิจิทัลได้อย่างมีประสิทธิภาพ

4.2.3 ด้านระบบภูมิคุ้มกันดิจิทัล

ผลการวิเคราะห์พบว่า ด้านระบบภูมิคุ้มกันดิจิทัล (DIS) มีผลต่อสมการเชิงโครงสร้างแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยเป็นอิทธิพลทางตรงจำนวน 2 เส้นทาง และอิทธิพลทางอ้อมจำนวน 1 เส้นทาง สรุปได้ดังนี้

4.2.3.1 ด้านระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางตรงเชิงลบต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) เท่ากับ -0.28 แสดงให้เห็นว่า ความซับซ้อนของระบบป้องกันและการรักษาความมั่นคงปลอดภัยทางไซเบอร์อาจส่งผลต่อการบูรณาการสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

4.2.3.2 ด้านระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัล (DIM) สูงที่สุด เท่ากับ 0.72 แสดงให้เห็นว่า ระบบเฝ้าระวัง ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ เป็นองค์ประกอบสำคัญที่ช่วยเสริมสร้างภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา

4.2.3.3 ด้านระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางอ้อมเชิงลบต่อการจัดการภูมิคุ้มกันดิจิทัลผ่านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เท่ากับ -0.02 และมีอิทธิพลรวมเท่ากับ 0.70 แสดงให้เห็นว่า แม้จะมีอิทธิพลทางอ้อมเชิงลบ แต่ภาพรวมยังส่งผลเชิงบวกต่อการจัดการภูมิคุ้มกันดิจิทัลในระดับสูง

4.2.4 ด้านการจัดการองค์กรดิจิทัล

ผลการวิเคราะห์พบว่า ด้านการจัดการองค์กรดิจิทัล (DEM) มีผลต่อสมการเชิงโครงสร้างแบบจำลองปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยเป็นอิทธิพลทางตรงจำนวน 2 เส้นทาง และอิทธิพลทางอ้อมจำนวน 1 เส้นทาง สรุปได้ดังนี้

4.2.4.1 ด้านการจัดการองค์กรดิจิทัลมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) สูงที่สุด เท่ากับ 0.83 แสดงให้เห็นว่า การบริหารจัดการองค์กรดิจิทัลที่มีประสิทธิภาพ ทั้งด้านกลยุทธ์ โครงสร้างพื้นฐาน และการจัดการข้อมูล สามารถสนับสนุนการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ได้อย่างชัดเจน

4.2.4.2 ด้านการจัดการองค์กรดิจิทัลมีอิทธิพลทางตรงเชิงลบต่อการจัดการภูมิคุ้มกันดิจิทัล (DIM) เท่ากับ -0.10 แสดงให้เห็นว่า การเปลี่ยนผ่านองค์กรสู่ดิจิทัลอย่างรวดเร็ว อาจก่อให้เกิดความเสี่ยงหรือช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์

4.2.4.3 ด้านการจัดการองค์กรดิจิทัลมีอิทธิพลทางอ้อมต่อการจัดการภูมิคุ้มกันดิจิทัลผ่านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เท่ากับ 0.06 และมีอิทธิพลรวมเท่ากับ -0.04 แสดงให้เห็นว่าแม้การจัดการองค์กรดิจิทัลจะช่วยสนับสนุนสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ แต่ในภาพรวมยังมีผลกระทบเชิงลบต่อการจัดการภูมิคุ้มกันดิจิทัล

4.2.5 ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการวิเคราะห์พบว่า ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) มีผลต่อสมการเชิงโครงสร้างแบบจำลองปัจจัยที่มีอิทธิพลต่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยเป็นอิทธิพลทางตรงจำนวน 1 เส้นทาง สรุปได้ดังนี้

4.2.5.1 ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์มีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัล (DIM) เท่ากับ 0.07 แสดงให้เห็นว่า การบูรณาการสถาปัตยกรรมองค์กรร่วมกับเทคโนโลยีปัญญาประดิษฐ์สามารถช่วยสนับสนุนการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ และการบริหารจัดการความเสี่ยงของสถาบันอุดมศึกษาได้

4.2.6 ด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการวิเคราะห์พบว่า แบบจำลองสามารถอธิบายความแปรปรวนของการจัดการภูมิคุ้มกันดิจิทัล (DIM) ได้ร้อยละ 81 ($R^2 = 0.81$) แสดงให้เห็นว่า ตัวแปรด้านโครงสร้างองค์กร ด้านเทคโนโลยีอัจฉริยะ ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล และด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ สามารถร่วมกันอธิบายการจัดการภูมิคุ้มกันดิจิทัลได้ในระดับสูง โดยเฉพาะด้านระบบภูมิคุ้มกันดิจิทัลที่มีอิทธิพลรวมสูงที่สุด เท่ากับ 0.70 รองลงมาคือ ด้านโครงสร้างองค์กร เท่ากับ 0.18 และด้านเทคโนโลยีอัจฉริยะ เท่ากับ 0.12 ตามลำดับ

4.3 ผลการวิเคราะห์เส้นอิทธิพลสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

จากผลการวิเคราะห์แบบจำลองสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ประกอบด้วย ด้านโครงสร้างองค์กร ด้านเทคโนโลยีอัจฉริยะ ด้านระบบภูมิคุ้มกันดิจิทัล ด้านการจัดการองค์กรดิจิทัล ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และตัวแปรผลด้านการจัดการภูมิคุ้มกันดิจิทัล สรุปผลการทดสอบอิทธิพลทางตรง อิทธิพลทางอ้อม อิทธิพลรวม และสรุปผลการทดสอบสมมติฐานงานวิจัยของแบบจำลองสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ได้ดังตารางที่ 4-21 ดังนี้

ตารางที่ 4-21 ผลการวิเคราะห์เส้นอิทธิพลสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตัวแปร	อิทธิพล	ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	ด้านการจัดการภูมิคุ้มกันดิจิทัล
ด้านโครงสร้างองค์กร	อิทธิพลทางตรง	0.02	0.09
	อิทธิพลทางอ้อม	-	0.09
	อิทธิพลโดยรวม	0.02	0.18
ด้านเทคโนโลยีอัจฉริยะ	อิทธิพลทางตรง	0.24	0.10
	อิทธิพลทางอ้อม	-	0.02
	อิทธิพลโดยรวม	0.24	0.12
ด้านระบบภูมิคุ้มกันดิจิทัล	อิทธิพลทางตรง	-0.28	0.72
	อิทธิพลทางอ้อม	-	-0.02
	อิทธิพลโดยรวม	-0.28	0.70
ด้านการจัดการองค์กรดิจิทัล	อิทธิพลทางตรง	0.83	-0.10
	อิทธิพลทางอ้อม	-	0.06
	อิทธิพลโดยรวม	0.83	-0.04
ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	อิทธิพลทางตรง	-	0.07
	อิทธิพลทางอ้อม	-	-
	อิทธิพลโดยรวม	-	0.07
R^2		**0.70 (70.0%)**	**0.81 (81.0%)**

ผลการวิเคราะห์ค่าอิทธิพลแบบจำลองสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา สรุปได้ว่า ปัจจัยที่มีอิทธิพลต่อการจัดการภูมิคุ้มกันดิจิทัลสูงที่สุด คือ ด้านระบบภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ 0.70 รองลงมา คือ ด้านโครงสร้างองค์กร มีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ 0.18 ด้านเทคโนโลยีอัจฉริยะ มีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ 0.12 และด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ 0.07 ตามลำดับ ในขณะที่ด้านการจัดการองค์กรดิจิทัลมีอิทธิพลเชิงลบ โดยมีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ -0.04 ทั้งนี้ ตัวแปรทั้งหมดสามารถร่วมกันอธิบายความแปรปรวนของการจัดการภูมิคุ้มกันดิจิทัลได้ร้อยละ 81.0 สำหรับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สูงที่สุด คือ ด้านการจัดการองค์กรดิจิทัล มีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ 0.83 รองลงมา คือ ด้านเทคโนโลยีอัจฉริยะ มีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ 0.24 ด้านโครงสร้างองค์กร มีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ 0.02 และด้านระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลเชิงลบ โดยมีค่าสัมประสิทธิ์อิทธิพลโดยรวมเท่ากับ -0.28 ทั้งนี้ ตัวแปรทั้งหมดสามารถร่วมกันอธิบายความแปรปรวนของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ได้ร้อยละ 70.0 จากผลการวิเคราะห์เส้นอิทธิพลแบบจำลองสมการเชิง

โครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา สามารถสรุปผลการทดสอบสมมติฐานการวิจัยได้ดังนี้

สมมติฐาน H1 : องค์ประกอบด้านโครงสร้างองค์กรส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H1 หรือองค์ประกอบด้านโครงสร้างองค์กรส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์เส้นทาง 0.02 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 70.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H2 : องค์ประกอบด้านโครงสร้างองค์กรส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการทดสอบเป็นการยอมรับ H2 หรือองค์ประกอบด้านโครงสร้างองค์กรส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์เส้นทาง 0.09 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H3 : องค์ประกอบด้านเทคโนโลยีอัจฉริยะส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H3 หรือองค์ประกอบด้านเทคโนโลยีอัจฉริยะส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์เส้นทาง 0.24 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 70.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H4 : องค์ประกอบด้านเทคโนโลยีอัจฉริยะส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการทดสอบเป็นการยอมรับ H4 หรือองค์ประกอบด้านเทคโนโลยีอัจฉริยะส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์เส้นทาง 0.10 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H5 : องค์ประกอบด้านระบบภูมิคุ้มกันดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H5 หรือองค์ประกอบด้านระบบภูมิคุ้มกันดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์เส้นทาง -0.28 ในเชิงลบ และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 70.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H6 : องค์ประกอบด้านระบบภูมิคุ้มกันดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการทดสอบเป็นการยอมรับ H6 หรือองค์ประกอบด้านระบบภูมิคุ้มกันดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์เส้นทาง 0.72 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H7 : องค์ประกอบด้านการจัดการองค์กรดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H7 หรือองค์ประกอบด้านการจัดการองค์กรดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์เส้นทาง 0.83 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 70.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H8 : องค์ประกอบด้านการจัดการองค์กรดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการทดสอบเป็นการยอมรับ H8 หรือองค์ประกอบด้านการจัดการองค์กรดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์เส้นทาง -0.10 ในเชิงลบ และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H9 : องค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัลได้รับอิทธิพลทางตรงและทางอ้อมจากองค์ประกอบด้านโครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล และสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H9 หรือองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัลได้รับอิทธิพลทั้งทางตรงและทางอ้อมจากองค์ประกอบด้านโครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล และสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ โดยแบบจำลองสามารถอธิบายการเปลี่ยนแปลงขององค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัลได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

ตารางที่ 4-22 สรุปผลการทดสอบสมมติฐานปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

สมมติฐาน		ผลการทดสอบ	อิทธิพล	สัมประสิทธิ์	R^2
H1	โครงสร้างองค์กรมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	ยอมรับสมมติฐาน	เชิงบวก	0.02	0.70
H2	โครงสร้างองค์กรมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัล	ยอมรับสมมติฐาน	เชิงบวก	0.18	0.81
H3	เทคโนโลยีอัจฉริยะมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	ยอมรับสมมติฐาน	เชิงบวก	0.24	0.70

สมมติฐาน		ผลการทดสอบ	อิทธิพล	สัมประสิทธิ์	R^2
H4	เทคโนโลยีอัจฉริยะมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัล	ยอมรับสมมติฐาน	เชิงบวก	0.12	0.81
H5	ระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	ยอมรับสมมติฐาน	เชิงลบ	-0.28	0.70
H6	ระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัล	ยอมรับสมมติฐาน	เชิงบวก	0.70	0.81
H7	การจัดการองค์กรดิจิทัลมีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	ยอมรับสมมติฐาน	เชิงบวก	0.83	0.70
H8	การจัดการองค์กรดิจิทัลมีอิทธิพลทางตรงต่อการจัดการภูมิคุ้มกันดิจิทัล	ยอมรับสมมติฐาน	เชิงลบ	–0.10	0.81
H9	การจัดการภูมิคุ้มกันดิจิทัลได้รับอิทธิพลทั้งทางตรงและทางอ้อมผ่านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์	ยอมรับสมมติฐาน	เชิงบวก	0.07	0.81

บทที่ 5
สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

การวิเคราะห์และการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาที่เป็นเป้าหมายในการวางแผนพัฒนาความสามารถของสถาบันอุดมศึกษาในการป้องกัน รับมือ และปรับตัวต่อความเสี่ยงและภัยคุกคามทางดิจิทัลได้อย่างมีประสิทธิภาพและยั่งยืน โดยอาศัยการบูรณาการองค์ประกอบด้านสถาปัตยกรรมองค์กร เทคโนโลยีปัญญาประดิษฐ์ ระบบดิจิทัล และกลไกการบริหารจัดการเชิงกลยุทธ์เข้าด้วยกันอย่างเป็นรูปธรรม โดยใช้เป็นกรอบในการวางแผนและพัฒนาระบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ซึ่งประกอบด้วยการวิเคราะห์และออกแบบระบบสารสนเทศดิจิทัลเชิงบูรณาการ ทั้งในมิติของสถาปัตยกรรมองค์กรภาพรวม การกำหนดสถาปัตยกรรมด้านกระบวนการที่สอดคล้องกับยุทธศาสตร์การดำเนินงานและการบริหารความเสี่ยงของสถาบันอุดมศึกษา การกำหนดสถาปัตยกรรมด้านระบบสารสนเทศที่สนับสนุนการตัดสินใจเชิงอัจฉริยะ รวมถึงสถาปัตยกรรมด้านข้อมูลที่รองรับการวิเคราะห์ข้อมูลขนาดใหญ่ การเชื่อมโยงและบูรณาการข้อมูลจากหลายแหล่งอย่างเป็นระบบที่สามารถสนับสนุนระบบงานต่าง ๆ ของมหาวิทยาลัยให้มีประสิทธิภาพรายละเอียดพอสังเขปดังนี้

5.1 แผนและนโยบายที่เกี่ยวข้อง

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา มีความเกี่ยวข้องและสอดรับกับแผนและนโยบายภาครัฐอื่นๆ ที่เกี่ยวข้องดังนี้

5.1.1 แผนยุทธศาสตร์ชาติ

แผนยุทธศาสตร์ชาติเป็นกรอบการพัฒนาประเทศระยะยาวที่กำหนดทิศทางการพัฒนาในช่วงเวลา 20 ปี (พ.ศ. 2561-2580) โดยมีเป้าหมายเพื่อสร้างความมั่นคง มั่งคั่ง และยั่งยืนให้กับประเทศ ภายใต้บริบทของการเปลี่ยนแปลงทางเศรษฐกิจ สังคม และเทคโนโลยีระดับโลก ยุทธศาสตร์ชาติมีความสำคัญในฐานะกรอบแม่บทที่ทุกหน่วยงานภาครัฐ รวมถึงสถาบันอุดมศึกษา ต้องใช้เป็นแนวทางในการกำหนดนโยบาย แผนงาน และโครงการพัฒนา

ยุทธศาสตร์ชาติประกอบด้วยหลายด้านที่มีความเชื่อมโยงกับการพัฒนาเทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ ได้แก่

1.1 ด้านการสร้างความสามารถในการแข่งขัน

ยุทธศาสตร์ด้านนี้มุ่งเน้นการยกระดับขีดความสามารถของประเทศผ่านการใช้เทคโนโลยี นวัตกรรม และดิจิทัลแพลตฟอร์ม เพื่อเพิ่มผลิตภาพ (Productivity) และสร้างมูลค่าเพิ่มในระบบเศรษฐกิจ การส่งเสริมเทคโนโลยีขั้นสูง เช่น ปัญญาประดิษฐ์ (AI) การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) และระบบอัตโนมัติ ถือเป็นกลไกสำคัญในการขับเคลื่อนประเทศสู่เศรษฐกิจดิจิทัล

สำหรับสถาบันอุดมศึกษา ยุทธศาสตร์ด้านนี้ส่งผลโดยตรงต่อการพัฒนาระบบสารสนเทศ การวิจัยด้าน AI และการผลิตกำลังคนที่มีทักษะดิจิทัลขั้นสูง ซึ่งสอดคล้องกับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อรองรับการบริหารจัดการและนวัตกรรมในมหาวิทยาลัย

1.2 ด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์

ยุทธศาสตร์ชาติมุ่งเน้นการพัฒนาทักษะใหม่ (New Skills) ที่สอดคล้องกับโลกดิจิทัล โดยเฉพาะทักษะด้านเทคโนโลยีดิจิทัล การคิดวิเคราะห์ข้อมูล และความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ สถาบันอุดมศึกษาจึงมีบทบาทสำคัญในการพัฒนาหลักสูตร งานวิจัย และการฝึกอบรมเพื่อยกระดับทักษะดังกล่าว การออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์จึงควรบูรณาการกลไกการพัฒนาบุคลากร การจัดการองค์ความรู้ และการสร้างวัฒนธรรมองค์กรที่ขับเคลื่อนด้วยข้อมูล เพื่อให้สอดคล้องกับยุทธศาสตร์การพัฒนาทุนมนุษย์ของประเทศ

1.3 ด้านการสร้างโอกาสและความเสมอภาคทางสังคม

การใช้เทคโนโลยีดิจิทัลเพื่อเพิ่มโอกาสการเข้าถึงการศึกษาและบริการสาธารณะอย่างทั่วถึงเป็นอีกหนึ่งเป้าหมายสำคัญของยุทธศาสตร์ชาติ เทคโนโลยี AI สามารถช่วยวิเคราะห์ข้อมูลนักศึกษาเพื่อพัฒนาระบบช่วยเหลือเฉพาะบุคคล ลดความเหลื่อมล้ำทางการศึกษา และสนับสนุนการเรียนรู้ตลอดชีวิต

1.4 ด้านการสร้างความมั่นคงและความปลอดภัย

ในยุคดิจิทัล ความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นสำคัญระดับชาติ ยุทธศาสตร์ชาติจึงเน้นการพัฒนาระบบป้องกันภัยคุกคามไซเบอร์และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งเชื่อมโยงโดยตรงกับแนวคิด “ภูมิคุ้มกันดิจิทัล (Digital Immunity)” ในสถาบันอุดมศึกษา ที่ต้องมีระบบเฝ้าระวัง ตรวจจับ และตอบสนองต่อภัยคุกคามอย่างมีประสิทธิภาพ

ยุทธศาสตร์ชาติถือเป็นแผนแม่บทสูงสุดของประเทศ โดยงานวิจัยนี้ตอบสนองต่อยุทธศาสตร์หลัก 2 ด้าน คือ 1) ด้านความมั่นคง มุ่งเน้นการสร้างสภาพแวดล้อมที่ปลอดภัยจากภัยคุกคามทุกรูปแบบ โดยเฉพาะภัยคุกคามในมิติใหม่ งานวิจัยเรื่อง "ภูมิคุ้มกันดิจิทัล (Digital Immunity)" สอดคล้องกับเป้าหมายการเพิ่มขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์เพื่อรักษาความมั่นคงของฐานข้อมูลงานวิจัยและข้อมูลส่วนบุคคลในสถาบันการศึกษา และ 2) ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ มุ่งเน้นการใช้เทคโนโลยีดิจิทัลในการบริหาร

จัดการองค์กรให้มีประสิทธิภาพ (Digital Government) การออกแบบ "สถาปัตยกรรมองค์กร (EA)" จึงเป็นเครื่องมือสำคัญตามแนวทางของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

5.1.2 แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

ในยุคแห่งการเปลี่ยนผ่านสู่ดิจิทัล (Digital Transformation) ประเทศไทยได้ให้ความสำคัญกับการวางรากฐานเชิงยุทธศาสตร์เพื่อใช้เทคโนโลยีดิจิทัลเป็นกลไกหลักในการขับเคลื่อนประเทศ โดยมี แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (Digital Economy Plan) เป็นพิมพ์เขียวสำคัญที่กำหนดทิศทางให้ประเทศไทยมุ่งสู่การเป็นประเทศที่สามารถใช้ประโยชน์จากนวัตกรรมดิจิทัลได้อย่างเต็มศักยภาพ แผนดังกล่าวมิได้จำกัดเพียงการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีเท่านั้น แต่ยังครอบคลุมถึงการสร้างสังคมที่เท่าเทียม การยกระดับขีดความสามารถในการแข่งขัน และการสร้างความมั่นคงปลอดภัยในโลกไซเบอร์ ซึ่งสอดคล้องอย่างมีนัยสำคัญกับบริบทของสถาบันอุดมศึกษาที่ต้องปรับตัวสู่การเป็นมหาวิทยาลัยอัจฉริยะ (Smart University)

ภายใต้คุณลักษณะสำคัญของพลวัตเทคโนโลยีดิจิทัล แผนพัฒนาฯ ได้ชี้ให้เห็นว่าเทคโนโลยีจะแทรกซึมไปในทุกมิติของกิจกรรมทางเศรษฐกิจและสังคม โดยมีปัจจัยชี้ขาดคือการเปลี่ยนบทบาทของประชาชนจาก "ผู้ใช้" สู่ "ผู้สร้างมูลค่า" (Value Creator) ผ่านการเข้าถึงทรัพยากรอย่างไร้พรมแดนและการใช้ประโยชน์จากข้อมูลมหาศาล (Big Data) ด้วยเหตุนี้ การออกแบบ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) จึงถือเป็นหัวใจสำคัญในการจัดระเบียบโครงสร้างองค์กรให้มีความยืดหยุ่นและรองรับนวัตกรรมพลิกผัน (Disruptive Innovation) ตามเจตนารมณ์ของแผนพัฒนาประเทศ

ในการพัฒนาประเทศด้วยเทคโนโลยีดิจิทัลในบริบทของสถาบันอุดมศึกษาสามารถพิจารณาผ่านมิติที่สำคัญ 5 ด้านหลัก ดังนี้

มิติที่ 1 การเชื่อมต่อ (Connectivity) ซึ่งไม่ได้จำกัดเพียงการพัฒนาโครงสร้างพื้นฐานทางกายภาพหรือเครือข่ายบรอดแบนด์คุณภาพสูงเท่านั้น แต่ยังมุ่งเน้นการสร้างระบบนิเวศดิจิทัลที่เชื่อมโยงทรัพยากร บุคคล และอุปกรณ์อัจฉริยะ (Internet of Everything) เข้าด้วยกันอย่างเป็นระบบ เพื่อเป็นรากฐานสำคัญในการจัดวางสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ที่สามารถตอบสนองต่อการใช้งานและเสริมสร้างภูมิคุ้มกันดิจิทัลได้อย่างไร้รอยต่อ

มิติที่ 2 ด้านทักษะดิจิทัล (Human Capital/Digital Skill) ซึ่งถือเป็นกลไกสำคัญในการขับเคลื่อนขีดความสามารถทางการแข่งขันของสถาบัน การพัฒนาทักษะด้านดิจิทัลในยุคปัญญาประดิษฐ์จึงเป็นทักษะพื้นฐานที่จำเป็นอย่างยิ่ง ไม่เพียงเพื่อการใช้ประโยชน์จากเทคโนโลยีอย่างสร้างสรรค์เท่านั้น แต่ยังรวมถึงการสร้างความตระหนักรู้และการเฝ้าระวังภัยคุกคามทางไซเบอร์

เพื่อลดผลกระทบเชิงลบที่อาจเกิดขึ้นจากการใช้งานเทคโนโลยีในทางที่ไม่เหมาะสม ซึ่งสอดคล้องกับแนวคิดการสร้างภูมิคุ้มกันดิจิทัลที่ให้ความสำคัญกับศักยภาพของบุคลากรเป็นอันดับต้นๆ

มิติที่ 3 การขับเคลื่อนด้วยข้อมูลผ่านเครือข่าย (Data Driven) ซึ่งเป็นปัจจัยชี้ขาดในการเปลี่ยนผ่านสู่ยุคอุตสาหกรรม 4.0 และมหาวิทยาลัยดิจิทัล เมื่อโลกทางกายภาพและโลกเสมือนผนวกเข้าด้วยกัน สถาบันอุดมศึกษาจึงกลายเป็นแหล่งผลิตและแลกเปลี่ยนข้อมูลจำนวนมหาศาลบนระบบเครือข่าย การออกแบบสถาปัตยกรรมองค์กรในงานวิจัยนี้จึงมุ่งเน้นการนำข้อมูลขนาดใหญ่ (Big Data) มาทำการวิเคราะห์และประมวลผลด้วยปัญญาประดิษฐ์ เพื่อให้เกิดประโยชน์สูงสุดในการบริหารจัดการความปลอดภัยเชิงรุก ช่วยให้การตอบสนองต่อสถานการณ์ความเสี่ยงเป็นไปอย่างรวดเร็วและมีประสิทธิภาพสูงสุดตามทิศทางการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศ

มิติที่ 4 เทคโนโลยีเปลี่ยนโลก (Digital Disruption) ซึ่งเทคโนโลยีดิจิทัลที่ทันสมัยได้เข้ามาพลิกโฉมกฎเกณฑ์และโครงสร้างการดำเนินชีวิตรวมถึงรูปแบบธุรกิจเดิมอย่างสิ้นเชิง สถาบันอุดมศึกษาจึงจำเป็นต้องปรับตัวจากการเป็นเพียงแหล่งส่งผ่านความรู้ สู่การเป็นองค์กรที่ขับเคลื่อนด้วยเทคโนโลยีอุบัติใหม่ การออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ในงานวิจัยนี้ จึงทำหน้าที่เป็นโครงสร้างรองรับการเปลี่ยนแปลง (Adaptive Structure) ที่เปลี่ยนจากการจัดเก็บข้อมูลในรูปแบบเดิมไปสู่ระบบคลาวด์คอมพิวติ้ง (Cloud Computing) และการใช้ AI ในการบริหารจัดการองค์กร เพื่อให้สถาบันสามารถดำรงอยู่และก้าวหน้าได้ภายใต้กระแสการเปลี่ยนแปลงทางเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็ว

มิติที่ 5 การสร้างบริการสาธารณะในระบบดิจิทัล (Digital Public Service) ซึ่งเน้นการพัฒนาคุณภาพชีวิตและความสะดวกสบายผ่านการเข้าถึงบริการได้ทุกที่ทุกเวลา สถาปัตยกรรมองค์กรที่ผู้วิจัยนำเสนอได้ประยุกต์ใช้แนวคิดนี้ผ่านการสร้างระบบนิเวศการเรียนรู้และบริการสนับสนุนที่เป็นดิจิทัล (Digital Campus Services) โดยมี "ภูมิคุ้มกันดิจิทัล" เป็นหัวใจสำคัญในการสร้างความมั่นใจและความปลอดภัยให้แก่ผู้ใช้งาน การบูรณาการ AI เข้ามาในระบบบริการสาธารณะของสถาบันอุดมศึกษา ไม่เพียงแต่ช่วยอำนวยความสะดวกในการเข้าถึงข้อมูลและการเรียนรู้ผ่านแอปพลิเคชันเคลื่อนที่ แต่ยังเป็นการสร้างมาตรฐานใหม่ของบริการภาครัฐที่ทุกคนสามารถเข้าถึงได้อย่างเท่าเทียม ปลอดภัย และมีประสิทธิภาพสูง สอดคล้องกับยุทธศาสตร์การพัฒนาประเทศสู่สังคมดิจิทัลอย่างยั่งยืน (สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, 2561)

ความก้าวหน้าอย่างก้าวกระโดดของเทคโนโลยีดิจิทัลในปัจจุบันส่งผลกระทบเชิงโครงสร้างต่อสถาบันอุดมศึกษาในฐานะหน่วยงานหลักของการพัฒนาประเทศ ผู้วิจัยจึงได้นำประเด็นสำคัญมาวิเคราะห์เพื่อกำหนดทิศทางการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ดังนี้

1. การปรับตัวต่อการเปลี่ยนแปลงทางนวัตกรรมและระบบอัจฉริยะ (Disruptive Innovation & Smart Everything) สถาบันอุดมศึกษาต้องเผชิญกับนวัตกรรมพลิกผัน เช่น AI, 5G

และ Predictive Analytics ซึ่งเปลี่ยนบทบาทของมหาวิทยาลัยจากเพียงผู้ส่งผ่านความรู้สู่การเป็น "Smart Campus" ที่ใช้ระบบอัจฉริยะในการบริหารจัดการ สถาปัตยกรรมที่ออกแบบจึงต้องรองรับการเชื่อมต่อกับอุปกรณ์เซ็นเซอร์และแอปพลิเคชันอัจฉริยะในทุกกิจกรรม ตั้งแต่การเรียนการสอนไปจนถึงการเฝ้าระวังภัยพิบัติ เพื่อสร้างสภาพแวดล้อมที่เอื้อต่อการเรียนรู้ยุคใหม่

2. การเปลี่ยนผ่านสู่เศรษฐกิจนวัตกรรมและการผลิต (Consumption to Production & Innovation Economy) ในยุคที่ผู้บริโภคกลายเป็นผู้ผลิต (Prosumer) และการแข่งขันตั้งอยู่บนพื้นฐานของนวัตกรรมสินค้าและบริการ มหาวิทยาลัยจึงต้องปรับกระบวนการทางธุรกิจ (Business Architecture) เพื่อสร้างมูลค่าเพิ่มให้นักศึกษาและนักวิจัย โดยการใช้ระบบ Cloud และ AI เข้ามาเพิ่มความยืดหยุ่นในการทำงานร่วมกัน ทำให้ห่วงโซ่อุปทานของการผลิตองค์ความรู้มีประสิทธิภาพสูงขึ้นและตอบสนองความต้องการของตลาดที่เปลี่ยนแปลงตลอดเวลา

3. การบริหารจัดการข้อมูลขนาดใหญ่และความเป็นส่วนตัว (Big Data & Data Privacy) เมื่อข้อมูลกลายเป็นทรัพยากรที่มีค่าที่สุด สถาปัตยกรรมข้อมูล (Data Architecture) ในงานวิจัยนี้จึงมุ่งเน้นการเพิ่มศักยภาพในการวิเคราะห์ข้อมูลมหาศาลที่เกิดจากผู้ใช้งานและอุปกรณ์ IoT โดยเฉพาะอย่างยิ่งการให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ซึ่งเป็นประเด็นที่ละเอียดอ่อนที่สุดในยุค Big Data เพื่อสร้างความเชื่อมั่นในการแลกเปลี่ยนข้อมูลภายในสถาบัน

4. การจัดการความเสี่ยงและภูมิคุ้มกันไซเบอร์ (Cybersecurity & Digital Immunity) ประเด็นสำคัญที่สุดคือความเสี่ยงด้านความปลอดภัยไซเบอร์ที่ซับซ้อนขึ้น เช่น การจารกรรมข้อมูลและการโจมตีโครงสร้างพื้นฐาน ภูมิคุ้มกันดิจิทัล (Digital Immunity) ที่ผู้วิจัยนำเสนอจึงถูกออกแบบให้เป็นระบบเชิงรุกที่สามารถตรวจจับความผิดปกติได้โดยอัตโนมัติ เพื่อป้องกันระบบเศรษฐกิจดิจิทัลของสถาบันไม่ให้หยุดชะงัก และรักษาความปลอดภัยต่อชีวิตและทรัพย์สินของบุคลากรจากการโจมตีที่พัฒนาอย่างรวดเร็ว

5. การพลิกโฉมโครงสร้างกำลังคนและบทบาททางการศึกษา (Human Capital Transformation) อิทธิพลของเทคโนโลยีดิจิทัลส่งผลต่อการเปลี่ยนบทบาทของบุคลากร เช่น อาจารย์เปลี่ยนจาก "ผู้สอน" เป็น "ผู้อำนวยการสอน" (Facilitator) และความต้องการผู้เชี่ยวชาญด้านข้อมูลและไซเบอร์ที่เพิ่มขึ้น สถาปัตยกรรมองค์กรที่ออกแบบจึงต้องรองรับการพัฒนาทักษะ (Upskill/Reskill) และการทำงานร่วมกับระบบอัตโนมัติ เพื่อให้กำลังคนในสถาบันอุดมศึกษาสามารถก้าวข้ามผลกระทบเชิงลบและใช้ประโยชน์จากเทคโนโลยีได้อย่างสูงสุด

โดยแนวทางการพัฒนาสถาปัตยกรรมองค์กรในงานวิจัยนี้ ตั้งอยู่บนคุณลักษณะสำคัญของพลวัตเทคโนโลยีดิจิทัลที่ส่งผลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ดังนี้

1. การสร้างเครือข่ายความร่วมมือไร้พรมแดน (Seamless Connectivity & Global Collaboration) สถาปัตยกรรมองค์กรที่ออกแบบมุ่งเน้นการใช้เทคโนโลยีดิจิทัลเป็นเครื่องมือหลักในการเชื่อมต่อกิจกรรมทางวิชาการและงานวิจัยระหว่างประชาคมภายในสถาบันและระดับโลก การออกแบบในเลเยอร์สถาปัตยกรรมธุรกิจ (Business Architecture) จึงเน้นการแบ่งปันทรัพยากรและองค์ความรู้แนวใหม่ที่เปิดโอกาสให้คณาจารย์และนักศึกษาเข้าถึงข้อมูลได้อย่างทั่วถึงและเท่าเทียม โดยมีระบบ AI ช่วยบริหารจัดการสิทธิและการเข้าถึงอย่างปลอดภัย เพื่อสร้างความเชื่อมั่นในการร่วมมือระดับนานาชาติ

2. การขับเคลื่อนด้วยนวัตกรรมดิจิทัลเพื่อสร้างคุณค่า (Innovation-Driven & Value Creation) เพื่อยกระดับขีดความสามารถทางการแข่งขันในระดับสากล สถาปัตยกรรมองค์กรปัญญาประดิษฐ์นี้ถูกออกแบบมาเพื่อสร้าง "คุณค่า" (Value Creation) ผ่านกระบวนการทำงานที่ชาญฉลาด การนำ AI มาจัดการภูมิคุ้มกันดิจิทัลไม่เพียงแต่ทำหน้าที่ป้องกันภัยคุกคาม แต่ยังช่วยยกระดับคุณภาพชีวิตดิจิทัล (Digital Well-being) ให้กับพลเมืองในมหาวิทยาลัย ทำให้การประกอบกิจกรรมทางเศรษฐกิจและสังคมภายในสถาบันมีความคล่องตัวและปลอดภัย นำไปสู่การพัฒนาอย่างยั่งยืนตามทิศทางนวัตกรรมดิจิทัลของประเทศ

3. การใช้ประโยชน์จากข้อมูลมหาศาลและการวิเคราะห์เชิงลึก (Big Data Analytics & IoT) หัวใจสำคัญของสถาปัตยกรรมข้อมูล (Data Architecture) คือการบริหารจัดการข้อมูลจำนวนมหาศาลที่เกิดขึ้นทั้งจากการบันทึกโดยบุคคลและข้อมูลจากอุปกรณ์ Internet of Things (IoT) ระบบที่ผู้วิจัยนำเสนอใช้ปัญญาประดิษฐ์ในการวิเคราะห์ข้อมูลผ่านระบบประมวลผลขนาดใหญ่ เพื่อปรับปรุงประสิทธิภาพการดำเนินงานและการให้บริการทางการศึกษา ข้อมูลเหล่านี้จะถูกนำมาวิเคราะห์พฤติกรรมเสี่ยงเพื่อสร้างภูมิคุ้มกันเชิงรุก (Predictive Security) ช่วยให้สถาบันมีความได้เปรียบในการแข่งขันและสามารถตอบสนองความต้องการของประชาชนและผู้เรียนได้อย่างแม่นยำ

4. การแทรกซึมทางเทคโนโลยีเพื่อสร้างโอกาสและสังคมแห่งผู้ผลิต (Digital Pervasiveness & Prosumer Society) ในมิตินี้ สถาปัตยกรรมแอปพลิเคชัน (Application Architecture) ถูกออกแบบให้เทคโนโลยีดิจิทัลแทรกซึมไปสู่ทุกภาคส่วนของมหาวิทยาลัย เพื่อสร้างโอกาสให้คนทุกกลุ่มได้มีส่วนร่วมในการเปลี่ยนสถานะจาก "ผู้ใช้" สู่ "ผู้ผลิต" (Prosumer) ที่สามารถสร้างนวัตกรรมและมูลค่าเพิ่มได้เอง ภูมิคุ้มกันดิจิทัลที่เข้มแข็งจะทำหน้าที่เป็นเกราะป้องกันให้นักศึกษาสามารถสร้างสรรค์ผลงานดิจิทัลและประกอบกิจกรรมทางเศรษฐกิจยุคใหม่ได้อย่างมั่นใจ ส่งเสริมให้สถาบันอุดมศึกษากลายเป็นฐานรากสำคัญในการนำพาประเทศไทยไปสู่สังคมที่ทุกคนสามารถสร้างมูลค่าจากเทคโนโลยีได้อย่างแท้จริง

5.1.3 แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นที่ 23 การวิจัยและพัฒนานวัตกรรม (พ.ศ. 2561 – 2580)

การออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาในงานวิจัยนี้ มีความสอดคล้องอย่างมีนัยสำคัญกับ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นที่ 23 การวิจัยและพัฒนานวัตกรรม (พ.ศ. 2561 – 2580) ที่มุ่งเน้นการใช้นวัตกรรมเป็นตัวขับเคลื่อนการพัฒนาประเทศเพื่อเปลี่ยนโครงสร้างเศรษฐกิจไปสู่การสร้างมูลค่า (Value-Based Economy) โดยการวิจัยนี้ได้บูรณาการแนวทางจาก แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อยกระดับสถาบันอุดมศึกษาให้ก้าวสู่การเป็นมหาวิทยาลัยอัจฉริยะที่สามารถรองรับ เทคโนโลยีเปลี่ยนโลก (Digital Disruption)ได้อย่างมีประสิทธิภาพ ผ่านการประยุกต์ใช้เทคโนโลยีอุบัติใหม่ เช่น ปัญญาประดิษฐ์ (AI), การประมวลผลบนคลาวด์ (Cloud Computing) และระบบความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เพื่อสร้างกลไกการป้องกันเชิงรุกที่เรียกว่า "ภูมิคุ้มกันดิจิทัล" ซึ่งเป็นปัจจัยชี้ขาดในการสร้างความเชื่อมั่นและความปลอดภัย (Trust & Security) ให้กับทรัพยากรดิจิทัลของสถาบันสอดคล้องกับมาตรฐานของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

ในการขับเคลื่อนสถาบันสู่เศรษฐกิจและสังคมดิจิทัลนั้น ผู้วิจัยได้ยึดคุณลักษณะสำคัญ 5 มิติ เป็นฐานรากในการออกแบบสถาปัตยกรรม เริ่มจากการสร้าง การเชื่อมต่อ (Connectivity) ที่ไม่ได้จำกัดเพียงโครงสร้างพื้นฐานทางกายภาพ แต่เป็นการเชื่อมโยงทรัพยากรและบุคคลเข้าด้วยกันอย่างไร้พรมแดน เพื่อส่งเสริม มิติด้านทักษะดิจิทัล (Human Capital) ให้แก่บุคลากรและนักศึกษา ให้มีความฉลาดรู้และเท่าทันต่อภัยคุกคาม ควบคู่ไปกับ การใช้ข้อมูลผ่านเครือข่าย (Data Driven) ซึ่งเป็นการนำข้อมูลมหาศาล (Big Data) ที่เกิดจากทั้งผู้ใช้งานและอุปกรณ์เซ็นเซอร์ (IoT) มาวิเคราะห์ผ่านระบบประมวลผลขนาดใหญ่เพื่อปรับปรุงประสิทธิภาพการดำเนินงานและการบริการสาธารณะในระบบดิจิทัล (Digital Public Service) อันจะนำไปสู่การเพิ่มขีดความสามารถทางการแข่งขันในระดับสากลและยกระดับคุณภาพชีวิตของประชาคมในสถาบันอุดมศึกษาอย่างยั่งยืน

นอกจากนี้ อิทธิพลของเทคโนโลยีดิจิทัลยังก่อให้เกิดการเปลี่ยนแปลงเชิงโครงสร้างใน 8 ประเด็นหลัก โดยเฉพาะการเกิด นวัตกรรมอย่างพลิกผัน (Disruptive Innovation) และการเปลี่ยนผ่านจาก สังคมการบริโภคสู่สังคมแห่งการผลิต (Consumption to Production) ที่ทุกคนสามารถสร้างมูลค่าเพิ่มได้ด้วยตนเอง สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ที่นำเสนอนี้จึงทำหน้าที่เป็นโครงสร้างรองรับการเปลี่ยนแปลงของกำลังคน ที่เปลี่ยนบทบาทจากผู้สอนสู่ผู้อำนวยการสอน และเตรียมความพร้อมในการรับมือกับ ความเสี่ยงด้านความปลอดภัยไซเบอร์ ที่พัฒนาอย่างรวดเร็วและสลับซับซ้อน การที่เทคโนโลยีดิจิทัลแทรกซึมไปในทุกภาคส่วน (Smart Everything) จึงเป็นทั้งโอกาสและประเด็นสำคัญที่ต้องมีการคุ้มครองข้อมูลส่วนบุคคลอย่างเข้มงวด สถาปัตยกรรมนี้จึง

เปรียบเสมือนพิมพ์เขียวที่ช่วยให้สถาบันอุดมศึกษาสามารถปรับตัวและสร้างนวัตกรรมสินค้าและบริการที่ตอบสนองต่อตลาดโลกได้อย่างมั่นคงภายใต้ระบบภูมิคุ้มกันดิจิทัลที่ชาญฉลาด

แผนแม่บทประเด็นนี้มุ่งเน้นการใช้ "การวิจัยและนวัตกรรม" เป็นตัวขับเคลื่อนการพัฒนาประเทศในทุกมิติ เพื่อเปลี่ยนโครงสร้างเศรษฐกิจไปสู่การสร้างมูลค่า (Value-Based Economy) โดยมีประเด็นที่สอดรับกับงานวิจัยดังนี้

1. การพัฒนาระบบนิเวศวิจัยและนวัตกรรม (Research and Innovation Ecosystem)

เป้าหมายแผนแม่บท มุ่งสร้างโครงสร้างพื้นฐานและระบบสนับสนุนที่เอื้อต่อการสร้างนวัตกรรมที่ใช้ประโยชน์ได้จริง

การประยุกต์ในงานวิจัย การออกแบบ "สถาปัตยกรรมองค์กร (EA)" ในเลเยอร์เทคโนโลยีและแอปพลิเคชัน คือการสร้างระบบนิเวศดิจิทัลภายในสถาบันอุดมศึกษา AI จะทำหน้าที่เป็นเครื่องมืออัจฉริยะที่ช่วยจัดการโครงสร้างพื้นฐานให้มีความยืดหยุ่นและพร้อมรับการเปลี่ยนแปลง (Agility) สอดคล้องกับแนวทางการพัฒนาระบบนิเวศที่ทันสมัย

2. การพัฒนานวัตกรรมเพื่อความมั่นคงปลอดภัย (Innovation for Security)

เป้าหมายแผนแม่บท สนับสนุนงานวิจัยที่สร้างความมั่นคงในมิติต่างๆ รวมถึงภัยคุกคามรูปแบบใหม่

การประยุกต์ในงานวิจัย แนวคิด "ภูมิคุ้มกันดิจิทัล (Digital Immunity)" ถือเป็นนวัตกรรมเชิงกระบวนการ (Process Innovation) ที่ใช้ AI ในการวิเคราะห์และป้องกันภัยไซเบอร์เชิงรุก ซึ่งตอบโจทย์การสร้างนวัตกรรมเพื่อความปลอดภัยของฐานข้อมูลงานวิจัยและทรัพยากรดิจิทัลของสถาบันอุดมศึกษา

3. การขับเคลื่อนด้วยข้อมูลและปัญญาประดิษฐ์ (Data-Driven & AI Innovation)

เป้าหมายแผนแม่บท เร่งส่งเสริมการใช้ข้อมูลขนาดใหญ่ (Big Data) และปัญญาประดิษฐ์ (AI) เพื่อยกระดับประสิทธิภาพการดำเนินงานของหน่วยงานภาครัฐและสถานศึกษา

การประยุกต์ในงานวิจัย สถาปัตยกรรมข้อมูลที่คุณออกแบบ มุ่งเน้นการจัดเก็บและวิเคราะห์ข้อมูลผ่านเครือข่าย เพื่อการตัดสินใจที่มีประสิทธิภาพ (Informed Decision Making) และการตรวจจับความผิดปกติแบบ Real-time ซึ่งเป็นการใช้เทคโนโลยีขั้นสูงตามที่แผนแม่บทประเด็นที่ 23 กำหนดไว้

5.1.4 นโยบายปัญญาประดิษฐ์แห่งชาติ (National AI Policy)

การออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลในงานวิจัยนี้ ได้ดำเนินการโดยสอดคล้องกับแนวทางของ แผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (พ.ศ. 2565 – 2570) ซึ่งถือเป็นนโยบายระดับชาติที่มุ่งเน้นการสร้างระบบนิเวศ AI ให้เป็นกลไกสำคัญในการยกระดับโครงสร้างพื้นฐานดิจิทัลและความมั่นคงของประเทศ โดยในส่วน

ของ ยุทธศาสตร์ที่ 1 ด้านจริยธรรมและกฎระเบียบ (AI Ethics & Governance) ผู้วิจัยได้นำมาเป็นพื้นฐานในการออกแบบธรรมาภิบาลข้อมูล (Data Governance) ภายในสถาบันอุดมศึกษา เพื่อให้มั่นใจว่าการใช้ AI ในการเฝ้าระวังภัยคุกคามและการวิเคราะห์พฤติกรรมผู้ใช้งานนั้นตั้งอยู่บนหลักความโปร่งใส ความรับผิดชอบ และการคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานสากลและกฎหมายที่เกี่ยวข้อง

ในมิติของ ยุทธศาสตร์ที่ 4 และ 5 การส่งเสริมการวิจัย นวัตกรรม และการประยุกต์ใช้ AI ในภาครัฐ สถาปัตยกรรมองค์กรที่นำเสนอได้เปลี่ยนบทบาทของ AI จากเพียงเครื่องมือประมวลผลทั่วไปสู่การเป็น "กลไกภูมิคุ้มกันดิจิทัลอัจฉริยะ" ที่มีความสามารถในการเรียนรู้และปรับตัว (Adaptive Learning) ต่อรูปแบบการโจมตีทางไซเบอร์ที่ซับซ้อน การบูรณาการ AI เข้ากับสถาปัตยกรรมระบบ (System Architecture) ช่วยให้มหาวิทยาลัยสามารถวิเคราะห์ข้อมูลขนาดใหญ่ที่ไหลผ่านเครือข่ายและอุปกรณ์เซ็นเซอร์ต่างๆ ได้แบบเรียลไทม์ เพื่อพยากรณ์และป้องกันการจารกรรมข้อมูลงานวิจัยหรือความเสียหายต่อระบบเทคโนโลยีสารสนเทศ

นอกจากนี้นโยบายในการพัฒนาทรัพยากรมนุษย์ โดยมุ่งหวังให้สถาปัตยกรรมที่ออกแบบมานี้เป็นเครื่องมือสนับสนุนการสร้าง ความฉลาดรู้ด้านปัญญาประดิษฐ์ (AI Literacy) ให้แก่ประชาคมในสถาบันอุดมศึกษา การจัดการภูมิคุ้มกันดิจิทัลที่เข้มแข็งจะช่วยสร้างความเชื่อมั่น (Trust) ในการนำเทคโนโลยี AI มาใช้ในการเรียนการสอนและการบริหารจัดการองค์กร ซึ่งเป็นการเปลี่ยนผ่านสถาบันสู่อนาคตตามนโยบายปัญญาประดิษฐ์แห่งชาติ ที่มุ่งหวังให้ประเทศไทยมีความมั่นคงปลอดภัยและมีขีดความสามารถในการแข่งขันในยุคเศรษฐกิจดิจิทัลอย่างยั่งยืน

5.1.5 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ในการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ผู้วิจัยได้กำหนดให้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เป็นฐานรากสำคัญในมิติด้านกฎหมายและจริยธรรมข้อมูล (Data Ethics) โดยเฉพาะอย่างยิ่งในสถาบันอุดมศึกษาซึ่งเป็นแหล่งรวบรวมข้อมูลส่วนบุคคลจำนวนมหาศาล ทั้งข้อมูลนิสิตนักศึกษา บุคลากร และข้อมูลการวิจัยที่ละเอียดอ่อน สถาปัตยกรรมที่นำเสนอจึงมุ่งเน้นการสร้างกลไกการกำกับดูแลข้อมูล (Data Governance) ที่สอดคล้องกับหลักการสำคัญของ PDPA ดังนี้

1. การรักษาความมั่นคงปลอดภัยและความถูกต้องของข้อมูล (Data Security and Integrity) สถาปัตยกรรมในเลเยอร์ข้อมูล (Data Architecture) ได้รับการออกแบบให้มีมาตรการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access) และการรั่วไหลของข้อมูล (Data Breach) โดยใช้ปัญญาประดิษฐ์เป็นเครื่องมือหลักในการตรวจจับพฤติกรรมที่ผิดปกติ (Anomaly Detection) ซึ่งถือเป็นส่วนหนึ่งของ "ภูมิคุ้มกันดิจิทัล" ที่ช่วยให้สถาบันสามารถปฏิบัติหน้าที่ตามที่กฎหมายกำหนดในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างเข้มงวด

2. การประยุกต์ใช้หลัก Privacy-by-Design ในระบบ AI ผู้วิจัยได้นำแนวคิดการคุ้มครองความเป็นส่วนตัวตั้งแต่เริ่มต้นออกแบบ (Privacy-by-Design) มาใช้ในระบบภูมิคุ้มกันดิจิทัล โดย AI จะทำการคัดกรองและประมวลผลข้อมูลในลักษณะที่ลดการระบุตัวตน (De-identification) หรือการใช้นามแฝง (Pseudonymization) ในขั้นตอนการวิเคราะห์พฤติกรรมเสี่ยงบนเครือข่าย เพื่อให้มั่นใจว่าการสร้างความปลอดภัยไซเบอร์จะไม่กระทบต่อสิทธิและเสรีภาพส่วนบุคคลของประชาคมในสถาบัน ตามเจตนารมณ์ของกฎหมาย PDPA ที่มุ่งสร้างความสมดุลระหว่างการใช้ประโยชน์จากข้อมูลและการคุ้มครองเจ้าของข้อมูล

3. การตอบสนองต่อเหตุละเมิดข้อมูลส่วนบุคคลอย่างทันท่วงที (Data Breach Response) หนึ่งในข้อกำหนดสำคัญของ PDPA คือการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายในเวลาที่กำหนด สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ในงานวิจัยนี้จึงออกแบบให้มีระบบการรายงานเหตุการณ์อัตโนมัติ (Automated Incident Reporting) เมื่อ AI ตรวจพบการบุกรุกหรือความเสี่ยงที่อาจนำไปสู่การรั่วไหลของข้อมูล ช่วยให้ผู้บริหารสถาบันสามารถตัดสินใจและดำเนินการเยียวยาได้อย่างรวดเร็ว ลดผลกระทบและความเสียหายที่จะเกิดขึ้นต่อชื่อเสียงและทรัพย์สินของสถาบัน

5.1.6 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

การบริหารจัดการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ผ่านสถาปัตยกรรมภูมิคุ้มกันดิจิทัล การออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลในงานวิจัยนี้ มีความสอดคล้องอย่างเคร่งครัดกับเจตนารมณ์ของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยเฉพาะในมิติของการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อโครงสร้างพื้นฐานสำคัญของสถาบันอุดมศึกษา ซึ่งมีประเด็นสำคัญที่นำมาบูรณาการ ดังนี้

1. การยกระดับการเฝ้าระวังภัยคุกคามในระดับโครงสร้างพื้นฐานสำคัญ (Critical Information Infrastructure: CII) ตามบทบัญญัติของ พ.ร.บ. ไซเบอร์ฯ สถาบันอุดมศึกษาถือเป็นหน่วยงานที่มีความสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศระดับชาติ สถาปัตยกรรมเทคโนโลยีที่นำเสนอจึงออกแบบให้มีระบบตรวจจับและแจ้งเตือนภัยคุกคามล่วงหน้าโดยใช้ AI (Predictive AI) เพื่อเฝ้าระวังเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงของระบบเครือข่ายวิจัยและฐานข้อมูลกลาง สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กำหนด

2. กลไกภูมิคุ้มกันดิจิทัลเพื่อการรับมือและเผชิญเหตุ (Incident Response & Mitigation) พ.ร.บ. ฉบับนี้เน้นย้ำถึงกระบวนการเผชิญเหตุอย่างมีประสิทธิภาพ ระบบภูมิคุ้มกันดิจิทัลที่ผู้วิจัยพัฒนาขึ้นจึงมิใช่เพียงระบบตั้งรับ แต่เป็นระบบที่สามารถตอบโต้ภัยคุกคามโดยอัตโนมัติ

(Automated Response) ในกรณีที่พบภัยคุกคามในระดับร้ายแรงหรือระดับวิกฤต การใช้ AI ช่วยลดระยะเวลาในการวิเคราะห์การโจมตี (Mean Time to Detect) และเพิ่มความรวดเร็วในการจำกัดวงความเสียหาย (Containment) ทำให้สถาบันสามารถประคับประคองการให้บริการทางการศึกษาได้อย่างต่อเนื่อง แม้จะอยู่ภายใต้สถานการณ์การโจมตีทางไซเบอร์

3. การสร้างความยืดหยุ่นและการทำงานร่วมกันตามกรอบกฎหมาย (Cyber Resilience & Collaboration) เพื่อให้สอดคล้องกับมาตรการป้องกันภายใต้ พ.ร.บ. ไซเบอร์ฯ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์นี้ได้ออกแบบเลเยอร์การบริหารจัดการ (Governance Layer) ให้รองรับการเชื่อมโยงข้อมูลภัยคุกคามกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) ที่เกี่ยวข้อง การมีภูมิคุ้มกันดิจิทัลที่ชาญฉลาดช่วยให้สถาบันอุดมศึกษามี "ความยืดหยุ่นทางไซเบอร์" (Cyber Resilience) ที่สามารถฟื้นฟูระบบให้กลับมาทำงานปกติได้โดยเร็ว ซึ่งเป็นตัวชี้วัดสำคัญขององค์กรดิจิทัลสมัยใหม่ตามแนวทางกฎหมายความมั่นคงไซเบอร์ของประเทศ

5.1.7 แผนยุทธศาสตร์การพัฒนาสถาบันอุดมศึกษา

การออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ในงานวิจัยนี้ ได้คำนึงถึงกรอบแนวทางตาม แผนยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (พ.ศ. 2566 – 2570) และยุทธศาสตร์การพัฒนาสถาบันอุดมศึกษาไทยที่มุ่งเน้นการปฏิรูปสถาบันให้เป็นกลไกหลักในการขับเคลื่อนเศรษฐกิจฐานนวัตกรรม โดยมีประเด็นสำคัญที่นำมาบูรณาการในสถาปัตยกรรมภูมิคุ้มกันดิจิทัล ดังนี้

1. การยกระดับสถาบันอุดมศึกษาสู่มหาวิทยาลัยดิจิทัลอัจฉริยะ (Smart Digital University) ตามยุทธศาสตร์การอุดมศึกษาที่เน้นการใช้เทคโนโลยีดิจิทัลเพื่อยกระดับประสิทธิภาพการบริหารจัดการและบริการการศึกษา สถาปัตยกรรมองค์กรที่ผู้วิจัยนำเสนอได้วางรากฐานการบริหารจัดการด้วยปัญญาประดิษฐ์ (AI-Driven Management) เพื่อเปลี่ยนผ่านระบบงานจากรูปแบบดั้งเดิมสู่ระบบอัตโนมัติที่มีความคล่องตัวสูง การสร้างภูมิคุ้มกันดิจิทัลจึงเปรียบเสมือนโครงสร้างความปลอดภัยที่เอื้อให้เกิดการเรียนรู้และการทำวิจัยบนระบบคลาวด์และเครือข่ายความเร็วสูงได้อย่างมั่นใจ สอดคล้องกับเป้าหมายการสร้าง "ระบบนิเวศการเรียนรู้แห่งอนาคต" ของกระทรวง อว.

2. การสร้างความเข้มแข็งของระบบวิจัยและความมั่นคงของฐานข้อมูลความรู้ (Research Security and Excellence) ยุทธศาสตร์การพัฒนาการอุดมศึกษามุ่งเน้นการผลิตงานวิจัยและนวัตกรรมที่มีผลกระทบสูง (High Impact) สถาปัตยกรรมภูมิคุ้มกันดิจิทัลที่ผู้วิจัยพัฒนาขึ้นจึงมุ่งเน้นการปกป้อง "ทรัพย์สินทางปัญญาดิจิทัล" และ "ฐานข้อมูลงานวิจัย" ของสถาบัน โดยการใช้ AI ในการวิเคราะห์และป้องกันการจารกรรมข้อมูลเชิงรุก ซึ่งเป็นปัจจัยสำคัญในการสร้างความเชื่อมั่นให้กับนักวิจัยและพันธมิตรในระดับสากล สอดคล้องกับนโยบายการสร้างความสามารถในการแข่งขันผ่านนวัตกรรมที่ปลอดภัยและยั่งยืน

3. การพัฒนาความเป็นธรรมาภิบาลดิจิทัลในสถาบันอุดมศึกษา (Digital Governance in Higher Education) แผนยุทธศาสตร์การอุดมศึกษาให้ความสำคัญกับธรรมาภิบาลและการบริหารจัดการที่มีความโปร่งใสและตรวจสอบได้ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ในงานวิจัยนี้ได้ออกแบบเลเยอร์การบริหารจัดการข้อมูล (Data Governance) ที่สอดคล้องกับมาตรฐานความปลอดภัยและกฎหมาย PDPA การนำ AI มาใช้จัดการภูมิคุ้มกันดิจิทัลจึงมิใช่เพียงการป้องกันภัยทางเทคนิค แต่เป็นการสร้างระบบบริหารความเสี่ยงระดับองค์กรที่ช่วยให้สถาบันสามารถประเมินและรายงานสถานะความปลอดภัยได้แบบเรียลไทม์ อันเป็นพื้นฐานสำคัญของสถาบันอุดมศึกษาสมรรถนะสูงตามแนวทางแผนพัฒนาการศึกษาชาติ

5.2 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

จากการสำรวจและวิเคราะห์สภาพปัจจุบันของสถาบันอุดมศึกษา สังกัดสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) ผู้วิจัยได้ศึกษาความพร้อมและความสามารถในการดำเนินงานด้านดิจิทัลของสถาบันอุดมศึกษา โดยพิจารณาครอบคลุมองค์ประกอบสำคัญของสถาปัตยกรรมองค์กรตามกรอบงาน 7 มิติ ได้แก่ ด้านธุรกิจ (Business) ด้านข้อมูล (Data) ด้านแอปพลิเคชัน (Application) ด้านเทคโนโลยี (Technology) ด้านความมั่นคงปลอดภัย (Security) ด้านการบูรณาการ (Integration) และด้านการกำกับดูแล (Governance) ซึ่งเป็นองค์ประกอบพื้นฐานที่สะท้อนความสามารถขององค์กรในการบริหารจัดการทรัพยากร กระบวนการ ข้อมูล ระบบสารสนเทศ เทคโนโลยี และการกำกับดูแลให้สามารถสนับสนุนพันธกิจและยุทธศาสตร์ของสถาบันอุดมศึกษาได้อย่างมีประสิทธิภาพ สามารถสรุปสาระสำคัญได้ดังนี้

5.2.1 การวิเคราะห์สภาพปัจจุบันของสถาบันอุดมศึกษาตามกรอบงาน 7 มิติของโครงสร้างองค์กร

การวิเคราะห์ทั้ง 7 มิติเป็นการพิจารณาความสัมพันธ์ระหว่างยุทธศาสตร์และภารกิจของสถาบัน กระบวนการดำเนินงาน ข้อมูล ระบบสารสนเทศ เทคโนโลยี ความมั่นคงปลอดภัย กลไกการเชื่อมโยงระบบ และการกำกับดูแล โดยมีเป้าหมายเพื่อระบุสภาพปัจจุบัน (As-Is Architecture) และนำผลที่ได้ไปใช้กำหนดสถาปัตยกรรมเป้าหมาย (Target Architecture) สำหรับการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ทั้งนี้แนวทางการจัดทำโครงสร้างองค์การให้ความสำคัญกับการจัดทำภาพสถาปัตยกรรมในสถานะปัจจุบันและอนาคต รวมถึงการวิเคราะห์ช่องว่างระหว่างสถานะปัจจุบันกับสถานะเป้าหมายเพื่อใช้กำหนดแนวทางการเปลี่ยนผ่านขององค์กร

5.2.1.1 ด้านธุรกิจ (Business) การวิเคราะห์สภาพปัจจุบันของโครงสร้างองค์กรด้านธุรกิจประกอบไปด้วยยุทธศาสตร์และกระบวนการดำเนินงานภายในองค์กร

การวิเคราะห์สภาพปัจจุบันของโครงสร้างองค์กรด้านธุรกิจ (Business Architecture) เป็นขั้นตอนสำคัญในการศึกษาสถาปัตยกรรมองค์กร เนื่องจาก Business Architecture เป็นองค์ประกอบที่สะท้อนทิศทาง เป้าหมาย พันธกิจ โครงสร้างองค์กร บทบาทหน้าที่ และกระบวนการดำเนินงานที่องค์กรใช้ในการสร้างคุณค่าและบรรลุเป้าหมายเชิงยุทธศาสตร์ สำหรับบริบทของสถาบันอุดมศึกษา Business Architecture จึงครอบคลุมทั้งระดับยุทธศาสตร์และระดับกระบวนการดำเนินงาน ได้แก่ การจัดการศึกษา การวิจัย การบริการวิชาการ การทำนุบำรุงศิลปวัฒนธรรม การบริหารทรัพยากร การบริหารงบประมาณ และการบริหารจัดการองค์กร

การวิเคราะห์ในงานวิจัยนี้มุ่งพิจารณาสภาพปัจจุบันของสถาบันอุดมศึกษาไทยใน 2 องค์ประกอบหลัก ได้แก่ 1) ยุทธศาสตร์ (Strategy) และ 2) กระบวนการดำเนินงานภายในองค์กร (Business Processes) เพื่อให้เห็นความเชื่อมโยงระหว่างเป้าหมายระดับองค์กรกับการดำเนินงานจริง และนำผลการวิเคราะห์ไปใช้เป็นข้อมูลพื้นฐานในการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล

5.2.1.1.1 ยุทธศาสตร์ (Strategy)

สถาบันอุดมศึกษาในปัจจุบันต้องดำเนินงานภายใต้สภาพแวดล้อมที่มีการเปลี่ยนแปลงทั้งด้านเศรษฐกิจ สังคม เทคโนโลยี และความต้องการของตลาดแรงงาน ส่งผลให้การกำหนดยุทธศาสตร์ของสถาบันไม่ได้มุ่งเน้นเฉพาะการจัดการเรียนการสอน แต่ต้องครอบคลุมการพัฒนากำลังคน การสร้างองค์ความรู้ การวิจัยและนวัตกรรม การสร้างความร่วมมือกับภาคอุตสาหกรรม การเปลี่ยนผ่านสู่ดิจิทัล และการเพิ่มขีดความสามารถในการแข่งขันของสถาบัน

ในระดับประเทศ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรมได้กำหนดแผนด้านการอุดมศึกษาเพื่อผลิตและพัฒนากำลังคนของประเทศ พ.ศ. 2564–2570 ฉบับปรับปรุง พ.ศ. 2566–2570 เพื่อใช้เป็นกรอบทิศทางการพัฒนาระบบอุดมศึกษาของประเทศ ซึ่งสะท้อนให้เห็นว่าการจัดการอุดมศึกษาต้องเชื่อมโยงกับการพัฒนากำลังคนและการเปลี่ยนแปลงของบริบทประเทศ

นอกจากนี้ กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรมยังมีแผนปฏิบัติราชการระยะ 5 ปี พ.ศ. 2566–2570 ซึ่งเป็นกรอบในการขับเคลื่อนภารกิจของกระทรวงและหน่วยงานในระบบ อววน. ดังนั้น สถาบันอุดมศึกษาจึงจำเป็นต้องนำกรอบนโยบายระดับประเทศมาถ่ายทอดเป็นยุทธศาสตร์ของสถาบัน และแปลงยุทธศาสตร์ดังกล่าวไปสู่แผนงาน โครงการ และกระบวนการดำเนินงานที่สามารถวัดผลได้

จากการวิเคราะห์จึงสามารถสรุปได้ว่า ยุทธศาสตร์ของสถาบันอุดมศึกษาควรมีความเชื่อมโยงเป็นลำดับตั้งแต่ วิสัยทัศน์ พันธกิจ เป้าประสงค์ ยุทธศาสตร์ กลยุทธ์ แผนงาน/โครงการ ตัวชี้วัดผล

การดำเนินงาน เพื่อให้สามารถติดตามและประเมินผลการบรรลุเป้าหมายขององค์กรได้อย่างเป็นระบบ

ในบริบทของการพัฒนา AI Enterprise Architecture ความเชื่อมโยงดังกล่าวมีความสำคัญอย่างยิ่ง เนื่องจากการนำ AI มาใช้ในองค์กรไม่ควรดำเนินการในลักษณะของการนำเทคโนโลยีมาใช้โดยปราศจากเป้าหมายทางธุรกิจ แต่ควรกำหนดจากปัญหาและความต้องการขององค์กร เช่น การเพิ่มประสิทธิภาพกระบวนการให้บริการนักศึกษา การวิเคราะห์ความเสี่ยง การสนับสนุนการตัดสินใจของผู้บริหาร การตรวจจับความผิดปกติของระบบสารสนเทศ และการยกระดับความสามารถในการบริหารจัดการภัยคุกคามดิจิทัล นอกจากนี้ นโยบายของกระทรวง อว. ในปัจจุบันให้ความสำคัญกับการพัฒนากำลังคน การสร้างองค์ความรู้ งานวิจัย เทคโนโลยี และนวัตกรรม รวมถึงการใช้เทคโนโลยีปัญญาประดิษฐ์เป็นประเด็นสำคัญของการพัฒนาประเทศ จึงแสดงให้เห็นว่าสถาบันอุดมศึกษาจำเป็นต้องปรับยุทธศาสตร์องค์กรให้สามารถรองรับการเปลี่ยนแปลงจาก AI และเทคโนโลยีดิจิทัลอย่างเป็นระบบ

5.2.1.1.2 กระบวนการดำเนินงานภายในองค์กร

กระบวนการดำเนินงาน (Business Processes) เป็นกลไกสำคัญในการแปลงยุทธศาสตร์ของสถาบันอุดมศึกษาไปสู่การปฏิบัติ โดยสามารถจำแนกกระบวนการหลักตามภารกิจของสถาบันอุดมศึกษาออกเป็น 3 กลุ่ม ได้แก่ กระบวนการบริหารและกำกับองค์กร กระบวนการหลัก และกระบวนการสนับสนุน

5.2.1.1.2.1 กระบวนการบริหารและกำกับองค์กร

กระบวนการบริหารและกำกับองค์กรครอบคลุมการกำหนดนโยบายและยุทธศาสตร์ การวางแผน การจัดสรรงบประมาณ การบริหารความเสี่ยง การกำกับติดตามผล การประกันคุณภาพ การบริหารความร่วมมือ และการประเมินผลการดำเนินงานขององค์กร

กระบวนการดังกล่าวมีความสำคัญต่อการจัดการภูมิคุ้มกันดิจิทัล เนื่องจากความเสี่ยงด้านดิจิทัลไม่ใช่เพียงประเด็นทางเทคนิคของฝ่ายเทคโนโลยีสารสนเทศ แต่มีผลต่อการบริหารและการดำเนินงานในระดับองค์กร ดังนั้น การจัดการความเสี่ยงดิจิทัลควรถูกบูรณาการเข้ากับกระบวนการบริหารความเสี่ยงและการกำกับดูแลของสถาบัน

ในระดับนโยบายของประเทศ แผนพัฒนารัฐบาลดิจิทัล พ.ศ. 2566–2570 ให้ความสำคัญกับการยกระดับการเปลี่ยนผ่านดิจิทัล เพื่อให้การบริหารงานมีความยืดหยุ่น คล่องตัว และสามารถพัฒนาบริการที่สะดวกและเข้าถึงได้ แม้แผนดังกล่าวจะเป็นกรอบสำหรับภาครัฐโดยรวม แต่หลักการดังกล่าวสามารถนำมาใช้เป็นบริบทสนับสนุนการพัฒนา Business Architecture ของสถาบันอุดมศึกษาที่มีภารกิจด้านบริการสาธารณะและการจัดการข้อมูลจำนวนมาก

5.2.1.1.2.2 กระบวนการหลักของสถาบันอุดมศึกษา

กระบวนการหลักเป็นกระบวนการที่สร้างคุณค่าโดยตรงต่อผู้มีส่วนได้ส่วนเสียของสถาบันอุดมศึกษา ได้แก่ นักศึกษา ผู้เรียน บุคลากร ผู้ประกอบการ หน่วยงานภาครัฐ ภาคอุตสาหกรรม และสังคม โดยสามารถจำแนกได้เป็นกระบวนการสำคัญ ได้แก่

1) กระบวนการจัดการเรียนการสอน ครอบคลุมการวิเคราะห์ความต้องการของผู้เรียน การพัฒนาหลักสูตร การรับสมัครนักศึกษา การลงทะเบียน การจัดการเรียนการสอน การประเมินผล การติดตามผลสัมฤทธิ์ทางการศึกษา และการสำเร็จการศึกษา กระบวนการเหล่านี้มีข้อมูลจำนวนมากและมีการใช้ระบบดิจิทัลในหลายขั้นตอน จึงมีศักยภาพในการนำ AI มาใช้เพื่อวิเคราะห์ข้อมูลผู้เรียน คาดการณ์ความเสี่ยงด้านการเรียน สนับสนุนการให้บริการ และเพิ่มประสิทธิภาพการบริหารจัดการ

2) กระบวนการวิจัยและสร้างนวัตกรรม ครอบคลุมการกำหนดโจทย์วิจัย การเสนอขอทุน การดำเนินโครงการวิจัย การจัดการข้อมูลวิจัย การเผยแพร่ผลงาน การคุ้มครองทรัพย์สินทางปัญญา และการถ่ายทอดเทคโนโลยี การใช้ AI สามารถสนับสนุนกระบวนการดังกล่าวได้ตั้งแต่การวิเคราะห์ข้อมูล การค้นหาองค์ความรู้ การวิเคราะห์แนวโน้มงานวิจัย และการสนับสนุนการตัดสินใจ อย่างไรก็ตาม จำเป็นต้องมีกลไกกำกับดูแลการใช้ข้อมูลและ AI เพื่อรักษาความถูกต้อง ความน่าเชื่อถือ และความรับผิดชอบทางวิชาการ

3) กระบวนการบริการวิชาการและการถ่ายทอดองค์ความรู้ เป็นกระบวนการที่เชื่อมโยงองค์ความรู้ของสถาบันกับชุมชน หน่วยงานภาครัฐ และภาคธุรกิจ ประกอบด้วยการให้บริการวิชาการ การฝึกอบรม การให้คำปรึกษา การถ่ายทอดเทคโนโลยี และการสร้างความร่วมมือ กระบวนการดังกล่าวสามารถใช้เทคโนโลยีดิจิทัลและ AI เพื่อวิเคราะห์ความต้องการของผู้รับบริการ ออกแบบบริการเฉพาะกลุ่ม และสนับสนุนการบริหารความสัมพันธ์กับผู้มีส่วนได้ส่วนเสีย

4) กระบวนการทำนุบำรุงศิลปวัฒนธรรมและการมีส่วนร่วมกับสังคม เป็นภารกิจที่สะท้อนบทบาทของสถาบันอุดมศึกษาต่อสังคม โดยสามารถนำระบบดิจิทัลมาสนับสนุนการจัดเก็บองค์ความรู้ การเผยแพร่ข้อมูล และการสร้างเครือข่ายความร่วมมือ

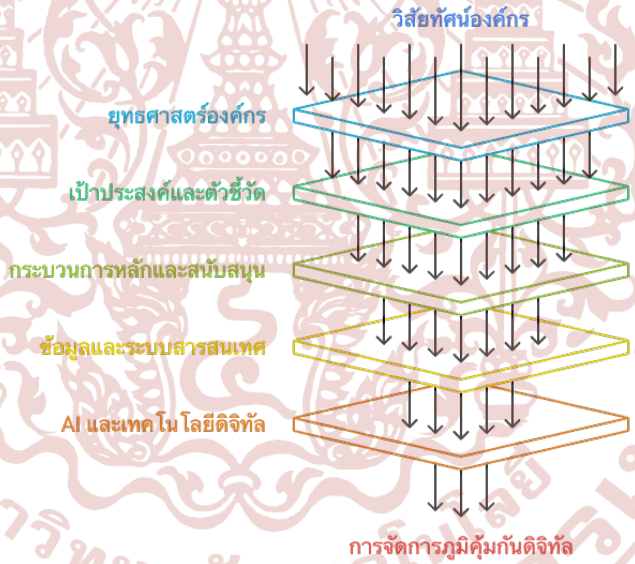
5.2.1.1.2.3 กระบวนการสนับสนุนองค์กร

กระบวนการสนับสนุนเป็นกลไกที่ทำให้กระบวนการหลักสามารถดำเนินงานได้อย่างมีประสิทธิภาพ ได้แก่ การบริหารทรัพยากรบุคคล การบริหารการเงินและงบประมาณ การจัดซื้อจัดจ้าง การบริหารพัสดุ การบริหารเทคโนโลยีสารสนเทศ การจัดการข้อมูล การประชาสัมพันธ์ และการบริหารอาคารสถานที่ ในบริบทของ AI Enterprise Architecture กระบวนการสนับสนุนเหล่านี้เป็นแหล่งข้อมูลสำคัญสำหรับการวิเคราะห์เชิงองค์กร เช่น ข้อมูลทรัพยากรบุคคล ข้อมูลการใช้

งบประมาณ ข้อมูลการใช้ทรัพยากร และข้อมูลเหตุการณ์ด้านเทคโนโลยีสารสนเทศ ซึ่งสามารถนำมาวิเคราะห์เพื่อเพิ่มประสิทธิภาพและสนับสนุนการคาดการณ์ความเสี่ยง

5.2.1.1.2.3 การวิเคราะห์ความสัมพันธ์ระหว่างยุทธศาสตร์กับกระบวนการดำเนินงาน

จากการวิเคราะห์ Business Architecture พบว่า ยุทธศาสตร์และกระบวนการดำเนินงานมีความสัมพันธ์กันเป็นลำดับ กล่าวคือ ยุทธศาสตร์ของสถาบันเป็นตัวกำหนดทิศทางและเป้าหมาย ขณะที่กระบวนการดำเนินงานเป็นกลไกในการทำให้เป้าหมายดังกล่าวเกิดขึ้นจริง ดังนั้น การพัฒนา AI Enterprise Architecture ควรเริ่มจากการวิเคราะห์ว่า “กระบวนการใดขององค์กรมีความสำคัญต่อยุทธศาสตร์ กระบวนการใดมีความเสี่ยง และกระบวนการใดมีศักยภาพในการใช้ AI เพื่อเพิ่มประสิทธิภาพหรือเพิ่มภูมิคุ้มกันดิจิทัล” สามารถแสดงความสัมพันธ์เชิงสถาปัตยกรรมได้ดังภาพที่ 5-1



ภาพที่ 5-1 แสดงความสัมพันธ์เชิงสถาปัตยกรรม

5.2.1.1.3 การวิเคราะห์ช่องว่างด้านธุรกิจ (Business Gap)

จากการสังเคราะห์สภาพปัจจุบันสามารถกำหนดประเด็นช่องว่างด้าน Business Architecture ที่มีความเกี่ยวข้องกับงานวิจัยได้ดังตารางที่ 5-1

ตารางที่ 5-1 การวิเคราะห์ช่วงว่างด้านธุรกิจ

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
ยุทธศาสตร์	มีแผนยุทธศาสตร์และแผนดิจิทัล	การบูรณาการ AI กับ Digital Immunity ยังต้องมีกรอบระดับองค์กร	AI & Digital Immunity Strategy
กระบวนการ	มีกระบวนการหลักและสนับสนุนจำนวนมาก	กระบวนการบางส่วนยังแยกตามหน่วยงาน	Integrated Business Process
การตัดสินใจ	ใช้ข้อมูลและรายงานเพื่อสนับสนุนผู้บริหาร	การวิเคราะห์เชิงคาดการณ์ยังมีข้อจำกัด	AI-enabled Decision Support
การบริหารความเสี่ยง	มีการบริหารความเสี่ยงระดับองค์กร	ความเสี่ยงดิจิทัลจำเป็นต้องเชื่อมกับกระบวนการธุรกิจ	Digital Risk Management
ความต่อเนื่องของธุรกิจ	มีการวางแผนและบริหารความเสี่ยง	ต้องเพิ่มความสามารถในการรับรู้และตอบสนองต่อเหตุการณ์ดิจิทัล	Digital Resilience
การสร้างคุณค่า	มุ่งเน้นคุณภาพการศึกษาและบริการ	ต้องเพิ่มการใช้ AI เพื่อสร้างคุณค่าและประสิทธิภาพ	AI-enabled Value Creation

การวิเคราะห์สภาพปัจจุบันของโครงสร้างองค์กรด้านธุรกิจพบว่า สถาบันอุดมศึกษามีองค์ประกอบด้านยุทธศาสตร์และกระบวนการดำเนินงานที่เป็นพื้นฐานสำหรับการพัฒนาองค์กรดิจิทัลอยู่แล้ว แต่ความท้าทายสำคัญคือการทำให้ ยุทธศาสตร์ กระบวนการ ข้อมูล เทคโนโลยี AI และการจัดการความเสี่ยงดิจิทัลทำงานในทิศทางเดียวกัน บริบทเชิงนโยบายระดับประเทศสนับสนุนให้สถาบันอุดมศึกษาพัฒนากำลังคน องค์ความรู้ งานวิจัย เทคโนโลยี และนวัตกรรม รวมถึงการปรับตัวต่อการเปลี่ยนแปลงทางดิจิทัล โดยสำนักงานปลัดกระทรวง อว. มีทั้งแผนด้านการอุดมศึกษา พ.ศ. 2564–2570 ฉบับปรับปรุง พ.ศ. 2566–2570 และแผนปฏิบัติราชการระยะ 5 ปี พ.ศ. 2566–2570 เป็นกรอบสำคัญในการขับเคลื่อนระบบอุดมศึกษา ดังนั้น Business Architecture ของสถาบันอุดมศึกษาในระยะต่อไปจึงควรเปลี่ยนจากแนวคิด “Digital Transformation” ที่มุ่งนำเทคโนโลยีมาเพิ่มประสิทธิภาพการทำงาน ไปสู่ “AI-Enabled and Resilient Business Architecture” ที่สามารถใช้ AI และข้อมูลเพื่อสนับสนุนการตัดสินใจ คาดการณ์ความเสี่ยง เพิ่มประสิทธิภาพกระบวนการ และสร้างความสามารถในการรับมือกับเหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงานขององค์กร ประเด็นดังกล่าวเป็นพื้นฐานสำคัญในการออกแบบ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา เนื่องจาก AI จะต้องถูกออกแบบให้สอดคล้องกับยุทธศาสตร์และกระบวนการขององค์กร ขณะที่กลไก Digital Immunity

จะต้องถูกฝังอยู่ในกระบวนการบริหารความเสี่ยงและกระบวนการดำเนินงานที่สำคัญของสถาบัน ไม่ใช่เป็นระบบด้านความมั่นคงปลอดภัยที่แยกออกจาก Business Architecture

5.2.1.2 ด้านข้อมูล (Data)

การวิเคราะห์สภาพปัจจุบันของโครงสร้างองค์กรด้านข้อมูล (Data Architecture) เป็นการศึกษาถึงโครงสร้าง แหล่งที่มา ประเภท การจัดเก็บ การไหลเวียน การแลกเปลี่ยน การใช้ประโยชน์ คุณภาพ การรักษาความมั่นคงปลอดภัย และการกำกับดูแลข้อมูลของสถาบันอุดมศึกษา โดยข้อมูลถือเป็นทรัพยากรสำคัญที่สนับสนุนการดำเนินงานในทุกระดับ ตั้งแต่ระดับปฏิบัติการ ระดับบริหาร ไปจนถึงระดับยุทธศาสตร์ ทั้งยังเป็นทรัพยากรพื้นฐานสำหรับการพัฒนาและประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เนื่องจากประสิทธิภาพและความน่าเชื่อถือของระบบ AI มีความสัมพันธ์โดยตรงกับคุณภาพ ความครบถ้วน ความถูกต้อง ความเป็นตัวแทน และความเหมาะสมของข้อมูลที่นำมาใช้

ในบริบทของสถาบันอุดมศึกษา ข้อมูลเกิดขึ้นจากกระบวนการดำเนินงานจำนวนมาก ทั้งข้อมูลด้านการบริหารจัดการ การจัดการศึกษา การวิจัย การบริการวิชาการ การบริหารบุคลากร การเงินและงบประมาณ รวมถึงข้อมูลจากระบบเทคโนโลยีสารสนเทศและเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ดังนั้น การจัดการข้อมูลจึงไม่ควรพิจารณาเฉพาะการจัดเก็บข้อมูลในฐานข้อมูลเท่านั้น แต่ควรพิจารณาข้อมูลตลอดวงจรชีวิต ตั้งแต่การสร้างหรือเก็บรวบรวม การจัดประเภท การจัดเก็บ การประมวลผล การแลกเปลี่ยน การนำไปใช้ การเก็บรักษา ตลอดจนการทำลายข้อมูลอย่างเหมาะสม

5.2.1.2.1 แหล่งที่มาของข้อมูล

สถาบันอุดมศึกษามีแหล่งข้อมูลที่หลากหลายและเกิดขึ้นจากทั้งกระบวนการภายในและสภาพแวดล้อมภายนอกองค์กร โดยสามารถจำแนกได้เป็น 2 กลุ่ม ได้แก่ ข้อมูลภายในองค์กร และ ข้อมูลภายนอกองค์กร

ข้อมูลภายในองค์กรประกอบด้วยข้อมูลนักศึกษา เช่น ข้อมูลประวัติ การสมัครเข้าเรียน การลงทะเบียน ผลการเรียน การเข้าชั้นเรียน และการสำเร็จการศึกษา ข้อมูลบุคลากร เช่น ข้อมูลประวัติ การปฏิบัติงาน ภาระงาน และการพัฒนาศักยภาพ ข้อมูลด้านการเงินและงบประมาณ ข้อมูลหลักสูตร ข้อมูลการวิจัยและผลงานทางวิชาการ ข้อมูลการให้บริการ และข้อมูลการใช้ระบบสารสนเทศ นอกจากนี้ ยังมีข้อมูลด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัย เช่น ข้อมูลการเข้าใช้งานระบบ (Authentication Logs) ข้อมูล Network Traffic ข้อมูล Endpoint Logs ข้อมูลเหตุการณ์ผิดปกติ และข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัย ซึ่งข้อมูลเหล่านี้มีความสำคัญต่อการพัฒนาระบบภูมิคุ้มกันดิจิทัล เนื่องจากสามารถนำมาใช้เป็นข้อมูลสำหรับตรวจจับ วิเคราะห์ และประเมินความเสี่ยงของเหตุการณ์ดิจิทัล

ส่วนข้อมูลภายนอกองค์กรอาจประกอบด้วยข้อมูลจากหน่วยงานภาครัฐ หน่วยงานกำกับดูแล แหล่งข้อมูลทางวิชาการ คู่ความร่วมมือ ภาคอุตสาหกรรม และแหล่งข้อมูลสาธารณะ ทั้งนี้ การนำข้อมูลภายนอกมาใช้จำเป็นต้องพิจารณาความน่าเชื่อถือ แหล่งที่มา เงื่อนไขการใช้งาน และข้อกำหนดด้านกฎหมายและสิทธิในข้อมูล

NIST ระบุว่าการเตรียมข้อมูลสำหรับ AI จำเป็นต้องพิจารณาแหล่งที่มา วิธีการเก็บรวบรวม ความครอบคลุม ความแปรปรวน ความถูกต้อง การป้องกันการเปลี่ยนแปลงข้อมูล ตลอดจนการคุ้มครองข้อมูลส่วนบุคคลและทรัพย์สินทางปัญญา เพราะข้อมูลที่ดูเหมือนถูกต้องอาจไม่เหมาะสมสำหรับการใช้งาน AI หากไม่สามารถสะท้อนบริบทหรือวัตถุประสงค์ของการใช้งานได้อย่างเหมาะสม

5.2.1.2.2 ประเภทและโครงสร้างของข้อมูล

ข้อมูลในสถาบันอุดมศึกษามีลักษณะและรูปแบบที่แตกต่างกัน สามารถแบ่งออกเป็นข้อมูลที่มีโครงสร้าง (Structured Data) ข้อมูลกึ่งโครงสร้าง (Semi-structured Data) และข้อมูลไม่มีโครงสร้าง (Unstructured Data)

ข้อมูลที่มีโครงสร้าง ได้แก่ ข้อมูลที่จัดเก็บในฐานข้อมูลเชิงสัมพันธ์ เช่น ข้อมูลนักศึกษา ข้อมูลบุคลากร ข้อมูลการลงทะเบียน ข้อมูลการเงิน และข้อมูลหลักสูตร

ข้อมูลกึ่งโครงสร้าง ได้แก่ ข้อมูลที่มีรูปแบบบางส่วนแต่ไม่ได้จัดเก็บในรูปแบบตารางทั้งหมด เช่น JSON, XML, Log Files และข้อมูลจาก API

ข้อมูลไม่มีโครงสร้าง ได้แก่ เอกสาร รายงาน งานวิจัย รูปภาพ เสียง วิดีโอ อีเมล และข้อความจากช่องทางการสื่อสารต่าง ๆ

การจำแนกข้อมูลดังกล่าวมีความสำคัญต่อ AI Enterprise Architecture เนื่องจากเทคโนโลยี AI แต่ละประเภทต้องการข้อมูลที่แตกต่างกัน เช่น Machine Learning ต้องอาศัยข้อมูลสำหรับการฝึกและทดสอบโมเดล ขณะที่ Natural Language Processing ต้องอาศัยข้อมูลข้อความ และ Computer Vision ต้องอาศัยข้อมูลภาพหรือวิดีโอ ดังนั้น การออกแบบ Data Architecture จึงจำเป็นต้องรองรับข้อมูลหลายรูปแบบและสามารถจัดเตรียมข้อมูลให้เหมาะสมกับวัตถุประสงค์ของ AI แต่ละประเภท

5.2.1.2.3 การจัดเก็บและบริหารจัดการข้อมูล

สภาพแวดล้อมของสถาบันอุดมศึกษาประกอบด้วยระบบสารสนเทศจำนวนมาก ส่งผลให้ข้อมูลอาจถูกจัดเก็บอยู่ในฐานข้อมูลหลายระบบและอยู่ภายใต้ความรับผิดชอบของหน่วยงานที่แตกต่างกัน เช่น ระบบทะเบียนและประวัตินักศึกษา ระบบบริหารทรัพยากรบุคคล ระบบการเงิน ระบบวิจัย ระบบการเรียนรู้ และระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

ลักษณะดังกล่าวทำให้เกิดความท้าทายในการบริหารข้อมูล โดยเฉพาะกรณีที่ข้อมูลชุดเดียวกันถูกจัดเก็บมากกว่าหนึ่งระบบ หรือมีการกำหนดนิยามและมาตรฐานข้อมูลแตกต่างกันระหว่าง

หน่วยงาน อาจส่งผลให้เกิดข้อมูลซ้ำซ้อน ข้อมูลไม่ตรงกัน และทำให้การนำข้อมูลมาวิเคราะห์ในระดับองค์กรมีข้อจำกัด ดังนั้น Data Architecture ของสถาบันอุดมศึกษาจึงควรมีแนวทางกำหนด แหล่งข้อมูลหลัก (Source of Truth) การจัดทำ Metadata การกำหนด Data Owner และ Data Steward รวมถึงการกำหนดมาตรฐานการจัดเก็บและแลกเปลี่ยนข้อมูลระหว่างระบบ

ประเด็นนี้มีความสำคัญเพิ่มขึ้นเมื่อสถาบันนำ AI มาใช้ เพราะ AI มีการพึ่งพาข้อมูลในระดับสูง และปัญหาด้านคุณภาพข้อมูลอาจส่งผลต่อความน่าเชื่อถือของผลลัพธ์จาก AI โดย NIST ระบุว่าปัญหาคุณภาพข้อมูล อคติของข้อมูล การเปลี่ยนแปลงของข้อมูล และข้อมูลที่ล้าสมัยสามารถส่งผลกระทบต่อความน่าเชื่อถือของระบบ AI ได้

5.2.1.2.4 คุณภาพข้อมูล (Data Quality)

คุณภาพข้อมูลเป็นองค์ประกอบสำคัญของ Data Architecture โดยเฉพาะเมื่อข้อมูลถูกนำไปใช้สำหรับการวิเคราะห์ การคาดการณ์ และการฝึกโมเดล AI คุณภาพข้อมูลควรพิจารณาอย่างน้อยในด้านความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้อง (Consistency) ความเป็นปัจจุบัน (Timeliness) ความถูกต้องตามรูปแบบ (Validity) และความไม่ซ้ำซ้อน (Uniqueness)

ในบริบทของสถาบันอุดมศึกษา ตัวอย่างปัญหาที่อาจเกิดขึ้น ได้แก่ ข้อมูลนักศึกษาที่ไม่เป็นปัจจุบัน ข้อมูลจากหลายระบบมีรูปแบบแตกต่างกัน การบันทึกข้อมูลซ้ำซ้อน หรือข้อมูลที่ไม่สามารถเชื่อมโยงกันได้เนื่องจากไม่มีรหัสอ้างอิงร่วมกัน

ปัญหาดังกล่าวมีผลต่อการนำ AI มาใช้โดยตรง เพราะหากข้อมูลสำหรับฝึกโมเดลมีความไม่ครบถ้วนหรือมีอคติ ผลลัพธ์ของ AI อาจมีความคลาดเคลื่อนและส่งผลต่อการตัดสินใจของผู้ใช้งานได้ NIST จึงให้ความสำคัญกับการประเมินคุณภาพข้อมูล ความเหมาะสมของข้อมูล และความเสี่ยงที่เกิดจากกระบวนการจัดการข้อมูลตลอดวงจรชีวิตของระบบ AI ดังนั้น สถาปัตยกรรมเป้าหมายควรมีกลไก Data Quality Management ที่สามารถตรวจสอบคุณภาพข้อมูลอย่างต่อเนื่อง รวมถึงกำหนดตัวชี้วัดคุณภาพข้อมูลและกระบวนการแก้ไขข้อมูลที่ผิดพลาด

5.2.1.2.5 การบูรณาการและการแลกเปลี่ยนข้อมูล

สถาบันอุดมศึกษามีระบบสารสนเทศจำนวนมาก การบูรณาการข้อมูลระหว่างระบบจึงเป็นประเด็นสำคัญของ Data Architecture โดยเฉพาะการนำข้อมูลจากหลายแหล่งมาวิเคราะห์ร่วมกันเพื่อสนับสนุนการบริหารจัดการและการตัดสินใจ

การบูรณาการข้อมูลควรมีการกำหนดมาตรฐานด้านข้อมูล โครงสร้างข้อมูล Metadata และรูปแบบการแลกเปลี่ยนข้อมูล รวมถึงกลไก API หรือ Integration Platform เพื่อให้ระบบต่าง ๆ สามารถแลกเปลี่ยนข้อมูลได้โดยไม่จำเป็นต้องสร้างการเชื่อมต่อแบบเฉพาะระบบทุกคู่

สำหรับงานวิจัยนี้ การบูรณาการข้อมูลมีความสำคัญเป็นพิเศษ เนื่องจากการจัดการภูมิคุ้มกันดิจิทัลต้องอาศัยข้อมูลจากหลายแหล่ง เช่น ข้อมูลผู้ใช้งาน ข้อมูลระบบเครือข่าย ข้อมูล Endpoint ข้อมูลเหตุการณ์ด้านความปลอดภัย และข้อมูลจากระบบบริหารจัดการองค์กร หากข้อมูลเหล่านี้ไม่สามารถนำมาวิเคราะห์ร่วมกันได้ ความสามารถในการตรวจจับความผิดปกติและประเมินความเสี่ยงในระดับองค์กรจะลดลง

5.2.1.2.6 ข้อมูลสำหรับปัญญาประดิษฐ์

จากการวิเคราะห์สภาพปัจจุบันของสถาบันอุดมศึกษา พบว่าข้อมูลสำหรับปัญญาประดิษฐ์ (Data for Artificial Intelligence) เป็นองค์ประกอบสำคัญของสถาปัตยกรรมข้อมูล เนื่องจากข้อมูลเป็นทรัพยากรพื้นฐานที่ใช้ในการพัฒนา ฝึกฝน ทดสอบ ประเมินผล และนำระบบปัญญาประดิษฐ์ไปประยุกต์ใช้ในการสนับสนุนการดำเนินงานขององค์กร โดยเฉพาะในบริบทของสถาบันอุดมศึกษาที่มีข้อมูลเกิดขึ้นจากกระบวนการดำเนินงานจำนวนมาก ทั้งด้านการจัดการศึกษา การวิจัย การบริหารบุคลากร การเงินและงบประมาณ การบริการนักศึกษา ตลอดจนข้อมูลจากระบบเทคโนโลยีสารสนเทศและข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ข้อมูลดังกล่าวจึงมีศักยภาพในการนำมาวิเคราะห์เพื่อสร้างสารสนเทศ องค์ความรู้ และข้อมูลเชิงลึกสำหรับสนับสนุนการตัดสินใจของผู้บริหารและการเพิ่มประสิทธิภาพการดำเนินงานของสถาบัน

อย่างไรก็ตามการมีข้อมูลจำนวนมากไม่ได้หมายความว่าข้อมูลจะสามารถนำไปใช้กับปัญญาประดิษฐ์ได้ทันที ข้อมูลที่จะนำมาใช้ในการพัฒนา AI จำเป็นต้องผ่านกระบวนการจัดเตรียมและตรวจสอบความพร้อมอย่างเป็นระบบ โดยต้องพิจารณาคุณภาพข้อมูล ความถูกต้อง ความครบถ้วน ความสอดคล้อง ความเป็นปัจจุบัน ความเหมาะสมกับวัตถุประสงค์ของการใช้งาน ตลอดจนแหล่งที่มาและสิทธิในการนำข้อมูลไปใช้ เนื่องจากคุณภาพของข้อมูลมีผลโดยตรงต่อคุณภาพและความน่าเชื่อถือของผลลัพธ์จากแบบจำลองปัญญาประดิษฐ์ หากข้อมูลที่ใช้ในการฝึกหรือทดสอบแบบจำลองมีความคลาดเคลื่อน มีข้อมูลซ้ำซ้อน ขาดข้อมูลที่สำคัญ หรือมีอคติ ผลลัพธ์ที่เกิดขึ้นจาก AI อาจมีความคลาดเคลื่อนและนำไปสู่การตัดสินใจที่ไม่เหมาะสมได้ ดังนั้น การเตรียมข้อมูลจึงถือเป็นขั้นตอนสำคัญก่อนการนำ AI ไปใช้งานในระดับองค์กร

สำหรับสถาบันอุดมศึกษาข้อมูลสำหรับ AI สามารถจำแนกตามลักษณะของการใช้งานออกเป็นข้อมูลเพื่อการบริหารจัดการ ข้อมูลเพื่อการจัดการศึกษา ข้อมูลเพื่อการวิจัยและนวัตกรรม ข้อมูลเพื่อการบริการ และข้อมูลเพื่อการรักษาความมั่นคงปลอดภัยและการจัดการภูมิคุ้มกันดิจิทัล โดยข้อมูลแต่ละประเภทสามารถนำมาสร้างความสามารถของ AI ที่แตกต่างกัน เช่น ข้อมูลผลการเรียนและพฤติกรรมการเรียนรู้สามารถนำมาใช้ในการวิเคราะห์และคาดการณ์ความเสี่ยงของผู้เรียน ข้อมูลด้านบุคลากรสามารถใช้สนับสนุนการวางแผนกำลังคนและการพัฒนาบุคลากร ข้อมูลด้านการเงินสามารถใช้ในการวิเคราะห์แนวโน้มและสนับสนุนการจัดสรรทรัพยากร ขณะที่ข้อมูลด้าน

ระบบเครือข่ายและเหตุการณ์ด้านความมั่นคงปลอดภัยสามารถนำมาใช้ในการตรวจจับความผิดปกติ วิเคราะห์รูปแบบภัยคุกคาม และประเมินความเสี่ยงด้านดิจิทัล

ในบริบทของการจัดการภูมิคุ้มกันดิจิทัล ข้อมูลสำหรับ AI มีบทบาทสำคัญในการเปลี่ยนรูปแบบการบริหารความมั่นคงปลอดภัยจากการตอบสนองต่อเหตุการณ์ภายหลังเกิดปัญหา ไปสู่การเฝ้าระวัง วิเคราะห์ และคาดการณ์ความเสี่ยงเชิงรุก โดยข้อมูลจาก Firewall, ระบบตรวจจับภัยคุกคาม, Server, Endpoint, Network, ระบบยืนยันตัวตน และระบบสารสนเทศต่าง ๆ สามารถนำมาบูรณาการเพื่อสร้างฐานข้อมูลสำหรับการวิเคราะห์เหตุการณ์ผิดปกติ เมื่อ AI สามารถวิเคราะห์ข้อมูลจากหลายแหล่งร่วมกัน จะช่วยให้สถาบันสามารถระบุรูปแบบพฤติกรรมที่ผิดปกติ ตรวจจับเหตุการณ์ที่มีแนวโน้มเป็นภัยคุกคาม และจัดลำดับความสำคัญของความเสี่ยงได้อย่างมีประสิทธิภาพมากขึ้น

นอกจากนี้การนำข้อมูลมาใช้กับ AI จำเป็นต้องคำนึงถึง วงจรชีวิตของข้อมูล (Data Life Cycle) ตั้งแต่การรวบรวมข้อมูล การตรวจสอบและทำความสะอาดข้อมูล การบูรณาการข้อมูล การจัดเก็บ การเตรียมข้อมูลสำหรับการฝึกแบบจำลอง การฝึกและทดสอบแบบจำลอง การนำแบบจำลองไปใช้งาน ตลอดจนการติดตามและปรับปรุงข้อมูลอย่างต่อเนื่อง เนื่องจากข้อมูลของสถาบันอุดมศึกษามีการเปลี่ยนแปลงอยู่ตลอดเวลา เช่น จำนวนนักศึกษา บุคลากร หลักสูตร พฤติกรรมการใช้งานระบบ และรูปแบบภัยคุกคามทางไซเบอร์ หากข้อมูลที่ใช้กับ AI ไม่ได้รับการปรับปรุงให้สอดคล้องกับสภาพแวดล้อมปัจจุบัน อาจทำให้ประสิทธิภาพของแบบจำลองลดลงและไม่สามารถสะท้อนสถานการณ์จริงขององค์กรได้

ประเด็นสำคัญอีกประการหนึ่งคือ การกำกับดูแลข้อมูลสำหรับ AI (AI Data Governance) เนื่องจากข้อมูลของสถาบันอุดมศึกษาบางประเภทเกี่ยวข้องกับข้อมูลส่วนบุคคล ข้อมูลทางการศึกษา ข้อมูลบุคลากร และข้อมูลที่มีความสำคัญต่อความมั่นคงปลอดภัยขององค์กร ดังนั้น ก่อนนำข้อมูลไปใช้ในการพัฒนา AI จำเป็นต้องกำหนดสิทธิในการเข้าถึง แหล่งที่มาของข้อมูล วัตถุประสงค์ในการใช้ข้อมูล ระยะเวลาในการจัดเก็บ และมาตรการรักษาความปลอดภัย รวมถึงสามารถตรวจสอบย้อนกลับได้ว่าข้อมูลถูกนำไปใช้ในกระบวนการใดและเพื่อวัตถุประสงค์ใด ทั้งนี้แนวทางของ NIST AI Risk Management Framework ให้ความสำคัญกับการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลตลอดวงจรชีวิตของ AI รวมถึงคุณภาพข้อมูล ความเป็นส่วนตัว ความน่าเชื่อถือ และความเหมาะสมของข้อมูลกับบริบทการใช้งาน

ดังนั้น จากการวิเคราะห์สภาพปัจจุบันจึงเห็นได้ว่า สถาบันอุดมศึกษาจำเป็นต้องพัฒนาข้อมูลจาก “ข้อมูลที่มีอยู่ในองค์กร (Available Data)” ไปสู่ “ข้อมูลที่พร้อมสำหรับปัญญาประดิษฐ์ (AI-Ready Data)” โดยต้องมีกระบวนการคัดเลือก ตรวจสอบ ทำความสะอาด จัดโครงสร้าง บูรณาการ

และกำกับดูแลข้อมูลอย่างเป็นระบบ รวมถึงต้องมีการจัดทำ Metadata และกำหนดเจ้าของข้อมูลอย่างชัดเจน เพื่อให้สามารถตรวจสอบคุณภาพและแหล่งที่มาของข้อมูลได้ตลอดวงจรชีวิต

ในงานวิจัยนี้ ผู้วิจัยจึงเห็นว่าข้อมูลสำหรับปัญญาประดิษฐ์ควรทำหน้าที่เป็นฐานข้อมูลอัจฉริยะ (Intelligent Data Foundation) ของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ โดยเชื่อมโยงข้อมูลจาก Business Architecture, Application Architecture, Technology Architecture และ Security Architecture เข้าด้วยกัน ก่อนนำเข้าสู่กระบวนการวิเคราะห์ด้วย AI เพื่อสร้างข้อมูลเชิงลึกและความสามารถด้านการคาดการณ์ จากนั้นผลการวิเคราะห์จะถูกนำไปใช้สนับสนุนการตัดสินใจ การบริหารความเสี่ยง และการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา

5.2.1.2.7 การจัดการข้อมูลเพื่อการจัดการภูมิคุ้มกันดิจิทัล

ข้อมูลไม่ได้ทำหน้าที่เพียงสนับสนุนการดำเนินงานของสถาบัน แต่เป็น ฐานข้อมูลสำหรับการสร้างภูมิคุ้มกันดิจิทัล โดยข้อมูลด้านความมั่นคงปลอดภัยสามารถนำมาใช้เพื่อสร้างความสามารถในการรับรู้สถานการณ์ วิเคราะห์ความเสี่ยง และสนับสนุนการตอบสนองต่อเหตุการณ์ ข้อมูลที่มีความสำคัญ ได้แก่

- ข้อมูลการเข้าสู่ระบบและการยืนยันตัวตน
- ข้อมูลการใช้งานระบบสารสนเทศ
- ข้อมูล Network Traffic
- ข้อมูล Firewall และระบบรักษาความปลอดภัย
- ข้อมูล Endpoint และอุปกรณ์ผู้ใช้งาน
- ข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัย
- ข้อมูล Vulnerability และ Risk Assessment
- ข้อมูลการสำรองและการกู้คืนระบบ
- ข้อมูลเหตุการณ์ผิดปกติจากระบบ AI
- ข้อมูล Incident Response และประวัติการแก้ไขเหตุการณ์

ข้อมูลดังกล่าวสามารถนำเข้าสู่กระบวนการวิเคราะห์เพื่อสร้าง Threat Intelligence, Anomaly Detection, Risk Prediction และ Security Analytics ซึ่งเป็นความสามารถสำคัญของระบบภูมิคุ้มกันดิจิทัล กล่าวได้ว่า Data Architecture เป็นกลไกที่ทำให้ระบบสามารถเปลี่ยนจากการตอบสนองต่อเหตุการณ์หลังเกิดเหตุ ไปสู่การ ตรวจจับและคาดการณ์ความเสี่ยงเชิงรุก ได้มากขึ้น

5.2.1.2.8 การคุ้มครองข้อมูล ความเป็นส่วนตัว และสิทธิในการเข้าถึง

เนื่องจากสถาบันอุดมศึกษาจัดเก็บข้อมูลจำนวนมากที่เกี่ยวข้องกับบุคคล การออกแบบ Data Architecture จึงต้องคำนึงถึงการรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล รวมถึงการกำหนดสิทธิในการเข้าถึงข้อมูลตามบทบาทหน้าที่ การนำข้อมูลไปใช้กับ AI ทำให้ประเด็น

ดังกล่าวมีความซับซ้อนมากขึ้น เนื่องจาก AI สามารถเชื่อมโยงหรือวิเคราะห์ข้อมูลจำนวนมากจากหลายแหล่งได้ NIST จึงเน้นให้มีการกำหนดสิทธิการเข้าถึงข้อมูลสำหรับชุดข้อมูลที่มีข้อมูลส่วนบุคคล รวมถึงการประเมินความเสี่ยงด้าน Privacy และการใช้เทคนิคที่ช่วยเพิ่มความเป็นส่วนตัวตามความเหมาะสม ดังนั้น Data Architecture ควรเชื่อมโยงกับ Security Architecture และ Governance Architecture ผ่านกลไก เช่น Data Classification, Access Control, Data Protection, Data Monitoring, Audit, Compliance เพื่อให้สามารถควบคุมการเข้าถึงและการใช้ข้อมูลได้ตลอดวงจรชีวิต

5.2.1.2.9 การกำกับดูแลข้อมูล (Data Governance)

การกำกับดูแลข้อมูลเป็นองค์ประกอบสำคัญที่ทำให้การจัดการข้อมูลเป็นมาตรฐานเดียวกันในระดับองค์กร โดยควรกำหนดบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้องกับข้อมูลอย่างชัดเจน เช่น Data Owner, Data Steward, Data Custodian และ Data User การกำกับดูแลควรครอบคลุมประเด็นสำคัญ ได้แก่

- นโยบายและมาตรฐานข้อมูล
- การจำแนกประเภทข้อมูล
- Data Ownership
- Metadata Management
- Data Quality
- Data Lifecycle Management
- Data Access Control
- Data Privacy
- Data Security
- Data Retention
- Data Audit
- Data Sharing

NIST ระบุว่าการกำกับดูแลข้อมูลมีความสัมพันธ์กับความเป็นส่วนตัว ความมั่นคงปลอดภัย และการบริหารความเสี่ยงของ AI โดยเฉพาะประเด็น Data Quality, Data Stewardship และ Data Accountability ดังนั้น สำหรับสถาบันอุดมศึกษาที่ต้องการพัฒนา AI Enterprise Architecture จำเป็นต้องมี Data Governance ที่สามารถรองรับทั้งข้อมูลสำหรับการดำเนินงานปกติและข้อมูลสำหรับ AI โดยต้องกำหนดหลักเกณฑ์ที่ชัดเจนตั้งแต่การรวบรวมข้อมูล การนำข้อมูลไปใช้ การแบ่งปันข้อมูล ไปจนถึงการเก็บรักษาและทำลายข้อมูล

5.2.1.2.10 การวิเคราะห์ช่องว่างด้านข้อมูล (Data Gap Analysis)

จากการวิเคราะห์สภาพปัจจุบันสามารถสังเคราะห์ช่องว่างด้าน Data Architecture ได้ดังตารางที่ 5-2

ตารางที่ 5-2 การวิเคราะห์ช่องว่างด้านข้อมูล

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
แหล่งข้อมูล	มีข้อมูลจากหลายระบบและหลายหน่วยงาน	ข้อมูลกระจายและมี Data Silo	Integrated Data Sources
คุณภาพข้อมูล	มีการตรวจสอบในบางระบบ	มาตรฐานคุณภาพอาจแตกต่างกัน	Data Quality Management
การบูรณาการ	มีการแลกเปลี่ยนข้อมูลระหว่างบางระบบ	การเชื่อมโยงระดับองค์กรยังมีข้อจำกัด	Enterprise Data Integration
Metadata	มีการจัดทำในบางระบบ	ขาดมาตรฐาน Metadata ร่วม	Metadata Management
AI Data	มีข้อมูลจำนวนมาก	ข้อมูลยังไม่พร้อมสำหรับ AI ทุกประเภท	AI-Ready Data
Security Data	มี Log และข้อมูลเหตุการณ์จากหลายระบบ	การวิเคราะห์ร่วมกันยังมีข้อจำกัด	Security Data Lake / Analytics
Data Governance	มีนโยบายและแนวปฏิบัติในบางส่วน	การกำกับดูแลแบบบูรณาการยังต้องพัฒนา	Enterprise Data Governance
Privacy	มีการควบคุมข้อมูลส่วนบุคคล	ต้องควบคุมการใช้ข้อมูลกับ AI เพิ่มเติม	Privacy-aware AI Data Management
Data Lifecycle	มีการจัดเก็บและใช้งานข้อมูล	การบริหารวงจรชีวิตยังไม่เป็นระบบเดียวกัน	Data Lifecycle Management

การวิเคราะห์สภาพปัจจุบันด้านข้อมูลพบว่า สถาบันอุดมศึกษามีข้อมูลจำนวนมากและมีศักยภาพในการนำข้อมูลมาใช้สนับสนุนการบริหารจัดการ การตัดสินใจ และการพัฒนาระบบ AI อย่างไรก็ตาม ความท้าทายสำคัญอยู่ที่ ความหลากหลายของแหล่งข้อมูล การกระจายตัวของข้อมูล คุณภาพข้อมูล การเชื่อมโยงข้อมูล ความเป็นส่วนตัว และการกำกับดูแลข้อมูล โดยเฉพาะอย่างยิ่งเมื่อพิจารณาในบริบทของ AI และ Digital Immunity ข้อมูลต้องมีคุณสมบัติมากกว่าการเป็นข้อมูลที่ “จัดเก็บได้” แต่ต้องเป็นข้อมูลที่ ถูกต้อง เชื่อถือได้ มีบริบท มีแหล่งที่มาชัดเจน ตรวจสอบย้อนกลับได้ ปลอดภัย และพร้อมสำหรับการวิเคราะห์ด้วย AI ดังนั้น ผู้วิจัยจึงสังเคราะห์แนวทางการพัฒนา Data Architecture จากสภาพปัจจุบันไปสู่สถาปัตยกรรมเป้าหมาย โดยมุ่งพัฒนา AI-Ready Data

Architecture ที่ประกอบด้วย Data Integration, Data Quality Management, Metadata Management, Data Governance, Data Security, Privacy Management และ Security Data Analytics เพื่อสนับสนุนทั้งการบริหารจัดการองค์กรและการจัดการภูมิคุ้มกันดิจิทัล

5.2.1.3 ด้านแอปพลิเคชัน (Application)

การวิเคราะห์สภาพปัจจุบันของโครงสร้างองค์กรด้านแอปพลิเคชัน (Application Architecture) เป็นการศึกษาระบบงานและซอฟต์แวร์ที่สถาบันอุดมศึกษาใช้สนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ขององค์กร ครอบคลุมตั้งแต่ระบบสารสนเทศเพื่อการบริหารจัดการ ระบบสนับสนุนการเรียนการสอน ระบบงานวิจัย ระบบบริการนักศึกษา ระบบบริหารทรัพยากรบุคคล ระบบการเงินและงบประมาณ ตลอดจนระบบที่เกี่ยวข้องกับการบริหารจัดการเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางดิจิทัล โดยแอปพลิเคชันถือเป็นกลไกสำคัญในการแปลงข้อมูลและกระบวนการดำเนินงานขององค์กรให้สามารถนำไปใช้ในการปฏิบัติงาน การให้บริการ การวิเคราะห์ และการสนับสนุนการตัดสินใจได้อย่างเป็นระบบ

จากการวิเคราะห์สภาพปัจจุบันพบว่า สถาบันอุดมศึกษามีการนำระบบสารสนเทศและแอปพลิเคชันมาใช้ในกระบวนการดำเนินงานอย่างครอบคลุมมากขึ้น ทั้งในระดับงานปฏิบัติการและระดับบริหาร เช่น ระบบรับสมัครและทะเบียนนักศึกษา ระบบบริหารการเรียนรู้ ระบบบริหารบุคลากร ระบบการเงินและงบประมาณ ระบบจัดการงานวิจัย ระบบห้องสมุด ระบบบริการนักศึกษา ระบบประชุมและสื่อสารออนไลน์ รวมถึงระบบสารสนเทศเพื่อการบริหารและระบบรายงานสำหรับผู้บริหาร การมีแอปพลิเคชันเหล่านี้ช่วยลดภาระงานที่ดำเนินการด้วยเอกสาร เพิ่มความรวดเร็วในการให้บริการ และทำให้สามารถจัดเก็บข้อมูลจากกระบวนการดำเนินงานในรูปแบบดิจิทัลได้มากขึ้น อย่างไรก็ตามการพัฒนาแอปพลิเคชันของสถาบันอุดมศึกษามักเกิดขึ้นตามความต้องการของแต่ละหน่วยงานและแต่ละช่วงเวลา ส่งผลให้ระบบที่ใช้งานภายในองค์กรอาจมีความหลากหลายทั้งด้านผู้พัฒนา เทคโนโลยี ฐานข้อมูล รูปแบบการเชื่อมต่อ และมาตรฐานการจัดการข้อมูล ในบางกรณีอาจพบว่าระบบแต่ละระบบสามารถทำงานได้อย่างมีประสิทธิภาพภายในขอบเขตของหน่วยงาน แต่ยังไม่สามารถเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับระบบอื่นได้อย่างสมบูรณ์ ลักษณะดังกล่าวอาจนำไปสู่ Application Silo และส่งผลให้ข้อมูลชุดเดียวกันถูกจัดเก็บหรือบันทึกซ้ำในหลายระบบ

5.2.1.3.1 ระบบแอปพลิเคชันเพื่อสนับสนุนภารกิจหลักของสถาบัน

ระบบแอปพลิเคชันของสถาบันอุดมศึกษาสามารถจำแนกตามภารกิจหลักได้หลายกลุ่ม โดยระบบที่เกี่ยวข้องกับการจัดการศึกษา ได้แก่ ระบบรับสมัครนักศึกษา ระบบทะเบียนและประวัตินักศึกษา ระบบลงทะเบียนเรียน ระบบจัดตารางเรียนและตารางสอบ ระบบประเมินผลการศึกษา ระบบบริหารหลักสูตร และระบบการเรียนรู้แบบออนไลน์ ระบบเหล่านี้ทำหน้าที่สนับสนุนกระบวนการตั้งแต่การรับนักศึกษาเข้าสู่ระบบ การจัดการเรียนรู้ การประเมินผล ไปจนถึงการสำเร็จการศึกษา

ในส่วนของการวิจัยและนวัตกรรม ประกอบด้วยระบบบริหารโครงการวิจัย ระบบจัดการทุนวิจัย ระบบฐานข้อมูลผลงานวิจัย ระบบเผยแพร่ผลงานทางวิชาการ และระบบบริหารทรัพย์สินทางปัญญา ซึ่งช่วยสนับสนุนการจัดเก็บและติดตามข้อมูลตลอดกระบวนการวิจัย

สำหรับด้านการบริหารจัดการองค์กร มีระบบบริหารทรัพยากรบุคคล ระบบเงินเดือน ระบบการเงินและบัญชี ระบบงบประมาณ ระบบจัดซื้อจัดจ้าง ระบบพัสดุ และระบบบริหารทรัพย์สิน ซึ่งเป็นระบบสนับสนุนที่มีข้อมูลสำคัญต่อการบริหารทรัพยากรและการตัดสินใจของผู้บริหาร นอกจากนี้ยังมีระบบสนับสนุนการให้บริการ เช่น ระบบบริการนักศึกษา ระบบบริการบุคลากร ระบบสารบรรณอิเล็กทรอนิกส์ ระบบการประชุม ระบบร้องเรียนและรับข้อเสนอแนะ รวมถึงระบบประชาสัมพันธ์และการสื่อสารดิจิทัล

5.2.1.3.2 ระบบแอปพลิเคชันเพื่อสนับสนุนการบริหารและการตัดสินใจ

การบริหารสถาบันอุดมศึกษาในปัจจุบันต้องอาศัยข้อมูลจากหลายระบบเพื่อใช้ประกอบการตัดสินใจ ดังนั้น ระบบสารสนเทศเพื่อการบริหาร (Management Information System) และระบบสนับสนุนการตัดสินใจ (Decision Support System) จึงมีความสำคัญในการรวบรวมและนำเสนอข้อมูลในรูปแบบรายงาน Dashboard และตัวชี้วัดผลการดำเนินงาน

อย่างไรก็ตาม การนำข้อมูลจากหลายแอปพลิเคชันมาวิเคราะห์ในระดับองค์กรจำเป็นต้องอาศัยการบูรณาการข้อมูล หากระบบต้นทางมีโครงสร้างข้อมูลแตกต่างกัน หรือไม่มีมาตรฐานในการเชื่อมต่อ อาจทำให้การจัดทำรายงานระดับองค์กรต้องอาศัยการรวบรวมข้อมูลจากหลายหน่วยงานด้วยกระบวนการที่ใช้แรงงานและใช้เวลา ส่งผลต่อความรวดเร็วและความเป็นปัจจุบันของข้อมูลที่นำมาใช้ในการตัดสินใจ ในบริบทของงานวิจัย การพัฒนา Application Architecture จึงควรมุ่งไปสู่ระบบที่สามารถเชื่อมโยงข้อมูลจากหลายแหล่ง และสามารถนำความสามารถของ AI เข้ามาสนับสนุนการวิเคราะห์และการตัดสินใจ เช่น AI Dashboard, Predictive Analytics, Intelligent Decision Support และระบบแจ้งเตือนความเสี่ยงแบบอัตโนมัติ

5.2.1.3.3 การบูรณาการระหว่างแอปพลิเคชัน

ประเด็นสำคัญของสภาพปัจจุบันด้านแอปพลิเคชัน คือความสามารถในการทำงานร่วมกันระหว่างระบบ (Application Interoperability) เนื่องจากสถาบันอุดมศึกษามีระบบสารสนเทศจำนวนมากและมีผู้ใช้งานหลายกลุ่ม การทำให้ระบบสามารถแลกเปลี่ยนข้อมูลและเรียกใช้บริการระหว่างกันจึงเป็นปัจจัยสำคัญต่อการสร้างระบบดิจิทัลระดับองค์กร

การบูรณาการสามารถดำเนินการผ่านเทคโนโลยี เช่น Application Programming Interface (API), API Gateway, Middleware, Enterprise Service Bus (ESB), Message Broker และ Event-driven Architecture ทั้งนี้ การเลือกใช้รูปแบบการบูรณาการควรพิจารณาจากลักษณะของระบบ ความต้องการด้านประสิทธิภาพ ความมั่นคงปลอดภัย และปริมาณข้อมูล

สำหรับสถาบันอุดมศึกษา การมี Integration Architecture ที่เหมาะสมจะช่วยลดการเชื่อมต่อแบบจุดต่อจุดระหว่างระบบ และทำให้สามารถเพิ่มแอปพลิเคชันหรือบริการใหม่ได้ง่ายขึ้น โดยเฉพาะการเพิ่ม AI Services เข้ามาในระบบเดิมโดยไม่จำเป็นต้องปรับเปลี่ยนระบบต้นทางทั้งหมด

5.2.1.3.4 การประยุกต์ใช้ปัญญาประดิษฐ์ในระดับแอปพลิเคชัน

จากการเปลี่ยนแปลงทางเทคโนโลยี แอปพลิเคชันของสถาบันอุดมศึกษามีแนวโน้มเปลี่ยนจากระบบที่ทำหน้าที่เพียงบันทึกและประมวลผลข้อมูลไปสู่ Intelligent Applications ที่สามารถวิเคราะห์ข้อมูล เรียนรู้รูปแบบของข้อมูล และให้คำแนะนำหรือการแจ้งเตือนแก่ผู้ใช้งานได้ ในบริบทของงานวิจัย สามารถนำ AI มาเพิ่มความสามารถให้กับแอปพลิเคชันในหลายลักษณะ เช่น ระบบวิเคราะห์ความเสี่ยงของนักศึกษา ระบบคาดการณ์แนวโน้มการลงทะเบียน ระบบผู้ช่วยอัจฉริยะสำหรับนักศึกษา ระบบวิเคราะห์ข้อมูลการบริหาร ระบบตรวจจับพฤติกรรมผิดปกติ และระบบสนับสนุนการตัดสินใจสำหรับผู้บริหาร

การพัฒนาในลักษณะดังกล่าวจะทำให้แอปพลิเคชันไม่ได้ทำหน้าที่เพียงเป็นช่องทางให้ผู้ใช้เข้าถึงข้อมูล แต่สามารถทำหน้าที่เป็น Intelligent Service Layer ที่นำข้อมูลและ AI มาใช้สร้างความสามารถใหม่ให้กับองค์กร

5.2.1.3.5 แอปพลิเคชันด้านความมั่นคงปลอดภัยและภูมิคุ้มกันดิจิทัล

แอปพลิเคชันที่เกี่ยวข้องกับความมั่นคงปลอดภัยมีความสำคัญเป็นพิเศษ เนื่องจากเป็นองค์ประกอบที่ช่วยให้สถาบันสามารถป้องกัน ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามดิจิทัลได้ ระบบที่เกี่ยวข้องอาจประกอบด้วยระบบบริหารจัดการตัวตนและสิทธิการเข้าถึง (Identity and Access Management: IAM) ระบบรักษาความปลอดภัยเครือข่าย ระบบป้องกันและตรวจจับการบุกรุก ระบบจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ระบบบริหารช่องโหว่ ระบบบริหารเหตุการณ์ และระบบสำรองและกู้คืนข้อมูล เมื่อผนวก AI เข้ากับระบบดังกล่าว จะสามารถเพิ่มความสามารถด้านการตรวจจับความผิดปกติ การวิเคราะห์พฤติกรรม การจัดลำดับความสำคัญของเหตุการณ์ และการคาดการณ์ความเสี่ยง ตัวอย่างเช่น การนำ Machine Learning มาวิเคราะห์รูปแบบการเข้าสู่ระบบที่ผิดปกติ หรือวิเคราะห์ Network Traffic เพื่อระบุพฤติกรรมที่อาจมีความเสี่ยง ดังนั้น Application Architecture ในสถาปัตยกรรมเป้าหมายจึงควรสนับสนุนการทำงานร่วมกันระหว่าง ระบบธุรกิจ ระบบข้อมูล ระบบ AI และระบบความมั่นคงปลอดภัย เพื่อให้ข้อมูลจากเหตุการณ์ด้านความปลอดภัยสามารถถูกนำไปวิเคราะห์และส่งผลกลับไปยังผู้รับผิดชอบหรือระบบที่เกี่ยวข้องได้อย่างรวดเร็ว

5.2.1.3.6 ความสามารถในการรองรับ AI และการขยายระบบ

สภาพแวดล้อมด้านแอปพลิเคชันของสถาบันอุดมศึกษาจำเป็นต้องรองรับการเปลี่ยนแปลงของเทคโนโลยีอย่างต่อเนื่อง ดังนั้น การออกแบบ Application Architecture ไม่ควรพิจารณาเฉพาะ

ความสามารถของระบบในปัจจุบัน แต่ต้องคำนึงถึงความสามารถในการขยายระบบ (Scalability) ความยืดหยุ่น (Flexibility) การบำรุงรักษา (Maintainability) และความสามารถในการนำบริการใหม่มาเชื่อมต่อในอนาคต โดยเฉพาะการนำ AI มาใช้ จำเป็นต้องออกแบบให้สามารถเพิ่มหรือเปลี่ยน AI Model และ AI Services ได้โดยไม่ส่งผลกระทบต่อระบบหลักขององค์กรมากเกินไป แนวทางดังกล่าวอาจดำเนินการผ่านการออกแบบแบบ Modular Architecture, Service-oriented Architecture หรือ Microservices รวมถึงการให้บริการ AI ผ่าน API การออกแบบในลักษณะนี้จะช่วยให้สถาบันสามารถนำ AI มาใช้แบบค่อยเป็นค่อยไป เริ่มจากกระบวนการที่มีความสำคัญหรือมีความพร้อมสูง และสามารถขยายไปยังกระบวนการอื่นได้ในอนาคต

5.2.1.3.7 ความมั่นคงปลอดภัยของแอปพลิเคชัน

เนื่องจากแอปพลิเคชันเป็นช่องทางสำคัญในการเข้าถึงข้อมูลและบริการของสถาบัน จึงจำเป็นต้องมีการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของแอปพลิเคชัน ตั้งแต่การออกแบบ การพัฒนา การทดสอบ การนำไปใช้งาน การบำรุงรักษา และการยกเลิกระบบ

ประเด็นสำคัญ ได้แก่ การพิสูจน์และยืนยันตัวตน การกำหนดสิทธิการเข้าถึง การเข้ารหัสข้อมูล การจัดการ Session การตรวจสอบช่องโหว่ การบันทึก Log และการติดตามเหตุการณ์ผิดปกติ นอกจากนี้ การพัฒนาแอปพลิเคชันที่มี AI จำเป็นต้องพิจารณาความเสี่ยงเฉพาะของ AI เพิ่มเติม เช่น ความถูกต้องของผลลัพธ์ การป้องกันการใช้ข้อมูลโดยไม่ได้รับอนุญาต และการควบคุมการเข้าถึง AI Services แนวคิดดังกล่าวมีความสอดคล้องกับการพัฒนาสถาปัตยกรรมที่มุ่งสร้างภูมิคุ้มกันดิจิทัล ซึ่งไม่ได้พิจารณาเฉพาะการป้องกันโครงสร้างพื้นฐาน แต่ต้องครอบคลุมแอปพลิเคชันและบริการดิจิทัลที่เป็นส่วนหนึ่งของกระบวนการทางธุรกิจด้วย

5.2.1.3.8 การวิเคราะห์ช่องว่างด้านแอปพลิเคชัน (Application Gap Analysis)

จากการวิเคราะห์สภาพปัจจุบัน สามารถสังเคราะห์ช่องว่างด้าน Application Architecture ได้ดังตารางที่ 5-3

ตารางที่ 5-3 การวิเคราะห์ช่องว่างด้านแอปพลิเคชัน

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
ระบบสารสนเทศ	มีระบบสนับสนุนภารกิจหลายประเภท	ระบบมีความหลากหลายและแยกส่วน	Integrated Application Architecture
การเชื่อมโยงระบบ	มีการเชื่อมต่อระหว่างระบบบางส่วน	Interoperability ยังไม่ครอบคลุม	API & Integration Platform

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
การใช้ข้อมูล	ระบบสามารถจัดเก็บข้อมูลได้	การนำข้อมูลข้ามระบบมาวิเคราะห์ยังมีข้อจำกัด	Data-driven Applications
ปัญญาประดิษฐ์	เริ่มมีการนำ AI มาใช้ในบางงาน	ยังไม่เป็นความสามารถระดับองค์กร	AI-enabled Applications
การตัดสินใจ	มีรายงานและ Dashboard	การวิเคราะห์เชิงคาดการณ์ยังมีข้อจำกัด	Intelligent Decision Support
ความมั่นคงปลอดภัย	มีระบบรักษาความปลอดภัย	การวิเคราะห์เหตุการณ์แบบอัจฉริยะต้องพัฒนาเพิ่ม	AI-driven Security Applications
ความยืดหยุ่น	ระบบเดิมบางส่วนมีข้อจำกัดด้านการปรับเปลี่ยน	การเพิ่มบริการใหม่อาจกระทบระบบเดิม	Modular & Scalable Architecture
การบริหารวงจรชีวิต	มีการดูแลระบบตามภารกิจ	ต้องมีการบริหาร Application Portfolio ระดับองค์กร	Enterprise Application Portfolio Management

การวิเคราะห์สภาพปัจจุบันด้านแอปพลิเคชันพบว่า สถาบันอุดมศึกษามีระบบสารสนเทศที่สนับสนุนภารกิจหลักและภารกิจสนับสนุนเป็นจำนวนมาก และระบบเหล่านี้เป็นกลไกสำคัญในการขับเคลื่อนการดำเนินงานขององค์กรในรูปแบบดิจิทัล อย่างไรก็ตาม ความหลากหลายของระบบและการพัฒนาแอปพลิเคชันตามความต้องการของแต่ละหน่วยงานอาจทำให้เกิดข้อจำกัดด้านการเชื่อมโยงข้อมูล ความซ้ำซ้อนของระบบ ความแตกต่างของมาตรฐาน และข้อจำกัดในการนำข้อมูลมาใช้ในระดับองค์กร

5.2.1.4 ด้านเทคโนโลยี (Technology)

การวิเคราะห์สภาพปัจจุบันด้านเทคโนโลยี (Technology Architecture) ของสถาบันอุดมศึกษา พบว่า เทคโนโลยีเป็นโครงสร้างพื้นฐานสำคัญที่สนับสนุนการดำเนินงานขององค์กรในทุกระดับ ตั้งแต่การบริหารจัดการ การจัดการเรียนการสอน การบริหารนักศึกษา การวิจัยและนวัตกรรม การบริหารบุคลากร การเงินและงบประมาณ ตลอดจนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยเทคโนโลยีที่เกี่ยวข้องครอบคลุมทั้งโครงสร้างพื้นฐานด้านเครือข่าย ระบบประมวลผล ระบบจัดเก็บข้อมูล ระบบฐานข้อมูล ระบบคลาวด์ อุปกรณ์ปลายทาง และแพลตฟอร์มสำหรับให้บริการระบบสารสนเทศของสถาบัน

จากการวิเคราะห์พบว่า สถาบันอุดมศึกษามีการนำเทคโนโลยีดิจิทัลมาใช้สนับสนุนกระบวนการทางธุรกิจอย่างต่อเนื่อง โดยโครงสร้างพื้นฐานด้านเทคโนโลยีทำหน้าที่เป็นฐานในการให้บริการแอปพลิเคชันและระบบสารสนเทศต่าง ๆ ขณะที่ข้อมูลจากระบบเหล่านี้ถูกนำไปใช้ในการ

บริหารและสนับสนุนการตัดสินใจของผู้บริหาร อย่างไรก็ตาม เมื่อพิจารณาในบริบทของการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ พบว่าโครงสร้างพื้นฐานเทคโนโลยีแบบเดิมจำเป็นต้องได้รับการพัฒนาเพิ่มเติมเพื่อรองรับการประมวลผลข้อมูลปริมาณมาก การวิเคราะห์ข้อมูลแบบใกล้เคียงเวลาจริง การพัฒนาและใช้งานโมเดลปัญญาประดิษฐ์ ตลอดจนการขยายขีดความสามารถของระบบให้สามารถรองรับการเปลี่ยนแปลงในอนาคต

5.2.1.4.1 สภาพปัจจุบันด้านเทคโนโลยี

สภาพปัจจุบันของ Technology Architecture สามารถพิจารณาได้จากองค์ประกอบสำคัญ ได้แก่ โครงสร้างพื้นฐานเครือข่าย (Network Infrastructure) ระบบประมวลผล (Computing Infrastructure) ระบบจัดเก็บข้อมูล (Storage Infrastructure) ระบบฐานข้อมูล (Database Infrastructure) ระบบคลาวด์ (Cloud Infrastructure) อุปกรณ์ปลายทาง (Endpoint) และแพลตฟอร์มด้านปัญญาประดิษฐ์และการวิเคราะห์ข้อมูล (AI and Analytics Platform)

ในด้านเครือข่าย สถาบันจำเป็นต้องมีระบบเครือข่ายที่สามารถรองรับการเชื่อมต่อระหว่างผู้ใช้งาน ระบบสารสนเทศ อุปกรณ์ IoT และแหล่งข้อมูลต่าง ๆ ทั้งภายในและภายนอกองค์กร ขณะที่ระบบประมวลผลและระบบจัดเก็บข้อมูลทำหน้าที่รองรับการให้บริการแอปพลิเคชัน การจัดเก็บข้อมูล และการประมวลผลสารสนเทศขององค์กร

สำหรับการประยุกต์ใช้ปัญญาประดิษฐ์ โครงสร้างพื้นฐานดังกล่าวจำเป็นต้องรองรับการประมวลผลที่มีความต้องการทรัพยากรสูง เช่น การฝึกโมเดล Machine Learning และ Deep Learning การประมวลผลข้อมูลขนาดใหญ่ การวิเคราะห์ข้อมูลแบบต่อเนื่อง และการให้บริการโมเดล AI แก่ระบบงานต่าง ๆ ดังนั้น การออกแบบ Technology Architecture สำหรับสถาบันอุดมศึกษาจึงต้องพิจารณาความสามารถในการขยายระบบ ความยืดหยุ่น ความพร้อมใช้งาน และความต่อเนื่องของบริการควบคู่กัน

5.2.1.4.2 ความสัมพันธ์ระหว่างเทคโนโลยีกับกระบวนการธุรกิจ

เทคโนโลยีมีความสัมพันธ์กับกระบวนการธุรกิจของสถาบันอุดมศึกษาโดยตรง เนื่องจากกระบวนการดำเนินงานแต่ละประเภทต้องอาศัยโครงสร้างพื้นฐานและแพลตฟอร์มดิจิทัลในการสนับสนุน ดังตารางที่ 5.4

ตารางที่ 5.4 ความสัมพันธ์ระหว่างเทคโนโลยีกับกระบวนการธุรกิจของสถาบันอุดมศึกษา

กระบวนการธุรกิจ	เทคโนโลยีที่ใช้สนับสนุน	ข้อมูลที่เกี่ยวข้อง	ความสามารถที่ต้องการ
การบริหารองค์กร	Cloud, Server, Network, BI	KPI, แผนยุทธศาสตร์, ผลการดำเนินงาน	AI Decision Support

กระบวนการธุรกิจ	เทคโนโลยีที่ใช้สนับสนุน	ข้อมูลที่เกี่ยวข้อง	ความสามารถที่ต้องการ
การจัดการเรียนการสอน	LMS, Cloud, Network	ข้อมูลการเรียน ผลการเรียน การเข้าเรียน	Learning Analytics
การบริหารนักศึกษา	SIS, Mobile, Cloud	ข้อมูลนักศึกษา การลงทะเบียน ผลการเรียน	Predictive Analytics
การวิจัยและนวัตกรรม	Cloud, HPC/Computing Platform	ข้อมูลโครงการ ผลงานวิจัย	AI Analytics
การบริหารบุคลากร	HRIS, Cloud, Database	ประวัติ ภาระงาน ผลการประเมิน	Workforce Analytics
การเงินและงบประมาณ	ERP, Database, Cloud	งบประมาณ รายรับรายจ่าย	Forecasting
การบริหารระบบสารสนเทศ	Network, Server, Cloud, Monitoring	System Log, Performance Data	Intelligent Monitoring
ความมั่นคงปลอดภัย	Firewall, SIEM, Endpoint, IAM	Security Log, Event, Incident	AI Threat Detection
การจัดการภูมิคุ้มกันดิจิทัล	AI/ML Platform, Security Platform	Risk Data, Threat Data, Incident Data	Detect–Predict–Respond–Recover

จากตารางที่ 5-4 พบว่า เทคโนโลยีไม่ได้ทำหน้าที่เพียงสนับสนุนการดำเนินงานของแต่ละหน่วยงานเท่านั้น แต่ยังเป็นโครงสร้างพื้นฐานที่เชื่อมโยง กระบวนการธุรกิจ ข้อมูล แอปพลิเคชัน ความมั่นคงปลอดภัย และความสามารถด้านปัญญาประดิษฐ์ เข้าด้วยกัน ดังนั้น การออกแบบ Technology Architecture จึงต้องพิจารณาในระดับองค์กรและต้องสามารถรองรับกระบวนการที่มีการใช้ AI ในอนาคต

5.2.1.4.3 ปัญหาและข้อจำกัด

จากการวิเคราะห์สภาพปัจจุบัน พบว่าข้อจำกัดด้านเทคโนโลยีที่มีความสำคัญต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ได้แก่ การมีโครงสร้างพื้นฐานที่กระจายตามระบบหรือหน่วยงาน ความแตกต่างของเทคโนโลยีที่ใช้ในแต่ละระบบ ข้อจำกัดด้านทรัพยากรการประมวลผลสำหรับงาน AI ความสามารถในการขยายระบบ และการบริหารจัดการทรัพยากรเทคโนโลยีในภาพรวมขององค์กร นอกจากนี้ การนำ AI มาใช้ยังต้องการโครงสร้างพื้นฐานเฉพาะด้าน เช่น ทรัพยากรสำหรับการประมวลผลโมเดล AI ระบบจัดเก็บข้อมูลขนาดใหญ่ แพลตฟอร์มสำหรับพัฒนาและให้บริการโมเดล ตลอดจนระบบติดตามประสิทธิภาพของ AI ซึ่งแตกต่างจากความต้องการของระบบสารสนเทศทั่วไป อีกประเด็นหนึ่งคือ การให้บริการดิจิทัลของสถาบันอุดมศึกษามีความจำเป็นต้องดำเนินงานอย่างต่อเนื่อง หากโครงสร้างพื้นฐานเกิดความขัดข้องอาจส่งผลกระทบต่อ

กระบวนการเรียนการสอน การบริหารนักศึกษา การบริหารองค์กร และการให้บริการต่าง ๆ ดังนั้น Technology Architecture จึงต้องมีความสามารถด้านความพร้อมใช้งาน ความยืดหยุ่น การสำรองการกู้คืน และความต่อเนื่องของบริการ

5.2.1.4.4 การวิเคราะห์ช่องว่างด้านเทคโนโลยี (Technology Gap)

จากการเปรียบเทียบระหว่างสภาพปัจจุบันกับความต้องการในการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ พบช่องว่างสำคัญด้านเทคโนโลยี คือ ช่องว่างระหว่างโครงสร้างพื้นฐานดิจิทัลที่รองรับระบบสารสนเทศทั่วไปกับโครงสร้างพื้นฐานที่สามารถรองรับการทำงานของปัญญาประดิษฐ์ในระดับองค์กร สามารถสรุปช่องว่างได้ดังตารางที่ 5-5

ตารางที่ 5-5 การวิเคราะห์ช่องว่างด้านเทคโนโลยี

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
โครงสร้างพื้นฐานด้านเครือข่าย	มีโครงสร้างพื้นฐานเครือข่ายสำหรับรองรับการให้บริการระบบสารสนเทศและการเชื่อมต่อของผู้ใช้งาน	ความสามารถในการรองรับการเชื่อมต่ออุปกรณ์และระบบดิจิทัลจำนวนมาก รวมถึงการรับส่งข้อมูลสำหรับ AI ยังต้องได้รับการพัฒนา	AI-Ready Network Infrastructure ที่มีความยืดหยุ่น รองรับปริมาณข้อมูลสูง และสามารถบริหารจัดการเครือข่ายได้อย่างมีประสิทธิภาพ
ระบบประมวลผล	ใช้ Server และทรัพยากรประมวลผลสำหรับระบบสารสนเทศทั่วไป	ทรัพยากรประมวลผลอาจไม่เพียงพอสำหรับ AI Workload และการประมวลผลข้อมูลขนาดใหญ่	Scalable Computing Infrastructure และ AI Computing Infrastructureสำหรับรองรับการประมวลผล AI
การประมวลผลปัญญาประดิษฐ์	การใช้งาน AI ยังอยู่ในลักษณะของระบบหรือโครงการเฉพาะด้าน	ขาดโครงสร้างพื้นฐานและแพลตฟอร์มกลางสำหรับพัฒนา ฝึก และให้บริการโมเดล AI	Enterprise AI/ML Platform รองรับการพัฒนา ฝึก ทดสอบ นำไปใช้งาน และติดตามโมเดล AI
ระบบจัดเก็บข้อมูล	มีระบบจัดเก็บข้อมูลและฐานข้อมูลแยกตามระบบงาน	การจัดเก็บข้อมูลเพื่อรองรับข้อมูลขนาดใหญ่และ AI ยังขาดการบริหารจัดการในระดับองค์กร	Enterprise Storage และ Data Platform ที่รองรับข้อมูลขนาดใหญ่และ AI-Ready Data

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
Cloud Computing	มีการนำ Cloud Computing มาใช้สนับสนุนระบบและบริการดิจิทัลบางส่วน	การบริหารทรัพยากร Cloud ให้สามารถรองรับ AI และการขยายตัวของระบบยังมีข้อจำกัด	Cloud/Hybrid Cloud Architecture ที่สามารถปรับขนาดทรัพยากรให้เหมาะสมกับภาระงาน
แพลตฟอร์มข้อมูลและการวิเคราะห์	มีฐานข้อมูลและระบบสารสนเทศสำหรับจัดเก็บข้อมูลจากกระบวนการดำเนินงาน	ข้อมูลยังไม่สามารถนำมาวิเคราะห์ร่วมกันเพื่อสนับสนุน AI และการตัดสินใจเชิงคาดการณ์ได้อย่างเต็มประสิทธิภาพ	Enterprise Data Platform และ AI Analytics Platform สำหรับการวิเคราะห์ข้อมูลและสนับสนุนการตัดสินใจ
การติดตามและเฝ้าระวังระบบ	มีระบบ Monitoring สำหรับตรวจสอบสถานะและประสิทธิภาพของระบบ	การตรวจจับรูปแบบความผิดปกติและการคาดการณ์เหตุการณ์ที่อาจเกิดขึ้นยังมีข้อจำกัด	Intelligent Monitoring Platform ที่ใช้ AI ในการตรวจจับ Anomaly และวิเคราะห์แนวโน้ม
ความต่อเนื่องของบริการ	มีการสำรองข้อมูลและแนวทางการกู้คืนระบบสำหรับระบบสำคัญ	ความสามารถในการฟื้นฟูระบบและให้บริการอย่างต่อเนื่องเมื่อเกิดเหตุการณ์ผิดปกติยังต้องพัฒนา	Resilient Technology Infrastructure รองรับ Backup, Recovery, Redundancy และ Business Continuity
การบริหารทรัพยากรเทคโนโลยี	การบริหารทรัพยากรดำเนินการตามระบบและหน่วยงาน	ขาดการบริหารทรัพยากรเทคโนโลยีแบบรวมศูนย์และการวิเคราะห์การใช้ทรัพยากรเชิงคาดการณ์	Intelligent Technology Management สำหรับติดตาม วิเคราะห์ และคาดการณ์การใช้ทรัพยากร
การสนับสนุนภูมิคุ้มกันดิจิทัล	เทคโนโลยีสนับสนุนการป้องกันและแก้ไขปัญหาด้านระบบเป็นหลัก	ยังขาดความสามารถในการใช้ AI เพื่อเฝ้าระวัง ตรวจจับ วิเคราะห์ คาดการณ์ และตอบสนองต่อความเสี่ยงอย่างเป็นระบบ	AI-Enabled Digital Immunity Infrastructure สนับสนุน Monitor ⟶ Detect ⟶ Analyze ⟶ Predict ⟶ Respond ⟶ Recover

จากตารางที่ 5.5 ผลการวิเคราะห์ช่องว่างด้านเทคโนโลยีพบว่า สถาบันอุดมศึกษามีโครงสร้างพื้นฐานด้านเทคโนโลยีที่สามารถรองรับการดำเนินงานของระบบสารสนเทศและบริการดิจิทัลในปัจจุบัน แต่เมื่อพิจารณาความต้องการในการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล พบว่ายังมีช่องว่างสำคัญในด้านความสามารถของโครงสร้างพื้นฐานในการ

รองรับการประมวลผลปัญญาประดิษฐ์ การจัดการข้อมูลขนาดใหญ่ การขยายทรัพยากร การติดตามความผิดปกติ และการรักษาความต่อเนื่องของบริการ ดังนั้น ผู้วิจัยจึงกำหนดสถาปัตยกรรมเป้าหมายด้านเทคโนโลยีให้มุ่งสู่ AI-Ready Technology Architecture ซึ่งประกอบด้วยโครงสร้างพื้นฐานเครือข่ายและการประมวลผลที่สามารถขยายได้ ระบบ Cloud หรือ Hybrid Cloud แพลตฟอร์มสำหรับการจัดการข้อมูลและ AI/ML ระบบ Intelligent Monitoring และโครงสร้างพื้นฐานที่มีความยืดหยุ่นและสามารถฟื้นฟูได้เมื่อเกิดเหตุการณ์ผิดปกติ โดยองค์ประกอบเหล่านี้จะทำหน้าที่เป็นโครงสร้างพื้นฐานสนับสนุนการทำงานของ AI และเชื่อมโยงกับด้านข้อมูล แอปพลิเคชัน ความมั่นคงปลอดภัย และการบูรณาการของสถาปัตยกรรมองค์กร ในมิติของการจัดการภูมิคุ้มกันดิจิทัล เทคโนโลยีเป้าหมายจะยกระดับความสามารถของสถาบันจากการป้องกันและแก้ไขปัญหาภายหลังเกิดเหตุ ไปสู่การเฝ้าระวัง ตรวจจับ วิเคราะห์ คาดการณ์ ตอบสนอง และฟื้นฟูอย่างเป็นระบบ โดยใช้ปัญญาประดิษฐ์เป็นกลไกสำคัญในการเพิ่มความสามารถในการรับรู้และตอบสนองต่อความเสี่ยงทางดิจิทัลของสถาบันอุดมศึกษา

5.2.1.4.5 ความต้องการด้านเทคโนโลยี (Technology Requirements)

จากการวิเคราะห์ช่องว่าง ผู้วิจัยสังเคราะห์ความต้องการด้านเทคโนโลยีสำหรับสถาปัตยกรรมเป้าหมาย ประกอบด้วย 6 ประการ ได้แก่

- AI Computing สำหรับรองรับการประมวลผลและการให้บริการโมเดล AI
- Cloud/Hybrid Cloud เพื่อเพิ่มความยืดหยุ่นและความสามารถในการขยายระบบ
- Enterprise Data Platform สำหรับรองรับการจัดเก็บและประมวลผลข้อมูลจากหลายแหล่ง
- AI/ML Platform สำหรับการพัฒนา ฝึก ทดสอบ นำไปใช้งาน และติดตามโมเดล AI
- Intelligent Monitoring สำหรับติดตามประสิทธิภาพของโครงสร้างพื้นฐาน ระบบสารสนเทศ และเหตุการณ์ผิดปกติ
- Resilient Infrastructure สำหรับรองรับความต่อเนื่องของบริการ การสำรอง และการฟื้นฟูระบบ

5.2.1.4.6 การออกแบบด้านเทคโนโลยีใน Target Architecture

จากผลการวิเคราะห์ ผู้วิจัยกำหนด Technology Architecture ในสถาปัตยกรรมเป้าหมายให้เป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของ AI และการจัดการภูมิคุ้มกันดิจิทัล โดยประกอบด้วย Network Infrastructure, Cloud/Hybrid Cloud, Computing Infrastructure, AI Computing, Storage, Enterprise Data Platform, AI/ML Platform และ Monitoring & Resilience Platform

โครงสร้างดังกล่าวทำหน้าที่เป็นพื้นฐานให้กับสถาปัตยกรรมในมิติอื่น โดยเฉพาะ Data Architecture, Application Architecture, Security Architecture และIntegration Architecture ขณะเดียวกันยังรองรับการนำเทคโนโลยี AI เช่น Machine Learning, Deep Learning, Predictive Analytics และ Anomaly Detection มาใช้ในการวิเคราะห์ข้อมูลและตรวจจับเหตุการณ์ผิดปกติ

ในบริบทของการจัดการภูมิคุ้มกันดิจิทัล เทคโนโลยีดังกล่าวจะสนับสนุนความสามารถขององค์กรในลักษณะเป็นวงจร ได้แก่ การเฝ้าระวัง (Monitoring) การตรวจจับ (Detection) การวิเคราะห์ (Analysis) การคาดการณ์ (Prediction) การตอบสนอง (Response) และการฟื้นฟู (Recovery) ซึ่งช่วยยกระดับการบริหารจัดการจากการแก้ไขปัญหาหลังเกิดเหตุไปสู่การบริหารความเสี่ยงเชิงรุกและเชิงคาดการณ์

ตารางที่ 5-6 สรุปผลการวิเคราะห์ด้านเทคโนโลยี

ประเด็น	ผลการวิเคราะห์
Current Architecture	โครงสร้างพื้นฐานเครือข่าย Server, Storage, Cloud และระบบประมวลผลเพื่อรองรับระบบสารสนเทศ
Business Relationship	สนับสนุนการเรียนการสอน การบริหาร นักศึกษา วิจัย บุคลากร การเงิน และ Security
Problem	โครงสร้างพื้นฐานบางส่วนแยกตามระบบและมีข้อจำกัดในการรองรับ AI Workload
Gap	Digital Infrastructure ยังไม่เป็น AI-Ready Infrastructure อย่างสมบูรณ์
Requirement	Scalable, Secure, Resilient และ AI-Ready Infrastructure
AI Technology	Machine Learning, Deep Learning, Predictive Analytics, Anomaly Detection
Target Architecture	Cloud/Hybrid Cloud + AI Computing + Data Platform + AI/ML Platform + Monitoring
Digital Immunity Capability	Monitor ⟶ Detect ⟶ Analyze ⟶ Predict ⟶ Respond ⟶ Recover

จากผลการวิเคราะห์ด้านเทคโนโลยี ผู้วิจัยพบว่า Technology Architecture เป็นโครงสร้างพื้นฐานที่เชื่อมโยงและสนับสนุนองค์ประกอบทั้งหมดของสถาปัตยกรรมองค์กร ปัญญาประดิษฐ์ โดยเฉพาะการประมวลผลข้อมูล การให้บริการแอปพลิเคชัน การรักษาความมั่นคงปลอดภัย และการนำ AI มาใช้ในการจัดการความเสี่ยงดิจิทัล ดังนั้น สถาปัตยกรรมเป้าหมายจึงต้องเปลี่ยนจากโครงสร้างพื้นฐานที่รองรับระบบสารสนเทศทั่วไปไปสู่ AI-Ready, Scalable และ

Resilient Technology Architecture ซึ่งสามารถรองรับการประมวลผล AI การวิเคราะห์ข้อมูล และการดำเนินงานด้านภูมิคุ้มกันดิจิทัลได้อย่างต่อเนื่องและมีประสิทธิภาพ

5.2.1.5 ด้านความมั่งคงปลอดภัย (Security)

ผลการวิเคราะห์สภาพปัจจุบันด้านความมั่นคงปลอดภัย (Security Architecture) ของสถาบันอุดมศึกษา พบว่า ความมั่นคงปลอดภัยเป็นองค์ประกอบสำคัญของสถาปัตยกรรมองค์กร เนื่องจากสถาบันอุดมศึกษามีการจัดเก็บและประมวลผลข้อมูลจำนวนมาก ทั้งข้อมูลนักศึกษา ข้อมูลบุคลากร ข้อมูลการเรียนการสอน ข้อมูลการวิจัย ข้อมูลการเงิน ข้อมูลการบริหาร ตลอดจนข้อมูลที่เกิดจากการใช้งานระบบสารสนเทศและโครงสร้างพื้นฐานดิจิทัล ดังนั้น การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบจึงมีความสัมพันธ์โดยตรงกับความต่อเนื่องของกระบวนการดำเนินงานของสถาบัน

จากการวิเคราะห์พบว่า สถาบันอุดมศึกษามีการนำมาตรการและเทคโนโลยีด้านความมั่นคงปลอดภัยมาใช้เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น การควบคุมสิทธิ์การเข้าถึง การยืนยันตัวตน การรักษาความปลอดภัยของเครือข่าย การป้องกันมัลแวร์ การสำรองข้อมูล การจัดเก็บบันทึกเหตุการณ์ และการตรวจสอบการใช้งานระบบ อย่างไรก็ตาม ลักษณะของภัยคุกคามทางดิจิทัลมีความซับซ้อนและเปลี่ยนแปลงอย่างต่อเนื่อง จึงจำเป็นต้องพัฒนาความสามารถด้านความมั่นคงปลอดภัยจากการป้องกันและตรวจจับในรูปแบบเดิม ไปสู่การใช้ข้อมูลและปัญญาประดิษฐ์เพื่อสนับสนุนการวิเคราะห์ คาดการณ์ และตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็ว

5.2.1.5.1 สภาพปัจจุบันด้านความมั่นคงปลอดภัย

สภาพปัจจุบันของ Security Architecture สามารถพิจารณาได้จากองค์ประกอบสำคัญ ได้แก่ การบริหารจัดการตัวตนและสิทธิ์การเข้าถึง (Identity and Access Management) ความมั่นคงปลอดภัยของเครือข่าย (Network Security) ความมั่นคงปลอดภัยของข้อมูล (Data Security) ความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง (Endpoint Security) การตรวจสอบและเฝ้าระวังเหตุการณ์ (Security Monitoring) การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response) และการสำรองและฟื้นฟูระบบ (Backup and Recovery)

ในบริบทของสถาบันอุดมศึกษา ระบบความมั่นคงปลอดภัยต้องรองรับผู้ใช้งานจำนวนมากและมีความหลากหลาย ทั้งผู้บริหาร บุคลากร นักศึกษา นักวิจัย และผู้ใช้งานภายนอก รวมถึงต้องรองรับการเข้าถึงระบบจากทั้งภายในและภายนอกสถาบัน การเชื่อมต่อระบบสารสนเทศหลายประเภท และการใช้บริการ Cloud และอุปกรณ์ดิจิทัลที่เพิ่มขึ้น ดังนั้น การรักษาความมั่นคงปลอดภัยจึงไม่สามารถจำกัดอยู่เฉพาะการป้องกันเครือข่ายหรือระบบสารสนเทศ แต่ต้องครอบคลุมตั้งแต่ ผู้ใช้งาน ข้อมูล แอปพลิเคชัน โครงสร้างพื้นฐาน การเชื่อมต่อระบบ และกระบวนการบริหารจัดการความเสี่ยง โดยมีการติดตามและประเมินความเสี่ยงอย่างต่อเนื่อง

5.2.1.5.2 ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยกับกระบวนการธุรกิจ

ความมั่นคงปลอดภัยมีความสัมพันธ์กับกระบวนการธุรกิจของสถาบันอุดมศึกษาในทุกระดับ เนื่องจากการหยุดชะงักหรือการสูญเสียความน่าเชื่อถือของระบบสารสนเทศอาจส่งผลโดยตรงต่อการดำเนินงานขององค์กร ดังตารางที่ 5-7

ตารางที่ 5-7 ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยกับกระบวนการธุรกิจ

กระบวนการธุรกิจ	สภาพการใช้งาน/ระบบที่เกี่ยวข้อง	ข้อมูลที่ต้องปกป้อง	ความสามารถด้านความมั่นคงปลอดภัยที่ต้องการ
การบริหารองค์กร	ระบบบริหารและระบบสารสนเทศเพื่อการตัดสินใจ	ข้อมูลยุทธศาสตร์ รายงาน และข้อมูลบริหาร	Access Control, Audit, Data Security
การจัดการเรียนการสอน	LMS, ระบบทะเบียน และระบบการเรียนรู้	ข้อมูลนักศึกษา ผลการเรียน และข้อมูลการเรียนรู้	Identity Management, Access Control
การบริหารนักศึกษา	ระบบรับสมัคร ทะเบียน และบริการนักศึกษา	ข้อมูลส่วนบุคคลและข้อมูลการศึกษา	IAM, Privacy, Data Protection
การบริหารบุคลากร	HRIS และระบบบุคลากร	ข้อมูลส่วนบุคคล ประวัติ และข้อมูลการปฏิบัติงาน	IAM, Data Security, Audit
การวิจัย	ระบบบริหารงานวิจัยและคลังข้อมูล	ข้อมูลงานวิจัยและทรัพย์สินทางปัญญา	Data Protection, Access Control
การเงินและงบประมาณ	ERP และระบบการเงิน	ข้อมูลธุรกรรม งบประมาณ และการเงิน	Transaction Security, Fraud Detection
การบริหารระบบ IT	Network, Server, Cloud และ Application	System Log และ Configuration	Monitoring, Threat Detection
การให้บริการดิจิทัล	Web, Mobile และ Online Services	ข้อมูลผู้ใช้และข้อมูลธุรกรรม	Application Security, WAF, IAM
การจัดการเหตุการณ์	SIEM, Log และ Security Platform	Security Event และ Incident Data	AI Threat Detection, Incident Response
การจัดการภูมิคุ้มกันดิจิทัล	Security Operations และ AI Platform	Risk, Threat, Event และ Incident Data	Detect, Analyze, Predict, Respond, Recover

จากตารางที่ 5-7 จะเห็นได้ว่า Security Architecture มีความสัมพันธ์กับกระบวนการธุรกิจตั้งแต่ระดับการป้องกันข้อมูลและการควบคุมสิทธิ์ ไปจนถึงการตรวจจับและตอบสนองต่อเหตุการณ์

ด้านความมั่นคงปลอดภัย ดังนั้น ความมั่นคงปลอดภัยจึงควรได้รับการออกแบบให้เป็นองค์ประกอบที่ทำงานร่วมกับทุกมิติของโครงสร้างองค์กร ไม่ใช่เป็นระบบที่แยกออกจากกระบวนการธุรกิจ

5.2.1.5.3 ปัญหาและข้อจำกัดด้านความมั่นคงปลอดภัย

จากการวิเคราะห์สภาพปัจจุบัน พบว่าความท้าทายสำคัญของสถาบันอุดมศึกษาคือความหลากหลายของระบบ ผู้ใช้งาน อุปกรณ์ และข้อมูล รวมถึงการเชื่อมต่อระบบสารสนเทศระหว่างหน่วยงานและการใช้บริการดิจิทัลจากภายนอก ส่งผลให้ขอบเขตของการรักษาความมั่นคงปลอดภัยมีความซับซ้อนมากขึ้น นอกจากนี้ การรักษาความมั่นคงปลอดภัยในรูปแบบเดิมมักให้ความสำคัญกับการป้องกันและตรวจจับเหตุการณ์ที่เกิดขึ้นแล้ว ขณะที่ความสามารถในการวิเคราะห์พฤติกรรมที่ผิดปกติ การเชื่อมโยงเหตุการณ์จากหลายแหล่ง และการคาดการณ์ความเสี่ยงก่อนที่จะเกิดเหตุการณ์ยังมีข้อจำกัด

อีกประเด็นหนึ่งคือ ข้อมูลด้านความมั่นคงปลอดภัย เช่น Log, Event, Alert และ Incident มีปริมาณมากและเกิดขึ้นอย่างต่อเนื่อง การวิเคราะห์ข้อมูลดังกล่าวด้วยบุคลากรเพียงอย่างเดียวอาจไม่สามารถประมวลผลเหตุการณ์ทั้งหมดได้อย่างรวดเร็ว จึงมีความจำเป็นต้องนำ AI และ Machine Learning มาใช้ในการวิเคราะห์รูปแบบความผิดปกติและจัดลำดับความสำคัญของเหตุการณ์ ดังนั้น ปัญหาสำคัญไม่ได้อยู่เพียงการมีหรือไม่มีเครื่องมือรักษาความปลอดภัย แต่เป็นความสามารถในการบูรณาการข้อมูลและเทคโนโลยีความมั่นคงปลอดภัยเพื่อสร้างความสามารถในการรับรู้ วิเคราะห์ คาดการณ์ และตอบสนองต่อภัยคุกคามอย่างเป็นระบบ

5.2.1.5.4 การวิเคราะห์ช่องว่างด้านความมั่นคงปลอดภัย (Security Gap)

จากการเปรียบเทียบสภาพปัจจุบันกับความต้องการของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัล ผู้วิจัยได้วิเคราะห์ช่องว่างด้านความมั่นคงปลอดภัย ดังตารางที่ 5-8

ตารางที่ 5-8 การวิเคราะห์ช่องว่างด้านความมั่นคงปลอดภัย (Security Gap)

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
การบริหารตัวตนและสิทธิ์	มีการกำหนดบัญชีผู้ใช้และสิทธิ์การเข้าถึงระบบ	การบริหารสิทธิ์ในสภาพแวดล้อมที่มีระบบและผู้ใช้งานจำนวนมากมีความซับซ้อน	Integrated Identity and Access Management (IAM)
การยืนยันตัวตน	ใช้การยืนยันตัวตนตามระบบและบริการ	จำเป็นต้องเพิ่มความเข้มแข็งและลดความเสี่ยงจากบัญชีผู้ใช้ถูกบุกรุก	Adaptive/Strong Authentication

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
ความมั่นคงปลอดภัยของข้อมูล	มีการควบคุมการเข้าถึงและป้องกันข้อมูลในระดับระบบ	การกำกับดูแลและการป้องกันข้อมูลแบบองค์รวมยังต้องได้รับการพัฒนา	Enterprise Data Security & Privacy Architecture
ความมั่นคงปลอดภัยเครือข่าย	มี Firewall และระบบรักษาความปลอดภัยเครือข่าย	การตรวจจับภัยคุกคามที่มีรูปแบบซับซ้อนและเปลี่ยนแปลงตลอดเวลายังมีข้อจำกัด	AI-Enabled Network Security
ความมั่นคงปลอดภัยอุปกรณ์	มีการป้องกันอุปกรณ์ปลายทาง	การวิเคราะห์พฤติกรรมและตรวจจับความผิดปกติจากอุปกรณ์จำนวนมากยังจำกัด	Intelligent Endpoint Security
การเฝ้าระวัง	มีการจัดเก็บ Log และติดตามเหตุการณ์	ข้อมูลจากหลายระบบยังต้องได้รับการวิเคราะห์และเชื่อมโยงอย่างเป็นระบบ	SIEM + AI Analytics
การตรวจจับภัยคุกคาม	ตรวจจับจากกฎและรูปแบบภัยคุกคามที่กำหนด	อาจตรวจจับภัยคุกคามรูปแบบใหม่ได้ไม่ครอบคลุม	AI Threat Detection & Anomaly Detection
การวิเคราะห์พฤติกรรม	วิเคราะห์เหตุการณ์จากข้อมูลที่มีอยู่	ขาดความสามารถในการเรียนรู้รูปแบบพฤติกรรมของผู้ใช้งานและระบบ	UEBA และ Behavioral Analytics
การตอบสนองต่อเหตุการณ์	มีขั้นตอนการจัดการ Incident	การตอบสนองบางส่วนยังต้องอาศัยการดำเนินงานโดยบุคลากร	AI-Assisted Incident Response / SOAR
การคาดการณ์ความเสี่ยง	ประเมินความเสี่ยงจากข้อมูลและเหตุการณ์ที่ผ่านมา	ขาดความสามารถในการคาดการณ์ความเสี่ยงเชิงรุก	Predictive Security Analytics
การสำรองและฟื้นฟู	มี Backup และกระบวนการ Recovery	ต้องเพิ่มความสามารถในการฟื้นฟูอย่างรวดเร็วและต่อเนื่อง	Resilient Backup & Recovery Architecture
การจัดการภูมิคุ้มกันดิจิทัล	เน้นการป้องกันและแก้ไขเหตุการณ์	ความสามารถในการเชื่อมโยง Detect–Predict–Respond–Recover ยังไม่เป็นระบบเดียวกัน	AI-Enabled Digital Immunity Architecture

5.2.1.5.5 ความต้องการด้านความมั่นคงปลอดภัย (Security Requirements)

จากผลการวิเคราะห์ช่องว่าง ผู้วิจัยสังเคราะห์ความต้องการด้านความมั่นคงปลอดภัยสำหรับสถาปัตยกรรมเป้าหมาย โดยมุ่งเน้นการเปลี่ยนแปลงจากระบบรักษาความปลอดภัยแบบเชิงรับไปสู่ระบบที่สามารถรับรู้และตอบสนองต่อภัยคุกคามเชิงรุก ประกอบด้วยความต้องการสำคัญ ได้แก่

1. ต้องมีระบบบริหารตัวตนและสิทธิ์การเข้าถึงที่สามารถควบคุมผู้ใช้งานและทรัพยากรดิจิทัลได้อย่างเหมาะสม

2. ต้องมีระบบรวบรวมและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยจากหลายแหล่ง เพื่อสร้างมุมมองด้านความเสี่ยงในระดับองค์กร

3. ต้องมีการนำ AI และ Machine Learning มาใช้ในการตรวจจับความผิดปกติ วิเคราะห์พฤติกรรม และคาดการณ์ภัยคุกคาม

4. ต้องมีความสามารถในการตอบสนองต่อเหตุการณ์อย่างรวดเร็วและสามารถเชื่อมโยงกับกระบวนการจัดการ Incident Response

5. ต้องมีความสามารถด้านการสำรองและฟื้นฟูระบบ เพื่อให้สถาบันสามารถกลับมาดำเนินงานได้ภายหลังเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบดิจิทัล

6) การออกแบบด้านความมั่นคงปลอดภัยใน Target Architecture

จากผลการวิเคราะห์ ผู้วิจัยกำหนด Security Architecture ในสถาปัตยกรรมเป้าหมายให้มีลักษณะเป็น AI-Enabled Security Architecture ซึ่งทำงานครอบคลุมตั้งแต่การป้องกัน การตรวจจับ การวิเคราะห์ การคาดการณ์ การตอบสนอง และการฟื้นฟู โดยเชื่อมโยงกับข้อมูลและระบบสารสนเทศของสถาบันอุดมศึกษา

องค์ประกอบสำคัญของสถาปัตยกรรมเป้าหมายประกอบด้วย Identity and Access Management, Network Security, Endpoint Security, Data Security, Security Monitoring, SIEM, Threat Intelligence, AI Threat Detection, UEBA, Incident Response, SOAR และ Backup & Recovery โดยมี AI เป็นกลไกสำคัญในการวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยและสนับสนุนการตัดสินใจ โครงสร้างดังกล่าวทำให้ Security Architecture ไม่ได้ทำหน้าที่เฉพาะการป้องกันภัยคุกคาม แต่สามารถทำงานร่วมกับ Data Architecture, Application Architecture, Technology Architecture และ Integration Architecture เพื่อสร้างความสามารถด้านภูมิคุ้มกันดิจิทัลในระดับองค์กร

ตารางที่ 5-9 สรุปผลการวิเคราะห์ด้านความมั่นคงปลอดภัย

ประเด็น	ผลการวิเคราะห์
Current Architecture	ระบบควบคุมสิทธิ์ ความปลอดภัยเครือข่าย Endpoint, Log และระบบป้องกันภัยคุกคาม
Business Relationship	สนับสนุนความปลอดภัยของการเรียนการสอน นักศึกษา บุคลากร วิจัย การเงิน และบริการดิจิทัล

ประเด็น	ผลการวิเคราะห์
Problem	ภัยคุกคามมีความซับซ้อน ข้อมูล Security Event มีจำนวนมาก และการวิเคราะห์เชิงรุกยังจำกัด
Gap	ขาดการบูรณาการข้อมูล Security และ AI เพื่อการตรวจจับ วิเคราะห์ และคาดการณ์
Requirement	Integrated, Intelligent, Predictive และ Resilient Security
AI Technology	Machine Learning, Anomaly Detection, UEBA, Predictive Analytics, Generative AI
Target Architecture	AI-Enabled Security Architecture
Digital Immunity Capability	Detect ⟶ Analyze ⟶ Predict ⟶ Respond ⟶ Recover

จากผลการวิเคราะห์ด้านความมั่นคงปลอดภัย ผู้วิจัยพบว่า การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สำหรับสถาบันอุดมศึกษาจำเป็นต้องยกระดับ Security Architecture จากการรักษาความมั่นคงปลอดภัยในลักษณะเชิงรับไปสู่ระบบรักษาความมั่นคงปลอดภัยที่สามารถเรียนรู้ วิเคราะห์ และคาดการณ์ได้ด้วยปัญญาประดิษฐ์ โดยมีการบูรณาการข้อมูลจากระบบสารสนเทศ เครือข่าย อุปกรณ์ ผู้ใช้งาน และเหตุการณ์ด้านความมั่นคงปลอดภัยเข้าด้วยกัน

5.2.1.6 ด้านการบูรณาการ (Integration)

ผลการวิเคราะห์สภาพปัจจุบันด้านการบูรณาการ (Integration Architecture) ของสถาบันอุดมศึกษา พบว่า การบูรณาการเป็นองค์ประกอบสำคัญในการเชื่อมโยงกระบวนการทางธุรกิจ ข้อมูล แอปพลิเคชัน เทคโนโลยี และระบบความมั่นคงปลอดภัยให้สามารถทำงานร่วมกันได้อย่างต่อเนื่อง เนื่องจากสถาบันอุดมศึกษามีระบบสารสนเทศที่สนับสนุนภารกิจหลายด้าน เช่น ระบบบริหารจัดการองค์กร ระบบทะเบียนและบริการนักศึกษา ระบบบริหารการเรียนรู้ ระบบบริหารบุคลากร ระบบการเงิน ระบบงานวิจัย ระบบห้องสมุด และระบบด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัย ซึ่งแต่ละระบบมีรูปแบบข้อมูล เทคโนโลยี และวิธีการแลกเปลี่ยนข้อมูลที่แตกต่างกัน จากการวิเคราะห์พบว่า ระบบสารสนเทศของสถาบันมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลเพื่อสนับสนุนกระบวนการดำเนินงานอยู่ในระดับหนึ่ง แต่การบูรณาการระหว่างระบบในบางส่วนยังมีลักษณะเป็นการเชื่อมต่อเฉพาะระบบหรือเฉพาะกระบวนการ ทำให้การแลกเปลี่ยนข้อมูลในระดับองค์กรยังไม่เป็นรูปแบบเดียวกัน และอาจส่งผลต่อความถูกต้อง ความรวดเร็ว และความต่อเนื่องของข้อมูล เมื่อมีความต้องการนำข้อมูลจากหลายระบบมาประมวลผลร่วมกันเพื่อสนับสนุนการตัดสินใจหรือการทำงานของปัญญาประดิษฐ์ ดังนั้น การออกแบบ Integration Architecture สำหรับงานวิจัยนี้จึงมุ่งเน้นการพัฒนาจากการเชื่อมโยงระบบสารสนเทศแบบเฉพาะส่วน ไปสู่การบูรณาการระดับ

องค์กร (Enterprise Integration) โดยมีมาตรฐานกลางสำหรับการแลกเปลี่ยนข้อมูลและบริการ รวมถึงสามารถรองรับการเชื่อมโยงกับ AI Platform และระบบจัดการภูมิคุ้มกันดิจิทัลได้

5.2.1.6.1 สภาพปัจจุบันด้านการบูรณาการ

สภาพปัจจุบันของ Integration Architecture สามารถพิจารณาได้จากการเชื่อมโยงระหว่าง กระบวนการธุรกิจ ระบบแอปพลิเคชัน ฐานข้อมูล โครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัย โดยระบบต่าง ๆ มีการแลกเปลี่ยนข้อมูลเพื่อสนับสนุนการดำเนินงาน เช่น การเชื่อมโยงข้อมูลนักศึกษาระหว่างระบบรับสมัคร ระบบทะเบียน และระบบการเรียนรู้ การเชื่อมโยงข้อมูลบุคลากรกับระบบบริหารทรัพยากรบุคคลและระบบเงินเดือน ตลอดจนการเชื่อมโยงข้อมูลทางการเงินกับระบบบริหารงบประมาณและระบบจัดซื้อจัดจ้าง เมื่อพิจารณาในระดับองค์กร พบว่าการเชื่อมโยงระบบจำนวนมากยังขึ้นอยู่กับโครงสร้างและเทคโนโลยีของแต่ละระบบ ทำให้การเพิ่มระบบใหม่หรือปรับเปลี่ยนระบบเดิมอาจต้องมีการพัฒนาการเชื่อมต่อเพิ่มเติม ส่งผลให้เกิดความซับซ้อนในการบริหารจัดการและเพิ่มภาระในการดูแลระบบ ในบริบทของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ความต้องการด้าน Integration มีความซับซ้อนมากขึ้น เนื่องจาก AI จำเป็นต้องเข้าถึงข้อมูลจากหลายแหล่งและต้องสามารถส่งผลการวิเคราะห์กลับไปยังระบบที่เกี่ยวข้องได้ ดังนั้น การบูรณาการจึงต้องรองรับทั้ง Data Integration, Application Integration, API Integration และ AI Integration

5.2.1.6.2 ความสัมพันธ์ระหว่างการบูรณาการกับกระบวนการธุรกิจ

Integration Architecture มีความสัมพันธ์กับกระบวนการธุรกิจในลักษณะเป็นกลไกกลางที่ทำให้ข้อมูลและบริการสามารถเคลื่อนที่ระหว่างระบบต่าง ๆ ได้อย่างต่อเนื่อง ดังตารางที่ 5-10

ตารางที่ 5-10 ความสัมพันธ์ระหว่างการบูรณาการกับกระบวนการธุรกิจ

กระบวนการธุรกิจ	ระบบ/แหล่งข้อมูลที่เกี่ยวข้อง	การบูรณาการที่ต้องการ	ผลลัพธ์ที่ต้องการ
การบริหารองค์กร	ERP, BI, ระบบบริหาร	Data/API Integration	ข้อมูลสำหรับการตัดสินใจแบบองค์รวม
การรับสมัครนักศึกษา	Admission, SIS, CRM	Application/Data Integration	ข้อมูลผู้สมัครเชื่อมโยงตลอดกระบวนการ
การจัดการนักศึกษา	SIS, LMS, Mobile Application	API/Data Integration	ข้อมูลนักศึกษาแบบต่อเนื่อง
การจัดการเรียนการสอน	LMS, SIS, Digital Learning Platform	API/Event Integration	ข้อมูลการเรียนรู้เพื่อวิเคราะห์ผลการเรียน
การบริหารบุคลากร	HRIS, Payroll, ERP	Data/API Integration	ข้อมูลบุคลากรที่สอดคล้องกัน

กระบวนการธุรกิจ	ระบบ/แหล่งข้อมูลที่เกี่ยวข้อง	การบูรณาการที่ต้องการ	ผลลัพธ์ที่ต้องการ
การบริหารการเงิน	ERP, Finance, Procurement	Transaction/Data Integration	ข้อมูลการเงินที่ถูกต้องและทันเวลา
การวิจัย	Research System, Repository	Data/API Integration	ข้อมูลการวิจัยที่สามารถใช้ร่วมกัน
ความมั่นคงปลอดภัย	SIEM, Firewall, Endpoint, IAM	Security/Event Integration	ข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยแบบรวมศูนย์
การวิเคราะห์ด้วย AI	Data Platform, AI/ML Platform, Application	AI/API/Data Integration	ผลการวิเคราะห์และการคาดการณ์จาก AI
การจัดการภูมิคุ้มกันดิจิทัล	Security, Data, AI, Monitoring	Real-time/Event Integration	Detect ⟶ Analyze ⟶ Predict ⟶ Respond ⟶ Recover

จากตารางที่ 5-10 พบว่า Integration Architecture ทำหน้าที่เป็นกลไกเชื่อมโยงกระบวนการทางธุรกิจทั้งหมด โดยเฉพาะกระบวนการที่ต้องใช้ข้อมูลจากหลายระบบร่วมกัน ดังนั้นประสิทธิภาพของการบูรณาการจึงส่งผลโดยตรงต่อความสามารถในการใช้ข้อมูลและ AI เพื่อสนับสนุนการบริหารจัดการและการจัดการภูมิคุ้มกันดิจิทัล

5.2.1.6.3 ปัญหาและข้อจำกัดด้านการบูรณาการ

จากการวิเคราะห์สภาพปัจจุบัน พบว่าข้อจำกัดด้านการบูรณาการที่สำคัญ ได้แก่ ความหลากหลายของระบบสารสนเทศและเทคโนโลยี การใช้รูปแบบข้อมูลที่แตกต่างกัน การมีฐานข้อมูลหลายแหล่ง และการเชื่อมต่อระบบที่อาจขึ้นอยู่กับการพัฒนาเฉพาะระบบ ส่งผลให้การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานและระบบมีความซับซ้อน นอกจากนี้ เมื่อมีการเพิ่มระบบใหม่หรือปรับปรุงระบบเดิม อาจจำเป็นต้องปรับปรุงจุดเชื่อมต่อที่เกี่ยวข้องหลายส่วน ทำให้เกิดภาระในการบำรุงรักษาและเพิ่มความเสี่ยงต่อความไม่สอดคล้องของข้อมูล ในด้าน AI ปัญหาดังกล่าวมีความสำคัญมากขึ้น เนื่องจากประสิทธิภาพของ AI ขึ้นอยู่กับความสามารถในการเข้าถึงข้อมูลที่มีคุณภาพและข้อมูลจากหลายแหล่ง หากข้อมูลไม่สามารถเชื่อมโยงกันได้อย่างเหมาะสม จะส่งผลต่อความสามารถในการวิเคราะห์และคาดการณ์ของ AI ดังนั้น ปัญหาของ Integration Architecture ไม่ได้จำกัดเฉพาะการเชื่อมโยงระบบเท่านั้น แต่รวมถึงการขาดกลไกกลางในการจัดการการไหลของข้อมูล บริการ และเหตุการณ์ระหว่าง Business, Application, Data, Security และปัญญาประดิษฐ์

5.2.1.6.4 การวิเคราะห์ช่องว่างด้านการบูรณาการ (Integration Gap)

จากการเปรียบเทียบสภาพปัจจุบันกับความต้องการของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ผู้วิจัยได้สังเคราะห์ช่องว่างด้านการบูรณาการ ดังตารางที่ 5-11

ตารางที่ 5-11 การวิเคราะห์ช่องว่างด้านการบูรณาการ (Integration Gap)

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
การเชื่อมโยงระบบ	ระบบสารสนเทศมีการเชื่อมโยงระหว่างกันตามความต้องการของแต่ละระบบ	การเชื่อมโยงยังไม่เป็นสถาปัตยกรรมกลางระดับองค์กร	Enterprise Integration Architecture
การเชื่อมโยงข้อมูล	มีการแลกเปลี่ยนข้อมูลระหว่างฐานข้อมูลและระบบงาน	รูปแบบข้อมูลและมาตรฐานการแลกเปลี่ยนข้อมูลมีความหลากหลาย	Enterprise Data Integration
API	บางระบบมี API สำหรับให้บริการข้อมูลหรือบริการระบบ	การบริหาร API ยังไม่เป็นมาตรฐานเดียวกันทั้งองค์กร	API Gateway & API Management
การเชื่อมต่อระหว่างแอปพลิเคชัน	มีการเชื่อมต่อระหว่าง Application ตามภารกิจ	การเพิ่มหรือเปลี่ยนระบบอาจทำให้การเชื่อมต่อมีความซับซ้อน	Application Integration Platform
การบูรณาการแบบเหตุการณ์	การแลกเปลี่ยนข้อมูลเน้นการร้องขอหรือส่งข้อมูลระหว่างระบบ	ขาดความสามารถในการรับส่งเหตุการณ์แบบต่อเนื่องหรือใกล้เคียงเวลาจริง	Event-Driven Architecture
การบูรณาการด้านความมั่นคงปลอดภัย	Security Event มาจากหลายระบบ	ข้อมูล Security Event ยังต้องบูรณาการเพื่อวิเคราะห์ในภาพรวม	Security Integration Layer
การบูรณาการ AI	AI ทำงานในระบบหรือโครงการเฉพาะด้าน	ขาดช่องทางมาตรฐานในการเชื่อม AI กับระบบองค์กร	Enterprise AI Integration Layer
การแลกเปลี่ยนข้อมูลแบบเวลาจริง	มีการแลกเปลี่ยนข้อมูลตามกระบวนการของระบบ	ความสามารถในการส่งข้อมูลและเหตุการณ์แบบ Real-time ยังมีข้อจำกัด	Real-Time Data/Event Integration
การบริหารการเชื่อมต่อ	ดูแลการเชื่อมต่อแยกตามระบบ	ขาดการบริหารและติดตาม Integration แบบรวมศูนย์	Integration Management & Monitoring
การสนับสนุนภูมิคุ้มกันดิจิทัล	ระบบ Security และระบบงานทำงานเป็นส่วน ๆ	ข้อมูลเหตุการณ์ไม่สามารถไหลเข้าสู่ AI และระบบตอบสนองได้อย่างต่อเนื่อง	Intelligent Digital Immunity Integration

5.2.1.6.5 ความต้องการด้านการบูรณาการ (Integration Requirements)

จากการวิเคราะห์ช่องว่าง ผู้วิจัยสังเคราะห์ความต้องการด้านการบูรณาการเพื่อรองรับสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ดังนี้

1. ต้องมีแพลตฟอร์มกลางสำหรับเชื่อมโยงระบบสารสนเทศและบริการต่าง ๆ ของสถาบัน เพื่อให้การเพิ่มระบบใหม่หรือปรับปรุงระบบเดิมสามารถดำเนินการได้โดยไม่เพิ่มความซับซ้อนของสถาปัตยกรรมโดยรวม

2. ต้องกำหนดมาตรฐานกลางสำหรับการแลกเปลี่ยนข้อมูลและบริการ โดยใช้ API และกลไกการแลกเปลี่ยนข้อมูลที่มีมาตรฐานเดียวกัน

3. ต้องสามารถรองรับการบูรณาการข้อมูลแบบ Batch และ Real-time รวมถึงการรับส่ง Event จากระบบต่าง ๆ

4. ต้องสามารถเชื่อมโยง AI Platform เข้ากับระบบงานของสถาบัน เพื่อให้ AI สามารถรับข้อมูล วิเคราะห์ และส่งผลลัพธ์กลับไปสนับสนุนกระบวนการทางธุรกิจ

5. ต้องสามารถเชื่อมโยงข้อมูลด้านความมั่นคงปลอดภัย เช่น Log, Alert, Threat Intelligence และ Incident เข้ากับ AI เพื่อสนับสนุนการตรวจจับและคาดการณ์ภัยคุกคาม

5.2.1.6.6 การออกแบบด้านการบูรณาการใน Target Architecture

จากผลการวิเคราะห์ ผู้วิจัยกำหนด Integration Architecture ในสถาปัตยกรรมเป้าหมายให้เป็น Intelligent Enterprise Integration Architecture ซึ่งทำหน้าที่เป็นชั้นกลางสำหรับเชื่อมโยง Business Process, Application, Data, Technology, Security และ AI เข้าด้วยกัน องค์ประกอบสำคัญประกอบด้วย API Gateway, API Management, Integration Platform, Enterprise Service Bus (ESB) หรือ Message Broker, Event-Driven Architecture, Data Integration, AI Integration Layer และ Integration Monitoring

การออกแบบดังกล่าวทำให้ข้อมูลสามารถไหลจากแหล่งข้อมูลต่าง ๆ เข้าสู่ Enterprise Data Platform และ AI/ML Platform เพื่อดำเนินการวิเคราะห์ จากนั้นผลลัพธ์จาก AI สามารถส่งกลับไปยัง Application หรือกระบวนการทางธุรกิจที่เกี่ยวข้องได้ โดยมี Security และ Governance กำกับการแลกเปลี่ยนข้อมูลและบริการตลอดกระบวนการ ในบริบทของการจัดการภูมิคุ้มกันดิจิทัล Integration Architecture จะทำหน้าที่เชื่อมโยงข้อมูลจาก Network, Endpoint, Application, Identity, Cloud และ Security System เข้าสู่ระบบวิเคราะห์และ AI เพื่อให้สามารถตรวจจับ วิเคราะห์ และคาดการณ์เหตุการณ์ได้อย่างต่อเนื่อง และส่งผลการวิเคราะห์ไปยังระบบตอบสนองเหตุการณ์เพื่อดำเนินการตามกระบวนการที่กำหนด

ตารางที่ 5-12 สรุปผลการวิเคราะห์ด้านการบูรณาการ

ประเด็น	ผลการวิเคราะห์
Current Architecture	การเชื่อมโยงระบบและข้อมูลระหว่าง Application ตามภารกิจ
Business Relationship	เชื่อมโยงกระบวนการนักศึกษา การเรียนการสอน บุคลากร การเงิน วิจัย และ Security
Problem	ระบบและข้อมูลมีความหลากหลาย การเชื่อมต่อมีความซับซ้อน และขาดกลไกกลาง
Gap	ขาด Enterprise Integration และ AI Integration ที่เป็นมาตรฐานเดียวกัน
Requirement	Integrated, Standardized, Scalable และ Real-Time Integration
AI Technology	AI Integration, Event Analytics, Real-Time Analytics, Intelligent Automation
Target Architecture	API Gateway + Integration Platform + Event-Driven + AI Integration Layer
Digital Immunity Capability	Monitor ⟶ Detect ⟶ Analyze ⟶ Predict ⟶ Respond ⟶ Recover

จากผลการวิเคราะห์ด้านการบูรณาการ ผู้วิจัยพบว่า Integration Architecture เป็นองค์ประกอบสำคัญที่ทำให้สถาปัตยกรรมองค์กรสามารถทำงานในลักษณะองค์รวม โดยเชื่อมโยงกระบวนการทางธุรกิจ ระบบแอปพลิเคชัน ข้อมูล เทคโนโลยี และระบบความมั่นคงปลอดภัยเข้าด้วยกัน การพัฒนาสถาปัตยกรรมเป้าหมายจึงควรมุ่งสู่ Intelligent Enterprise Integration ที่สามารถรองรับการแลกเปลี่ยนข้อมูลและบริการทั้งแบบปกติและแบบใกล้เคียงเวลาจริง รวมถึงสามารถเชื่อมโยง AI เข้ากับระบบงานขององค์กร

สำหรับการจัดการภูมิคุ้มกันดิจิทัล Integration Architecture จะเป็นกลไกที่ทำให้ข้อมูลเหตุการณ์จากระบบต่าง ๆ สามารถเข้าสู่กระบวนการ Detect ⟶ Analyze ⟶ Predict ⟶ Respond ⟶ Recover ได้อย่างต่อเนื่อง ส่งผลให้ AI ไม่ได้ทำงานเป็นระบบแยกส่วน แต่เป็นส่วนหนึ่งของกระบวนการดำเนินงานและการบริหารความเสี่ยงดิจิทัลของสถาบันอุดมศึกษาอย่างเป็นระบบ

5.2.1.7 ด้านการกำกับดูแล (Governance)

ผลการวิเคราะห์สภาพปัจจุบันด้านการกำกับดูแล (Governance Architecture) ของสถาบันอุดมศึกษา พบว่า การกำกับดูแลเป็นองค์ประกอบสำคัญที่ทำหน้าที่กำหนดทิศทาง หลักเกณฑ์ นโยบาย มาตรฐาน บทบาทหน้าที่ และกลไกการตัดสินใจที่เกี่ยวข้องกับการบริหารจัดการเทคโนโลยีดิจิทัล ข้อมูล ปัญญาประดิษฐ์ และความมั่นคงปลอดภัยขององค์กร โดยมีเป้าหมายเพื่อให้การนำเทคโนโลยีมาใช้สอดคล้องกับยุทธศาสตร์ พันธกิจ กฎหมาย ระเบียบ และนโยบายที่เกี่ยวข้องของสถาบันอุดมศึกษา ในบริบทของงานวิจัยเรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา”การกำกับดูแลมีความสำคัญเพิ่มขึ้น เนื่องจากการนำ AI มาใช้ในระดับองค์กรไม่ได้เกี่ยวข้องเฉพาะด้านเทคโนโลยี แต่ครอบคลุมถึงการกำกับดูแลข้อมูล ความเป็นส่วนตัว ความมั่นคงปลอดภัย จริยธรรมในการใช้ AI ความรับผิดชอบของผู้เกี่ยวข้อง ความโปร่งใสของกระบวนการตัดสินใจ และการบริหารความเสี่ยงจากการใช้ AI ดังนั้น Governance Architecture จึงต้องทำหน้าที่เป็นกลไกกำกับองค์ประกอบทั้ง 7 มิติ ได้แก่ Business, Data, Application, Technology, Security, Integration และ Governance ให้มีทิศทางและมาตรฐานที่สอดคล้องกัน และต้องสามารถเชื่อมโยงไปยังสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และความสามารถด้านการจัดการภูมิคุ้มกันดิจิทัลของสถาบันได้

5.2.1.7.1 สภาพปัจจุบันด้านการกำกับดูแล

จากการวิเคราะห์สภาพปัจจุบัน พบว่า การกำกับดูแลของสถาบันอุดมศึกษาครอบคลุมการกำหนดนโยบายและแนวทางการบริหารจัดการองค์กร การกำกับดูแลเทคโนโลยีสารสนเทศ การบริหารข้อมูล การรักษาความมั่นคงปลอดภัย และการบริหารความเสี่ยง โดยมีผู้บริหารและหน่วยงานที่เกี่ยวข้องทำหน้าที่กำหนดนโยบายและควบคุมการดำเนินงานให้เป็นไปตามกรอบและข้อกำหนดขององค์กร เมื่อพิจารณาในบริบทของการนำปัญญาประดิษฐ์มาใช้ พบว่า Governance จำเป็นต้องขยายขอบเขตจากการกำกับดูแลระบบสารสนเทศทั่วไปไปสู่ AI Governance ซึ่งต้องครอบคลุมวงจรชีวิตของ AI ตั้งแต่การกำหนดวัตถุประสงค์ การจัดเตรียมข้อมูล การพัฒนาและฝึกโมเดล การนำ AI ไปใช้งาน การติดตามประสิทธิภาพ ตลอดจนการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้น นอกจากนี้ การจัดการภูมิคุ้มกันดิจิทัลจำเป็นต้องมีการกำหนดผู้รับผิดชอบและกระบวนการตัดสินใจที่ชัดเจนในกรณีเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์ผิดปกติ โดยเฉพาะกรณีที่ AI ถูกนำมาใช้เพื่อแจ้งเตือน วิเคราะห์ หรือเสนอแนวทางตอบสนองต่อเหตุการณ์ ดังนั้นจำเป็นต้องกำหนดขอบเขตความรับผิดชอบระหว่าง AI กับผู้ปฏิบัติงาน (Human Oversight) อย่างชัดเจน

5.2.1.7.2 ความสัมพันธ์ระหว่างการกำกับดูแลกับกระบวนการธุรกิจ

การกำกับดูแลมีความสัมพันธ์กับกระบวนการธุรกิจในทุกระดับของสถาบัน เนื่องจากเป็นกลไกที่กำหนดว่าแต่ละกระบวนการต้องดำเนินการภายใต้นโยบาย มาตรฐาน สิทธิ์ และความรับผิดชอบอย่างไร ดังตารางที่ 5-13

ตารางที่ 5-13 ความสัมพันธ์ระหว่างการกำกับดูแลกับกระบวนการธุรกิจ

กระบวนการธุรกิจ	ประเด็นที่ต้องกำกับดูแล	ข้อมูล/ทรัพยากรที่เกี่ยวข้อง	กลไกการกำกับดูแลที่ต้องการ
การบริหารองค์กร	ยุทธศาสตร์ นโยบาย และการตัดสินใจ	แผนยุทธศาสตร์ KPI รายงานผล	Strategic Governance
การจัดการเรียนการสอน	การใช้ระบบดิจิทัลและ AI เพื่อการเรียนรู้	ข้อมูลนักศึกษา ผลการเรียน	Digital & AI Governance
การบริหารนักศึกษา	การใช้และคุ้มครองข้อมูลส่วนบุคคล	Student Data	Data Governance & Privacy
การบริหารบุคลากร	สิทธิ์การเข้าถึงและการใช้ข้อมูลบุคลากร	Personnel Data	Data Governance & Access Control
การวิจัย	การใช้ข้อมูลและ AI ในงานวิจัย	Research Data	Research Data Governance
การบริหารการเงิน	ความถูกต้องและตรวจสอบได้ของธุรกรรม	Financial Data	IT Governance & Audit
การบริหารเทคโนโลยี	มาตรฐานและการใช้ทรัพยากร IT	Infrastructure, Application	IT Governance
ความมั่นคงปลอดภัย	การบริหารความเสี่ยงและเหตุการณ์	Security Event, Incident	Security Governance
การใช้ AI	ความโปร่งใส ความรับผิดชอบและความเสี่ยง	AI Model, Training Data	AI Governance
การจัดการภูมิคุ้มกันดิจิทัล	การกำหนดบทบาทและกระบวนการตอบสนอง	Risk, Threat, Incident	Digital Immunity Governance

จากตารางจะเห็นได้ว่า Governance Architecture เป็นกลไกที่กำกับกระบวนการธุรกิจตั้งแต่ระดับยุทธศาสตร์จนถึงระดับปฏิบัติการ และมีบทบาทสำคัญในการกำหนดมาตรฐานและความรับผิดชอบในการใช้ข้อมูล เทคโนโลยี และ AI

5.2.1.7.3 ปัญหาและข้อจำกัดด้านการกำกับดูแล

จากการวิเคราะห์สภาพปัจจุบัน สามารถสรุปปัญหาและข้อจำกัดด้าน Governance ที่มีความสำคัญต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ได้ดังนี้

1. การกำกับดูแลมีลักษณะกระจายตามหน่วยงาน ทำให้การกำหนดนโยบายและมาตรฐานด้านข้อมูล เทคโนโลยี และ AI อาจมีความแตกต่างกันระหว่างหน่วยงาน

2. การกำกับดูแลข้อมูลยังต้องได้รับการบูรณาการในระดับองค์กร เนื่องจากข้อมูลเดียวกันอาจถูกจัดเก็บและใช้งานในหลายระบบและหลายหน่วยงาน จึงจำเป็นต้องกำหนดเจ้าของข้อมูล ผู้รับผิดชอบข้อมูล สิทธิ์การเข้าถึง และมาตรฐานคุณภาพข้อมูลอย่างชัดเจน

3. การกำกับดูแล AI มีความซับซ้อนกว่าการกำกับดูแลระบบสารสนเทศทั่วไป เนื่องจากต้องพิจารณาความถูกต้อง ความน่าเชื่อถือ ความโปร่งใส ความเสี่ยงของโมเดล และความรับผิดชอบในการนำผลลัพธ์จาก AI ไปใช้

4. การบริหารความเสี่ยงยังจำเป็นต้องเชื่อมโยงกับข้อมูลและเทคโนโลยีแบบต่อเนื่อง โดยเฉพาะความเสี่ยงด้านไซเบอร์และความเสี่ยงจาก AI ซึ่งมีการเปลี่ยนแปลงตามสภาพแวดล้อมดิจิทัล

5. ยังจำเป็นต้องมีกลไกติดตามและประเมินผลที่ชัดเจน เพื่อให้สามารถตรวจสอบได้ว่านโยบาย มาตรฐาน และมาตรการด้าน AI และความมั่นคงปลอดภัยถูกนำไปปฏิบัติอย่างมีประสิทธิผลหรือไม่

5.2.1.7.4 การวิเคราะห์ช่องว่างด้านการกำกับดูแล (Governance Gap)

จากการเปรียบเทียบสภาพปัจจุบันกับความต้องการของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ผู้วิจัยได้สังเคราะห์ช่องว่างด้านการกำกับดูแล ดังตารางที่ 5-14

ตารางที่ 5-14 การวิเคราะห์ช่องว่างด้านการกำกับดูแล (Governance Gap)

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
การกำกับดูแลระดับองค์กร	มีนโยบายและแนวทางการบริหารตามโครงสร้างองค์กร	การกำกับดูแล AI และ Digital Immunity ยังต้องเชื่อมโยงเป็นภาพรวม	Enterprise Governance Framework
การกำกับดูแลเทคโนโลยี	มีการกำกับดูแลระบบและทรัพยากร IT	ยังต้องเชื่อมโยง Technology Governance กับ AI และความเสี่ยงดิจิทัล	Integrated IT & AI Governance
การกำกับดูแลข้อมูล	มีการจัดการข้อมูลตามระบบและหน่วยงาน	ขาดกลไก Data Governance ที่เป็นมาตรฐานเดียวกันทั้งองค์กร	Enterprise Data Governance

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
เจ้าของข้อมูล	หน่วยงานเป็นผู้รับผิดชอบข้อมูลของตน	บทบาท Data Owner และ Data Steward อาจไม่ชัดเจนในระดับองค์กร	Data Ownership & Stewardship Model
การกำกับดูแล AI	การใช้ AI เกิดขึ้นตามโครงการหรือระบบ	ขาดกรอบกำกับดูแล AI ตลอดวงจรชีวิต	AI Governance Framework
จริยธรรมและความรับผิดชอบ AI	การพิจารณาด้านจริยธรรมอาจอยู่ในแต่ละโครงการ	ขาดหลักเกณฑ์กลางสำหรับ Responsible AI	Responsible AI Governance
การบริหารความเสี่ยง	มีการบริหารความเสี่ยงในระดับองค์กร	ความเสี่ยงจาก AI และ Cyber Threat ยังต้องบูรณาการ	AI & Digital Risk Governance
ความเป็นส่วนตัวและข้อมูลส่วนบุคคล	มีมาตรการคุ้มครองข้อมูลตามข้อกำหนดที่เกี่ยวข้อง	ต้องบูรณาการ Privacy เข้ากับ Data และ AI Lifecycle	Privacy-by-Design Governance
การตรวจสอบและประเมินผล	มีการติดตามและตรวจสอบตามระบบงาน	ขาด Dashboard และตัวชี้วัดสำหรับ AI/Digital Immunity แบบองค์รวม	Governance Monitoring & Audit
การกำกับดูแลเหตุการณ์	มีขั้นตอนตอบสนองเหตุการณ์ด้าน IT/Security	การเชื่อมโยง AI กับการตัดสินใจและการตอบสนองยังไม่เป็นระบบ	AI-Assisted Incident Governance
การกำกับดูแลภูมิคุ้มกันดิจิทัล	เน้นการบริหารความเสี่ยงและความมั่นคงปลอดภัย	ขาด Governance ที่เชื่อม Detect–Predict–Respond–Recover	Digital Immunity Governance

5.2.1.7.5 ความต้องการด้านการกำกับดูแล (Governance Requirements)

จากการวิเคราะห์ช่องว่าง ผู้วิจัยสังเคราะห์ความต้องการด้าน Governance สำหรับสถาปัตยกรรมเป้าหมาย โดยประกอบด้วยองค์ประกอบสำคัญดังนี้

1. Enterprise Governance กำหนดโครงสร้าง บทบาท อำนาจหน้าที่ และความรับผิดชอบในการกำกับดูแลสถาปัตยกรรมองค์กรในระดับสถาบัน
2. Data Governance กำหนดเจ้าของข้อมูล ผู้รับผิดชอบข้อมูล มาตรฐานข้อมูล คุณภาพข้อมูล การเข้าถึงข้อมูล และการใช้ข้อมูลอย่างเหมาะสม
3. AI Governance กำหนดหลักเกณฑ์สำหรับการจัดหา พัฒนา ใช้งาน ติดตาม และยกเลิกการใช้งาน AI ตลอดวงจรชีวิตของระบบ

4. Responsible AI กำหนดหลักการด้านความโปร่งใส ความรับผิดชอบ ความเป็นธรรม ความน่าเชื่อถือ และการมีมนุษย์กำกับดูแลในกระบวนการที่มีความสำคัญ
5. Digital Risk Governance บูรณาการการบริหารความเสี่ยงด้าน AI ไซเบอร์ ข้อมูล และเทคโนโลยีเข้ากับการบริหารความเสี่ยงระดับองค์กร
6. Security Governance กำหนดนโยบาย มาตรฐาน และกระบวนการในการรักษาความมั่นคงปลอดภัยของระบบ ข้อมูล และโครงสร้างพื้นฐาน
7. Governance Monitoring and Audit กำหนดตัวชี้วัด กลไกติดตาม การประเมิน และการตรวจสอบ เพื่อให้สามารถประเมินประสิทธิผลของการกำกับดูแลได้อย่างต่อเนื่อง

5.2.1.7.6 การออกแบบด้านการกำกับดูแลใน Target Architecture

จากผลการวิเคราะห์ ผู้วิจัยกำหนด Governance Architecture ในสถาปัตยกรรมเป้าหมายให้เป็น Integrated AI and Digital Immunity Governance Architecture ซึ่งทำหน้าที่กำกับดูแลการดำเนินงานของสถาปัตยกรรมทั้ง 7 มิติ และสร้างความเชื่อมโยงระหว่างยุทธศาสตร์ของสถาบันกับการใช้ AI และการจัดการภูมิคุ้มกันดิจิทัล

โครงสร้าง Governance Architecture ประกอบด้วย 5 กลไกหลัก ได้แก่

1. Strategic Governance ทำหน้าที่กำหนดทิศทาง ยุทธศาสตร์ นโยบาย และเป้าหมายด้าน AI ดิจิทัล และภูมิคุ้มกันดิจิทัลให้สอดคล้องกับพันธกิจของสถาบัน

2. Data and AI Governance ทำหน้าที่กำกับดูแลข้อมูลและ AI ตั้งแต่การจัดหา การใช้ การประมวลผล การพัฒนาโมเดล ไปจนถึงการติดตามผล

3. Security and Risk Governance ทำหน้าที่กำกับความเสี่ยงด้านไซเบอร์ เทคโนโลยี ข้อมูล และ AI รวมถึงกำหนดแนวทางตอบสนองต่อเหตุการณ์

4. Architecture Governance ทำหน้าที่กำกับให้การพัฒนา Business, Data, Application, Technology, Security และ Integration เป็นไปตามมาตรฐานและหลักการสถาปัตยกรรมองค์กรที่กำหนด

5. Monitoring, Compliance and Audit ทำหน้าที่ติดตาม ประเมิน ตรวจสอบ และรายงานผลการดำเนินงาน รวมถึงนำผลการประเมินกลับมาปรับปรุงนโยบายและสถาปัตยกรรมอย่างต่อเนื่อง

ตารางที่ 5-15 สรุปผลการวิเคราะห์ด้านการกำกับดูแล

ประเด็น	ผลการวิเคราะห์
Current Architecture	นโยบาย การกำกับดูแล IT ข้อมูล ความมั่นคงปลอดภัย และการบริหารความเสี่ยง

ประเด็น	ผลการวิเคราะห์
Business Relationship	กำกับกระบวนการบริหาร การเรียนการสอน นักศึกษา บุคลากร วิจัย การเงิน และบริการดิจิทัล
Problem	การกำกับดูแล AI ข้อมูล และ Digital Immunity ยังต้องบูรณาการในระดับองค์กร
Gap	ขาด Integrated AI, Data, Security และ Digital Immunity Governance
Requirement	Integrated, Responsible, Risk-based และ Continuous Governance
AI Technology	AI Governance Platform, AI Monitoring, Risk Analytics, Governance Dashboard
Target Architecture	Integrated AI & Digital Immunity Governance Architecture
Digital Immunity Capability	Govern ⟶ Monitor ⟶ Assess ⟶ Improve ⟶ Adapt

จากผลการวิเคราะห์ด้านการกำกับดูแล พบว่า Governance Architecture เป็นองค์ประกอบที่ทำหน้าที่กำกับและควบคุมองค์ประกอบทั้ง 7 มิติของโครงสร้างองค์กร ให้ดำเนินงานไปในทิศทางเดียวกัน และเป็นกลไกสำคัญในการเชื่อมโยงยุทธศาสตร์ของสถาบันเข้ากับการใช้ข้อมูล เทคโนโลยี AI และการจัดการความมั่นคงปลอดภัย ดังนั้น สถาปัตยกรรมเป้าหมายด้าน Governance จึงควรมุ่งสู่ Integrated AI and Digital Immunity Governance ที่ครอบคลุมการกำกับดูแลระดับองค์กร การกำกับดูแลข้อมูล การกำกับดูแล AI การบริหารความเสี่ยง ความมั่นคงปลอดภัย ความเป็นส่วนตัว จริยธรรม และการตรวจสอบประสิทธิผลของระบบ โดยมีการติดตามและปรับปรุงอย่างต่อเนื่อง

5.2.2 ด้านเทคโนโลยีอัจฉริยะ (Intelligent Technology)

จากการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา พบว่าเทคโนโลยีอัจฉริยะ (Intelligent Technology) เป็นองค์ประกอบสำคัญในการเพิ่มขีดความสามารถของสถาบันอุดมศึกษาในการจัดการข้อมูล วิเคราะห์รูปแบบการดำเนินงาน ตรวจจับความผิดปกติ และสนับสนุนการตัดสินใจเชิงรุก โดยเฉพาะในบริบทที่สถาบันมีข้อมูลจากระบบสารสนเทศจำนวนมากและมีความหลากหลายทั้งในด้านประเภท แหล่งที่มา และลักษณะการใช้งาน

5.2.2.1 การเรียนรู้ของเครื่อง (Machine Learning)

การเรียนรู้ของเครื่องเป็นเทคโนโลยีที่ทำให้ระบบคอมพิวเตอร์สามารถเรียนรู้รูปแบบและความสัมพันธ์จากข้อมูลโดยไม่จำเป็นต้องกำหนดกฎการทำงานทุกขั้นตอนโดยมนุษย์ โดยระบบสามารถนำข้อมูลในอดีตมาใช้สร้างแบบจำลองสำหรับการจำแนกประเภท การพยากรณ์ และการ

ตรวจจับรูปแบบที่ผิดปกติ ในบริบทของสถาบันอุดมศึกษา Machine Learning สามารถประยุกต์ใช้กับข้อมูลจากกระบวนการทางธุรกิจ เช่น ข้อมูลนักศึกษา ผลการเรียน การลงทะเบียน การใช้บริการระบบสารสนเทศ ข้อมูลบุคลากร รวมถึงข้อมูลจากระบบเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัย เพื่อค้นหารูปแบบและแนวโน้มที่อาจไม่สามารถสังเกตได้จากการวิเคราะห์ข้อมูลแบบทั่วไป สำหรับการจัดการภูมิคุ้มกันดิจิทัล Machine Learning สามารถนำมาใช้ในการวิเคราะห์ข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัย การจำแนกเหตุการณ์ที่มีความเสี่ยง การตรวจจับความผิดปกติ และการประเมินแนวโน้มของภัยคุกคาม โดยผลลัพธ์ที่ได้สามารถนำไปใช้ประกอบการตัดสินใจและกำหนดแนวทางตอบสนองต่อเหตุการณ์ได้อย่างเหมาะสม

5.2.2.2 การเรียนรู้เชิงลึก (Deep Learning)

การเรียนรู้เชิงลึกเป็นแขนงหนึ่งของ Machine Learning ที่ใช้โครงข่ายประสาทเทียมหลายชั้นในการเรียนรู้ลักษณะและรูปแบบที่มีความซับซ้อนจากข้อมูลจำนวนมาก โดยเฉพาะข้อมูลที่มีความสัมพันธ์หลายระดับหรือไม่สามารถกำหนดคุณลักษณะของข้อมูลได้โดยง่าย สำหรับสถาบันอุดมศึกษา Deep Learning สามารถนำมาใช้กับข้อมูลที่มีความซับซ้อน ได้แก่ ข้อมูลข้อความ รูปภาพ เสียง หรือข้อมูลเหตุการณ์จำนวนมากจากระบบดิจิทัล เพื่อสนับสนุนการวิเคราะห์และการจำแนกเหตุการณ์ที่มีรูปแบบซับซ้อน ในบริบทของการจัดการภูมิคุ้มกันดิจิทัล Deep Learning สามารถนำมาใช้ในการวิเคราะห์รูปแบบการใช้งานระบบ การตรวจจับพฤติกรรมที่แตกต่างจากรูปแบบปกติ การจำแนกเหตุการณ์ด้านความมั่นคงปลอดภัย และการวิเคราะห์รูปแบบของภัยคุกคามที่มีความซับซ้อน ซึ่งช่วยเพิ่มความสามารถในการตรวจจับภัยคุกคามที่อาจไม่สามารถระบุได้ด้วยกฎหรือเงื่อนไขแบบเดิม

5.2.2.3 การประมวลผลภาษาธรรมชาติ (Natural Language Processing: NLP)

การประมวลผลภาษาธรรมชาติเป็นเทคโนโลยีปัญญาประดิษฐ์ที่ช่วยให้คอมพิวเตอร์สามารถประมวลผล วิเคราะห์ และทำความเข้าใจภาษามนุษย์ในรูปแบบข้อความหรือภาษาเสียงได้ เทคโนโลยีดังกล่าวมีความสำคัญต่อสถาบันอุดมศึกษา เนื่องจากองค์กรมีข้อมูลที่อยู่ในรูปแบบข้อความจำนวนมาก เช่น หนังสือราชการ รายงานการประชุม เอกสารวิชาการ ข้อร้องเรียน คำถามจากนักศึกษา และข้อมูลจากช่องทางบริการดิจิทัล ในบริบทของการจัดการภูมิคุ้มกันดิจิทัล NLP สามารถนำมาใช้ในการวิเคราะห์ข้อความจากรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย การจัดหมวดหมู่เหตุการณ์ การค้นหาคำหรือรูปแบบที่มีความเสี่ยง ตลอดจนการสกัดสารสนเทศจากเอกสารที่เกี่ยวข้องกับภัยคุกคามและเหตุการณ์ผิดปกติ นอกจากนี้ NLP ยังสามารถสนับสนุนการให้บริการอัจฉริยะ เช่น ระบบผู้ช่วยเสมือนและระบบตอบคำถามอัตโนมัติ โดยสามารถประมวลผลคำถามของผู้ใช้งานและเชื่อมโยงกับฐานความรู้ของสถาบัน

5.2.2.4 ความรู้เชิงพฤติกรรม (Behavioral AI)

ความรู้เชิงพฤติกรรม หรือ Behavioral AI เป็นแนวทางการประยุกต์ใช้ปัญญาประดิษฐ์เพื่อเรียนรู้และวิเคราะห์รูปแบบพฤติกรรมของผู้ใช้งาน ระบบ หรือองค์ประกอบต่าง ๆ จากข้อมูลที่เกิดขึ้นในระหว่างการดำเนินงาน โดยมุ่งเน้นการสร้าง Baseline ของพฤติกรรมปกติ (Normal Behavioral Baseline) และตรวจจับพฤติกรรมที่มีความแตกต่างหรือมีแนวโน้มผิดปกติ ในบริบทของสถาบันอุดมศึกษา Behavioral AI สามารถนำมาใช้วิเคราะห์พฤติกรรมการใช้งานระบบของนักศึกษา บุคลากร ผู้ดูแลระบบ และผู้ใช้งานประเภทต่าง ๆ เช่น รูปแบบการเข้าสู่ระบบ ช่วงเวลาการใช้งานระบบที่เข้าถึง ตำแหน่งหรือบริบทของการเข้าถึง และรูปแบบการใช้ทรัพยากรสารสนเทศ ทั้งนี้ การนำข้อมูลพฤติกรรมมาใช้ต้องอยู่ภายใต้หลักการกำกับดูแลข้อมูล ความเป็นส่วนตัว และสิทธิ์ในการเข้าถึงข้อมูลที่เหมาะสม สำหรับการจัดการภูมิคุ้มกันดิจิทัล Behavioral AI มีบทบาทสำคัญในการตรวจจับพฤติกรรมที่อาจเป็นสัญญาณของความเสี่ยง เช่น รูปแบบการเข้าสู่ระบบที่ผิดไปจากพฤติกรรมเดิม การเข้าถึงทรัพยากรสารสนเทศผิดปกติ หรือรูปแบบการใช้งานระบบที่แตกต่างจากพฤติกรรมปกติ โดยผลการวิเคราะห์สามารถนำไปประกอบการประเมินความเสี่ยงและการตอบสนองต่อเหตุการณ์ได้

5.2.2.5 ความสัมพันธ์ระหว่างเทคโนโลยีอัจฉริยะกับกระบวนการธุรกิจ

เพื่อให้สอดคล้องกับรูปแบบการวิเคราะห์ใน 7 มิติของโครงสร้างองค์กร ผู้วิจัยสามารถนำเทคโนโลยีอัจฉริยะทั้ง 4 องค์ประกอบมาเชื่อมโยงกับกระบวนการธุรกิจได้ดังตารางที่ 5-16

ตารางที่ 5-16 ความสัมพันธ์ระหว่างเทคโนโลยีอัจฉริยะกับกระบวนการธุรกิจ

กระบวนการธุรกิจ	Machine Learning	Deep Learning	NLP	Behavioral AI
การบริหารองค์กร	วิเคราะห์และพยากรณ์ข้อมูล	วิเคราะห์ข้อมูลซับซ้อน	วิเคราะห์เอกสารและรายงาน	วิเคราะห์พฤติกรรมการใช้ระบบ
การจัดการนักศึกษา	วิเคราะห์ความเสี่ยง	วิเคราะห์รูปแบบข้อมูลจำนวนมาก	วิเคราะห์ข้อคำถาม/ข้อร้องเรียน	วิเคราะห์รูปแบบการใช้บริการ
การเรียนการสอน	พยากรณ์ผลการเรียน	วิเคราะห์รูปแบบการเรียนรู้	วิเคราะห์เนื้อหา	วิเคราะห์พฤติกรรมการเรียน
การบริหารบุคลากร	Workforce Analytics	วิเคราะห์ข้อมูลหลายมิติ	วิเคราะห์เอกสาร	วิเคราะห์รูปแบบการใช้ระบบ
การวิจัย	วิเคราะห์ข้อมูลวิจัย	วิเคราะห์ข้อมูลซับซ้อน	วิเคราะห์บทความและเอกสาร	วิเคราะห์รูปแบบการใช้ทรัพยากร

กระบวนการธุรกิจ	Machine Learning	Deep Learning	NLP	Behavioral AI
ความมั่นคงปลอดภัย	จำแนกและตรวจจับเหตุการณ์	ตรวจจับรูปแบบภัยคุกคาม	วิเคราะห์รายงานเหตุการณ์	ตรวจจับพฤติกรรมผิดปกติ
การจัดการภูมิคุ้มกันดิจิทัล	ประเมินความเสี่ยง	วิเคราะห์ภัยคุกคามซับซ้อน	วิเคราะห์ข้อมูลเหตุการณ์	วิเคราะห์พฤติกรรมและตรวจจับความผิดปกติ

5.2.2.6 การวิเคราะห์ช่องว่างด้านเทคโนโลยีอัจฉริยะ

ตารางที่ 5-17 การวิเคราะห์ช่องว่างด้านเทคโนโลยีอัจฉริยะ (Intelligent Technology Gap)

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
Machine Learning	มีการนำ ML มาใช้กับงานหรือข้อมูลบางประเภท	ขาดแพลตฟอร์ม ML ที่สามารถใช้งานร่วมกันในระดับองค์กร	Enterprise Machine Learning Platform
Deep Learning	มีการประยุกต์ใช้กับงานที่มีข้อมูลซับซ้อนเป็นบางกรณี	ยังขาดความสามารถในการวิเคราะห์ข้อมูลขนาดใหญ่และรูปแบบซับซ้อนอย่างเป็นระบบ	Deep Learning Intelligence Layer
NLP	มีข้อมูลข้อความจำนวนมาก แต่การวิเคราะห์ยังดำเนินการด้วยวิธีทั่วไปหรือแยกตามระบบ	ขาดระบบกลางสำหรับวิเคราะห์และสกัดองค์ความรู้จากข้อมูลข้อความ	Enterprise NLP Platform
Behavioral AI	มีการจัดเก็บ Log และข้อมูลกิจกรรมของผู้ใช้งาน	ขาดความสามารถในการสร้าง Behavioral Baseline และตรวจจับพฤติกรรมผิดปกติ	Behavioral Intelligence Layer
การบูรณาการ AI	AI ทำงานแยกตามระบบหรือโครงการ	ขาดการเชื่อมโยง AI กับข้อมูล Application และ Security ในระดับองค์กร	Enterprise AI Integration
การสนับสนุนภูมิคุ้มกันดิจิทัล	มีระบบรักษาความมั่นคงปลอดภัยและข้อมูลเหตุการณ์	ขาด AI ที่สามารถวิเคราะห์ข้อมูลแบบองค์รวมเพื่อคาดการณ์ความเสี่ยง	AI-Driven Digital Immunity Platform

5.2.2.7 ความต้องการด้านเทคโนโลยีอัจฉริยะ

จากการวิเคราะห์ช่องว่าง ผู้วิจัยกำหนดความต้องการด้านเทคโนโลยีอัจฉริยะ ดังนี้

1. ต้องมีความสามารถในการเรียนรู้จากข้อมูล เพื่อให้ระบบสามารถค้นหารูปแบบและความสัมพันธ์ของข้อมูลได้อย่างต่อเนื่อง

2. ต้องรองรับการวิเคราะห์ข้อมูลที่มีความซับซ้อน โดยเฉพาะข้อมูลขนาดใหญ่ ข้อมูลแบบลำดับเวลา ข้อมูลพฤติกรรม และข้อมูลจากระบบความมั่นคงปลอดภัย

3. ต้องสามารถวิเคราะห์ข้อมูลภาษาและเอกสาร เพื่อเปลี่ยนข้อมูลที่ไม่มีโครงสร้างให้เป็นสารสนเทศที่สามารถนำไปใช้ในการตัดสินใจได้

4. ต้องสามารถสร้างแบบจำลองพฤติกรรมปกติ และตรวจจับความเบี่ยงเบนจากรูปแบบดังกล่าว เพื่อสนับสนุนการตรวจจับเหตุการณ์ผิดปกติ

5. ต้องสามารถเชื่อมโยงเทคโนโลยีอัจฉริยะกับระบบภูมิคุ้มกันดิจิทัล เพื่อให้ข้อมูลจากระบบต่าง ๆ สามารถนำมาวิเคราะห์และสร้างความสามารถในการตรวจจับ คาดการณ์ และตอบสนองต่อความเสี่ยง

5.2.2.8 การออกแบบเทคโนโลยีอัจฉริยะในสถาปัตยกรรมเป้าหมาย

จากผลการวิเคราะห์ กำหนดให้ Intelligent Technology Architecture เป็นชั้นความสามารถอัจฉริยะของสถาปัตยกรรมองค์กร โดยประกอบด้วย 4 องค์ประกอบหลัก ได้แก่ Machine Learning, Deep Learning, Natural Language Processing และ Behavioral AI ทั้ง 4 องค์ประกอบจะทำงานร่วมกับ Data Architecture เพื่อรับข้อมูลจากแหล่งข้อมูลของสถาบัน และเชื่อมโยงผ่าน Integration Architecture ไปยังระบบแอปพลิเคชันและระบบความมั่นคงปลอดภัย โดยมี Governance Architecture ทำหน้าที่กำกับการใช้ข้อมูลและเทคโนโลยี AI ให้เป็นไปตามนโยบาย มาตรฐาน และหลักเกณฑ์ที่กำหนด

โดย Machine Learning ทำหน้าที่เรียนรู้รูปแบบจากข้อมูล Deep Learning สนับสนุนการวิเคราะห์รูปแบบที่มีความซับซ้อน NLP วิเคราะห์ข้อมูลภาษาและเอกสาร และ Behavioral AI วิเคราะห์รูปแบบพฤติกรรมเพื่อค้นหาความผิดปกติ ผลลัพธ์จากกระบวนการดังกล่าวสามารถนำไปใช้สนับสนุนการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษาได้อย่างเป็นระบบ

ตารางที่ 5-18 สรุปสำหรับเชื่อมไปสู่ Target Architecture

ประเด็น	Current Architecture	Gap	Target Architecture	Digital Immunity Capability
Machine Learning	วิเคราะห์ข้อมูลเฉพาะระบบ	ขาด ML ระดับองค์กร	Enterprise ML	Predict & detect
Deep Learning	วิเคราะห์ข้อมูลซับซ้อนเฉพาะงาน	ขาด Deep Learning Intelligence	Deep Learning Layer	Advanced Detection
NLP	มีข้อมูลข้อความจำนวนมาก	ขาดการวิเคราะห์ข้อความแบบรวมศูนย์	Enterprise NLP	Analyze & Intelligence
Behavioral AI	มีข้อมูลกิจกรรมและ Log	ขาด Behavioral Baseline	Behavioral Intelligence	Detect & predict

ประเด็น	Current Architecture	Gap	Target Architecture	Digital Immunity Capability
AI Integration	AI แยกตามระบบ	ขาดการเชื่อมโยง AI ระดับองค์กร	Enterprise AI Integration	Respond
Digital Immunity	Security ทำงานเป็นส่วน ๆ	ขาด Intelligence Layer	AI-Driven Digital Immunity	Monitor ⟶ Detect ⟶ Analyze ⟶ Predict ⟶ Respond ⟶ Recover

5.2.3 ด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity)

จากการศึกษาสภาพปัจจุบันของสถาบันอุดมศึกษา พบว่า การเปลี่ยนแปลงของเทคโนโลยีดิจิทัลและการเพิ่มขึ้นของการให้บริการผ่านระบบสารสนเทศ ส่งผลให้สถาบันมีการพึ่งพาโครงสร้างพื้นฐานดิจิทัล ข้อมูล แอปพลิเคชัน ระบบเครือข่าย และบริการออนไลน์มากขึ้น ขณะเดียวกัน สถาบันต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ เหตุการณ์ผิดปกติ การรั่วไหลของข้อมูล การเข้าถึงระบบโดยไม่ได้รับอนุญาต และความขัดข้องของระบบสารสนเทศ ดังนั้น การจัดการภูมิคุ้มกันดิจิทัลจึงไม่ได้มุ่งเน้นเฉพาะการป้องกันภัยคุกคามเท่านั้น แต่ครอบคลุมความสามารถขององค์กรในการมองเห็น ตรวจจับ วิเคราะห์ ตอบสนอง ป้องกันเชิงรุก ฟื้นฟู และเรียนรู้จากเหตุการณ์ เพื่อให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่องและสามารถปรับตัวต่อภัยคุกคามที่เปลี่ยนแปลงได้

5.2.3.1 การมองเห็นและเฝ้าระวัง (Observability & Visibility)

การมองเห็นและเฝ้าระวังเป็นพื้นฐานของระบบภูมิคุ้มกันดิจิทัล เนื่องจากการบริหารความมั่นคงปลอดภัยของสถาบันจำเป็นต้องสามารถมองเห็นสถานะของระบบดิจิทัล ทรัพยากรสารสนเทศ ผู้ใช้งาน อุปกรณ์ เครือข่าย แอปพลิเคชัน และบริการต่าง ๆ ได้อย่างครอบคลุม ในบริบทของสถาบันอุดมศึกษา ข้อมูลที่ใช้ในการสร้างความสามารถด้าน Observability & Visibility อาจมาจากระบบเครือข่าย ระบบปฏิบัติการ ระบบฐานข้อมูล ระบบแอปพลิเคชัน ระบบยืนยันตัวตน อุปกรณ์ปลายทาง ระบบ Cloud และระบบความมั่นคงปลอดภัย โดยข้อมูลเหล่านี้สามารถนำมารวบรวมและวิเคราะห์เพื่อสร้างภาพรวมของสถานะระบบดิจิทัลขององค์กร การมีความสามารถด้านการมองเห็นที่ดีช่วยให้สถาบันสามารถทราบได้ว่า มีทรัพยากรดิจิทัลอะไร อยู่ที่ใด มีใครกำลังใช้งาน และเกิดเหตุการณ์อะไรขึ้นในระบบ ซึ่งเป็นข้อมูลพื้นฐานสำหรับการตรวจจับและวิเคราะห์ภัยคุกคามในขั้นตอนต่อไป

5.2.3.2 การตรวจจับภัยคุกคาม (Threat Detection)

การตรวจจับภัยคุกคามเป็นความสามารถในการระบุเหตุการณ์หรือพฤติกรรมที่อาจเป็นภัยต่อระบบสารสนเทศและข้อมูลของสถาบัน โดยอาศัยข้อมูลจากระบบเฝ้าระวังและข้อมูลเหตุการณ์ที่เกิดขึ้นในสภาพแวดล้อมดิจิทัล

การตรวจจับภัยคุกคามในสถาปัตยกรรมที่นำเสนอควรพัฒนาจากการตรวจจับตามกฎที่กำหนดไว้ล่วงหน้าไปสู่การตรวจจับโดยใช้ Artificial Intelligence และ Machine Learning เพื่อให้สามารถเรียนรู้รูปแบบพฤติกรรมปกติและระบุความผิดปกติที่มีความซับซ้อนได้ เช่น การตรวจจับการเข้าสู่ระบบที่มีรูปแบบผิดปกติ การเข้าถึงทรัพยากรสารสนเทศที่แตกต่างจากพฤติกรรมปกติ การเปลี่ยนแปลงรูปแบบ Network Traffic หรือการเกิดเหตุการณ์หลายรูปแบบที่มีความสัมพันธ์กัน

5.2.3.3 การสืบสวนและวิเคราะห์ (Investigation & Analysis)

การสืบสวนและวิเคราะห์เป็นกระบวนการที่นำข้อมูลจากเหตุการณ์ด้านความมั่นคงปลอดภัยมาวิเคราะห์เพื่อค้นหาสาเหตุ ลักษณะ ขอบเขต ผลกระทบ และความสัมพันธ์ของเหตุการณ์ เพื่อสนับสนุนการตัดสินใจในการตอบสนอง ในสถาปัตยกรรมที่นำเสนอข้อมูลจากระบบต่าง ๆ จะถูกนำมาวิเคราะห์ร่วมกัน โดย AI สามารถช่วยค้นหารูปแบบและความสัมพันธ์ของเหตุการณ์ที่เกิดขึ้นในหลายระบบ ซึ่งช่วยลดข้อจำกัดของการวิเคราะห์ข้อมูลที่แยกออกจากกัน Machine Learning และ Deep Learning สามารถนำมาใช้ในการวิเคราะห์รูปแบบเหตุการณ์ ขณะที่ NLP สามารถนำมาใช้วิเคราะห์รายงาน เหตุการณ์ หรือข้อมูลข้อความที่เกี่ยวข้องกับความมั่นคงปลอดภัย ส่วน Behavioral AI สามารถนำมาใช้วิเคราะห์พฤติกรรมของผู้ใช้งานและระบบเพื่อค้นหาความผิดปกติ

5.2.3.4 การตอบสนองและการป้องกันเชิงรุก (Response & Proactive Defense)

การตอบสนองและการป้องกันเชิงรุกเป็นความสามารถในการดำเนินการหลังจากตรวจพบหรือวิเคราะห์เหตุการณ์ รวมถึงการดำเนินการล่วงหน้าเพื่อป้องกันเหตุการณ์ที่อาจเกิดขึ้น ในบริบทของสถาบันอุดมศึกษา การตอบสนองอาจประกอบด้วยการแจ้งเตือนผู้รับผิดชอบ การจำกัดสิทธิ์การเข้าถึง การแยกอุปกรณ์ที่มีความเสี่ยง การกำหนดมาตรการป้องกันเพิ่มเติม และการดำเนินการตาม Incident Response Process การนำ AI มาใช้จะช่วยให้สามารถจัดลำดับความสำคัญของเหตุการณ์ ประเมินระดับความเสี่ยง และเสนอแนวทางตอบสนองที่เหมาะสมได้ โดยการดำเนินการอัตโนมัติควรอยู่ภายใต้หลักเกณฑ์และระดับสิทธิ์ที่กำหนดโดย Governance Architecture

5.2.3.5 ความทนทานและการฟื้นฟู (Resilience & Recovery)

ความทนทานและการฟื้นฟูเป็นความสามารถของสถาบันในการรักษาความต่อเนื่องของบริการดิจิทัลและสามารถฟื้นฟูระบบกลับสู่สภาวะปกติหลังจากเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศ การจัดการด้าน Resilience & Recovery ไม่ควรมุ่งเน้นเฉพาะการกู้คืนระบบหลังเกิดเหตุการณ์เท่านั้น แต่ควรครอบคลุมการเตรียมความพร้อม การสำรองข้อมูล การออกแบบระบบที่มีความทนทาน การจัดทำแผนความต่อเนื่องทางธุรกิจ และการทดสอบกระบวนการฟื้นฟูอย่างสม่ำเสมอ ในบริบทของ AI สามารถนำข้อมูลในอดีตมาวิเคราะห์เพื่อประเมินแนวโน้มของความล้มเหลวของระบบ และสนับสนุนการวางแผนความต่อเนื่องของบริการได้

5.2.3.6 ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ (Collaboration & Cybersecurity Awareness)

ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์เป็นองค์ประกอบที่ให้ความสำคัญกับ People ซึ่งเป็นส่วนสำคัญของภูมิคุ้มกันดิจิทัลของสถาบัน เนื่องจากผู้ใช้งานเป็นส่วนหนึ่งของระบบนิเวศดิจิทัล และพฤติกรรมของผู้ใช้งานอาจส่งผลต่อความมั่นคงปลอดภัยขององค์กร สถาบันจึงควรมีการสร้างความรู้ ความเข้าใจ และทักษะด้านความมั่นคงปลอดภัยให้แก่ผู้บริหาร บุคลากร นักศึกษา และผู้ใช้งานระบบสารสนเทศ รวมถึงสร้างช่องทางในการรายงานเหตุการณ์และแลกเปลี่ยนข้อมูลด้านความเสี่ยง นอกจากนี้ ข้อมูลจากการฝึกอบรม การทดสอบความรู้ และเหตุการณ์ด้านความมั่นคงปลอดภัยสามารถนำมาวิเคราะห์ด้วย AI เพื่อประเมินแนวโน้มความเสี่ยงและกำหนดแนวทางการสร้างความตระหนักรู้ให้เหมาะสมกับกลุ่มผู้ใช้งาน

5.2.3.7 ความสัมพันธ์ระหว่างระบบภูมิคุ้มกันดิจิทัลกับกระบวนการธุรกิจ

ตารางที่ 5-19 ความสัมพันธ์ระหว่างระบบภูมิคุ้มกันดิจิทัลกับกระบวนการธุรกิจ

กระบวนการธุรกิจ	Digital Immunity Capability	เทคโนโลยีที่เกี่ยวข้อง	ข้อมูลที่ใช้
การบริหารองค์กร	Visibility, Risk Management	Monitoring, AI Analytics	KPI, Risk Data, System Status
การจัดการนักศึกษา	Detection, Response	Behavioral AI, ML	Student Activity, Authentication Log
การเรียนการสอน	Visibility, Resilience	Monitoring, Backup	LMS Log, Availability Data
การบริหารบุคลากร	Detection, Awareness	Behavioral AI, NLP	User Activity, Training Data
การวิจัย	Protection, Resilience	Security Analytics, Backup	Research Data, Access Log
การบริหารระบบ IT	Observability, Detection, Recovery	SIEM, AI, Monitoring	System Log, Network Traffic
การรักษาความมั่นคงปลอดภัย	Detection, Investigation	ML, DL, SIEM	Security Event, Threat Intelligence
การจัดการเหตุการณ์	Investigation, Response	AI Analytics, SOAR	Incident Data, Risk Data
การบริหารความต่อเนื่อง	Resilience & Recovery	DR, Backup, Predictive AI	Availability, Recovery Data

กระบวนการธุรกิจ	Digital Immunity Capability	เทคโนโลยีที่เกี่ยวข้อง	ข้อมูลที่ใช้
การสร้างความตระหนักรู้	Awareness & Collaboration	NLP, Generative AI, Analytics	Training Data, Awareness Data

5.2.3.8 การวิเคราะห์ช่องว่างด้านระบบภูมิคุ้มกันดิจิทัล

ตารางที่ 5-20 การวิเคราะห์ช่องว่างด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity Gap)

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
การมองเห็นและเฝ้าระวัง	มีระบบ Monitoring และ Log จากหลายระบบ	ข้อมูลยังไม่เป็นภาพรวมและขาด Intelligent Observability	Integrated Intelligent Observability
การตรวจจับภัยคุกคาม	ตรวจจับจากกฎและระบบ Security	ขาดความสามารถในการเรียนรู้รูปแบบภัยคุกคามใหม่	AI-Based Threat Detection
การสืบสวนและวิเคราะห์	วิเคราะห์เหตุการณ์โดยผู้ปฏิบัติงานและระบบเฉพาะด้าน	ขาดการวิเคราะห์เหตุการณ์แบบเชื่อมโยงหลายแหล่ง	AI Security Analytics
การตอบสนอง	มีขั้นตอน Incident Response	การตอบสนองยังต้องอาศัยการดำเนินการของบุคลากรในหลายขั้นตอน	AI-Assisted / Automated Response
การป้องกันเชิงรุก	เน้นการป้องกันตามมาตรการที่กำหนด	ขาด Predictive Threat Intelligence	Predictive & Proactive Defense
ความทนทาน	มี Backup และ Recovery ตามระบบ	การประเมินความเสี่ยงและการคาดการณ์ความล้มเหลวยังจำกัด	AI-Enabled Resilience
การฟื้นฟู	มีกระบวนการกู้คืนระบบ	ขาดการวิเคราะห์และปรับปรุง Recovery จากข้อมูลเหตุการณ์	Intelligent Recovery
ความร่วมมือ	มีหน่วยงานรับผิดชอบด้าน IT/Security	การแบ่งปันข้อมูลเหตุการณ์ระหว่างหน่วยงานยังต้องพัฒนา	Collaborative Security Platform
Cybersecurity Awareness	มีการอบรมและประชาสัมพันธ์	การสร้างความตระหนักรู้ยังไม่ปรับตามพฤติกรรมและความเสี่ยงของผู้ใช้	AI-Based Adaptive Awareness

5.2.3.9 ความต้องการด้านระบบภูมิคุ้มกันดิจิทัล

จากการวิเคราะห์สภาพปัจจุบันและช่องว่าง ผู้วิจัยสังเคราะห์ความต้องการของระบบภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาออกเป็น 6 ด้าน ดังนี้

1. ต้องมีความสามารถในการมองเห็นสภาพแวดล้อมดิจิทัลอย่างครอบคลุม สามารถรวบรวมข้อมูลจากระบบ เครือข่าย อุปกรณ์ ผู้ใช้งาน และบริการดิจิทัลเพื่อสร้างภาพรวมของสถานะระบบ

2. ต้องมีความสามารถในการตรวจจับภัยคุกคามด้วย AI สามารถใช้ Machine Learning, Deep Learning และ Behavioral AI ในการตรวจจับความผิดปกติและภัยคุกคาม

3. ต้องมีความสามารถในการสืบสวนและวิเคราะห์แบบบูรณาการ สามารถเชื่อมโยงข้อมูลจากหลายแหล่งเพื่อวิเคราะห์สาเหตุ ความสัมพันธ์ และผลกระทบของเหตุการณ์

4. ต้องมีความสามารถในการตอบสนองและป้องกันเชิงรุก สามารถจัดลำดับความสำคัญของภัยคุกคามและสนับสนุนการตอบสนอง รวมถึงการป้องกันเหตุการณ์ที่อาจเกิดขึ้นในอนาคต

5. ต้องมีความสามารถในการรักษาความต่อเนื่องและฟื้นฟูระบบ สามารถรักษาความพร้อมใช้งานของบริการและฟื้นฟูระบบภายหลังเกิดเหตุการณ์

6. ต้องมีความสามารถด้านบุคลากรและความร่วมมือ สามารถสร้างความตระหนักรู้และส่งเสริมความร่วมมือระหว่างผู้บริหาร บุคลากร นักศึกษา และหน่วยงานที่เกี่ยวข้อง

5.2.3.10 การออกแบบระบบภูมิคุ้มกันดิจิทัลใน Target Architecture

จากผลการวิเคราะห์กำหนด Digital Immunity Architecture ให้เป็นสถาปัตยกรรมความสามารถที่เชื่อมโยงเทคโนโลยีอัจฉริยะ ระบบความมั่นคงปลอดภัย ข้อมูล แอปพลิเคชัน และกระบวนการธุรกิจเข้าด้วยกัน โดยมีเป้าหมายเพื่อทำให้สถาบันสามารถจัดการความเสี่ยงดิจิทัลได้อย่างต่อเนื่องและปรับตัวได้ตามสถานการณ์ โครงสร้างการทำงานของระบบภูมิคุ้มกันดิจิทัลสามารถอธิบายเป็นวงจร ดังนี้



ภาพที่ 5-2 โครงสร้างการทำงานของระบบภูมิคุ้มกันดิจิทัล

ตารางที่ 5-21 สรุปสำหรับเชื่อม Current Architecture ⟶ Target Architecture

ประเด็น	Current Architecture	Gap	Target Architecture	AI Technology	Digital Immunity Capability
Observability & Visibility	Monitoring และ Log แยกตามระบบ	ขาดภาพรวมแบบบูรณาการ	Intelligent Observability	ML, Behavioral AI	Monitor

ประเด็น	Current Architecture	Gap	Target Architecture	AI Technology	Digital Immunity Capability
Threat Detection	Detection ตามกฎ	ตรวจจับภัยคุกคามรูปแบบใหม่ได้จำกัด	AI Threat Detection	ML, DL, Behavioral AI	Detect
Investigation & Analysis	วิเคราะห์โดยบุคลากรและระบบเฉพาะ	ขาด Correlation ระหว่างข้อมูล	AI Security Analytics	ML, DL, NLP	Analyze
Response & Proactive Defense	Incident Response ตามขั้นตอน	การตอบสนองยังใช้แรงงานมนุษย์มาก	Intelligent Response	ML, Behavioral AI	Respond
Resilience & Recovery	Backup/Recovery	ขาด Predictive Resilience	Intelligent Resilience	ML, Predictive Analytics	Recover
Collaboration & Awareness	อบรมและประสานงาน	ขาดการวิเคราะห์ความเสี่ยงเชิงพฤติกรรม	Collaborative Cybersecurity	NLP, Behavioral AI	Learn & Improve

จากการวิเคราะห์ด้านระบบภูมิคุ้มกันดิจิทัล ผู้วิจัยพบว่า สถาบันอุดมศึกษาจำเป็นต้องพัฒนาจากแนวทางการรักษาความมั่นคงปลอดภัยที่เน้นการป้องกันและตอบสนองต่อเหตุการณ์ ไปสู่ระบบภูมิคุ้มกันดิจิทัลที่มีความสามารถในการมองเห็น ตรวจจับ วิเคราะห์ คาดการณ์ ตอบสนอง ฟื้นฟู และเรียนรู้อย่างต่อเนื่อง ทั้ง 6 องค์ประกอบจึงมีความสัมพันธ์ในลักษณะวงจร ไม่ใช่การทำงานแบบแยกส่วน โดย Observability & Visibility เป็นฐานของข้อมูล Threat Detection ทำหน้าที่ค้นหาความผิดปกติ Investigation & Analysis ทำหน้าที่วิเคราะห์สาเหตุและความสัมพันธ์ Response & Proactive Defense สนับสนุนการจัดการเหตุการณ์และการป้องกันเชิงรุก Resilience & Recovery ทำให้สถาบันสามารถดำเนินงานต่อและฟื้นฟูระบบ และ Collaboration & Cybersecurity Awareness ทำหน้าที่เสริมสร้างภูมิคุ้มกันในระดับบุคลากรและองค์กร เมื่อผนวกกับ Intelligent Technology ซึ่งประกอบด้วย Machine Learning, Deep Learning, NLP และ Behavioral AI ระบบภูมิคุ้มกันดิจิทัลจะสามารถยกระดับจากการรักษาความมั่นคงปลอดภัยแบบตอบสนอง ไปสู่ AI-Driven Digital Immunity ที่สามารถเรียนรู้จากข้อมูล ตรวจจับรูปแบบความผิดปกติ วิเคราะห์ความเสี่ยง และสนับสนุนการป้องกันเชิงรุกได้อย่างเป็นระบบ

5.2.4 ด้านการจัดการองค์กรดิจิทัล (Digital Enterprise Management)

จากการวิเคราะห์สภาพปัจจุบันของสถาบันอุดมศึกษาพบว่า การเปลี่ยนแปลงทางเทคโนโลยีดิจิทัลส่งผลต่อรูปแบบการบริหารจัดการ การจัดการทรัพยากร การให้บริการ การจัดการข้อมูล และกระบวนการดำเนินงานของสถาบันอย่างต่อเนื่อง สถาบันอุดมศึกษาจึงจำเป็นต้องปรับรูปแบบการ

บริหารจากการดำเนินงานที่พึ่งพากระบวนการแบบเดิมไปสู่การบริหารจัดการที่ขับเคลื่อนด้วยข้อมูล เทคโนโลยีดิจิทัล และระบบอัจฉริยะ

5.2.4.1 กลยุทธ์ดิจิทัล (Digital Strategy)

กลยุทธ์ดิจิทัลเป็นองค์ประกอบที่กำหนดทิศทางและเป้าหมายในการนำเทคโนโลยีดิจิทัลมาใช้สนับสนุนยุทธศาสตร์ของสถาบันอุดมศึกษา โดยต้องมีความสอดคล้องกับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ และเป้าหมายขององค์กร ตลอดจนบริบทการเปลี่ยนแปลงของเทคโนโลยีและสภาพแวดล้อมภายนอก ในสภาพปัจจุบัน สถาบันอุดมศึกษามีการกำหนดแผนและโครงการด้านดิจิทัลเพื่อสนับสนุนการบริหารจัดการ การเรียนการสอน การวิจัย และการบริการ แต่การดำเนินงานด้านดิจิทัลอาจมีลักษณะแยกตามหน่วยงานหรือโครงการ ส่งผลให้การลงทุนและการพัฒนาเทคโนโลยีบางส่วนขาดการเชื่อมโยงในระดับองค์กร สำหรับสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ กลยุทธ์ดิจิทัลควรครอบคลุมถึง AI Strategy และ Digital Immunity Strategy เพื่อกำหนดทิศทางการนำ AI มาใช้ในการสร้างความสามารถขององค์กร รวมถึงการจัดการความเสี่ยงและภูมิคุ้มกันดิจิทัล

5.2.4.2 โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure)

โครงสร้างพื้นฐานเทคโนโลยีเป็นพื้นฐานสำคัญที่สนับสนุนการดำเนินงานของระบบดิจิทัลทั้งหมดของสถาบัน ครอบคลุมระบบเครือข่าย ศูนย์ข้อมูล Cloud Computing เครื่องแม่ข่าย ระบบจัดเก็บข้อมูล อุปกรณ์ปลายทาง และโครงสร้างพื้นฐานสำหรับรองรับระบบ AI สถาบันอุดมศึกษามีการใช้งานโครงสร้างพื้นฐานที่หลากหลายและอาจประกอบด้วยทั้งระบบ On-premises และ Cloud อย่างไรก็ตาม ความแตกต่างของเทคโนโลยีและการกระจายตัวของระบบอาจทำให้เกิดข้อจำกัดในการบริหารจัดการและการเชื่อมโยงระบบ สำหรับสถาปัตยกรรมเป้าหมาย โครงสร้างพื้นฐานควรสามารถรองรับ AI Workload, Data Processing, Security Monitoring และ Digital Immunity Services รวมถึงสามารถขยายทรัพยากรตามปริมาณการใช้งานได้

5.2.4.3 การจัดการข้อมูล (Data Management)

การจัดการข้อมูลเป็นองค์ประกอบสำคัญขององค์กรดิจิทัล เนื่องจากข้อมูลเป็นทรัพยากรพื้นฐานสำหรับการบริหาร การตัดสินใจ และการพัฒนา AI ของสถาบัน ข้อมูลของสถาบันอุดมศึกษามีหลายประเภท ได้แก่ ข้อมูลนักศึกษา ข้อมูลบุคลากร ข้อมูลการเรียนการสอน ข้อมูลการเงิน ข้อมูลการวิจัย ข้อมูลระบบสารสนเทศ และข้อมูลด้านความมั่นคงปลอดภัย ซึ่งข้อมูลเหล่านี้มาจากหลายหน่วยงานและหลายระบบ ปัญหาที่สำคัญคือข้อมูลอาจมีรูปแบบแตกต่างกัน มีการจัดเก็บแบบกระจาย และมีระดับคุณภาพข้อมูลที่แตกต่างกัน ดังนั้น การจัดการข้อมูลใน Target Architecture จำเป็นต้องมุ่งสู่ Enterprise Data Management ที่มีมาตรฐานข้อมูล การกำกับดูแลข้อมูล การบูรณาการข้อมูล และการจัดการข้อมูลสำหรับ AI

5.2.4.4 กระบวนการอัตโนมัติ (Process Automation)

กระบวนการอัตโนมัติเป็นการนำเทคโนโลยีดิจิทัลมาใช้ลดขั้นตอนที่ต้องดำเนินการด้วยบุคลากร เพิ่มความรวดเร็ว ลดความผิดพลาด และเพิ่มประสิทธิภาพของกระบวนการทำงาน ในสถาบันอุดมศึกษา สามารถนำกระบวนการอัตโนมัติมาใช้กับงานด้านการรับสมัครนักศึกษา การลงทะเบียน การจัดการเอกสาร การให้บริการนักศึกษา การจัดการบุคลากร การเงิน และการบริหารระบบสารสนเทศ กระบวนการอัตโนมัติมีความสำคัญมากขึ้นเมื่อเชื่อมโยงกับ AI โดยสามารถพัฒนาเป็น Intelligent Process Automation ซึ่งใช้ผลการวิเคราะห์จาก AI เพื่อสนับสนุนการตัดสินใจและดำเนินการบางขั้นตอนโดยอัตโนมัติ ในด้าน Digital Immunity สามารถนำระบบอัตโนมัติมาใช้ในการแจ้งเตือนเหตุการณ์ การจัดลำดับความเสี่ยง การเปิด Incident Ticket การจำกัดสิทธิ์ หรือการดำเนินการตอบสนองตามนโยบายที่กำหนด

5.2.4.5 ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

ความมั่นคงปลอดภัยทางไซเบอร์เป็นองค์ประกอบสำคัญของการจัดการองค์กรดิจิทัล เนื่องจากการเพิ่มขึ้นของการใช้ระบบดิจิทัลทำให้สถาบันต้องเผชิญกับความเสี่ยงด้านข้อมูล ระบบสารสนเทศ และบริการออนไลน์ การจัดการความมั่นคงปลอดภัยทางไซเบอร์ครอบคลุมการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability) รวมถึงการบริหารสิทธิ์ การยืนยันตัวตน การจัดการเหตุการณ์ และการบริหารความเสี่ยง สำหรับสถาปัตยกรรมเป้าหมาย Cybersecurity ควรเชื่อมโยงกับ AI และ Digital Immunity เพื่อให้สามารถตรวจจับความผิดปกติ วิเคราะห์เหตุการณ์ และสนับสนุนการตอบสนองได้อย่างรวดเร็ว

5.2.4.6 ความสัมพันธ์ระหว่างการจัดการองค์กรดิจิทัลกับกระบวนการธุรกิจ

ตารางที่ 5-22 ความสัมพันธ์ระหว่างการจัดการองค์กรดิจิทัลกับกระบวนการธุรกิจ

องค์ประกอบ	กระบวนการธุรกิจที่เกี่ยวข้อง	เทคโนโลยีที่ใช้	ข้อมูลที่ใช้
Digital Strategy	การกำหนดยุทธศาสตร์และแผนองค์กร	Digital Platform, BI, AI Analytics	Strategic Data, KPI, Risk Data
Technology Infrastructure	การให้บริการระบบดิจิทัล	Cloud, Network, Data Center, Edge	Infrastructure Data, Performance Data
Data Management	การบริหารและใช้ข้อมูล	Data Warehouse, Data Lake, Data Governance	Master Data, Metadata, Transaction Data

องค์ประกอบ	กระบวนการธุรกิจที่เกี่ยวข้อง	เทคโนโลยีที่ใช้	ข้อมูลที่ใช้
Process Automation	การบริหารกระบวนการและบริการ	Workflow, RPA, AI Automation	Process Data, Workflow Data
Cybersecurity	การรักษาความมั่นคงปลอดภัย	SIEM, IAM, AI Security	Security Log, Incident Data
Digital Management	การบริหารองค์กรแบบบูรณาการ	AI Analytics, Dashboard	Enterprise Data

5.2.4.7 ปัญหาและข้อจำกัด

จากการวิเคราะห์สภาพปัจจุบัน สามารถสังเคราะห์ปัญหาและข้อจำกัดด้านการจัดการองค์กรดิจิทัลได้ดังนี้

1. การดำเนินงานด้านดิจิทัลยังมีความแตกต่างระหว่างหน่วยงาน
2. กลยุทธ์ด้านดิจิทัลและ AI ยังจำเป็นต้องเชื่อมโยงกับยุทธศาสตร์องค์กรให้ชัดเจนยิ่งขึ้น
3. โครงสร้างพื้นฐานเทคโนโลยีมีความหลากหลายและกระจายตัว
4. ข้อมูลมีจำนวนมากแต่ยังขาดการจัดการแบบบูรณาการระดับองค์กร
5. กระบวนการบางส่วนยังต้องอาศัยการดำเนินงานด้วยบุคลากร
6. การนำ AI มาใช้ในกระบวนการอัตโนมัติยังมีข้อจำกัด
7. ระบบ Cybersecurity ยังจำเป็นต้องพัฒนาความสามารถด้านการตรวจจับและคาดการณ์เชิงรุก
8. การเชื่อมโยงข้อมูลระหว่าง Digital Management, AI และ Digital Immunity ยังไม่เป็นระบบเดียวกัน

5.2.4.8 การวิเคราะห์ช่องว่างด้านการจัดการองค์กรดิจิทัล

ตารางที่ 5-23 การวิเคราะห์ช่องว่างด้านการจัดการองค์กรดิจิทัล

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
Digital Strategy	มีแผนและยุทธศาสตร์ดิจิทัล	การเชื่อมโยง Digital Strategy กับ AI และ Digital Immunity ยังไม่สมบูรณ์	AI-Driven Digital Strategy
Technology Infrastructure	มีโครงสร้างพื้นฐาน IT หลายประเภท	ขาดโครงสร้างพื้นฐานที่ออกแบบรองรับ AI และการขยายตัว	AI-Ready Infrastructure

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
Data Management	มีข้อมูลจากหลายระบบ	ข้อมูลกระจายและมีมาตรฐานแตกต่างกัน	Enterprise Data Platform
Process Automation	มีการใช้ระบบอัตโนมัติบางกระบวนการ	ยังขาด Intelligent Process Automation	AI-Enabled Process Automation
Cybersecurity	มีระบบ Security พื้นฐาน	ความสามารถด้าน AI-based Detection และ Proactive Defense ยังจำกัด	AI-Driven Cybersecurity
Enterprise Integration	ระบบทำงานแยกตามหน่วยงาน	ขาดการบริหารแบบบูรณาการ	Integrated Digital Enterprise

5.2.4.9 ความต้องการด้านการจัดการองค์กรดิจิทัล

จากการวิเคราะห์ช่องว่าง ผู้วิจัยสังเคราะห์ความต้องการด้านการจัดการองค์กรดิจิทัล ดังนี้

1) Digital Strategy Alignment ต้องสามารถเชื่อมโยงยุทธศาสตร์ดิจิทัลกับยุทธศาสตร์หลักของสถาบัน รวมถึงยุทธศาสตร์ AI และการจัดการภูมิคุ้มกันดิจิทัล

2) AI-Ready Technology Infrastructure ต้องมีโครงสร้างพื้นฐานที่สามารถรองรับการประมวลผลข้อมูลและ AI รวมถึงการขยายระบบในอนาคต

3) Enterprise Data Management ต้องมีระบบจัดการข้อมูลระดับองค์กรที่สนับสนุนคุณภาพข้อมูล การบูรณาการข้อมูล และการนำข้อมูลไปใช้กับ AI

4) Intelligent Process Automation ต้องสามารถนำ AI มาเพิ่มประสิทธิภาพกระบวนการ ลดงานที่ซ้ำซ้อน และสนับสนุนการตัดสินใจ

5) AI-Driven Cybersecurity ต้องสามารถนำ AI มาเพิ่มความสามารถในการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคาม

5.2.4.10 การออกแบบการจัดการองค์กรดิจิทัลใน Target Architecture

จากผลการวิเคราะห์กำหนดให้ Digital Enterprise Management Architecture เป็นชั้นที่ทำหน้าที่เชื่อมโยงยุทธศาสตร์ การบริหารจัดการ เทคโนโลยี ข้อมูล กระบวนการ และ Cybersecurity เข้าด้วยกัน โดยมี AI เป็นกลไกสนับสนุนการบริหารจัดการและการตัดสินใจ สถาปัตยกรรมเป้าหมายประกอบด้วย 5 องค์ประกอบหลัก ได้แก่



ภาพที่ 5-3 องค์ประกอบกลไกสนับสนุนการบริหารจัดการและการตัดสินใจสถาปัตยกรรมเป้าหมาย

โดยทั้ง 5 องค์ประกอบทำงานร่วมกันเป็นระบบ กล่าวคือ Digital Strategy กำหนดทิศทางขององค์กร Technology Infrastructure เป็นพื้นฐานของการดำเนินงาน Data Management ทำหน้าที่จัดเตรียมข้อมูลสำหรับการบริหารและ AI Process Automation เพิ่มประสิทธิภาพของกระบวนการ และ Cybersecurity ทำหน้าที่ปกป้องทรัพยากรดิจิทัลทั้งหมด เมื่อเชื่อมโยงกับ Intelligent Technology ระบบจะสามารถยกระดับจาก Digital Enterprise Management ไปสู่ AI-Enabled Digital Enterprise Management ซึ่งมีความสามารถในการวิเคราะห์ข้อมูล คาดการณ์แนวโน้ม สนับสนุนการตัดสินใจ และดำเนินงานบางส่วนแบบอัตโนมัติ

ตารางที่ 5-24 สรุป Current Architecture ⟶ Gap ⟶ Target Architecture

ประเด็น	Current Architecture	Gap	Target Architecture	AI Technology	Digital Immunity Capability
Digital Strategy	แผนดิจิทัลขององค์กร	ขาดการเชื่อมโยง AI และ Digital Immunity	AI-Driven Digital Strategy	ML, AI Analytics	Strategic Resilience
Technology Infrastructure	IT Infrastructure แบบผสมผสาน	ยังไม่รองรับ AI อย่างเป็นระบบ	AI-Ready Infrastructure	ML/DL Infrastructure	Infrastructure Resilience
Data Management	ข้อมูลกระจายหลายระบบ	ขาด Enterprise Data Integration	Enterprise Data Platform	ML, DL, NLP	Data Resilience
Process Automation	Automation บางกระบวนการ	ขาด Intelligent Automation	AI-Enabled Process Automation	ML, Behavioral AI	Automated Response
Cybersecurity	Security Systems	ขาด Predictive/AI Security	AI-Driven Cybersecurity	ML, DL, Behavioral AI	Threat Detection & Response
Digital Enterprise	การบริหารแบบแยกส่วน	ขาด Enterprise-wide Integration	AI-Enabled Digital Enterprise	AI + Analytics	Enterprise Digital Immunity

จากการวิเคราะห์ด้านการจัดการองค์กรดิจิทัล พบว่า Digital Enterprise Management เป็นองค์ประกอบที่ทำหน้าที่เชื่อมโยงระดับยุทธศาสตร์ ระดับการบริหาร และระดับการปฏิบัติการของสถาบันเข้าด้วยกัน โดยมี Digital Strategy, Technology Infrastructure, Data Management, Process Automation และ Cybersecurity เป็นองค์ประกอบหลัก

5.2.5 ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (Artificial Intelligence Enterprise Architecture)

จากการวิเคราะห์สภาพปัจจุบันของสถาบันอุดมศึกษาพบว่า การนำปัญญาประดิษฐ์มาใช้ในองค์กรมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ทั้งในด้านการบริหารจัดการ การจัดการเรียนการสอน การวิจัย การบริการนักศึกษา การวิเคราะห์ข้อมูล และการรักษาความมั่นคงปลอดภัย อย่างไรก็ตาม การนำ AI มาใช้ในหลายกรณียังมีลักษณะเป็นการพัฒนาเฉพาะระบบหรือเฉพาะหน่วยงาน ทำให้ขาดกรอบสถาปัตยกรรมที่สามารถเชื่อมโยง AI เข้ากับยุทธศาสตร์ กระบวนการ ข้อมูล แอปพลิเคชัน เทคโนโลยี ความมั่นคงปลอดภัย และการกำกับดูแลขององค์กรอย่างเป็นระบบ ดังนั้น สถาปัตยกรรมองค์กรปัญญาประดิษฐ์จึงมีบทบาทในการทำหน้าที่เป็นกรอบกลางสำหรับการบูรณาการความสามารถของ AI เข้ากับสถาปัตยกรรมองค์กร (Enterprise Architecture) เพื่อให้การพัฒนาและการนำ AI ไปใช้งานสามารถตอบสนองต่อเป้าหมายของสถาบัน มีความยืดหยุ่น สามารถปรับตัวต่อการเปลี่ยนแปลง และสามารถบริหารความเสี่ยงที่เกิดจากการใช้เทคโนโลยี AI ได้

5.2.5.1 การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ (EA–AI Integration)

การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์เป็นความสามารถในการเชื่อมโยงเทคโนโลยี AI เข้ากับองค์ประกอบต่าง ๆ ของ Enterprise Architecture โดยไม่พิจารณา AI เป็นเพียงเทคโนโลยีเพิ่มเติม แต่พิจารณา AI เป็นความสามารถเชิงยุทธศาสตร์ที่สนับสนุนกระบวนการดำเนินงานและการตัดสินใจขององค์กร สำหรับสถาบันอุดมศึกษา การบูรณาการดังกล่าวครอบคลุมการเชื่อมโยง AI กับ Business Architecture, Data Architecture, Application Architecture, Technology Architecture, Security Architecture, Integration Architecture และ Governance Architecture เพื่อให้ข้อมูลและความสามารถของ AI สามารถสนับสนุนกระบวนการธุรกิจได้อย่างต่อเนื่อง

5.2.5.2 กรอบการทำงานเชิงสถาปัตยกรรม (Architectural Framework)

กรอบการทำงานเชิงสถาปัตยกรรมเป็นโครงสร้างที่ใช้กำหนดองค์ประกอบ ความสัมพันธ์ หลักการ และแนวทางในการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ให้เป็นระบบ ในงานวิจัยนี้ กรอบสถาปัตยกรรมควรทำหน้าที่เชื่อมโยง Business, Data, Application, Technology, Security, Integration และ Governance เข้ากับ Intelligent Technology, Digital Immunity และ AI Enterprise Architecture การกำหนดกรอบดังกล่าวช่วยลดการพัฒนา AI แบบแยกส่วน และทำให้การพัฒนาระบบ AI สามารถตรวจสอบความสัมพันธ์ระหว่างยุทธศาสตร์ กระบวนการ ข้อมูล เทคโนโลยี และผลลัพธ์ทางธุรกิจได้อย่างชัดเจน

5.2.5.3 การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ (AI-driven Information System Design & Development)

การออกแบบและพัฒนาระบบสารสนเทศด้วย AI เป็นความสามารถในการนำ AI เข้ามาเป็นส่วนหนึ่งของการออกแบบระบบสารสนเทศ ตั้งแต่การวิเคราะห์ความต้องการ การออกแบบข้อมูล การเลือกเทคโนโลยี การพัฒนาโมเดล การทดสอบ การนำไปใช้งาน และการติดตามผล สำหรับสถาบันอุดมศึกษา สามารถนำไปใช้ในการพัฒนาระบบ เช่น ระบบวิเคราะห์ความเสี่ยง ระบบสนับสนุนการตัดสินใจ ระบบบริการอัจฉริยะ ระบบวิเคราะห์พฤติกรรม และระบบตรวจจับเหตุการณ์ผิดปกติ การออกแบบระบบควรคำนึงถึงทั้งประสิทธิภาพของ AI และข้อกำหนดด้านข้อมูล ความปลอดภัย ความเป็นส่วนตัว ความสามารถในการตรวจสอบ และความรับผิดชอบของระบบ

5.2.5.4 การปรับตัวต่อการเปลี่ยนแปลง (Adaptability & Agility)

การปรับตัวต่อการเปลี่ยนแปลงเป็นความสามารถของสถาปัตยกรรมในการรองรับการเปลี่ยนแปลงของเทคโนโลยี สภาพแวดล้อม ภัยคุกคาม นโยบาย และความต้องการของผู้ใช้งาน สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ควรมีลักษณะ Modular และสามารถเพิ่ม เปลี่ยน หรือปรับปรุงองค์ประกอบของ AI ได้โดยไม่จำเป็นต้องปรับเปลี่ยนระบบทั้งหมด ในบริบทของ Digital Immunity ความสามารถด้าน Adaptability & Agility มีความสำคัญ เนื่องจากรูปแบบของภัยคุกคามสามารถเปลี่ยนแปลงได้ตลอดเวลา ระบบจึงจำเป็นต้องสามารถเรียนรู้และปรับปรุงรูปแบบการตรวจจับและการตอบสนองได้อย่างต่อเนื่อง

5.2.5.5 การรับมือภัยคุกคามและความเสี่ยง (Threat & Risk Responsiveness)

การรับมือภัยคุกคามและความเสี่ยงเป็นความสามารถของสถาปัตยกรรมในการระบุ ประเมิน และตอบสนองต่อความเสี่ยงที่เกี่ยวข้องกับระบบ AI และระบบดิจิทัลขององค์กร ความเสี่ยงอาจเกิดจากภัยคุกคามทางไซเบอร์ ความผิดพลาดของข้อมูล ความไม่ถูกต้องของโมเดล การใช้ AI อย่างไม่เหมาะสม การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการเปลี่ยนแปลงของสภาพแวดล้อมทางเทคโนโลยี ดังนั้น สถาปัตยกรรมเป้าหมายจึงควรเชื่อมโยง AI กับระบบ Risk Management และ Digital Immunity เพื่อให้สามารถตรวจจับ วิเคราะห์ ประเมิน และตอบสนองต่อความเสี่ยงได้อย่างเป็นระบบ

5.2.5.6 จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ (AI Ethics and Responsibility)

การนำ AI มาใช้ในสถาบันอุดมศึกษาจำเป็นต้องคำนึงถึงจริยธรรมและความรับผิดชอบ เนื่องจาก AI สามารถนำข้อมูลจำนวนมากมาใช้ในการวิเคราะห์และสนับสนุนการตัดสินใจ ซึ่งอาจส่งผลกระทบต่อบุคคลและองค์กร ประเด็นสำคัญประกอบด้วย ความโปร่งใส ความสามารถในการอธิบายผลลัพธ์ของ AI ความเป็นธรรม ความเป็นส่วนตัว ความปลอดภัย ความรับผิดชอบ และการ

กำหนดบทบาทของมนุษย์ในการกำกับผลลัพธ์จาก AI ดังนั้น AI Architecture ของสถาบันควรมี AI Governance และ AI Ethics เป็นองค์ประกอบที่กำกับการพัฒนาและการใช้งาน AI ตลอดวงจรชีวิต

5.2.5.7 ความสัมพันธ์ระหว่าง AI Enterprise Architecture กับกระบวนการธุรกิจ

ตารางที่ 5-25 ความสัมพันธ์ระหว่าง AI Enterprise Architecture กับกระบวนการธุรกิจ

องค์ประกอบ	กระบวนการธุรกิจ	เทคโนโลยี/กลไก	ข้อมูลที่ใช้
EA–AI Integration	การบริหารองค์กรและระบบสารสนเทศ	EA, API, AI Platform	Enterprise Data
Architectural Framework	การวางแผนและพัฒนาระบบ	Architecture Framework	Architecture Repository
AI-driven IS Design	การพัฒนาบริการและระบบอัจฉริยะ	ML, DL, NLP	Training/Operational Data
Adaptability & Agility	การปรับปรุงระบบและกระบวนการ	Modular Architecture, Cloud	Performance/Change Data
Threat & Risk Responsiveness	การบริหารความเสี่ยง	AI Security, Analytics	Risk/Incident Data
AI Ethics & Responsibility	การกำกับดูแล AI	AI Governance	AI Model/Data/Decision Data

5.2.5.8 การวิเคราะห์ช่องว่างด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ตารางที่ 5-26 การวิเคราะห์ช่องว่าง (AI Enterprise Architecture Gap)

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
EA–AI Integration	AI ถูกพัฒนาในบางระบบหรือบางหน่วยงาน	ขาดการบูรณาการ AI กับ EA ระดับองค์กร	Integrated EA–AI Architecture
Architectural Framework	มีกรอบ EA แต่ AI ยังไม่ได้บูรณาการอย่างชัดเจน	ขาดกรอบสำหรับ AI Enterprise Architecture	AI Enterprise Architecture Framework
AI-driven IS Design	พัฒนาระบบ AI เป็นรายโครงการ	ขาดมาตรฐานการออกแบบและพัฒนา AI ระดับองค์กร	AI-driven IS Architecture
Adaptability & Agility	การปรับเปลี่ยนระบบใช้เวลาและทรัพยากร	ขาดสถาปัตยกรรมที่ยืดหยุ่น	Adaptive & Agile AI Architecture
Threat & Risk Responsiveness	มีการจัดการความเสี่ยงและ Security แยกส่วน	ขาดการเชื่อมโยง AI กับ Risk Management	AI Risk & Threat Architecture
AI Ethics & Responsibility	มีนโยบายด้านข้อมูลและ IT	ยังขาดกรอบ AI Ethics ที่ครอบคลุม	Responsible AI Governance

5.2.5.9 ความต้องการด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

จากการวิเคราะห์ช่องว่าง ผู้วิจัยสังเคราะห์ความต้องการออกเป็น 6 ประเด็น ได้แก่

1. EA–AI Integration ต้องสามารถเชื่อมโยง AI กับสถาปัตยกรรมองค์กรทั้ง 7 มิติ
2. Architectural Framework ต้องมีกรอบที่ใช้กำหนดองค์ประกอบ ความสัมพันธ์ และหลักการของ AI Architecture
3. AI-driven IS Design & Development ต้องมีแนวทางมาตรฐานสำหรับการออกแบบและพัฒนาระบบสารสนเทศที่ใช้ AI
4. Adaptability & Agility ต้องสามารถปรับเปลี่ยนสถาปัตยกรรมและโมเดล AI ตามสถานการณ์ได้
5. Threat & Risk Responsiveness ต้องสามารถเชื่อมโยง AI กับการบริหารความเสี่ยงและภูมิคุ้มกันดิจิทัล
6. AI Ethics & Responsibility ต้องมีกลไกกำกับการใช้ AI ให้มีความโปร่งใส ปลอดภัย เป็นธรรม และตรวจสอบได้

5.2.6 ด้านการจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)

การจัดการภูมิคุ้มกันดิจิทัลเป็นองค์ประกอบปลายทางที่มุ่งนำความสามารถด้าน Enterprise Architecture, Intelligent Technology และ Digital Immunity มาบูรณาการเพื่อให้สถาบันอุดมศึกษาสามารถบริหารความเสี่ยงและภัยคุกคามทางดิจิทัลได้อย่างเป็นระบบ

5.2.6.1 การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection)

เป็นความสามารถในการรวบรวมและวิเคราะห์ข้อมูลจากระบบเครือข่าย แอปพลิเคชัน อุปกรณ์ปลายทาง และกิจกรรมของผู้ใช้งาน เพื่อค้นหาเหตุการณ์หรือพฤติกรรมที่อาจเป็นภัยคุกคาม การนำ Machine Learning, Deep Learning และ Behavioral AI เข้ามาใช้ช่วยเพิ่มความสามารถในการตรวจจับรูปแบบความผิดปกติที่อาจไม่สามารถตรวจพบด้วยกฎแบบดั้งเดิม

5.2.6.2 การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response)

เป็นกระบวนการจัดการเหตุการณ์ตั้งแต่การรับแจ้ง การวิเคราะห์ การจำแนกระดับความรุนแรง การตอบสนอง การควบคุมผลกระทบ และการฟื้นฟูระบบ

5.2.6.3 การประเมินและจัดการความเสี่ยง (Risk Assessment and Management)

เป็นกระบวนการในการระบุ วิเคราะห์ ประเมิน และจัดการความเสี่ยงที่อาจส่งผลต่อข้อมูล ระบบสารสนเทศ และการดำเนินงานของสถาบัน

5.2.6.4 การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy)

การปกป้องข้อมูลและความเป็นส่วนตัวมุ่งให้ข้อมูลของนักศึกษา บุคลากร งานวิจัย และข้อมูลขององค์กรได้รับการจัดการอย่างเหมาะสมตลอดวงจรชีวิตข้อมูล

สถาปัตยกรรมเป้าหมายควรเชื่อมโยง Data Architecture, Security Architecture และ AI Architecture เพื่อควบคุมการเข้าถึง การใช้ การจัดเก็บ และการประมวลผลข้อมูล

5.2.6.5 การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย (Security Awareness Training)

บุคลากรและนักศึกษาเป็นองค์ประกอบสำคัญของภูมิคุ้มกันดิจิทัล ดังนั้นสถาบันจำเป็นต้องพัฒนาความรู้และทักษะด้าน Cybersecurity อย่างต่อเนื่อง ใน Target Architecture สามารถนำข้อมูลการอบรม ผลการประเมิน และข้อมูลเหตุการณ์มาวิเคราะห์เพื่อกำหนดรูปแบบการฝึกอบรมให้เหมาะสมกับระดับความเสี่ยงของแต่ละกลุ่มผู้ใช้งาน

5.2.6.6 นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance)

เป็นกลไกที่กำหนดหลักเกณฑ์ มาตรฐาน และแนวทางการปฏิบัติด้านความมั่นคงปลอดภัยขององค์กร รวมถึงการติดตามและประเมินการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง ในสถาปัตยกรรมเป้าหมาย Policy และ Compliance จะทำหน้าที่เป็นกลไกกำกับการดำเนินงานของระบบ Digital Immunity และ AI เพื่อให้การใช้เทคโนโลยีเป็นไปตามข้อกำหนดขององค์กรและกฎหมายที่เกี่ยวข้อง

5.2.6.7 ความสัมพันธ์กับกระบวนการธุรกิจ

ตารางที่ 5-27 ความสัมพันธ์กับกระบวนการธุรกิจ

องค์ประกอบ	กระบวนการธุรกิจ	เทคโนโลยี	ข้อมูล
Cyber Threat Detection	เฝ้าระวังและตรวจจับ	ML, DL, Behavioral AI, SIEM	Log, Network Traffic, Security Event
Incident Response	จัดการเหตุการณ์	SOAR, AI Analytics	Incident Data
Risk Assessment & Management	บริหารความเสี่ยง	AI Risk Analytics	Risk Data
Data Protection & Privacy	จัดการข้อมูล	Encryption, IAM, DLP	Personal/Sensitive Data
Security Awareness Training	พัฒนาบุคลากร	LMS, AI Analytics, NLP	Training Data
Security Policy & Compliance	กำกับและตรวจสอบ	GRC, AI Analytics	Policy, Audit, Compliance Data

5.2.6.8 การวิเคราะห์ช่องว่างด้านการจัดการภูมิคุ้มกันดิจิทัล

ตารางที่ 5-28 Digital Immunity Management Gap

ประเด็น	สภาพปัจจุบัน	ช่องว่าง	สถาปัตยกรรมเป้าหมาย
Cyber Threat Detection	มีระบบ Security Monitoring	ขาด AI-based Detection แบบบูรณาการ	AI Threat Detection
Incident Response	มีขั้นตอน Incident Response	การตอบสนองยังใช้บุคลากรในหลายขั้นตอน	Intelligent Incident Response
Risk Management	ประเมินความเสี่ยงตามกระบวนการ	ขาด Predictive Risk Analytics	AI-driven Risk Management
Data Protection	มีมาตรการป้องกันข้อมูล	การป้องกันข้อมูลยังแยกตามระบบ	Integrated Data Protection
Awareness Training	มีการอบรมตามรอบเวลา	ขาดการฝึกอบรมตามระดับความเสี่ยง	Adaptive Security Awareness
Policy & Compliance	มีนโยบายและข้อกำหนด	การติดตาม Compliance ยังมีข้อจำกัด	AI-enabled GRC & Compliance

5.3 การวิเคราะห์ปัจจัยภายใน ปัจจัยภายนอก และสภาพปัจจุบันของสถาบันอุดมศึกษา

จากการศึกษาปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา รวมถึงผลการวิเคราะห์แบบจำลองสมการโครงสร้าง (Structural Equation Modeling: SEM) และผลการวิเคราะห์สภาพปัจจุบันของสถาบันอุดมศึกษา ผู้วิจัยได้ดำเนินการวิเคราะห์บริบทภายในและภายนอกขององค์กร เพื่อใช้เป็นข้อมูลประกอบการกำหนดองค์ประกอบและทิศทางของสถาปัตยกรรมเป้าหมาย

การวิเคราะห์ดังกล่าวดำเนินการโดยบูรณาการเครื่องมือเชิงกลยุทธ์ 4 แนวทาง ได้แก่ 7-S Model สำหรับวิเคราะห์ปัจจัยภายในองค์กร PEST Model สำหรับวิเคราะห์ปัจจัยแวดล้อมภายนอก SWOT Analysis สำหรับสังเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค และ TOWS Matrix สำหรับกำหนดแนวทางเชิงกลยุทธ์จากความสัมพันธ์ระหว่างปัจจัยภายในและภายนอก

5.3.1 การวิเคราะห์ปัจจัยภายในตามหลัก 7-S Model

กรอบแนวคิด McKinsey 7-S Model ในการวิเคราะห์ปัจจัยภายในของสถาบันอุดมศึกษา เนื่องจากสามารถพิจารณาองค์ประกอบขององค์กรทั้งด้านโครงสร้าง กลยุทธ์ ระบบ บุคลากร ทักษะ รูปแบบการบริหาร และค่านิยมร่วม ซึ่งมีความเกี่ยวข้องโดยตรงกับความพร้อมในการเปลี่ยนผ่านสู่การเป็นองค์กรดิจิทัลและการนำ AI มาใช้ในระดับองค์กร

ตารางที่ 5-29 การวิเคราะห์ปัจจัยภายในตามกรอบ 7-S Model

องค์ประกอบ	สภาพปัจจุบันของสถาบันอุดมศึกษา	ประเด็นที่เกี่ยวข้องกับ AI และ Digital Immunity
Strategy	มีแผนยุทธศาสตร์และแผนพัฒนาดิจิทัล	จำเป็นต้องเชื่อมโยงยุทธศาสตร์ดิจิทัลกับ AI และภูมิคุ้มกันดิจิทัล
Structure	มีโครงสร้างบริหารและหน่วยงานด้าน IT/ดิจิทัล	การจัดการ AI และ Cybersecurity อาจกระจายอยู่หลายหน่วยงาน
Systems	มีระบบสารสนเทศสนับสนุนงานบริหาร การเรียน การวิจัย และบริการ	ระบบจำนวนมากต้องได้รับการบูรณาการและเชื่อมโยงข้อมูล
Staff	มีบุคลากรหลายกลุ่มที่เกี่ยวข้องกับระบบดิจิทัล	ต้องพัฒนาบุคลากรให้มี AI และ Cybersecurity Literacy
Skills	มีบุคลากรที่มีความรู้ด้าน IT และเทคโนโลยีในระดับหนึ่ง	ต้องเพิ่มทักษะ AI, Data Analytics และ Cybersecurity
Style	การบริหารมีทั้งการตัดสินใจระดับนโยบายและระดับหน่วยงาน	ต้องส่งเสริม Data-driven และ AI-assisted Decision Making
Shared Values	ให้ความสำคัญกับคุณภาพการศึกษา การบริการ และการพัฒนาองค์กร	ควรเพิ่มค่านิยมด้าน Digital Trust, Security และ Responsible AI

5.3.2 การวิเคราะห์ปัจจัยภายนอกตามหลัก PEST Model

กรอบ PEST Model เพื่อวิเคราะห์ปัจจัยแวดล้อมภายนอกที่มีผลต่อการพัฒนาและการนำ AI Enterprise Architecture มาใช้ในสถาบันอุดมศึกษา โดยพิจารณา 4 ด้าน ได้แก่ Political, Economic, Social และ Technological

ตารางที่ 5-30 การวิเคราะห์ปัจจัยภายนอกตาม PEST Model

ปัจจัย	สภาพแวดล้อมภายนอก	ผลกระทบต่อสถาบันอุดมศึกษา
Political	นโยบายภาครัฐด้าน Digital Transformation, AI, Cybersecurity และการคุ้มครองข้อมูล	สถาบันต้องปรับระบบและการกำกับดูแลให้สอดคล้องกับนโยบายและกฎระเบียบ
Economic	ข้อจำกัดด้านงบประมาณและต้นทุนเทคโนโลยี รวมถึงการแข่งขันระหว่างสถาบัน	จำเป็นต้องลงทุนเทคโนโลยีอย่างคุ้มค่าและกำหนดลำดับความสำคัญของโครงการ
Social	พฤติกรรมผู้เรียนและบุคลากรเปลี่ยนไป มีความคาดหวังต่อบริการดิจิทัล	ต้องพัฒนาบริการที่รวดเร็ว เข้าถึงง่าย และปลอดภัย
Technological	AI, Cloud, Big Data, IoT และ Cybersecurity พัฒนาอย่างรวดเร็ว	สถาบันต้องมีสถาปัตยกรรมที่ยืดหยุ่นและสามารถรองรับเทคโนโลยีใหม่

5.3.3 การวิเคราะห์ SWOT Analysis

จากผลการวิเคราะห์ 7-S Model และ PEST Model ผู้วิจัยนำข้อมูลมาสังเคราะห์เป็น SWOT Analysis เพื่อระบุจุดแข็ง (Strengths) จุดอ่อน (Weaknesses) โอกาส (Opportunities) และอุปสรรค (Threats) ที่เกี่ยวข้องกับการพัฒนา AI Enterprise Architecture

ตารางที่ 5-31 การวิเคราะห์ SWOT

ด้าน	ประเด็นสำคัญ
Strengths (S)	มีโครงสร้างการบริหารและระบบสารสนเทศพื้นฐาน มีบุคลากรที่มีความรู้ด้านเทคโนโลยี มีข้อมูลจากกระบวนการดำเนินงานจำนวนมาก และมีประสบการณ์ในการใช้ระบบดิจิทัล
Weaknesses (W)	ระบบและข้อมูลบางส่วนกระจายตามหน่วยงาน ขาดมาตรฐานการบูรณาการ AI ขาดบุคลากร AI เฉพาะทาง และกระบวนการบางส่วนยังพึ่งพาการดำเนินงานแบบ Manual
Opportunities (O)	เทคโนโลยี AI มีความก้าวหน้า การสนับสนุนจากนโยบายภาครัฐ การพัฒนา Cloud และ Data Platform และการเพิ่มขึ้นของความต้องการบริการดิจิทัล
Threats (T)	ภัยคุกคามทางไซเบอร์เพิ่มขึ้น ความเสี่ยงด้านข้อมูลส่วนบุคคล การเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็ว งบประมาณจำกัด และความเสี่ยงจากการใช้ AI อย่างไม่เหมาะสม

5.3.4 การวิเคราะห์ TOWS Matrix

จากากรนำผล SWOT Analysis มาวิเคราะห์ต่อด้วย TOWS Matrix เพื่อกำหนดแนวทางเชิงกลยุทธ์ที่สามารถนำไปใช้เป็นข้อกำหนดสำหรับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ตารางที่ 5-32 TOWS Matrix สำหรับสถาบันอุดมศึกษา

กลยุทธ์	แนวทาง
SO Strategy	ใช้ความพร้อมด้านระบบสารสนเทศ ข้อมูล และบุคลากร ร่วมกับโอกาสจาก AI และ Cloud เพื่อพัฒนา AI Enterprise Architecture ระดับองค์กร
ST Strategy	ใช้ความสามารถด้าน IT และข้อมูลของสถาบันเพื่อพัฒนาระบบ AI สำหรับตรวจจับภัยคุกคามและบริหารความเสี่ยง
WO Strategy	ใช้เทคโนโลยี AI, Cloud และแพลตฟอร์มดิจิทัลเพื่อแก้ปัญหาระบบที่กระจายตัวและเพิ่มประสิทธิภาพกระบวนการ
WT Strategy	พัฒนามาตรฐาน Governance, Security, Privacy และ AI Ethics เพื่อลดความเสี่ยงจากภัยคุกคามและข้อจำกัดด้านทรัพยากร

5.3.5 การสังเคราะห์ผลการวิเคราะห์เพื่อกำหนดข้อกำหนดของสถาปัตยกรรม

ผลการวิเคราะห์ทั้ง 7-S Model, PEST Model, SWOT และ TOWS สามารถสังเคราะห์เป็นข้อกำหนดสำหรับการออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ได้ดังนี้

ตารางที่ 5-33 การเชื่อมโยงผลการวิเคราะห์กับข้อกำหนดสถาปัตยกรรม

ผลการวิเคราะห์	ประเด็นที่พบ	ข้อกำหนดของสถาปัตยกรรม	องค์ประกอบ Target Architecture
7-S: Strategy	ต้องเชื่อมโยง AI กับยุทธศาสตร์องค์กร	Strategic AI Alignment	AI Enterprise Architecture
7-S: Structure	การบริหาร AI กระจายหลายหน่วยงาน	Integrated Governance	Governance Architecture
7-S: Systems	ระบบสารสนเทศหลายระบบ	Enterprise Integration	Integration Architecture
7-S: Staff/Skills	ทักษะ AI และ Cybersecurity ไม่เท่ากัน	AI & Cybersecurity Competency	Digital Immunity Management
PEST: Political	กฎระเบียบและนโยบายเพิ่มขึ้น	Policy & Compliance	Security/Governance
PEST: Economic	งบประมาณจำกัด	Cost-effective Architecture	Cloud/Shared Infrastructure
PEST: Social	ผู้ใช้ต้องการบริการดิจิทัล	Intelligent Digital Services	AI Applications
PEST: Technology	เทคโนโลยีเปลี่ยนแปลงรวดเร็ว	Adaptability & Agility	AI Enterprise Architecture
SWOT: Strength	มีระบบและข้อมูลจำนวนมาก	Data Integration	Data Architecture
SWOT: Weakness	ระบบกระจายตัว	System Integration	Integration Architecture
SWOT: Opportunity	AI และ Cloud พัฒนาเร็ว	AI Adoption	Intelligent Technology
SWOT: Threat	ภัยคุกคามไซเบอร์เพิ่มขึ้น	Proactive Defense	Digital Immunity
TOWS: SO	ใช้ทรัพยากรเดิมต่อยอด AI	AI-enabled Transformation	AI Enterprise Architecture
TOWS: ST	ใช้ AI รับมือภัยคุกคาม	AI Security	Digital Immunity
TOWS: WO	ใช้เทคโนโลยีแก้ข้อจำกัด	Intelligent Automation	Digital Enterprise Management
TOWS: WT	ลดความเสี่ยงและข้อจำกัด	AI Governance & Security	Governance Architecture

5.3.6 การสังเคราะห์สภาพแวดล้อมสู่การออกแบบสถาปัตยกรรมเป้าหมาย

จากการวิเคราะห์ปัจจัยภายในด้วย 7-S Model ปัจจัยภายนอกด้วย PEST Model และการสังเคราะห์ SWOT และ TOWS Matrix พบว่า การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สำหรับสถาบันอุดมศึกษาไม่ควรพิจารณาเฉพาะการเลือกเทคโนโลยี AI แต่ต้องพิจารณาความพร้อมขององค์กร ระบบ กระบวนการ ข้อมูล บุคลากร การกำกับดูแล และสภาพแวดล้อมภายนอกร่วมกัน ผลการวิเคราะห์นำไปสู่ข้อกำหนดเชิงสถาปัตยกรรมที่สำคัญ ได้แก่

1. สถาปัตยกรรมต้องสอดคล้องกับยุทธศาสตร์และโครงสร้างการบริหารของสถาบัน
2. สามารถบูรณาการข้อมูลและระบบสารสนเทศที่มีอยู่เดิมเข้ากับเทคโนโลยี AI
3. มีโครงสร้างพื้นฐานที่รองรับการประมวลผลข้อมูลและ AI และสามารถขยายได้ตามความต้องการ
4. สามารถนำ AI มาใช้ในการตรวจจับ วิเคราะห์ คาดการณ์ และตอบสนองต่อภัยคุกคาม
5. มี Governance ที่ครอบคลุมทั้งข้อมูล AI ความมั่นคงปลอดภัย และความเป็นส่วนตัว
6. มีความยืดหยุ่นและสามารถปรับตัวต่อการเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคาม
7. คำนึงถึงจริยธรรม ความโปร่งใส และความรับผิดชอบในการใช้ปัญญาประดิษฐ์

ตารางที่ 5-34 สรุปสำหรับเชื่อมเข้าสู่การออกแบบ Target Architecture

ระดับการวิเคราะห์	ผลลัพธ์	สิ่งที่นำไปออกแบบ
7-S Model	ความพร้อมและข้อจำกัดภายในองค์กร	Business, Governance, People, Skills
PEST Model	โอกาสและแรงกดดันจากภายนอก	Policy, Technology, Risk, Compliance
SWOT Analysis	จุดแข็ง จุดอ่อน โอกาส และอุปสรรค	Strategic Requirements
TOWS Matrix	ทางเลือกเชิงกลยุทธ์	Architecture Requirements
Organizational Structure	โครงสร้างองค์กร 7 มิติ	Business/Data/Application/Technology/Security/Integration/Governance
Intelligent Technology	ความสามารถของ AI	ML/DL/NLP/Behavioral AI
Digital Immunity	ความสามารถในการป้องกันและรับมือภัยคุกคาม	Detect/Analyze/Respond/Recover
Digital Enterprise Management	ความสามารถในการบริหารองค์กรดิจิทัล	Strategy/Data/Automation/Cybersecurity
AI Enterprise Architecture	กรอบบูรณาการ EA กับ AI	EA–AI Integration/AI Governance/AI-driven IS

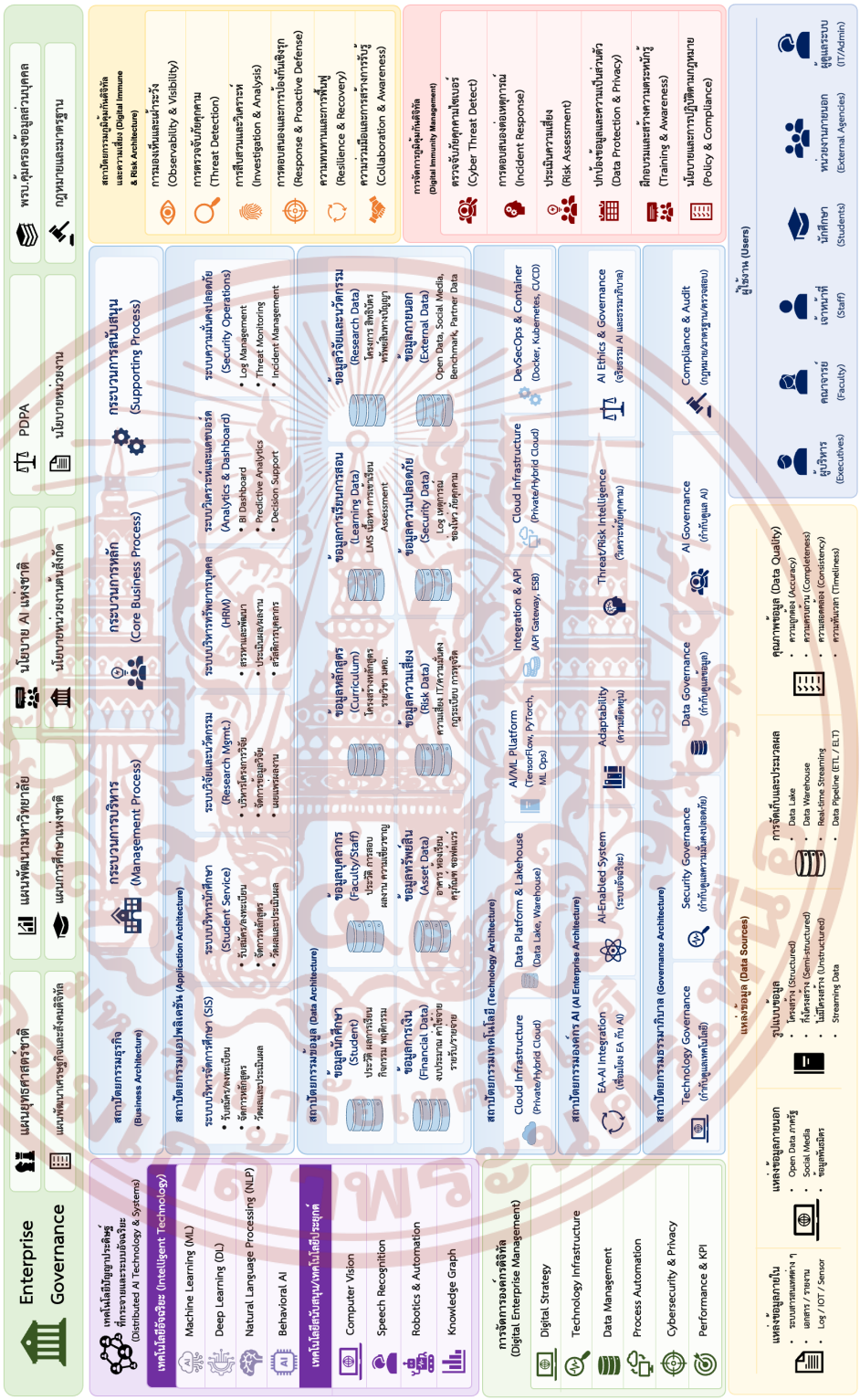
ระดับการวิเคราะห์	ผลลัพธ์	สิ่งที่นำไปออกแบบ
Digital Immunity Management	การบริหารภูมิคุ้มกันระดับองค์กร	Risk/Incident/Data Protection/Awareness/Compliance

5.3 การออกแบบสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

จากผลการศึกษาปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ผลการวิเคราะห์แบบจำลองสมการโครงสร้าง (Structural Equation Modeling: SEM) ตลอดจนผลการสำรวจและวิเคราะห์สภาพปัจจุบันของสถาบันอุดมศึกษาในบริบทของประเทศไทย ผู้วิจัยได้นำข้อมูลเชิงประจักษ์และองค์ความรู้ที่เกี่ยวข้องมาสังเคราะห์และบูรณาการเพื่อใช้เป็นพื้นฐานในการออกแบบสถาปัตยกรรมองค์กร โดยพิจารณาครอบคลุมกรอบงานสถาปัตยกรรมองค์กร 7 มิติ ได้แก่ ด้านธุรกิจ (Business) ด้านข้อมูล (Data) ด้านแอปพลิเคชัน (Application) ด้านเทคโนโลยี (Technology) ด้านความมั่นคงปลอดภัย (Security) ด้านการบูรณาการ (Integration) และด้านการกำกับดูแล (Governance) เพื่อสะท้อนความสัมพันธ์ระหว่างยุทธศาสตร์ กระบวนการดำเนินงาน ข้อมูล ระบบสารสนเทศ เทคโนโลยี ความมั่นคงปลอดภัย และการกำกับดูแลของสถาบันอุดมศึกษาอย่างเป็นระบบ ทั้งนี้ ผู้วิจัยได้ดำเนินการวิเคราะห์ปัจจัยภายในตามหลัก 7-S Model และปัจจัยภายนอกตามหลัก PEST Model เพื่อประเมินความพร้อม ศักยภาพ ข้อจำกัด และสภาพแวดล้อมที่มีอิทธิพลต่อการพัฒนาองค์กร จากนั้นนำผลการวิเคราะห์มาสังเคราะห์ด้วย SWOT Analysis และ TOWS Matrix เพื่อระบุจุดแข็ง จุดอ่อน โอกาส อุปสรรค และกำหนดแนวทางเชิงกลยุทธ์สำหรับการพัฒนาและปรับปรุงประสิทธิภาพขององค์กรควบคู่กับการศึกษาแผน ยุทธศาสตร์ นโยบาย และกรอบการดำเนินงานที่เกี่ยวข้องทั้งในระดับประเทศและระดับสถาบัน ตลอดจนพิจารณาการเปลี่ยนแปลงและแนวโน้มของเทคโนโลยีดิจิทัล โดยเฉพาะเทคโนโลยีปัญญาประดิษฐ์ การวิเคราะห์ข้อมูล ระบบคลาวด์ การเชื่อมโยงระบบสารสนเทศ และเทคโนโลยีด้านความมั่นคงปลอดภัย เพื่อให้สถาปัตยกรรมที่ออกแบบสามารถรองรับการเปลี่ยนแปลงทางเทคโนโลยีและภัยคุกคามทางดิจิทัลที่มีความซับซ้อนเพิ่มขึ้น ผลจากการบูรณาการผลการวิเคราะห์ดังกล่าวนำไปสู่การพัฒนา “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมุ่งให้สถาปัตยกรรมสามารถเชื่อมโยงยุทธศาสตร์ โครงสร้างองค์กร กระบวนการ ข้อมูล ระบบสารสนเทศ เทคโนโลยีอัจฉริยะ ความมั่นคงปลอดภัย การบูรณาการ และการกำกับดูแลเข้าด้วยกันอย่างเป็นระบบ รวมทั้งนำปัญญาประดิษฐ์มาใช้สนับสนุนการเฝ้าระวัง การตรวจจับ การวิเคราะห์ การตอบสนอง และการฟื้นฟูจากภัยคุกคามทาง

ดิจิทัล อันจะช่วยยกระดับความสามารถของสถาบันอุดมศึกษาในการบริหารจัดการความเสี่ยงและสร้างภูมิคุ้มกันดิจิทัลได้อย่างมีประสิทธิภาพและต่อเนื่อง โดยสถาปัตยกรรมที่พัฒนาขึ้นสามารถจำแนกองค์ประกอบเชิงระบบออกเป็น 6 ด้านหลักได้แก่ ด้านโครงสร้างองค์กร (Enterprise Architecture) ด้านเทคโนโลยีอัจฉริยะ (Intelligent Technology) ด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity) ด้านการจัดการองค์กรดิจิทัล (Digital Enterprise Management) ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (Artificial Intelligence Enterprise Architecture) และด้านการจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) ซึ่งแต่ละด้านมีองค์ประกอบและบทบาทที่แตกต่างกัน แต่ได้รับการออกแบบให้มีความสัมพันธ์เชื่อมโยงและเกื้อหนุนกันในลักษณะของระบบนิเวศดิจิทัลของสถาบันอุดมศึกษา โดยมีเป้าหมายเพื่อสนับสนุนการพัฒนาองค์กรให้สามารถใช้เทคโนโลยีปัญญาประดิษฐ์ได้อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความยืดหยุ่นและสามารถปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยีและภัยคุกคามดิจิทัลได้อย่างต่อเนื่องและยั่งยืน รายละเอียดองค์ประกอบและความสัมพันธ์ของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา แสดงดังภาพที่ 5-4

พระจอมเกล้าพระนครเหนือ มหาวิทยาลัยเทคโนโลยี



ภาพที่ 5-4 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา



ภาพที่ 5-5 ธรรมาภิบาลองค์กร

5.3.1 ธรรมาภิบาลองค์กร (Enterprise Governance)

ธรรมาภิบาลองค์กรเป็นกลไกการกำกับดูแลระดับองค์กรที่ทำหน้าที่กำหนดทิศทาง นโยบาย หลักเกณฑ์ มาตรฐาน และกรอบการดำเนินงานสำหรับการพัฒนาสถาบันอุดมศึกษาไปสู่องค์กรดิจิทัล และองค์กรที่ใช้ปัญญาประดิษฐ์ โดยเป็นชั้นบนสุดของสถาปัตยกรรม ทำหน้าที่กำหนดกรอบให้ทุกองค์ประกอบของสถาปัตยกรรมดำเนินงานไปในทิศทางเดียวกัน และสอดคล้องกับกฎหมาย แผนยุทธศาสตร์ และนโยบายที่เกี่ยวข้อง โดยสามารถจัดการด้านความเสี่ยงและการใช้ทรัพยากรด้วยความรับผิดชอบ ประกอบด้วย 3 ประเด็นหลัก ดังนี้

1. แผนและนโยบายระดับชาติ ประกอบด้วย
    1.1 แผนยุทธศาสตร์ชาติ
    1.2 แผนพัฒนาเศรษฐกิจและสังคมดิจิทัล
    1.3 แผนการศึกษาแห่งชาติ
    1.4 นโยบายปัญญาประดิษฐ์แห่งชาติ
2. แผนและนโยบายระดับสถาบัน ประกอบด้วย
    2.1 แผนพัฒนามหาวิทยาลัย
    2.2 แผนยุทธศาสตร์มหาวิทยาลัย
    2.3 นโยบายของหน่วยงานต้นสังกัด
    2.4 นโยบายของผู้บริหาร
3. กฎหมาย มาตรฐานและระเบียบข้อบังคับ (Regulatory Compliance) ประกอบด้วย
    3.1 กฎหมายเพื่อความมั่นคงปลอดภัยข้อมูล (Information Security Laws)
        3.1.1 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
        3.1.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
        3.1.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
        3.1.4 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
        3.1.5 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

3.1.6 พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565

3.1.7 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และที่แก้ไขเพิ่มเติม

3.1.8 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

3.1.9 พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563

3.1.10 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. 2562

3.1.11 กฎหมายเฉพาะด้านที่เกี่ยวข้องกับหน่วยงาน

3.2 นโยบายการรักษาความมั่นคงปลอดภัยข้อมูล ประกอบด้วย

3.2.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

3.2.2 นโยบายการกำกับดูแลข้อมูล

3.2.3 นโยบายการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว

3.2.4 นโยบายการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

3.2.5 นโยบายการรักษาความมั่นคงปลอดภัยเครือข่ายและโครงสร้างพื้นฐานดิจิทัล

3.2.6 นโยบายการสำรองและกู้คืนข้อมูล

3.2.7 นโยบายการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

3.2.8 นโยบายการบริหารความเสี่ยงด้านสารสนเทศและไซเบอร์

3.2.9 นโยบายการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม

3.2.10 นโยบายการรักษาความมั่นคงปลอดภัยสำหรับการใช้บริการ Cloud

3.2.11 นโยบายการบริหารจัดการผู้ให้บริการและบุคคลภายนอก

3.2.12 นโยบายการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

3.2.13 นโยบายการใช้ปัญญาประดิษฐ์อย่างมีความรับผิดชอบ

3.2.14 นโยบายการจัดการข้อมูลสำหรับปัญญาประดิษฐ์

3.2.15 นโยบายการบริหารความต่อเนื่องทางธุรกิจและการฟื้นฟูระบบ

3.3 ข้อกำหนดและแนวปฏิบัติเพื่อความมั่นคงปลอดภัยข้อมูล

3.3.1 การรักษาความมั่นคงปลอดภัยทางไซเบอร์

3.3.2 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.3.3 การจัดการความเสี่ยง

3.3.4 ธรรมาภิบาลข้อมูล

3.3.5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

3.3.6 การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

3.3.7 การสำรองข้อมูลและการฟื้นฟูระบบ

3.3.8 ข้อกำหนดการใช้สื่อสังคมออนไลน์ในการทำงาน

3.3.9 แนวปฏิบัติการใช้อุปกรณ์ส่วนตัวในการทำงาน

3.3.10 แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างปลอดภัยและมีความรับผิดชอบ

3.4 มาตรฐานเพื่อความมั่นคงปลอดภัยข้อมูล

3.4.1 มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563

3.4.2 มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563

3.4.3 มาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน 3.0 (มสพร. 11-2566)

3.4.4 มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001



ภาพที่ 5-6 โครงสร้างองค์กร

5.3.2 โครงสร้างองค์กร (Organizational Structure)

5.3.2.1 สถาปัตยกรรมธุรกิจ (Business Architecture)

เป็นส่วนที่อธิบายว่าสถาบันอุดมศึกษาดำเนินงานอะไร และดำเนินงานอย่างไร เพื่อให้บรรลุยุทธศาสตร์และพันธกิจ แบ่งกระบวนการธุรกิจออกเป็น 3 กลุ่ม ได้แก่

1. กระบวนการบริหาร (Management Process) ประกอบด้วย

1.1 การวางแผนยุทธศาสตร์

1.2 การบริหารงบประมาณ

1.3 การบริหารทรัพยากร

1.4 การบริหารความเสี่ยง

1.5 การกำกับติดตามและประเมินผล

2. กระบวนการหลัก (Core Business Process)

เป็นกระบวนการที่เกี่ยวข้องโดยตรงกับพันธกิจของสถาบัน ประกอบด้วย

2.1 การจัดการเรียนการสอน

2.2 การผลิตบัณฑิต

2.3 การวิจัย

2.4 การบริการวิชาการ

2.5 การทำนุบำรุงศิลปวัฒนธรรม

3. กระบวนการสนับสนุน (Supporting Process)

เป็นกระบวนการที่สนับสนุนการดำเนินงานหลัก ประกอบด้วย

3.1 การบริหารบุคลากร

3.2 การเงินและบัญชี

3.3 งานพัสดุ

3.4 เทคโนโลยีสารสนเทศ

3.5 งานธุรการ

3.6 งานอาคารสถานที่

5.3.2.2 สถาปัตยกรรมแอปพลิเคชัน (Application Architecture)

เป็นส่วนที่กำหนดระบบสารสนเทศและแอปพลิเคชันที่สนับสนุนกระบวนการดำเนินงานของสถาบันอุดมศึกษา ประกอบด้วยระบบสำคัญ 6 กลุ่ม ได้แก่

1. ระบบบริหารจัดการการศึกษา (SIS)

1.1 รับสมัคร/ลงทะเบียน

1.2 จัดการหลักสูตร

1.3 วัดผลและประเมินผล

2. ระบบบริการนักศึกษา (Student Service)

2.1 ทุนการศึกษา/สวัสดิการ

2.2 แนะแนว/ให้คำปรึกษา

2.3 กิจกรรมนักศึกษา

3. ระบบวิจัยและนวัตกรรม (Research Management)

3.1 บริหารโครงการวิจัย

3.2 จัดการข้อมูลวิจัย

3.3 แผยแพร่ผลงานวิจัย

4. ระบบบริหารทรัพยากรบุคคล (HRM)

4.1 สรรหาและพัฒนา

4.2 ประเมินผลการปฏิบัติงาน

4.3 สวัสดิการบุคลากร

5. ระบบวิเคราะห์และแดชบอร์ด (Analytics & Dashboard) ประกอบด้วย

5.1 BI Dashboard

5.2 Predictive Analytics

5.3 Decision Support

6. ระบบความมั่นคงปลอดภัย (Security Operations) ประกอบด้วย

6.1 Log Management

6.2 Threat Monitoring

6.3 Incident Management

5.3.2.3 สถาปัตยกรรมข้อมูล (Data Architecture)

เป็นโครงสร้างที่กำหนดว่าองค์กรมีข้อมูลอะไร ข้อมูลอยู่ที่ใด ถูกจัดเก็บและบริหารอย่างไร และนำข้อมูลไปใช้ประโยชน์อย่างไร แบ่งข้อมูลหลักออกเป็น 10 กลุ่ม ได้แก่

1. ข้อมูลนักศึกษา (Student Data) ประวัติการศึกษา กิจกรรม และพฤติกรรม

2. ข้อมูลบุคลากร (Faculty/Staff Data) ประวัติการทำงานและความเชี่ยวชาญ

3. ข้อมูลหลักสูตร (Curriculum Data) โครงสร้างหลักสูตร รายวิชา และรายละเอียดรายวิชา

4. ข้อมูลการเรียนการสอน (Learning Data) LMS, ผลการเรียน และ Assessment

5. ข้อมูลวิจัยและนวัตกรรม (Research Data) โครงการวิจัย ผลงาน และทรัพย์สินทางปัญญา

6. ข้อมูลการเงิน (Financial Data) งบประมาณ ค่าใช้จ่าย และรายรับ/รายจ่าย

7. ข้อมูลทรัพย์สิน (Asset Data) อาคาร ห้องเรียน และครุภัณฑ์

8. ข้อมูลความเสี่ยง (Risk Data) ความเสี่ยงด้าน IT ความเสี่ยงด้านการดำเนินงาน และเหตุการณ์ความเสี่ยง

9. ข้อมูลความปลอดภัย (Security Data) Log, เหตุการณ์ด้านความปลอดภัย และข้อมูลภัยคุกคาม

10. ข้อมูลภายนอก (External Data) Open Data, social media, Benchmark และ Partner Data

5.3.2.4 สถาปัตยกรรมเทคโนโลยี (Technology Architecture)

เป็นโครงสร้างพื้นฐานทางเทคโนโลยีที่ใช้รองรับ Application, Data และ AI ประกอบด้วย 6 ส่วน ได้แก่

1. โครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure) ประกอบด้วย

1.1 Private Cloud

1.2 Hybrid Cloud

2. แพลตฟอร์มข้อมูลและ Data Lakehouse (Data Platform & Lakehouse) ประกอบด้วย

2.1 Data Lake

2.2 Data Warehouse

3. แพลตฟอร์มปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง (AI/ML Platform) ประกอบด้วย

3.1 TensorFlow

3.2 PyTorch

3.3 ML Ops

4. Integration & API ประกอบด้วย

4.1 API Gateway

4.2 ESB

5. Network & Edge Computing ประกอบด้วย

5.1 5G

5.2 IoT

5.3 Edge

5.4 CDN

6. DevSecOps & Container ประกอบด้วย

6.1 Docker

6.2 Kubernetes

6.3 Continuous Integration/Continuous Delivery

5.3.2.5 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) ประกอบด้วย

1. EA–AI Integration การบูรณาการสถาปัตยกรรมองค์กร กับปัญญาประดิษฐ์ เพื่อให้ AI ไม่ได้ทำงานเป็นระบบแยกส่วน แต่เป็นส่วนหนึ่งของกระบวนการและสถาปัตยกรรมองค์กร

2. Architectural Framework ประกอบด้วย

2.1 หลักการและแนวทางสถาปัตยกรรม (Architecture Principles)

2.2 ชั้นสถาปัตยกรรม (Architecture Layers)

2.3 การบูรณาการ AI (AI Integration)

2.4 กรอบการเปลี่ยนผ่านจาก Current สู่ Target Architecture

2.5 กลไกการกำกับดูแลและประเมินผล

3. AI-Enabled System ประกอบด้วย

3.1 Predictive Analytics

3.2 Intelligent Decision Support

3.3 Automated Detection

3.4 Intelligent Recommendation

4. Adaptability ประกอบด้วย

4.1 การเปลี่ยนแปลงของเทคโนโลยี

4.2 รูปแบบภัยคุกคามใหม่

4.3 ความต้องการของผู้ใช้

4.4 การเปลี่ยนแปลงเชิงนโยบาย

5. Threat/Risk Intelligence ประกอบด้วย

5.1 วิเคราะห์รูปแบบการโจมตี

5.2 ตรวจจับพฤติกรรมผิดปกติ

5.3 วิเคราะห์แนวโน้มภัยคุกคาม

5.4 ประเมินระดับความเสี่ยง

6. AI Ethics & Governance ประกอบด้วย

6.1 ความโปร่งใส

6.2 ความรับผิดชอบ

6.3 ความเป็นธรรม

6.4 การคุ้มครองข้อมูล

6.5 การตรวจสอบได้

5.3.2.6 สถาปัตยกรรมธรรมาภิบาล (Governance Architecture) ประกอบด้วย

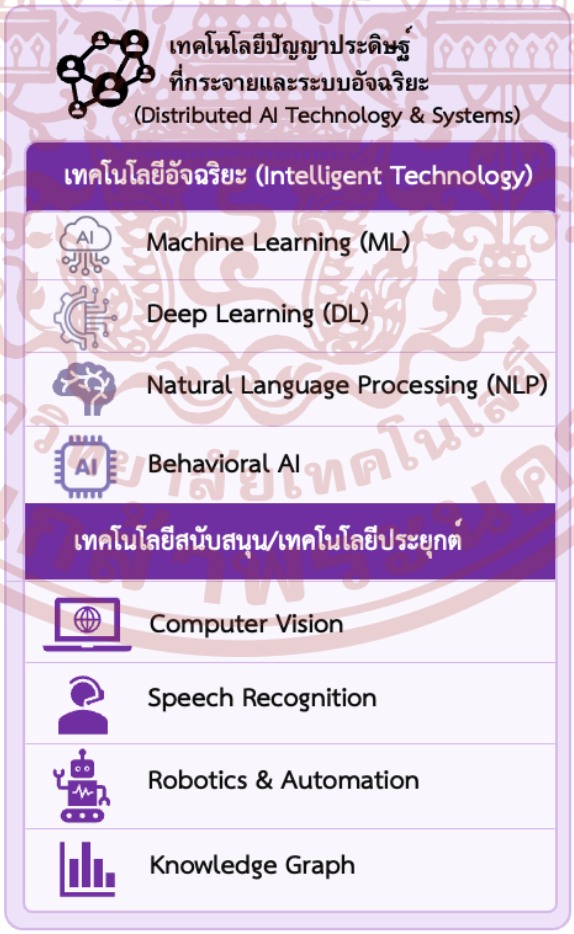
1. Technology Governance กำกับดูแลเทคโนโลยีและมาตรฐานทางเทคนิค

2. Security Governance กำกับดูแลความมั่นคงปลอดภัย

3. Data Governance กำกับดูแลคุณภาพ สิทธิ์ และการใช้ข้อมูล

4. AI Governance กำกับดูแลการพัฒนาและการใช้ AI

5. Compliance & Audit กำกับให้การดำเนินงานเป็นไปตามกฎหมาย มาตรฐาน และสามารถตรวจสอบได้



ภาพที่ 5-7 เทคโนโลยีปัญญาประดิษฐ์ที่กระจาย และระบบอัจฉริยะ

5.3.3 เทคโนโลยีปัญญาประดิษฐ์ที่กระจาย และระบบอัจฉริยะ (Intelligent Technology) ประกอบด้วย

5.3.3.1 เทคโนโลยีอัจฉริยะ

1. Machine Learning (ML)
2. Deep Learning (DL)
3. Natural Language Processing (NLP)
4. Behavioral AI

5.3.3.2 เทคโนโลยีสนับสนุน/เทคโนโลยีประยุกต์

1. Computer Vision
2. Speech Recognition
3. Robotics & Automation
4. Knowledge Graph



ภาพที่ 5-8 การจัดการองค์กรดิจิทัล

5.3.4 การจัดการองค์กรดิจิทัล (Digital Enterprise Management)

เป็นแนวทางการบริหารจัดการสถาบันอุดมศึกษาโดยประยุกต์ใช้เทคโนโลยีดิจิทัล ข้อมูล ระบบสารสนเทศ และระบบอัตโนมัติ เพื่อเพิ่มประสิทธิภาพของกระบวนการดำเนินงาน สนับสนุนการตัดสินใจ ยกระดับการให้บริการ และสร้างความสามารถในการปรับตัวต่อการเปลี่ยนแปลงของ

สภาพแวดล้อมทางดิจิทัล โดยมุ่งให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพ เชื่อมโยงข้อมูลและกระบวนการระหว่างหน่วยงาน และมีความพร้อมต่อการประยุกต์ใช้ปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลประกอบด้วย

1. Digital Strategy — กลยุทธ์ดิจิทัล
2. Technology Infrastructure — โครงสร้างพื้นฐานเทคโนโลยี
3. Data Management — การจัดการข้อมูล
4. Process Automation — การทำให้กระบวนการเป็นอัตโนมัติ
5. Cybersecurity & Privacy — ความมั่นคงปลอดภัยและความเป็นส่วนตัว
6. Performance & KPI — การวัดผลและตัวชี้วัด



ภาพที่ 5-9 สถาปัตยกรรมภูมิคุ้มกันดิจิทัลและความเสี่ยง

5.3.5 สถาปัตยกรรมภูมิคุ้มกันดิจิทัลและความเสี่ยง (Digital Immunity & Risk Architecture)

เป็นชั้นสถาปัตยกรรมที่ทำหน้าที่ ป้องกัน ลดผลกระทบ และเพิ่มความสามารถของสถาบันอุดมศึกษาในการรับมือกับภัยคุกคาม ความเสี่ยง และเหตุการณ์ผิดปกติทางดิจิทัล โดยเชื่อมโยงข้อมูลจากสถาปัตยกรรมธุรกิจ ข้อมูล แอปพลิเคชัน เทคโนโลยี และการกำกับดูแล เข้ากับกลไกด้านความมั่นคงปลอดภัย การบริหารความเสี่ยง และเทคโนโลยีปัญญาประดิษฐ์ เพื่อให้สถาบันสามารถ มองเห็น ตรวจจับ วิเคราะห์ ตอบสนอง ฟื้นฟู และเรียนรู้จากเหตุการณ์ ได้อย่างต่อเนื่อง

ในบริบทของสถาบันอุดมศึกษา ชั้นสถาปัตยกรรมนี้มีความสำคัญเนื่องจากสถาบันมีระบบสารสนเทศและข้อมูลจำนวนมาก เช่น ข้อมูลนักศึกษา บุคลากร งานวิจัย การเงิน ทรัพย์สินทางปัญญา และข้อมูลส่วนบุคคล ซึ่งมีการเชื่อมโยงระหว่างระบบภายในและหน่วยงานภายนอก ดังนั้นการจัดการภูมิคุ้มกันดิจิทัลจึงจำเป็นต้องพัฒนาจากแนวทางการป้องกันเพียงอย่างเดียวไปสู่การบริหารความเสี่ยงเชิงรุกและการตอบสนองแบบอัจฉริยะ สามารถแบ่งองค์ประกอบออกเป็น 6 องค์ประกอบหลัก ดังนี้

5.3.5.1 การมองเห็นและเฝ้าระวัง (Observability & Visibility)

เป็นความสามารถพื้นฐานในการสร้างการมองเห็นสถานะของระบบดิจิทัลและทรัพยากรสารสนเทศของสถาบันอย่างต่อเนื่อง เพื่อให้ทราบถึงสถานะ ประสิทธิภาพ และกิจกรรมที่เกิดขึ้นภายในระบบ ประกอบด้วย

1. System Monitoring
2. Network Monitoring
3. Application Monitoring
4. Endpoint Monitoring
5. Log Management
6. Security Monitoring
7. Asset Visibility
8. User Activity Monitoring
9. Security Dashboard
10. Real-time Monitoring

เทคโนโลยีที่สนับสนุน คือ

1. SIEM
2. Observability Platform
3. Log Analytics
4. Machine Learning
5. Behavioral AI

6. Cloud Monitoring

5.3.5.2 การตรวจจับภัยคุกคาม (Threat Detection)

เป็นความสามารถในการระบุและตรวจจับพฤติกรรม เหตุการณ์ หรือรูปแบบการใช้งานที่มีแนวโน้มเป็นภัยคุกคามทางไซเบอร์ โดยอาศัยข้อมูลจากระบบเฝ้าระวังและข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัย ประกอบด้วย

1. Anomaly Detection
2. Intrusion Detection
3. Malware Detection
4. Phishing Detection
5. Account Compromise Detection
6. Insider Threat Detection
7. Threat Intelligence
8. Behavioral Analysis

เทคโนโลยีที่สนับสนุน คือ

1. Machine Learning
2. Deep Learning
3. Behavioral AI
4. Threat Intelligence Platform
5. SIEM
6. IDS/IPS

5.3.5.3 การสืบสวนและวิเคราะห์ (Investigation & Analysis)

เป็นความสามารถในการวิเคราะห์เหตุการณ์และข้อมูลที่ตรวจพบ เพื่อระบุสาเหตุ ลักษณะ ขอบเขต ผลกระทบ และความสัมพันธ์ของภัยคุกคาม รวมถึงสนับสนุนการตัดสินใจของผู้รับผิดชอบ ประกอบด้วย

1. Incident Investigation
2. Log Analysis
3. Threat Analysis
4. Root Cause Analysis
5. Digital Forensics
6. Attack Pattern Analysis
7. Risk Analysis

8. Threat Correlation

เทคโนโลยีที่สนับสนุน คือ

1. AI/ML Analytics
2. NLP
3. Knowledge Graph
4. Threat Intelligence
5. Big Data Analytics
6. Security Analytics

5.3.5.4 การตอบสนองและการป้องกันเชิงรุก (Response & Proactive Defense) เป็นความสามารถในการดำเนินการตอบสนองต่อเหตุการณ์ที่ตรวจพบ รวมถึงการป้องกันภัยคุกคามก่อนที่จะสร้างผลกระทบต่อระบบและข้อมูล ประกอบด้วย

1. Incident Response
2. Incident Containment
3. Automated Response
4. Vulnerability Management
5. Patch Management
6. Threat Hunting
7. Security Policy Enforcement
8. Proactive Defense
9. Security Orchestration

เทคโนโลยีที่สนับสนุน คือ

1. SOAR
2. AI-enabled Security Automation
3. Machine Learning
4. Behavioral AI
5. Threat Intelligence
6. Zero Trust Security

5.3.5.5 ความทนทานและการฟื้นฟู (Resilience & Recovery) เป็นความสามารถในการรักษาความต่อเนื่องของการดำเนินงานและฟื้นฟูระบบข้อมูล และบริการสำคัญหลังเกิดเหตุการณ์หรือภัยคุกคาม ประกอบด้วย

1. Business Continuity

2. Disaster Recovery
3. Backup & Recovery
4. High Availability
5. Redundancy
6. Failover
7. Recovery Planning
8. Crisis Management

เทคโนโลยีที่สนับสนุน คือ

1. Cloud Infrastructure
2. Backup System
3. Disaster Recovery Platform
4. High Availability
5. Replication
6. AI-based Predictive Analytics

5.3.5.6 ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Collaboration & Cybersecurity Awareness)

เป็นความสามารถด้านบุคลากรและองค์กรที่สนับสนุนให้ทุกภาคส่วนมีความรู้ ความตระหนัก และมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยของสถาบัน ประกอบด้วย

1. Cybersecurity Awareness
2. Security Awareness Training
3. Cybersecurity Training
4. Phishing Awareness
5. Incident Communication
6. Collaboration
7. Knowledge Sharing
8. Security Culture
9. Roles & Responsibilities

เทคโนโลยีที่สนับสนุน คือ

1. Learning Management System
2. AI Chatbot
3. NLP

4. Generative AI

5. Behavioral AI

6. Cybersecurity Simulation



ภาพที่ 5-10 การจัดการภูมิคุ้มกันดิจิทัล

5.3.6 การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)

กระบวนการบริหารจัดการความสามารถของสถาบันอุดมศึกษาในการป้องกัน ตรวจจับ ประเมิน ตอบสนอง ลดผลกระทบ และฟื้นฟูจากภัยคุกคามและความเสี่ยงทางดิจิทัล โดยอาศัยการบูรณาการด้านนโยบาย กระบวนการ บุคลากร ข้อมูล เทคโนโลยีปัญญาประดิษฐ์ และระบบความมั่นคงปลอดภัยเข้าด้วยกัน เพื่อให้สถาบันสามารถดำเนินพันธกิจทางการศึกษา การวิจัย การบริการวิชาการ และการบริหารจัดการได้อย่างต่อเนื่องและปลอดภัย ประกอบด้วย 6 องค์ประกอบหลัก ดังนี้

5.3.6.1 การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection)

เป็นกระบวนการในการเฝ้าระวัง ตรวจสอบ และระบุภัยคุกคามหรือกิจกรรมที่มีความผิดปกติ ซึ่งอาจส่งผลกระทบต่อระบบสารสนเทศ เครือข่าย แอปพลิเคชัน ข้อมูล และผู้ใช้งานของสถาบัน ประกอบด้วย

1. การเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัย
2. การตรวจจับความผิดปกติ
3. การวิเคราะห์พฤติกรรมผู้ใช้งาน
4. การตรวจจับ Malware และ Phishing
5. การตรวจจับการเข้าถึงระบบที่ผิดปกติ
6. Threat Intelligence
7. Security Monitoring

เทคโนโลยีที่สนับสนุน คือ

1. Machine Learning
2. Deep Learning
3. Behavioral AI
4. Anomaly Detection

5.3.6.2 การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response)

เป็นกระบวนการดำเนินการเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย โดยมุ่งควบคุมเหตุการณ์ ลดขอบเขตความเสียหาย และทำให้ระบบสามารถกลับมาดำเนินงานได้ตามปกติ ประกอบด้วย

1. Incident Identification
2. Incident Triage
3. Incident Containment
4. Incident Eradication
5. Incident Recovery
6. Incident Communication
7. Post-Incident Review

5.3.6.3 การประเมินและจัดการความเสี่ยง (Risk Assessment and Management)

เป็นกระบวนการระบุ ประเมิน วิเคราะห์ จัดลำดับ และควบคุมความเสี่ยงที่อาจส่งผลกระทบต่อทรัพย์สินดิจิทัล ข้อมูล ระบบสารสนเทศ และพันธกิจของสถาบัน ประกอบด้วย

1. Risk Identification
2. Risk Assessment
3. Risk Analysis
4. Risk Prioritization
5. Risk Treatment

6. Risk Monitoring

7. Risk Reporting

5.3.6.4 การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy)

เป็นการบริหารจัดการข้อมูลของสถาบันตลอดวงจรชีวิต เพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล รวมถึงการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

1. Data Classification

2. Access Control

3. Encryption

4. Data Loss Prevention

5. Privacy Management

6. Data Backup

7. Data Retention

8. Data Access Monitoring

9. Personal Data Protection

5.3.6.5. การฝึกอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัย (Security Awareness Training)

เป็นกระบวนการพัฒนาความรู้ ทักษะ และความตระหนักของผู้บริหาร บุคลากร อาจารย์ นักศึกษา และผู้ปฏิบัติงานที่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติตนได้อย่างปลอดภัยและลดความเสี่ยงจากปัจจัยมนุษย์ ประกอบด้วย

1. Cybersecurity Awareness

2. Phishing Awareness

3. Security Training

4. Incident Reporting Training

5. Data Privacy Training

6. Secure Password Practices

7. Social Engineering Awareness

8. Cybersecurity Simulation

5.3.6.6. นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance)

เป็นกลไกในการกำหนดนโยบาย หลักเกณฑ์ มาตรฐาน และข้อกำหนดด้านความมั่นคงปลอดภัย รวมถึงติดตามให้หน่วยงานและผู้ใช้งานปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง ประกอบด้วย

1. Security Policy
2. Cybersecurity Policy
3. Data Protection Policy
4. Privacy Policy
5. Access Control Policy
6. Incident Response Policy
7. AI Governance
8. Compliance Monitoring
9. Audit
10. Regulatory Compliance



ภาพที่ 5-11 แหล่งข้อมูล

5.3.7 แหล่งข้อมูล (Data Sources)

เป็นองค์ประกอบพื้นฐานของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ทำหน้าที่เป็นแหล่งกำเนิดข้อมูลสำหรับสนับสนุนการดำเนินงาน การวิเคราะห์ การตรวจจับภัยคุกคาม การประเมินความเสี่ยง การตัดสินใจ และการพัฒนาระบบปัญญาประดิษฐ์ โดยข้อมูลจากแหล่งต่าง ๆ จะถูกนำมารวบรวม เชื่อมโยง จัดเก็บ และประมวลผลภายใต้หลักธรรมาภิบาลข้อมูล ความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

5.3.7.1 แหล่งข้อมูลภายใน

1. ระบบสารสนเทศต่าง ๆ
2. ฐานข้อมูล
3. Log
4. IoT/Sensor

5.3.7.2 แหล่งข้อมูลภายนอก

1. Open Data ภาครัฐ
2. Social Media
3. ข้อมูลพันธมิตร

5.3.7.3 รูปแบบข้อมูล

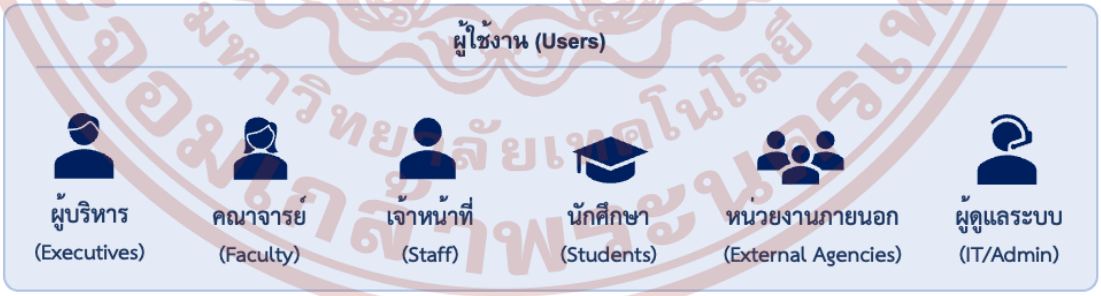
1. Structured
2. Semi-structured
3. Unstructured
4. Streaming Data

5.3.7.4 การจัดเก็บและประมวลผล

1. Data Lake
2. Data Warehouse
3. Real-time Streaming
4. Data Pipeline / ETL/ELT

5.3.7.5 คุณภาพข้อมูล

1. ความถูกต้อง (Accuracy)
2. ความครบถ้วน (Completeness)
3. ความสอดคล้อง (Consistency)
4. ความทันเวลา (Timeliness)



ภาพที่ 5-12 ผู้ใช้งาน

5.3.8 ผู้ใช้งาน (Users)

เป็นองค์ประกอบสำคัญของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา เนื่องจากผู้ใช้งานเป็นทั้งผู้ใช้บริการดิจิทัล ผู้สร้างข้อมูล ผู้มีส่วนเกี่ยวข้องกับกระบวนการทางธุรกิจ และเป็นปัจจัยสำคัญต่อความมั่นคงปลอดภัยขององค์กร ดังนั้น การออกแบบสถาปัตยกรรมจึงต้องคำนึงถึงบทบาท ความต้องการ สิทธิในการเข้าถึงข้อมูล และระดับ

ความรับผิดชอบของผู้ใช้งานแต่ละกลุ่ม เพื่อให้การใช้เทคโนโลยีปัญญาประดิษฐ์และระบบดิจิทัลเป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และสอดคล้องกับหลักธรรมาภิบาล ประกอบด้วย

1. ผู้บริหาร (Executives)
2. คณาจารย์ (Faculty)
3. เจ้าหน้าที่ (Staff)
4. นักศึกษา (Students)
5. หน่วยงานภายนอก (External Agencies)
6. ผู้ดูแลระบบ (IT/Admin)

5.4 ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา จากผู้เชี่ยวชาญ จำนวน 9 ท่าน รายละเอียดดังตารางที่ 5-35

ตารางที่ 5-35 ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

รายการประเมิน	ระดับความคิดเห็น		
	$\bar{x}$	S.D.	ความเหมาะสม
1. ธรรมาภิบาลองค์กร (Enterprise Governance)			
1.1 ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561–2580)	4.78	0.44	มากที่สุด
1.2 ยุทธศาสตร์หลักระยะยาว 20 ปี ของประเทศไทย (พ.ศ.2561-2580)	4.89	0.33	มากที่สุด
1.3 แผนการศึกษาแห่งชาติ พ.ศ. 2560–2579	5.00	0.00	มากที่สุด
1.4 แผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (พ.ศ. 2565–2570)	4.89	0.33	มากที่สุด
1.5 วิสัยทัศน์ พันธกิจ เป้าหมาย กลยุทธ์	4.89	0.33	มากที่สุด
1.6 กฎหมายเพื่อความมั่นคงปลอดภัยข้อมูล	4.89	0.33	มากที่สุด
1.7 นโยบายการรักษาความมั่นคงปลอดภัยข้อมูล	4.89	0.33	มากที่สุด
1.8 ข้อกำหนดและแนวปฏิบัติเพื่อความมั่นคงปลอดภัยข้อมูล	5.00	0.00	มากที่สุด
1.9 มาตรฐานเพื่อความมั่นคงปลอดภัยข้อมูล	4.89	0.33	มากที่สุด
2. สถาปัตยกรรมธุรกิจ (Business Architecture)			
2.1 กระบวนการบริหาร (Management Process)	4.89	0.33	มากที่สุด

รายการประเมิน	ระดับความคิดเห็น		
	$\bar{x}$	S.D.	ความเหมาะสม
2.2 กระบวนการหลัก (Core Business Process)	4.89	0.33	มากที่สุด
2.3 กระบวนการสนับสนุน (Supporting Process)	4.89	0.33	มากที่สุด
3. สถาปัตยกรรมแอปพลิเคชัน (Application Architecture)			
3.1 ระบบบริหารจัดการการศึกษา (SIS)	4.78	0.44	มากที่สุด
3.2 ระบบบริการนักศึกษา (Student Service)	4.89	0.33	มากที่สุด
3.3 ระบบวิจัยและนวัตกรรม (Research Management)	4.89	0.33	มากที่สุด
3.4 ระบบบริหารทรัพยากรบุคคล (HRM)	4.89	0.33	มากที่สุด
3.5 ระบบวิเคราะห์และแดชบอร์ด (Analytics & Dashboard)	4.89	0.33	มากที่สุด
3.6 ระบบความมั่นคงปลอดภัย (Security Operations)	5.00	0.00	มากที่สุด
4. สถาปัตยกรรมข้อมูล (Data Architecture)			
4.1 ข้อมูลนักศึกษา (Student Data)	4.89	0.33	มากที่สุด
4.2 ข้อมูลบุคลากร (Faculty/Staff Data)	5.00	0.00	มากที่สุด
4.3 ข้อมูลหลักสูตร (Curriculum Data)	4.89	0.33	มากที่สุด
4.4 ข้อมูลการเรียนการสอน (Learning Data)	4.89	0.33	มากที่สุด
4.5 ข้อมูลวิจัยและนวัตกรรม (Research Data)	4.89	0.33	มากที่สุด
4.6 ข้อมูลการเงิน (Financial Data)	4.78	0.44	มากที่สุด
4.7 ข้อมูลทรัพย์สิน (Asset Data)	4.89	0.33	มากที่สุด
4.8 ข้อมูลความเสี่ยง (Risk Data)	4.89	0.33	มากที่สุด
4.9 ข้อมูลความปลอดภัย (Security Data)	4.78	0.44	มากที่สุด
4.10 ข้อมูลภายนอก (External Data)	4.89	0.33	มากที่สุด
5. สถาปัตยกรรมเทคโนโลยี (Technology Architecture)			
5.1 โครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure)	4.89	0.33	มากที่สุด
5.2 แพลตฟอร์มข้อมูลและ Data Lakehouse	4.78	0.44	มากที่สุด
5.3 แพลตฟอร์มปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง (AI/ML Platform)	4.78	0.44	มากที่สุด
5.4 Integration & API	4.78	0.44	มากที่สุด
5.5 Network & Edge Computing	4.89	0.33	มากที่สุด
5.6 DevSecOps & Container	4.89	0.33	มากที่สุด
6. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture)			
6.1 EA–AI Integration	5.00	0.00	มากที่สุด
6.2 Architectural Framework	4.89	0.33	มากที่สุด
6.3 AI-Enabled System	4.89	0.33	มากที่สุด
6.4 Adaptability	5.00	0.00	มากที่สุด

รายการประเมิน	ระดับความคิดเห็น		
	$\bar{x}$	S.D.	ความเหมาะสม
6.5 Threat/Risk Intelligence	5.00	0.00	มากที่สุด
6.6 AI Ethics & Governance	4.89	0.33	มากที่สุด
7. สถาปัตยกรรมธรรมาภิบาล (Governance Architecture)			
7.1 Technology Governance	5.00	0.00	มากที่สุด
7.2 Security Governance	4.89	0.33	มากที่สุด
7.3 Data Governance	4.89	0.33	มากที่สุด
7.4 AI Governance	4.89	0.33	มากที่สุด
7.5 Compliance & Audit	4.89	0.33	มากที่สุด
8. เทคโนโลยีปัญญาประดิษฐ์ และระบบอัจฉริยะ (Intelligent Technology)			
8.1 Machine Learning (ML)	5.00	0.00	มากที่สุด
8.2 Deep Learning (DL)	4.89	0.33	มากที่สุด
8.3 Natural Language Processing (NLP)	4.89	0.33	มากที่สุด
8.4 Behavioral AI	4.89	0.33	มากที่สุด
8.5 Computer Vision	4.89	0.33	มากที่สุด
8.6 Speech Recognition	4.78	0.44	มากที่สุด
8.7 Robotics & Automation	4.89	0.33	มากที่สุด
8.9 Knowledge Graph	4.89	0.33	มากที่สุด
9. การจัดการองค์กรดิจิทัล (Digital Enterprise Management)			
9.1 กลยุทธ์ดิจิทัล	4.89	0.33	มากที่สุด
9.2 โครงสร้างพื้นฐานเทคโนโลยี	4.89	0.33	มากที่สุด
9.3 การจัดการข้อมูล	4.89	0.33	มากที่สุด
9.4 การทำให้กระบวนการเป็นอัตโนมัติ	5.00	0.00	มากที่สุด
9.5 ความมั่นคงปลอดภัยและความเป็นส่วนตัว	4.89	0.33	มากที่สุด
9.6 การวัดผลและตัวชี้วัด	4.89	0.33	มากที่สุด
10. สถาปัตยกรรมภูมิคุ้มกันดิจิทัลและความเสี่ยง (Digital Immunity & Risk Architecture)			
10.1 การมองเห็นและเฝ้าระวัง	4.89	0.33	มากที่สุด
10.2 การตรวจจับภัยคุกคาม	4.89	0.33	มากที่สุด
10.3 การสืบสวนและวิเคราะห์	4.89	0.33	มากที่สุด
10.4 การตอบสนองและการป้องกันเชิงรุก	4.89	0.33	มากที่สุด
10.5 ความทนทานและการฟื้นฟู	5.00	0.00	มากที่สุด
10.6 ความร่วมมือและการสร้างความตระหนักรู้	4.89	0.33	มากที่สุด
11.การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)			
11.1 การตรวจจับภัยคุกคามทางไซเบอร์	4.89	0.33	มากที่สุด

รายการประเมิน	ระดับความคิดเห็น		
	$\bar{x}$	S.D.	ความเหมาะสม
11.2 การตอบสนองต่อเหตุการณ์ทางไซเบอร์	4.89	0.33	มากที่สุด
11.3 การประเมินและจัดการความเสี่ยง	5.00	0.00	มากที่สุด
11.4 การปกป้องข้อมูลและความเป็นส่วนตัว	4.89	0.33	มากที่สุด
11.5 การฝึกอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัย	4.89	0.33	มากที่สุด
11.6 นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ	4.78	0.44	มากที่สุด
12. แหล่งข้อมูล (Data Sources)			
12.1 แหล่งข้อมูลภายใน	4.89	0.33	มากที่สุด
12.2 แหล่งข้อมูลภายนอก	4.89	0.33	มากที่สุด
12.3 รูปแบบข้อมูล	4.89	0.33	มากที่สุด
12.4 การจัดเก็บและประมวลผล	4.78	0.44	มากที่สุด
12.5 คุณภาพข้อมูล	4.89	0.33	มากที่สุด
13. ผู้ใช้งาน (Users)			
13.1 ผู้บริหาร (Executives)	5.00	0.00	มากที่สุด
13.2 คณาจารย์ (Faculty)	4.78	0.44	มากที่สุด
13.3 เจ้าหน้าที่ (Staff)	4.89	0.33	มากที่สุด
13.4 นักศึกษา (Students)	4.78	0.44	มากที่สุด
13.5 หน่วยงานภายนอก (External Agencies)	4.78	0.44	มากที่สุด
13.6 ผู้ดูแลระบบ (IT/Admin)	5.00	0.00	มากที่สุด
ผลเฉลี่ยรวม	4.89	0.31	มากที่สุด

จากตารางที่ 5-35 ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา จากผู้เชี่ยวชาญ จำนวน 9 ท่าน พบว่า ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาโดยภาพรวม มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{x}$=4.89, *S.D.*=0.31) เมื่อพิจารณารายด้าน พบว่า สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) มีความเหมาะสมอยู่ในระดับมากที่สุด มีค่าเฉลี่ยสูงสุด ($\bar{x}$=4.94, *S.D.*=0.16) รองลงมาคือ สถาปัตยกรรมธรรมาภิบาล (Governance Architecture) ($\bar{x}$=4.91, *S.D.*=0.26) การจัดการองค์กรดิจิทัล (Digital Enterprise Management) ($\bar{x}$=4.91, *S.D.*=0.28) สถาปัตยกรรมภูมิคุ้มกันดิจิทัลและความเสี่ยง (Digital Immunity & Risk Architecture) ($\bar{x}$=4.91, *S.D.*=0.28) ธรรมาภิบาลองค์กร (Enterprise Governance) ($\bar{x}$=4.90, *S.D.*=0.27) เทคโนโลยีปัญญาประดิษฐ์และระบบอัจฉริยะ (Intelligent Technology) ($\bar{x}$=4.89, *S.D.*=0.30) สถาปัตยกรรมธุรกิจ (Business

Architecture) ($\bar{X}$=4.89, *S.D.*=0.33) สถาปัตยกรรมแอปพลิเคชัน (Application Architecture) ($\bar{X}$=4.89, *S.D.*=0.29) การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) ($\bar{X}$=4.89, *S.D.*=0.29) สถาปัตยกรรมข้อมูล (Data Architecture) ($\bar{X}$=4.88, *S.D.*=0.32) แหล่งข้อมูล (Data Sources) ($\bar{X}$=4.87, *S.D.*=0.35) ผู้ใช้งาน (Users) ($\bar{X}$=4.87, *S.D.*=0.27) และสถาปัตยกรรมเทคโนโลยี (Technology Architecture) ($\bar{X}$=4.84, *S.D.*=0.38) ตามลำดับ โดยทุกด้านมีระดับความเหมาะสมอยู่ในระดับมากที่สุด แสดงให้เห็นว่าองค์ประกอบของสถาปัตยกรรมที่ผู้วิจัยพัฒนาขึ้นมีความครอบคลุมทั้งด้านการกำกับดูแล กระบวนการทางธุรกิจ ข้อมูล แอปพลิเคชัน เทคโนโลยี ปัญญาประดิษฐ์ การจัดการองค์กรดิจิทัล ตลอดจนการจัดการภูมิคุ้มกันดิจิทัลและความเสี่ยง และสามารถนำมาเชื่อมโยงเป็นโครงสร้างสถาปัตยกรรมองค์กรที่สนับสนุนการประยุกต์ใช้ปัญญาประดิษฐ์เพื่อเสริมสร้างภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษาได้อย่างเหมาะสม

เมื่อพิจารณาความเหมาะสมประเด็นย่อยในแต่ละด้าน รายละเอียดดังนี้

1. ธรรมาภิบาลองค์กร (Enterprise Governance) พบว่า ประเด็นย่อยข้อที่ 1.3 แผนการศึกษาแห่งชาติ พ.ศ. 2560–2579 และข้อที่ 1.8 ข้อกำหนดและแนวปฏิบัติเพื่อความมั่นคงปลอดภัยข้อมูล มีความเหมาะสมอยู่ในระดับมากที่สุดเท่ากัน ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 1.2 ยุทธศาสตร์หลักระยะยาว 20 ปี ของประเทศไทย (พ.ศ. 2561–2580) ข้อที่ 1.4 แผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (พ.ศ. 2565–2570) ข้อที่ 1.5 วิสัยทัศน์ พันธกิจ เป้าหมาย กลยุทธ์ ข้อที่ 1.6 กฎหมายเพื่อความมั่นคงปลอดภัยข้อมูล ข้อที่ 1.7 นโยบายการรักษาความมั่นคงปลอดภัยข้อมูล และข้อที่ 1.9 มาตรฐานเพื่อความมั่นคงปลอดภัยข้อมูล มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33)

2. สถาปัตยกรรมธุรกิจ (Business Architecture) พบว่า ประเด็นย่อยข้อที่ 2.1 กระบวนการบริหาร (Management Process) ข้อที่ 2.2 กระบวนการหลัก (Core Business Process) และข้อที่ 2.3 กระบวนการสนับสนุน (Supporting Process) มีความเหมาะสมอยู่ในระดับมากที่สุดเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33)

3. สถาปัตยกรรมแอปพลิเคชัน (Application Architecture) พบว่า ประเด็นย่อยข้อที่ 3.6 ระบบความมั่นคงปลอดภัย (Security Operations) มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 3.2 ระบบบริการนักศึกษา (Student Service) ข้อที่ 3.3 ระบบวิจัยและนวัตกรรม (Research Management) ข้อที่ 3.4 ระบบบริหารทรัพยากรบุคคล (HRM) ข้อที่ 3.5 ระบบวิเคราะห์และแดชบอร์ด (Analytics & Dashboard) มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33) และข้อที่ 3.1 ระบบบริหารจัดการการศึกษา (SIS) ($\bar{X}$=4.78, *S.D.*=0.44) ตามลำดับ

4. สถาปัตยกรรมข้อมูล (Data Architecture) พบว่า ประเด็นย่อยข้อที่ 4.2 ข้อมูลบุคลากร (Faculty/Staff Data) มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 4.1 ข้อมูลนักศึกษา (Student Data) ข้อที่ 4.3 ข้อมูลหลักสูตร (Curriculum Data) ข้อที่ 4.4 ข้อมูลการเรียนการสอน (Learning Data) ข้อที่ 4.5 ข้อมูลวิจัยและนวัตกรรม (Research Data) ข้อที่ 4.7 ข้อมูลทรัพย์สิน (Asset Data) ข้อที่ 4.8 ข้อมูลความเสี่ยง (Risk Data) ข้อที่ 4.10 ข้อมูลภายนอก (External Data) มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33) และข้อที่ 4.6 ข้อมูลการเงิน (Financial Data) และข้อที่ 4.9 ข้อมูลความปลอดภัย (Security Data) มีความเหมาะสมเท่ากัน ($\bar{X}$=4.78, *S.D.*=0.44) ตามลำดับ

5. สถาปัตยกรรมเทคโนโลยี (Technology Architecture) พบว่า ประเด็นย่อยข้อที่ 5.1 โครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure) ข้อที่ 5.5 Network & Edge Computing และข้อที่ 5.6 DevSecOps & Container มีความเหมาะสมอยู่ในระดับมากที่สุดเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33) รองลงมาคือ ข้อที่ 5.2 แพลตฟอร์มข้อมูลและ Data Lakehouse ข้อที่ 5.3 แพลตฟอร์มปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง (AI/ML Platform) และข้อที่ 5.4 Integration & API มีความเหมาะสมเท่ากัน ($\bar{X}$=4.78, *S.D.*=0.44) ตามลำดับ

6. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) พบว่า ประเด็นย่อยข้อที่ 6.1 EA–AI Integration ข้อที่ 6.4 Adaptability และข้อที่ 6.5 Threat/Risk Intelligence มีความเหมาะสมอยู่ในระดับมากที่สุดเท่ากัน ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 6.2 Architectural Framework ข้อที่ 6.3 AI-Enabled System และข้อที่ 6.6 AI Ethics & Governance มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33)

7. สถาปัตยกรรมธรรมาภิบาล (Governance Architecture) พบว่า ประเด็นย่อยข้อที่ 7.1 Technology Governance มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 7.2 Security Governance ข้อที่ 7.3 Data Governance ข้อที่ 7.4 AI Governance และข้อที่ 7.5 Compliance & Audit มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33)

8. เทคโนโลยีปัญญาประดิษฐ์ และระบบอัจฉริยะ (Intelligent Technology) พบว่า ประเด็นย่อยข้อที่ 8.1 Machine Learning (ML) มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 8.2 Deep Learning (DL) ข้อที่ 8.3 Natural Language Processing (NLP) ข้อที่ 8.4 Behavioral AI ข้อที่ 8.5 Computer Vision ข้อที่ 8.7 Robotics & Automation และข้อที่ 8.9 Knowledge Graph มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33) และข้อที่ 8.6 Speech Recognition ($\bar{X}$=4.78, *S.D.*=0.44) ตามลำดับ

9. การจัดการองค์กรดิจิทัล (Digital Enterprise Management) พบว่า ประเด็นย่อยข้อที่ 9.4 การทำให้กระบวนการเป็นอัตโนมัติ มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 9.1 กลยุทธ์ดิจิทัล ข้อที่ 9.2 โครงสร้างพื้นฐานเทคโนโลยี ข้อที่ 9.3 การจัดการข้อมูล ข้อที่ 9.5 ความมั่นคงปลอดภัยและความเป็นส่วนตัว และข้อที่ 9.6 การวัดผลและตัวชี้วัด มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33)

10. สถาปัตยกรรมภูมิคุ้มกันดิจิทัลและความเสี่ยง (Digital Immunity & Risk Architecture) พบว่า ประเด็นย่อยข้อที่ 10.5 ความทนทานและการฟื้นฟู มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 10.1 การมองเห็นและเฝ้าระวัง ข้อที่ 10.2 การตรวจจับภัยคุกคาม ข้อที่ 10.3 การสืบสวนและวิเคราะห์ ข้อที่ 10.4 การตอบสนองและการป้องกันเชิงรุก และข้อ 10.6 ความร่วมมือและการสร้างความตระหนักรู้ มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33)

11.การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) พบว่า ประเด็นย่อยข้อที่ 11.3 การประเมินและจัดการความเสี่ยง มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 11.1 การตรวจจับภัยคุกคามทางไซเบอร์ ข้อที่ 11.2 การตอบสนองต่อเหตุการณ์ทางไซเบอร์ ข้อที่ 11.4 การปกป้องข้อมูลและความเป็นส่วนตัว และข้อที่ 11.5 การฝึกอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัย มีความเหมาะสมเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33) และข้อที่ 11.6 นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ ($\bar{X}$=4.78, *S.D.*=0.44) ตามลำดับ

12. แหล่งข้อมูล (Data Sources) พบว่า ประเด็นย่อยข้อที่ 12.1 แหล่งข้อมูลภายใน ข้อที่ 12.2 แหล่งข้อมูลภายนอก ข้อที่ 12.3 รูปแบบข้อมูล และข้อที่ 12.5 คุณภาพข้อมูล มีความเหมาะสมอยู่ในระดับมากที่สุดเท่ากัน ($\bar{X}$=4.89, *S.D.*=0.33) รองลงมาคือ ข้อที่ 12.4 การจัดเก็บและประมวลผล ($\bar{X}$=4.78, *S.D.*=0.44)

13. ผู้ใช้งาน (Users) พบว่า ประเด็นย่อยข้อที่ 13.1 ผู้บริหาร (Executives) และข้อที่ 13.6 ผู้ดูแลระบบ (IT/Admin) มีความเหมาะสมอยู่ในระดับมากที่สุดเท่ากัน ($\bar{X}$=5.00, *S.D.*=0.00) รองลงมาคือ ข้อที่ 13.3 เจ้าหน้าที่ (Staff) ($\bar{X}$=4.89, *S.D.*=0.33) และข้อที่ 13.2 คณาจารย์ (Faculty) ข้อที่ 13.4 นักศึกษา (Students) และข้อที่ 13.5 หน่วยงานภายนอก (External Agencies) มีความเหมาะสมเท่ากัน ($\bar{X}$=4.78, *S.D.*=0.44) ตามลำดับ

บทที่ 6
สรุปผล อภิปรายผล และข้อเสนอแนะ

การวิจัยเรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” เป็นการวิจัยแบบผสานวิธี (Mixed-Methodology Research) ประกอบด้วยการวิจัยเชิงปริมาณ (Quantitative Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) โดยแบ่งการดำเนินการวิจัยออกเป็น 4 ระยะ ได้แก่ ระยะที่ 1 การวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ระยะที่ 2 การสร้างแบบจำลองสมการโครงสร้างสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ระยะที่ 3 การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา และระยะที่ 4 การประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยสามารถสรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ รายละเอียดดังต่อไปนี้

6.1 สรุปผลการวิจัย

6.2 อภิปรายผล

6.3 ข้อเสนอแนะ

6.1 สรุปผลการวิจัย

การวิจัยเรื่อง สถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา สามารถสรุปผลแบ่งตามวัตถุประสงค์ของการวิจัย มีรายละเอียดดังนี้

6.1.1 ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ สรุปได้ดังนี้

6.1.1.1 สรุปผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ประกอบด้วย 6 ปัจจัย 156 ข้อ ดังนี้ 1. โครงสร้างองค์กร แบ่งออกเป็น 7 ด้าน 28 ข้อ ได้แก่ สถาปัตยกรรมธุรกิจ สถาปัตยกรรมข้อมูล สถาปัตยกรรมระบบแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยี สถาปัตยกรรมด้านความปลอดภัย สถาปัตยกรรมการบูรณาการ และสถาปัตยกรรมการกำกับดูแล 2. เทคโนโลยีอัจฉริยะ แบ่งออกเป็น 4 ด้าน 16 ข้อ ได้แก่ การเรียนรู้ของเครื่อง การเรียนรู้เชิงลึก การประมวลผลภาษาธรรมชาติ และความรู้เชิงพฤติกรรม 3. ระบบภูมิคุ้มกันดิจิทัล แบ่งออกเป็น 6 ด้าน 24 ข้อ ได้แก่ การมองเห็นและเฝ้าระวัง การตรวจจับภัยคุกคาม การสืบสวนและวิเคราะห์ การตอบสนองและการป้องกันเชิงรุก ความทนทานและการฟื้นฟู และความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ 4. การจัดการองค์กรดิจิทัล แบ่งออกเป็น 5 ด้าน 24 ข้อ ได้แก่ กลยุทธ์ดิจิทัล โครงสร้างพื้นฐานเทคโนโลยี การจัดการข้อมูล กระบวนการอัตโนมัติ

และความมั่นคงปลอดภัยทางไซเบอร์ 5. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ แบ่งออกเป็น 6 ด้าน 28 ข้อ ได้แก่ การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ กรอบการทำงานเชิงสถาปัตยกรรมการออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ความสามารถในการปรับตัวต่อการเปลี่ยนแปลง ความสามารถในการรับมือภัยคุกคามและความเสี่ยง และจริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ และ 6. การจัดการภูมิคุ้มกันดิจิทัล แบ่งออกเป็น 6 ด้าน 36 ข้อ ได้แก่ การตรวจจับภัยคุกคามทางไซเบอร์ การตอบสนองต่อเหตุการณ์ทางไซเบอร์ การประเมินและจัดการความเสี่ยง การปกป้องข้อมูลและความเป็นส่วนตัว การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย และนโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ การสอบถามความคิดเห็นที่มีต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยกลุ่มตัวอย่าง 500 คน พบว่า โดยภาพรวมมีความเหมาะสมในระดับมาก ($\bar{X}$=3.90) เมื่อพิจารณารายด้าน พบว่า 1. ด้านโครงสร้างองค์กร โดยรวมมีความเหมาะสมอยู่ในระดับมาก ($\bar{X}$=3.85, *S.D.*=0.92) แบ่งออกเป็น สถาปัตยกรรมด้านความปลอดภัย ($\bar{X}$=3.95, *S.D.*=0.86) สถาปัตยกรรมการกำกับดูแล ($\bar{X}$=3.91, *S.D.*=0.90) สถาปัตยกรรมเทคโนโลยี ($\bar{X}$=3.86, *S.D.*=0.95) สถาปัตยกรรมระบบแอปพลิเคชัน ($\bar{X}$=3.86, *S.D.*=0.94) สถาปัตยกรรมการบูรณาการ ($\bar{X}$=3.83, *S.D.*=0.92) สถาปัตยกรรมข้อมูล ($\bar{X}$=3.79, *S.D.*=0.55) และสถาปัตยกรรมธุรกิจ ($\bar{X}$=3.77, *S.D.*=0.93) 2. ด้านเทคโนโลยีอัจฉริยะ โดยรวมมีความเหมาะสมอยู่ในระดับมาก ($\bar{X}$=3.92, *S.D.*=0.85) แบ่งออกเป็น การเรียนรู้ของเครื่อง ($\bar{X}$=3.95, *S.D.*=0.88) การเรียนรู้เชิงลึก ($\bar{X}$=3.93, *S.D.*=0.80) ความรู้เชิงพฤติกรรม ($\bar{X}$=3.91, *S.D.*=0.87) และการประมวลผลภาษาธรรมชาติ ($\bar{X}$=3.90, *S.D.*=0.84) 3. ด้านระบบภูมิคุ้มกันดิจิทัล โดยรวมมีความเหมาะสมอยู่ในระดับมาก ($\bar{X}$=3.93, *S.D.*=0.80) แบ่งออกเป็น การมองเห็นและเฝ้าระวัง ($\bar{X}$=3.97, *S.D.*=0.81) การตรวจจับภัยคุกคาม และการสืบสวนและวิเคราะห์ ($\bar{X}$=3.95, *S.D.*=0.79) ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ มีค่าเฉลี่ย ($\bar{X}$=3.92, *S.D.*=0.80) ความทนทานและการฟื้นฟู ($\bar{X}$=3.91, *S.D.*=0.80) และการตอบสนองและการป้องกันเชิงรุก ($\bar{X}$=3.89, *S.D.*=0.79) 4. ด้านการจัดการองค์กรดิจิทัล โดยรวมมีความเหมาะสมอยู่ในระดับมาก ($\bar{X}$=3.90, *S.D.*=0.80) แบ่งออกเป็น โครงสร้างพื้นฐานเทคโนโลยี ($\bar{X}$=3.94, *S.D.*=0.80) กลยุทธ์ดิจิทัล และการจัดการข้อมูล ($\bar{X}$=3.92, *S.D.*=0.80) ความมั่นคงปลอดภัยทางไซเบอร์ ($\bar{X}$=3.88, *S.D.*=0.79) และกระบวนการอัตโนมัติ ($\bar{X}$=3.82, *S.D.*=0.81) 5. ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ โดยรวมมีความเหมาะสมอยู่ในระดับมาก ($\bar{X}$=3.87, *S.D.*=0.92) แบ่งออกเป็น จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ ($\bar{X}$=3.96, *S.D.*=0.86) ความสามารถในการรับมือภัยคุกคามและความเสี่ยง ($\bar{X}$=3.88, *S.D.*=0.94) ความสามารถในการ

ปรับตัวต่อการเปลี่ยนแปลง ($\bar{X}$=3.87, *S.D.*=0.88) กรอบการทำงานเชิงสถาปัตยกรรม และการออกแบบ ($\bar{X}$=3.84, *S.D.*=0.94) พัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ($\bar{X}$=3.84, *S.D.*= 0.98) และการบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ ($\bar{X}$=3.83, *S.D.*=0.90) 6. ด้านการจัดการภูมิคุ้มกันดิจิทัล โดยรวมมีความเหมาะสมอยู่ในระดับมาก ($\bar{X}$=3.93, *S.D.*=0.82) แบ่งออกเป็นการปกป้องข้อมูลและความเป็นส่วนตัว ($\bar{X}$=3.97, *S.D.*=0.81) นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ ($\bar{X}$=3.97, *S.D.*=0.77) การประเมินและจัดการความเสี่ยง ($\bar{X}$=3.94, *S.D.*=0.84) การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย ($\bar{X}$=3.93, *S.D.*=0.82) การตอบสนองต่อเหตุการณ์ทางไซเบอร์ ($\bar{X}$=3.89, *S.D.*=0.86) และการตรวจจับภัยคุกคามทางไซเบอร์ ($\bar{X}$=3.88, *S.D.*=0.83)

6.1.1.2 สรุปผลการวิเคราะห์องค์ประกอบเชิงยืนยันปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผลการวิเคราะห์ค่าสถิติองค์ประกอบเชิงยืนยันปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาโดยมีนัยสำคัญทางสถิติที่ 0.001 ประกอบด้วย 6 ตัวแปร ได้แก่ ด้านโครงสร้างองค์กร ประกอบไปด้วย 1. สถาปัตยกรรมธุรกิจ 2. สถาปัตยกรรมข้อมูล 3. สถาปัตยกรรมระบบแอปพลิเคชัน 4. สถาปัตยกรรมเทคโนโลยี 5. สถาปัตยกรรมด้านความมั่งคงปลอดภัย 6. สถาปัตยกรรมการบูรณาการ และ 7. สถาปัตยกรรมการกำกับดูแล ด้านเทคโนโลยีอัจฉริยะ ประกอบด้วย 1. การเรียนรู้ของเครื่อง 2. การเรียนรู้เชิงลึก 3. การประมวลผลภาษาธรรมชาติ และ 4. ความรู้เชิงพฤติกรรม ด้านระบบภูมิคุ้มกันดิจิทัล ประกอบด้วย 1. การมองเห็นและเฝ้าระวัง 2. การตรวจจับภัยคุกคาม 3. การสืบสวนและวิเคราะห์ 4. การตอบสนองและการป้องกันเชิงรุก 5. ความทนทานและการฟื้นฟู และ 6. ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ ด้านการจัดการองค์กรดิจิทัล ประกอบด้วย 1. กลยุทธ์ดิจิทัล 2. โครงสร้างพื้นฐานเทคโนโลยี 3. การจัดการข้อมูล 4. กระบวนการอัตโนมัติ และ 5. ความมั่นคงปลอดภัยทางไซเบอร์ ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ประกอบด้วย 1. การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ 2. กรอบการทำงานเชิงสถาปัตยกรรม 3. การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ 4. การปรับตัวต่อการเปลี่ยนแปลง 5. การรับมือภัยคุกคามและความเสี่ยง และ6. จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ และด้านการจัดการภูมิคุ้มกันดิจิทัล ประกอบด้วย 1. การตรวจจับภัยคุกคามทางไซเบอร์ 2. การตอบสนองต่อเหตุการณ์ทางไซเบอร์ 3. การประเมินและจัดการความเสี่ยง 4. การปกป้องข้อมูลและความเป็นส่วนตัว 5. การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย และ 6. นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ รวมทั้งหมด 34 ตัวแปรสังเกตได้ ผลวิเคราะห์พบว่ามีน้ำหนักสัมประสิทธิ์

ระหว่าง -0.28 ถึง 0.83 โดยมีทั้งอิทธิพลเชิงบวกและเชิงลบ ทั้งนี้ การจัดการองค์กรดิจิทัล (Digital Enterprise Management: DEM) มีอิทธิพลต่อ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) สูงที่สุด มีค่าน้ำหนักสัมประสิทธิ์เท่ากับ 0.83 แสดงให้เห็นว่า ความพร้อมด้านกลยุทธ์ดิจิทัล โครงสร้างพื้นฐานเทคโนโลยี การจัดการข้อมูล กระบวนการอัตโนมัติ และความมั่นคงปลอดภัยทางไซเบอร์ เป็นปัจจัยสำคัญต่อการพัฒนาและขับเคลื่อนสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ของสถาบันอุดมศึกษา รองลงมาคือ ระบบภูมิคุ้มกันดิจิทัล (Digital Immunity System: DIS) มีอิทธิพลต่อ การจัดการภูมิคุ้มกันดิจิทัล (DIM) เท่ากับ 0.72 แสดงให้เห็นว่า ความสามารถด้านการมองเห็นและเฝ้าระวัง การตรวจจับภัยคุกคาม การสืบสวนและวิเคราะห์ การตอบสนองและการป้องกันเชิงรุก ตลอดจนความทนทานและการฟื้นฟู เป็นกลไกสำคัญที่สนับสนุนการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา

สำหรับ เทคโนโลยีอัจฉริยะ (Intelligent Technology: AIT) มีอิทธิพลต่อ AIA เท่ากับ 0.24 แสดงให้เห็นว่าเทคโนโลยีปัญญาประดิษฐ์ เช่น Machine Learning, Deep Learning, Natural Language Processing และ Behavioral AI มีส่วนสนับสนุนการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ขณะที่ โครงสร้างองค์กร (EAC) มีอิทธิพลต่อ AIA เท่ากับ 0.02 และมีอิทธิพลต่อ DIM เท่ากับ 0.09 ส่วน AIT มีอิทธิพลต่อ DIM เท่ากับ 0.10 ซึ่งสะท้อนว่าปัจจัยดังกล่าวมีบทบาทสนับสนุนในแบบจำลอง แต่มีขนาดอิทธิพลทางตรงต่ำกว่า DEM และ DIS

ในส่วนของเส้นทางที่มีอิทธิพลเชิงลบ พบว่า DIS มีอิทธิพลต่อ AIA เท่ากับ -0.28 และ DEM มีอิทธิพลต่อ DIM เท่ากับ -0.10 ทั้งนี้ ค่าสัมประสิทธิ์เชิงลบดังกล่าวควรตีความในบริบทของแบบจำลองสมการโครงสร้าง ซึ่งเป็นการวิเคราะห์อิทธิพลของตัวแปรแต่ละตัวเมื่อพิจารณาตัวแปรอื่นในแบบจำลองร่วมกัน มิได้หมายความว่า DIS หรือ DEM เป็นปัจจัยที่ส่งผลเสียต่อการพัฒนาสถาปัตยกรรมหรือการจัดการภูมิคุ้มกันดิจิทัลโดยตรง โดยเฉพาะเมื่อพิจารณาผลการวิเคราะห์โดยรวมพบว่า DIS มีอิทธิพลต่อ DIM ในระดับสูงที่ 0.72 และ DEM มีอิทธิพลต่อ AIA ในระดับสูงมากที่ 0.83 จึงแสดงว่าตัวแปรทั้งสองยังคงมีบทบาทสำคัญต่อระบบโดยรวม แต่มีรูปแบบความสัมพันธ์ทางตรงกับตัวแปรปลายทางที่แตกต่างกันภายใต้โครงสร้างของแบบจำลอง

6.1.2 ผลการสร้างแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

การสร้างแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา เป็นการนำผลจากการศึกษาค้นคว้าและสังเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาจากข้อมูล เอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับโครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล สถาปัตยกรรม

องค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัล ในการดำเนินงานในระยะที่ 1 และผ่านการตรวจสอบโดยการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis) พบว่าตัวแปรทั้งหมดมีความสอดคล้องตามเกณฑ์สามารถนำไปสร้างโมเดลแบบจำลองสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

แบบจำลองสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ประกอบด้วยตัวแปรแฝงจำนวน 6 ตัว และตัวแปรสังเกตที่ใช้เป็นองค์ประกอบของแต่ละตัวแปรแฝง ได้แก่ 1. โครงสร้างองค์กร ประกอบด้วย สถาปัตยกรรมธุรกิจ สถาปัตยกรรมข้อมูล สถาปัตยกรรมระบบแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยี สถาปัตยกรรมด้านความมั่นคงปลอดภัย สถาปัตยกรรมการบูรณาการ และสถาปัตยกรรมการกำกับดูแล 2. เทคโนโลยีอัจฉริยะ ประกอบด้วย การเรียนรู้ของเครื่อง การเรียนรู้เชิงลึก การประมวลผลภาษาธรรมชาติ และความรู้เชิงพฤติกรรม 3. ระบบภูมิคุ้มกันดิจิทัล ประกอบด้วย การมองเห็นและเฝ้าระวัง การตรวจจับภัยคุกคาม การสืบสวนและวิเคราะห์ การตอบสนองและการป้องกันเชิงรุก ความทนทานและการฟื้นฟู และความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ 4. การจัดการองค์กรดิจิทัล ประกอบด้วย กลยุทธ์ดิจิทัล โครงสร้างพื้นฐานเทคโนโลยี การจัดการข้อมูล กระบวนการอัตโนมัติ และความมั่นคงปลอดภัยทางไซเบอร์ 5. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ประกอบด้วย การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ กรอบการทำงานเชิงสถาปัตยกรรม การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ การปรับตัวต่อการเปลี่ยนแปลง การรับมือภัยคุกคามและความเสี่ยง และจริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ และ 6. การจัดการภูมิคุ้มกันดิจิทัล ประกอบด้วย การตรวจจับภัยคุกคามทางไซเบอร์ การตอบสนองต่อเหตุการณ์ทางไซเบอร์ การประเมินและจัดการความเสี่ยง การปกป้องข้อมูลและความเป็นส่วนตัว การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย และนโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ รวมทั้งหมด 34 ตัวแปรสังเกตได้ โดยองค์ประกอบดังกล่าวถูกนำมาพิจารณาความสัมพันธ์เชิงโครงสร้างร่วมกัน เพื่อยืนยันองค์ประกอบและตรวจสอบความเหมาะสมของแบบจำลองที่ใช้ในการอธิบายปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

6.1.3 สรุปผลการตรวจสอบยืนยันแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สามารถสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

6.1.3.1 ผลการวิเคราะห์ทดสอบสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลสำหรับ

สถาบันอุดมศึกษา (Structural Equation Modeling: SEM) ประกอบด้วย ตัวแปรแฝงจำนวน 6 ตัว ได้แก่ 1. โครงสร้างองค์กร (EAC) 2. เทคโนโลยีอัจฉริยะ (AIT) 3. ระบบภูมิคุ้มกันดิจิทัล (DIS) 4. การจัดการองค์กรดิจิทัล (DEM) 5. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) และ 6. การจัดการภูมิคุ้มกันดิจิทัล (DIM) โดยกำหนดให้ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) และการจัดการภูมิคุ้มกันดิจิทัล (DIM) เป็นตัวแปรผล และดำเนินการวิเคราะห์ความสัมพันธ์เชิงโครงสร้างระหว่างตัวแปรแฝงด้วยวิธีการเชื่อมตัวแปรตามแบบจำลองสมการโครงสร้าง จากนั้นตรวจสอบความเหมาะสมและความถูกต้องของโมเดลด้วยการพิจารณาค่าสัมประสิทธิ์การตัดสินใจ (R^2) ค่าน้ำหนักสัมประสิทธิ์เส้นทาง และค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระในรูปคะแนนมาตรฐาน เพื่อพิจารณาทิศทางและขนาดของอิทธิพลของตัวแปรที่มีต่อตัวแปรผล โดยผลการตรวจสอบความสอดคล้องของแบบจำลองกับข้อมูลเชิงประจักษ์ พบว่า Chi-Square = 517.17, df = 499, p-value = 0.27784 และ RMSEA = 0.012 แสดงว่าแบบจำลองมีความสอดคล้องกับข้อมูลเชิงประจักษ์ในระดับดี นอกจากนี้ แบบจำลองสามารถอธิบายความแปรปรวนของ AIA ได้ร้อยละ 70 (R^2 = 0.70) และ DIM ได้ร้อยละ 81 (R^2 = 0.81) โดยมีรายละเอียดผลการทดสอบ ดังนี้

1. โครงสร้างองค์กร (EAC) มีจำนวน 7 ตัวแปรสังเกตได้ ได้แก่ สถาปัตยกรรมธุรกิจ สถาปัตยกรรมข้อมูล สถาปัตยกรรมระบบแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยี สถาปัตยกรรมด้านความมั่นคงปลอดภัย สถาปัตยกรรมการบูรณาการ และสถาปัตยกรรมการกำกับดูแล ซึ่งเป็นองค์ประกอบที่สะท้อนโครงสร้างพื้นฐานเชิงสถาปัตยกรรมของสถาบันอุดมศึกษา ทั้งในด้านธุรกิจ ข้อมูล ระบบเทคโนโลยี ความมั่นคงปลอดภัย การเชื่อมโยงระบบ และการกำกับดูแล โดยผลการวิเคราะห์พบว่า EAC มีอิทธิพลต่อ AIA เท่ากับ 0.02 และมีอิทธิพลต่อ DIM เท่ากับ 0.09 แสดงว่าโครงสร้างองค์กรมีบทบาทสนับสนุนการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัล แต่มีขนาดอิทธิพลทางตรงในระดับต่ำเมื่อเปรียบเทียบกับปัจจัยด้านการจัดการองค์กรดิจิทัลและระบบภูมิคุ้มกันดิจิทัล

2. เทคโนโลยีอัจฉริยะ (AIT) มีจำนวน 4 ตัวแปรสังเกตได้ ได้แก่ การเรียนรู้ของเครื่อง การเรียนรู้เชิงลึก การประมวลผลภาษาธรรมชาติ และความรู้เชิงพฤติกรรม ผลการวิเคราะห์พบว่า AIT มีอิทธิพลต่อ AIA เท่ากับ 0.24 และมีอิทธิพลต่อ DIM เท่ากับ 0.10 แสดงให้เห็นว่าเทคโนโลยีอัจฉริยะเป็นองค์ประกอบสำคัญที่ช่วยสนับสนุนการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ โดยเฉพาะการนำเทคนิค AI มาใช้ในการวิเคราะห์ข้อมูล สนับสนุนการตัดสินใจ และเพิ่มขีดความสามารถของระบบสารสนเทศ ขณะที่อิทธิพลต่อ DIM โดยตรงมีขนาดต่ำกว่า

3. ระบบภูมิคุ้มกันดิจิทัล (DIS) มีจำนวน 6 ตัวแปรสังเกตได้ ได้แก่ การมองเห็นและเฝ้าระวัง การตรวจจับภัยคุกคาม การสืบสวนและวิเคราะห์ การตอบสนองและการป้องกันเชิงรุก ความทนทานและการฟื้นฟู และความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย

บนไซเบอร์ ผลการวิเคราะห์พบว่า DIS มีอิทธิพลต่อ AIA เท่ากับ -0.28 และมีอิทธิพลต่อ DIM เท่ากับ 0.72 โดยอิทธิพลต่อ DIM มีขนาดสูง แสดงให้เห็นว่าระบบภูมิคุ้มกันดิจิทัลเป็นกลไกสำคัญในการสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา ส่วนค่าสัมประสิทธิ์เชิงลบของ DIS ต่อ AIA ควรตีความภายใต้ความสัมพันธ์ร่วมของตัวแปรทั้งหมดในแบบจำลอง มิได้หมายความว่า DIS เป็นปัจจัยที่ส่งผลเสียต่อ AIA โดยตรง

4. การจัดการองค์กรดิจิทัล (DEM) มีจำนวน 5 ตัวแปรสังเกตได้ ได้แก่ กลยุทธ์ดิจิทัล โครงสร้างพื้นฐานเทคโนโลยี การจัดการข้อมูล กระบวนการอัตโนมัติ และความมั่นคงปลอดภัยทางไซเบอร์ ผลการวิเคราะห์พบว่า DEM มีอิทธิพลต่อ AIA เท่ากับ 0.83 ซึ่งเป็นค่าสัมประสิทธิ์ที่สูงที่สุดในแบบจำลอง แสดงให้เห็นว่าการจัดการองค์กรดิจิทัลเป็นปัจจัยสำคัญอย่างยิ่งต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ขณะที่ DEM มีอิทธิพลต่อ DIM เท่ากับ -0.10 ซึ่งเป็นอิทธิพลเชิงลบในระดับต่ำ ทั้งนี้ ค่าดังกล่าวแสดงถึงอิทธิพลทางตรงเมื่อพิจารณาตัวแปรอื่นร่วมกันในแบบจำลอง มิได้หมายความว่าการจัดการองค์กรดิจิทัลส่งผลเสียต่อการจัดการภูมิคุ้มกันดิจิทัลโดยตรง

5. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) มีจำนวน 6 ตัวแปรสังเกตได้ ได้แก่ การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ กรอบการทำงานเชิงสถาปัตยกรรม การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ การปรับตัวต่อการเปลี่ยนแปลง การรับมือภัยคุกคามและความเสี่ยง และจริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ โดย AIA มีอิทธิพลต่อ DIM เท่ากับ 0.07 แสดงให้เห็นว่าสถาปัตยกรรมองค์กรปัญญาประดิษฐ์มีบทบาทในการเชื่อมโยงการประยุกต์ใช้ AI กับการจัดการภูมิคุ้มกันดิจิทัลในระดับองค์กร และทำหน้าที่เป็นกลไกเชิงสถาปัตยกรรมในการบูรณาการองค์ประกอบด้านองค์กร เทคโนโลยี ข้อมูล ความมั่นคงปลอดภัย และ AI เข้าด้วยกัน

6. การจัดการภูมิคุ้มกันดิจิทัล (DIM) มีจำนวน 6 ตัวแปรสังเกตได้ ได้แก่ การตรวจจับภัยคุกคามทางไซเบอร์ การตอบสนองต่อเหตุการณ์ทางไซเบอร์ การประเมินและจัดการความเสี่ยง การปกป้องข้อมูลและความเป็นส่วนตัว การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย และนโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ โดย DIM เป็นตัวแปรผลสำคัญของแบบจำลอง และสามารถอธิบายความแปรปรวนได้ร้อยละ 81 ($R^2 = 0.81$) แสดงให้เห็นว่าองค์ประกอบของแบบจำลองสามารถร่วมกันอธิบายการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษาได้ในระดับสูง

6.1.3.2 สรุปผลการวิเคราะห์เส้นอิทธิพลแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สามารถสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผลการวิเคราะห์แบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์สามารถสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา นำมาสรุปการทำสอบเส้นทางอิทธิพลทางตรง อิทธิพลทางอ้อม และอิทธิพลรวม ได้ดังนี้

ตารางที่ 6-1 ผลการวิเคราะห์อิทธิพลแบบจำลองสมการโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

เส้นทางอิทธิพล	อิทธิพลทางตรง	อิทธิพลทางอ้อม	อิทธิพลรวม
โครงสร้างองค์กร ⟶ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์	0.02	–	0.02
เทคโนโลยีอัจฉริยะ ⟶ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์	0.24	–	0.24
ระบบภูมิคุ้มกันดิจิทัล ⟶ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์	-0.28	–	-0.28
การจัดการองค์กรดิจิทัล ⟶ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์	0.83	–	0.83
โครงสร้างองค์กร ⟶ การจัดการภูมิคุ้มกันดิจิทัล	0.09	0.09	0.18
เทคโนโลยีอัจฉริยะ ⟶ การจัดการภูมิคุ้มกันดิจิทัล	0.10	0.02	0.12
ระบบภูมิคุ้มกันดิจิทัล ⟶ การจัดการภูมิคุ้มกันดิจิทัล	0.72	-0.02	0.70
การจัดการองค์กรดิจิทัล ⟶ การจัดการภูมิคุ้มกันดิจิทัล	-0.10	0.06	-0.04
สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ⟶ การจัดการภูมิคุ้มกันดิจิทัล	0.07	–	0.07
R^2 (สถาปัตยกรรมองค์กรปัญญาประดิษฐ์)	0.70	–	70%
R^2 (การจัดการภูมิคุ้มกันดิจิทัล)	0.81	–	81%

ผลการวิเคราะห์ค่าอิทธิพลแบบจำลองสมการเชิงโครงสร้างปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา สรุปผลการทดสอบเส้นทางอิทธิพลได้ว่า ปัจจัยที่ส่งผลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) มากที่สุด คือ การจัดการองค์กรดิจิทัล (DEM) มีค่าสัมประสิทธิ์อิทธิพลรวม 0.83 รองลงมา คือ เทคโนโลยีอัจฉริยะ (AIT) มีค่าสัมประสิทธิ์อิทธิพลรวม 0.24 โครงสร้างองค์กร (EAC) มีค่าสัมประสิทธิ์อิทธิพลรวม 0.02 และ ระบบภูมิคุ้มกันดิจิทัล (DIS) มีค่าสัมประสิทธิ์อิทธิพลรวม -0.28 ตามลำดับ โดยตัวแปรดังกล่าวสามารถร่วมกันอธิบายความแปรปรวนของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ได้ร้อยละ 70.0 (R^2 = 0.70) สำหรับปัจจัยที่ส่งผลต่อ การจัดการภูมิคุ้มกันดิจิทัล (DIM) พบว่า ระบบภูมิคุ้มกันดิจิทัล (DIS) มีค่าสัมประสิทธิ์อิทธิพลรวมสูงที่สุดเท่ากับ 0.70 รองลงมา คือ โครงสร้างองค์กร (EAC) มีค่าสัมประสิทธิ์อิทธิพลรวม 0.18 เทคโนโลยีอัจฉริยะ (AIT) มีค่าสัมประสิทธิ์อิทธิพลรวม 0.12 สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) มีค่าสัมประสิทธิ์อิทธิพลรวม 0.07 และ การจัดการองค์กรดิจิทัล (DEM) มีค่าสัมประสิทธิ์อิทธิพลรวม -

0.04 ตามลำดับ โดยตัวแปรในแบบจำลองสามารถร่วมกันอธิบายความแปรปรวนของการจัดการภูมิคุ้มกันดิจิทัลได้ร้อยละ 81.0 (R^2 = 0.81) ทั้งนี้ เมื่อพิจารณาอิทธิพลทางตรงและอิทธิพลทางอ้อม พบว่าโครงสร้างองค์กรมีอิทธิพลทางตรงต่อ DIM เท่ากับ 0.09 และมีอิทธิพลทางอ้อมเท่ากับ 0.09 ส่งผลให้มีอิทธิพลรวม 0.18 เทคโนโลยีอัจฉริยะมีอิทธิพลทางตรง 0.10 และทางอ้อม 0.02 ส่งผลให้มีอิทธิพลรวม 0.12 ระบบภูมิคุ้มกันดิจิทัลมีอิทธิพลทางตรง 0.72 และทางอ้อม -0.02 ส่งผลให้มีอิทธิพลรวม 0.70 การจัดการองค์กรดิจิทัลมีอิทธิพลทางตรง -0.10 และทางอ้อม 0.06 ส่งผลให้มีอิทธิพลรวม -0.04 และสถาปัตยกรรมองค์กรปัญญาประดิษฐ์มีอิทธิพลทางตรงและอิทธิพลรวมต่อการจัดการภูมิคุ้มกันดิจิทัลเท่ากับ 0.07 จากผลการวิเคราะห์ดังกล่าวแสดงให้เห็นว่า การจัดการองค์กรดิจิทัลเป็นปัจจัยสำคัญที่สุดต่อการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ขณะที่ระบบภูมิคุ้มกันดิจิทัลเป็นปัจจัยสำคัญที่สุดต่อการจัดการภูมิคุ้มกันดิจิทัล และแบบจำลองสามารถอธิบายตัวแปรผลทั้งสองได้ในระดับสูง นำมาสรุปผลการวิเคราะห์สมมติฐานได้ดังนี้

สมมติฐาน H1 : องค์ประกอบด้านโครงสร้างองค์กรส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H1 หรือองค์ประกอบด้านโครงสร้างองค์กรส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์เส้นทาง 0.02 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 70.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H2 : องค์ประกอบด้านโครงสร้างองค์กรส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการทดสอบเป็นการยอมรับ H2 หรือองค์ประกอบด้านโครงสร้างองค์กรส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์เส้นทาง 0.09 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H3 : องค์ประกอบด้านเทคโนโลยีอัจฉริยะส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H3 หรือองค์ประกอบด้านเทคโนโลยีอัจฉริยะส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์เส้นทาง 0.24 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 70.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H4 : องค์ประกอบด้านเทคโนโลยีอัจฉริยะส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการทดสอบเป็นการยอมรับ H4 หรือองค์ประกอบด้านเทคโนโลยีอัจฉริยะส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์เส้นทาง 0.10 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H5 : องค์ประกอบด้านระบบภูมิคุ้มกันดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H5 หรือองค์ประกอบด้านระบบภูมิคุ้มกันดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์เส้นทาง -0.28 ในเชิงลบ และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 70.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H6 : องค์ประกอบด้านระบบภูมิคุ้มกันดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการทดสอบเป็นการยอมรับ H6 หรือองค์ประกอบด้านระบบภูมิคุ้มกันดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์เส้นทาง 0.72 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H7 : องค์ประกอบด้านการจัดการองค์กรดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H7 หรือองค์ประกอบด้านการจัดการองค์กรดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์เส้นทาง 0.83 ในเชิงบวก และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 70.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H8 : องค์ประกอบด้านการจัดการองค์กรดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล

ผลการทดสอบเป็นการยอมรับ H8 หรือองค์ประกอบด้านการจัดการองค์กรดิจิทัลส่งอิทธิพลทางตรงต่อองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัล มีค่าสัมประสิทธิ์เส้นทาง -0.10 ในเชิงลบ และมีอิทธิพลต่อการเปลี่ยนแปลงได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐาน H9 : องค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัลได้รับอิทธิพลทางตรงและทางอ้อมจากองค์ประกอบด้านโครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล และสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการทดสอบเป็นการยอมรับ H9 หรือองค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัลได้รับอิทธิพลทั้งทางตรงและทางอ้อมจากองค์ประกอบด้านโครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล และสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ โดยแบบจำลองสามารถอธิบายการเปลี่ยนแปลงขององค์ประกอบด้านการจัดการภูมิคุ้มกันดิจิทัลได้ร้อยละ 81.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

6.1.4 ผลการประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา จากผู้เชี่ยวชาญ จำนวน 9 ท่าน พบว่า ผลการประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาโดยภาพรวม มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$=4.89, *S.D.*=0.31) เมื่อพิจารณารายด้าน พบว่า สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture) มีความเหมาะสมอยู่ในระดับมากที่สุด มีค่าเฉลี่ยสูงสุด ($\bar{X}$=4.94, *S.D.*=0.16) รองลงมาคือ สถาปัตยกรรมธรรมาภิบาล (Governance Architecture) ($\bar{X}$=4.91, *S.D.*=0.26) การจัดการองค์กรดิจิทัล (Digital Enterprise Management) ($\bar{X}$=4.91, *S.D.*=0.28) สถาปัตยกรรมภูมิคุ้มกันดิจิทัลและความเสี่ยง (Digital Immunity & Risk Architecture) ($\bar{X}$=4.91, *S.D.*=0.28) ธรรมาภิบาลองค์กร (Enterprise Governance) ($\bar{X}$=4.90, *S.D.*=0.27) เทคโนโลยีปัญญาประดิษฐ์และระบบอัจฉริยะ (Intelligent Technology) ($\bar{X}$=4.89, *S.D.*=0.30) สถาปัตยกรรมธุรกิจ (Business Architecture) ($\bar{X}$=4.89, *S.D.*=0.33) สถาปัตยกรรมแอปพลิเคชัน (Application Architecture) ($\bar{X}$=4.89, *S.D.*=0.29) การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management) ($\bar{X}$=4.89, *S.D.*=0.29) สถาปัตยกรรมข้อมูล (Data Architecture) ($\bar{X}$=4.88, *S.D.*=0.32) แหล่งข้อมูล (Data Sources) ($\bar{X}$=4.87, *S.D.*=0.35) ผู้ใช้งาน (Users) ($\bar{X}$=4.87, *S.D.*=0.27) และสถาปัตยกรรมเทคโนโลยี (Technology Architecture) ($\bar{X}$=4.84, *S.D.*=0.38) ตามลำดับ

6.2 อภิปรายผล

การวิจัยเรื่อง สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา จากการศึกษา วิเคราะห์ และสังเคราะห์เอกสาร แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง ตลอดจนการวิเคราะห์ปัจจัย การพัฒนาแบบจำลองสมการโครงสร้าง การพัฒนาสถาปัตยกรรม และการประเมินความเหมาะสมของสถาปัตยกรรมโดยผู้เชี่ยวชาญ สามารถนำผลการวิจัยมาอภิปรายผลตามวัตถุประสงค์ของการวิจัย โดยเชื่อมโยงผลการวิเคราะห์เชิงปริมาณและเชิงคุณภาพ รวมถึงบริบทการเปลี่ยนแปลงของเทคโนโลยีดิจิทัล การบริหารจัดการองค์กร และความมั่นคงปลอดภัยทางไซเบอร์ของสถาบันอุดมศึกษา ทั้งนี้ ผลการวิจัยสะท้อนให้เห็นว่า การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลจำเป็นต้องพิจารณาองค์ประกอบขององค์กร เทคโนโลยี การจัดการองค์กรดิจิทัล ระบบภูมิคุ้มกันดิจิทัล ตลอดจนการกำกับดูแลและการบริหารความเสี่ยงให้เชื่อมโยงกันอย่างเป็นระบบ โดยสามารถอภิปรายผลตามวัตถุประสงค์การวิจัยได้ดังนี้

6.2.1 อภิปรายผลตามวัตถุประสงค์ข้อที่ 1 การวิเคราะห์ปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผลการวิจัยพบว่า ปัจจัยที่เกี่ยวข้องกับการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลประกอบด้วยตัวแปรแฝง 6 ด้าน ได้แก่ โครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ และการจัดการภูมิคุ้มกันดิจิทัล โดยแต่ละด้านมีองค์ประกอบย่อยที่ครอบคลุมทั้งมิติขององค์กร ข้อมูล เทคโนโลยี ระบบสารสนเทศ ความมั่นคงปลอดภัย การกำกับดูแล และการบริหารจัดการ สะท้อนให้เห็นว่าการนำปัญญาประดิษฐ์มาใช้ในสถาบันอุดมศึกษาจำเป็นต้องดำเนินการในลักษณะองค์รวม ไม่ควรแยกการพัฒนา AI ออกจากโครงสร้างและกระบวนการบริหารจัดการขององค์กร

ประเด็นที่มีความสำคัญเป็นพิเศษคือ การจัดการองค์กรดิจิทัล (DEM) มีอิทธิพลต่อ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) สูงที่สุด โดยมีค่าสัมประสิทธิ์อิทธิพลทางตรงและอิทธิพลรวมเท่ากับ 0.83 ผลดังกล่าวสามารถอภิปรายได้ว่า การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์จำเป็นต้องมีพื้นฐานมาจากความพร้อมขององค์กร ทั้งด้านกลยุทธ์ดิจิทัล โครงสร้างพื้นฐานเทคโนโลยี การจัดการข้อมูล กระบวนการอัตโนมัติ และความมั่นคงปลอดภัยทางไซเบอร์ กล่าวคือ แม้สถาบันอุดมศึกษาจะมีเทคโนโลยี AI ที่มีประสิทธิภาพ แต่หากองค์กรยังขาดกลยุทธ์ โครงสร้างพื้นฐาน ข้อมูล และกระบวนการบริหารจัดการที่เหมาะสม ก็อาจไม่สามารถนำ AI มาใช้ให้เกิดประโยชน์ในระดับองค์กรได้อย่างเต็มศักยภาพ

นอกจากนี้ เทคโนโลยีอัจฉริยะ (AIT) มีอิทธิพลต่อ AIA เท่ากับ 0.24 สะท้อนว่าเทคโนโลยี เช่น การเรียนรู้ของเครื่อง การเรียนรู้เชิงลึก การประมวลผลภาษาธรรมชาติ และความรู้เชิงพฤติกรรม เป็นกลไกสำคัญที่ช่วยเพิ่มขีดความสามารถของสถาปัตยกรรมองค์กรให้สามารถประมวลผลข้อมูล วิเคราะห์รูปแบบความผิดปกติ สนับสนุนการตัดสินใจ และตอบสนองต่อสถานการณ์ที่มีความซับซ้อนได้ อย่างไรก็ตาม ผลดังกล่าวยังชี้ให้เห็นว่าเทคโนโลยีเพียงอย่างเดียวไม่ใช่ปัจจัยหลักที่สุด แต่ต้องทำงานร่วมกับการจัดการองค์กรดิจิทัลและองค์ประกอบด้านสถาปัตยกรรมอื่น ๆ

สำหรับ ระบบภูมิคุ้มกันดิจิทัล (DIS) พบว่ามีอิทธิพลทางตรงต่อ AIA เท่ากับ -0.28 ซึ่งเป็นความสัมพันธ์เชิงลบ ขณะที่มีอิทธิพลทางตรงต่อ DIM สูงถึง 0.72 ผลดังกล่าวควรตีความในบริบทของแบบจำลองสมการโครงสร้างที่พิจารณาตัวแปรหลายตัวพร้อมกัน โดยค่าดังกล่าวสะท้อนความสัมพันธ์ทางตรงของ DIS ต่อ AIA เมื่อควบคุมอิทธิพลของตัวแปรอื่นในแบบจำลอง มิได้หมายความว่าระบบภูมิคุ้มกันดิจิทัลเป็นปัจจัยที่ไม่พึงประสงค์ต่อองค์กร ในทางตรงกันข้าม ค่า 0.72 ที่มีต่อ DIM แสดงให้เห็นอย่างชัดเจนว่า ระบบภูมิคุ้มกันดิจิทัลเป็นพื้นฐานสำคัญของการจัดการภูมิคุ้มกันดิจิทัล โดยเฉพาะความสามารถด้านการมองเห็นและเฝ้าระวัง การตรวจจับภัยคุกคาม การสืบสวนและวิเคราะห์ การตอบสนอง การฟื้นฟู และการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย

6.2.2 อภิปรายผลตามวัตถุประสงค์ข้อที่ 2 การสร้างแบบจำลองสมการโครงสร้าง

ผลการวิเคราะห์แบบจำลองสมการโครงสร้างพบว่า แบบจำลองมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยมีค่า Chi-Square = 517.17, df = 499, p-value = 0.27784 และ RMSEA = 0.012 แสดงให้เห็นว่าแบบจำลองที่พัฒนาขึ้นสามารถอธิบายความสัมพันธ์ระหว่างปัจจัยต่าง ๆ ได้อย่างเหมาะสม อีกทั้งแบบจำลองสามารถอธิบายความแปรปรวนของ AIA ได้ ร้อยละ 70.0 (R^2 = 0.70) และสามารถอธิบายความแปรปรวนของ DIM ได้ ร้อยละ 81.0 (R^2 = 0.81) จึงสะท้อนว่าองค์ประกอบที่นำเข้าสู่แบบจำลองสามารถร่วมกันอธิบายการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์และการจัดการภูมิคุ้มกันดิจิทัลได้ในระดับสูง

เมื่อพิจารณาความสัมพันธ์ระหว่าง AIA และ DIM พบว่า AIA มีอิทธิพลทางตรงต่อ DIM เท่ากับ 0.07 แม้ขนาดอิทธิพลจะไม่สูง แต่แสดงให้เห็นถึงบทบาทของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ในฐานะกลไกเชื่อมโยงการนำ AI มาใช้กับการจัดการภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษา กล่าวคือ AIA ทำหน้าที่เป็นกรอบในการจัดวางและบูรณาการองค์ประกอบด้านองค์กร ข้อมูล ระบบสารสนเทศ เทคโนโลยี AI ความมั่นคงปลอดภัย และการกำกับดูแล เพื่อให้สามารถสนับสนุนการบริหารจัดการภูมิคุ้มกันดิจิทัลได้อย่างเป็นระบบ

6.2.3 อภิปรายผลตามวัตถุประสงค์ข้อที่ 3 การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์

ผลการวิจัยนำไปสู่การพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษาโดยบูรณาการผลจากการวิเคราะห์องค์ประกอบ ผล SEM การวิเคราะห์สภาพแวดล้อมภายในและภายนอกด้วย 7-S Model, PEST, SWOT Analysis และ TOWS Matrix รวมถึงแผนและนโยบายที่เกี่ยวข้อง และการเปลี่ยนแปลงของเทคโนโลยีดิจิทัล ผลการบูรณาการดังกล่าวทำให้สถาปัตยกรรมที่พัฒนาขึ้นไม่ได้มุ่งเน้นเฉพาะการนำ AI มาใช้ในระบบสารสนเทศ แต่ครอบคลุมถึงการกำกับดูแล การจัดการองค์กรดิจิทัล ความมั่นคงปลอดภัย ระบบภูมิคุ้มกันดิจิทัล การบริหารความเสี่ยง และการจัดการภูมิคุ้มกันดิจิทัล

โครงสร้างสถาปัตยกรรมจึงมีลักษณะเป็นระบบที่เชื่อมโยงตั้งแต่ระดับธรรมาภิบาลองค์กร (Enterprise Governance) ลงสู่ระดับสถาปัตยกรรมองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล และการจัดการภูมิคุ้มกันดิจิทัล โดยมีข้อมูล ผู้ใช้งาน และโครงสร้างพื้นฐานดิจิทัลเป็นองค์ประกอบสนับสนุน การออกแบบในลักษณะดังกล่าวสอดคล้องกับบริบทของสถาบันอุดมศึกษาที่มีระบบสารสนเทศและข้อมูลจำนวนมาก รวมถึงมีผู้ใช้งานหลากหลายกลุ่ม จึงจำเป็นต้องมีสถาปัตยกรรมที่สามารถบูรณาการระบบเดิมกับเทคโนโลยีใหม่ และสามารถปรับตัวต่อการเปลี่ยนแปลงของภัยคุกคามและเทคโนโลยีได้อย่างต่อเนื่อง

6.2.4 อภิปรายผลตามวัตถุประสงค์ข้อที่ 4 การประเมินความเหมาะสมของสถาปัตยกรรม

ผลการประเมินความเหมาะสมของสถาปัตยกรรมโดยผู้เชี่ยวชาญจากสถาบันอุดมศึกษา จำนวน 9 คน พบว่า สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษามีความเหมาะสมในภาพรวมในระดับสูงมาก โดยมีค่าเฉลี่ยรวม 4.89 ผลการประเมินดังกล่าวสะท้อนว่าองค์ประกอบ โครงสร้าง และความสัมพันธ์ของสถาปัตยกรรมที่พัฒนาขึ้นมีความเหมาะสมต่อการนำไปประยุกต์ใช้ในบริบทของสถาบันอุดมศึกษา

ผลการประเมินยังสนับสนุนผลการวิเคราะห์เชิงปริมาณจากแบบจำลอง SEM กล่าวคือ ผล SEM ชี้ให้เห็นถึงความสำคัญของการจัดการองค์กรดิจิทัล ระบบภูมิคุ้มกันดิจิทัล และสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ ขณะที่การประเมินโดยผู้เชี่ยวชาญสะท้อนความเหมาะสมของการนำองค์ประกอบเหล่านี้มาบูรณาการเป็นสถาปัตยกรรมในระดับองค์กร จึงกล่าวได้ว่า ผลการวิจัยทั้งสองส่วนมีความสอดคล้องและสนับสนุนซึ่งกันและกัน โดยเฉพาะแนวคิดที่ว่า การสร้างภูมิคุ้มกันดิจิทัลของสถาบันอุดมศึกษาไม่ควรดำเนินการในลักษณะของระบบรักษาความปลอดภัยที่แยกส่วน แต่ควรเป็นความสามารถเชิงองค์กรที่บูรณาการ AI ข้อมูล เทคโนโลยี กระบวนการ บุคลากร การกำกับดูแล และการบริหารความเสี่ยงเข้าด้วยกัน

ผลการอภิปรายทั้งหมดแสดงให้เห็นว่า สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เป็นกลไกสำคัญในการเชื่อมโยงความสามารถด้านการจัดการองค์กรดิจิทัลและเทคโนโลยีอัจฉริยะเข้ากับการจัดการภูมิคุ้มกันดิจิทัล โดยการจัดการองค์กรดิจิทัลเป็นปัจจัยที่มีอิทธิพลต่อ AIA สูงที่สุด ขณะที่ระบบภูมิคุ้มกันดิจิทัลเป็นปัจจัยที่มีอิทธิพลต่อ DIM สูงที่สุด และแบบจำลองสามารถอธิบายความแปรปรวนของ AIA และ DIM ได้ร้อยละ 70 และ 81 ตามลำดับ ประกอบกับผลการประเมินจากผู้เชี่ยวชาญที่มีค่าเฉลี่ยรวม 4.89 จึงสนับสนุนว่าสถาปัตยกรรมที่พัฒนาขึ้นมีทั้ง ความสอดคล้องเชิงทฤษฎี ความเหมาะสมเชิงโครงสร้าง และความเหมาะสมต่อการประยุกต์ใช้ในบริบทของสถาบันอุดมศึกษา

6.3 ข้อเสนอแนะ

จากผลการวิจัยเรื่องสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ซึ่งได้จากการวิเคราะห์ปัจจัย การสร้างแบบจำลองสมการโครงสร้าง การพัฒนาสถาปัตยกรรม และการประเมินความเหมาะสมโดยผู้เชี่ยวชาญ ผู้วิจัยมีข้อเสนอแนะในการนำผลการวิจัยไปประยุกต์ใช้และสำหรับการวิจัยครั้งถัดไป ดังนี้

6.3.1 ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

6.3.1.1 การนำสถาปัตยกรรมไปใช้ควรพิจารณาตามบริบทของสถาบันอุดมศึกษา เนื่องจากสถาบันอุดมศึกษาแต่ละแห่งมีความแตกต่างกันด้านขนาด โครงสร้างองค์กร พันธกิจ ระบบสารสนเทศ โครงสร้างพื้นฐานดิจิทัล บุคลากร งบประมาณ การบริหารจัดการข้อมูล และระดับความพร้อมด้านปัญญาประดิษฐ์และความมั่นคงปลอดภัยทางไซเบอร์ ดังนั้น ก่อนนำสถาปัตยกรรมไป

ประยุกต์ใช้ ควรจำแนกหรือพิจารณากลุ่มของสถาบันตามบริบทและระดับความพร้อม เพื่อกำหนดแนวทางการพัฒนาที่เหมาะสมกับแต่ละสถาบัน ไม่ควรนำสถาปัตยกรรมไปใช้ในรูปแบบเดียวกันทั้งหมด

6.3.1.2 สถาบันอุดมศึกษาควรประเมินสภาพปัจจุบันและระดับความพร้อมก่อนนำสถาปัตยกรรมไปใช้ โดยพิจารณาด้านโครงสร้างองค์กร เทคโนโลยีอัจฉริยะ ระบบภูมิคุ้มกันดิจิทัล การจัดการองค์กรดิจิทัล ข้อมูล ระบบงาน โครงสร้างพื้นฐาน และการกำกับดูแล เพื่อวิเคราะห์ช่องว่างระหว่างสถาปัตยกรรมปัจจุบัน (Current Architecture) กับสถาปัตยกรรมเป้าหมาย (Target Architecture) และนำผลไปกำหนดลำดับความสำคัญของการพัฒนา

6.3.1.3 ควรจัดทำแผนที่นำทาง (Roadmap) สำหรับการพัฒนาสถาปัตยกรรมของแต่ละสถาบัน โดยนำผลการประเมินความพร้อมและการวิเคราะห์ช่องว่างมาใช้กำหนดเป้าหมาย ลำดับการดำเนินงาน โครงการ งบประมาณ ผู้รับผิดชอบ และระยะเวลาในการพัฒนา ทั้งนี้ Roadmap ควรสามารถปรับเปลี่ยนได้ตามบริบทและระดับความพร้อมของสถาบันอุดมศึกษาแต่ละแห่ง

6.3.1.4 การนำสถาปัตยกรรมไปสู่การใช้งานจริง (Deployment) ควรดำเนินการเป็นลำดับขั้น เริ่มจากการประเมินความพร้อมของสถาบัน การวิเคราะห์ช่องว่าง การกำหนดสถาปัตยกรรมเป้าหมายและ Roadmap จากนั้นจึงเลือกหน่วยงานหรือระบบงานที่เหมาะสมสำหรับการทดลองใช้ (Pilot Implementation) ติดตามและประเมินผล ปรับปรุงสถาปัตยกรรมจากผลการใช้งานจริง และจึงขยายผลไปสู่หน่วยงานหรือระบบอื่นในระดับสถาบัน

6.3.1.5 ควรให้ความสำคัญกับการจัดการองค์กรดิจิทัลเป็นกลไกสำคัญในการพัฒนาสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เนื่องจากผลการวิเคราะห์แบบจำลองสมการโครงสร้างพบว่าการจัดการองค์กรดิจิทัล (DEM) มีอิทธิพลทางตรงต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AIA) สูงที่สุด โดยมีค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.83 ดังนั้น สถาบันควรให้ความสำคัญกับกลยุทธ์ดิจิทัล โครงสร้างพื้นฐานเทคโนโลยี การจัดการข้อมูล กระบวนการอัตโนมัติ และความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นระบบ

6.3.1.6 ควรพัฒนาระบบภูมิคุ้มกันดิจิทัลให้เป็นความสามารถระดับองค์กร โดยครอบคลุมการมองเห็นและเฝ้าระวัง การตรวจจับภัยคุกคาม การสืบสวนและวิเคราะห์ การตอบสนองและการป้องกันเชิงรุก ความทนทานและการฟื้นฟู ตลอดจนความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อสนับสนุนการจัดการภูมิคุ้มกันดิจิทัลอย่างต่อเนื่องและเป็นระบบ

6.3.1.7 ควรนำเทคโนโลยีปัญญาประดิษฐ์มาใช้สนับสนุนการดำเนินงานอย่างเหมาะสม ได้แก่ Machine Learning, Deep Learning, Natural Language Processing และ

Behavioral AI เพื่อสนับสนุนการวิเคราะห์ข้อมูล การตรวจจับความผิดปกติ การประเมินความเสี่ยง และการตัดสินใจ โดยต้องดำเนินการภายใต้การกำกับดูแลด้านจริยธรรม ความโปร่งใส ความรับผิดชอบ ความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล

6.3.1.8 ควรจัดให้มีกลไกการกำกับดูแลปัญญาประดิษฐ์ ข้อมูล และความมั่นคงปลอดภัยในระดับองค์กร โดยกำหนดนโยบาย บทบาท หน้าที่ ความรับผิดชอบ มาตรฐาน และกระบวนการกำกับดูแลที่ชัดเจน รวมถึงพัฒนาบุคลากรและสร้างความตระหนักรู้ด้าน AI และ Cybersecurity ให้แก่ผู้บริหาร บุคลากร นักศึกษา และผู้เกี่ยวข้องอย่างต่อเนื่อง

6.3.1.9 ควรติดตาม ประเมินผล และปรับปรุงสถาปัตยกรรมอย่างต่อเนื่อง เนื่องจากเทคโนโลยีปัญญาประดิษฐ์ รูปแบบภัยคุกคามทางไซเบอร์ กฎหมาย และมาตรฐานมีการเปลี่ยนแปลงสถาบันจึงควรกำหนดวงจรการประเมินและทบทวนสถาปัตยกรรมให้สอดคล้องกับบริบท ความเสี่ยง และความพร้อมขององค์กรที่เปลี่ยนแปลงไป

6.3.2 ข้อเสนอแนะสำหรับการวิจัยครั้งถัดไป

6.3.2.1 ควรนำสถาปัตยกรรมที่พัฒนาขึ้นไปทดลองใช้ในสถาบันอุดมศึกษาจริง เพื่อศึกษาความเป็นไปได้ ประสิทธิผล ปัญหาและข้อจำกัดในการนำสถาปัตยกรรมไปสู่การใช้งานจริง และนำผลที่ได้มาปรับปรุงสถาปัตยกรรมให้เหมาะสมยิ่งขึ้น

6.3.2.2 ควรศึกษาการประยุกต์ใช้สถาปัตยกรรมในสถาบันอุดมศึกษาที่มีประเภท ขนาด พันธกิจ และระดับความพร้อมด้านดิจิทัลแตกต่างกัน เพื่อเปรียบเทียบปัจจัย เงื่อนไข และแนวทางการนำสถาปัตยกรรมไปใช้ตามบริบทของแต่ละสถาบัน

6.3.2.3 ควรพัฒนาแบบประเมินระดับความพร้อมหรือแบบจำลองระดับวุฒิภาวะ (Maturity Model) เพื่อจำแนกระดับความพร้อมของสถาบัน และใช้เป็นข้อมูลสำหรับกำหนด Roadmap ในการพัฒนาจากสถาปัตยกรรมปัจจุบันไปสู่สถาปัตยกรรมเป้าหมาย

6.3.2.4 ควรศึกษาปัจจัยเพิ่มเติมที่อาจมีผลต่อการนำสถาปัตยกรรมไปใช้ เช่น ความพร้อมของบุคลากร วัฒนธรรมองค์กร ภาวะผู้นำดิจิทัล งบประมาณ และการบริหารการเปลี่ยนแปลง เพื่อขยายแบบจำลองให้ครอบคลุมปัจจัยเชิงองค์กรและการนำไปใช้จริงมากยิ่งขึ้น

6.3.2.5 ควรศึกษาการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์รูปแบบใหม่ เช่น Generative AI และ AI Agent ร่วมกับการจัดการภูมิคุ้มกันดิจิทัล โดยพิจารณาประเด็นด้านธรรมาภิบาลข้อมูล ความมั่นคงปลอดภัย ความเป็นส่วนตัว จริยธรรม และการปฏิบัติตามกฎหมาย

6.3.2.6 ควรศึกษาติดตามผลในระยะยาวภายหลังการนำสถาปัตยกรรมไปใช้ เพื่อประเมินการเปลี่ยนแปลงด้านประสิทธิผล ความพร้อม ความเสี่ยง และความสามารถในการปรับตัวของสถาบันต่อการเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคามทางไซเบอร์

บรรณานุกรม

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022a). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. In *Electronics (Switzerland)* (Vol. 11, Number 2). MDPI. https://doi.org/10.3390/electronics11020198

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022b). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. In *Electronics (Switzerland)* (Vol. 11, Number 2). MDPI. https://doi.org/10.3390/electronics11020198

Achaal, B., Adda, M., Berger, M., Ibrahim, H., & Awde, A. (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity*, *7*(1). https://doi.org/10.1186/s42400-023-00200-w

Adegbenjo, A. A., Onuiri, E. E., Kalesanwo, O. B., Agbaje, M. O., Abel, S. B., Fatade, O. B., Amusa, A. I., Umeaka, K. C., Ehioghae, E., & Onamade, K. O. (2023). Design and Analysis of an Automated IoT System for Data Flow Optimization in Higher Education Institutions. *Journal Europeen Des Systemes Automatises*, *56*(5), 889–897. https://doi.org/10.18280/jesa.560520

Al-Fugaha, Z. N. A., Alshurideh, M. T., Zighan, S. M., Alzoubi, A. E., Shatnawi, T. M., Aityassine, F. L. Y., Al-Aawawdeh, R., Alzyoud, M., Mohammad, A. A. S., & Al-Hawary, S. I. S. (2024). The Impact of Implementing Disruptive Technology on Organizational Change: A

Field Study in Private Universities in Jordan. In *Studies in Computational Intelligence* (Vol. 1151). https://doi.org/10.1007/978-3-031-56015-6_31

Alghamdi, H. (2024). Assessing the Impact of Enterprise Architecture on Digital Transformation Success: A Global Perspective. *Sustainability (Switzerland)*, *16*(20). https://doi.org/10.3390/su16208865

Alghushami, A. H., Zakaria, N. H., & Aji, Z. M. (2020). Factors influencing cloud computing adoption in higher education institutions of least developed countries: Evidence from Republic of Yemen. *Applied Sciences (Switzerland)*, *10*(22), 1–27. https://doi.org/10.3390/app10228098

Ali, N. H., Jalil, M., Jarno, A. D., Salimin, N., & Alamiah, M. (2025). A Framework for the Development of Risk-Based Guidelines for Cloud Service Subscribers. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *48*(2), 136–147. https://doi.org/10.37934/araset.48.2.136147

Alkhwaldi, A. F. (2023). Understanding learners' intention toward Metaverse in higher education institutions from a developing country perspective: UTAUT and ISS integrated model. *Kybernetes*. https://doi.org/10.1108/K-03-2023-0459

Alkhwaldi, A. F. (2024). Investigating the Social Sustainability of Immersive Virtual Technologies in Higher Educational Institutions: Students' Perceptions toward Metaverse Technology. *Sustainability (Switzerland)*, *16*(2). https://doi.org/10.3390/su16020934

Alotaibi, N. S., & Alshehri, A. H. (2023). Prospers and Obstacles in Using Artificial Intelligence in Saudi Arabia Higher Education

Institutions—The Potential of AI-Based Learning Outcomes. *Sustainability (Switzerland)*, *15*(13). https://doi.org/10.3390/su151310723

Al-Tarawneh, A., Haddad, E., Al-Dwairi, R. M., Al-Freijat, S. Y., Mansour, A., & Al-Obaidly, G. A. (2024). The impact of strategic and innovativeness entrepreneurship and social capital on business overall performance through building a sustainable supply chain management at Jordan Private Universities. *Uncertain Supply Chain Management*, *12*(1), 65–76. https://doi.org/10.5267/j.uscm.2023.10.017

Al-Turkistani, H. F., Aldobaian, S., & Latif, R. (2021a). Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review. *2021 1st International Conference on Artificial Intelligence and Data Analytics, CAIDA 2021*, 79–84. https://doi.org/10.1109/CAIDA51941.2021.9425343

Al-Turkistani, H. F., Aldobaian, S., & Latif, R. (2021b). Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review. *2021 1st International Conference on Artificial Intelligence and Data Analytics, CAIDA 2021*, 79–84. https://doi.org/10.1109/CAIDA51941.2021.9425343

Amin, F. A., Hussein, S. S., Daud, N. A., Bakar, N. A. A., & Ahmad, W. A. Z. W. (2024). Cultivating excellence: a case study of enterprise architecture transformational journey in higher education. *Indonesian Journal of Electrical Engineering and Computer Science*, *34*(1), 548–555. https://doi.org/10.11591/ijeecs.v34.i1.pp548-555

Andriushchenko, K., Rudyk, V., Riabchenko, O., Kachynska, M., Marynenko, N., Shergina, L., Kovtun, V., Tepliuk, M., Zhemba, A., & Kuchai, O. (2019). Processes of managing information infrastructure of a digital enterprise in the framework of the «Industry 4.0» concept. *Eastern-European Journal of Enterprise Technologies*, *1*(3–97), 60–72. https://doi.org/10.15587/1729-4061.2019.157765

Andry, J. F., Liliana, L., & Chakir, A. (2021). Enterprise architecture landscape using zachman framework and ward peppard analysis for electrical equipment export import company. *Trends in Sciences*, *18*(19). https://doi.org/10.48048/tis.2021.23

Anes Silveira, R., & Mamede, H. S. (2024). Strengthening the Resilience and Perseverance of Rural Accommodation Enterprises in the Iberian Depopulated Areas through Enterprise Architecture. *Sustainability (Switzerland)*, *16*(2). https://doi.org/10.3390/su16020533

Anthony Jnr, B., Abbas Petersen, S., Helfert, M., Ahlers, D., & Krogstie, J. (2021). Modeling pervasive platforms and digital services for smart urban transformation using an enterprise architecture framework. *Information Technology and People*, *34*(4), 1285–1312. https://doi.org/10.1108/ITP-07-2020-0511

Aoun, C. G., Mansour, N., Dornaika, F., & Lagadec, L. (2024a). Environmental Constraints for Intelligent Internet of Deep-Sea/Underwater Things Relying on Enterprise Architecture Approach. *Sensors*, *24*(8). https://doi.org/10.3390/s24082433

Aoun, C. G., Mansour, N., Dornaika, F., & Lagadec, L. (2024b). Environmental Constraints for Intelligent Internet of Deep-Sea/Underwater Things Relying on Enterprise Architecture Approach. *Sensors*, *24*(8). https://doi.org/10.3390/s24082433

Aprilia, K., Lee, F. S., Geasela, Y. M., Everlin, S., & Tampinongkol, F. F. (2024a). Design of Enterprise Architecture Using Zachman Framework at Private School in Center Jakarta. *Journal of Computer Science*, *20*(9), 1059–1068. https://doi.org/10.3844/JCSSP.2024.1059.1068

Aprilia, K., Lee, F. S., Geasela, Y. M., Everlin, S., & Tampinongkol, F. F. (2024b). Design of Enterprise Architecture Using Zachman Framework at Private School in Center Jakarta. *Journal of Computer Science*, *20*(9), 1059–1068. https://doi.org/10.3844/JCSSP.2024.1059.1068

Ashani, Z. N., Ilias, I. S. C., Ng, K. Y., Ariffin, M. R. K., Jarno, A. D., & Zamri, N. Z. (2025). Comparative Analysis of Deepfake Image Detection Method Using VGG16, VGG19 and ResNet50. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *47*(1), 16–28. https://doi.org/10.37934/araset.47.1.1628

Atencio, E., Mancini, M., & Bustos, G. (2024a). Enterprise architecture approach for project-based organizations modeling, design, and analysis: An ontology-driven tool proposal. *Alexandria Engineering Journal*, *98*, 312–327. https://doi.org/10.1016/j.aej.2024.04.052

Atencio, E., Mancini, M., & Bustos, G. (2024b). Enterprise architecture approach for project-based organizations modeling, design, and analysis: An ontology-driven tool proposal. *Alexandria Engineering Journal*, *98*, 312–327. https://doi.org/10.1016/j.aej.2024.04.052

Avkiran, N. K. (2018). Measuring the Systemic Risk of Regional Banks in Japan with PLS-SEM. *Theoretical Economics Letters*, *08*(11), 2024–2037. https://doi.org/10.4236/tel.2018.811132

Baidoo-Anu, D., & Owusu Ansah, L. (2023). Education in the Era of Generative Artificial Intelligence (AI): Understanding the Potential Benefits of ChatGPT in Promoting Teaching and Learning. In *Journal of AI* (Vol. 52, Number 7).

Barradas, A., Tejeda-Gil, A., & Cantón-Croda, R.-M. (2022). Real-Time Big Data Architecture for Processing Cryptocurrency and Social Media Data: A Clustering Approach Based on k-Means. *Algorithms*, *15*(5). https://doi.org/10.3390/a15050140

Beheshti, A., Yang, J., Sheng, Q. Z., Benatallah, B., Casati, F., Dustdar, S., Nezhad, H. R. M., Zhang, X., & Xue, S. (2023). ProcessGPT: Transforming Business Process Management with Generative Artificial Intelligence. *Proceedings - 2023 IEEE International Conference on Web Services, ICWS 2023*, 731–739. https://doi.org/10.1109/ICWS60048.2023.00099

Benvenuti, M., Cangelosi, A., Weinberger, A., Mazzoni, E., Benassi, M., Barbaresi, M., & Orsoni, M. (2023). Artificial intelligence and human behavioral development: A perspective on new skills and competences acquisition for the educational context. *Computers in Human Behavior*, *148*. https://doi.org/10.1016/j.chb.2023.107903

Bhatia, K., Pandey, S. K., Singh, V. K., & Gupta, D. N. (2023). Enterprises in the Era of Industry 5.0. *Proceedings of the 17th INDIACom; 2023 10th International Conference on Computing for Sustainable Global Development, INDIACom 2023*, 1065–1069.

Bhatt, D. G., Kyada, P. U., Rathore, R. S., Nallakaruppan, M. K., Alotaibi, F. M., & Jhaveri, R. H. (2025). Enhancing Anomaly Detection in Industrial Control Systems through Supervised Learning and Explainable

Artificial Intelligence. *Journal of Cybersecurity and Information Management*, *15*(1), 314–331. https://doi.org/10.54216/JCIM.150125

Binz, M., Dasgupta, I., Jagadish, A., Botvinick, M., Wang, J. X., & Schulz, E. (2024). Meta-learning: Data, architecture, and both. *The Behavioral and Brain Sciences*, *47*, e170. https://doi.org/10.1017/S0140525X24000311

Branytskyi, V., Golovianko, M., Gryshko, S., Malyk, D., Terziyan, V., & Tuunanen, T. (2022). Digital clones and digital immunity: adversarial training handles both. *International Journal of Simulation and Process Modelling*, *18*(2), 124–139. https://doi.org/10.1504/ijspm.2022.126106

Camatti, J. A., Rabelo, G. M., Borsato, M., & Pellicciari, M. (2020a). Comparative study of open IoT architectures with TOGAF for industry implementation. *Procedia Manufacturing*, *51*, 1132–1137. https://doi.org/10.1016/j.promfg.2020.10.159

Camatti, J. A., Rabelo, G. M., Borsato, M., & Pellicciari, M. (2020b). Comparative study of open IoT architectures with TOGAF for industry implementation. *Procedia Manufacturing*, *51*, 1132–1137. https://doi.org/10.1016/j.promfg.2020.10.159

Carlo, A., & Obergfaell, K. (2024). Cyber attacks on critical infrastructures and satellite communications. *International Journal of Critical Infrastructure Protection*, *46*. https://doi.org/10.1016/j.ijcip.2024.100701

Chandra, Y., & Legowo, N. (2022a). UTILIZING DATA FRAMEWORK TO SUPPORT DECISION MAKING PROCESS WITH ENTERPRISE ARCHITECTURE APPROACH BY USING TOGAF FRAMEWORK. *Journal*

of Theoretical and Applied Information Technology, *100*(20), 6226–6232.

Chandra, Y., & Legowo, N. (2022b). UTILIZING DATA FRAMEWORK TO SUPPORT DECISION MAKING PROCESS WITH ENTERPRISE ARCHITECTURE APPROACH BY USING TOGAF FRAMEWORK. *Journal of Theoretical and Applied Information Technology*, *100*(20), 6226–6232.

Chen, Y. J., Lin, L. C., Yang, S. T., Hwang, K. S., Liao, C. Te, & Ho, W. H. (2023). High-Reliability Non-Contact Photoplethysmography Imaging for Newborn Care by a Generative Artificial Intelligence. *IEEE Access*, *11*, 90801–90810. https://doi.org/10.1109/ACCESS.2023.3307637

Chenchen, J., Bin, X., & Li, T. X. (2023). Practices and Insights of Digital Transformation in Financial Management Education at Private Universities. *World Journal of Education and Humanities*, *5*(3), p134. https://doi.org/10.22158/wjeh.v5n3p134

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information (Switzerland)*, *13*(4). https://doi.org/10.3390/info13040192

Chiu, Y. H., & Chen, C. C. (2023). Investigating the Impact of Generative Artificial Intelligence on Brainstorming: A Preliminary Study. *2023 International Conference on Consumer Electronics - Taiwan, ICCE-Taiwan 2023 - Proceedings*, 193–194. https://doi.org/10.1109/ICCE-Taiwan58799.2023.10226617

Costa, A. B., & Brito, M. A. (2022). Enterprise Architecture Management Constant maintenance and updating of the Enterprise

Architecture. *Iberian Conference on Information Systems and Technologies, CISTI*, *2022-June*. https://doi.org/10.23919/CISTI54924.2022.9820068

Crespi, N., Drobot, A. T., & Minerva, R. (2023). The Digital Twin. In *The Digital Twin* (Vols. 1–2). https://doi.org/10.1007/978-3-031-21343-4

Denhere, P. T., Ruhode, E., & Zhou, M. (2023). A TOGAF based interoperable health information system needs assessment for practitioner–patient interaction. *Electronic Journal of Information Systems in Developing Countries*, *89*(6). https://doi.org/10.1002/isd2.12284

Denni-Fiberesima, D. (2024). Navigating the Generative AI-Enabled Enterprise Architecture Landscape: Critical Success Factors for AI Adoption and Strategic Integration. In *Lecture Notes in Networks and Systems: 1082 LNNS*. https://doi.org/10.1007/978-3-031-67434-1_20

Draxler-Weber, N., Paul, F.-H., & Hoppe, U. (2024). Continuing Digital Higher Education Teaching in the post COVID-19 Era: A Qualitative Survey on Success Factors. *International Conference on Higher Education Advances*, 724–731. https://doi.org/10.4995/HEAd24.2024.17257

Dumitriu, D., & Popescu, M. A. M. (2020a). Enterprise architecture framework design in IT management. *Procedia Manufacturing*, *46*, 932–940. https://doi.org/10.1016/j.promfg.2020.05.011

Dumitriu, D., & Popescu, M. A. M. (2020b). Enterprise architecture framework design in IT management. *Procedia Manufacturing*, *46*, 932–940. https://doi.org/10.1016/j.promfg.2020.05.011

Dwivedi, S., & Vig, S. (2023). Institutional Readiness to adopt Block Chain Technology in Higher Education. *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*. https://doi.org/10.1109/ICCCNT56998.2023.10308125

Egeten, A. E. J. (2023). Enterprise Architecture Framework in E-Marketplace Based on IT Governance - A Systematic Literature Review. *1st International Conference on Technology, Engineering, and Computing Applications: Trends in Technology Development in the Era of Society 5.0, ICTECA 2023*. https://doi.org/10.1109/ICTECA60133.2023.10490840

Fitriani, L., Khodra, M. L., & Surendro, K. (2023a). TOGAF-based Enterprise Architecture Framework for Utilizing Artificial Intelligence. *Proceedings - 2023 10th International Conference on Computer, Control, Informatics and Its Applications: Exploring the Power of Data: Leveraging Information to Drive Digital Innovation, IC3INA 2023*, 90–95. https://doi.org/10.1109/IC3INA60834.2023.10285801

Fitriani, L., Khodra, M. L., & Surendro, K. (2023b). TOGAF-based Enterprise Architecture Framework for Utilizing Artificial Intelligence. *Proceedings - 2023 10th International Conference on Computer, Control, Informatics and Its Applications: Exploring the Power of Data: Leveraging Information to Drive Digital Innovation, IC3INA 2023*, 90–95. https://doi.org/10.1109/IC3INA60834.2023.10285801

Frincu, S., & Frincu, M. (2025). Enabling Interdisciplinary Learning and Research through AI-Driven Transliteration of Historical Documents: A Case Study Proposal from Digital Humanities.

International Journal of Humanities Education, *23*(1), 1–24. https://doi.org/10.18848/2327-0063/CGP/v23i01/1-24

Gellweiler, C. (2020). Connecting enterprise architecture and project portfolio management: A review and a model for IT project alignment. *International Journal of Information Technology Project Management*, *11*(1), 99–114. https://doi.org/10.4018/IJITPM.2020010106

George, A. S., & Hovan George, A. S. (2023). *FMCG's Digital Dilemma: The Consequences of Insufficient IT Expertise in the Fast-Moving Consumer Goods Industry Partners Universal International Innovation Journal (PUIIJ) FMCG's Digital Dilemma: The Consequences of Insufficient IT Expertise in the Fast-Moving Consumer Goods Industry*. https://doi.org/10.5281/zenodo.8066759

George, A. S., Hovan George, A. S., & Baskar, T. (2023a). *Partners Universal International Innovation Journal (PUIIJ) Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats*. https://doi.org/10.5281/zenodo.8274514

George, A. S., Hovan George, A. S., & Baskar, T. (2023b). *Partners Universal International Innovation Journal (PUIIJ) Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats*. https://doi.org/10.5281/zenodo.8274514

George, A. S., Hovan George, A. S., & Baskar, T. (2023c). *Partners Universal International Innovation Journal (PUIIJ) Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats*. https://doi.org/10.5281/zenodo.8274514

George, A. S., Hovan George, A. S., & Baskar, T. (2023d). *Partners Universal International Innovation Journal (PUIIJ) Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats*. https://doi.org/10.5281/zenodo.8274514

Ghahremani-Nahr, J., Parviznejad, P. S., & Nozari, H. (2023). Applying the Zachman Framework for the Enterprise Architecture of Research Organizations (Case Study: Academic Center for Education, Culture and Research of Iran). *Journal of Industrial Integration and Management*. https://doi.org/10.1142/S2424862223500033

Golby, J., & Wood, P. (2016). The Effects of Psychological Skills Training on Mental Toughness and Psychological Well-Being of Student-Athletes. *Psychology*, *07*(06), 901–913. https://doi.org/10.4236/psych.2016.76092

Gomes, R., Da Cruz, A. M. R., & Cruz, E. F. (2020). EA in the Digital Transformation of Higher Education Institutions. *Iberian Conference on Information Systems and Technologies, CISTI*, *2020-June*. https://doi.org/10.23919/CISTI49556.2020.9141086

Guo, H., Petersen, S. A., Gao, S., Li, J., & Bokolo, A. J. (2020). Embracing modern technologies and urban development trends: Initial evaluation of a smart city enterprise architecture frameworks. In *Lecture Notes in Business Information Processing: 381 LNBIP*. https://doi.org/10.1007/978-3-030-44322-1_19

Haipinge, E., & Kadhila, N. (2024). Models of Quality Assurance: Towards a Quality Assurance Framework of Digital Learning in Higher Education in Africa. In *Sustainable Development Goals Series: Part F3144*. https://doi.org/10.1007/978-3-031-46242-9_2

Halgamuge, M. N., & Niyato, D. (2025). Adaptive edge security framework for dynamic IoT security policies in diverse environments. *Computers and Security*, *148*. https://doi.org/10.1016/j.cose.2024.104128

Han, L., Long, X., & Wang, K. (2024). The analysis of educational informatization management learning model under the internet of things and artificial intelligence. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-68963-x

Han, X., Zheng, G., Jin, B., Zhou, M., Chen, Q., Xu, Z., & Fu, L. (2021). Application of Artificial Intelligence Technology in Power Grid Enterprises based on Enterprise Architecture Method. *Journal of Physics: Conference Series*, *1756*(1). https://doi.org/10.1088/1742-6596/1756/1/012016

Hanandeh, R., Alharafsheh, M., Albloush, A., Lehyeh, S. M. A., & Kilani, Q. (2024). The impact of entrepreneurship self-concept, work motivation, and risk taking on human resource department performance and business overall performance at Jordan private universities. *Uncertain Supply Chain Management*, *12*(1), 143–150. https://doi.org/10.5267/j.uscm.2023.10.010

Hassanin, M., Keshk, M., Salim, S., Alsubaie, M., & Sharma, D. (2025). PLLM-CS: Pre-trained Large Language Model (LLM) for cyber threat detection in satellite networks. In *Ad Hoc Networks* (Vol. 166). Elsevier B.V. https://doi.org/10.1016/j.adhoc.2024.103645

Hemachandran, K., Verma, P., Pareek, P., Arora, N., Rajesh Kumar, K. V., Ahanger, T. A., Pise, A. A., & Ratna, R. (2022). Artificial Intelligence: A Universal Virtual Tool to Augment Tutoring in Higher Education. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/1410448

Hidayat, M., & Pamuji, G. C. (2023). Optimizing New Student Admissions System Using Zachman Framework for Vocational High School: Case Study at SMK Al Hikmah Anjatan. *INCITEST 2023 - Proceedings of the 2023 International Conference on Informatics Engineering, Science and Technology*. https://doi.org/10.1109/INCITEST59455.2023.10397056

Hiran, K. K., & Dadhich, M. (2024). Predicting the core determinants of cloud-edge computing adoption (CECA) for sustainable development in the higher education institutions of Africa: A high order SEM-ANN analytical approach. *Technological Forecasting and Social Change*, *199*. https://doi.org/10.1016/j.techfore.2023.122979

Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. C., Ávila, M., & Caro, A. (2024a). A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review*, *57*(8). https://doi.org/10.1007/s10462-024-10805-3

Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. C., Ávila, M., & Caro, A. (2024b). A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review*, *57*(8). https://doi.org/10.1007/s10462-024-10805-3

Hossain, E., Cox, A. L., Dowthwaite, A., & Rogers, Y. (2024). Adaptive, Sociable and Ready for Anything: Undergraduate Students Are Resilient When Faced with Technological Change. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1). https://doi.org/10.1145/3653689

Hossain, Md. A., Ahammad, I., Ahmed, Md. K., & Ahmed, M. I. (2023). Prediction of the Computer Science Department's Educational Performance Through Machine Learning Model by Analyzing

Students' Academic Statements. *Artificial Intelligence Evolution*, 70–87. https://doi.org/10.37256/aie.4120232569

Hrosul, V., Buhrimenko, R., Kolesnyk, A., Smirnova, P., & Balamut, H. (2022a). Adaptive Management of Business Entities in the Context of Digitalization of the Economy. *Economic Affairs (New Delhi)*, *67*(4), 947–957. https://doi.org/10.46852/0424-2513.4s.2022.28

Hrosul, V., Buhrimenko, R., Kolesnyk, A., Smirnova, P., & Balamut, H. (2022b). Adaptive Management of Business Entities in the Context of Digitalization of the Economy. *Economic Affairs (New Delhi)*, *67*(4), 947–957. https://doi.org/10.46852/0424-2513.4s.2022.28

Huang, H., Li, T., Ding, Y., Li, B., & Liu, A. (2023a). An artificial immunity based intrusion detection system for unknown cyberattacks. *Applied Soft Computing*, *148*. https://doi.org/10.1016/j.asoc.2023.110875

Huang, H., Li, T., Ding, Y., Li, B., & Liu, A. (2023b). An artificial immunity based intrusion detection system for unknown cyberattacks. *Applied Soft Computing*, *148*. https://doi.org/10.1016/j.asoc.2023.110875

Hussein, S. S., Alfiansyah, M. W., Daud, R., Ya'acob, S., & Lokman, A. M. (2023). Developing an Effective ICT Strategic Framework for Higher Education Institutions: A Case of Mataram University. In *Communications in Computer and Information Science: 1825 CCIS*. https://doi.org/10.1007/978-3-031-34045-1_18

Integrating Machine Learning with Two-Person Intuitionistic Neutrosophic Soft Games for Cyberthreat Detection in Blockchain Environment.

(2025). *International Journal of Neutrosophic Science*, *25*(2). https://doi.org/10.54216/ijns.250204

Jiang, W., Liu, B., Wang, C., & Yang, X. (2021). Security-Oriented Network Architecture. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/6694650

Jiang, Y., Jeusfeld, M. A., Mosaad, M., & Oo, N. (2024a). Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review. *International Journal of Critical Infrastructure Protection*, *46*. https://doi.org/10.1016/j.ijcip.2024.100700

Jiang, Y., Jeusfeld, M. A., Mosaad, M., & Oo, N. (2024b). Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review. In *International Journal of Critical Infrastructure Protection* (Vol. 46). Elsevier B.V. https://doi.org/10.1016/j.ijcip.2024.100700

Jiang, Y., Jeusfeld, M. A., Mosaad, M., & Oo, N. (2024c). Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review. *International Journal of Critical Infrastructure Protection*, *46*. https://doi.org/10.1016/j.ijcip.2024.100700

Jokhan, A., Chand, A. A., Singh, V., & Mamun, K. A. (2022). Increased Digital Resource Consumption in Higher Educational Institutions and the Artificial Intelligence Role in Informing Decisions Related to Student Performance. *Sustainability (Switzerland)*, *14*(4). https://doi.org/10.3390/su14042377

Jonathan, E., & Andry, J. F. (2024). Business enterprise architecture in fitness center using the open group architecture framework. *International Journal of Advances in Applied Sciences*, *13*(1), 160–167. https://doi.org/10.11591/ijaas.v13.i1.pp160-167

Jumansyah, R., Sidik, R., & Soegoto, E. S. (2022a). IT BLUEPRINT DESIGN WITH TOGAF ADM FRAMEWORK FOR INFORMATION SYSTEM DEVELOPMENT. *Journal of Engineering Science and Technology*, *17*(5), 3267–3285.

Jumansyah, R., Sidik, R., & Soegoto, E. S. (2022b). IT BLUEPRINT DESIGN WITH TOGAF ADM FRAMEWORK FOR INFORMATION SYSTEM DEVELOPMENT. *Journal of Engineering Science and Technology*, *17*(5), 3267–3285.

Kamalabai, N. E., Donoghue, I., & Hannola, L. (2024). Sustainable Enterprise Architecture: A Critical Imperative for Substantiating Artificial Intelligence. *PICMET 2024 - 2024 Portland International Conference on Management of Engineering and Technology: Technology Management in the Artificial Intelligence Era, Proceedings*. https://doi.org/10.23919/PICMET64035.2024.10653061

Karande, A., & Joshi, P. (2022a). Common quality measures for Enterprise Architecture. *Proceedings - 2022 22nd International Conference on Computational Science and Its Applications, ICCSA 2022*, 41–45. https://doi.org/10.1109/ICCSA57511.2022.00017

Karande, A., & Joshi, P. (2022b). Common quality measures for Enterprise Architecture. *Proceedings - 2022 22nd International Conference on Computational Science and Its Applications, ICCSA 2022*, 41–45. https://doi.org/10.1109/ICCSA57511.2022.00017

Kaur, A., Majid, N. L. A., Bakar, N. A. A., Hussien, S. S., & Salehuddin, H. (2024). Strategic Integration of Knowledge and Talent Management: Enhancing Academic Operations in Higher Education Through Enterprise Architecture Implementation. In *Communications in Computer and Information Science: 2152 CCIS*. https://doi.org/10.1007/978-3-031-63269-3_15

Khairina, D. M., Purwanto, P., & Nugraheni, D. M. K. (2024a). Systematic literature review on evaluation models and methods in enterprise architecture research. In *Bulletin of Electrical Engineering and Informatics* (Vol. 13, Number 4, pp. 2851–2864). Institute of Advanced Engineering and Science. https://doi.org/10.11591/eei.v13i4.6943

Khairina, D. M., Purwanto, P., & Nugraheni, D. M. K. (2024b). Systematic literature review on evaluation models and methods in enterprise architecture research. *Bulletin of Electrical Engineering and Informatics*, *13*(4), 2851–2864. https://doi.org/10.11591/eei.v13i4.6943

Kharbouch, M., Vizcaino, A., García-Berná, J. A., García, F., Toval, A., Pedreira, O., Idri, A., & Fernández-Alemán, J. L. (2025). Uncharted dimensions, gaps, and future trends of serious games in software engineering. *Computer Standards and Interfaces*, *92*. https://doi.org/10.1016/j.csi.2024.103915

Kornyshova, E., & Barrios, J. (2020). Industry 4.0 impact propagation on enterprise architecture models. *Procedia Computer Science*, *176*, 2497–2506. https://doi.org/10.1016/j.procs.2020.09.326

Kotusev, S., & Kurnia, S. (2021). The theoretical basis of enterprise architecture: A critical review and taxonomy of relevant theories.

Journal of Information Technology, *36*(3), 275–315. https://doi.org/10.1177/0268396220977873

Krauze, B., & Grabis, J. (2024a). A Conceptual Model of Digital Immune System to Increase the Resilience of Technology Ecosystems. In *Lecture Notes in Business Information Processing* (Vol. 513). https://doi.org/10.1007/978-3-031-59465-6_6

Krauze, B., & Grabis, J. (2024b). A Conceptual Model of Digital Immune System to Increase the Resilience of Technology Ecosystems. In *Lecture Notes in Business Information Processing* (Vol. 513). https://doi.org/10.1007/978-3-031-59465-6_6

Krauze, B., & Grabis, J. (2024c). A Conceptual Model of Digital Immune System to Increase the Resilience of Technology Ecosystems. In *Lecture Notes in Business Information Processing* (Vol. 513). https://doi.org/10.1007/978-3-031-59465-6_6

Kshetri, N., & Schordan, M. (2023). Can China Catch Up to the United States in Generative Artificial Intelligence? *IT Professional*, *25*(4), 94–97. https://doi.org/10.1109/MITP.2023.3297384

Kuzlu, M., Xiao, Z., Sarp, S., Catak, F. O., Gurler, N., & Guler, O. (2023). The Rise of Generative Artificial Intelligence in Healthcare. *12th Mediterranean Conference on Embedded Computing, MECO 2023*. https://doi.org/10.1109/MECO58584.2023.10155107

La Gatta, V., Moscato, V., Postiglione, M., & Sperlì, G. (2024). An eXplainable Artificial Intelligence Methodology on Big Data Architecture. *Cognitive Computation*, *16*(5), 2642–2659. https://doi.org/10.1007/s12559-024-10272-6

Le Blond, S., Cuevas, A., Troncoso-Pastoriza, J. R., Jovanovic, P., Ford, B., & Hubaux, J. P. (2018). On Enforcing the Digital Immunity of a Large Humanitarian Organization. *Proceedings - IEEE Symposium on Security and Privacy*, *2018-May*, 424–440. https://doi.org/10.1109/SP.2018.00019

Li, D., & Liang, S. (2023a). Blockchain and digital enterprise management based on embedded processing system. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-023-02166-x

Li, D., & Liang, S. (2023b). Blockchain and digital enterprise management based on embedded processing system. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-023-02166-x

Li, X., & Zhang, S. (2024). Management mode and path of digital transformation of power grid enterprises based on artificial intelligence algorithm. *International Journal of Thermofluids*, *21*. https://doi.org/10.1016/j.ijft.2023.100552

Lizby Suarez Torres, B., Cinthia Sangay Cabanillas, K., Alberto Gratelli Meléndez, F., Rodrigo Marreros Arqueros, E., & Marissa Baca Rodriguez, N. (2024). Business Architecture Model for a microenterprise in the textile sector | Modelo de Arquitectura del Negocio para una microempresa del sector textil. *Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology*. https://doi.org/10.18687/LACCEI2024.1.1.1485

Long, Y., Li, X., Wei, W., & Long, N. (2022). Data Governance Architecture of Digital Grid Based on Blockchain Technology and Nanomaterial

Technology. *Integrated Ferroelectrics*, *228*(1), 35–50. https://doi.org/10.1080/10584587.2022.2072120

Louis Cohen, L. M. K. M. (2002). *Research Methods in Education*.

Madyatmadja, E. D., Liliana, L., Chakir, A., & Andry, J. F. (2021). Implementation of the Zachman framework using capsicum model for electrical equipment trading industry. *ICIC Express Letters, Part B: Applications*, *12*(3), 207–213. https://doi.org/10.24507/icicelb.12.03.207

Martel, Y., Roßmann, A., Sultanow, E., Weiß, O., Wissel, M., Pelzel, F., & Seßler, M. (2020). Software Architecture Best Practices for Enterprise Artificial Intelligence. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *P-307*, 165–181. https://doi.org/10.18420/inf2020_16

Masadeh, S. A., & El-Haggar, N. (2023). Analyzing factors influencing IoT adoption in higher educational institutions in Saudi Arabia using a modified TAM model. *Education and Information Technologies*. https://doi.org/10.1007/s10639-023-12039-2

Mazher, N., Asharaf, Z., Ganne, M. A., & Avinash Ganne, M. (2023). *Artificial Intelligence Based Architecture to Enhance Cloud Computing Security*. https://doi.org/10.22541/au.167451372.26119798/v1

Meepung, T., Nilsook, P., & Wannapiroon, P. (2021). Conceptual Framework for High Performance Digital Entrepreneurial University. *ACM International Conference Proceeding Series*, 47–53. https://doi.org/10.1145/3485768.3485769

Meepung, T., Wannapiroon, P., & Nilsook, P. (2021). Transition Elements, Enterprise Architecture for Digital Entrepreneurial University.

Proceedings - 2021 Research, Invention, and Innovation Congress: Innovation Electricals and Electronics, RI2C 2021, 167–175. https://doi.org/10.1109/RI2C51727.2021.9559833

Meng, D., Hou, R., Shi, G., Tu, B., Yu, A., Zhu, Z., Jia, X., & Liu, P. (2018). Security-first architecture: deploying physically isolated active security processors for safeguarding the future of computing. *Cybersecurity*, *1*(1). https://doi.org/10.1186/s42400-018-0001-z

Miethlich, B., Belotserkovich, D., Abasova, S., Zatsarinnaya, E., & Veselitsky, O. (2021). The Impact of COVID-19 on Digital Enterprise Management. *IEEE Engineering Management Review*, *49*(4), 16–29. https://doi.org/10.1109/EMR.2021.3119222

Miethlich, B., Belotserkovich, D., Abasova, S., Zatsarinnaya, E., & Veselitsky, O. (2022a). Transformation of Digital Management in Enterprises Amidst the COVID-19 Pandemic. *Institutions and Economies*, *14*(1), 1–26. https://doi.org/10.22452/IJIE.vol14no1.1

Miethlich, B., Belotserkovich, D., Abasova, S., Zatsarinnaya, E., & Veselitsky, O. (2022b). Transformation of Digital Management in Enterprises Amidst the COVID-19 Pandemic. *Institutions and Economies*, *14*(1), 1–26. https://doi.org/10.22452/IJIE.vol14no1.1

Mkhwanazi, K., & Beharry-Ramraj, A. (2023). Emerging Trends during the COVID-19 Pandemic: Digital Transformation and Social Inclusion. *African Renaissance*, *2023*, 95–116. https://doi.org/10.31920/2516-5305/2023/sin1a5

Monlezun, D. J. (2024). Responsible Artificial Intelligence Re-engineering the Global Public Health Ecosystem: A Humanity Worth Saving. In *Responsible Artificial Intelligence Re-engineering the Global Public*

Health Ecosystem: A Humanity Worth Saving. https://doi.org/10.1016/C2022-0-03368-7

Mukherjee, P. K. (2022). Artificial Intelligence Based Smart Government Enterprise Architecture (AI-SGEA) Framework. In *Communications in Computer and Information Science: 1695 CCIS*. https://doi.org/10.1007/978-3-031-22485-0_30

Muslih, M., Maulana, M. R., & Arianti, N. D. (2024a). Development of a Web-Based Job and Career Compatibility System Using the Federal Enterprise Architecture Framework Method: A Case Study in Nusa Putra University. *Ingenierie Des Systemes d'Information*, *29*(3), 895–908. https://doi.org/10.18280/isi.290310

Muslih, M., Maulana, M. R., & Arianti, N. D. (2024b). Development of a Web-Based Job and Career Compatibility System Using the Federal Enterprise Architecture Framework Method: A Case Study in Nusa Putra University. *Ingenierie Des Systemes d'Information*, *29*(3), 895–908. https://doi.org/10.18280/isi.290310

Muslih, M., Maulana, M. R., & Arianti, N. D. (2024c). Development of a Web-Based Job and Career Compatibility System Using the Federal Enterprise Architecture Framework Method: A Case Study in Nusa Putra University. *Ingenierie Des Systemes d'Information*, *29*(3), 895–908. https://doi.org/10.18280/isi.290310

Muslih, M., Maulana, M. R., & Arianti, N. D. (2024d). Development of a Web-Based Job and Career Compatibility System Using the Federal Enterprise Architecture Framework Method: A Case Study in Nusa Putra University. *Ingenierie Des Systemes d'Information*, *29*(3), 895–908. https://doi.org/10.18280/isi.290310

Mustafa, M. F., Isa, M. R. M., Rauf, U. F. A., Ismail, M. N., Shukran, M. A. M., Khairuddin, M. A., Wahab, N., & Safar, N. Z. M. (2021). Student Perception Study On Smart Campus: A Case Study On Higher Education Institution. *Malaysian Journal of Computer Science*, *2021*(Special Is), 1–20. https://doi.org/10.22452/mjcs.sp2021no1.1

Myauo, M. (2020). Corporate Cybersecurity Strategy to Enable Artificial Intelligence and Internet of Things. In *Artificial Intelligence to Solve Pervasive Internet of Things Issues*. https://doi.org/10.1016/B978-0-12-818576-6.00015-0

Nagwani, N. K., & Suri, J. S. (2023). An artificial intelligence framework on software bug triaging, technological evolution, and future challenges: A review. In *International Journal of Information Management Data Insights* (Vol. 3, Number 1). Elsevier B.V. https://doi.org/10.1016/j.jjimei.2022.100153

Nakakawa, A., de Manuel Keenoy, E., Zabala, A. F., Berastegui, D. V., & Suarez, J. T. (2024). Mutual Adoption of Soft Systems Methodology, Co-Creation, Enterprise Architecture, and Balanced Scorecard for Continuous Assessment and Improvement of Programmes on Integrated Care for Multimorbid Patients. *Systemic Practice and Action Research*, *37*(4), 351–386. https://doi.org/10.1007/s11213-023-09648-w

Noranita, B., Nugraheni, D. M. K., Fitriyani, M. I., & Nurhayati, Y. (2021a). Business architecture and information system architecture design in savings and payment unit Koperasi Pegawai Republik Indonesia (KPRI) Diponegoro University using TOGAF 9 framework. *Journal of Physics: Conference Series*, *1943*(1). https://doi.org/10.1088/1742-6596/1943/1/012105

Noranita, B., Nugraheni, D. M. K., Fitriyani, M. I., & Nurhayati, Y. (2021b). Business architecture and information system architecture design in savings and payment unit Koperasi Pegawai Republik Indonesia (KPRI) Diponegoro University using TOGAF 9 framework. *Journal of Physics: Conference Series*, *1943*(1). https://doi.org/10.1088/1742-6596/1943/1/012105

Ortiz-Garcés, I., Govea, J., Sánchez-Viteri, S., & Villegas-Ch., W. (2024a). CyberEduPlatform: an educational tool to improve cybersecurity through anomaly detection with Artificial Intelligence. *PeerJ Computer Science*, *10*. https://doi.org/10.7717/PEERJ-CS.2041

Ortiz-Garcés, I., Govea, J., Sánchez-Viteri, S., & Villegas-Ch., W. (2024b). CyberEduPlatform: an educational tool to improve cybersecurity through anomaly detection with Artificial Intelligence. *PeerJ Computer Science*, *10*. https://doi.org/10.7717/PEERJ-CS.2041

Ortiz-Garcés, I., Govea, J., Sánchez-Viteri, S., & Villegas-Ch., W. (2024c). CyberEduPlatform: an educational tool to improve cybersecurity through anomaly detection with Artificial Intelligence. *PeerJ Computer Science*, *10*. https://doi.org/10.7717/PEERJ-CS.2041

Ovalle, C., Lezcano, G. C., & Luna, R. F. (2024). Design of an Enterprise Architecture Model Applying TOGAF in the Sales Management of Fast Food SMEs. *International Journal of Engineering Trends and Technology*, *72*(3), 331–348. https://doi.org/10.14445/22315381/IJETT-V72I3P129

Pan, Y., & Zhang, L. (2021). Roles of artificial intelligence in construction engineering and management: A critical review and future trends. In *Automation in Construction* (Vol. 122). Elsevier B.V. https://doi.org/10.1016/j.autcon.2020.103517

Pańkowska, M. (2023). Business Information System Analysis Techniques Acceptance. In *Lecture Notes in Networks and Systems* (Vol. 578). https://doi.org/10.1007/978-981-19-7660-5_30

Pastor-Galindo, J., Sandlin, H.-Â., Mármol, F. G., Bovet, G., & Pérez, G. M. (2024). A Big Data architecture for early identification and categorization of dark web sites. *Future Generation Computer Systems*, *157*, 67–81. https://doi.org/10.1016/j.future.2024.03.025

Pexyean, T., Saraubon, K., & Nilsook, P. (2022). IoT, AI and Digital Twin For Smart Campus. *Proceedings - 2022 Research, Invention, and Innovation Congress: Innovative Electricals and Electronics, RI2C 2022*, 160–164. https://doi.org/10.1109/RI2C56397.2022.9910286

Pikulhom, P. (2025). *Digital Immunity Framework for Higher Education Institution*.

Polovina, S., von Rosing, M., & Etzel, G. (2020). Leading the practice in layered enterprise architecture. *CEUR Workshop Proceedings*, *2574*, 62–69.

Prasetyo, Y. A., & Habibie, I. (2022). Smart City Architecture Development Framework (SCADEF). *International Journal on Informatics Visualization*, *6*(4), 869–875. https://doi.org/10.30630/joiv.6.4.1537

Puntillo, G., Salazar, A., & Wong, L. (2022). Enterprise Architecture Based on TOGAF for the Adaptation of Educational Institutions to e-Learning Using the DLPCA Methodology and Google Classroom. In *Communications in Computer and Information Science: 1577 CCIS*. https://doi.org/10.1007/978-3-031-04447-2_11

Qasem, Y. A. M., Abdullah, R., Yaha, Y., & Atana, R. (2020). Continuance use of cloud computing in higher education institutions: A conceptual

model. *Applied Sciences (Switzerland)*, *10*(19). https://doi.org/10.3390/APP10196628

Qurtubi, A. (2024). Architecture Enterprise Model of Islamic College Management in Indonesian Industrial Era 5.0. *Philippine Journal of Science*, *153*(3), 1097–1105.

Rachmaniah, M., Suroso, A. I., Syukur, M., & Hermadi, I. (2022). Enterprise Architecture for Smart Enterprise System A Quest for Chili Agrosystem. *International Journal of Advanced Computer Science and Applications*, *13*(4), 341–350. https://doi.org/10.14569/IJACSA.2022.0130440

Ramasamy, L. K., Khan, F., Shah, M., Prasad, B. V. V. S., Iwendi, C., & Biamba, C. (2022). Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring. *Sensors*, *22*(3). https://doi.org/10.3390/s22031076

Rashid, A. B., & Kausik, M. A. K. (2024). AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications. *Hybrid Advances*, *7*. https://doi.org/10.1016/j.hybadv.2024.100277

Rave-Gómez, E. D., Pérez Castañeda, S. S., Montoya Agudelo, C. A., & Arias Vargas, F. J. (2024). Enterprise architecture in Colombian and Mexican restaurants during the covid-19 pandemic. Multiple intertwined cases | Arquitectura empresarial en restaurantes colombianos y mexicanos durante la pandemia covid-19. Casos múltiples entrelazados. *Revista Venezolana de Gerencia*, *29*(11 Special), 327–341. https://doi.org/10.52080/rvgluz.29.e11.19

Ravi, P., Najm, Z., Bhasin, S., Khairallah, M., Gupta, S. Sen, & Chattopadhyay, A. (2019). *Security is an Architectural Design Constraint*.

Rittelmeyer, J. D., & Sandkuhl, K. (2021). Effects of Artificial Intelligence on Enterprise Architectures - A Structured Literature Review. *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW*, 130–137. https://doi.org/10.1109/EDOCW52865.2021.00042

Rizal, R., Selamat, S. R., Mas'ud, M. Z., & Widiyasono, N. (2025). Enhanced Readiness Forensic Framework for the Complexity of Internet of Things (IoT) Investigation Based on Artificial Intelligence. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *50*(1), 121–135. https://doi.org/10.37934/araset.50.1.121135

Roslan, N., Jamil, J. M., Shaharanee, I. N. M., & Alawi, S. J. S. (2025a). Prediction of Student Dropout in Malaysian's Private Higher Education Institute using Data Mining Application. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *45*(2), 168–176. https://doi.org/10.37934/araset.45.2.168176

Roslan, N., Jamil, J. M., Shaharanee, I. N. M., & Alawi, S. J. S. (2025b). Prediction of Student Dropout in Malaysian's Private Higher Education Institute using Data Mining Application. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *45*(2), 168–176. https://doi.org/10.37934/araset.45.2.168176

Rujira, T., Nilsook, P., & Wannapiroon, P. (2020). Synthesis of vocational education college transformation process toward high-

performance digital organization. *International Journal of Information and Education Technology*, *10*(11), 832–837. https://doi.org/10.18178/ijiet.2020.10.11.1466

Rujira, T., Nilsook, P., & Wannapiroon, P. (2021). Vocational Education Digital Enterprise Architecture Framework (VEDEAF). *2021 9th International Conference on Information and Education Technology, ICIET 2021*, 63–67. https://doi.org/10.1109/ICIET51873.2021.9419576*s12885-024-12152-6*. (n.d.).

Safiah, M. H., Alchallah, M. O., ElHomsi, M. O., Kalalib Al Ashabi, K., Ataya, S., Alolabi, H., Mohsen, F., & Darjazini Nahas, L. (2024). The attitudes of Syrian Private University Medical Students towards E-Learning during the COVID-19 pandemic: a cross-sectional study. *BMC Medical Education*, *24*(1). https://doi.org/10.1186/s12909-024-05817-0

Said, D., Youssef, D., El-Bayaa, N., Alzoubi, Y. I., & Zaim, H. (2023). THE IMPACT OF DIVERSITY ON JOB PERFORMANCE: EVIDENCE FROM PRIVATE UNIVERSITIES IN EGYPT. *Acta Innovations*, *2023*(49), 17–30. https://doi.org/10.32933/ActaInnovations.49.2

Saini, H., Singh, G., Dalal, S., Lilhore, U. K., Simaiya, S., & Dalal, S. (2024). Enhancing cloud network security with a trust-based service mechanism using k-anonymity and statistical machine learning approach. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-024-01759-y

Saleh Alrubayyi, H. (2023a). *Artificial Immune Systems for Detecting Unknown Malware in the IoT*.

Saleh Alrubayyi, H. (2023b). *Artificial Immune Systems for Detecting Unknown Malware in the IoT*.

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00957-y

Saoud, A., & Bellabdaoui, A. (2023). Towards generic platform to support collaboration in freight transportation: taxonomic literature and design based on Zachman framework. *Enterprise Information Systems*, *17*(2). https://doi.org/10.1080/17517575.2021.1939894

Sararuch, S., Wannapiroon, P., & Nilsook, P. (2023a). The Development of Agile Enterprise Architecture for Digital Transformation in Higher Education Institutions. *Higher Education Studies*, *13*(3), 69. https://doi.org/10.5539/hes.v13n3p69

Sararuch, S., Wannapiroon, P., & Nilsook, P. (2023b). The Development of Agile Enterprise Architecture for Digital Transformation in Higher Education Institutions. *Higher Education Studies*, *13*(3), 69. https://doi.org/10.5539/hes.v13n3p69

Schoonderbeek, J. A. H., & Proper, H. A. (2024). Toward an ontology for EA modeling and EA model quality. *Software and Systems Modeling*, *23*(3), 535–558. https://doi.org/10.1007/s10270-023-01146-w

Sharma, S., & Sarkar, P. (2023). Biological knowledge capture and representation inspired by Zachman Framework principles. *International Journal on Interactive Design and Manufacturing*. https://doi.org/10.1007/s12008-023-01259-y

Shishakly, R., Almaiah, M. A., Lutfi, A., & Alrawad, M. (2024). The influence of using smart technologies for sustainable development in higher education institutions. *International Journal of Data and Network Science*, *8*(1), 77–90. https://doi.org/10.5267/j.ijdns.2023.10.015

Shuhan, W., Chengzhi, Y., Xiaoxiao, L., & Siyu, W. (2024). Smart infrastructure design: Machine learning solutions for securing modern cities. *Sustainable Cities and Society*, *107*. https://doi.org/10.1016/j.scs.2024.105439

Shvartsman, A. A. (1993). Historical object base in an enterprise management director. In *IFIP Transactions C: Communication Systems* (Numbers C–12).

Sidorenko, D., Pushkov, S., Sakip, A., Leung, G. H. D., Lok, S. W. Y., Urban, A., Zagirova, D., Veviorskiy, A., Tihonova, N., Kalashnikov, A., Ren, F., & Zhavoronkov, A. (2024). Precious2GPT: the combination of multiomics pretrained transformer and conditional diffusion for artificial multi-omics multi-species multi-tissue sample generation. *Npj Aging*, *10*(1). https://doi.org/10.1038/s41514-024-00163-3

Sneesl, R., Jusoh, Y. Y., Jabar, M. A., & Abdullah, S. (2022). Conceptualizing IoT-based Smart Campus Adoption Model for Higher Education Institutions: A Systematic Literature Review. *Proceedings - AiIC 2022: 2022 Applied Informatics International Conference: Digital Innovation in Applied Informatics during the Pandemic*, 7–12. https://doi.org/10.1109/AiIC54368.2022.9914033

Splunk. (2023). *Digital Resilience Pays Off*.

Srisawat, S., Wannapiroon, P., & Nilsook, P. (2023). A Conceptual Framework of a High-performance Digital Education Organization. *4th*

Research, Invention, and Innovation Congress: Innovative Electricals and Electronics: Innovation for Better Life, RI2C 2023, 40–45. https://doi.org/10.1109/RI2C60382.2023.10355985

Srisawat, S., Wannapiroon, P., & Nilsook, P. (2024). Distributed Digital Enterprise Architecture for Transformation of Educational Organizations. *TEM Journal*, *13*(2), 1645–1657. https://doi.org/10.18421/TEM132-77

Sudarsono, B. G., Abd Rahman, A. B., Lestari, S. P., & Bani, A. U. (2020). Systematic review of the builder method and product of the information system strategic planning at higher education institutions in indonesia. *Journal of Advanced Research in Dynamical and Control Systems*, *12*(6), 939–947. https://doi.org/10.5373/JARDCS/V12I6/S20201113

Sultanow, E., Brockmann, C., & Czarnecki, C. (2021). Enterprise architecture management in the age of agility and artificial intelligence | Unternehmensarchitekturmanagement im Zeitalter von Agilität und Künstlicher Intelligenz. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *P-314*, 1263.

Sutton, S. M. (2024). Capability Modeling for Corporate Cognition. *ACM International Conference Proceeding Series*, 24–35. https://doi.org/10.1145/3666015.3666023

Takeuchi, H., Husen, J. H., Tun, H. T., Washizaki, H., & Yoshioka, N. (2024a). Enterprise architecture-based metamodel for machine learning projects and its management. *Future Generation Computer Systems*, *161*, 135–145. https://doi.org/10.1016/j.future.2024.06.062

Takeuchi, H., Husen, J. H., Tun, H. T., Washizaki, H., & Yoshioka, N. (2024b). Enterprise architecture-based metamodel for machine learning projects and its management. *Future Generation Computer Systems*, *161*, 135–145. https://doi.org/10.1016/j.future.2024.06.062

Takeuchi, H., Husen, J. H., Tun, H. T., Washizaki, H., & Yoshioka, N. (2024c). Enterprise architecture-based metamodel for machine learning projects and its management. *Future Generation Computer Systems*, *161*, 135–145. https://doi.org/10.1016/j.future.2024.06.062

Teodoro Ramírez Guija, O., Andree Sanchez Rodriguez, S., Fernanda Oliva Marquez, L., Alberto Luzquiños Cruces, C., & Leonor Guevara Izquierdo, A. (2024). Business architecture model based on the TOGAF method for the travel and tourism agency "Viajes Reales SAC" | Modelo de arquitectura empresarial basado en el método TOGAF para la agencia de viajes y turismo "Viajes Reales SAC." *Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology.* https://doi.org/10.18687/LACCEI2024.1.1.576

Termanini, R. (2020). The miraculous anatomy of the digital immunity ecosystem. In *Storing Digital Binary Data in Cellular DNA* (pp. 39–77). Elsevier. https://doi.org/10.1016/b978-0-12-823295-8.00003-3

Terziyan, V., Gryshko, S., & Golovianko, M. (2021). Taxonomy of generative adversarial networks for digital immunity of Industry 4.0 systems. *Procedia Computer Science*, *180*, 676–685. https://doi.org/10.1016/j.procs.2021.01.290

Terziyan, V., & Kaikova, O. (2025). Guardians of Reliability, Robustness, and Resilience: Adversarial Maintenance in the Era of Industry 4.0 and

5.0. *Procedia Computer Science*, *253*, 13–24. https://doi.org/10.1016/j.procs.2025.01.065

Thangam, S., & Jana, S. (2025). Interval-Valued Neutrosophic Set with Optimization Algorithm for Cyberthreat Detection and Classification in IoT Infrastructure. *International Journal of Neutrosophic Science*, *25*(2), 268–278. https://doi.org/10.54216/IJNS.250223

Thongprasit, J., & Wannapiroon, P. (2022). Framework of Artificial Intelligence Learning Platform for Education. *International Education Studies*, *15*(1), 76. https://doi.org/10.5539/ies.v15n1p76

TomassMHultt, G. (2021). *Classroom Companion: Business Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R AAWorkbook*. http://www.

Tooki, O. O., & Popoola, O. M. (2024). A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems. In *Renewable Energy Focus* (Vol. 51). Elsevier Ltd. https://doi.org/10.1016/j.ref.2024.100628

Trad, A. (2021). The business, societal, and enterprise architecture framework: An artificial intelligence-, data sciences-, and big data-based approach. In *Handbook of Research on Applied Data Science and Artificial Intelligence in Business and Industry*. https://doi.org/10.4018/978-1-7998-6985-6.ch022

Trad, A. (2022). Business transformation and enterprise architecture projects: Machine learning integration for projects (MLI4P). In

Unmanned Aerial Vehicles and Multidisciplinary Applications Using AI Techniques. https://doi.org/10.4018/978-1-7998-8763-8.ch009

Trad, A. T. (2024). Enterprise transformation projects: The Polymathic Enterprise Architecture-Based Generic Learning Processes (PEAbGLP). In *Machine Learning and Data Science Techniques for Effective Government Service Delivery*. https://doi.org/10.4018/978-1-6684-9716-6.ch002

Tshuma, G., Kritzinger, E., & Singh, S. (2024). A Framework for Promoting Digital Transformation and the Adoption of Enterprise Architecture in South Africa's Public Sector. In *IFIP Advances in Information and Communication Technology* (Vol. 709). https://doi.org/10.1007/978-3-031-66986-6_2

Tungpantong, C., Nilsook, P., & Wannapiroon, P. (2022). Confirmatory Factor Analysis of Enterprise Architecture for Higher Education Institutions. *2022 International Conference on Decision Aid Sciences and Applications, DASA 2022*, 965–969. https://doi.org/10.1109/DASA54658.2022.9764970

Ukolov, V. F., & Afanasyev, V. Y. (2020a). Supply chain management for digital enterprise, psychological aspect of adaptation. *International Journal of Supply Chain Management*, *9*(1), 670–675.

Ukolov, V. F., & Afanasyev, V. Y. (2020b). Supply chain management for digital enterprise, psychological aspect of adaptation. *International Journal of Supply Chain Management*, *9*(1), 670–675.

Uruntie, R. O., Oputa, C. H., Peters, E., & Otovwe, A. (2024). Correction: Effect of educational intervention on the knowledge, attitude and practice of breast self-examination among female students at a

private university in Southern Nigeria (BMC Cancer, (2024), 24, 1, (355), 10.1186/s12885-024-12116-w). *BMC Cancer*, *24*(1). https://doi.org/10.1186/s12885-024-12152-6

Uzhakova, N., & Fischer, S. (2024a). Data-Driven Enterprise Architecture for Pharmaceutical R&D. *Digital*, *4*(2), 333–371. https://doi.org/10.3390/digital4020017

Uzhakova, N., & Fischer, S. (2024b). Data-Driven Enterprise Architecture for Pharmaceutical R&D. *Digital*, *4*(2), 333–371. https://doi.org/10.3390/digital4020017

Vial, G., Cameron, A. F., Giannelia, T., & Jiang, J. (2023). Managing artificial intelligence projects: Key insights from an AI consulting firm. *Information Systems Journal*, *33*(3), 669–691. https://doi.org/10.1111/isj.12420

Vokony, I., Szekeres, M. B., & Nemeth, V. G. (2020). Agile application landscape planning in energy sector – architectural experiences. *Renewable Energy and Power Quality Journal*, *18*, 626–630. https://doi.org/10.24084/repqj18.450

Wang, X., Shu, L., Hong, X., & Fang, H. (2024). A Research on Multimodal Interaction Data Architecture and Application Scenarios of Intelligent Educational Robots Based on the Theory of Multiple Intelligences. *ACM International Conference Proceeding Series*, 16–22. https://doi.org/10.1145/3675812.3675842

Wang, Y., & Lee, E. L. W. (2023a). Realizing Excellence in Enterprise Management through Digital Innovation. *Journal of Logistics, Informatics and Service Science*, *10*(2), 197–211. https://doi.org/10.33168/JLISS.2023.0214

Wang, Y., & Lee, E. L. W. (2023b). Realizing Excellence in Enterprise Management through Digital Innovation. *Journal of Logistics, Informatics and Service Science*, *10*(2), 197–211. https://doi.org/10.33168/JLISS.2023.0214

Watcharinrat, D., Butdisuwan, S., Boonyarutkalin, T., Phasinam, K., Watcharinrat, C., Saengngam, N., Supamattra, S., & Boonsong, S. (2024). The 21st century skills of the master's degree students in the school of liberal arts in private Universities. *Multidisciplinary Science Journal*, *6*(11). https://doi.org/10.31893/multiscience.2024249

Wood-Harper, T. (2020). Emerging EdTechs amidst the COVID-19 pandemic: Cases in higher education institutions. In *Fostering Communication and Learning With Underutilized Technologies in Higher Education*. https://doi.org/10.4018/978-1-7998-4846-2.ch007

Xiao, S., Shanthini, A., & Thilak, D. (2022). Instructor Performance Prediction Model Using Artificial Intelligence for Higher Education Systems. *Journal of Interconnection Networks*, *22*. https://doi.org/10.1142/S0219265921440035

Xie, Y., & Zhang, M. (2024). Synergy of higher education resources and digital infrastructure construction in China: Regional differences, dynamic evolution and trend forecasting. *PLoS ONE*, *19*(6 June). https://doi.org/10.1371/journal.pone.0304613

Yang, T., & Zheng, B. (2023a). A Deep Learning-Based Multimodal Resource Reconstruction Scheme for Digital Enterprise Management. *Journal of Circuits, Systems and Computers*, *32*(11). https://doi.org/10.1142/S0218126623501876

Yin, X. (2024a). Research on the Innovative Application of Particle Swarm Algorithm in the Improvement of Management Efficiency of Digital Enterprises. *Applied Mathematics and Nonlinear Sciences*, *9*(1). https://doi.org/10.2478/amns.2023.2.01368

Zhang, C., Xu, Q., Yu, Y., Zhou, G., Zeng, K., Chang, F., & Ding, K. (2025). A survey on potentials, pathways and challenges of large language models in new-generation intelligent manufacturing. *Robotics and Computer-Integrated Manufacturing*, *92*. https://doi.org/10.1016/j.rcim.2024.102883

Zimmermann, A., Schmidt, R., Alt, R., Masuda, Y., & Chehri, A. (2023). Digital Strategy and Architecture for Human-Centered Intelligent Systems. In *Smart Innovation, Systems and Technologies: 359 SIST*. https://doi.org/10.1007/978-981-99-3424-9_4

Zulfikar, F., Selo, & Winarno, W. W. (2023). Evaluating the Influence of EA Capabilities on Digital Transformation in the Ministry of Finance of Indonesia. *E3S Web of Conferences*, *448*. https://doi.org/10.1051/e3sconf/202344802039

ภาคผนวก



ภาคผนวก ก

รายชื่อผู้เชี่ยวชาญ ผู้ทรงคุณวุฒิและหนังสือขอความอนุเคราะห์

รายชื่อผู้เชี่ยวชาญและผู้ทรงคุณวุฒิประเมินเครื่องมือเพื่อการวิจัย
สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตารางที่ ก-1 รายชื่อผู้เชี่ยวชาญประเมินความเหมาะสมแบบสอบถามปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ลำดับที่	ชื่อ-นามสกุล
1	รองศาสตราจารย์ ดร.วิเชียร ชุติมาสกุล อาจารย์ประจำคณะเทคโนโลยีสารสนเทศ/ที่ปรึกษาฝ่ายประกันคุณภาพ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
2	ผู้ช่วยศาสตราจารย์ ดร.กัญณัฏฐ์ หอมทรัพย์ อาจารย์ประจำคณะวิทยาศาสตร์ ศรีราชา มหาวิทยาลัยเกษตรศาสตร์
3	ดร.สุรศักดิ์ ศรีสวัสดิ์ ผู้อำนวยการกลุ่มพัฒนาและส่งเสริมการวัดและประเมินผลการเรียนรู้ สำนักวิชาการและมาตรฐานการศึกษา สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
4	ผู้ช่วยศาสตราจารย์ ดร.ทิพวรรณ มีพึ่ง อาจารย์ผู้รับผิดชอบหลักสูตรบริหารธุรกิจบัณฑิต คณะบริหารธุกิจและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก วิทยาเขตจักรพงษภูวนารถ
5	ดร.กิติยา พรหมสอน ศึกษานิเทศก์ชำนาญการพิเศษ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาปทุมธานี
6	ผศ.ดร.นพดล ผู้มีจรรยา อาจารย์ประจำสาขาวิชาคอมพิวเตอร์ศึกษา มหาวิทยาลัยราชภัฏนครปฐม
7	รศ.ดร.ปริญญา สงวนสัตย์ หัวหน้าสาขาวิชาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์ คณะวิศวกรรมศาสตร์และเทคโนโลยี สถาบันการจัดการปัญญาภิวัฒน์
8	ผศ.ดร.อรพรรณ อำนวยศิลป์ อาจารย์ประจำหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชานวัตกรรมคอมพิวเตอร์และอุตสาหกรรมดิจิทัล คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏนครศรีธรรมราช
9	ดร.จารุวรรณ กาฬภักดี

ลำดับที่	ชื่อ-นามสกุล
	รักษาการแทนผู้ช่วยผู้อำนวยการฝ่ายวิชาการ สถาบันวิจัยพัฒนาและสาธิตการศึกษา มหาวิทยาลัยศรีนครินทรวิโรฒ
10	ดร.บุรินทร์ นรินทร์ รองอธิการบดี มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
11	ผศ.ดร.ศศิธร อิสโร สาขาวิชานวัตกรรมคอมพอและอุตสาหกรรมดิจิทัล คณะเทคโนโลยีอุตสาหกรรม มหาลัยราชภัฏนครศรีธรรมราช

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ตารางที่ ก-2 รายชื่อผู้ทรงคุณวุฒิประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ลำดับที่	ชื่อ-นามสกุล
1	รองศาสตราจารย์ ดร.วิเชียร ชุติมาสกุล อาจารย์ประจำคณะเทคโนโลยีสารสนเทศ/ที่ปรึกษาฝ่ายประกันคุณภาพ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
2	ผู้ช่วยศาสตราจารย์ ดร.กัญณัฏฐ์ หอมทรัพย์ อาจารย์ประจำคณะวิทยาศาสตร์ ศรีราชา มหาวิทยาลัยเกษตรศาสตร์
3	ดร.สุรศักดิ์ ศรีสวัสดิ์ ผู้อำนวยการกลุ่มพัฒนาและส่งเสริมการวัดและประเมินผลการเรียนรู้ สำนักวิชาการและมาตรฐานการศึกษา สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
4	ผู้ช่วยศาสตราจารย์ ดร.ทิพวรรณ มีพึ่ง อาจารย์ผู้รับผิดชอบหลักสูตรบริหารธุรกิจบัณฑิต คณะบริหารธุกิจและเทคโนโลยีสารสนเทศ มหาวิททยาลัยเทคโนโลยีราชมงคลตะวันออก วิทยาเขตจักรพงษภูวนารถ
5	ดร.กิติยา พรหมสอน ศึกษานิเทศก์ชำนาญการพิเศษ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาปทุมธานี
6	ผศ.ดร.นพดล ผู้มีจรรยา อาจารย์ประจำสาขาวิชาคอมพิวเตอร์ศึกษา มหาวิทยาลัยราชภัฏนครปฐม
7	รศ.ดร.ปริญญา สงวนสัตย์ หัวหน้าสาขาวิชาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์ คณะวิศวกรรมศาสตร์และเทคโนโลยี สถาบันการจัดการปัญญาภิวัฒน์
8	ดร.บุรินทร์ นรินทร์ รองอธิการบดี มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
9	ผศ.ดร.ศศิธร อิสโร สาขาวิชานวัตกรรมคอมพอและอุตสาหกรรมดิจิทัล คณะเทคโนโลยีอุตสาหกรรม มหาลัยราชภัฏนครศรีธรรมราช



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย

เรียน รองศาสตราจารย์ ดร.วิเชียร ชุติมาสกุล อาจารย์ประจำคณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ผู้ช่วยศาสตราจารย์ ดร.กัญณัฏฐ์ หอมทรัพย์ อาจารย์ประจำคณะวิทยาศาสตร์
มหาวิทยาลัยเกษตรศาสตร์ (ศรีราชา)

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ดร.สุรศักดิ์ ศรีสวัสดิ์ ผู้อำนวยการกลุ่มพัฒนาและส่งเสริมการวัดและประเมินผลการเรียนรู้
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ (ศาลายา)

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ผู้ช่วยศาสตราจารย์ ดร.ทิพวรรณ มีพึ่ง อาจารย์ผู้รับผิดชอบหลักสูตรบริหารธุรกิจบัณฑิต
คณะบริหารธุรกิจและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก
วิทยาเขตจักรพงษภูวนารถ

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ดร.กิติยา พรหมสอน ศึกษานิเทศก์ชำนาญการพิเศษ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษา ปทุมธานี

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ผู้ช่วยศาสตราจารย์ ดร.นพดล ผู้มีจรรยา อาจารย์ประจำสาขาวิชาคอมพิวเตอร์ศึกษา
มหาลัยราชภัฏนครปฐม

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าวเพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน รองศาสตราจารย์ ดร.ปริญญา สงวนสัตย์ หัวหน้าสาขาวิชาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์
คณะวิศวกรรมศาสตร์และเทคโนโลยี สถาบันการจัดการปัญญาภิวัฒน์

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ผู้ช่วยศาสตราจารย์ ดร.อรพรรณ อำนวยศิลป์ อาจารย์ประจำสาขาวิชานวัตกรรมคอมพิวเตอร์และอุตสาหกรรมดิจิทัล คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏนครศรีธรรมราช

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ดร.จารุวรรณ กาฬภักดี รักษาการแทนผู้ช่วยผู้อำนวยการฝ่ายวิชาการ
สถาบันวิจัยพัฒนาและสาธิตการศึกษา มหาวิยาลัยศรีนครินทรวิโรฒ

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ดร.บุรินทร์ นรินทร์ รองอธิการบดี มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าว เพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔



ที่ อว ๗๑๐๔.๕/๑๙

คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพมหานคร ๑๐๘๐๐

๒๗ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอเชิญเป็นผู้เชี่ยวชาญในการประเมินเครื่องมือการวิจัย

เรียน ผู้ช่วยศาสตราจารย์ ดร.ศศิธร อิสโร อาจารย์ประจำสาขาวิชานวัตกรรมคอมพิวเตอร์และอุตสาหกรรมดิจิทัล คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏนครศรีธรรมราช

สิ่งที่ส่งมาด้วย แบบประเมินสำหรับผู้เชี่ยวชาญ

ด้วย นางสาวเนาวรัตน์ ปิ่นอำนาจ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ คณะครุศาสตร์อุตสาหกรรม ได้รับอนุมัติให้ทำวิทยานิพนธ์ เรื่อง “สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา” โดยมีคณะกรรมการที่ปรึกษาวิทยานิพนธ์ คือ ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์เชิญท่าน เป็นผู้เชี่ยวชาญในการประเมินเครื่องมือเพื่อการวิจัย โดยนักศึกษาขอติดต่อประสานงานในรายละเอียดโดยตรงด้วยตนเอง ทั้งนี้จะนำข้อมูลที่ได้มาพัฒนาให้ได้เครื่องมือเพื่อการวิจัยที่เหมาะสม สำหรับประกอบการทำวิทยานิพนธ์เรื่องดังกล่าวเพื่อประโยชน์สูงสุดทางการศึกษาต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ)
หัวหน้าภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ

ภาควิชาครุศาสตร์เทคโนโลยีและสารสนเทศ
โทรศัพท์ / โทรสาร ๐๒-๕๘๗-๘๒๕๙
นักศึกษา โทรศัพท์ ๐๘๑-๘๘๖๘๔๗๔

ภาคผนวก ข

เครื่องมือที่ใช้ในการวิจัย



แบบประเมินความเที่ยงตรงของแบบสอบถามปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ชื่องานวิจัย สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

อาจารย์ที่ปรึกษา ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข
ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ

ผู้วิจัย นางสาวเนาวรัตน์ ปิ่นอำนาจ
นักศึกษาปริญญาเอก สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินฉบับนี้ จัดทำขึ้นเพื่อประเมินความเที่ยงตรงของแบบสอบถามปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผู้วิจัยจึงใคร่ขอความกรุณาจากท่านผู้ทรงคุณวุฒิ ได้ทำการประเมินฯ ตามความคิดเห็นของท่าน โดยใส่เครื่องหมาย ✓ ลงในช่องตามความเป็นจริงมากที่สุด และผลการประเมินจากผู้ทรงคุณวุฒิจะนำไปใช้ในการพัฒนาแบบสอบถามเพื่อนำไปใช้ในการเก็บข้อมูลจากกลุ่มตัวอย่างต่อไป

แบบประเมินความเหมาะสมแบ่งการประเมินออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลผู้ประเมิน

ตอนที่ 2 แบบประเมินความเที่ยงตรงของแบบสอบถามปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตอนที่ 3 ข้อคิดเห็นและข้อเสนอแนะอื่นๆ

ตอนที่ 1 สถานภาพทั่วไป

ชื่อผู้ประเมิน : .....

ตำแหน่ง : .....

สถานที่ทำงาน : .....

เบอร์โทรศัพท์/email : .....

ตอนที่ 2 แบบประเมินความเที่ยงตรงของแบบสอบถามเกี่ยวกับระดับความคิดเห็น เรื่องปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์การพิจารณา ดังนี้

1 หมายถึง ข้อคำถามนี้มีความเหมาะสม

0 หมายถึง ไม่แน่ใจว่าข้อคำถามนี้มีความเหมาะสม

-1 หมายถึง ข้อคำถามนี้ไม่มีความเหมาะสม

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
ด้านสถาปัตยกรรมองค์กร (Enterprise Architecture)				
1. สถาปัตยกรรมธุรกิจ (Business Architecture)				
1.1 กำหนดวิสัยทัศน์และกลยุทธ์ด้านปัญญาประดิษฐ์ที่สอดคล้องกับพันธกิจขององค์กร				
1.2 บูรณาการการใช้ปัญญาประดิษฐ์เข้ากับกระบวนการหลักของมหาวิทยาลัย				
1.3 ประเมินความพร้อมและศักยภาพของหน่วยงานในการใช้เทคโนโลยีปัญญาประดิษฐ์อย่างต่อเนื่อง				
1.4 ผู้บริหารระดับสูงสนับสนุนและส่งเสริมการใช้เทคโนโลยีปัญญาประดิษฐ์เพื่อพัฒนาองค์กร				
2. สถาปัตยกรรมข้อมูล (Data Architecture)				
2.1 มีกลยุทธ์ข้อมูลที่สนับสนุนการใช้งานปัญญาประดิษฐ์อย่างชัดเจน				
2.2 มีมาตรการควบคุมคุณภาพและความมั่นคงปลอดภัยของข้อมูลอย่างเป็นระบบ				
2.3 โครงสร้างข้อมูลรองรับการจัดเก็บและประมวลผล Big Data และข้อมูลแบบ Unstructured				
2.4 มีระบบติดป้ายกำกับและจัดการข้อมูลเพื่อสนับสนุนการเรียนรู้ของโมเดลปัญญาประดิษฐ์				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
3. สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture)				
3.1 มีการพัฒนาแอปพลิเคชันหรือระบบสารสนเทศที่เชื่อมโยงกับปัญญาประดิษฐ์				
3.2 ระบบแอปพลิเคชันได้รับการออกแบบให้สามารถปรับขนาดและเชื่อมต่อได้ง่าย				
3.3 มีมาตรฐานกลางในการพัฒนาและบูรณาการแอปพลิเคชัน				
3.4 มีการปรับปรุงระบบงานอย่างต่อเนื่องเพื่อรองรับเทคโนโลยีปัญญาประดิษฐ์ใหม่ ๆ				
4. สถาปัตยกรรมเทคโนโลยี (Technology Architecture)				
4.1 มีโครงสร้างพื้นฐานด้านเทคโนโลยีที่รองรับการประมวลผลของปัญญาประดิษฐ์				
4.2 ใช้แพลตฟอร์มคลาวด์ในการพัฒนาปัญญาประดิษฐ์				
4.3 มีแผนการบำรุงรักษาและอัปเดตเทคโนโลยีอย่างต่อเนื่อง				
4.4 มีการนำเทคโนโลยี Edge AI หรือระบบประมวลผลแบบกระจายมาใช้เพื่อเพิ่มประสิทธิภาพ				
5. สถาปัตยกรรมด้านความมั่งคงปลอดภัย (Security Architecture)				
5.1 มีกลยุทธ์และนโยบายความปลอดภัยทางไซเบอร์ที่ชัดเจน				
5.2 มีการประเมินและป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์				
5.3 มีการเข้ารหัสและจำกัดสิทธิ์การเข้าถึงข้อมูลอย่างเหมาะสม				
5.4 มีแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลและระบบปัญญาประดิษฐ์				
6. สถาปัตยกรรมการบูรณาการ (Integration Architecture)				
6.1 มีสถาปัตยกรรมเชื่อมต่อโมเดลปัญญาประดิษฐ์กับระบบหลักขององค์กร				
6.2 มีมาตรฐานหรือ API กลางสำหรับการแลกเปลี่ยนข้อมูลระหว่างระบบ				
6.3 มีการตรวจสอบและทดสอบการเชื่อมต่อระหว่างระบบอย่างสม่ำเสมอ				
6.4 ระบบบูรณาการมีความยืดหยุ่นรองรับการเปลี่ยนแปลงของเทคโนโลยี				
7. สถาปัตยกรรมการกำกับดูแล (Governance Architecture)				
7.1 มีกรอบการกำกับดูแล (Governance Framework) ด้านปัญญาประดิษฐ์ที่ชัดเจน				
7.2 มีการติดตามและประเมินผลการใช้ปัญญาประดิษฐ์อย่างต่อเนื่อง				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
7.3 มีการกำหนดบทบาทและความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับปัญญาประดิษฐ์				
7.4 กำหนดตัวชี้วัดความสำเร็จของโครงการปัญญาประดิษฐ์สอดคล้องกับเป้าหมายองค์กร				
ด้านเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence)				
1. การเรียนรู้ของเครื่อง (Machine Learning)				
1.1 มีการนำเทคโนโลยีการเรียนรู้ของเครื่องมาใช้ในการวิเคราะห์ข้อมูล				
1.2 โมเดลการเรียนรู้ของเครื่องช่วยสนับสนุนการตัดสินใจของผู้บริหารและบุคลากร				
1.3 มีการปรับปรุงและพัฒนาโมเดลอย่างต่อเนื่องตามข้อมูลใหม่				
1.4 ผลลัพธ์จากการเรียนรู้ของเครื่องมีความแม่นยำและเชื่อถือได้				
2. การเรียนรู้เชิงลึก (Deep Learning)				
2.1 มีการประยุกต์ใช้การเรียนรู้เชิงลึกกับข้อมูลขนาดใหญ่หรือข้อมูลซับซ้อน				
2.2 ระบบการเรียนรู้เชิงลึกช่วยเพิ่มประสิทธิภาพในการคาดการณ์หรือจำแนกข้อมูล				
2.3 โครงสร้างพื้นฐานรองรับการประมวลผลของโมเดลเชิงลึกได้อย่างเหมาะสม				
2.4 มีการประเมินประสิทธิภาพของโมเดลการเรียนรู้เชิงลึกอย่างสม่ำเสมอ				
3. การประมวลผลภาษาธรรมชาติ (Natural Language Processing - NLP)				
3.1 มีการใช้เทคโนโลยี NLP ในการวิเคราะห์ข้อมูลข้อความหรือภาษา				
3.2 ระบบ NLP ช่วยเพิ่มประสิทธิภาพในการให้บริการหรือการสื่อสารกับผู้ใช้				
3.3 การประมวลผลภาษามีความถูกต้องและสอดคล้องกับบริบทของสถาบัน				
3.4 มีการพัฒนาและปรับปรุงระบบ NLP อย่างต่อเนื่อง				
4. ความรู้เชิงพฤติกรรม (Behavioral AI)				
4.1 มีการใช้ปัญญาประดิษฐ์ในการวิเคราะห์พฤติกรรมของผู้ใช้หรือผู้เรียน				
4.2 ผลการวิเคราะห์พฤติกรรมช่วยสนับสนุนการวางแผนและปรับปรุงบริการ				
4.3 ระบบสามารถเรียนรู้และปรับตัวตามพฤติกรรมที่เปลี่ยนแปลงได้				
4.4 การใช้ Behavioral AI คำนึงถึงจริยธรรมและความเป็นส่วนตัวของผู้ใช้				
ด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity)				
1. การมองเห็นและเฝ้าระวัง (Observability & Visibility)				
1.1 ติดตั้งเครื่องมือสำหรับการมองเห็นและเฝ้าระวังที่ครอบคลุมเครือข่ายแอปพลิเคชัน และโครงสร้างพื้นฐาน				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
1.2 มีมาตรการสร้างความโปร่งใสและตรวจสอบการทำงานของระบบปัญญาประดิษฐ์				
1.3 มีการเข้ารหัสข้อมูลทั้งขณะส่งและจัดเก็บ				
1.4 ระบบสามารถแสดงภาพรวมสถานะการทำงานและแจ้งเตือนเหตุการณ์ผิดปกติได้แบบเรียลไทม์				
2. การตรวจจับภัยคุกคาม (Threat Detection)				
2.1 ระบบสามารถตรวจจับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ				
2.2 มีการใช้เทคโนโลยีปัญญาประดิษฐ์วิเคราะห์ Log และ Traffic เพื่อระบุพฤติกรรมที่ผิดปกติ				
2.3 มีการจำลองและทดสอบสถานการณ์โจมตีทางไซเบอร์เพื่อประเมินความแข็งแกร่งของระบบอย่างสม่ำเสมอ				
2.4 มีการตรวจสอบช่องโหว่ของระบบแอปพลิเคชัน และโครงสร้างพื้นฐานเป็นประจำ				
3. การสืบสวนและวิเคราะห์ (Investigation & Analysis)				
3.1 มีระบบสนับสนุนการรวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่งได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย				
3.2 มีทีมผู้เชี่ยวชาญวิเคราะห์เชิงลึกระบุแหล่งและขอบเขตความเสียหาย				
3.3 มีการใช้เครื่องมือวิเคราะห์เหตุการณ์ เพื่อสืบหาต้นตอของภัยคุกคามอย่างเป็นระบบ				
3.4 ผลการวิเคราะห์ถูกนำมาใช้ปรับปรุงมาตรการความปลอดภัยและเพิ่มประสิทธิภาพการป้องกันในอนาคต				
4. การตอบสนองและการป้องกันเชิงรุก (Response & Proactive Defense)				
4.1 มีแผนตอบสนองเหตุการณ์ไซเบอร์ที่ชัดเจนและเป็นปัจจุบัน				
4.2 ระบบสามารถตอบสนองและป้องกันภัยคุกคามเชิงรุกได้โดยอัตโนมัติ				
4.3 มีการดำเนินกิจกรรม Threat Hunting เพื่อตรวจหาภัยคุกคามที่อาจแฝงอยู่ในระบบอย่างต่อเนื่อง				
4.4 มีการบังคับใช้มาตรการ Zero Trust เพื่อควบคุมสิทธิ์การเข้าถึงข้อมูลและทรัพยากรภายในองค์กร				
5. ความทนทานและการฟื้นฟู (Resilience & Recovery)				
5.1 ระบบได้รับการออกแบบให้สามารถดำเนินงานต่อได้แม้บางส่วนได้รับความเสียหาย				
5.2 มีการทดสอบแผนกู้คืนระบบหลังภัยพิบัติอย่างสม่ำเสมอ				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
5.3 มีการจัดเก็บข้อมูลสำรองในพื้นที่แยกหรือระบบคลาวด์ เพื่อป้องกันการสูญหายจาก Ransomware				
5.4 มีมาตรการในการฟื้นฟูระบบและบริการให้กลับมาทำงานได้อย่างรวดเร็วหลังเหตุการณ์โจมตี				
6. ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์ (Collaboration & Cybersecurity Awareness)				
6.1 มีทีมปฏิบัติการด้านความมั่นคงปลอดภัยหรือใช้บริการภายนอกในการเฝ้าระวังระบบอย่างมีประสิทธิภาพ				
6.2 มีการแลกเปลี่ยนและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอกอย่างต่อเนื่อง				
6.3 มีการจัดฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรเป็นประจำ				
6.4 องค์กรปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยสากล				
การจัดการองค์กรดิจิทัล()Digital Enterprise Management)				
1. กลยุทธ์ดิจิทัล (Digital Strategy)				
1.1 มีการกำหนดและสื่อสารกลยุทธ์ดิจิทัลไปยังทุกหน่วยงานในองค์กรอย่างชัดเจน				
1.2 มีกระบวนการวัดผลความสำเร็จของกลยุทธ์ผ่านตัวชี้วัดที่เชื่อมโยงกับพันธกิจองค์กร				
1.3 มีคณะกรรมการกำกับดูแลดิจิทัล (Digital Governance Committee)				
1.4 มีการจัดสรรคงบประมาณและประเมินผลตอบแทนการลงทุนของโครงการ AI และโครงสร้างพื้นฐานดิจิทัลอย่างเป็นระบบ				
2. โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure)				
2.1 มีการลงทุนในโครงสร้างพื้นฐานเทคโนโลยีเพื่อรองรับการเติบโตในระยะ 3–5 ปีข้างหน้า				
2.2 มีแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อให้ระบบ AI ทำงานต่อได้ในภาวะวิกฤต				
2.3 มีระบบสำรองข้อมูลและศูนย์ข้อมูลสำรอง (Disaster Recovery Site) เพื่อป้องกันการสูญเสียข้อมูล				
2.4 มีการปรับปรุงและอัปเกรดเทคโนโลยีให้สอดคล้องกับนวัตกรรมดิจิทัลสมัยใหม่อย่างต่อเนื่อง				
3. การจัดการข้อมูล (Data Management)				
3.1 มีการบริหารจัดการข้อมูลให้เป็นสินทรัพย์หลักขององค์กร				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
3.2 มีการพัฒนาและบำรุงรักษาคลังข้อมูลเพื่อรองรับการทำงานของปัญญาประดิษฐ์				
3.3 ใช้เทคโนโลยีดิจิทัลเพิ่มประสิทธิภาพการทำงานร่วมกันระหว่างหน่วยงาน				
3.4 มีมาตรการควบคุมคุณภาพและความถูกต้องของข้อมูล (Data Quality & Integrity) เพื่อการตัดสินใจที่แม่นยำ				
4. กระบวนการอัตโนมัติ (Process Automation)				
4.1 มีการใช้ระบบอัตโนมัติในกระบวนการภายในเพื่อลดภาระงานบริหาร				
4.2 มีการประเมินและปรับปรุงประสบการณ์ดิจิทัลของนักศึกษาและบุคลากรอย่างต่อเนื่อง				
4.3 มีการบูรณาการระบบอัตโนมัติเข้ากับระบบสารสนเทศหลักขององค์กร				
4.4 มีการติดตามผลลัพธ์จากการปรับใช้กระบวนการอัตโนมัติเพื่อเพิ่มประสิทธิภาพการดำเนินงาน				
5. ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)				
5.1 มีการรวมความปลอดภัยตั้งแต่ต้นทางของทุกโครงการดิจิทัล				
5.2 มีการสื่อสารความเสี่ยงไซเบอร์ต่อผู้บริหารในรูปผลกระทบทางธุรกิจ				
5.3 มีการประเมินช่องโหว่และทดสอบการเจาะระบบ (Vulnerability Assessment & Penetration Test) อย่างต่อเนื่อง				
5.4 มีการจัดทำรายงานสถานะความปลอดภัยไซเบอร์และแผนการปรับปรุงอย่างเป็นระบบ				
6. นวัตกรรมและความคล่องตัว (Innovation and Agility)				
6.1 ส่งเสริมวัฒนธรรมนวัตกรรมให้บุคลากรทดลองและเรียนรู้เทคโนโลยีใหม่ ๆ				
6.2 มีการจัดตั้งห้องปฏิบัติการนวัตกรรมหรือกลไกนำร่องเพื่อพัฒนาโซลูชันใหม่				
6.3 มีความคล่องตัวในการปรับเปลี่ยนหรือปรับขนาดโครงการดิจิทัลให้สอดคล้องกับการเปลี่ยนแปลงของตลาด				
6.4 ใช้แนวทางการพัฒนาแบบ Agile/Scrum เพื่อเพิ่มความเร็วและความยืดหยุ่นในการดำเนินงาน				
ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (Artificial Intelligence Enterprise Architecture)				
1. การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ (EA–AI Integration)				
1.1 มีการบูรณาการการใช้ปัญญาประดิษฐ์เข้ากับสถาปัตยกรรมองค์กรอย่างเป็นระบบ				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
1.2 โครงสร้างสถาปัตยกรรมองค์กรของสถาบันสนับสนุนการนำปัญญาประดิษฐ์ไปใช้ในกระบวนการหลักได้อย่างเหมาะสม				
1.3 การพัฒนาปัญญาประดิษฐ์ของสถาบันสอดคล้องกับแผนสถาปัตยกรรมองค์กรในภาพรวม				
1.4 การบูรณาการสถาปัตยกรรมองค์กร และปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพและความยืดหยุ่นในการดำเนินงานของสถาบัน				
2. กรอบการทำงานเชิงสถาปัตยกรรม (Architectural Framework)				
2.1 มีกรอบการทำงานเชิงสถาปัตยกรรมที่ชัดเจนสำหรับการพัฒนาและใช้งานปัญญาประดิษฐ์				
2.2 สามารถกำหนดทิศทางและมาตรฐานของระบบปัญญาประดิษฐ์ได้อย่างเหมาะสม				
2.3 ช่วยลดความซ้ำซ้อนและความซับซ้อนของระบบสารสนเทศ				
2.4 สามารถปรับปรุงและพัฒนาให้สอดคล้องกับเทคโนโลยีปัญญาประดิษฐ์ที่เปลี่ยนแปลงได้				
3.การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ (AI-driven Information System Design & Development)				
3.1 ระบบสารสนเทศของสถาบันถูกออกแบบให้ใช้ปัญญาประดิษฐ์ เพื่อเพิ่มประสิทธิภาพการทำงาน				
3.2 การพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ช่วยสนับสนุนการตัดสินใจของผู้บริหารและผู้ปฏิบัติงาน				
3.3 ระบบปัญญาประดิษฐ์สามารถเชื่อมโยงและทำงานร่วมกับระบบสารสนเทศเดิมได้อย่างราบรื่น				
3.4 การออกแบบระบบสารสนเทศด้วยปัญญาประดิษฐ์ ที่คำนึงถึงความปลอดภัยและความน่าเชื่อถือของข้อมูล				
4.การจัดการทรัพยากรอย่างชาญฉลาด (Intelligent Resource Management)				
4.1 ใช้ปัญญาประดิษฐ์ในการบริหารจัดการทรัพยากรด้านเทคโนโลยีอย่างมีประสิทธิภาพ				
4.2 ระบบปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพในการใช้ทรัพยากรบุคคลและงบประมาณของสถาบัน				
4.3 การจัดการทรัพยากรด้วยปัญญาประดิษฐ์ช่วยลดต้นทุนและเพิ่มความคุ้มค่าในการดำเนินงาน				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
4.4 สามารถติดตามและประเมินการใช้ทรัพยากรผ่านระบบอัจฉริยะได้อย่างเหมาะสม				
5.ความสามารถในการปรับตัวต่อการเปลี่ยนแปลง (Adaptability & Agility)				
5.1 สามารถปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยีได้รวดเร็ว				
5.2 ระบบปัญญาประดิษฐ์สนับสนุนการปรับปรุงกระบวนการทำงานให้มีความคล่องตัวมากขึ้น				
5.3 สามารถปรับเปลี่ยนหรือขยายระบบปัญญาประดิษฐ์ได้ตามความต้องการในอนาคต				
5.4 ตอบสนองต่อการเปลี่ยนแปลงด้านนโยบายและสภาพแวดล้อมได้อย่างมีประสิทธิภาพ				
6.ความสามารถในการรับมือภัยคุกคามและความเสี่ยง (Threat & Risk Responsiveness)				
6.1 สนับสนุนการตรวจจับภัยคุกคามทางดิจิทัลได้อย่างรวดเร็ว				
6.2 ระบบปัญญาประดิษฐ์มีบทบาทในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ				
6.3 สามารถตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ				
6.4 การใช้ปัญญาประดิษฐ์ช่วยเพิ่มความสามารถในการป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์				
7. จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ (AI Ethics and Responsibility)				
7.1 มีการกำหนดหลักจริยธรรมในการพัฒนาและใช้ปัญญาประดิษฐ์อย่างชัดเจน				
7.2 มีระบบปัญญาประดิษฐ์ถูกออกแบบให้โปร่งใสและสามารถอธิบายผลลัพธ์ได้				
7.3 มีมาตรการลดอคติในข้อมูลและโมเดลปัญญาประดิษฐ์				
7.4 มีการอบรมและส่งเสริมความรู้เรื่องจริยธรรมและความรับผิดชอบในการใช้ปัญญาประดิษฐ์				
ด้านการจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)				
1. การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection)				
1.1 มีการทดสอบเจาะระบบ และตรวจสอบโค้ดของแอปพลิเคชันเพื่อค้นหาช่องโหว่อย่างสม่ำเสมอ				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
1.2 มีการประเมินประสิทธิภาพของมาตรการป้องกันภัยไซเบอร์อย่างต่อเนื่องเพื่อลดความเสี่ยง				
1.3 ใช้เทคโนโลยี AI หรือ Machine Learning ในการตรวจจับพฤติกรรมที่ผิดปกติในระบบเครือข่าย				
1.4 มีระบบแจ้งเตือนภัยคุกคามแบบเรียลไทม์ เพื่อให้ทีมสามารถตอบสนองได้อย่างรวดเร็ว				
2. การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response)				
2.1 มีแผนขั้นตอนการตอบสนองเหตุการณ์ทางไซเบอร์ที่ครอบคลุมทุกระบบ				
2.2 มีแนวทางเฉพาะในการจัดการเหตุการณ์ที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์				
2.3 มีการกำหนดบทบาทและความรับผิดชอบของทีม IR (Incident Response Team) อย่างชัดเจน				
2.4 มีการทดสอบจำลองเหตุการณ์โจมตี (Cyber Drill) เพื่อประเมินความพร้อมของบุคลากรและระบบ				
3. การประเมินและจัดการความเสี่ยง (Risk Assessment and Management)				
3.1 มีการประเมินและจัดการความเสี่ยงทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง				
3.2 มีระบบบริหารจัดการการเปลี่ยนแปลงของ IT และ AI อย่างเป็นระบบ				
3.3 มีการบริหารจัดการแพตช์ (Patch Management) และอัปเดตซอฟต์แวร์อย่างรวดเร็วและมีประสิทธิภาพ				
3.4 มีการจัดทำรายงานความเสี่ยงและความปลอดภัยทางไซเบอร์ที่ชัดเจนสำหรับผู้บริหาร				
4. การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy)				
4.1 มีนโยบายและมาตรการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย PDPA				
4.2 มีการเข้ารหัสและควบคุมการเข้าถึงข้อมูลเพื่อป้องกันการรั่วไหลหรือการโจมตี				
4.3 มีการบริหารจัดการความเสี่ยงของข้อมูลที่ใช้โดยระบบปัญญาประดิษฐ์อย่างเป็นระบบ				
4.4 มีการตรวจสอบและประเมินการจัดการข้อมูลอย่างสม่ำเสมอเพื่อรักษาความเป็นส่วนตัวของผู้ใช้				
5. การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย (Security Awareness Training)				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
5.1 มีการจัดฝึกอบรมภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับสถาบันอุดมศึกษาอย่างสม่ำเสมอ				
5.2 บุคลากรได้รับการอบรมและอัปเดตความรู้ด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง				
5.3 มีการจัดกิจกรรมหรือการรณรงค์สร้างจิตสำนึกด้านความปลอดภัยดิจิทัลภายในองค์กร				
5.4 มีระบบประเมินผลหลังการฝึกอบรมเพื่อวัดผลการเรียนรู้และการนำไปใช้จริงของผู้เข้าร่วม				
6. นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance)				
6.1 มีนโยบายและข้อบังคับด้านความปลอดภัยสำหรับ AI และ Cloud				
6.2 ผู้บริหารมีการทบทวนและประเมินสถานะความปลอดภัยของระบบอย่างสม่ำเสมอ				
6.3 จัดทำสัญญากับผู้ให้บริการภายนอก พร้อมข้อกำหนดด้านความปลอดภัย				
6.4 ใช้เครื่องมืออัตโนมัติในการตรวจสอบและบังคับใช้ข้อกำหนดด้านความปลอดภัย				
7. ความมั่นคงปลอดภัยของเครือข่าย (Network Security)				
7.1 มีมาตรการความปลอดภัยเครือข่ายเข้มงวดโดยเฉพาะ IoT และอุปกรณ์นักศึกษา				
7.2 มีการกำหนดสิทธิ์การเข้าถึงตามหลัก “Least Privilege” อย่างชัดเจน				
7.3 ระบบเครือข่ายได้รับการตรวจสอบและอัปเดตการป้องกันภัยอย่างต่อเนื่อง				
7.4 มีการใช้ไฟร์วอลล์ ระบบ IDS/IPS และระบบตรวจสอบการจราจรเครือข่ายเพื่อป้องกันภัยคุกคาม				
8. โซลูชันความมั่นคงปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI-driven Security Solutions)				
8.1 ใช้โซลูชัน AI เพื่อช่วยตรวจจับและตอบสนองต่อภัยคุกคามโดยอัตโนมัติ				
8.2 ระบบ AI ถูกฝึกด้วยข้อมูลภัยคุกคามจริงเพื่อเพิ่มความแม่นยำในการวิเคราะห์				
8.3 มีการประเมินและปรับปรุงโมเดล AI ด้านความปลอดภัยอย่างต่อเนื่อง				
8.4 มีการผสานระบบ AI Security เข้ากับระบบปฏิบัติการด้านความปลอดภัยขององค์กรอย่างเป็นเอกภาพ				
9. ความปลอดภัยบนคลาวด์ (Cloud Security)				

รายการประเมิน	ระดับความคิดเห็น			
	1	0	-1	ข้อเสนอแนะ
9.1 มีมาตรการจัดการการตั้งค่าที่ผิดพลาด (Misconfiguration) ในระบบคลาวด์อย่างเข้มงวด				
9.2 มีการควบคุมสิทธิ์การเข้าถึงข้อมูลบนคลาวด์ตามระดับผู้ใช้งานอย่างเหมาะสม				
9.3 มีการเข้ารหัสและตรวจสอบการรับส่งข้อมูลระหว่างคลาวด์และระบบภายใน				
9.4 มีการสำรองข้อมูลและแผนฟื้นฟูข้อมูลบนคลาวด์เพื่อรองรับเหตุการณ์ไม่คาดคิด				

ตอนที่ 3 ข้อเสนอแนะอื่นๆ

.....

.....

.....

.....

ขอขอบพระคุณเป็นอย่างสูง
ที่ท่านให้ความอนุเคราะห์สละเวลาตอบแบบประเมินอันเป็นประโยชน์ต่องานวิจัย

นางสาวเนาวรัตน์ ปิ่นอำนาจ
โทรศัพท์ 0818868474, email: s6602052910038@email.kmutnb.ac.th



แบบสอบถามปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์
เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ชื่องานวิจัย สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

อาจารย์ที่ปรึกษา ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข
ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ

ผู้วิจัย นางสาวเนาวรัตน์ ปิ่นอำนาจ
นักศึกษาปริญญาเอก สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบสอบถามฉบับนี้ เป็นส่วนหนึ่งของดุษฎีนิพนธ์ระดับปริญญาเอก สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ เรื่อง สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยมีวัตถุประสงค์เพื่อหาปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา คำตอบของท่านมีคุณค่าอย่างยิ่งต่องานวิจัยโดยจะใช้ข้อมูลเพื่อนำไปสรุปเป็นภาพรวม คำตอบของท่านจะไม่มีผลกระทบต่อตัวท่านหรือองค์กรของท่าน ข้อมูลที่ตรงกับความเป็นจริงและสมบูรณ์เท่านั้นที่จะช่วยให้ผลการวิจัยเป็นไปด้วยความถูกต้องและก่อให้เกิดประโยชน์ต่อส่วนรวม ผู้วิจัยจึงใคร่ขอให้ท่านช่วยกรุณาตอบแบบสอบถามฉบับนี้

แบบสอบถามแบ่งออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 แบบสอบถามเกี่ยวกับสถานภาพทั่วไป จำนวน 4 ข้อ

ตอนที่ 2 แบบสอบถามเกี่ยวกับปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา ลักษณะแบบสอบถามเป็นแบบมาตรส่วนประเมินค่า (Rating Scale) จำนวน 156 ข้อ

โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณา ดังนี้

5 หมายถึง เหมาะสมมากที่สุด
4 หมายถึง เหมาะสมมาก
3 หมายถึง เหมาะสมปานกลาง
2 หมายถึง เหมาะสมน้อย
1 หมายถึง เหมาะสมน้อยที่สุด

ตอนที่ 3 แบบสอบถามเกี่ยวกับข้อคิดเห็น และข้อเสนอแนะอื่นๆ ที่มีต่อปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ผู้วิจัยขอขอบพระคุณอย่างสูงที่ท่านให้ความอนุเคราะห์ตอบแบบสอบถามมา ณ โอกาสนี้

นางสาวเนาวรัตน์ ปิ่นอำนาจ
ผู้วิจัย

ติดต่อผู้วิจัย
โทรศัพท์ 081 886 8474 LINE ID: nawaratpin
อีเมล s6602052910038@email.kmutnb.ac.th

ตอนที่ 1 สถานภาพทั่วไป

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่านมากที่สุดเพียงตัวเลือกเดียว

1. เพศ

☐ 1. ชาย ☐ 2. หญิง

2. วุฒิการศึกษา

☐ 1. ต่ำกว่าปริญญาตรี

☐ 2. ปริญญาตรี

☐ 3. ปริญญาโท

☐ 4. ปริญญาเอก

3. สถานภาพ

☐ 1. ผู้บริหาร

☐ 2. อาจารย์

☐ 3. บุคลากรสายสนับสนุน

4. สถาบันอุดมศึกษาที่สังกัด

ตอนที่ 2 แบบสอบถามเกี่ยวกับระดับความคิดเห็น เรื่องปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
ด้านสถาปัตยกรรมองค์กร (Enterprise Architecture)					
1. สถาปัตยกรรมธุรกิจ (Business Architecture)					
1.1 กำหนดวิสัยทัศน์และกลยุทธ์ด้านปัญญาประดิษฐ์ที่สอดคล้องกับพันธกิจขององค์กร					
1.2 บูรณาการการใช้ปัญญาประดิษฐ์เข้ากับกระบวนการหลักของมหาวิทยาลัย					
1.3 ประเมินความพร้อมและศักยภาพของหน่วยงานในการใช้เทคโนโลยีปัญญาประดิษฐ์อย่างต่อเนื่อง					
1.4 ผู้บริหารระดับสูงสนับสนุนและส่งเสริมการใช้เทคโนโลยีปัญญาประดิษฐ์เพื่อพัฒนาองค์กร					
2. สถาปัตยกรรมข้อมูล (Data Architecture)					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
2.1 มีกลยุทธ์ข้อมูลที่สนับสนุนการใช้งานปัญญาประดิษฐ์อย่างชัดเจน					
2.2 มีมาตรการควบคุมคุณภาพและความมั่นคงปลอดภัยของข้อมูลอย่างเป็นระบบ					
2.3 โครงสร้างข้อมูลรองรับการจัดเก็บและประมวลผล Big Data และข้อมูลแบบ Unstructured					
2.4 มีระบบติดป้ายกำกับและจัดการข้อมูลเพื่อสนับสนุนการเรียนรู้ของโมเดลปัญญาประดิษฐ์					
3. สถาปัตยกรรมระบบแอปพลิเคชัน (Application Architecture)					
3.1 มีการพัฒนาแอปพลิเคชันหรือระบบสารสนเทศที่เชื่อมโยงกับปัญญาประดิษฐ์					
3.2 ระบบแอปพลิเคชันได้รับการออกแบบให้สามารถปรับขนาดและเชื่อมต่อได้ง่าย					
3.3 มีมาตรฐานกลางในการพัฒนาและบูรณาการแอปพลิเคชัน					
3.4 มีการปรับปรุงระบบงานอย่างต่อเนื่องเพื่อรองรับเทคโนโลยีปัญญาประดิษฐ์ใหม่ ๆ					
4. สถาปัตยกรรมเทคโนโลยี (Technology Architecture)					
4.1 มีโครงสร้างพื้นฐานด้านเทคโนโลยีที่รองรับการประมวลผลของปัญญาประดิษฐ์					
4.2 ใช้แพลตฟอร์มคลาวด์ในการพัฒนาปัญญาประดิษฐ์					
4.3 มีแผนการบำรุงรักษาและอัปเดตเทคโนโลยีอย่างต่อเนื่อง					
4.4 มีการนำเทคโนโลยี Edge AI หรือระบบประมวลผลแบบกระจายมาใช้เพื่อเพิ่มประสิทธิภาพ					
5. สถาปัตยกรรมด้านความมั่งคงปลอดภัย (Security Architecture)					
5.1 มีกลยุทธ์และนโยบายความปลอดภัยทางไซเบอร์ที่ชัดเจน					
5.2 มีการประเมินและป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์					
5.3 มีการเข้ารหัสและจำกัดสิทธิ์การเข้าถึงข้อมูลอย่างเหมาะสม					
5.4 มีแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลและระบบปัญญาประดิษฐ์					
6. สถาปัตยกรรมการบูรณาการ (Integration Architecture)					
6.1 มีสถาปัตยกรรมเชื่อมต่อโมเดลปัญญาประดิษฐ์กับระบบหลักขององค์กร					
6.2 มีมาตรฐานหรือ API กลางสำหรับการแลกเปลี่ยนข้อมูลระหว่างระบบ					
6.3 มีการตรวจสอบและทดสอบการเชื่อมต่อระหว่างระบบอย่างสม่ำเสมอ					
6.4 ระบบบูรณาการมีความยืดหยุ่นรองรับการเปลี่ยนแปลงของเทคโนโลยี					
7. สถาปัตยกรรมการกำกับดูแล (Governance Architecture)					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
7.1 มีกรอบการกำกับดูแล (Governance Framework) ด้านปัญญาประดิษฐ์ที่ชัดเจน					
7.2 มีการติดตามและประเมินผลการใช้ปัญญาประดิษฐ์อย่างต่อเนื่อง					
7.3 มีการกำหนดบทบาทและความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับปัญญาประดิษฐ์					
7.4 กำหนดตัวชี้วัดความสำเร็จของโครงการปัญญาประดิษฐ์สอดคล้องกับเป้าหมายองค์กร					
ด้านเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence)					
1. การเรียนรู้ของเครื่อง (Machine Learning)					
1.1 มีการนำเทคโนโลยีการเรียนรู้ของเครื่องมาใช้ในการวิเคราะห์ข้อมูล					
1.2 โมเดลการเรียนรู้ของเครื่องช่วยสนับสนุนการตัดสินใจของผู้บริหารและบุคลากร					
1.3 มีการปรับปรุงและพัฒนาโมเดลอย่างต่อเนื่องตามข้อมูลใหม่					
1.4 ผลลัพธ์จากการเรียนรู้ของเครื่องมีความแม่นยำและเชื่อถือได้					
2. การเรียนรู้เชิงลึก (Deep Learning)					
2.1 มีการประยุกต์ใช้การเรียนรู้เชิงลึกกับข้อมูลขนาดใหญ่หรือข้อมูลซับซ้อน					
2.2 ระบบการเรียนรู้เชิงลึกช่วยเพิ่มประสิทธิภาพในการคาดการณ์หรือจำแนกข้อมูล					
2.3 โครงสร้างพื้นฐานรองรับการประมวลผลของโมเดลเชิงลึกได้อย่างเหมาะสม					
2.4 มีการประเมินประสิทธิภาพของโมเดลการเรียนรู้เชิงลึกอย่างสม่ำเสมอ					
3. การประมวลผลภาษาธรรมชาติ (Natural Language Processing - NLP)					
3.1 มีการใช้เทคโนโลยี NLP ในการวิเคราะห์ข้อมูลข้อความหรือภาษา					
3.2 ระบบ NLP ช่วยเพิ่มประสิทธิภาพในการให้บริการหรือการสื่อสารกับผู้ใช้					
3.3 การประมวลผลภาษามีความถูกต้องและสอดคล้องกับบริบทของสถาบัน					
3.4 มีการพัฒนาและปรับปรุงระบบ NLP อย่างต่อเนื่อง					
4. ความรู้เชิงพฤติกรรม (Behavioral AI)					
4.1 มีการใช้ปัญญาประดิษฐ์ในการวิเคราะห์พฤติกรรมของผู้ใช้หรือผู้เรียน					
4.2 ผลการวิเคราะห์พฤติกรรมช่วยสนับสนุนการวางแผนและปรับปรุงบริการ					
4.3 ระบบสามารถเรียนรู้และปรับตัวตามพฤติกรรมที่เปลี่ยนแปลงได้					
4.4 การใช้ Behavioral AI คำนึงถึงจริยธรรมและความเป็นส่วนตัวของผู้ใช้					
ด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity)					
1. การมองเห็นและเฝ้าระวัง (Observability & Visibility)					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
1.1 ติดตั้งเครื่องมือสำหรับการมองเห็นและเฝ้าระวังที่ครอบคลุมเครือข่ายแอปพลิเคชัน และโครงสร้างพื้นฐาน					
1.2 มีมาตรการสร้างความโปร่งใสและตรวจสอบการทำงานของระบบปัญญาประดิษฐ์					
1.3 มีการเข้ารหัสข้อมูลทั้งขณะส่งและจัดเก็บ					
1.4 ระบบสามารถแสดงภาพรวมสถานะการทำงานและแจ้งเตือนเหตุการณ์ผิดปกติได้แบบเรียลไทม์					
2. การตรวจจับภัยคุกคาม (Threat Detection)					
2.1 ระบบสามารถตรวจจับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ					
2.2 มีการใช้เทคโนโลยีปัญญาประดิษฐ์วิเคราะห์ Log และ Traffic เพื่อระบุพฤติกรรมที่ผิดปกติ					
2.3 มีการจำลองและทดสอบสถานการณ์โจมตีทางไซเบอร์เพื่อประเมินความแข็งแกร่งของระบบอย่างสม่ำเสมอ					
2.4 มีการตรวจสอบช่องโหว่ของระบบแอปพลิเคชัน และโครงสร้างพื้นฐานเป็นประจำ					
3. การสืบสวนและวิเคราะห์ (Investigation & Analysis)					
3.1 มีระบบสนับสนุนการรวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่งได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย					
3.2 มีทีมผู้เชี่ยวชาญวิเคราะห์เชิงลึกระบุแหล่งและขอบเขตความเสียหาย					
3.3 มีการใช้เครื่องมือวิเคราะห์เหตุการณ์ เพื่อสืบหาต้นตอของภัยคุกคามอย่างเป็นระบบ					
3.4 ผลการวิเคราะห์ถูกนำมาใช้ปรับปรุงมาตรการความปลอดภัยและเพิ่มประสิทธิภาพการป้องกันในอนาคต					
4. การตอบสนองและการป้องกันเชิงรุก (Response & Proactive Defense)					
4.1 มีแผนตอบสนองเหตุการณ์ไซเบอร์ที่ชัดเจนและเป็นปัจจุบัน					
4.2 ระบบสามารถตอบสนองและป้องกันภัยคุกคามเชิงรุกได้โดยอัตโนมัติ					
4.3 มีการดำเนินกิจกรรม Threat Hunting เพื่อตรวจหาภัยคุกคามที่อาจแฝงอยู่ในระบบอย่างต่อเนื่อง					
4.4 มีการบังคับใช้มาตรการ Zero Trust เพื่อควบคุมสิทธิ์การเข้าถึงข้อมูลและทรัพยากรภายในองค์กร					
5. ความทนทานและการฟื้นฟู (Resilience & Recovery)					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
5.1 ระบบได้รับการออกแบบให้สามารถดำเนินงานต่อได้แม้บางส่วนได้รับความเสียหาย					
5.2 มีการทดสอบแผนกู้คืนระบบหลังภัยพิบัติอย่างสม่ำเสมอ					
5.3 มีการจัดเก็บข้อมูลสำรองในพื้นที่แยกหรือระบบคลาวด์ เพื่อป้องกันการสูญหายจาก Ransomware					
5.4 มีมาตรการในการฟื้นฟูระบบและบริการให้กลับมาทำงานได้อย่างรวดเร็วหลังเหตุการณ์โจมตี					
6. ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์)Collaboration & Cybersecurity Awareness)					
6.1 มีทีมปฏิบัติการด้านความมั่นคงปลอดภัยหรือใช้บริการภายนอกในการเฝ้าระวังระบบอย่างมีประสิทธิภาพ					
6.2 มีการแลกเปลี่ยนและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอกอย่างต่อเนื่อง					
6.3 มีการจัดฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรเป็นประจำ					
6.4 องค์กรปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยสากล					
การจัดการองค์กรดิจิทัล (Digital Enterprise Management)					
1. กลยุทธ์ดิจิทัล (Digital Strategy)					
1.1 มีการกำหนดและสื่อสารกลยุทธ์ดิจิทัลไปยังทุกหน่วยงานในองค์กรอย่างชัดเจน					
1.2 มีกระบวนการวัดผลความสำเร็จของกลยุทธ์ผ่านตัวชี้วัดที่เชื่อมโยงกับพันธกิจองค์กร					
1.3 มีคณะกรรมการกำกับดูแลดิจิทัล (Digital Governance Committee)					
1.4 มีการจัดสรรคงบประมาณและประเมินผลตอบแทนการลงทุนของโครงการ AI และโครงสร้างพื้นฐานดิจิทัลอย่างเป็นระบบ					
2. โครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure)					
2.1 มีการลงทุนในโครงสร้างพื้นฐานเทคโนโลยีเพื่อรองรับการเติบโตในระยะ 3–5 ปีข้างหน้า					
2.2 มีแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อให้ระบบ AI ทำงานต่อได้ในภาวะวิกฤต					
2.3 มีระบบสำรองข้อมูลและศูนย์ข้อมูลสำรอง (Disaster Recovery Site) เพื่อป้องกันการสูญเสียข้อมูล					
2.4 มีการปรับปรุงและอัปเกรดเทคโนโลยีให้สอดคล้องกับนวัตกรรมดิจิทัลสมัยใหม่อย่างต่อเนื่อง					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
3. การจัดการข้อมูล (Data Management)					
3.1 มีการบริหารจัดการข้อมูลให้เป็นสินทรัพย์หลักขององค์กร					
3.2 มีการพัฒนาและบำรุงรักษาคลังข้อมูลเพื่อรองรับการทำงานของปัญญาประดิษฐ์					
3.3 ใช้เทคโนโลยีดิจิทัลเพิ่มประสิทธิภาพการทำงานร่วมกันระหว่างหน่วยงาน					
3.4 มีมาตรการควบคุมคุณภาพและความถูกต้องของข้อมูล (Data Quality & Integrity) เพื่อการตัดสินใจที่แม่นยำ					
4. กระบวนการอัตโนมัติ (Process Automation)					
4.1 มีการใช้ระบบอัตโนมัติในกระบวนการภายในเพื่อลดภาระงานบริหาร					
4.2 มีการประเมินและปรับปรุงประสบการณ์ดิจิทัลของนักศึกษาและบุคลากรอย่างต่อเนื่อง					
4.3 มีการบูรณาการระบบอัตโนมัติเข้ากับระบบสารสนเทศหลักขององค์กร					
4.4 มีการติดตามผลลัพธ์จากการปรับใช้กระบวนการอัตโนมัติเพื่อเพิ่มประสิทธิภาพการดำเนินงาน					
5. ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)					
5.1 มีการรวมความปลอดภัยตั้งแต่ต้นทางของทุกโครงการดิจิทัล					
5.2 มีการสื่อสารความเสี่ยงไซเบอร์ต่อผู้บริหารในรูปผลกระทบทางธุรกิจ					
5.3 มีการประเมินช่องโหว่และทดสอบการเจาะระบบ (Vulnerability Assessment & Penetration Test) อย่างต่อเนื่อง					
5.4 มีการจัดทำรายงานสถานะความปลอดภัยไซเบอร์และแผนการปรับปรุงอย่างเป็นระบบ					
6. นวัตกรรมและความคล่องตัว (Innovation and Agility)					
6.1 ส่งเสริมวัฒนธรรมนวัตกรรมให้บุคลากรทดลองและเรียนรู้เทคโนโลยีใหม่ ๆ					
6.2 มีการจัดตั้งห้องปฏิบัติการนวัตกรรมหรือกลไกนำร่องเพื่อพัฒนาโซลูชันใหม่					
6.3 มีความคล่องตัวในการปรับเปลี่ยนหรือปรับขนาดโครงการดิจิทัลให้สอดคล้องกับการเปลี่ยนแปลงของตลาด					
6.4 ใช้แนวทางการพัฒนาแบบ Agile/Scrum เพื่อเพิ่มความเร็วและความยืดหยุ่นในการดำเนินงาน					
ด้านสถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (Artificial Intelligence Enterprise Architecture)					
1. การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์ (EA–AI Integration)					
1.1 มีการบูรณาการการใช้ปัญญาประดิษฐ์เข้ากับสถาปัตยกรรมองค์กรอย่างเป็นระบบ					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
1.2 โครงสร้างสถาปัตยกรรมองค์กรของสถาบันสนับสนุนการนำปัญญาประดิษฐ์ไปใช้ในกระบวนการหลักได้อย่างเหมาะสม					
1.3 การพัฒนาปัญญาประดิษฐ์ของสถาบันสอดคล้องกับแผนสถาปัตยกรรมองค์กรในภาพรวม					
1.4 การบูรณาการสถาปัตยกรรมองค์กร และปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพและความยืดหยุ่นในการดำเนินงานของสถาบัน					
2. กรอบการทำงานเชิงสถาปัตยกรรม (Architectural Framework)					
2.1 มีกรอบการทำงานเชิงสถาปัตยกรรมที่ชัดเจนสำหรับการพัฒนาและใช้งานปัญญาประดิษฐ์					
2.2 สามารถกำหนดทิศทางและมาตรฐานของระบบปัญญาประดิษฐ์ได้อย่างเหมาะสม					
2.3 ช่วยลดความซ้ำซ้อนและความซับซ้อนของระบบสารสนเทศ					
2.4 สามารถปรับปรุงและพัฒนาให้สอดคล้องกับเทคโนโลยีปัญญาประดิษฐ์ที่เปลี่ยนแปลงได้					
3.การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ (AI-driven Information System Design & Development)					
3.1 ระบบสารสนเทศของสถาบันถูกออกแบบให้ใช้ปัญญาประดิษฐ์ เพื่อเพิ่มประสิทธิภาพการทำงาน					
3.2 การพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ช่วยสนับสนุนการตัดสินใจของผู้บริหารและผู้ปฏิบัติงาน					
3.3 ระบบปัญญาประดิษฐ์สามารถเชื่อมโยงและทำงานร่วมกับระบบสารสนเทศเดิมได้อย่างราบรื่น					
3.4 การออกแบบระบบสารสนเทศด้วยปัญญาประดิษฐ์ ที่คำนึงถึงความปลอดภัยและความน่าเชื่อถือของข้อมูล					
4.การจัดการทรัพยากรอย่างชาญฉลาด (Intelligent Resource Management)					
4.1 ใช้ปัญญาประดิษฐ์ในการบริหารจัดการทรัพยากรด้านเทคโนโลยีอย่างมีประสิทธิภาพ					
4.2 ระบบปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพในการใช้ทรัพยากรบุคคลและงบประมาณของสถาบัน					
4.3 การจัดการทรัพยากรด้วยปัญญาประดิษฐ์ช่วยลดต้นทุนและเพิ่มความคุ้มค่าในการดำเนินงาน					
4.4 สามารถติดตามและประเมินการใช้ทรัพยากรผ่านระบบอัจฉริยะได้อย่างเหมาะสม					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
5.ความสามารถในการปรับตัวต่อการเปลี่ยนแปลง (Adaptability & Agility)					
5.1 สามารถปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยีได้รวดเร็ว					
5.2 ระบบปัญญาประดิษฐ์สนับสนุนการปรับปรุงกระบวนการทำงานให้มีความคล่องตัวมากขึ้น					
5.3 สามารถปรับเปลี่ยนหรือขยายระบบปัญญาประดิษฐ์ได้ตามความต้องการในอนาคต					
5.4 ตอบสนองต่อการเปลี่ยนแปลงด้านนโยบายและสภาพแวดล้อมได้อย่างมีประสิทธิภาพ					
6.ความสามารถในการรับมือภัยคุกคามและความเสี่ยง (Threat & Risk Responsiveness)					
6.1 สนับสนุนการตรวจจับภัยคุกคามทางดิจิทัลได้อย่างรวดเร็ว					
6.2 ระบบปัญญาประดิษฐ์มีบทบาทในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ					
6.3 สามารถตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ					
6.4 การใช้ปัญญาประดิษฐ์ช่วยเพิ่มความสามารถในการป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์					
7. จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์ (AI Ethics and Responsibility)					
7.1 มีการกำหนดหลักจริยธรรมในการพัฒนาและใช้ปัญญาประดิษฐ์อย่างชัดเจน					
7.2 มีระบบปัญญาประดิษฐ์ถูกออกแบบให้โปร่งใสและสามารถอธิบายผลลัพธ์ได้					
7.3 มีมาตรการลดอคติในข้อมูลและโมเดลปัญญาประดิษฐ์					
7.4 มีการอบรมและส่งเสริมความรู้เรื่องจริยธรรมและความรับผิดชอบในการใช้ปัญญาประดิษฐ์					
ด้านการจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)					
1. การตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Detection)					
1.1 มีการทดสอบเจาะระบบ และตรวจสอบโค้ดของแอปพลิเคชันเพื่อค้นหาช่องโหว่อย่างสม่ำเสมอ					
1.2 มีการประเมินประสิทธิภาพของมาตรการป้องกันภัยไซเบอร์อย่างต่อเนื่องเพื่อลดความเสี่ยง					
1.3 ใช้เทคโนโลยี AI หรือ Machine Learning ในการตรวจจับพฤติกรรมที่ผิดปกติในระบบเครือข่าย					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
1.4 มีระบบแจ้งเตือนภัยคุกคามแบบเรียลไทม์ เพื่อให้ทีมสามารถตอบสนองได้อย่างรวดเร็ว					
2. การตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response)					
2.1 มีแผนขั้นตอนการตอบสนองเหตุการณ์ทางไซเบอร์ที่ครอบคลุมทุกระบบ					
2.2 มีแนวทางเฉพาะในการจัดการเหตุการณ์ที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์					
2.3 มีการกำหนดบทบาทและความรับผิดชอบของทีม IR (Incident Response Team) อย่างชัดเจน					
2.4 มีการทดสอบจำลองเหตุการณ์โจมตี (Cyber Drill) เพื่อประเมินความพร้อมของบุคลากรและระบบ					
3. การประเมินและจัดการความเสี่ยง (Risk Assessment and Management)					
3.1 มีการประเมินและจัดการความเสี่ยงทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง					
3.2 มีระบบบริหารจัดการการเปลี่ยนแปลงของ IT และ AI อย่างเป็นระบบ					
3.3 มีการบริหารจัดการแพตช์ (Patch Management) และอัปเดตซอฟต์แวร์อย่างรวดเร็วและมีประสิทธิภาพ					
3.4 มีการจัดทำรายงานความเสี่ยงและความปลอดภัยทางไซเบอร์ที่ชัดเจนสำหรับผู้บริหาร					
4. การปกป้องข้อมูลและความเป็นส่วนตัว (Data Protection and Privacy)					
4.1 มีนโยบายและมาตรการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย PDPA					
4.2 มีการเข้ารหัสและควบคุมการเข้าถึงข้อมูลเพื่อป้องกันการรั่วไหลหรือการโจมตี					
4.3 มีการบริหารจัดการความเสี่ยงของข้อมูลที่ใช้โดยระบบปัญญาประดิษฐ์อย่างเป็นระบบ					
4.4 มีการตรวจสอบและประเมินการจัดการข้อมูลอย่างสม่ำเสมอเพื่อรักษาความเป็นส่วนตัวของผู้ใช้					
5. การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย (Security Awareness Training)					
5.1 มีการจัดฝึกอบรมภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับสถาบันอุดมศึกษาอย่างสม่ำเสมอ					
5.2 บุคลากรได้รับการอบรมและอัปเดตความรู้ด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง					
5.3 มีการจัดกิจกรรมหรือการรณรงค์สร้างจิตสำนึกด้านความปลอดภัยดิจิทัลภายในองค์กร					

รายการประเมิน	ระดับความคิดเห็น				
	5	4	3	2	1
5.4 มีระบบประเมินผลหลังการฝึกอบรมเพื่อวัดผลการเรียนรู้และการนำไปใช้จริงของผู้เข้าร่วม					
6. นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ (Security Policy and Compliance)					
6.1 มีนโยบายและข้อบังคับด้านความปลอดภัยสำหรับ AI และ Cloud					
6.2 ผู้บริหารมีการทบทวนและประเมินสถานะความปลอดภัยของระบบอย่างสม่ำเสมอ					
6.3 จัดทำสัญญากับผู้ให้บริการภายนอก พร้อมข้อกำหนดด้านความปลอดภัย					
6.4 ใช้เครื่องมืออัตโนมัติในการตรวจสอบและบังคับใช้ข้อกำหนดด้านความปลอดภัย					
7. ความมั่นคงปลอดภัยของเครือข่าย (Network Security)					
7.1 มีมาตรการความปลอดภัยเครือข่ายเข้มงวดโดยเฉพาะ IoT และอุปกรณ์นักศึกษา					
7.2 มีการกำหนดสิทธิ์การเข้าถึงตามหลัก “Least Privilege” อย่างชัดเจน					
7.3 ระบบเครือข่ายได้รับการตรวจสอบและอัปเดตการป้องกันภัยอย่างต่อเนื่อง					
7.4 มีการใช้ไฟร์วอลล์ ระบบ IDS/IPS และระบบตรวจสอบการจราจรเครือข่ายเพื่อป้องกันภัยคุกคาม					
8. โซลูชันความมั่นคงปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI-driven Security Solutions)					
8.1 ใช้โซลูชัน AI เพื่อช่วยตรวจจับและตอบสนองต่อภัยคุกคามโดยอัตโนมัติ					
8.2 ระบบ AI ถูกฝึกด้วยข้อมูลภัยคุกคามจริงเพื่อเพิ่มความแม่นยำในการวิเคราะห์					
8.3 มีการประเมินและปรับปรุงโมเดล AI ด้านความปลอดภัยอย่างต่อเนื่อง					
8.4 มีการผสานระบบ AI Security เข้ากับระบบปฏิบัติการด้านความปลอดภัยขององค์กรอย่างเป็นเอกภาพ					
9. ความปลอดภัยบนคลาวด์ (Cloud Security)					
9.1 มีมาตรการจัดการการตั้งค่าที่ผิดพลาด (Misconfiguration) ในระบบคลาวด์อย่างเข้มงวด					
9.2 มีการควบคุมสิทธิ์การเข้าถึงข้อมูลบนคลาวด์ตามระดับผู้ใช้งานอย่างเหมาะสม					
9.3 มีการเข้ารหัสและตรวจสอบการรับส่งข้อมูลระหว่างคลาวด์และระบบภายใน					
9.4 มีการสำรองข้อมูลและแผนฟื้นฟูข้อมูลบนคลาวด์เพื่อรองรับเหตุการณ์ไม่คาดคิด					

ตอนที่ 3 ข้อคิดเห็นและข้อเสนอแนะที่มีต่อปัจจัยที่มีอิทธิพลต่อสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

คำชี้แจงโปรดแสดงความคิดเห็นและข้อเสนอแนะของท่านเพิ่มเติม (ถ้ามี)

.....

.....

.....

.....

ขอขอบพระคุณเป็นอย่างสูงที่ท่านให้ความอนุเคราะห์สละเวลาตอบแบบสอบถาม





แบบประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์
เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ชื่องานวิจัย สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

อาจารย์ที่ปรึกษา ศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข
ศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ

ผู้วิจัย นางสาวเนาวรัตน์ ปิ่นอำนาจ
นักศึกษาปริญญาเอก สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินความเหมาะสมของสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โดยท่านสามารถพิจารณารายละเอียดตามเอกสารที่ส่งมาด้วยนี้

แบบประเมินแบ่งออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลผู้ประเมิน

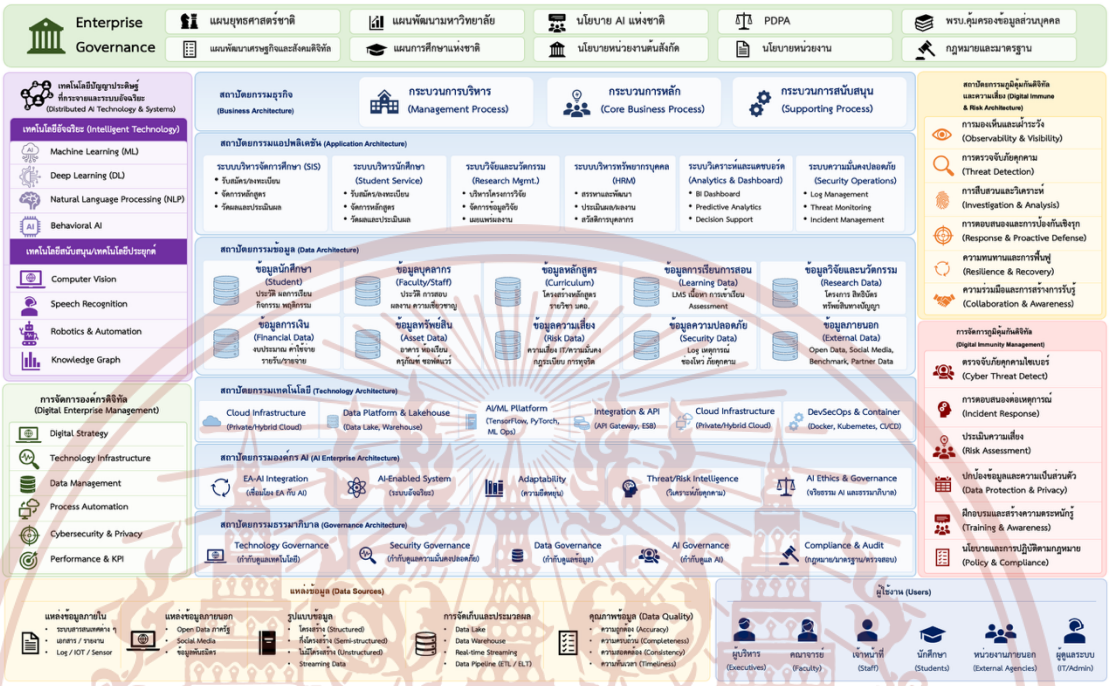
ตอนที่ 2 แบบประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

ตอนที่ 3 ข้อคิดเห็นและข้อเสนอแนะอื่นๆ

นางสาวเนาวรัตน์ ปิ่นอำนาจ
ผู้วิจัย

ติดต่อผู้วิจัย
โทรศัพท์ 081 886 8474 LINE ID: nawaratpin
อีเมล s6602052910038@email.kmutnb.ac.th

สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา
AI Enterprise Architecture for Digital Immunity Management in Higher Education Institutions



ตอนที่ 1 ข้อมูลผู้ประเมิน

ชื่อผู้ประเมิน:.....

ตำแหน่ง:.....

สถานที่ทำงาน:.....

เบอร์โทรศัพท์/email:.....

ตอนที่ 2 แบบประเมินสถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณา ดังนี้

5 หมายถึง	มีเหมาะสมมากที่สุด
4 หมายถึง	มีเหมาะสมมาก
3 หมายถึง	มีเหมาะสมปานกลาง
2 หมายถึง	มีเหมาะสมน้อย
1 หมายถึง	มีเหมาะสมน้อยที่สุด

รายการประเมิน	ระดับความเหมาะสม					หมายเหตุ
	5	4	3	2	1	
1. ธรรมาภิบาลองค์กร (Enterprise Governance)						
1.1 ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561–2580)						
1.2 ยุทธศาสตร์หลักระยะยาว 20 ปี ของประเทศไทย (พ.ศ. 2561–2580)						
1.3 แผนการศึกษาแห่งชาติ พ.ศ. 2560–2579						
1.4 แผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (พ.ศ. 2565–2570)						
1.5 วิสัยทัศน์ พันธกิจ เป้าหมาย กลยุทธ์						
1.6 กฎหมายเพื่อความมั่นคงปลอดภัยข้อมูล						
1.7 นโยบายการรักษาความมั่นคงปลอดภัยข้อมูล						
1.8 ข้อกำหนดและแนวปฏิบัติเพื่อความมั่นคงปลอดภัยข้อมูล						
1.9 มาตรฐานเพื่อความมั่นคงปลอดภัยข้อมูล						
2. สถาปัตยกรรมธุรกิจ (Business Architecture)						
2.1 กระบวนการบริหาร (Management Process)						
2.2 กระบวนการหลัก (Core Business Process)						
2.3 กระบวนการสนับสนุน (Supporting Process)						
3. สถาปัตยกรรมแอปพลิเคชัน (Application Architecture)						
3.1 ระบบบริหารจัดการการศึกษา (SIS)						
3.2 ระบบบริการนักศึกษา (Student Service)						
3.3 ระบบวิจัยและนวัตกรรม (Research Management)						
3.4 ระบบบริหารทรัพยากรบุคคล (HRM)						
3.5 ระบบวิเคราะห์และแดชบอร์ด (Analytics & Dashboard)						
3.6 ระบบความมั่นคงปลอดภัย (Security Operations)						
4. สถาปัตยกรรมข้อมูล (Data Architecture)						
4.1 ข้อมูลนักศึกษา (Student Data)						
4.2 ข้อมูลบุคลากร (Faculty/Staff Data)						
4.3 ข้อมูลหลักสูตร (Curriculum Data)						
4.4 ข้อมูลการเรียนการสอน (Learning Data)						
4.5 ข้อมูลวิจัยและนวัตกรรม (Research Data)						
4.6 ข้อมูลการเงิน (Financial Data)						

รายการประเมิน	ระดับความเหมาะสม					หมายเหตุ
	5	4	3	2	1	
4.7 ข้อมูลทรัพย์สิน (Asset Data)						
4.8 ข้อมูลความเสี่ยง (Risk Data)						
4.9 ข้อมูลความปลอดภัย (Security Data)						
4.10 ข้อมูลภายนอก (External Data)						
5. สถาปัตยกรรมเทคโนโลยี (Technology Architecture)						
5.1 โครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure)						
5.2 แพลตฟอร์มข้อมูลและ Data Lakehouse						
5.3 แพลตฟอร์มปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง (AI/ML Platform)						
5.4 Integration & API						
5.5 Network & Edge Computing						
5.6 DevSecOps & Container						
6. สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (AI Enterprise Architecture)						
6.1 EA–AI Integration						
6.2 Architectural Framework						
6.3 AI-Enabled System						
6.4 Adaptability						
6.5 Threat/Risk Intelligence						
6.6 AI Ethics & Governance						
7. สถาปัตยกรรมธรรมาภิบาล (Governance Architecture)						
7.1 Technology Governance						
7.2 Security Governance						
7.3 Data Governance						
7.4 AI Governance						
7.5 Compliance & Audit						
8. เทคโนโลยีปัญญาประดิษฐ์ และระบบอัจฉริยะ (Intelligent Technology)						
8.1 Machine Learning (ML)						
8.2 Deep Learning (DL)						
8.3 Natural Language Processing (NLP)						
8.4 Behavioral AI						
8.5 Computer Vision						

รายการประเมิน	ระดับความเหมาะสม					หมายเหตุ
	5	4	3	2	1	
8.6 Speech Recognition						
8.7 Robotics & Automation						
8.9 Knowledge Graph						
9. การจัดการองค์กรดิจิทัล (Digital Enterprise Management)						
9.1 กลยุทธ์ดิจิทัล						
9.2 โครงสร้างพื้นฐานเทคโนโลยี						
9.3 การจัดการข้อมูล						
9.4 การทำให้กระบวนการเป็นอัตโนมัติ						
9.5 ความมั่นคงปลอดภัยและความเป็นส่วนตัว						
9.6 การวัดผลและตัวชี้วัด						
10. สถาปัตยกรรมภูมิคุ้มกันดิจิทัลและความเสี่ยง (Digital Immunity & Risk Architecture)						
10.1 การมองเห็นและเฝ้าระวัง						
10.2 การตรวจจับภัยคุกคาม						
10.3 การสืบสวนและวิเคราะห์						
10.4 การตอบสนองและการป้องกันเชิงรุก						
10.5 ความทนทานและการฟื้นฟู						
10.6 ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์						
11.การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)						
11.1 การตรวจจับภัยคุกคามทางไซเบอร์						
11.2 การตอบสนองต่อเหตุการณ์ทางไซเบอร์						
11.3 การประเมินและจัดการความเสี่ยง						
11.4 การปกป้องข้อมูลและความเป็นส่วนตัว						
11.5 การฝึกอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัย						
11.6 นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ						
12. แหล่งข้อมูล (Data Sources)						
12.1 แหล่งข้อมูลภายใน						
12.2 แหล่งข้อมูลภายนอก						
12.3 รูปแบบข้อมูล						

รายการประเมิน	ระดับความเหมาะสม					หมายเหตุ
	5	4	3	2	1	
12.4 การจัดเก็บและประมวลผล						
12.5 คุณภาพข้อมูล						
13. ผู้ใช้งาน (Users)						
13.1 ผู้บริหาร (Executives)						
13.2 คณาจารย์ (Faculty)						
13.3 เจ้าหน้าที่ (Staff)						
13.4 นักศึกษา (Students)						
13.5 หน่วยงานภายนอก (External Agencies)						
13.6 ผู้ดูแลระบบ (IT/Admin)						

ตอนที่ 3 ข้อคิดเห็นและข้อเสนอแนะอื่นๆ

.....

.....

.....

.....

ขอขอบพระคุณเป็นอย่างสูงที่ท่านให้ความอนุเคราะห์สละเวลาตอบแบบประเมิน

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ตารางที่ ค-1 ตัวย่อและความหมายตัวแปรงานวิจัย

ตัวย่อ	ความหมาย
EAC	โครงสร้างองค์กร (Organizational Structure)
BA	สถาปัตยกรรมธุรกิจ
BA1	กำหนดวิสัยทัศน์และกลยุทธ์ด้านปัญญาประดิษฐ์ที่สอดคล้องกับพันธกิจ
BA2	บูรณาการการใช้ปัญญาประดิษฐ์เข้ากับกระบวนการหลัก
BA3	ประเมินความพร้อมและศักยภาพของหน่วยงานในการใช้เทคโนโลยีปัญญาประดิษฐ์อย่างต่อเนื่อง
BA4	ผู้บริหารระดับสูงสนับสนุนและส่งเสริมการใช้เทคโนโลยีปัญญาประดิษฐ์
DA	สถาปัตยกรรมข้อมูล
DA1	กลยุทธ์ข้อมูลที่สนับสนุนการใช้งานปัญญาประดิษฐ์อย่างชัดเจน
DA2	มาตรการควบคุมคุณภาพและความมั่นคงปลอดภัยของข้อมูลอย่างเป็นระบบ
DA3	โครงสร้างข้อมูลรองรับการจัดเก็บและประมวลผล Big Data และข้อมูลแบบ Unstructured
DA4	ระบบติดป้ายกำกับและจัดการข้อมูลเพื่อสนับสนุนการเรียนรู้ของโมเดลปัญญาประดิษฐ์
AA	สถาปัตยกรรมระบบแอปพลิเคชัน
AA1	การพัฒนาแอปพลิเคชันหรือระบบสารสนเทศที่เชื่อมโยงกับปัญญาประดิษฐ์
AA2	ระบบแอปพลิเคชันได้รับการออกแบบให้สามารถปรับขนาดและเชื่อมต่อได้ง่าย
AA3	มาตรฐานกลางในการพัฒนาและบูรณาการแอปพลิเคชัน
AA4	การปรับปรุงระบบงานอย่างต่อเนื่องเพื่อรองรับเทคโนโลยีปัญญาประดิษฐ์ใหม่ๆ
TA	สถาปัตยกรรมเทคโนโลยี
TA1	โครงสร้างพื้นฐานด้านเทคโนโลยีที่รองรับการประมวลผลของปัญญาประดิษฐ์
TA2	ใช้แพลตฟอร์มคลาวด์ในการพัฒนาปัญญาประดิษฐ์
TA3	แผนการบำรุงรักษาและอัปเดตเทคโนโลยีอย่างต่อเนื่อง
TA4	การนำเทคโนโลยี Edge AI หรือระบบประมวลผลแบบกระจายมาใช้เพื่อเพิ่มประสิทธิภาพ
SA	สถาปัตยกรรมด้านความปลอดภัย
SA1	กลยุทธ์และนโยบายความปลอดภัยทางไซเบอร์ที่ชัดเจน
SA2	การประเมินและป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์

ตัวย่อ	ความหมาย
SA3	การเข้ารหัสและจำกัดสิทธิ์การเข้าถึงข้อมูลอย่างเหมาะสม
SA4	แผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลและระบบปัญญาประดิษฐ์
IA	สถาปัตยกรรมการบูรณาการ
IA1	สถาปัตยกรรมเชื่อมต่อโมเดลปัญญาประดิษฐ์กับระบบหลักขององค์กร
IA2	มาตรฐานหรือ API กลางสำหรับการแลกเปลี่ยนข้อมูลระหว่างระบบ
IA3	การตรวจสอบและทดสอบการเชื่อมต่อระหว่างระบบอย่างสม่ำเสมอ
IA4	ระบบบูรณาการมีความยืดหยุ่นรองรับการเปลี่ยนแปลงของเทคโนโลยี
GA	สถาปัตยกรรมการกำกับดูแล
GA1	กรอบการกำกับดูแลด้านปัญญาประดิษฐ์ที่ชัดเจน
GA2	การติดตามและประเมินผลการใช้ปัญญาประดิษฐ์อย่างต่อเนื่อง
GA3	การกำหนดบทบาทและความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับปัญญาประดิษฐ์
GA4	กำหนดตัวชี้วัดความสำเร็จของโครงการปัญญาประดิษฐ์สอดคล้องกับเป้าหมายองค์กร
AIT	ด้านเทคโนโลยีอัจฉริยะ (Intelligent Technology)
ML	การเรียนรู้ของเครื่อง
ML1	การนำเทคโนโลยีการเรียนรู้ของเครื่องมาใช้ในการวิเคราะห์ข้อมูล
ML2	สนับสนุนการตัดสินใจของผู้บริหารและบุคลากร
ML3	การปรับปรุงและพัฒนาโมเดลอย่างต่อเนื่องตามข้อมูลใหม่
ML4	ความแม่นยำและเชื่อถือได้
DL	การเรียนรู้เชิงลึก
DL1	การประยุกต์ใช้การเรียนรู้เชิงลึกกับข้อมูลขนาดใหญ่หรือข้อมูลซับซ้อน
DL2	เพิ่มประสิทธิภาพในการคาดการณ์หรือจำแนกข้อมูล
DL3	โครงสร้างพื้นฐานรองรับการประมวลผลของโมเดลเชิงลึกได้อย่างเหมาะสม
DL4	การประเมินประสิทธิภาพของโมเดลการเรียนรู้เชิงลึกอย่างสม่ำเสมอ
NL	การประมวลผลภาษาธรรมชาติ
NL1	การวิเคราะห์ข้อมูลข้อความหรือภาษา
NL2	เพิ่มประสิทธิภาพในการให้บริการหรือการสื่อสารกับผู้ใช้
NL3	ความถูกต้องและสอดคล้องกับบริบทของสถาบัน
NL4	การพัฒนาและปรับปรุงระบบ NLP อย่างต่อเนื่อง
BI	ความรู้เชิงพฤติกรรม
BI1	การใช้ปัญญาประดิษฐ์ในการวิเคราะห์พฤติกรรมของผู้ใช้หรือผู้เรียน

ตัวย่อ	ความหมาย
BI2	สนับสนุนการวางแผนและปรับปรุงบริการ
BI3	ระบบสามารถเรียนรู้และปรับตัวตามพฤติกรรมที่เปลี่ยนแปลงได้
BI4	การคำนึงถึงจริยธรรมและความเป็นส่วนตัวของผู้ใช้
DIS	ด้านระบบภูมิคุ้มกันดิจิทัล (Digital Immunity)
OV	การมองเห็นและเฝ้าระวัง
OV1	ติดตั้งเครื่องมือสำหรับการมองเห็นและเฝ้าระวังที่ครอบคลุมเครือข่ายแอปพลิเคชันและโครงสร้างพื้นฐาน
OV2	มาตรการสร้างความโปร่งใสและตรวจสอบการทำงานของระบบปัญญาประดิษฐ์
OV3	การเข้ารหัสข้อมูลทั้งขณะส่งและจัดเก็บ
OV4	แสดงภาพรวมสถานะการทำงานและแจ้งเตือนเหตุการณ์ผิดปกติได้แบบเรียลไทม์
TD	การตรวจจับภัยคุกคาม
TD1	ระบบสามารถตรวจจับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ
TD2	การใช้เทคโนโลยีปัญญาประดิษฐ์วิเคราะห์ Log และ Traffic เพื่อระบุพฤติกรรมที่ผิดปกติ
TD3	การจำลองและทดสอบสถานการณ์โจมตีทางไซเบอร์เพื่อประเมินความแข็งแกร่งของระบบอย่างสม่ำเสมอ
TD4	การตรวจสอบช่องโหว่ของระบบแอปพลิเคชัน และโครงสร้างพื้นฐานเป็นประจำ
AN	การสืบสวนและวิเคราะห์
AN1	สนับสนุนการรวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่งได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
AN2	ผู้เชี่ยวชาญวิเคราะห์เชิงลึกระบุแหล่งและขอบเขตความเสียหาย
AN3	การใช้เครื่องมือวิเคราะห์เหตุการณ์ เพื่อสืบหาต้นตอของภัยคุกคามอย่างเป็นระบบ
AN4	การวิเคราะห์ถูกนำมาใช้ปรับปรุงมาตรการความปลอดภัยและเพิ่มประสิทธิภาพการป้องกันในอนาคต
RP	การตอบสนองและการป้องกันเชิงรุก
RP1	แผนตอบสนองเหตุการณ์ไซเบอร์ที่ชัดเจนและเป็นปัจจุบัน
RP2	ตอบสนองและป้องกันภัยคุกคามเชิงรุกได้โดยอัตโนมัติ
RP3	การดำเนินกิจกรรม Threat Hunting เพื่อตรวจหาภัยคุกคามที่อาจแฝงอยู่ในระบบอย่างต่อเนื่อง

ตัวย่อ	ความหมาย
RP4	การบังคับใช้มาตรการ Zero Trust เพื่อควบคุมสิทธิ์การเข้าถึงข้อมูลและทรัพยากรภายในองค์กร
RR	ความทนทานและการฟื้นฟู
RR1	การออกแบบให้สามารถดำเนินงานต่อได้แม้บางส่วนได้รับความเสียหาย
RR2	การทดสอบแผนกู้คืนระบบหลังภัยพิบัติอย่างสม่ำเสมอ
RR3	การจัดเก็บข้อมูลสำรองในพื้นที่แยกหรือระบบคลาวด์ เพื่อป้องกันการสูญหายจาก Ransomware
RR4	มาตรการในการฟื้นฟูระบบและบริการให้กลับมาทำงานได้อย่างรวดเร็วหลังเหตุการณ์โจมตี
CC	ความร่วมมือและการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยบนไซเบอร์
CC1	ทีมปฏิบัติการด้านความมั่นคงปลอดภัยหรือใช้บริการภายนอกในการเฝ้าระวังระบบอย่างมีประสิทธิภาพ
CC2	การแลกเปลี่ยนและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอกอย่างต่อเนื่อง
CC3	การจัดฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรเป็นประจำ
CC4	มาตรฐานความมั่นคงปลอดภัยสากล
DEM	การจัดการองค์กรดิจิทัล (Digital Enterprise Management)
DS	กลยุทธ์ดิจิทัล
OV1	การกำหนดและสื่อสารกลยุทธ์ดิจิทัลไปยังทุกหน่วยงานในองค์กรอย่างชัดเจน
OV2	กระบวนการวัดผลความสำเร็จของกลยุทธ์ผ่านตัวชี้วัดที่เชื่อมโยงกับพันธกิจองค์กร
OV3	คณะกรรมการกำกับดูแลดิจิทัล
OV4	การจัดสรรคงบประมาณและประเมินผลตอบแทนการลงทุนของโครงการ AI และโครงสร้างพื้นฐานดิจิทัลอย่างเป็นระบบ
TI	โครงสร้างพื้นฐานเทคโนโลยี
TI1	การลงทุนในโครงสร้างพื้นฐานเทคโนโลยีเพื่อรองรับการเติบโตในระยะ 3–5 ปีข้างหน้า
TI2	แผนบริหารความต่อเนื่องทางธุรกิจ เพื่อให้ระบบ AI ทำงานต่อได้ในภาวะวิกฤต
TI3	ระบบสำรองข้อมูลและศูนย์ข้อมูล เพื่อป้องกันการสูญเสียข้อมูล

ตัวย่อ	ความหมาย
TI4	การปรับปรุงและอัปเกรดเทคโนโลยีให้สอดคล้องกับนวัตกรรมดิจิทัลสมัยใหม่อย่างต่อเนื่อง
DM	การจัดการข้อมูล
DM1	การบริหารจัดการข้อมูลให้เป็นสินทรัพย์หลักขององค์กร
DM2	การพัฒนาและบำรุงรักษาคลังข้อมูลเพื่อรองรับการทำงานของปัญญาประดิษฐ์
DM3	ใช้เทคโนโลยีดิจิทัลเพิ่มประสิทธิภาพการทำงานร่วมกันระหว่างหน่วยงาน
DM4	มาตรการควบคุมคุณภาพและความถูกต้องของข้อมูล เพื่อการตัดสินใจที่แม่นยำ
PA	กระบวนการอัตโนมัติ
PA1	การใช้ระบบอัตโนมัติในกระบวนการภายในเพื่อลดภาระงานบริหาร
PA2	การประเมินและปรับปรุงประสบการณ์ดิจิทัลของนักศึกษาและบุคลากรอย่างต่อเนื่อง
PA3	การบูรณาการระบบอัตโนมัติเข้ากับระบบสารสนเทศหลักขององค์กร
PA4	การติดตามผลลัพธ์จากการปรับใช้กระบวนการอัตโนมัติเพื่อเพิ่มประสิทธิภาพการดำเนินงาน
CB	ความมั่นคงปลอดภัยทางไซเบอร์
CB1	การรวมความปลอดภัยตั้งแต่ต้นทางของทุกโครงการดิจิทัล
CB2	การสื่อสารความเสี่ยงไซเบอร์ต่อผู้บริหารในรูปผลกระทบทางธุรกิจ
CB3	การประเมินช่องโหว่และทดสอบการเจาะระบบอย่างต่อเนื่อง
CB4	การจัดทำรายงานสถานะความปลอดภัยไซเบอร์และแผนการปรับปรุงอย่างเป็นระบบ
AIA	สถาปัตยกรรมองค์กรปัญญาประดิษฐ์ (Artificial Intelligence Enterprise Architecture)
EI	การบูรณาการสถาปัตยกรรมองค์กรและปัญญาประดิษฐ์
EI1	การบูรณาการการใช้ปัญญาประดิษฐ์เข้ากับสถาปัตยกรรมองค์กรอย่างเป็นระบบ
EI2	โครงสร้างสถาปัตยกรรมองค์กรของสถาบันสนับสนุนการนำปัญญาประดิษฐ์ไปใช้ในกระบวนการหลักได้อย่างเหมาะสม
EI3	การพัฒนาปัญญาประดิษฐ์ของสถาบันสอดคล้องกับแผนสถาปัตยกรรมองค์กรในภาพรวม
EI4	การบูรณาการสถาปัตยกรรมองค์กร และปัญญาประดิษฐ์ช่วยเพิ่มประสิทธิภาพและความยืดหยุ่นในการดำเนินงานของสถาบัน
AF	กรอบการทำงานเชิงสถาปัตยกรรม

ตัวย่อ	ความหมาย
AF1	กรอบการทำงานเชิงสถาปัตยกรรมที่ชัดเจนสำหรับการพัฒนาและใช้งานปัญญาประดิษฐ์
AF2	สามารถกำหนดทิศทางและมาตรฐานของระบบปัญญาประดิษฐ์ได้อย่างเหมาะสม
AF3	ลดความซ้ำซ้อนและความซับซ้อนของระบบสารสนเทศ
AF4	สามารถปรับปรุงและพัฒนาให้สอดคล้องกับเทคโนโลยีปัญญาประดิษฐ์ที่เปลี่ยนแปลงได้
AS	การออกแบบและพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์
AS1	ระบบสารสนเทศของสถาบันถูกออกแบบให้ใช้ปัญญาประดิษฐ์ เพื่อเพิ่มประสิทธิภาพการทำงาน
AS2	การพัฒนาระบบสารสนเทศด้วยปัญญาประดิษฐ์ ช่วยสนับสนุนการตัดสินใจของผู้บริหารและผู้ปฏิบัติงาน
AS3	ระบบปัญญาประดิษฐ์สามารถเชื่อมโยงและทำงานร่วมกับระบบสารสนเทศเดิมได้อย่างราบรื่น
AS4	การออกแบบระบบสารสนเทศด้วยปัญญาประดิษฐ์ ที่คำนึงถึงความปลอดภัยและความน่าเชื่อถือของข้อมูล
AD	การปรับตัวต่อการเปลี่ยนแปลง
AD1	สามารถปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยีได้รวดเร็ว
AD2	ระบบปัญญาประดิษฐ์สนับสนุนการปรับปรุงกระบวนการทำงานให้มีความคล่องตัวมากขึ้น
AD3	สามารถปรับเปลี่ยนหรือขยายระบบปัญญาประดิษฐ์ได้ตามความต้องการในอนาคต
AD4	ตอบสนองต่อการเปลี่ยนแปลงด้านนโยบายและสภาพแวดล้อมได้อย่างมีประสิทธิภาพ
TR	การรับมือภัยคุกคามและความเสี่ยง
TR1	สนับสนุนการตรวจจับภัยคุกคามทางดิจิทัลได้อย่างรวดเร็ว
TR2	ระบบปัญญาประดิษฐ์มีบทบาทในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ
TR3	สามารถตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ
TR4	การใช้ปัญญาประดิษฐ์ช่วยเพิ่มความสามารถในการป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์
ER	จริยธรรมและความรับผิดชอบของปัญญาประดิษฐ์
ER1	การกำหนดหลักจริยธรรมในการพัฒนาและใช้ปัญญาประดิษฐ์อย่างชัดเจน

ตัวย่อ	ความหมาย
ER2	ระบบปัญญาประดิษฐ์ถูกออกแบบให้โปร่งใสและสามารถอธิบายผลลัพธ์ได้
ER3	มาตรการลดอคติในข้อมูลและโมเดลปัญญาประดิษฐ์
ER4	การอบรมและส่งเสริมความรู้เรื่องจริยธรรมและความรับผิดชอบในการใช้ปัญญาประดิษฐ์
DIM	การจัดการภูมิคุ้มกันดิจิทัล (Digital Immunity Management)
CD	การตรวจจับภัยคุกคามทางไซเบอร์
CD1	การทดสอบเจาะระบบ และตรวจสอบโค้ดของแอปพลิเคชันเพื่อค้นหาช่องโหว่อย่างสม่ำเสมอ
CD2	การประเมินประสิทธิภาพของมาตรการป้องกันภัยไซเบอร์อย่างต่อเนื่องเพื่อลดความเสี่ยง
CD3	ใช้เทคโนโลยี AI หรือ Machine Learning ในการตรวจจับพฤติกรรมที่ผิดปกติในระบบเครือข่าย
CD4	ระบบแจ้งเตือนภัยคุกคามแบบเรียลไทม์ เพื่อให้ทีมสามารถตอบสนองได้อย่างรวดเร็ว
IR	การตอบสนองต่อเหตุการณ์ทางไซเบอร์
IR1	แผนขั้นตอนการตอบสนองเหตุการณ์ทางไซเบอร์ที่ครอบคลุมทุกระบบ
IR2	แนวทางเฉพาะในการจัดการเหตุการณ์ที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์
IR3	การกำหนดบทบาทและความรับผิดชอบของทีม IR อย่างชัดเจน
IR4	การทดสอบจำลองเหตุการณ์โจมตีเพื่อประเมินความพร้อมของบุคลากรและระบบ
RA	การประเมินและจัดการความเสี่ยง
RA1	การประเมินและจัดการความเสี่ยงทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง
RA2	ระบบบริหารจัดการการเปลี่ยนแปลงของ IT และ AI อย่างเป็นระบบ
RA3	การบริหารจัดการแพตช์ (Patch Management) และอัปเดตซอฟต์แวร์อย่างรวดเร็วและมีประสิทธิภาพ
RA4	การจัดทำรายงานความเสี่ยงและความปลอดภัยทางไซเบอร์ที่ชัดเจนสำหรับผู้บริหาร
DP	การปกป้องข้อมูลและความเป็นส่วนตัว
DP1	นโยบายและมาตรการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย PDPA
DP2	การเข้ารหัสและควบคุมการเข้าถึงข้อมูลเพื่อป้องกันการรั่วไหลหรือการโจมตี
DP3	การบริหารจัดการความเสี่ยงของข้อมูลที่ใช้โดยระบบปัญญาประดิษฐ์อย่างเป็นระบบ
DP4	การตรวจสอบและประเมินการจัดการข้อมูลอย่างสม่ำเสมอเพื่อรักษาความเป็นส่วนตัวของผู้ใช้

ตัวย่อ	ความหมาย
ST	การฝึกอบรมการรับรู้ด้านความมั่นคงปลอดภัย
ST1	การจัดฝึกอบรมภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับสถาบันอุดมศึกษาอย่างสม่ำเสมอ
ST2	บุคลากรได้รับการอบรมและอัปเดตความรู้ด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง
ST3	การจัดกิจกรรมหรือการรณรงค์สร้างจิตสำนึกด้านความปลอดภัยดิจิทัลภายในองค์กร
ST4	ระบบประเมินผลหลังการฝึกอบรมเพื่อวัดผลการเรียนรู้และการนำไปใช้จริงของผู้เข้าร่วม
SC	นโยบายความมั่นคงปลอดภัยและการปฏิบัติตามกฎระเบียบ
SC1	นโยบายและข้อบังคับด้านความปลอดภัยสำหรับ AI และ Cloud
SC2	ผู้บริหารมีการทบทวนและประเมินสถานะความปลอดภัยของระบบอย่างสม่ำเสมอ
SC3	จัดทำสัญญากับผู้ให้บริการภายนอก พร้อมข้อกำหนดด้านความปลอดภัย
SC4	ใช้เครื่องมืออัตโนมัติในการตรวจสอบและบังคับใช้ข้อกำหนดด้านความปลอดภัย

ตารางที่ ค-2 สัญลักษณ์ที่ใช้ในการวิเคราะห์ข้อมูล

สัญลักษณ์	ความหมาย
n	จำนวนผู้ตอบแบบสอบถามที่เป็นกลุ่มตัวอย่าง
$\bar{x}$	ค่าเฉลี่ย (Mean)
S.D.	ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation)
C.V.	ค่าสัมประสิทธิ์การกระจาย (Coefficient of Variation)
r	ค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สัน (Pearson's Product Moment Correlation Coefficient)
χ^2	ค่าสถิติไค-สแควร์ (Chi-Square)
λ	น้ำหนักองค์ประกอบ (Factor Loading)
e	ค่าความคลาดเคลื่อนมาตรฐาน (Error) ของตัวบ่งชี้หรือตัวแปรสังเกต
Sig.	ค่าความน่าจะเป็นสำหรับบอกนัยสำคัญทางสถิติ (Significance)
df	ค่าองศาอิสระ (Degrees of Freedom)
R^2	ค่าสัมประสิทธิ์การตัดสินใจ (Coefficient of Determination)
β	ค่าสัมประสิทธิ์อิทธิพลในรูปคะแนนมาตรฐาน (Standardized Regression Coefficient)
DE	อิทธิพลทางตรง (Direct Effect)
IE	อิทธิพลทางอ้อม (Indirect Effect)
TE	อิทธิพลรวม (Total Effect)
CMIN/df	อัตราส่วนค่าสถิติไค-สแควร์ต่อองศาอิสระ (Chi-Square/Degrees of Freedom) ใช้พิจารณาความสอดคล้องของแบบจำลอง
CFI	ดัชนีวัดความสอดคล้องเชิงเปรียบเทียบ (Comparative Fit Index)
GFI	ดัชนีวัดระดับความสอดคล้อง (Goodness of Fit Index)
AGFI	ดัชนีวัดระดับความสอดคล้องที่ปรับแก้แล้ว (Adjusted Goodness of Fit Index)
NFI	ดัชนีความสอดคล้องเชิงนอร์ม (Normed Fit Index)
IFI	ดัชนีความสอดคล้องเชิงเพิ่ม (Incremental Fit Index)
RMR	ค่ารากที่สองของค่าเฉลี่ยกำลังสองของเศษเหลือ (Root Mean Square Residual)
RMSEA	ค่ารากที่สองของค่าเฉลี่ยความคลาดเคลื่อนกำลังสองของการประมาณค่า (Root Mean Square Error of Approximation)
CFA	การวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis)

สัญลักษณ์	ความหมาย
AVE	ค่าเฉลี่ยความแปรปรวนที่ถูกสกัดได้ (Average Variance Extracted)
CR	ค่าความเที่ยงรวม (Composite Reliability)
α	ค่าสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's Alpha) ใช้ตรวจสอบความเชื่อมั่นของเครื่องมือวิจัย
IOC	ดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ (Index of Item-Objective Congruence) ใช้ตรวจสอบความตรงเชิงเนื้อหา
*	มีนัยสำคัญทางสถิติที่ระดับ 0.05
**	มีนัยสำคัญทางสถิติที่ระดับ 0.001
SEM	แบบจำลองสมการโครงสร้าง (Structural Equation Modeling)

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ภาคผนวก ง

บทความและการนำเสนอผลงานระดับนานาชาติ

1. การนำเสนองานวิจัยในงานประชุมวิชาการระดับนานาชาติ

งาน the 6th Research, Invention, and Innovation Congress (RI2C 2025)



ภาพที่ ง-1 ประกาศนียบัตรเข้าร่วมนำเสนอผลงานวิชาการ

2. ผลงานตีพิมพ์

2.1 Enterprise Architecture for Digital Immunity Management. 2025 Research, Invention, and Innovation Congress: Innovative Electricals and Electronics (RI2C) | 979-8-3315-8898-4/25/$31.00 ©2025 IEEE | DOI: 10.1109/RI2C67120.2025.11282681

Enterprise Architecture for Digital Immunity Management

Nawarat Pinamnaj
Division of Information and Communication Technology for Education, Faculty of Technical Education, King Mongkut's University of Technology North Bangkok, (KMUTNB)
Bangkok,Thailand
s6602052910038@email.kmutnb.ac.th

Prachyanun Nilsook
Division of Information and Communication Technology for Education, Faculty of Technical Education, King Mongkut's University of Technology North Bangkok, (KMUTNB)
Bangkok,Thailand
prachyanunn@kmutnb.ac.th

Panita Wannapiroon
Division of Information and Communication Technology for Education, Faculty of Technical Education, King Mongkut's University of Technology North Bangkok, (KMUTNB)
Bangkok,Thailand
panita.w@fte.kmutnb.ac.th

2025 Research, Invention, and Innovation Congress: Innovative Electricals and Electronics (RI2C) | 979-8-3315-8898-4/25/$31.00 ©2025 IEEE | DOI: 10.1109/RI2C67120.2025.11282681

***Abstract*— This research on organizational architecture for digital immunity management consists of two stages. Stage 1 comprises three steps: (1) synthesis of the conceptual framework of the organizational architecture, (2) study of the elements of organizational architecture for digital immunity management, and (3) synthesis of the conceptual framework of digital immunity management. Stage 2 focuses on developing the conceptual framework of organizational architecture for digital immunity management. The results indicate that the conceptual framework consists of five components: Business Architecture, Data Architecture, Technology Architecture, Governance or Policy Layer, and Resilience or Risk or Sustainability.**

Keywords*— *Enterprise Architecture, Digital Immunity, Digital Immunity Management

I. Introduction

In the digital era, information technology plays a role in all dimensions of university operations, including teaching and learning. Therefore, universities need to adapt to cope with the risks of cyber threats that are increasingly complex and constantly emerging. This has led to the idea of developing a "Digital Immunity" strategy to strengthen the ability to resist, prevent, and recover from incidents that affect the organization's digital systems. [1]

Be concept of Digital Immunity is not limited to technology but also encompasses an integrated organizational management process. This approach requires strategic planning tools supported by a clear structural framework and systematic coordination between the organization's mission and its information systems. [2] One of the key tools enabling this integration is Enterprise Architecture (EA)[3], which facilitates the design, visualization, and organization of the relationships among various organizational components — including business, data, applications, and technology. [4]

However, currently there is still a gap in the application of the concepts of Enterprise Architecture and Digital Immunity Management in the context of educational institutions, especially in developing countries, which still lack a conceptual framework or model that can be adapted to the diverse structures, functions, and information systems of universities.

Based on this situation, this research aims to develop an Enterprise Architecture framework for Digital Immunity Management, to serve as a guide for planning, managing, and protecting the university's digital infrastructure — ensuring it is stable, resilient, and capable of effectively responding to cyber threats.

II. Research Purpose

This research aims to synthesize the elements of the enterprise architecture for digital immunity management and develop the conceptual framework of the enterprise architecture for digital immunity management.

III. Literature Review

A. Enterprise Architecture

Enterprise Architecture (EA) is a conceptual systems framework that helps design and organize the core elements of an organization across various dimensions, including business structure, data, applications, and technology, to create systematic connections and coherence among them.[5], [6] In addition, EA is a systematic approach that enables higher education institutions to comprehensively analyze cyber risks through four main elements: Business, Data, Application, and Technology Architectures. [3] It was also found that the concept has been expanded to include the integration of cybersecurity architecture within the EA framework. This integration reduces vulnerabilities and enhances the efficiency of digital security governance at the enterprise level. [5] The concept of Enterprise Architecture (EA) is considered as an "enterprise-level structure" that integrates the elements of business systems (e.g., processes and organizational structures of electrical engineering departments), data, applications, and technology or infrastructure. [7] In addition, research studies describe Enterprise Architecture (EA) as a conceptual systems framework that supports the design and organization of an organization's core elements. Based on the TOGAF Content Framework[8], [9], which includes four main components—Business Architecture, Application Architecture, Data Architecture, and Technology Architecture—EA also encompasses organizational transformation and systematic change management. [10] Its aim is to enhance the efficiency of planning and developing digital structures that align with strategic goals and enable continuous operational oversight. [8], [11]

B. Digital Immunity

Digital Immunity refers to the capabilities of intelligent digital systems that are enhanced through adversarial training. In this process, adversarial samples are used to train the system to recognize and resist disturbances, enabling it to

979-8-3315-8898-4/25/$31.00 ©2025 IEEE
Authorized licensed use limited to: King Mongkut's University of Technology North Bangkok. Downloaded on December 19,2025 at 11:15:16 UTC from IEEE Xplore. Restrictions apply.

ประวัติผู้เขียน

ชื่อ นางสาวเนาวรัตน์ ปิ่นอำนาจ

ชื่อดุษฎีนิพนธ์ สถาปัตยกรรมองค์กรปัญญาประดิษฐ์เพื่อการจัดการภูมิคุ้มกันดิจิทัลสำหรับสถาบันอุดมศึกษา

สาขาวิชา เทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา

ประวัติ ประวัติการศึกษา

พ.ศ.2569 สำเร็จการศึกษาระดับปริญญาเอก หลักสูตรปรัชญาดุษฎีบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

พ.ศ.2551 สำเร็จการศึกษาระดับปริญญาโท
หลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยรังสิต

พ.ศ.2544 สำเร็จการศึกษาระดับปริญญาตรี
หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง

ประวัติการทำงาน

2565 - ปัจจุบัน คณบดีคณะวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยเจ้าพระยา

2549 - 2565 หัวหน้าสาขาวิชา/ประธานหลักสูตร
สาขาวิชาวิทยาการคอมพิวเตอร์
มหาวิทยาลัยเจ้าพระยา

2544 - 2549 เจ้าหน้าที่ประจำสาขาวิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง

ผลงานวิจัยและวิชาการ

เนาวรัตน์ ปิ่นอำนาจ, อุทัยวรรณ แก้วตะคุ และรษา ทองคงอยู่. (2565). การสร้างแอพพลิเคชั่นให้กับเทศบาลตำบล เพื่อการบริหารจัดการรถรับ-ส่งผู้สูงอายุไปรักษาที่สถานพยาบาล. วารสารวิจยวิชาการ ปีที่ 5 ฉบับที่ 3 (พฤษภาคม-มิถุนายน 2565). 49-62.

เนาวรัตน์ ปิ่นอำนาจ, อุทัยวรรณ แก้วตะคุ และจักรพันธ์ จันทร์เขียว. (2563). การบริหารจัดการขยะชุมชนด้วยระบบอัจฉริยะเพื่อเพิ่มประสิทธิภาพในการบริหารจัดการสิ่งแวดล้อมของชุมชน. วารสารวิชาการสถาบันวิทยาการจัดการแห่งแปซิฟิค (สาขามนุษยศาสตร์และสังคมศาสตร์), 6(2), 208-215.

จักรพันธ์ จันทร์เขียว, มัจรี สุพรรณ และเนาวรัตน์ ปิ่นอำนาจ. (2563). การบริหารระบบการจองห้องประชุมออนไลน์ กรณีศึกษาสานักงานจังหวัดนครสวรรค์.วารสารวิชาการสถาบันวิทยาการจัดการแห่งแปซิฟิค (สาขามนุษยศาสตร์และสังคมศาสตร์), 6(2), 216-223.

เนาวรัตน์ ปิ่นอำนาจ, จิรนันท์ กมลสินธุ์, อุทัยวรรณ แก้วตะคุ . (2562). การพัฒนาอุปกรณ์ควบคุมเครื่อง MULTI SERVICE ACCESS NODE. ใน การประชุมวิชาการระดับชาติ ครั้งที่ 4 และระดับนานาชาติ ครั้งที่ 2 มหาวิทยาลัยเจ้าพระยา วันที่ 9 ธันวาคม 2562 (น.384-392). นครสวรรค์: มหาวิทยาลัยเจ้าพระยา.

เนาวรัตน์ ปิ่นอำนาจ. (2562). G SUITE FOR EDUCATION นวัตกรรมการศึกษาในศตวรรษที่ 21. การประชุมวิชาการระดับชาติ ครั้งที่ 4 และระดับนานาชาติ ครั้งที่ 2 มหาวิทยาลัยเจ้าพระยา วันที่ 9 ธันวาคม 2562 (น.365-374). นครสวรรค์: มหาวิทยาลัยเจ้าพระยา