

ระบบปัญญาประดิษฐ์สำหรับสกัดและเชื่อมโยงข้อกำหนดกฎหมายไซเบอร์ไทยเพื่อสร้างรายการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ

นายพลวัฒน์ สามพ่วงบุญ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ระบบปัญญาประดิษฐ์สำหรับสกัดและเชื่อมโยงข้อกำหนดกฎหมายไซเบอร์ไทยเพื่อสร้างรายการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ

นายพลวัฒน์ สามพ่วงบุญ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง ระบบปัญญาประดิษฐ์สำหรับสกัดและเชื่อมโยงข้อกำหนดกฎหมายไซเบอร์ไทยเพื่อสร้างรายการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ

โดย นายพลวัฒน์ สามพ่วงบุญ

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ

.....
(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)
คณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

คณะกรรมการสอบการค้นคว้าอิสระ

.....
(ผู้ช่วยศาสตราจารย์ ดร.อัครนันท์ พงศธรวิวัฒน์)
ประธาน

.....
(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)
อาจารย์ที่ปรึกษา

.....
(ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์)
กรรมการ

ชื่อ : นายพลวัฒน์ สามพ่วงบุญ
ชื่อการค้นคว้าอิสระ : ระบบปัญญาประดิษฐ์สำหรับสกัดและเชื่อมโยงข้อกำหนดกฎหมายไซเบอร์ไทยเพื่อสร้างรายการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ
สาขาวิชา : การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์
ปีการศึกษา : 2568

บทคัดย่อ

การวิจัยนี้มุ่งพัฒนาระบบปัญญาประดิษฐ์เพื่อสกัดและเชื่อมโยงข้อกำหนดจากกฎหมายไซเบอร์ไทย 3 ฉบับ (พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม และพรบ คุ้มครองข้อมูลส่วนบุคคล) ระบบทำงานผ่านสถาปัตยกรรมผสมผสาน (Hybrid AI Pipeline) 7 ขั้นตอน ที่บูรณาการระบบกฎเกณฑ์ (Rule-based) โมเดลภาษาขนาดใหญ่ (LLM) และ WangchanBERTa เพื่อจัดหมวดหมู่ สกัดข้อมูลสำคัญ และแยกแยะภาระหน้าที่ขององค์กรออกจากบทลงโทษได้อย่างแม่นยำ

ผลลัพธ์คือรายการตรวจสอบความสอดคล้อง (Compliance Checklist) ที่ระบุสิ่งที่ต้องทำและหลักฐานชัดเจน พร้อมเชื่อมโยงมาตรฐาน ISO/IEC 27001:2022 และ NIST CSF 2.0 ในระบบเดียว โดยต้องผ่านกระบวนการรับรองจากผู้เชี่ยวชาญ 3 ท่าน (3-Expert Validation) ก่อนเผยแพร่ ผลการประเมินจากผู้เชี่ยวชาญ 3 ท่านและองค์กรตัวอย่าง 5 แห่ง พบว่าประสิทธิภาพและความพึงพอใจอยู่ในระดับ "มาก" (คะแนนเฉลี่ย 4.23 และ 4.33 จาก 5.00 ตามลำดับ) นอกจากนี้ระบบยังช่วยลดระยะเวลาตรวจสอบความสอดคล้องกับกฎหมายได้เฉลี่ยถึง 64% เมื่อเทียบกับกระบวนการเดิม

(มีจำนวนทั้งสิ้น 47 หน้า)

คำสำคัญ : กฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย, การประมวลผลภาษาธรรมชาติ, รายการตรวจสอบความสอดคล้อง

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Pollawat Samphuangbun

Independent Study Title : AI-Based System for Extracting and Mapping Thai Cybersecurity Legal Requirements to Generate a Cybersecurity Compliance Checklist

Major Field : Digital Network and Information Security Management
King Mongkut's University of Technology North Bangkok

Independent Study Advisor : Assistant Professor Dr. Pongsarun Boonyopakorn

Academic Year : 2025

ABSTRACT

This research aims to develop an artificial intelligence system for extracting and mapping requirements from three Thai cybersecurity laws: the Cybersecurity Act B.E. 2562, the Computer-Related Offences Act B.E. 2550 and its amendments, and the Personal Data Protection Act. The system operates on a 7-stage Hybrid AI Pipeline architecture that integrates rule-based processing, large language models (LLMs), and WangchanBERTa to classify, extract five key entity types, and accurately separate organizational obligations from legal penalties.

The resulting output is a Compliance Checklist featuring clear required actions and evidence, simultaneously mapped to ISO/IEC 27001:2022 and NIST CSF 2.0 standards. Prior to publication, all checklists must undergo a 3-Expert Validation process. System evaluation by three experts and five sample organizations revealed "High" levels of efficiency and user satisfaction, achieving mean scores of 4.23 and 4.33 out of 5.00, respectively. Furthermore, the system demonstrated an average time saving of 64% in the compliance review process compared to traditional methods.

(Total 47 Pages)

Keywords: Thai Cybersecurity Law, Natural Language Processing, Compliance

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระในครั้งนี้ สำเร็จลงด้วยดีเนื่องจากได้รับความกรุณาจากอาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์ ที่ให้คำชี้แนะ ตรวจทาน และแก้ไขข้อบกพร่องต่างๆ ตลอดการดำเนินงานวิจัย ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูง

นอกจากนี้ขอขอบพระคุณผู้เชี่ยวชาญทั้ง 3 ท่าน ที่ให้เกียรติตรวจสอบความถูกต้องของการประมวลผลกฎหมายและ พรบ คุ้มครองข้อมูลส่วนบุคคล ตลอดจนขอขอบคุณองค์กรตัวอย่างทั้ง 5 แห่ง ที่อนุเคราะห์ร่วมทดสอบระบบและให้ข้อเสนอแนะอันเป็นประโยชน์ยิ่งต่อการประเมินประสิทธิผลของงานวิจัย

ท้ายนี้ ขอกราบขอบพระคุณอาจารย์ ดร.ธนวรรธน์ โยชะนัง และคณาจารย์ประจำสาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ที่ประสิทธิ์ประสาทวิชาความรู้ ตลอดจนบิดา มารดา ครอบครัว และเพื่อนๆ ที่คอยสนับสนุนและเป็นกำลังใจสำคัญเสมอมา จนทำให้การค้นคว้าอิสระฉบับนี้เสร็จสมบูรณ์

พลวัฒน์ สามพ่วงบุญ

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	จ
กิตติกรรมประกาศ	ฉ
สารบัญตาราง	ฌ
สารบัญภาพ	ฎ
บทที่ 1 บทนำ	
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของงานวิจัย	2
1.3 ขอบเขตของการวิจัย	2
1.4 ข้อจำกัด	4
1.5 ประโยชน์ที่คาดว่าจะได้รับ	4
บทที่ 2 แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง	
2.1 กฎหมายและความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย	6
2.2 มาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ	8
2.3 เทคโนโลยีการประมวลผลภาษาธรรมชาติสำหรับกฎหมายไทย	10
2.4 การออกแบบ AI Pipeline สำหรับการประมวลผลเอกสารกฎหมาย	12
2.5 การทบทวนงานวิจัยที่เกี่ยวข้อง	13
บทที่ 3 วิธีการดำเนินการวิจัย	
3.1 การรวบรวมและจัดเตรียมเอกสารกฎหมาย	16
3.2 การออกแบบโครงสร้างข้อมูล	18
3.3 การออกแบบสถาปัตยกรรมระบบ	19
3.4 กระบวนการตรวจสอบโดยผู้เชี่ยวชาญ	22
3.5 การออกแบบระบบเชื่อมโยงมาตรฐานสากล	23
3.6 การออกแบบการทดลองและเกณฑ์การวัดผล	23
3.7 การออกแบบเว็บแอปพลิเคชัน	26
3.8 ขั้นตอนการสรุปผลและการนำไปใช้จริง	29

สารบัญ (ต่อ)

หน้า

บทที่ 4 ผลการวิจัย

4.1 ผลการประเมินโดยผู้เชี่ยวชาญ 30

4.2 ผลการประเมินความพึงพอใจจากองค์กรตัวอย่าง 33

4.3 การอภิปรายผล 36

4.4 สรุปผลการประเมินทั้งสองกลุ่ม 37

บทที่ 5 สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

5.1 สรุปผลการดำเนินงานวิจัย 39

5.2 การอภิปรายผล 41

5.3 ข้อจำกัดของการวิจัย 42

5.4 ข้อเสนอแนะ 43

5.5 สรุปปิดท้าย 43

บรรณานุกรม 45

ประวัติผู้วิจัย 47

สารบัญตาราง

		หน้า
2-1	เปรียบเทียบกฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย 3 ฉบับ	6
2-2	กลุ่มมาตรการควบคุม ISO/IEC 27001:2022 และความเกี่ยวข้องกับกฎหมายไทย	8
2-3	6 ฟังก์ชันของ NIST CSF 2.0 และ Subcategories ที่เกี่ยวข้องกับกฎหมายไทย	9
2-4	เปรียบเทียบงานวิจัยที่เกี่ยวข้องกับระบบที่พัฒนาขึ้น	14
3-1	กระบวนการประมวลผล AI 7 ขั้นตอน พร้อมวิธีหลักและกลไกสำรอง	19
3-2	สถานะของเอกสารกฎหมาย 13 ระยะในระบบ	20
3-3	ตารางหลักในฐานข้อมูลและข้อมูลที่จัดเก็บ	21
3-4	เกณฑ์การคัดเลือกผู้เชี่ยวชาญประเมินระบบ	23
3-5	เกณฑ์การคัดเลือกองค์กรตัวอย่าง	25
3-6	ตารางเกณฑ์การแปลผลคะแนน	26
3-7	หน้าจอในระบบแบ่งตามบทบาทผู้ใช้งาน	26
4-1	ผลการประเมินหมวด B ความถูกต้องของ AI Mapping โดยผู้เชี่ยวชาญ 3 ท่าน	30
4-2	ผลการประเมินหมวด C ความสะดวกในการใช้งาน	31
4-3	ผลการประเมินหมวด D ความน่าเชื่อถือของกระบวนการตรวจสอบ	31
4-4	ผลการประเมินหมวด E ความเพียงพอของผลลัพธ์	32
4-5	สรุปคะแนนเฉลี่ยรายหมวดและความพึงพอใจโดยรวมจากผู้เชี่ยวชาญ 3 ท่าน	32
4-6	ผลการประเมินหมวด B ประสิทธิภาพในการตรวจสอบ	33
4-7	ผลการประเมินหมวด C ความสะดวกในการใช้งาน	34
4-8	ผลการประเมินหมวด D ความเหมาะสมกับองค์กร	34
4-9	ผลการประเมินหมวด E ผลกระทบและคุณค่า	35
4-10	สรุปคะแนนเฉลี่ยรายหมวดและความพึงพอใจโดยรวมจากองค์กรตัวอย่าง 5 แห่ง	35
4-11	สรุปข้อสังเกตเชิงคุณภาพจากผู้ประเมินทั้งสองกลุ่ม	37
4-12	สรุปผลการประเมินทั้งสองกลุ่ม	38
5-1	สรุปผลตามวัตถุประสงค์การวิจัย	39
5-2	สรุปผลการประเมินโดยผู้เชี่ยวชาญ 3 ท่าน	39
5-3	สรุปผลการประเมินความพึงพอใจจากองค์กรตัวอย่าง 5 แห่ง	40
5-4	ข้อจำกัดของการวิจัยและผลกระทบ	42

สารบัญรูปภาพ

หน้า

1-1 ภาพรวมปัญหาการไม่ปฏิบัติตามกฎหมายและแนวทางแก้ไขด้วยระบบปัญญาประดิษฐ์ 1

1-2 แผนภาพกระบวนการประมวลผล AI 7 ขั้นตอน 2

1-3 แผนภาพสถาปัตยกรรมระบบ 5 ส่วนหลักใน Docker 3

1-4 แผนภาพขั้นตอนการทำงานจากต้นจนจบ แบ่งตามผู้ปฏิบัติ 4

2-1 แผนภาพกระบวนการสกัดข้อมูลสำคัญจากกฎหมายไซเบอร์ไทย 11

2-2 แผนภาพแสดงความสัมพันธ์ระหว่างทฤษฎีและเทคโนโลยีที่ใช้ในงานวิจัย 15

3-1 แหล่งที่มาของเอกสารกฎหมายและหน่วยงานกำกับดูแล 17

3-2 แผนภาพการไหลของข้อมูลในกระบวนการประมวลผล AI 7 ขั้นตอน 20

3-3 แผนภาพการเปลี่ยนสถานะของเอกสาร 13 ระยะ 21

3-4 แผนภาพความสัมพันธ์ระหว่างตารางหลักในฐานข้อมูล 22

3-5 กระบวนการตรวจสอบโดยผู้เชี่ยวชาญ 3 ท่าน 22

3-6 ตัวอย่างหน้าจอหลักของระบบ (ผู้ดูแลระบบ) 27

3-7 ตัวอย่างหน้าจอหลักของระบบ (ผู้เชี่ยวชาญ) 28

3-8 ตัวอย่างหน้าจอหลักของระบบ (ผู้ใช้งาน) 28

3-9 แผนภาพขั้นตอนการทำงานจากต้นจนจบ 29

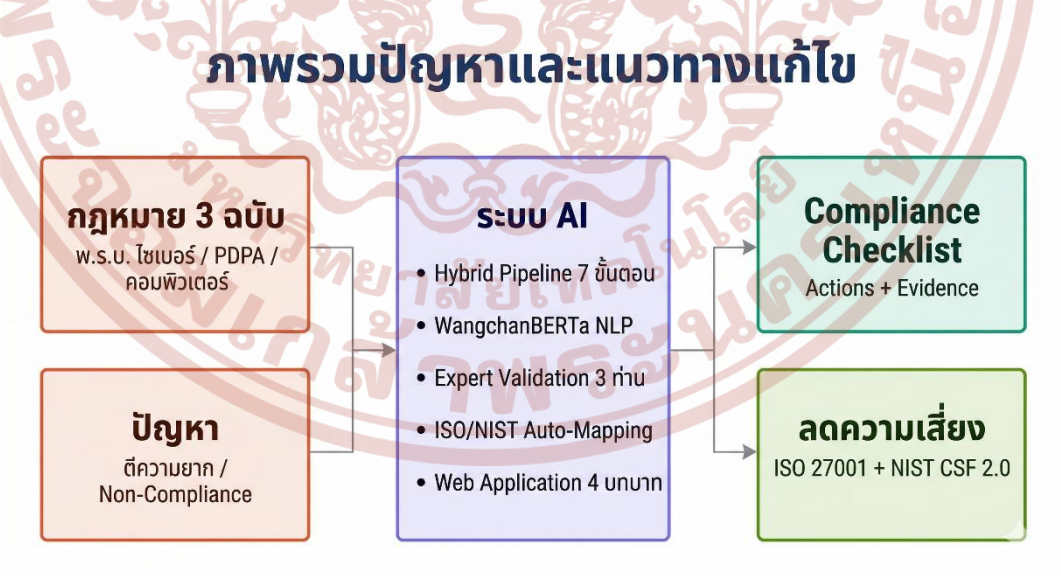
4-1 แผนภูมิแสดงคะแนนผู้เชี่ยวชาญรายหมวด B–E เปรียบเทียบทั้ง 3 ท่าน 33

4-2 แผนภูมิแสดงคะแนนความพึงพอใจรายหมวด B–E จากองค์กรตัวอย่าง 35

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การพึ่งพาเทคโนโลยีสารสนเทศในภาคธุรกิจและบริการเพิ่มขึ้นอย่างต่อเนื่องรัฐบาลไทยได้ออกกฎหมายสำคัญ 3 ฉบับ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไข พ.ศ. 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อกำหนดกรอบการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศสำหรับองค์กร [1] อย่างไรก็ตาม กฎหมายเหล่านี้ใช้ภาษากฎหมายที่มีโครงสร้างซับซ้อนบางมาตราระบุภาระหน้าที่และบทลงโทษไว้ในประโยคเดียวกัน ทำให้องค์กรจำนวนมากประสบปัญหาในการตีความและปฏิบัติตาม อาจนำไปสู่บทลงโทษทางกฎหมาย ความเสียหายทางการเงิน และการสูญเสียความน่าเชื่อถือขององค์กร [2] งานวิจัยนี้จึงพัฒนาระบบช่วยจัดทำรายการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยไซเบอร์ด้วยปัญญาประดิษฐ์ ที่ประมวลผลเอกสารกฎหมายแบบกึ่งอัตโนมัติผ่านกระบวนการ 7 ขั้นตอน เชื่อมโยงกับมาตรฐาน ISO/IEC 27001:2022 และ NIST CSF 2.0 พร้อมระบบตรวจสอบโดยผู้เชี่ยวชาญก่อนเผยแพร่ทุกครั้ง



ภาพที่ 1-1 ภาพรวมปัญหาการไม่ปฏิบัติตามกฎหมายและแนวทางแก้ไขด้วยระบบปัญญาประดิษฐ์

1.2 วัตถุประสงค์

พัฒนาระบบปัญญาประดิษฐ์สำหรับสกัดข้อกำหนดที่องค์กรต้องปฏิบัติตามจากกฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย 3 ฉบับออกแบบรายการตรวจสอบกึ่งอัตโนมัติที่เชื่อมโยงกับมาตรฐาน ISO/IEC 27001:2022 และ NIST CSF 2.0 พร้อมระบุสิ่งที่ต้องดำเนินการและหลักฐานที่ต้องมีพัฒนากระบวนการตรวจสอบโดยผู้เชี่ยวชาญอย่างน้อย 3 ท่าน และเว็บแอปพลิเคชันรองรับผู้ใช้งาน 4 ประเภท ประเมินประสิทธิผลของระบบโดยผู้เชี่ยวชาญด้านกฎหมายไซเบอร์และองค์กรตัวอย่าง

1.3 ขอบเขตของการวิจัย

1.3.1 กฎหมายที่ครอบคลุม

1.3.1.1 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.3.1.2 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไข พ.ศ. 2560

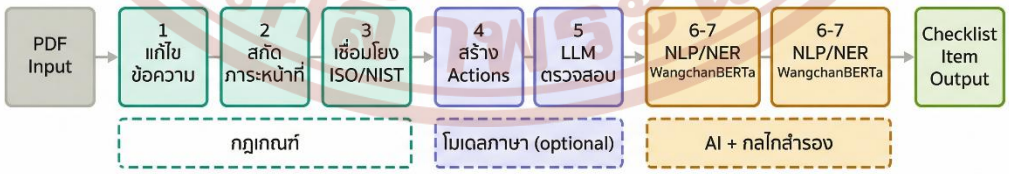
1.3.1.3 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.3.2 การประเมินผลของระบบ

1.3.2.1 แบบประเมินโดยผู้เชี่ยวชาญ 3 ท่าน

1.3.2.2 แบบประเมินความพึงพอใจขององค์กรตัวอย่าง 5 แห่ง

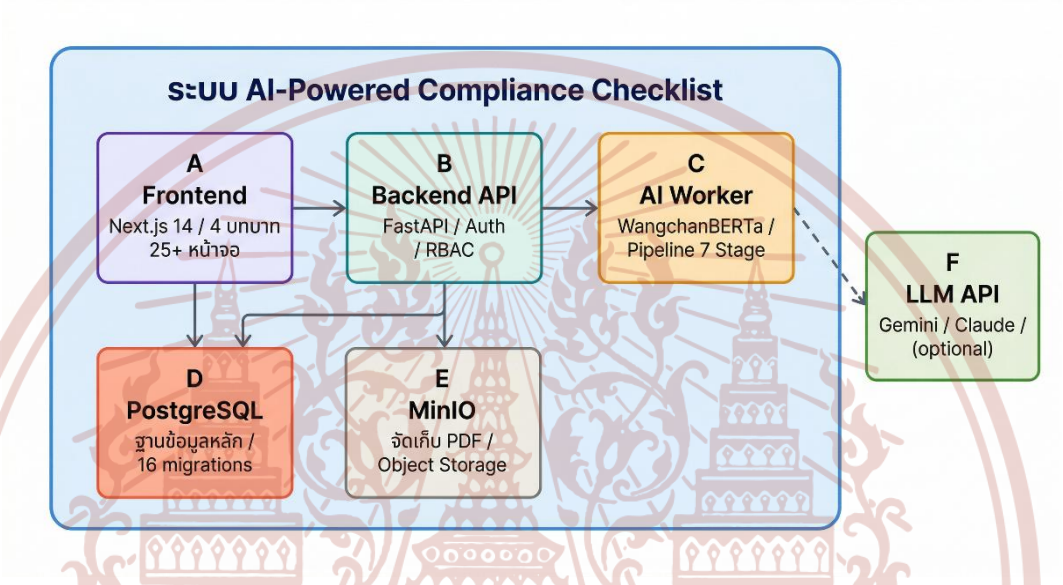
1.3.3 ขั้นตอนการประมวลผลด้วยปัญญาประดิษฐ์



ภาพที่ 1-2 แผนภาพกระบวนการประมวลผล AI 7 ขั้นตอน

1.3.4 สถาปัตยกรรมระบบ

ระบบประกอบด้วย 5 ส่วนหลักที่ทำงานร่วมกัน ได้แก่ ฐานข้อมูล PostgreSQL คลังเก็บไฟล์ MinIO เซิร์ฟเวอร์หลัก FastAPI ตัวประมวลผล AI และเว็บแอปพลิเคชัน Next.js 14



ภาพที่ 1-3 แผนภาพสถาปัตยกรรมระบบ 5 ส่วนหลักใน Docker

1.3.5 กระบวนการตรวจสอบโดยผู้เชี่ยวชาญ

1.3.5.1อัปโหลดและตรวจสอบข้อความ

1.3.5.2 ทบทวนการเชื่อมโยง

1.3.5.3 ตรวจสอบโดยผู้เชี่ยวชาญ

1.3.5.4 เผยแพร่โดยผู้ดูแลระบบ

1.3.5.5 การประเมินตนเองขององค์กร

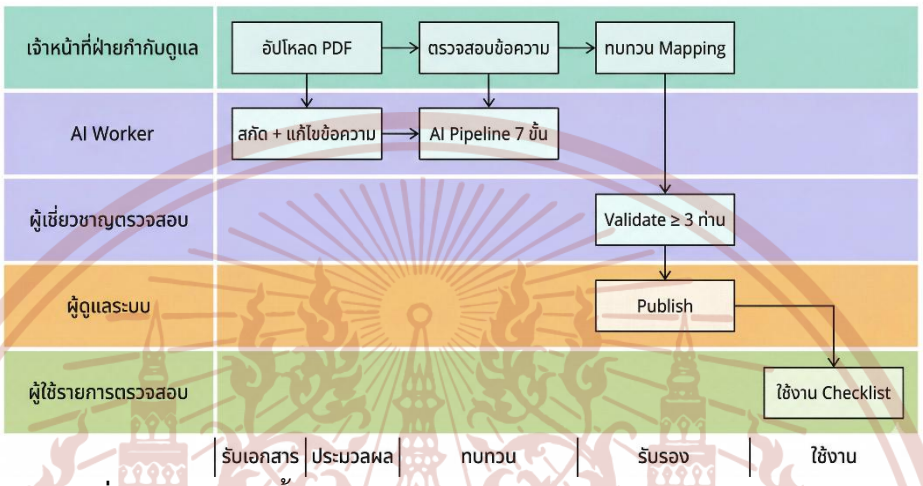
1.3.6 ผู้ใช้งานและสิทธิ์

1.3.6.1 ผู้ดูแลระบบ มีสิทธิ์การใช้งาน คือ จัดการบัญชีผู้ใช้, เผยแพร่รายการตรวจสอบ, ดูผลการประเมิน และส่งออกรายงาน

1.3.6.2 เจ้าหน้าที่ฝ่ายกำกับดูแล มีสิทธิ์การใช้งาน คือ อัปโหลดเอกสาร, ตรวจสอบข้อความ และทบทวนการเชื่อมโยงมาตรฐาน

1.3.6.3 ผู้เชี่ยวชาญ มีสิทธิ์การใช้งาน คือ ตรวจสอบรายการตรวจสอบ, ให้คะแนนเพิ่มความเห็น และดูประวัติการตรวจสอบ

1.3.6.4 ผู้ใช้งาน มีสิทธิ์การใช้งาน คือ เลือกรายการ, บันทึกสถานะการปฏิบัติตาม และแนบหลักฐาน



ภาพที่ 1-4 แผนภาพขั้นตอนการทำงานจากต้นจนจบ แบ่งตามผู้ปฏิบัติ

1.4 ข้อจำกัด

1.4.1 ลักษณะพิเศษของภาษากฎหมายไทย บางมาตราเขียนภาระหน้าที่รวมกับบทลงโทษในประโยคเดียว อาจมีข้อผิดพลาดในบางกรณีที่ซับซ้อน

1.4.2 คุณภาพของการแปลง PDF เอกสารบางฉบับมีปัญหาการเข้ารหัสอักขระ ระบบแก้ไขได้ส่วนใหญ่

1.4.3 การพึ่งพาโมเดลภาษา ขั้นตอนที่ 4–5 ทำงานได้เต็มประสิทธิภาพเมื่อมีการเชื่อมต่อบริการโมเดลภาษาภายนอก

1.4.4 โมเดล WangchanBERTa ยังไม่ได้ปรับแต่งสำหรับกฎหมายไทย ขั้นตอนที่ 6–7 ใช้โมเดลพื้นฐาน ความแม่นยำจะเพิ่มขึ้นในระยะต่อไป

1.4.5 ผลลัพธ์ต้องผ่านการรับรองจากผู้เชี่ยวชาญ อย่างน้อย 3 ท่านก่อนนำไปใช้งานจริงเสมอ

1.4.6 ขนาดกลุ่มตัวอย่าง ผู้เชี่ยวชาญ 3 ท่านและองค์กร 5 แห่ง เหมาะสำหรับการพิสูจน์แนวคิดเบื้องต้น

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ช่วยให้องค์กรปฏิบัติตามกฎหมายไซเบอร์ไทยทั้ง 3 ฉบับอย่างเป็นระบบ

1.5.2 ลดภาระการตีความกฎหมาย ด้วยรายการสิ่งที่ต้องดำเนินการในภาษาปฏิบัติงาน

1.5.3 เชื่อมโยงกฎหมายไทยกับมาตรฐานสากลในระบบเดียว

1.5.4 ลดต้นทุนการกำกับดูแลด้านไอทีและการพึ่งพาที่ปรึกษาภายนอก

1.5.5 สร้างรากฐานฐานความรู้กฎหมายไซเบอร์ไทยที่พัฒนาต่อเนื่องได้

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ในการพัฒนาระบบปัญญาประดิษฐ์สำหรับสกัดและเชื่อมโยงข้อกำหนดกฎหมายไซเบอร์ไทย ผู้วิจัยได้รวบรวมและวิเคราะห์แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องจาก 5 กลุ่มหลัก ได้แก่ กฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย มาตรฐานสากล เทคโนโลยีประมวลผลภาษาธรรมชาติ การออกแบบ AI Pipeline และงานวิจัยที่เกี่ยวข้อง เพื่อใช้เป็นฐานในการออกแบบสถาปัตยกรรมระบบ

2.1 กฎหมายและความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย

ประเทศไทยมีกฎหมายความมั่นคงปลอดภัยไซเบอร์และคุ้มครองข้อมูลที่ประกาศใช้ใน พ.ศ. 2562 สองฉบับหลัก ควบคู่กับกฎหมายคอมพิวเตอร์ที่แก้ไขใน พ.ศ. 2560 ทั้งสามฉบับส่งผลต่อองค์กรพร้อมกันและมีจุดเชื่อมโยงกันในหลายประเด็น ตารางที่ 2.1 สรุปลักษณะเปรียบเทียบ

ประเด็น	พ.ร.บ. ไซเบอร์ 2562	PDPA 2562	พ.ร.บ. คอมพิวเตอร์ 2550/2560
กลุ่มเป้าหมาย	หน่วยงาน CII และผู้ประกอบการ	ทุกองค์กรที่เก็บข้อมูลส่วนบุคคล	ผู้ให้บริการอินเทอร์เน็ต/แพลตฟอร์ม
หน่วยงานกำกับ	สำนักงาน กสทช. / NCSC	PDPC	กระทรวงดิจิทัล (MDES)
ภาระหน้าที่หลัก	จัดทำแผน IRP ตรวจสอบประจำปี รายงานเหตุ	ความยินยอม DSR DPO RoPA แจ้งเหตุ 72 ชม.	เก็บ Log ≥ 90 วัน กลั่นกรองเนื้อหา ห้ามเปิดเผย
ความท้าทาย NLP	ประโยคยาว อ้างอิงข้ามหมวด	คำศัพท์เฉพาะ GDPR ยืม	บทลงโทษปนกับภาระหน้าที่ในประโยคเดียว
ISO Controls หลัก	5.23–5.28, 8.8	5.34, 5.12, 8.10	8.15–8.17, 5.33, 5.19–5.20
NIST Functions หลัก	RS, RC, ID	GV, PR	DE, PR

ตารางที่ 2-1 เปรียบเทียบกฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย 3 ฉบับ

2.1.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

กฎหมายฉบับนี้มีวัตถุประสงค์เพื่อเฝ้าระวัง ป้องกัน และรับมือกับภัยคุกคามทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญ (Critical Information Infrastructure: CII) เช่น ภาคการเงิน

โทรคมนาคม พลังงาน และสาธารณสุข กฎหมายกำหนดให้หน่วยงาน CII ต้องปฏิบัติตามมาตรการขั้นต่ำ 3 ระดับ ได้แก่ ระดับพื้นฐาน ระดับสำคัญ และระดับวิกฤต [8]

ภาระหน้าที่หลักที่ระบบต้องสกัดและเชื่อมโยง ได้แก่ การจัดทำนโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ การจัดทำแผนรับมือภัยคุกคาม (Incident Response Plan: IRP) การตรวจสอบและประเมินความเสี่ยงประจำปี การฝึกซ้อมรับมือเหตุการณ์ไซเบอร์ (Cyber Drill) และการรายงานเหตุการณ์ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC) ภายในระยะเวลาที่กำหนด

ความท้าทายสำหรับระบบ NLP คือกฎหมายฉบับนี้มีการอ้างอิงข้ามหมวดหมู่และประกาศลำดับรองจำนวนมาก ระบบจึงต้องอาศัยกลไกพิเศษในการจัดการ multi-level cross-reference เพื่อให้รายการตรวจสอบครอบคลุมครบถ้วน

2.1.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

PDPA เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ได้รับแรงบันดาลใจจาก GDPR ของสหภาพยุโรป ส่งผลกระทบต่อทุกองค์กรที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลในประเทศไทย [7] กฎหมายแบ่งผู้ที่เกี่ยวข้องเป็น 2 ฝ่ายหลัก ได้แก่ ผู้ควบคุมข้อมูล (Data Controller) ซึ่งกำหนดวัตถุประสงค์และวิธีการประมวลผล และผู้ประมวลผลข้อมูล (Data Processor) ซึ่งประมวลผลตามคำสั่ง

ภาระหน้าที่สำคัญที่ระบบต้องวิเคราะห์ครอบคลุม 7 ด้านหลัก ได้แก่ (1) การได้รับความยินยอมอย่างชัดแจ้งก่อนเก็บข้อมูล (2) การเคารพสิทธิเจ้าของข้อมูล เช่น สิทธิเข้าถึง แก้ไข ลบ และพกพา (3) การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) สำหรับองค์กรที่เข้าเกณฑ์ (4) การจัดทำบันทึกรายการประมวลผลข้อมูล (RoPA) (5) การแจ้งเหตุละเมิดต่อ PDPC ภายใน 72 ชั่วโมง (6) การทำข้อตกลงกับผู้ประมวลผลข้อมูล (Data Processing Agreement) และ (7) การปฏิบัติตามเงื่อนไขพิเศษก่อนโอนข้อมูลไปต่างประเทศ [4]

2.1.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไข พ.ศ. 2560

กฎหมายฉบับนี้กำหนดฐานความผิดและบทลงโทษสำหรับการกระทำทางคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมาย รวมถึงกำหนดภาระหน้าที่เฉพาะสำหรับผู้ให้บริการอินเทอร์เน็ตและแพลตฟอร์ม ลักษณะพิเศษที่ท้าทายระบบ NLP คือการเขียนภาระหน้าที่ปนกับบทลงโทษในประโยคเดียวกัน [1]

ตัวอย่างเช่น มาตรา 15 บัญญัติว่า "ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14... ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14"

ประโยคนี้มีทั้งส่วนที่เป็นภาระหน้าที่ (ห้ามสนับสนุน) และส่วนที่เป็นบทลงโทษ (ระวางโทษเช่นเดียวกัน) ระบบต้องใช้กลไก split-clause logic เพื่อแยกออกจากกัน

ภาระหน้าที่สำคัญที่สกัดได้ ได้แก่ (1) มาตรา 15: ผู้ให้บริการต้องไม่สนับสนุนหรือยินยอมให้มีการเผยแพร่เนื้อหาผิดกฎหมาย และฉบับ 2560 เพิ่มภาระในการระงับเนื้อหาตามขั้นตอนที่รัฐมนตรีกำหนด (2) มาตรา 22: ห้ามเปิดเผยหรือส่งมอบข้อมูลที่ได้มาจากการสืบสวน และ (3) มาตรา 26: ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วัน สูงสุดไม่เกิน 2 ปีในกรณีมีคำสั่งพิเศษ

2.2 มาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ

งานวิจัยนี้เชื่อมโยงข้อกำหนดกฎหมายไทยกับมาตรฐานสากล 2 ชุดพร้อมกัน เพื่อให้รายการตรวจสอบสามารถนำไปใช้ได้จริงในองค์กรที่ดำเนินการตามมาตรฐานระดับนานาชาติ

2.2.1 มาตรฐาน ISO/IEC 27001:2022

ISO/IEC 27001 คือมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ที่องค์กรนำไปใช้เพื่อพิสูจน์ว่ามีกระบวนการจัดการความเสี่ยงด้านข้อมูลอย่างเป็นระบบ ฉบับ ค.ศ. 2022 ปรับโครงสร้างจาก 114 มาตรการควบคุม (Annex A ฉบับ 2013) เป็น 93 มาตรการควบคุมใน 4 กลุ่ม และเพิ่มมาตรการใหม่ที่ตอบรับภัยคุกคามยุคใหม่ เช่น Threat Intelligence (5.7), Cloud Security (5.23) และ Data Masking (8.11) [ก2]

การจัดกลุ่มมาตรการควบคุมและตัวอย่างที่เกี่ยวข้องกับกฎหมายไซเบอร์ไทย แสดงในตารางที่ 2.2

กลุ่ม	จำนวน Controls	Controls ที่เกี่ยวข้องกับกฎหมายไซเบอร์ไทย
Organizational (5.x)	37	5.12 การจัดชั้นข้อมูล · 5.19–5.23 ความสัมพันธ์กับคู่ค้า · 5.24–5.28 รับมือเหตุการณ์ · 5.33–5.34 ความเป็นส่วนตัว
People (6.x)	8	6.6 ข้อตกลงรักษาความลับ
Physical (7.x)	14	7.10 สื่อบันทึกข้อมูล (กรณีจัดเก็บ Log ในสื่อกายภาพ)
Technological (8.x)	34	8.10 การลบข้อมูล · 8.15–8.17 การบันทึก · 8.20–8.22 เครือข่าย · 8.24 การเข้ารหัส

ตารางที่ 2-2 กลุ่มมาตรการควบคุม ISO/IEC 27001:2022 และความเกี่ยวข้องกับกฎหมายไทย

ระบบที่พัฒนาขึ้นสร้างพจนานุกรมการเชื่อมโยงจากคำสำคัญในกฎหมายไปยัง ISO Controls โดยอัตโนมัติ ตัวอย่างเช่น คำว่า "เก็บรักษาข้อมูลจราจร" จะเชื่อมโยงกับ Controls 8.15, 8.16, 8.17 และ 5.33 คำว่า "มาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล" จะเชื่อมโยงกับ Controls 5.34 และ 8.10 ผลการเชื่อมโยงผ่านการตรวจสอบและรับรองจากผู้เชี่ยวชาญก่อนเผยแพร่ทุกครั้ง

2.2.2 กรอบการทำงาน NIST Cybersecurity Framework 2.0

NIST CSF 2.0 เป็นกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (NIST) ฉบับ 2.0 ที่ประกาศใช้ใน ค.ศ. 2024 เพิ่มฟังก์ชันการกำกับดูแล (Govern: GV) เป็นแกนกลาง ซึ่งเน้นการกำหนดนโยบาย กลยุทธ์ และบทบาทหน้าที่จากระดับบริหาร รวมเป็น 6 ฟังก์ชันหลัก [3]

ฟังก์ชัน	จุดมุ่งเน้น	Subcategories ที่เชื่อมโยงกับกฎหมายไทย
Govern (GV)	นโยบายและกลยุทธ์ระดับบริหาร	GV.OC-03 ความต้องการทางกฎหมาย · GV.PO-01 นโยบาย · GV.SC-04 ห่วงโซ่อุปทาน
Identify (ID)	ทำความเข้าใจทรัพยากรและความเสี่ยง	ID.AM-01/02 รายการทรัพย์สิน · ID.RA-01 ประเมินความเสี่ยง
Protect (PR)	วางมาตรการป้องกัน	PR.AA-01–06 การยืนยันตัวตน · PR.DS-01/02 คุ้มครองข้อมูล · PR.PT-01 บันทึก
Detect (DE)	เฝ้าระวังและตรวจจับ	DE.CM-01/06 ติดตามเครือข่าย · DE.AE-02/03 วิเคราะห์เหตุการณ์
Respond (RS)	ตอบสนองเมื่อเกิดเหตุ	RS.MA-01/02 จัดการเหตุการณ์ · RS.CO-02/03 สื่อสาร · RS.MI-01 กักกัน
Recover (RC)	กู้คืนระบบและบริการ	RC.RP-01–03 แผนกู้คืน · GV.OC-04 ความต่อเนื่องทางธุรกิจ

ตารางที่ 2-3 6 ฟังก์ชันของ NIST CSF 2.0 และ Subcategories ที่เกี่ยวข้องกับกฎหมายไทย

ประโยชน์ของการเชื่อมโยงกับ NIST CSF 2.0 คือช่วยให้ฝ่ายไอทีสามารถสื่อสารความเสี่ยงทางกฎหมายให้ผู้บริหารเข้าใจได้ง่ายขึ้น โดยระบุว่ากฎหมายแต่ละมาตราส่งผลต่อวงจรความมั่นคงปลอดภัย (Cybersecurity Lifecycle) ในขั้นตอนใด ซึ่งต่างจากการอ่านตัวบทกฎหมายโดยตรง

2.3 เทคโนโลยีการประมวลผลภาษาธรรมชาติสำหรับกฎหมายไทย

2.3.1 สถาปัตยกรรม Transformer และกลไก Self-Attention

Transformer คือสถาปัตยกรรมโครงข่ายประสาทเทียมที่ Vaswani และคณะเสนอใน ค.ศ. 2017 [ก4] กลไกหลักคือ Self-Attention ซึ่งช่วยให้โมเดลประเมินความสำคัญของคำแต่ละคำเทียบกับคำอื่นในประโยคเดียวกัน แทนที่จะอ่านตามลำดับเหมือนโมเดลแบบ Recurrent ข้อได้เปรียบสำหรับภาษากฎหมายไทย ได้แก่

2.3.1.1 จัดการประโยคยาวได้ดี เนื่องจากกฎหมายไทยมักใช้ประโยคยาวที่มีส่วนขยายซ้อนหลายชั้น

2.3.1.2 จับความสัมพันธ์ระยะไกลได้ เช่น มาตราที่อ้างอิงถึงนิยามที่ให้ไว้ในมาตราอื่น

2.3.1.3 ไม่ต้องพึ่งการตัดคำ เนื่องจากภาษาไทยไม่มีช่องว่างระหว่างคำ

BERT (Bidirectional Encoder Representations from Transformers) เป็นโมเดลที่พัฒนาจาก Transformer โดยอ่านข้อความทั้งจากซ้ายไปขวาและจากขวาไปซ้ายพร้อมกัน ทำให้เข้าใจบริบทได้ดีขึ้นสำหรับงานจำแนกประเภทและสกัดข้อมูล [5]

2.3.2 โมเดล WangchanBERTa และความเหมาะสมสำหรับกฎหมายไทย

WangchanBERTa เป็นโมเดลภาษาไทยที่พัฒนาโดยทีม VISTEC ฝึกด้วยชุดข้อมูล Thai Wikipedia, Thai web crawl, Thai news และเอกสารภาครัฐ รวมกว่า 78 กิกะไบต์ มีสถาปัตยกรรม RoBERTa ซึ่งปรับปรุงจาก BERT ให้มีประสิทธิภาพดีขึ้นสำหรับงาน Downstream [5]

ความโดดเด่นของ WangchanBERTa สำหรับงานวิจัยนี้ได้แก่ การจัดการภาษาทางการและคำศัพท์ราชการที่พบในเอกสารกฎหมายได้ดีกว่าโมเดลทั่วไป เนื่องจากชุดข้อมูลฝึกมีเอกสารราชการและข่าวสารจำนวนมาก อย่างไรก็ตาม โมเดลยังเป็นเวอร์ชันพื้นฐานที่ยังไม่ได้ปรับแต่งเฉพาะสำหรับภาษากฎหมายไทยโดยตรง ความแม่นยำของการจำแนกประเภทและสกัดข้อมูลจะเพิ่มขึ้นเมื่อมีข้อมูลที่ผู้เชี่ยวชาญทำเครื่องหมายไว้เพียงพอสำหรับการปรับแต่งเพิ่มเติมในระยะต่อไป

2.3.3 การสกัดข้อมูลสำคัญจากกฎหมาย (Named Entity Recognition)

Named Entity Recognition (NER) คือกระบวนการระบุและจำแนกข้อมูลสำคัญในข้อความ เช่น ชื่อ วันที่ สถานที่ และองค์กร ในบริบทกฎหมายไซเบอร์ไทย งานวิจัยนี้กำหนด Entity ที่ต้องสกัด 5 ประเภทเฉพาะ

2.3.3.1 ชื่อกฎหมาย (LAW_NAME) เช่น "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550"

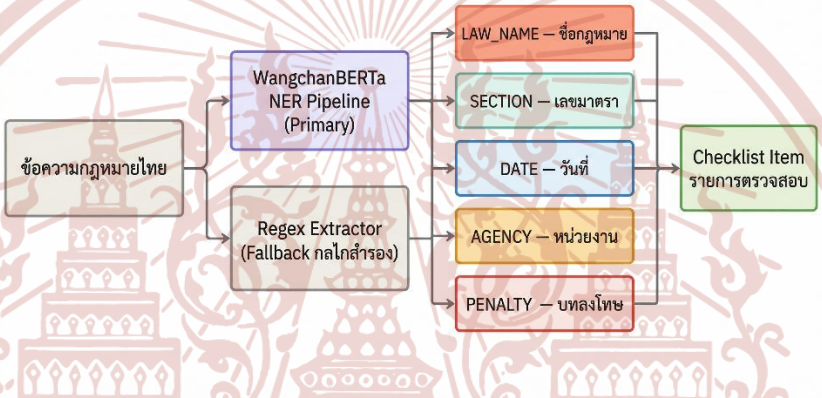
2.3.3.2 เลขมาตรา (SECTION) เช่น "มาตรา 26", "มาตรา 37", "หมวด 3"

2.3.3.3 วันที่ (DATE) วันประกาศ วันบังคับใช้ เช่น "18 มิถุนายน 2550"

2.3.3.4 หน่วยงาน/ผู้ที่ต้องปฏิบัติ (AGENCY) เช่น "ผู้ให้บริการ", "สำนักงาน กสทช."

2.3.3.5 บทลงโทษ (PENALTY) เช่น "ระวางโทษปรับไม่เกินห้าแสนบาท", "จำคุกไม่เกินสามปี"

ระบบใช้ WangchanBERTa NER pipeline เป็นวิธีหลัก โดยมีตัวสกัดแบบรูปแบบข้อความเป็นกลไกสำรองที่ทำงานได้ตลอดเวลา



ภาพที่ 2-1 แผนภาพกระบวนการสกัดข้อมูลสำคัญจากกฎหมายไซเบอร์ไทย

2.3.4 ปัญหาพิเศษของภาษากฎหมายไทยในการประมวลผล

ภาษากฎหมายไทยมีลักษณะพิเศษที่ท้าทายระบบ NLP มากกว่าภาษากฎหมายอังกฤษหลายประการ

2.3.4.1 ประโยครวมภาระหน้าที่กับบทลงโทษ กฎหมายไทยมักเขียน "ผู้ใด...กระทำ...ต้องระวางโทษ" รวมกัน ทำให้ระบบต้องมีกลไก split-clause logic เพื่อแยกส่วนที่เป็นภาระหน้าที่ออกจากบทลงโทษ

2.3.4.2 ไม่มีช่องว่างระหว่างคำ ภาษาไทยไม่ใช้ช่องว่างคั่นคำ การตัดคำจึงต้องอาศัยโมเดลภาษาที่เข้าใจบริบท

2.3.4.3 การอ้างอิงข้ามมาตราหลายทอด เช่น "ให้นำบทบัญญัติตามมาตรา X มาใช้บังคับโดยอนุโลม" ทำให้การสกัดข้อมูลต้องติดตามการอ้างอิงไปยังมาตราอื่น

2.3.4.4 คำศัพท์เฉพาะและไม่มีมาตรฐาน คำเดียวกันอาจมีการสะกดต่างกันในเอกสารต่างฉบับ เช่น "ผู้ให้บริการ" และ "ผู้ให้บริการอินเทอร์เน็ต" หมายถึงกลุ่มเดียวกัน

2.3.4.5 ปัญหา OCR ภาษาไทย เอกสาร PDF ที่สแกนจากกระดาษมักมีสระหลุด วรรณยุกต์ผิดตำแหน่ง หรือสระอำที่แยกเป็น 2 ตัวอักษร

2.4 การออกแบบ AI Pipeline สำหรับการประมวลผลเอกสารกฎหมาย

2.4.1 แนวคิด Hybrid AI Pipeline

การออกแบบระบบ AI สำหรับงานกฎหมายที่มีความสำคัญสูงต้องพิจารณาสมดุลระหว่างความแม่นยำ ความสามารถในการอธิบายผล และความน่าเชื่อถือ แนวทาง Hybrid ที่รวมกฎเกณฑ์แบบ Rule-Based กับโมเดลภาษาได้รับการพิสูจน์ว่าให้ผลดีกว่าการใช้วิธีใดวิธีหนึ่งเพียงอย่างเดียว โดยเฉพาะในงานที่ต้องการความสามารถในการตรวจสอบย้อนหลัง [12]
งานวิจัยนี้ออกแบบ Pipeline 7 ขั้นตอนที่มีลักษณะเด่น 3 ประการ ได้แก่

2.4.1.1 Deterministic at core ขั้นที่ 1–3 ใช้กฎเกณฑ์ที่ผลลัพธ์สามารถทำซ้ำได้และอธิบายได้ ไม่ขึ้นอยู่กับความน่าจะเป็นของโมเดล

2.4.1.2 LLM-augmented ขั้นที่ 4–5 ใช้ Large Language Model เสริมเมื่อมีการเชื่อมต่อบริการ เพื่อเพิ่มคุณภาพผลลัพธ์

2.4.1.3 Always-available fallback ทุกขั้นตอนมีกลไกสำรองที่ทำงานได้ในทุกสภาพแวดล้อม แม้ไม่มีอินเทอร์เน็ตหรืออุปกรณ์ GPU

2.4.2 กลไกสะสมกฎการแก้ไขจากผู้เชี่ยวชาญ

งานวิจัยนี้ออกแบบกลไกปรับปรุงระบบอย่างต่อเนื่องผ่านการสะสมกฎการแก้ไขข้อความ (Rule Learning) ซึ่งต่างจากวิธีการ Fine-tuning Neural Network ที่ต้องการข้อมูล annotated จำนวนมากและทรัพยากรการประมวลผลสูง กลไกนี้ทำงานใน 3 ระดับ

2.4.2.1 ระดับประโยค จำรูปแบบการแทนที่ทั้งประโยคสำหรับกรณีที่พบซ้ำบ่อย

2.4.2.2 ระดับคำ สร้างพจนานุกรมคำที่มักพิมพ์ผิดหรือ OCR อ่านผิด เช่น "หามมิให้" ปรับเป็น "ห้ามมิให้"

2.4.2.3 ระดับตัวอักษร แก้ไขปัญหาช่องว่างที่หลุดเข้ามาในคำ เช่น "ต้ อง" ปรับเป็น "ต้อง"
กฎที่สะสมถูกบันทึกในไฟล์ JSON ที่คงอยู่แม้ container รีสตาร์ท และถูกนำไปใช้โดยอัตโนมัติในขั้นตอนการแก้ไขข้อความของทุกเอกสารที่ประมวลผลในอนาคต

2.4.3 กระบวนการตรวจสอบโดยผู้เชี่ยวชาญหลายท่าน

เพื่อรับประกันคุณภาพของรายการตรวจสอบก่อนเผยแพร่ งานวิจัยนี้ออกแบบกระบวนการที่ต้องมีผู้เชี่ยวชาญอย่างน้อย 3 ท่านตรวจสอบและให้ความเห็นชอบ แนวทางนี้สอดคล้องกับหลักการ Human-in-the-Loop ที่เน้นความสำคัญของการตัดสินใจของมนุษย์ในระบบ AI ที่ส่งผลต่อการตัดสินใจสำคัญ [10]

ผลการตรวจสอบทุกรอบถูกบันทึกพร้อมรอบการตรวจสอบ (Review Round) ทำให้สามารถสืบค้นประวัติการตัดสินใจได้ และทุกรายการตรวจสอบสามารถ trace กลับไปยังมาตรากฎหมายต้นทางได้ ซึ่งเป็นหลักการสำคัญของ Explainable AI ในงานที่ต้องรับผิดชอบได้ [12]

2.4.4 Compliance Automation และการตรวจสอบย้อนหลัง

แนวคิด Compliance Automation คือการใช้เทคโนโลยีเพื่อลดการพึ่งพามนุษย์ในกระบวนการกำกับดูแลที่ซ้ำซ้อน Tiwari และ Shanmugam [2] ชี้ว่าระบบที่ดีต้องสร้างเอกสารหลักฐานที่ตรวจสอบย้อนหลังได้ (Audit Trail) ควบคู่กับการทำงานอัตโนมัติ ระบบที่พัฒนาขึ้นรองรับหลักการนี้ผ่านบันทึกกิจกรรมทุกอย่างในระบบ (Audit Log) รวมถึงเวลา ผู้ดำเนินการ และการเปลี่ยนแปลงที่เกิดขึ้น, ประวัติการตรวจสอบของผู้เชี่ยวชาญแต่ละท่าน พร้อมความเห็นและการแก้ไขที่เสนอ และบันทึกสถานะการปฏิบัติตามขององค์กร พร้อมหลักฐานที่แนบและวันที่บันทึก

2.5 การทบทวนงานวิจัยที่เกี่ยวข้อง

2.5.1 กรอบนโยบายและแนวปฏิบัติกฎหมายไซเบอร์ไทย

สำนักงานพัฒนารัฐบาลดิจิทัล (DGA) ได้จัดทำกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลของไทย เป็นมาตรฐานกลางสำหรับหน่วยงานภาครัฐ [1] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ออกแนวปฏิบัติสำหรับองค์กรขนาดกลางและเล็ก [4], [7] และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) กำหนดมาตรการระดับชาติ [8] งานวิจัยนี้นำแนวปฏิบัติเหล่านี้มาใช้เป็นฐานในการออกแบบหมวดหมู่รายการตรวจสอบและพจนานุกรมการเชื่อมโยงมาตรฐาน

2.5.2 การประยุกต์ใช้ AI และ NLP ในงานกฎหมายและ Compliance

Nithya และคณะ [5] พบว่าระบบ AI สามารถสกัดข้อมูลสำคัญจากตัวบทกฎหมายได้อย่างมีประสิทธิภาพ และยกระดับกระบวนการทางกฎหมายให้แม่นยำขึ้น Annu และ Audichya [9] เสนอการใช้ Machine Learning วิเคราะห์บรรทัดฐานทางกฎหมายเพื่อทำนายผลการตัดสินในคดีไซเบอร์ ซึ่งแสดงให้เห็นศักยภาพของ AI ในบริบทกฎหมายไทย Shaik และคณะ [6] พิสูจน์ว่าโมเดลภาษาสามารถตรวจสอบข้อบังคับจำนวนมากได้โดยอัตโนมัติ

Tiwari และ Shanmugam [2] ชี้ให้เห็นว่าการจัดการ Compliance ต้องควบคู่กับระบบเอกสารที่ตรวจสอบย้อนหลังได้ การนำ AI มาช่วยในภาค Regulated Industries ช่วยลดความเสี่ยงจากการตีความผิด [3] งานวิจัยด้าน Multi-Layered Intelligence Framework [10] แสดงให้เห็นว่าการบูรณาการกระบวนการตรวจสอบหลายระดับยกระดับความน่าเชื่อถือของระบบ AI ที่ใช้ในงานกำกับดูแล

งานวิจัยด้าน Hybrid XAI [12] แสดงว่าระบบที่รวม Rule-Based กับ AI ให้ความแม่นยำสูงและสามารถอธิบายเหตุผลของผลลัพธ์ในระดับมาตราได้ ซึ่งเป็นหัวใจของงานวิจัยนี้ เนื่องจากทุกรายการตรวจสอบสามารถสืบค้นกลับไปยังมาตรากฎหมายต้นทางได้

2.5.3 เปรียบเทียบงานวิจัยและช่องว่างที่งานวิจัยนี้แก้ไข

ตารางที่ 2.4 สรุปการเปรียบเทียบงานวิจัยที่เกี่ยวข้องกับระบบที่พัฒนาขึ้นในงานวิจัยนี้ ใน 5 มิติหลัก

งานวิจัย	แนวทาง	Thai Law NLP	ISO/NIST Mapping	Multi-Expert	Continuous Improvement
Nithya et al. [5]	AI/NLP สกัดข้อมูลกฎหมาย	✓ ทำได้	✗ ไม่มี	✗ ไม่มี	✗ ไม่มี
Annu & Audichya [9]	ML วิเคราะห์คดีไซเบอร์	✓ ทำได้	✗ ไม่มี	✗ ไม่มี	✗ ไม่มี
Shaik et al. [6]	ML ตรวจสอบข้อบังคับ	✗ ไม่ใช่ไทย	✓ มี Framework	✗ ไม่มี	✗ ไม่มี
Tiwari & Shanmugam [2]	Compliance Automation	✗ ไม่ใช่ไทย	✗ ไม่มี	✗ ไม่มี	✓ มีระบบเอกสาร
Hybrid XAI [12]	Rule-Based + AI อธิบายผล	✗ ไม่ใช่ไทย	✓ Article-level trace	✗ ไม่มี	✗ ไม่มี
งานวิจัยนี้	Hybrid Pipeline 7 ขั้น + WangchanBERTa	✓ กฎหมายไทย 3 ฉบับ	✓ ISO 27001+NIST CSF	✓ 3-Expert Threshold	✓ Rule Learning สะสม

ตารางที่ 2-4 เปรียบเทียบงานวิจัยที่เกี่ยวข้องกับระบบที่พัฒนาขึ้น

จากตารางที่ 2.4 เห็นได้ว่างานวิจัยก่อนหน้าแต่ละชิ้นมีจุดแข็งในด้านใดด้านหนึ่ง แต่ยังไม่มีงานใดที่ครอบคลุมครบทั้ง 5 มิติพร้อมกัน โดยเฉพาะการทำงานกับกฎหมายไทยโดยเฉพาะ งานวิจัยนี้จึงมุ่งแก้ไขช่องว่าง 3 ประการหลัก ได้แก่

2.5.3.1 การเชื่อมโยงอัตโนมัติกับทั้ง ISO/IEC 27001:2022 และ NIST CSF 2.0 พร้อมกันในระบบเดียว สำหรับกฎหมายไซเบอร์ไทยโดยเฉพาะ

2.5.3.2 กระบวนการตรวจสอบโดยผู้เชี่ยวชาญหลายท่าน (Multi-Expert Validation) ที่สามารถตรวจสอบย้อนหลังได้ในทุกระดับ

2.5.3.3 กลไกปรับปรุงระบบอย่างต่อเนื่องจากความเห็นของผู้เชี่ยวชาญผ่านการสะสมกฎการแก้ไขข้อความ

งานวิจัยนี้จึงเป็นการบูรณาการแนวคิด Compliance Automation [2], [6], Thai Legal NLP [5], [9], ระบบที่อธิบายผลได้ [12] และกรอบนโยบายไทย [1], [7], [8] เพื่อพัฒนาระบบต้นแบบที่ใช้งานได้จริงในองค์กรไทย



ภาพที่ 2-2 แผนภาพแสดงความสัมพันธ์ระหว่างทฤษฎีและเทคโนโลยีที่ใช้ในงานวิจัย

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยเรื่อง "ระบบปัญญาประดิษฐ์สำหรับสกัดและเชื่อมโยงข้อกำหนดกฎหมายไซเบอร์ไทยเพื่อสร้างรายการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ" เป็นงานวิจัยและพัฒนา (Research and Development) ที่ประยุกต์ใช้เทคโนโลยีการประมวลผลภาษาธรรมชาติเพื่อแก้ปัญหาความซับซ้อนในการตีความกฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย กระบวนการดำเนินงานประกอบด้วย 9 ขั้นตอนหลักครอบคลุมตั้งแต่การรวบรวมข้อมูลไปจนถึงการประเมินผล

3.1 การรวบรวมและจัดเตรียมเอกสารกฎหมาย

3.1.1 การคัดเลือกแหล่งข้อมูล

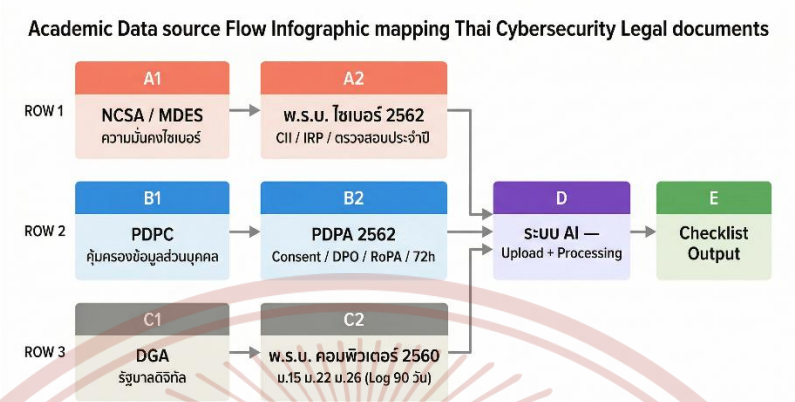
ผู้วิจัยรวบรวมตัวบทกฎหมาย ประกาศ และแนวปฏิบัติฉบับล่าสุดจากหน่วยงานกำกับดูแลโดยตรง เพื่อป้องกันความคลาดเคลื่อนของข้อมูล การเลือกแหล่งข้อมูลเป็นขั้นตอนสำคัญ เนื่องจากกฎหมายที่ผ่านการแก้ไขหลายรอบอาจมีฉบับที่ล้าสมัยเผยแพร่อยู่บนอินเทอร์เน็ต ผู้วิจัยจึงยึดแหล่งข้อมูลหลัก 3 กลุ่ม

3.1.1.1 ด้านความมั่นคงปลอดภัยไซเบอร์ ดำเนินการรวบรวมจากสำนักงาน NCSA และกระทรวง MDES โดยตรง ครอบคลุมทั้งตัวบทหลักและประกาศลำดับรองที่กำหนดมาตรการสำหรับหน่วยงาน CII

3.1.1.2 ด้านการคุ้มครองข้อมูลส่วนบุคคล ดำเนินการรวบรวมจากสำนักงาน PDPC ทั้งตัวบทกฎหมายหลักและแนวปฏิบัติด้านความปลอดภัยของข้อมูลส่วนบุคคล

3.1.1.3 ด้านโครงสร้างพื้นฐานรัฐบาลดิจิทัล ดำเนินการรวบรวมแนวปฏิบัติจาก DGA ใช้เป็นฐานเปรียบเทียบมาตรฐานของหน่วยงานภาครัฐ

เกณฑ์การคัดเลือกเนื้อหากำหนดว่าต้องเป็นข้อกำหนดที่บังคับใช้อยู่ในปัจจุบัน มีบทลงโทษที่ชัดเจน และเกี่ยวข้องกับระบบสารสนเทศขององค์กร



ภาพที่ 3-1 แหล่งที่มาของเอกสารกฎหมายและหน่วยงานกำกับดูแล

3.1.2 กระบวนการอัปโหลดและประมวลผลเอกสาร

ระบบรองรับการอัปโหลดเอกสาร PDF ผ่านเจ้าหน้าที่ฝ่ายกำกับดูแล โดยระบบจัดเก็บไฟล์ในคลังข้อมูล MinIO และส่งข้อมูล path ให้ตัวประมวลผล AI ดำเนินการต่อ มีขั้นตอนหลัก 4 ขั้น

3.1.2.1 การสกัดข้อความ คือขั้นตอนที่ตัวประมวลผล AI แปลง PDF เป็นข้อความดิบผ่านกระบวนการ OCR-aware extraction จากนั้นดำเนินการแก้ไขข้อผิดพลาดโดยอัตโนมัติ เช่น สระหลุด วรรณยุกต์ผิดตำแหน่ง สระอำที่แตกเป็น 2 ตัวอักษร และช่องว่างที่หลุดเข้ามาในคำ พร้อมบันทึกความแม่นยำของการแปลง

3.1.2.2 การตรวจสอบข้อความ คือขั้นตอนที่เจ้าหน้าที่ตรวจสอบข้อความทีละมาตราผ่านหน้าจอที่แสดงข้อความต้นฉบับและข้อความที่สกัดไว้เคียงกัน เจ้าหน้าที่สามารถแก้ไขข้อความก่ออนุมัติ การแก้ไขทุกครั้งถูกบันทึกเป็นบันทึกการแก้ไขข้อความเพื่อนำไปสร้างกฎสะสมอัตโนมัติ

3.1.2.3 การทบทวนการเชื่อมโยงมาตรฐาน คือขั้นตอนที่เจ้าหน้าที่ทบทวนการจับคู่ ISO/NIST ที่ AI สร้างขึ้น สามารถแก้ไขหรือเพิ่มการเชื่อมโยงได้ก่อนส่งต่อผู้เชี่ยวชาญ

3.1.2.4 การติดตามสถานะ คือขั้นตอนที่ระบบบันทึกสถานะของเอกสารแบบเรียลไทม์ผ่าน 13 ระยะตั้งแต่เริ่มอัปโหลดจนถึงได้รับการอนุมัติเผยแพร่

3.1.3 การทำความสะอาดและจัดระเบียบข้อมูล

หลังจากสกัดข้อความแล้ว ตัวประมวลผล AI ดำเนินการทำความสะอาดข้อมูลในหลายระดับ ดังนี้

ระดับเอกสาร ได้แก่ การขจัดเลขหน้า หัวกระดาษ ท้ายกระดาษ ชื่อผู้ออกประกาศ และสัญลักษณ์พิเศษที่เกิดจากการแปลงไฟล์ เช่น อักขระควบคุม หรือ encoding artifacts ที่ทำให้ข้อความอ่านไม่ออก

ระดับส่วน ได้แก่ การแบ่งข้อความตามโครงสร้างมาตรากฎหมาย โดยระบบจะระบุส่วนหัวมาตรา เลขมาตรา หมวดหมู่ และเนื้อความ การแบ่งส่วนนี้สำคัญมากเพราะกำหนดหน่วยของรายการตรวจสอบแต่ละรายการ

ระดับประโยค ได้แก่ การระบุประโยคที่มีภาระหน้าที่ (obligation sentences) ออกจากประโยคบริบท คำนิยาม หรือบทลงโทษ โดยใช้ชุดรูปแบบที่พัฒนาขึ้นเฉพาะสำหรับโครงสร้างประโยคกฎหมายไทย

3.2 การออกแบบโครงสร้างข้อมูล

3.2.1 โครงสร้างรายการตรวจสอบ

แต่ละมาตรากฎหมายถูกแปลงเป็นรายการตรวจสอบในฐานข้อมูล ซึ่งเก็บข้อมูลสำคัญ 6 รายการ ดังนี้

3.2.1.1 สิ่งที่ต้องดำเนินการ รายการในภาษาปฏิบัติงานที่เข้าใจง่าย ไม่ใช่การคัดลอกข้อความกฎหมาย

3.2.1.2 หลักฐานที่ต้องมี รายการที่ระบุทั้งชื่อภาษาไทยและภาษาอังกฤษ

3.2.1.3 มาตรฐาน ISO/IEC 27001:2022 ที่เกี่ยวข้อง

3.2.1.4 มาตรฐาน NIST CSF 2.0 ที่เกี่ยวข้อง

3.2.1.5 บทลงโทษ และประเภทองค์กรที่ต้องปฏิบัติตาม

3.2.1.6 วันที่ประกาศและวันที่มีผลบังคับใช้

3.2.2 ประเภทข้อมูลสำคัญที่สกัดจากกฎหมาย

ระบบสกัดข้อมูลสำคัญ 5 ประเภทจากกฎหมายไซเบอร์ไทย ได้แก่ ชื่อกฎหมาย เลขมาตรา วันที่ประกาศหรือบังคับใช้ หน่วยงานที่เกี่ยวข้อง และบทลงโทษ โดยมีโมเดล WangchanBERTa เป็นตัวหลักและรูปแบบข้อความเป็นกลไกสำรอง

3.2.3 กลไกสะสมกฎการแก้ไขข้อความ

เมื่อเจ้าหน้าที่หรือผู้เชี่ยวชาญแก้ไขข้อความที่สกัดได้ ระบบจะวิเคราะห์การแก้ไขและสร้างกฎอัตโนมัติเพื่อนำไปใช้กับเอกสารที่ประมวลผลต่อไป กฎแบ่งเป็น 3 ระดับ

3.2.3.1 ระดับประโยค คือจำรูปแบบการแทนที่ทั้งประโยคสำหรับกรณีเฉพาะ

3.2.3.2 ระดับคำ คือแก้ไขคำหรือวลีที่พบข้อผิดพลาดบ่อยครั้ง

3.2.3.3 ระดับตัวอักษร คือแก้ไขปัญหาระดับอักขระ เช่น ช่องว่างที่หลุดเข้ามาในคำ

กฎที่สะสมได้จะถูกนำไปใช้แก้ไขข้อความในเอกสารที่ประมวลผลต่อไปทุกครั้งโดยอัตโนมัติ ช่วยให้การแปลง PDF มีความแม่นยำเพิ่มขึ้นตามปริมาณการแก้ไขที่สะสม

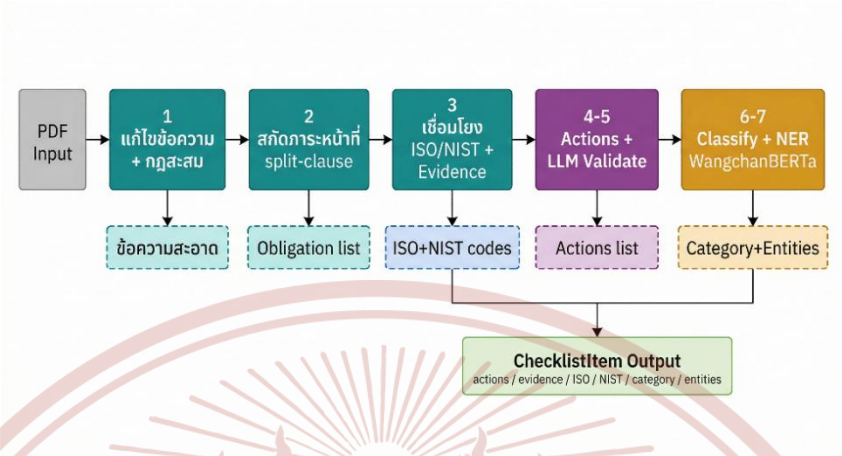
3.3 การออกแบบสถาปัตยกรรมระบบ

3.3.1 กระบวนการประมวลผล AI 7 ขั้นตอน

ตัวประมวลผล AI ทำงานผ่าน 7 ขั้นตอนต่อเนื่อง ทุกขั้นตอนมีกลไกสำรองเพื่อให้ระบบทำงานได้ในทุกสภาพแวดล้อม แม้ไม่มีอุปกรณ์ประมวลผลพิเศษหรือการเชื่อมต่อบริการภายนอก

ขั้นที่	ชื่อขั้นตอน	รายละเอียด	วิธีหลัก	กลไกสำรอง
1	แก้ไขข้อความ	แก้ไขปัญหาจากการแปลง PDF เช่น สระหลุด วรรณยุกต์ผิดตำแหน่ง สระอำแยก พร้อมนำกฎที่สะสมจากผู้เชี่ยวชาญมาใช้	กฎเกณฑ์	—
2	สกัดภาระหน้าที่	แยกประโยคที่กำหนดภาระหน้าที่ออกจากบทลงโทษที่มักเขียนรวมกันในกฎหมายไทย	กฎเกณฑ์	—
3	เชื่อมโยงมาตรฐาน	จับคู่ข้อกำหนดกับ ISO/IEC 27001:2022 และ NIST CSF 2.0 พร้อมระบุหลักฐานที่ต้องมี	กฎเกณฑ์	—
4	สร้างรายการปฏิบัติ	แปลงข้อกำหนดเป็นรายการสิ่งที่ต้องดำเนินการในภาษาปฏิบัติงาน	กฎเกณฑ์	โมเดลภาษา
5	ตรวจสอบด้วย AI	ส่งผลลัพธ์ให้บริการโมเดลภาษาตรวจสอบและเสริมความสมบูรณ์	โมเดลภาษา	กฎเกณฑ์
6	จัดหมวดหมู่	จำแนกข้อกำหนดเป็นหมวดหมู่ เช่น การคุ้มครองข้อมูล การควบคุมการเข้าถึง	WangchanBERTa	คำสำคัญ
7	สกัดข้อมูล	สกัดข้อมูลสำคัญ 5 ประเภท ได้แก่ ชื่อกฎหมาย เลขมาตรา วันที่ หน่วยงาน บทลงโทษ	WangchanBERTa	รูปแบบข้อความ

ตารางที่ 3-1 กระบวนการประมวลผล AI 7 ขั้นตอน พร้อมวิธีหลักและกลไกสำรอง



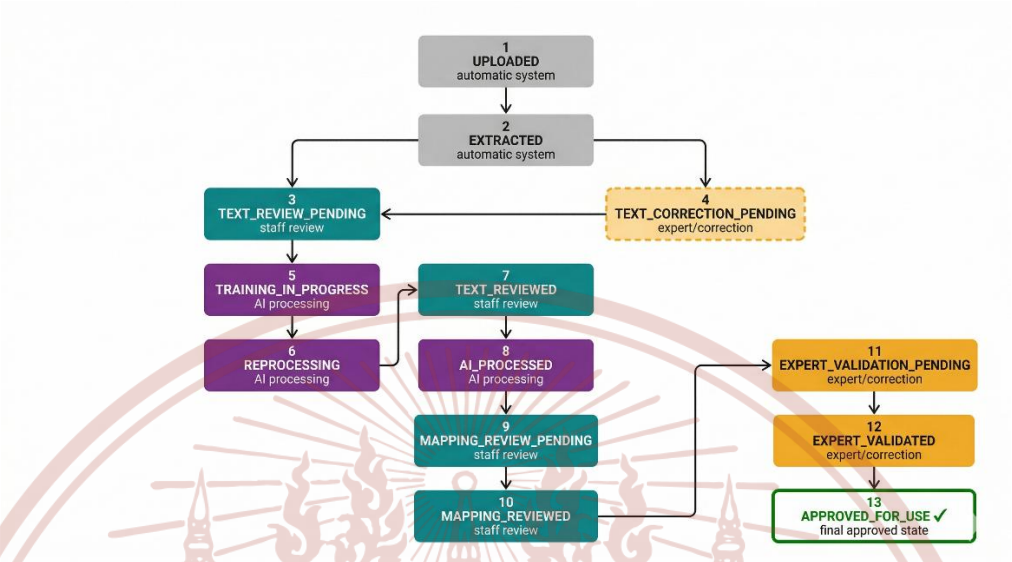
ภาพที่ 3-2 แผนภาพการไหลของข้อมูลในกระบวนการประมวลผล AI 7 ขั้นตอน

3.3.2 สถานะของเอกสารในระบบ

ระบบติดตามสถานะของเอกสารกฎหมายผ่าน 13 ระยะ ตั้งแต่รับเข้าจนถึงเผยแพร่ เพื่อให้ทุกฝ่ายทราบว่าเอกสารอยู่ในขั้นตอนใดและใครเป็นผู้รับผิดชอบต่อไป

สถานะ	ความหมาย	ผู้ดำเนินการ
อัปโหลดแล้ว	ไฟล์ PDF เข้าสู่ระบบเรียบร้อย	ระบบอัตโนมัติ
สกัดข้อความแล้ว	แปลง PDF เป็นข้อความและแก้ไขข้อผิดพลาดเบื้องต้น	ระบบอัตโนมัติ
รอตรวจสอบข้อความ	รอเจ้าหน้าที่ตรวจทานความถูกต้องของข้อความ	เจ้าหน้าที่ฝ่ายกำกับดูแล
แก้ไขข้อความแล้ว รอยืนยัน	เจ้าหน้าที่แก้ไขแล้ว รอการอนุมัติ	เจ้าหน้าที่ฝ่ายกำกับดูแล
ระบบกำลังเรียนรู้กฎใหม่	ประมวลผลกฎการแก้ไขข้อความใหม่	ระบบอัตโนมัติ
กำลังประมวลผลซ้ำ	นำกฎใหม่ไปใช้กับเอกสาร	ระบบอัตโนมัติ
ข้อความผ่านการตรวจสอบ	เจ้าหน้าที่อนุมัติข้อความแล้ว	เจ้าหน้าที่ฝ่ายกำกับดูแล
ประมวลผล AI แล้ว	AI สร้างรายการตรวจสอบครบถ้วน	ระบบอัตโนมัติ
รอทบทวนการเชื่อมโยง	รอเจ้าหน้าที่ทบทวน ISO/NIST	เจ้าหน้าที่ฝ่ายกำกับดูแล
ทบทวนการเชื่อมโยงแล้ว	เจ้าหน้าที่อนุมัติ ส่งต่อผู้เชี่ยวชาญ	เจ้าหน้าที่ฝ่ายกำกับดูแล
รอผู้เชี่ยวชาญตรวจสอบ	รอผู้เชี่ยวชาญอย่างน้อย 3 ท่าน	ผู้เชี่ยวชาญตรวจสอบ
ผ่านการตรวจสอบจากผู้เชี่ยวชาญ	ผู้เชี่ยวชาญ 3 ท่านอนุมัติโดยไม่มีการแก้ไข	ผู้เชี่ยวชาญตรวจสอบ
อนุมัติสำหรับการใช้งาน	ผู้ดูแลระบบเผยแพร่แล้ว พร้อมใช้งาน	ผู้ดูแลระบบ

ตารางที่ 3-2 สถานะของเอกสารกฎหมาย 13 ระยะในระบบ



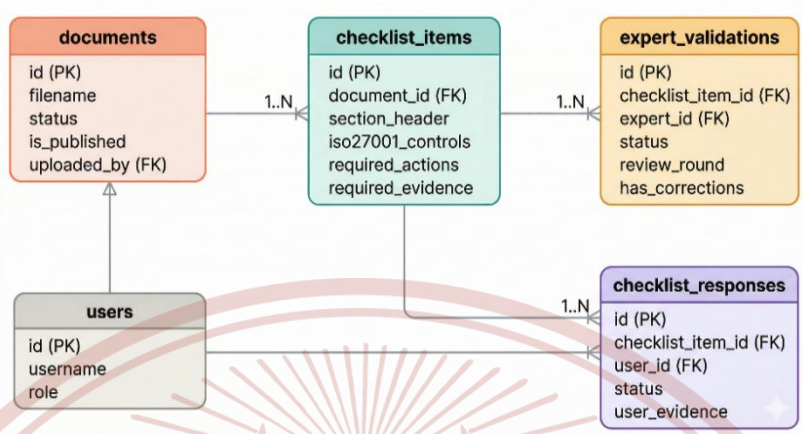
ภาพที่ 3-3 แผนภาพการเปลี่ยนสถานะของเอกสาร 13 ระยะ

3.3.3 โครงสร้างฐานข้อมูล

ระบบใช้ฐานข้อมูลเชิงสัมพันธ์ที่ออกแบบผ่านชุดการปรับโครงสร้าง 16 รอบ ประกอบด้วยตารางหลัก 7 ตาราง

ตาราง	ข้อมูลที่จัดเก็บ
เอกสาร	ชื่อไฟล์ สถานะ ข้อความที่สกัด ข้อความที่แก้ไข ความแม่นยำของการแปลง และข้อมูล Metadata
รายการตรวจสอบ	ข้อกำหนดแต่ละมาตรา รวมถึงสิ่งที่ต้องดำเนินการ หลักฐานที่ต้องมี มาตรฐาน ISO/NIST ที่เกี่ยวข้อง บทลงโทษ และผู้ที่ต้องปฏิบัติตาม
ผลการตรวจสอบ	ผลของผู้เชี่ยวชาญแต่ละท่าน รวมถึงสถานะ ความเห็น การแก้ไขที่เสนอ และรอบการตรวจสอบ
การตอบรับของผู้ใช้	สถานะการปฏิบัติตาม (ดำเนินการแล้ว กำลังดำเนินการ เสร็จสมบูรณ์ ไม่เกี่ยวข้อง) พร้อมหลักฐานที่แนบ
บันทึกกิจกรรม	กิจกรรมทุกอย่างในระบบ ผู้ดำเนินการ การกระทำ เวลา และ IP
ผู้ใช้งาน	ชื่อ อีเมล บทบาท แผนก และองค์กร
กฎการเชื่อมโยง	กฎเพิ่มเติมที่เจ้าหน้าที่สามารถเพิ่มเองสำหรับการจับคู่มาตรฐาน ISO/NIST

ตารางที่ 3-3 ตารางหลักในฐานข้อมูลและข้อมูลที่จัดเก็บ



ภาพที่ 3-4 แผนภาพความสัมพันธ์ระหว่างตารางหลักในฐานข้อมูล

3.4 กระบวนการตรวจสอบโดยผู้เชี่ยวชาญ

รายการตรวจสอบทุกชุดต้องผ่านการรับรองจากผู้เชี่ยวชาญก่อนเผยแพร่ เพื่อรับประกันความถูกต้องของการเชื่อมโยงมาตรฐานและความเหมาะสมของรายการปฏิบัติ

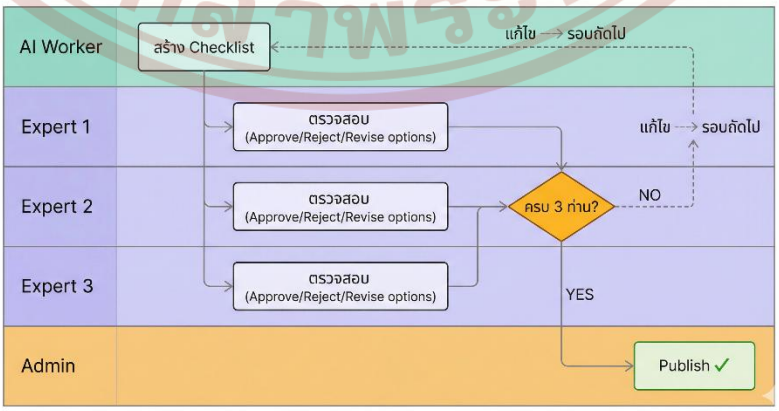
3.4.1 ขั้นตอนการตรวจสอบ

3.4.1.1 การตรวจสอบ โดยผู้เชี่ยวชาญตรวจสอบรายการแต่ละข้อ สามารถแก้ไขการเชื่อมโยงมาตรฐาน รายการสิ่งที่ต้องดำเนินการ การจัดหมวดหมู่ และเพิ่มความเห็น

3.4.1.2 การบันทึกผล โดยผลการตรวจสอบของผู้เชี่ยวชาญแต่ละท่านถูกบันทึกพร้อมสถานะ (อนุมัติ / ปฏิเสธ / ต้องแก้ไข) ความเห็น และรอบการตรวจสอบ

3.4.1.3 เงื่อนไขผ่าน โดยต้องมีผู้เชี่ยวชาญอย่างน้อย 3 ท่านอนุมัติ หากมีการแก้ไขจะเข้ารอบการพิจารณาเพิ่มเติม

3.4.1.4 การเผยแพร่ โดยผู้ดูแลระบบตรวจสอบผลสุดท้ายและอนุมัติการเผยแพร่ให้องค์กรใช้งาน



ภาพที่ 3-5 กระบวนการตรวจสอบโดยผู้เชี่ยวชาญ 3 ท่าน

3.4.2 การบันทึกประวัติและการตรวจสอบย้อนหลัง

ทุกรายการตรวจสอบสามารถสืบค้นกลับไปยังมาตรากฎหมายต้นทางได้ ผู้เชี่ยวชาญสามารถดูประวัติการตรวจสอบทุกรอบ ซึ่งช่วยให้กระบวนการมีความโปร่งใสและตรวจสอบย้อนหลังได้ตามหลักการ Explainable AI [12]

3.5 การออกแบบระบบเชื่อมโยงมาตรฐานสากล

3.5.1 การสร้างพจนานุกรมการเชื่อมโยง

ผู้วิจัยวิเคราะห์เนื้อหากฎหมายทั้ง 3 ฉบับและสร้างพจนานุกรมเชื่อมโยงคำสำคัญไปยัง ISO/IEC 27001:2022 และ NIST CSF 2.0 ครอบคลุมหมวดหมู่หลัก เช่น การควบคุมการเข้าถึง การคุ้มครองข้อมูล การบันทึกและติดตาม การรับมือเหตุการณ์ และความต่อเนื่องทางธุรกิจ นอกจากนี้เจ้าหน้าที่ยังสามารถเพิ่มกฎการเชื่อมโยงเองได้ผ่านหน้าจัดการกฎ โดยไม่ต้องปรับปรุงระบบ

3.5.2 การจัดการกรณีที่มีความไม่แน่นอน

ในกรณีที่การเชื่อมโยงไม่ชัดเจน ระบบจะส่งรายการนั้นให้ผู้เชี่ยวชาญพิจารณาโดยอัตโนมัติ และบันทึกว่ารายการใดถูกแก้ไขเพื่อใช้ประเมินความแม่นยำของระบบในภายหลัง

3.6 การออกแบบการทดลองและเกณฑ์การวัดผล

งานวิจัยนี้วัดประสิทธิผลจากแหล่งข้อมูล 2 แหล่ง ได้แก่ แบบประเมินโดยผู้เชี่ยวชาญ 3 ท่าน และแบบประเมินความพึงพอใจจากองค์กรตัวอย่าง 5 แห่ง ทั้งสองชุดใช้มาตรวัด Likert 5 ระดับ (1 = น้อยที่สุด ถึง 5 = มากที่สุด) พร้อมคะแนนความพึงพอใจโดยรวมในมาตราส่วน 1–10

3.6.1 เกณฑ์การคัดเลือกผู้เชี่ยวชาญ

ผู้วิจัยคัดเลือกผู้เชี่ยวชาญ 3 ท่าน ที่มีคุณสมบัติครบตามเกณฑ์ขั้นต่ำดังตารางที่ 3-4 โดยกำหนดให้ครอบคลุมทั้ง 3 มุมมองหลัก ได้แก่ ด้านกฎหมายนิติศาสตร์ ด้านความมั่นคงปลอดภัยสารสนเทศ และด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การประเมินระบบมีความรอบด้านและสะท้อนมุมมองที่หลากหลาย

เกณฑ์คุณสมบัติ	รายละเอียด
ด้านความเชี่ยวชาญ	มีความรู้และประสบการณ์โดยตรงในสาขาใดสาขาหนึ่งต่อไปนี้ ได้แก่ กฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย การกำกับดูแลข้อมูลส่วนบุคคล (PDPA) มาตรฐาน ISO/IEC 27001 หรือ NIST CSF หรือการตรวจสอบระบบสารสนเทศ (IT Audit)

เกณฑ์คุณสมบัติ	รายละเอียด
ด้านประสบการณ์	มีประสบการณ์ทำงานในสาขาที่เกี่ยวข้องอย่างน้อย 5 ปีขึ้นไป สำหรับผู้เชี่ยวชาญที่เป็นนักวิชาการหรืออาจารย์ต้องมีผลงานวิชาการหรืองานวิจัยที่เกี่ยวข้อง
ด้านการศึกษา	มีวุฒิการศึกษาระดับปริญญาตรีขึ้นไปในสาขาที่เกี่ยวข้อง ได้แก่ นิติศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ วิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ
ด้านความครอบคลุม	กลุ่มผู้เชี่ยวชาญ 3 ท่านต้องครอบคลุมทั้ง 3 มุมมอง ได้แก่ (1) ผู้เชี่ยวชาญด้านกฎหมายและนิติศาสตร์ดิจิทัล (2) ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบสารสนเทศ (CISO/IT Security) และ (3) ผู้เชี่ยวชาญด้านการกำกับดูแลข้อมูลและ Compliance
ด้านความเป็นอิสระ	ไม่มีส่วนได้ส่วนเสียโดยตรงกับการพัฒนาระบบในงานวิจัยนี้ และสามารถให้ความเห็นได้อย่างอิสระและเป็นกลาง
ด้านความสมัครใจ	ยินยอมเข้าร่วมการประเมินด้วยความสมัครใจ เข้าใจวัตถุประสงค์ของงานวิจัย และสามารถทดลองใช้ระบบได้อย่างครบถ้วน

ตารางที่ 3-4 เกณฑ์การคัดเลือกผู้เชี่ยวชาญประเมินระบบ

3.6.2 แบบประเมินโดยผู้เชี่ยวชาญ

ผู้วิจัยเชิญผู้เชี่ยวชาญด้านกฎหมายความมั่นคงปลอดภัยไซเบอร์และการตรวจสอบระบบ 3 ท่าน ประเมินระบบผ่านแบบประเมิน 19 ข้อ แบ่งเป็น 4 หมวด

3.6.1.1 หมวด B ประเมินความถูกต้องของ AI Mapping (6 ข้อ) การจำแนกประเภทข้อกำหนด การเชื่อมโยง ISO/NIST ความครบถ้วนของสิ่งที่ต้องดำเนินการ ความเหมาะสมของหลักฐาน และการสกัดบทลงโทษ

3.6.1.2 หมวด C ประเมินความสะดวกในการใช้งาน (5 ข้อ) กระบวนการตรวจสอบ การแสดงผล เครื่องมือแก้ไข และความครบถ้วนของข้อมูล

3.6.1.3 หมวด D ประเมินความน่าเชื่อถือของกระบวนการตรวจสอบ (4 ข้อ) กระบวนการ 3 ท่าน การบันทึกประวัติ ความโปร่งใสของการปรับปรุง และการแบ่งรอบ

3.6.1.4 หมวด E ประเมินความเพียงพอของผลลัพธ์ (4 ข้อ) คุณภาพแผงข้อมูล ตัวชี้วัด ความเพียงพอสำหรับการตัดสินใจ และการลดภาระงาน

นอกจากนี้ผู้เชี่ยวชาญแต่ละท่านยังให้คะแนนความพึงพอใจโดยรวม (1–10) จุดเด่นและข้อเสนอแนะ

3.6.3 เกณฑ์การคัดเลือกองค์กรตัวอย่าง

ผู้วิจัยคัดเลือกองค์กรตัวอย่าง 5 แห่ง ที่ผ่านเกณฑ์การคัดเลือกตามตารางที่ 3-5 เพื่อให้ผลการประเมินสะท้อนความต้องการที่หลากหลายของผู้ใช้งานจริงในบริบทองค์กรไทย

เกณฑ์การคัดเลือก	รายละเอียด
ประเภทองค์กร	เป็นนิติบุคคลที่ดำเนินธุรกิจหรือให้บริการในประเทศไทย ครอบคลุมภาคส่วนที่มีภาระหน้าที่ตามกฎหมายความมั่นคงปลอดภัยไซเบอร์ไทยทั้ง 3 ฉบับ
คุณสมบัติผู้ตอบ	ผู้ตอบแบบประเมินต้องเป็นบุคลากรที่ปฏิบัติงานด้านไอที ความมั่นคงปลอดภัยสารสนเทศ หรือฝ่ายกำกับดูแล (Compliance) โดยตรง และมีประสบการณ์ด้านที่เกี่ยวข้องอย่างน้อย 1 ปี
ความสมัครใจ	ผู้บริหารหรือผู้แทนองค์กรยินยอมเข้าร่วมโครงการ อนุญาตให้บุคลากรทดลองใช้ระบบจริง และให้ความร่วมมือในการตอบแบบประเมินโดยไม่มีเงื่อนไข
ความสมบูรณ์	ผู้ตอบแบบประเมินต้องทดลองใช้ระบบจนครบกระบวนการหลัก ได้แก่ การดูรายการตรวจสอบ การบันทึกสถานะ และการดูผล ก่อนตอบแบบประเมิน และต้องกรอกข้อมูลครบถ้วน

ตารางที่ 3-5 เกณฑ์การคัดเลือกองค์กรตัวอย่าง

3.6.4 แบบประเมินความพึงพอใจจากองค์กรตัวอย่าง

บุคลากรด้านไอทีและฝ่ายกำกับดูแลจาก 5 องค์กรตัวอย่างทดลองใช้ระบบจริง แล้วประเมินความพึงพอใจผ่านแบบประเมิน 19 ข้อ แบ่งเป็น 4 หมวด

3.6.2.1 หมวด B ประเมินการลดเวลา การลดความคลาดเคลื่อน ความถูกต้องของรายการ ความเหมาะสมของการเชื่อมโยง และการนำหลักฐานไปปฏิบัติ

3.6.2.2 หมวด C ประเมินการเรียนรู้ ความชัดเจนของการแสดงผล การบันทึกหลักฐาน การใช้งานบนอุปกรณ์ และการนำผลไปรายงาน

3.6.2.3 หมวด D ประเมินความครอบคลุม การรองรับหลายเอกสาร การเสริมกระบวนการเดิม และความน่าเชื่อถือ

3.6.2.4 หมวด E การยกระดับความสามารถ การลดภาระงาน การเพิ่มความเชื่อมั่น และแนวโน้มการนำไปใช้จริง

นอกจากนี้ผู้ตอบแบบประเมินยังให้คะแนนความพึงพอใจโดยรวม (1–10) พร้อมข้อเสนอแนะ

3.6.3 เกณฑ์การแปลผลคะแนน

ช่วงคะแนนเฉลี่ย	ระดับ
4.50 – 5.00	มากที่สุด
3.50 – 4.49	มาก
2.50 – 3.49	ปานกลาง
1.50 – 2.49	น้อย
1.00 – 1.49	น้อยที่สุด

ตารางที่ 3-6 ตารางเกณฑ์การแปลผลคะแนน

3.6.4 การวิเคราะห์ผล

ผู้วิจัยวิเคราะห์ข้อมูลจากแบบประเมินทั้งสองชุดโดยคำนวณค่าเฉลี่ยรายข้อ รายหมวด และคะแนนรวม นำเสนอในรูปตารางและแผนภูมิ พร้อมสรุปข้อสังเกตจากคะแนนและความเห็นเชิงคุณภาพของผู้ประเมิน

3.7 การออกแบบเว็บแอปพลิเคชัน

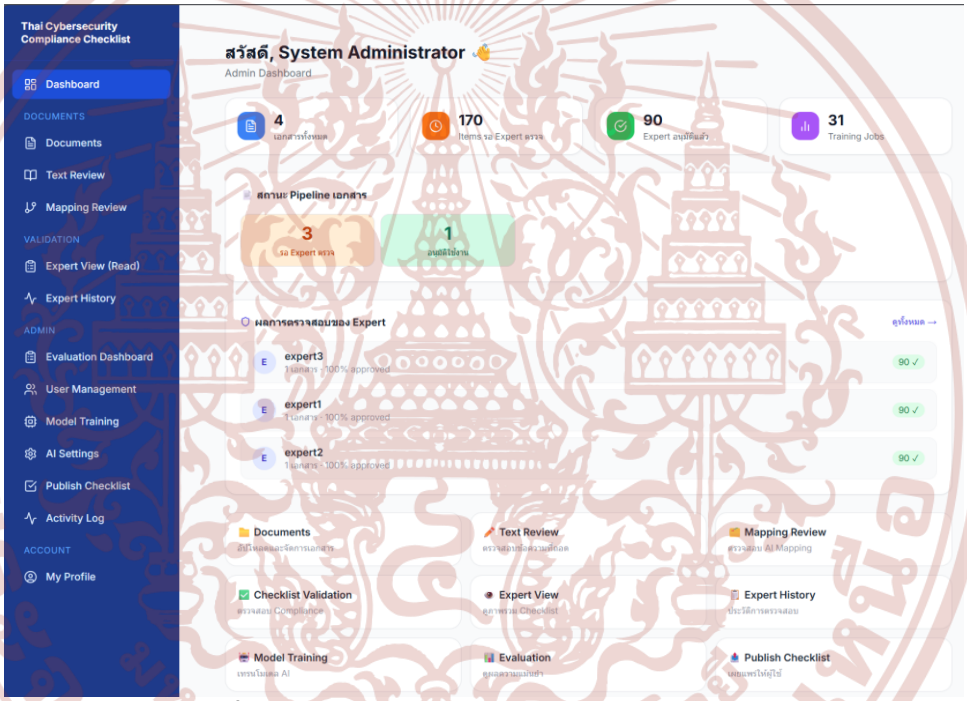
เว็บแอปพลิเคชันพัฒนาด้วยเฟรมเวิร์ก Next.js 14 รองรับผู้ใช้งาน 4 บทบาทผ่านกว่า 25 หน้าจอ โดยมีระบบควบคุมสิทธิ์ตามบทบาทที่ป้องกันการเข้าถึงข้ามหน้าที่

3.7.1 หน้าจอตามบทบาทผู้ใช้งาน

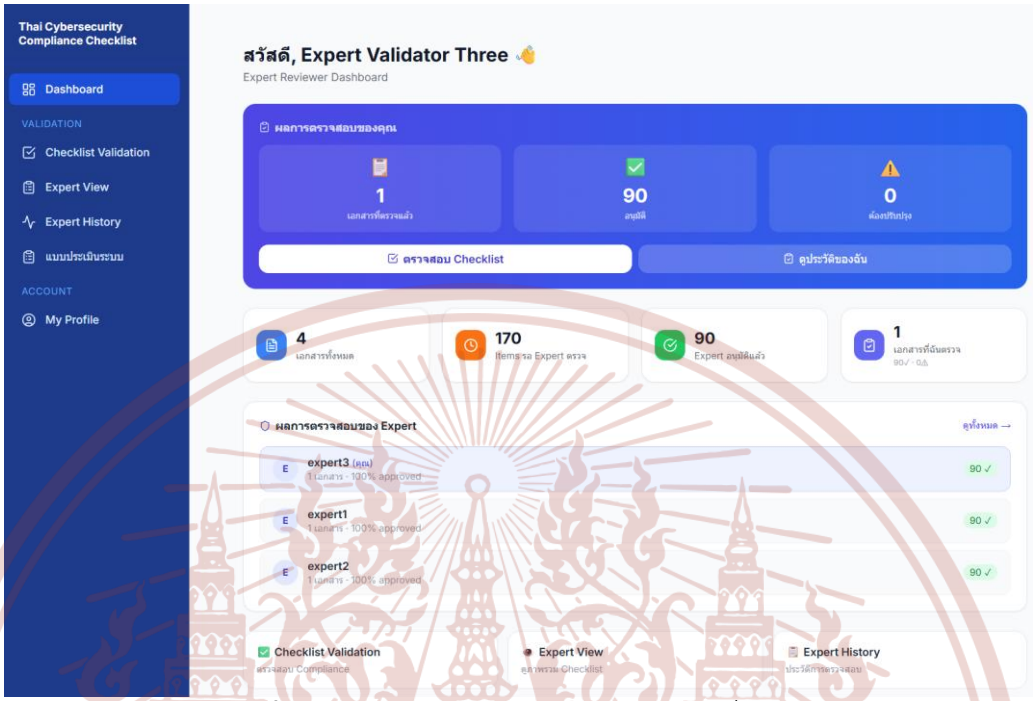
บทบาท	หน้าจอที่เข้าถึงได้
ผู้ดูแลระบบ	จัดการผู้ใช้, รายการตรวจสอบ, ผลการประเมิน, การตั้งค่าระบบ, แผงข้อมูลการวิจัย
เจ้าหน้าที่ฝ่ายกำกับดูแล	อัปโหลดเอกสาร, ตรวจสอบข้อความ, ทบทวนการเชื่อมโยงมาตรฐาน, จัดการกฎการเชื่อมโยง
ผู้เชี่ยวชาญตรวจสอบ	ตรวจสอบและให้คะแนนรายการตรวจสอบ, ดูประวัติการตรวจสอบ, ทำแบบประเมินระบบ

บทบาท	หน้าจอที่เข้าถึงได้
ผู้ใช้รายการตรวจสอบ	เลือกรายการตรวจสอบ, บันทึกสถานะการปฏิบัติตาม, แนบหลักฐาน, ดูผลการประเมินองค์กร
ทุกบทบาท	หน้าเข้าสู่ระบบ, แผงข้อมูลหลัก, โปรไฟล์, บันทึกกิจกรรม

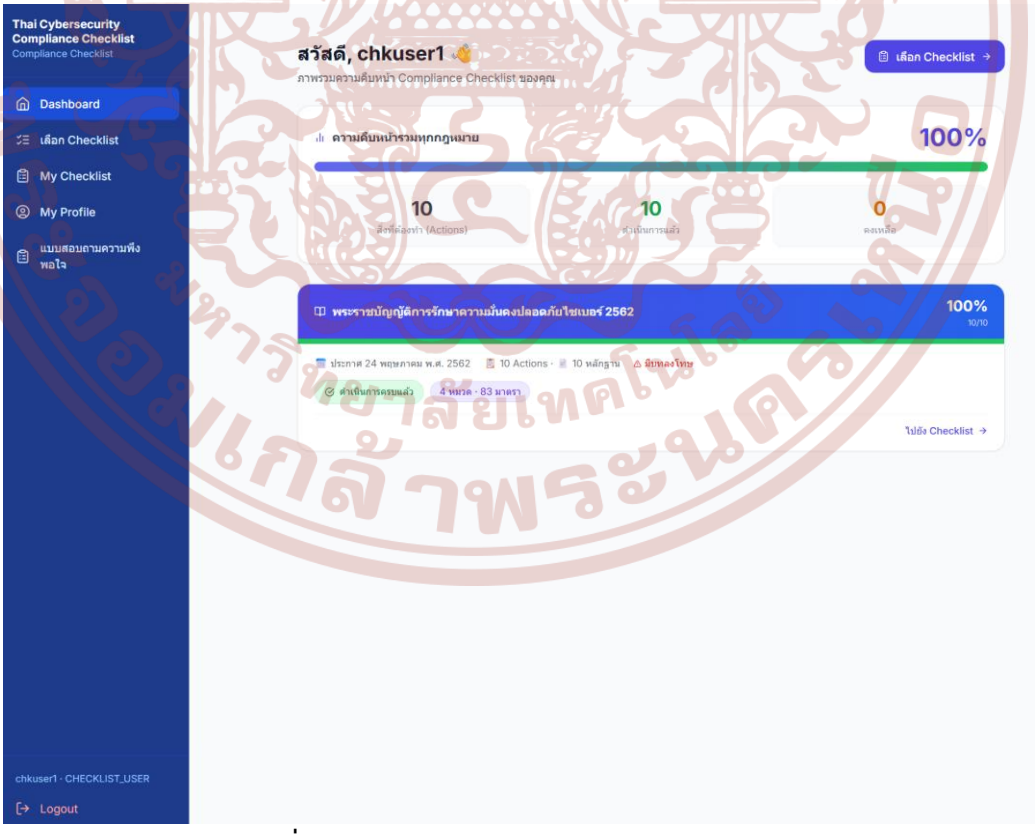
ตารางที่ 3-7 หน้าจอในระบบแบ่งตามบทบาทผู้ใช้งาน



ภาพที่ 3-6 ตัวอย่างหน้าจอหลักของระบบ (ผู้ดูแลระบบ)



ภาพที่ 3-7 ตัวอย่างหน้าจอหลักของระบบ (ผู้เชี่ยวชาญ)



ภาพที่ 3-8 ตัวอย่างหน้าจอหลักของระบบ (ผู้ใช้งาน)

3.7.2 คุณลักษณะสำคัญของระบบ

3.7.2.1 ออกจากระบบอัตโนมัติ โดยระบบออกจากระบบเมื่อไม่มีการใช้งานตามเวลาที่กำหนด พร้อมแจ้งเตือนล่วงหน้า

3.7.2.2 ประวัติการตรวจสอบ โดยผู้เชี่ยวชาญดูประวัติและสถิติการตรวจสอบทั้งหมดที่ผ่านมาได้

3.7.2.3 แผงข้อมูลการวิจัย โดยแสดงผลแบบประเมินทั้งหมดในรูปตารางและกราฟสำหรับผู้ดูแลระบบ

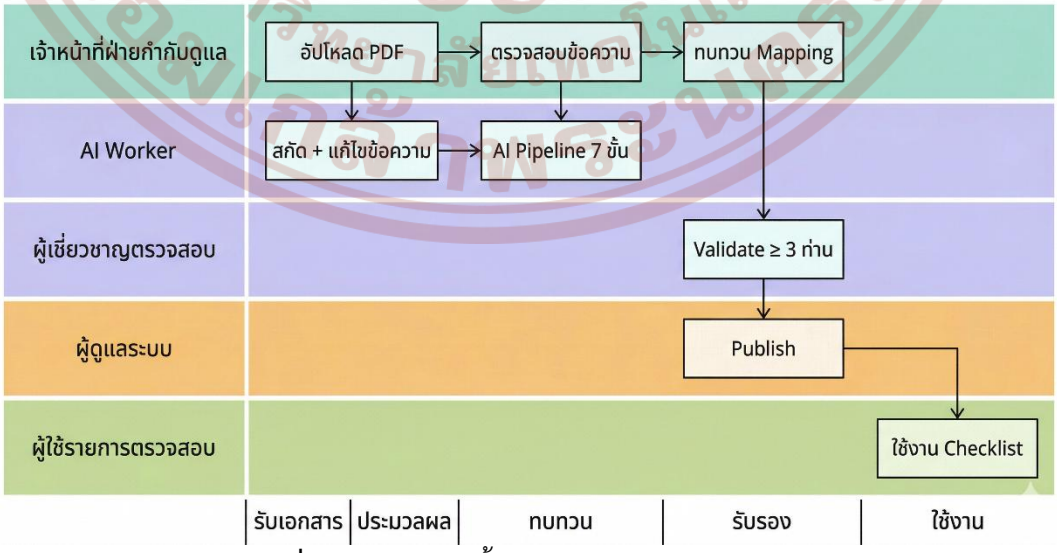
3.7.2.4 ส่งออกรายงาน โดยผู้ดูแลระบบส่งออกผลการประเมินเป็นเอกสาร PDF ได้

3.7.2.5 บันทึกกิจกรรม โดยระบบบันทึกกิจกรรมทุกอย่างของผู้ใช้ รวมถึงเวลาและ IP เพื่อการตรวจสอบย้อนหลัง

3.8 ขั้นตอนการสรุปผลและการนำไปใช้จริง

ในขั้นตอนสุดท้าย ผู้วิจัยรวบรวมผลจากแบบประเมินทั้งสองชุดมาวิเคราะห์และสรุป เพื่อยืนยันประสิทธิผลของระบบตามวัตถุประสงค์การวิจัย 4 ข้อ

ผู้วิจัยยังจัดทำเอกสารประกอบครอบคลุมคู่มือการใช้งานสำหรับผู้ใช้ทุกบทบาท และข้อแนะนำสำหรับองค์กรที่ต้องการนำระบบไปปรับใช้ โดยเฉพาะองค์กรขนาดกลางและเล็กที่มีทรัพยากรจำกัด ซึ่งระบบสามารถทำงานได้เต็มฟังก์ชันด้วยกลไกสำรองแบบกฎเกณฑ์ โดยไม่ต้องอาศัยอุปกรณ์ประมวลผลพิเศษหรือการเชื่อมต่อบริการโมเดลภาษาภายนอก



ภาพที่ 3-9 แผนภาพขั้นตอนการทำงานจากต้นจนจบ

บทที่ 4
ผลการวิจัย

งานวิจัยนี้ประเมินประสิทธิผลของระบบจาก 2 แหล่ง ได้แก่ แบบประเมินโดยผู้เชี่ยวชาญ 3 ท่าน และแบบประเมินความพึงพอใจจากองค์กรตัวอย่าง 5 แห่ง ซึ่งเป็นข้อมูลการวัดผลหลักของงานวิจัยนี้ทั้งหมด

4.1 ผลการประเมินโดยผู้เชี่ยวชาญ

ผู้เชี่ยวชาญ 3 ท่านประเมินระบบผ่านแบบประเมิน 5 ระดับ รวม 19 ข้อ แบ่งเป็น 4 หมวด

4.1.1 หมวด B ความถูกต้องของ AI Mapping (6 ข้อ)

รายการประเมิน	ผู้เชี่ยวชาญ 1	ผู้เชี่ยวชาญ 2	ผู้เชี่ยวชาญ 3	เฉลี่ย
B1 ระบบจำแนกประเภท Compliance ได้ถูกต้อง (เช่น ข้อมูลส่วนบุคคล, ความมั่นคงไซเบอร์)	4	4	4	4.00
B2 การ Mapping กับ ISO 27001:2022 สอดคล้องกับเนื้อหากฎหมาย	4	5	4	4.33
B3 การ Mapping กับ NIST CSF 2.0 สอดคล้องกับเนื้อหากฎหมาย	3	5	4	4.00
B4 รายการ Actions ที่ AI สร้างมีความครบถ้วน	3	4	3	3.33
B5 รายการหลักฐาน (Evidence) ที่ AI สร้างมีความเหมาะสม	4	4	5	4.33
B6 ระบบดึงบทลงโทษและเงื่อนไขระยะเวลาจากกฎหมายได้ถูกต้อง	4	4	4	4.00
เฉลี่ยหมวด B	3.67	4.33	4.00	

ตารางที่ 4-1 ผลการประเมินหมวด B ความถูกต้องของ AI Mapping โดยผู้เชี่ยวชาญ 3 ท่าน

4.1.2 หมวด C ความสะดวกในการใช้งาน (5 ข้อ)

รายการประเมิน	ผู้เชี่ยวชาญ 1	ผู้เชี่ยวชาญ 2	ผู้เชี่ยวชาญ 3	เฉลี่ย
C1 ขั้นตอนการตรวจสอบ Checklist เข้าใจง่ายและใช้งานสะดวก	4	5	4	4.33
C2 การแสดงผลคะแนนสอดคล้อง (%) ช่วยให้ตัดสินใจได้ดีขึ้น	4	4	5	4.33
C3 เครื่องมือแก้ไข Actions / Evidence / ISO / NIST ใช้งานได้ดี	3	5	4	4.00
C4 กระบวนการส่งผลตรวจสอบ (Validate) มีความชัดเจน	4	5	5	4.67
C5 ระบบแสดงข้อมูลที่จำเป็นครบถ้วนสำหรับการตรวจสอบ	4	4	4	4.00
เฉลี่ยหมวด C	3.80	4.60	4.40	

ตารางที่ 4-2 ผลการประเมินหมวด C ความสะดวกในการใช้งาน

4.1.3 หมวด D ความน่าเชื่อถือของกระบวนการตรวจสอบ (4 ข้อ)

รายการประเมิน	ผู้เชี่ยวชาญ 1	ผู้เชี่ยวชาญ 2	ผู้เชี่ยวชาญ 3	เฉลี่ย
D1 ระบบ 3-Expert Validation ทำให้ผลลัพธ์น่าเชื่อถือมากขึ้น	5	5	5	5.00
D2 การบันทึกประวัติการตรวจสอบ (Expert History) มีประโยชน์	4	5	4	4.33
D3 กระบวนการปรับปรุงระบบหลังแก้ไขมีความโปร่งใสและเข้าใจได้	4	4	5	4.33
D4 การแบ่งรอบการตรวจสอบ (Review Round) มีประสิทธิภาพ	4	4	4	4.00
เฉลี่ยหมวด D	4.25	4.50	4.50	

ตารางที่ 4-3 ผลการประเมินหมวด D ความน่าเชื่อถือของกระบวนการตรวจสอบ

4.1.4 หมวด E ความเพียงพอของผลลัพธ์ (4 ข้อ)

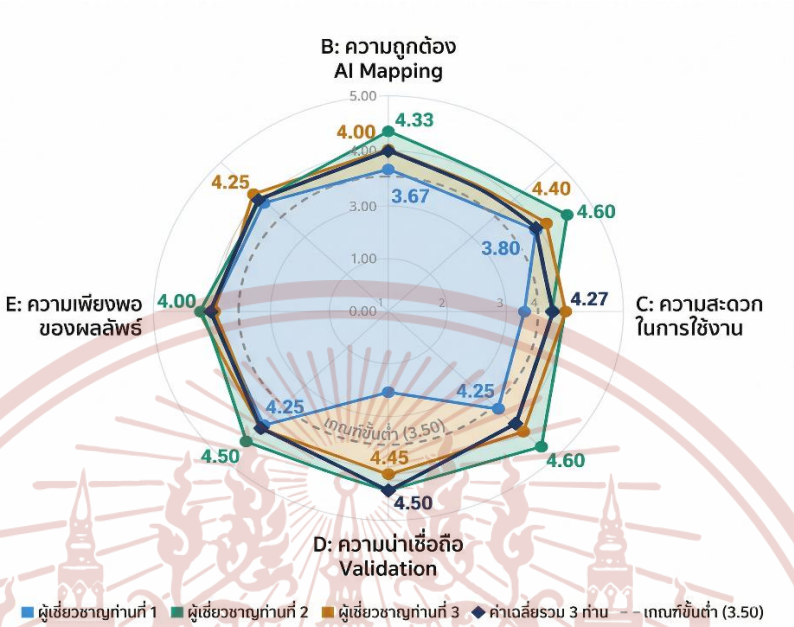
รายการประเมิน	ผู้เชี่ยวชาญ 1	ผู้เชี่ยวชาญ 2	ผู้เชี่ยวชาญ 3	เฉลี่ย
E1 ผลการประเมินใน Dashboard สะท้อนคุณภาพของระบบได้จริง	4	4	4	4.00
E2 ตัวชี้วัด (Actions %, ISO %, NIST %) มีความหมายและเป็นประโยชน์	4	5	4	4.33
E3 ข้อมูลที่ระบบนำเสนอเพียงพอสำหรับการตัดสินใจ Publish Checklist	4	4	5	4.33
E4 ระบบช่วยลดภาระงานของผู้เชี่ยวชาญในการตรวจสอบกฎหมายได้จริง	4	5	4	4.33
เฉลี่ยหมวด E	4.00	4.50	4.25	

ตารางที่ 4-4 ผลการประเมินหมวด E ความเพียงพอของผลลัพธ์

4.1.5 สรุปผลการประเมินโดยผู้เชี่ยวชาญ

หมวดการประเมิน	ผู้เชี่ยวชาญ 1	ผู้เชี่ยวชาญ 2	ผู้เชี่ยวชาญ 3	เฉลี่ย
B ความถูกต้องของ AI Mapping	3.67	4.33	4.00	4.00
C ความสะดวกในการใช้งาน	3.80	4.60	4.40	4.27
D ความน่าเชื่อถือของ Validation	4.25	4.50	4.50	4.42
E ความเพียงพอของผลลัพธ์	4.00	4.50	4.25	4.25
คะแนนเฉลี่ยรวมทุกหมวด	3.93	4.48	4.29	4.23
ความพึงพอใจโดยรวม (คะแนน 1–10)	8/10	9/10	8/10	8.3/10

ตารางที่ 4-5 สรุปคะแนนเฉลี่ยรายหมวดและความพึงพอใจโดยรวมจากผู้เชี่ยวชาญ 3 ท่าน



ภาพที่ 4-1 แผนภูมิแสดงคะแนนผู้เชี่ยวชาญรายหมวด B–E เปรียบเทียบทั้ง 3 ท่าน

ผลการประเมินภาพรวมอยู่ในระดับมาก โดยมีคะแนนเฉลี่ยจากผู้เชี่ยวชาญ 4.23 จาก 5 คะแนน และความพึงพอใจ 8.3 จาก 10 คะแนน ทั้งนี้ จุดแข็งสำคัญของระบบคือหมวด D (4.42) ซึ่งสะท้อนถึงประสิทธิภาพของกระบวนการ 3-Expert Threshold ในขณะที่ส่วนที่ควรพัฒนาเพิ่มเติมคือหมวด B (4.00) โดยเน้นไปที่การปรับปรุง Actions ให้มีความชัดเจนและสามารถนำไปปฏิบัติได้จริงมากยิ่งขึ้น

4.2 ผลการประเมินความพึงพอใจจากองค์กรตัวอย่าง

บุคลากรด้านไอทีและฝ่ายกำกับดูแลจากองค์กรตัวอย่าง 5 แห่ง ทดลองใช้ระบบจริงแล้วประเมินความพึงพอใจผ่านแบบประเมิน Likert 5 ระดับ รวม 19 ข้อ แบ่งเป็น 4 หมวด

4.2.1 หมวด B ประสิทธิภาพในการตรวจสอบ (5 ข้อ)

รายการประเมิน	บ.1	บ.2	บ.3	บ.4	บ.5	เฉลี่ย
B1 ลดระยะเวลาตรวจสอบ Compliance	5	4	5	5	4	4.60
B2 Checklist ถูกต้องและครอบคลุม	4	4	4	4	4	4.00
B3 ลดความคลาดเคลื่อนในการตีความ	4	5	4	5	4	4.40
B4 ISO/NIST Mapping เหมาะสมกับบริบท	5	4	3	4	4	4.00
B5 Evidence นำไปปฏิบัติได้จริง	4	4	4	4	4	4.00

รายการประเมิน	บ.1	บ.2	บ.3	บ.4	บ.5	เฉลี่ย
เฉลี่ยหมวด B	4.40	4.20	4.00	4.40	4.00	

ตารางที่ 4-6 ผลการประเมินหมวด B ประสิทธิภาพในการตรวจสอบ

4.2.2 หมวด C ความสะดวกในการใช้งาน (5 ข้อ)

รายการประเมิน	บ.1	บ.2	บ.3	บ.4	บ.5	เฉลี่ย
C1 ง่ายต่อการเรียนรู้	4	4	5	5	4	4.40
C2 แสดงผลและความคืบหน้าชัดเจน	5	4	4	4	4	4.20
C3 บันทึกหลักฐานและติดตามสะดวก	4	5	4	4	4	4.20
C4 ใช้งานได้ดีบนอุปกรณ์ต่างๆ	4	4	5	5	4	4.40
C5 นำผลรายงานผู้บริหารได้ทันที	5	4	4	4	4	4.20
เฉลี่ยหมวด C	4.40	4.20	4.40	4.40	4.00	

ตารางที่ 4-7 ผลการประเมินหมวด C ความสะดวกในการใช้งาน

4.2.3 หมวด D: ความเหมาะสมกับองค์กร (4 ข้อ)

รายการประเมิน	บ.1	บ.2	บ.3	บ.4	บ.5	เฉลี่ย
D1 Checklist ครอบคลุมกฎหมายที่ต้องปฏิบัติ	4	4	4	4	4	4.00
D2 รองรับการจัดการเอกสารหลายฉบับ	5	4	4	4	5	4.40
D3 เสริมกระบวนการ Compliance เดิมได้	5	4	5	4	4	4.40
D4 ความปลอดภัยของระบบยอมรับได้	4	5	4	4	4	4.20
เฉลี่ยหมวด D	4.50	4.25	4.25	4.00	4.25	

ตารางที่ 4-8 ผลการประเมินหมวด D ความเหมาะสมกับองค์กร

4.2.4 หมวด E ผลกระทบและคุณค่า (4 ข้อ)

รายการประเมิน	บ.1	บ.2	บ.3	บ.4	บ.5	เฉลี่ย
E1 ยกระดับ Cyber Compliance	5	4	5	5	4	4.60
E2 ลดภาระงานบุคลากร	5	4	5	5	4	4.60
E3 เพิ่มความเชื่อมั่นด้านธรรมาภิบาล	4	5	4	5	4	4.40

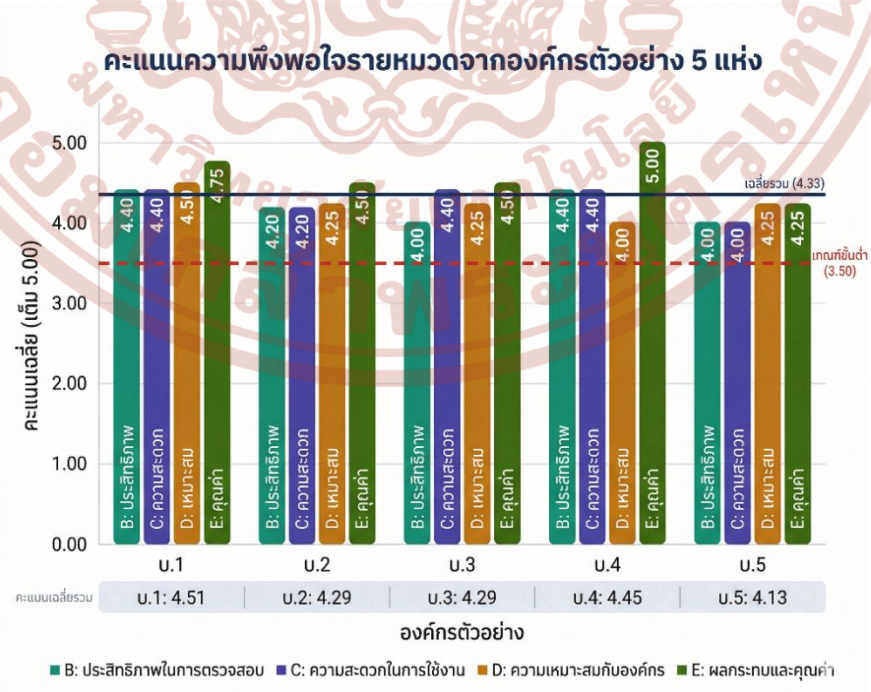
รายการประเมิน	บ.1	บ.2	บ.3	บ.4	บ.5	เฉลี่ย
E4 แนวโน้มนำไปใช้จริงในองค์กร	5	5	4	5	5	4.80
เฉลี่ยหมวด E	4.75	4.50	4.50	5.00	4.25	

ตารางที่ 4-9 ผลการประเมินหมวด E ผลกระทบและคุณค่า

4.2.5 สรุปผลการประเมินความพึงพอใจ

รายการประเมิน	บ.1	บ.2	บ.3	บ.4	บ.5	เฉลี่ย
B ประสิทธิภาพการตรวจสอบ	4.40	4.20	4.00	4.40	4.00	4.20
C ความสะดวกในการใช้งาน	4.40	4.20	4.40	4.40	4.00	4.28
D ความเหมาะสมกับองค์กร	4.50	4.25	4.25	4.00	4.25	4.25
E ผลกระทบและคุณค่า	4.75	4.50	4.50	5.00	4.25	4.60
คะแนนเฉลี่ยรวมทุกหมวด	4.51	4.29	4.29	4.45	4.13	4.33
ความพึงพอใจโดยรวม (1–10)	9/10	9/10	8/10	9/10	8/10	8.6/10
เวลาที่ประหยัดได้	~70%	~60%	~65%	~75%	~50%	~64%

ตารางที่ 4-10 สรุปคะแนนเฉลี่ยรายหมวดและความพึงพอใจโดยรวมจากองค์กรตัวอย่าง 5 แห่ง



ภาพที่ 4-2 แผนภูมิแสดงคะแนนความพึงพอใจรายหมวด B–E จากองค์กรตัวอย่าง

คะแนนเฉลี่ยรวมทุกหมวดจากองค์กรตัวอย่าง 5 แห่งเท่ากับ 4.33 จากคะแนนเต็ม 5.00 (ระดับมาก) ความพึงพอใจโดยรวมเฉลี่ย 8.6 จาก 10 คะแนน ระบบช่วยลดเวลาการตรวจสอบ Compliance ได้เฉลี่ยประมาณ 64% เมื่อเทียบกับวิธีเดิมที่ใช้ที่ปรึกษาหรือ Excel

4.3 การอภิปรายผล

4.3.1 ด้านความถูกต้องของระบบ (หมวด B ผู้เชี่ยวชาญ)

คะแนนหมวด B เฉลี่ย 4.00 จากผู้เชี่ยวชาญ 3 ท่านสะท้อนว่าระบบสามารถสกัดข้อกำหนดและเชื่อมโยงมาตรฐาน ISO/NIST ได้ในระดับที่ยอมรับได้ ซึ่งยืนยันว่ากระบวนการ 7 ขั้นตอนสามารถรับมือกับความซับซ้อนของภาษากฎหมายไทยได้จริง โดยเฉพาะกลไกพิเศษที่แยกภาระหน้าที่ออกจากบทลงโทษซึ่งมักเขียนรวมกันในกฎหมายไทย สอดคล้องกับงานวิจัยด้านระบบผสมผสานที่อธิบายผลได้ [12]

4.3.2 ด้านความสะดวกในการใช้งาน (หมวด C ทั้งสองกลุ่ม)

คะแนนหมวด C จากผู้เชี่ยวชาญเฉลี่ย 4.27 และจากองค์กรตัวอย่างเฉลี่ย 4.28 สะท้อนมุมมองที่สอดคล้องกันจากทั้งผู้ตรวจสอบและผู้ใช้งานรายการตรวจสอบ โดยทั้งสองกลุ่มให้คะแนนอยู่ในระดับมาก ใกล้เคียงกัน บ่งชี้ว่าระบบออกแบบ UX ได้สมดุลระหว่างความต้องการของผู้เชี่ยวชาญที่ต้องการความละเอียดในการตรวจสอบ และผู้ใช้งานทั่วไปที่ต้องการความเรียบง่าย

จุดที่น่าสังเกตคือ C4 (กระบวนการ Validate ชัดเจน) และ C5 (นำผลรายงานผู้บริหาร) ได้คะแนนสูงจากทั้งสองกลุ่ม แสดงว่าระบบตอบสนองทั้งความต้องการของระดับปฏิบัติการและระดับบริหารได้พร้อมกัน ขณะที่ C3 (เครื่องมือแก้ไข Actions/Evidence) ยังมีช่องว่างให้พัฒนาในมุมมองของผู้เชี่ยวชาญที่ต้องการความยืดหยุ่นในการแก้ไขมากขึ้น

4.3.3 ด้านความน่าเชื่อถือและการนำไปใช้ (หมวด D และ E)

คะแนนหมวด D เฉลี่ย 4.42 จากผู้เชี่ยวชาญเป็นหมวดที่ได้คะแนนสูงสุดในการประเมินกลุ่มนี้ ข้อ D1 (3-Expert Validation น่าเชื่อถือ) ได้ 5 คะแนนจากทั้งสามท่าน ยืนยันว่ากระบวนการตรวจสอบ 3 ท่านสร้างความน่าเชื่อถือให้กับผลลัพธ์ สอดคล้องกับหลักการ Human-in-the-Loop ที่เน้นบทบาทของมนุษย์ผู้เชี่ยวชาญในระบบ AI [10]

คะแนนหมวด E เฉลี่ย 4.60 จากองค์กรตัวอย่างเป็นหมวดที่ได้คะแนนสูงสุดในการประเมินกลุ่มนี้ สะท้อนว่าระบบสร้างคุณค่าจริงและมีแนวโน้มที่จะนำไปใช้งานในองค์กร องค์กรในกลุ่มที่เพิ่งเริ่มต้นทำ Compliance (ไม่มีกระบวนการเดิม) ให้คะแนนหมวด E สูงกว่าองค์กรที่มีกระบวนการเดิมอยู่แล้ว สอดคล้องกับแนวคิดการใช้ AI เพื่อลดภาระงานกำกับดูแล [3], [11]

4.3.4 ข้อสังเกตจากความเห็นของผู้ประเมิน

นอกจากคะแนน Likert แล้ว ผู้เชี่ยวชาญและองค์กรตัวอย่างยังให้ข้อเสนอแนะเพิ่มเติมซึ่งผู้วิจัยรวบรวมสรุปดังนี้

ประเด็น	รายละเอียดที่ผู้ประเมินระบุ
จุดเด่นที่ผู้ประเมินระบุร่วมกัน	ระบบแปลงภาษากฎหมายที่ซับซ้อนเป็นรายการปฏิบัติได้อย่างน่าประทับใจ โดยเฉพาะการแยก obligation ออกจาก penalty ซึ่งเป็นปัญหาหลักของกฎหมายไทย กระบวนการ 3-Expert Validation ทำให้ผลลัพธ์สามารถอ้างอิงได้ในเชิงกฎหมาย และ Evidence ที่แนะนำสำหรับ PDPA มีความถูกต้องและครบถ้วนสูง
ประเด็นที่ผู้ประเมินต้องการให้ปรับปรุง	Actions บางข้อยังเป็นภาษาทางการเกินไป ควรระบุ responsible party และ timeline ที่ชัดเจน ควรเพิ่มการรองรับประกาศลำดับรองของ NCSA และ PDPC และควรแยก Checklist ระหว่าง Data Controller กับ Data Processor ให้ชัดเจนยิ่งขึ้น
ข้อจำกัดที่พบระหว่างการใช้งาน	บางมาตรากฎหมายที่มีถ้อยคำกำกวมต้องอาศัยการตัดสินใจจากผู้เชี่ยวชาญโดยตรง ระบบยังไม่สามารถระบุได้อย่างชัดเจน โมเดล WangchanBERTa ยังเป็น base model ความแม่นยำจะเพิ่มขึ้นเมื่อมีการ fine-tune ด้วยข้อมูล annotated จากผู้เชี่ยวชาญ
ความต้องการเพิ่มเติมจากองค์กร	ต้องการรองรับกฎหมายเฉพาะภาคส่วน เช่น ประกาศ ธปท. กลต. MOIT Guidelines สำหรับการศึกษา และ OT Security สำหรับภาคการผลิต รวมถึงต้องการ export Checklist เป็น Excel และ dashboard แสดงเปอร์เซ็นต์ Compliance รวมขององค์กรแบบ real-time

ตารางที่ 4-11 สรุปข้อสังเกตเชิงคุณภาพจากผู้ประเมินทั้งสองกลุ่ม

4.4 สรุปผลการประเมินทั้งสองกลุ่ม

ภาพรวมของการประเมินจากทั้งสองกลุ่มสะท้อนว่าระบบมีประสิทธิผลในระดับ "มาก" ทุกหมวด คะแนนเฉลี่ยรวมจากผู้เชี่ยวชาญ 4.23 และจากองค์กรตัวอย่าง 4.33 แสดงให้เห็นว่าระบบตอบสนองความต้องการของทั้งผู้ตรวจสอบเชิงวิชาการและผู้ใช้งานเชิงปฏิบัติได้อย่างสมดุล ผลการวิจัยยืนยันว่าสถาปัตยกรรม Hybrid AI Pipeline 7 ขั้นตอนร่วมกับกระบวนการ 3-Expert Threshold สามารถสร้างรายการตรวจสอบที่ถูกต้อง น่าเชื่อถือ และนำไปปฏิบัติได้จริงสำหรับกฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย

หมวดการประเมิน	ผู้เชี่ยวชาญ 3 ท่าน	องค์กต 5 แห่ง	ระดับ (รวม)
B ความถูกต้อง / ประสิทธิภาพ	4.00	4.20	มาก
C ความสะดวกในการใช้งาน	4.27	4.28	มาก
D ความน่าเชื่อถือ / เหมาะสม	4.42	4.25	มาก
E ผลลัพธ์ / คุณค่า	4.25	4.60	มาก
คะแนนเฉลี่ยรวมทุกหมวด	4.23	4.33	มาก
ความพึงพอใจโดยรวม (1–10)	8.3/10	8.6/10	

ตารางที่ 4-12 สรุปผลการประเมินทั้งสองกลุ่ม

พระจอมเกล้าพระนครเหนือ มหาวิทยาลัยเทคโนโลยี

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

จากการวิจัยเรื่อง "ระบบปัญญาประดิษฐ์สำหรับสกัดและเชื่อมโยงข้อกำหนดกฎหมายไซเบอร์ไทยเพื่อสร้างรายการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ" ผู้วิจัยวัดประสิทธิผลจากแบบประเมินโดยผู้เชี่ยวชาญ 3 ท่าน และแบบประเมินความพึงพอใจจากองค์กรตัวอย่าง 5 แห่ง บทนี้สรุปผลตามวัตถุประสงค์ อภิปรายผล ระบุข้อจำกัด และเสนอแนวทางพัฒนาต่อยอด

5.1 สรุปผลการดำเนินงานวิจัย

จากการพัฒนาระบบและทดสอบกับผู้เชี่ยวชาญและองค์กรตัวอย่าง สรุปผลตามวัตถุประสงค์ดังตารางที่ 5-1

วัตถุประสงค์	ผลที่ได้	ผลการประเมิน	แหล่งข้อมูล
พัฒนาระบบ AI สกัดข้อกำหนดจากกฎหมาย 3 ฉบับ	✅ สำเร็จ	B Avg = 4.00/5.00	หมวด B ผู้เชี่ยวชาญ
เชื่อมโยงกับมาตรฐาน ISO 27001:2022 และ NIST CSF 2.0	✅ สำเร็จ	B Avg = 4.00/5.00	หมวด B ผู้เชี่ยวชาญ
กระบวนการตรวจสอบ 3 ท่าน และเว็บแอปพลิเคชัน 4 บทบาท	✅ สำเร็จ	D Avg = 4.42/5.00	หมวด D ผู้เชี่ยวชาญ
ประเมินประสิทธิผลกับผู้เชี่ยวชาญและองค์กรตัวอย่าง	✅ สำเร็จ	Expert 4.23 Org 4.33	ผู้เชี่ยวชาญ + องค์กร

ตารางที่ 5-1 สรุปผลตามวัตถุประสงค์การวิจัย

5.1.1 ผลจากแบบประเมินผู้เชี่ยวชาญ

หมวดการประเมิน	คะแนนเฉลี่ย	ระดับ	ข้อสังเกตสำคัญ
B ความถูกต้องของ AI Mapping (6 ข้อ)	4.00/5.00	มาก	B2 ISO Mapping และ B3 NIST Mapping ได้คะแนนสูง B4 Actions ควรพัฒนาเพิ่มเติม
C ความสะดวกในการใช้งาน (5 ข้อ)	4.27/5.00	มาก	C4 กระบวนการ Validate ชัดเจนได้คะแนนสูงสุดในหมวดนี้

หมวดการประเมิน	คะแนนเฉลี่ย	ระดับ	ข้อสังเกตสำคัญ
D ความน่าเชื่อถือ Validation (4 ข้อ)	4.42/5.00	มาก	D1 3-Expert Threshold ได้ 5 คะแนนจากทุกท่าน หมวดที่ได้คะแนนสูงสุด
E ความเพียงพอของผลลัพธ์ (4 ข้อ)	4.25/5.00	มาก	E4 ลดภาระงานผู้เชี่ยวชาญ และ E3 ข้อมูลเพียงพอสำหรับตัดสินใจได้คะแนนสูง
คะแนนเฉลี่ยรวมทุกหมวด	4.23/5.00	มาก	อยู่เหนือเกณฑ์ขั้นต่ำ 3.50 ทุกหมวด
ความพึงพอใจโดยรวม	8.33/10	—	ค่าเฉลี่ยจากท่านที่ 1=8, ท่านที่ 2=9, ท่านที่ 3=8

ตารางที่ 5-2 สรุปผลการประเมินโดยผู้เชี่ยวชาญ 3 ท่าน

คะแนนเฉลี่ยรวมจากผู้เชี่ยวชาญ 3 ท่านเท่ากับ 4.23 จากคะแนนเต็ม 5.00 (ระดับมาก) ความพึงพอใจโดยรวมเฉลี่ย 8.33 จาก 10 คะแนน หมวดที่ได้คะแนนสูงสุดคือหมวด D (4.42) สะท้อนว่ากระบวนการ 3-Expert Threshold เป็นจุดแข็งที่โดดเด่นที่สุดของระบบ

5.1.2 ผลจากแบบประเมินความพึงพอใจขององค์กรตัวอย่าง

บุคลากรด้านไอทีและฝ่ายกำกับดูแลจากองค์กรตัวอย่าง 5 แห่ง ประเมินระบบผ่านแบบประเมิน Likert 5 ระดับ จำนวน 19 ข้อ แบ่งเป็น 4 หมวด ได้ผลดังนี้

หมวดการประเมิน	คะแนนเฉลี่ย	ระดับ	ข้อสังเกตสำคัญ
B ประสิทธิภาพในการตรวจสอบ (5 ข้อ)	4.20/5.00	มาก	B1 ลดระยะเวลาตรวจสอบ ได้ 5 คะแนนจาก 3 องค์กร
C ความสะดวกในการใช้งาน (5 ข้อ)	4.28/5.00	มาก	C5 นำผลรายงานผู้บริหารได้ทันที ได้คะแนนสูงสุดในหมวดนี้
D ความเหมาะสมกับองค์กร (4 ข้อ)	4.25/5.00	มาก	D3 เสริมกระบวนการ Compliance เดิมได้ ได้คะแนนสูงสุดในหมวดนี้
E ผลกระทบและคุณค่า (4 ข้อ)	4.60/5.00	มากที่สุด	หมวดที่ได้คะแนนสูงสุด บ.ไทยชอปให้ 5.00 ทุกข้อ

หมวดการประเมิน	คะแนนเฉลี่ย	ระดับ	ข้อสังเกตสำคัญ
คะแนนเฉลี่ยรวมทุกหมวด	4.33/5.00	มาก	อยู่เหนือเกณฑ์ขั้นต่ำ 3.50 ทุกหมวด 3 บริษัทให้ 9/10, 2 บริษัทให้ 8/10
ความพึงพอใจโดยรวม	8.60/10	—	
เวลาที่ประหยัดได้	~64% โดยเฉลี่ย	—	ช่วง 50–75% ขึ้นอยู่กับองค์กร

ตารางที่ 5-3 สรุปผลการประเมินความพึงพอใจจากองค์กรตัวอย่าง 5 แห่ง

5.2 การอภิปรายผล

5.2.1 ความสำคัญของกระบวนการตรวจสอบโดยผู้เชี่ยวชาญ

คะแนนหมวด D จากผู้เชี่ยวชาญ 4.42 ซึ่งเป็นหมวดที่ได้คะแนนสูงสุดในการประเมินกลุ่มนี้ ยืนยันว่ากระบวนการตรวจสอบ 3 ท่านมีความจำเป็นและสร้างความน่าเชื่อถือให้กับรายการตรวจสอบที่เผยแพร่ โดยเฉพาะในส่วนที่เกี่ยวกับบทลงโทษและข้อยกเว้นทางกฎหมายที่ต้องอาศัยการตัดสินใจจากผู้มีความเชี่ยวชาญ ข้อ D1 (3-Expert Validation น่าเชื่อถือ) ได้คะแนน 5 เต็มจากทั้งสามท่าน สะท้อนฉันทามติที่ชัดเจนว่ากระบวนการนี้เป็นจุดแข็งสำคัญของระบบ สอดคล้องกับแนวทาง Explainable AI ที่เน้นการตรวจสอบย้อนหลังได้ [12]

5.2.2 คุณค่าต่อองค์กรจากมุมมองผู้ใช้

คะแนนหมวด E จากองค์กรตัวอย่าง 4.60 อยู่ในระดับ "มากที่สุด" ซึ่งเป็นระดับสูงสุดที่ได้รับในการประเมินครั้งนี้ สะท้อนว่าระบบสร้างคุณค่าจริงในการลดภาระงานด้านการกำกับดูแล โดยองค์กรที่เพิ่งเริ่มต้นทำ Compliance และองค์กรภาคการเงินที่มี ISO 27001 อยู่แล้วต่างให้คะแนนสูงเช่นเดียวกัน แสดงว่าระบบสามารถสร้างคุณค่าได้ในบริบทองค์กรที่หลากหลาย ซึ่งเป็นความต้องการสำคัญของ SMEs และองค์กรที่มีบุคลากรด้านความมั่นคงปลอดภัยจำกัด สอดคล้องกับงานวิจัยด้านการใช้ AI เพื่อการกำกับดูแล [3], [11]

ที่น่าสังเกตคือค่าเฉลี่ยเวลาที่ประหยัดได้ประมาณ 64% ซึ่งค่าเฉลี่ยนี้สัมพันธ์กับระดับความซับซ้อนของกระบวนการ Compliance เดิมขององค์กร ยิ่งกระบวนการเดิมซับซ้อนน้อยหรือไม่มีเลย ยิ่งได้ประโยชน์จากระบบมากกว่า

5.2.3 เปรียบเทียบมุมมองระหว่างผู้เชี่ยวชาญและองค์กร

การเปรียบเทียบคะแนนหมวด C ระหว่างสองกลุ่ม (ผู้เชี่ยวชาญ 4.27 และองค์กร 4.28) พบว่าใกล้เคียงกันมาก บ่งชี้ว่าระบบออกแบบ UX ได้สมดุลระหว่างความต้องการของผู้ตรวจสอบที่

ต้องการความละเอียดและผู้ใช้งานทั่วไปที่ต้องการความเรียบง่าย ซึ่งเป็นความท้าทายสำคัญในการออกแบบระบบที่รองรับผู้ใช้หลายระดับ

ความแตกต่างที่เห็นชัดที่สุดคือหมวด E ที่องค์กร (4.60) ให้คะแนนสูงกว่าผู้เชี่ยวชาญ (4.25) อย่างมีนัยสำคัญ สะท้อนว่ากลุ่มผู้ใช้งานจริงรับรู้ถึงคุณค่าของระบบในเชิงปฏิบัติสูงกว่า ซึ่งเป็นสัญญาณบวกสำหรับการนำไปใช้งานจริงในอนาคต ในทางกลับกัน ผู้เชี่ยวชาญให้คะแนนหมวด D สูงกว่า (4.42 เทียบกับ 4.25) สะท้อนว่าผู้ที่เข้าใจกระบวนการตรวจสอบเชิงวิชาการยิ่งเห็นคุณค่าของ 3-Expert Threshold มากกว่า

5.2.4 ความสอดคล้องกับงานวิจัยที่เกี่ยวข้อง

ผลการประเมินโดยรวม (Expert 4.23, Org 4.33) อยู่ในระดับ "มาก" ทุกหมวด สอดคล้องกับงานวิจัยที่เกี่ยวข้องหลายชิ้น ได้แก่

5.2.4.1 Nithya et al. [5] ยืนยันว่าระบบ AI สามารถสกัดข้อมูลสำคัญจากตัวบทกฎหมายได้อย่างมีประสิทธิภาพ งานวิจัยนี้ขยายผลสู่การสกัด obligation ซึ่งซับซ้อนกว่าและทำได้โดยใช้ Hybrid Pipeline

5.2.4.2 Shaik et al. [6] พิสูจน์ว่าโมเดลภาษาตรวจสอบข้อบังคับได้โดยอัตโนมัติ งานวิจัยนี้เพิ่มมิติการเชื่อมโยง ISO/NIST พร้อมกันสองมาตรฐานในระบบเดียว

5.2.4.3 Tiwari & Shanmugam [2] — เน้นความสำคัญของ audit trail ที่ตรวจสอบย้อนหลังได้ ระบบนี้บันทึกทุก review round และ correction สอดคล้องกับหลักการนี้

5.2.4.4 Hybrid XAI [12] — แสดงว่า Rule-Based + AI ให้ความแม่นยำและอธิบายผลได้ระดับมาตรา ระบบนี้ใช้หลักการเดียวกันในทุกขั้นตอนของ Pipeline

ผลการวิจัยนี้ยังเติมเต็มช่องว่างที่งานก่อนหน้าไม่ได้ครอบคลุม ได้แก่ การทำงานกับกฎหมายไทยโดยเฉพาะ กระบวนการ Multi-Expert Validation ที่ตรวจสอบย้อนหลังได้ และกลไก Rule Learning อัตโนมัติจากการแก้ไขของผู้เชี่ยวชาญ

5.3 ข้อจำกัดของการวิจัย

ข้อจำกัด	รายละเอียดและผลกระทบ
ขอบเขตกฎหมาย	ครอบคลุมเฉพาะกฎหมายหลัก 3 ฉบับ ยังไม่รองรับประกาศลำดับรองและกฎหมายเฉพาะภาคส่วน เช่น ประกาศ ธปท. กลต. และ MOIT Guidelines สำหรับการศึกษา
ขอบเขตด้านเทคนิค	เน้นการสกัดจากเอกสาร PDF ยังไม่สามารถตรวจสอบการตั้งค่าระบบสารสนเทศจริงหรือเชื่อมต่อกับระบบบริหารความเสี่ยงขององค์กรโดยตรง

ข้อจำกัด	รายละเอียดและผลกระทบ
การอ้างอิงข้ามมาตรา	กฎหมายบางมาตราที่มีการอ้างอิงข้ามหมวดหลายทอดอาจทำให้ระบบสกัดข้อมูลไม่ครบ ต้องอาศัยการตรวจสอบโดยผู้เชี่ยวชาญเพิ่มเติม
สถานะโมเดลภาษา	WangchanBERTa ยังเป็น base model ที่ยังไม่ได้ fine-tune บน Thai legal corpus โดยตรง ความแม่นยำจะเพิ่มขึ้นเมื่อมีข้อมูล annotated จากผู้เชี่ยวชาญสะสมเพียงพอ
ขนาดกลุ่มตัวอย่าง	ผู้เชี่ยวชาญ 3 ท่านและองค์กร 5 แห่ง เหมาะสำหรับการพิสูจน์แนวคิดเบื้องต้น (Proof of Concept) การศึกษาขนาดใหญ่จำเป็นต้องขยายกลุ่มตัวอย่างเพื่อเพิ่มนัยทางสถิติ
ถ้อยคำกำกวมในกฎหมาย	บางมาตราที่มีถ้อยคำกำกวมหรือต้องการการตีความเชิงบริบทยังต้องอาศัยการตัดสินใจจากผู้เชี่ยวชาญโดยตรง ระบบไม่สามารถทดแทนความเชี่ยวชาญทางกฎหมายได้ทั้งหมด

ตารางที่ 5-4 ข้อจำกัดของการวิจัยและผลกระทบ

5.4 ข้อเสนอแนะ

5.4.1 การฝึกโมเดลเพิ่มเติมสำหรับกฎหมายไทย

ขั้นตอนสำคัญถัดไปคือการฝึก WangchanBERTa เพิ่มเติมด้วยข้อมูลกฎหมายที่ผู้เชี่ยวชาญทำเครื่องหมายไว้ ซึ่งจะเพิ่มความแม่นยำของการจัดหมวดหมู่และการสกัดข้อมูล ส่งผลให้คะแนนหมวด B จากผู้เชี่ยวชาญในรุ่นต่อไปสูงขึ้น

5.4.2 การขยายฐานข้อมูลกฎหมายและกลุ่มตัวอย่าง

เพิ่มกฎหมายเฉพาะภาคส่วน และขยายการทดสอบกับองค์กรหลากหลายประเภทมากขึ้นเพื่อเพิ่มความเชื่อมั่นในผลการประเมิน

5.4.3 การพัฒนาต่อยอด

ควรพัฒนาต่อด้านการเชื่อมต่อกับระบบบริหารความเสี่ยงองค์กร การรองรับกฎหมายข้ามพรมแดน การเฝ้าระวังแบบเรียลไทม์ และแอปพลิเคชันมือถือ

5.5 สรุปปิดท้าย

งานวิจัยนี้พัฒนาระบบปัญญาประดิษฐ์สถาปัตยกรรม Hybrid Pipeline 7 ขั้นตอน สำหรับแปลงกฎหมายความมั่นคงปลอดภัยไซเบอร์ไทย 3 ฉบับให้เป็นรายการตรวจสอบที่ปฏิบัติได้จริงในองค์กร โดยเชื่อมโยงกับมาตรฐาน ISO/IEC 27001:2022 และ NIST CSF 2.0 อัตโนมัติ และผ่านกระบวนการรับรองจากผู้เชี่ยวชาญ 3 ท่านก่อนเผยแพร่ทุกครั้ง

ผลการประเมินยืนยันว่าระบบสามารถลดกำแพงระหว่างภาษากฎหมายที่ซับซ้อนและการปฏิบัติงานด้านไอทีได้อย่างมีประสิทธิภาพ โดยได้รับคะแนนเฉลี่ยรวม 4.23 จากผู้เชี่ยวชาญและ 4.33 จากองค์กรตัวอย่าง ซึ่งอยู่ในระดับมากทุกหมวด ผลนี้สอดคล้องกับสมมติฐานการวิจัยที่ว่าแนวทาง Hybrid AI ที่รวมกฎเกณฑ์กับโมเดลภาษาจะให้ผลลัพธ์ที่น่าเชื่อถือและอธิบายได้สำหรับงานกฎหมายไทย

ระบบที่พัฒนาขึ้นสร้างรากฐานสำหรับฐานความรู้กฎหมายไซเบอร์ไทยที่พัฒนาต่อเนื่องได้ กลไก Rule Learning ที่สะสมกฎการแก้ไขจากผู้เชี่ยวชาญทำให้ระบบแม่นยำขึ้นตามปริมาณข้อมูลที่สะสม และสถาปัตยกรรมแบบ Microservices ใน Docker ทำให้สามารถขยายรองรับกฎหมายใหม่และเทคโนโลยี AI รุ่นถัดไปได้โดยไม่ต้องออกแบบระบบใหม่ทั้งหมด

แนวทางการวิจัยนี้สามารถเป็นต้นแบบสำหรับการพัฒนาระบบ Legal AI สำหรับกฎหมายไทยในสาขาอื่นๆ ต่อไป เช่น กฎหมายภาษี กฎหมายแรงงาน และกฎระเบียบสิ่งแวดล้อม ซึ่งต่างมีความซับซ้อนของภาษากฎหมายไทยในรูปแบบที่คล้ายคลึงกัน

บรรณานุกรม

1. Digital Government Development Agency (DGA). Thailand Cybersecurity and Data Protection Framework. Digital Government Development Agency, 2024.
2. Tiwari, R., and S. Shanmugam. “Compliance Management, Compliance and Technical Documentation Management.” Conference Paper, 2024.
3. Deshpande, A. “Regulatory Compliance and AI: Navigating the Legal and Regulatory Challenges of AI in Finance.” Conference Paper, 2024.
4. PDPC Thailand. Guideline for SMEs on PDPA Compliance. Office of the Personal Data Protection Committee, 2023.
5. Nithya, M., S. Harini, S. Kavyadharshini, and K. Srinidhi. “AI-Driven Legal Automation to Enhance Legal Processes with Natural Language Processing.” Conference Paper, 2024.
6. Shaik, A. S., M. Mahima, J. Sravanthi, H. M. Ali, R. Agarwal, and V. D. Ganesh. “Machine Learning Applications for Enhancing Regulatory Compliance in Blockchain-Based Supply Chains.” Conference Paper, 2024.
7. Office of the Personal Data Protection Committee (PDPC). Guidelines for Compliance with the Personal Data Protection Act B.E. 2562 (2019). Office of the Personal Data Protection Committee, 2022. [In Thai].
8. Ministry of Digital Economy and Society (MDES). National Cybersecurity Measures and Guidelines of Thailand. Ministry of Digital Economy and Society, 2023. [In Thai].
9. Annu, K., and K. Audichya. “Evaluating Cybersecurity Compliance through Legal Jurisprudence: A Machine Learning Approach to Predicting Court Decisions.” Conference Paper, 2025.
10. Alapati, N. K. "AI in Risk Modeling for ESG Banking Compliance: A Multi-Layered Intelligence Framework." Proc. APCIT, 2025.
11. Venkatesan, V. and Arunachalam, C. "AI-Driven Digital Twin Framework for Security Threat Simulation and Compliance Optimization." Proc. ICCST, 2025.

12. Ali, F. A. R. et al. "Automated Regulatory Compliance Verification for GDPR and ePrivacy Directives Using Hybrid Systems and XAI Models." Proc. ICCR, 2025.

ประวัติผู้เขียน

ชื่อ พลวัฒน์ สามพ่วงบุญ

ชื่อการค้นคว้าอิสระ ระบบปัญญาประดิษฐ์สำหรับสกัดและเชื่อมโยงข้อกำหนดกฎหมายไซเบอร์ไทยเพื่อสร้างรายการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ

สาขาวิชา การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ประวัติ เกิดเมื่อวันที่ 2 พฤษภาคม 2534 ปัจจุบันอายุ 34 ปี โดยเกิดที่จังหวัดกรุงเทพมหานคร เข้าศึกษาระดับปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ ที่มหาวิทยาลัยสยาม จนสำเร็จการศึกษาในปีการศึกษา 2560 และเข้าศึกษาต่อระดับปริญญาโท สาขาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ในด้านการทำงาน มีประสบการณ์ดังต่อไปนี้

- พ.ศ. 2556 – 2559 ช่างเทคนิคระบบสารสนเทศ บริษัท ห้างหุ้นส่วนจำกัด เจ.เจ.แอล. คอมพิวเตอร์ เมนเทแนนซ์ เซอร์วิส
- พ.ศ. 2559 – 2564 หัวหน้าทีมวิศวะกรระบบสารสนเทศ บริษัท ซอฟท์เดบู จำกัด
- พ.ศ. 2564 – 2566 ผู้จัดการบริหารระบบสารสนเทศอาวุโส พ.ศ. 2567 – 2568 ผู้จัดการบริหารความปลอดภัยสารสนเทศอาวุโส บริษัท เทเวศประกันภัย จำกัด (มหาชน)
- พ.ศ. 2568 – 2569 ผู้จัดการที่ปรึกษาด้านความปลอดภัยและการปฏิบัติตามข้อบังคับ บริษัท ไซเบอร์เซ็คเอ็กซ์ จำกัด