แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

นายพชรพล สัตยพงศ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568

แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

นายพชรพล สัตยพงศ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568

ใบรับรองวิทยานิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

โดย นายพชรพล สัตยพงศ์

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม

..... คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

(ผู้ช่วยศาสตราจารย์ ดร.สุพจน์ จันทร์วิพัฒน์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(รองศาสตราจารย์ ดร.สมชาย ปราการเจริญ)

..... อาจารย์ที่ปรึกษา

(รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร)

..... กรรมการ

(อาจารย์ ดร.กาญจนา วิริยะพันธ์)

ชื่อ : นายพชรพล สัตยพงศ์
ชื่อวิทยานิพนธ์ : แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ
สาขาวิชา : วิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก : รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร
ปีการศึกษา : 2568

บทคัดย่อ

การศึกษานี้มีเป้าหมายเพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศในประเทศไทย โดยใช้การวิจัยเชิงคุณภาพ (Qualitative Research) ผ่านการสัมภาษณ์เชิงลึก (In-depth Interview) กับผู้เชี่ยวชาญ 6 คน ผลการศึกษาพบว่าปัจจัยสำคัญที่ส่งเสริมความสำเร็จ ได้แก่ ความเป็นอิสระของผู้ตรวจสอบ ความเชี่ยวชาญด้านเทคโนโลยี ความสามารถในการวิเคราะห์ความเสี่ยง ความรู้เกี่ยวกับมาตรฐานและกฎระเบียบ ตลอดจนการสนับสนุนจากผู้บริหารองค์กร ซึ่งล้วนมีบทบาทสำคัญต่อคุณภาพและประสิทธิภาพของกระบวนการตรวจสอบ

การศึกษานี้นำเสนอโมเดลการตรวจสอบเทคโนโลยีสารสนเทศ 5 ขั้นตอน ได้แก่ การวิเคราะห์ความเสี่ยง การวางแผน การดำเนินการตรวจสอบ การจัดทำรายงาน และการติดตามผล โดยเน้นความสำคัญของการวิเคราะห์ความเสี่ยง และการติดตามผลเพื่อเพิ่มประสิทธิภาพให้สอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยี ทั้งนี้ การพัฒนาและฝึกอบรมทักษะของผู้ตรวจสอบอย่างต่อเนื่องช่วยยกระดับความแม่นยำ ความน่าเชื่อถือ และคุณภาพของกระบวนการตรวจสอบ

งานวิจัยนี้ไม่เพียงแค่เสนอแนวทางปฏิบัติที่ดีในการตรวจสอบเทคโนโลยีสารสนเทศ แต่ยังให้ข้อมูลเชิงลึกที่สามารถนำไปใช้ปรับปรุงกระบวนการตรวจสอบในองค์กรให้มีประสิทธิภาพและตอบสนองต่อความเสี่ยงในโลกดิจิทัลได้อย่างทันท่วงทีและเหมาะสม

(มีจำนวนทั้งสิ้น 64 หน้า)

คำสำคัญ : เทคโนโลยีสารสนเทศ การตรวจสอบด้านเทคโนโลยีสารสนเทศ แนวทางปฏิบัติในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

_____ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Name : Mr. Pacharapon Sattayapong
Thesis Title : Good Practices in Information Technology Auditing.
Major Field : Data Science for Innovation
King Mongkut's University of Technology North Bangkok
Thesis Advisor : Associate Professor DR. Nalinpat Bhumpenpein
Academic Year : 2025

ABSTRACT

This study aims to analyze the factors contributing to the success of IT audits in Thailand using qualitative research through in-depth interviews with six experts. The findings reveal that key factors for success include auditor independence, technological expertise, risk analysis capability, knowledge of standards and regulations, as well as support from organizational management. These factors play a crucial role in enhancing the quality and effectiveness of the audit process.

This study presents a five-step IT audit model, which includes risk analysis, audit planning, audit execution, report preparation, and follow-up. It emphasizes the importance of risk analysis and follow-up in enhancing audit efficiency to keep pace with technological changes. Furthermore, continuous training and skill development for auditors play a vital role in improving accuracy, reliability, and overall audit quality. This research not only presents best practices in IT auditing but also provides valuable insights that can be used to improve auditing processes within organizations, ensuring they are effective and responsive to risks in the digital world.

(Total 64 Pages)

Keywords: Information Technology, Information Technology Audit, Information Technology Audit Practices

_____ Advisor

กิตติกรรมประกาศ

ข้าพเจ้าขอกราบขอบพระคุณ รองศาสตราจารย์ ดร.นลินภัสร์ บำเพ็ญเพียร อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก ที่ให้คำแนะนำ คำปรึกษา และชี้แนะแนวทางในการทำวิทยานิพนธ์ฉบับนี้ด้วยความเอาใจใส่ อาจารย์ได้ให้ความรู้ องค์ความคิด และข้อเสนอแนะที่มีค่าอย่างยิ่ง ซึ่งทำให้ข้าพเจ้าสามารถพัฒนาผลงานวิจัยนี้ให้สมบูรณ์และมีคุณภาพมากยิ่งขึ้น

นอกจากนี้ ข้าพเจ้าขอขอบคุณผู้ให้สัมภาษณ์เกี่ยวกับการเก็บข้อมูลต่างๆ รวมถึงเพื่อนร่วมรุ่น และบุคคลที่มีส่วนเกี่ยวข้องทุกท่าน ที่ให้การสนับสนุนและกำลังใจจนข้าพเจ้าสามารถดำเนินการวิจัยจนสำเร็จลุล่วง

ท้ายที่สุด ข้าพเจ้าขอขอบพระคุณครอบครัวที่เป็นกำลังใจสำคัญ คอยสนับสนุนและให้กำลังใจในทุกช่วงเวลาของการศึกษาและการทำวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อวงวิชาการและผู้ที่สนใจศึกษาในสาขานี้ต่อไป

พชรพล สัตยพงศ์

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในภาพรวมธุรกิจปัจจุบัน เทคโนโลยีสารสนเทศมีบทบาทสำคัญในการขับเคลื่อนประสิทธิภาพในกระบวนการต่าง ๆขององค์กร อย่างไรก็ตาม ประโยชน์ของเทคโนโลยีสารสนเทศมาพร้อมกับความเสี่ยงมากมาย ความเสี่ยงเหล่านี้รวมถึงการดัดแปลงข้อมูลที่อาจเกิดขึ้น การระบาดของไวรัส การละเมิดข้อมูล ความล้มเหลวของระบบ และการสูญเสียทางการเงิน ซึ่งบางครั้งอาจทำให้การลงทุนในเทคโนโลยีสารสนเทศดูน่าหวาดหวั่น (ประจิต หาวัตรและศรัณย์ ชูเกียรติ, 2560) ดังนั้นเมื่อองค์กรต่าง ๆ เริ่มมีการใช้เทคโนโลยีสารสนเทศ จำเป็นต้องพิจารณาความเสี่ยงที่ตามมาอย่างรอบคอบด้วย ความเสี่ยงเหล่านี้มีแนวโน้มที่จะขัดขวางการดำเนินงาน ลดความสมบูรณ์ของข้อมูล และแม้กระทั่งนำไปสู่การสูญเสียจำนวนมาก ช่องโหว่นี้เด่นชัดเป็นพิเศษในช่วงวิกฤตที่ไม่คาดฝัน เช่น การระบาดของไวรัสโควิด-19 เป็นต้น

ในกรณีที่องค์กรต่าง ๆ นำโมเดลการทำงานจากระยะไกลมาใช้ การพึ่งพาเทคโนโลยียิ่งเพิ่มสูงขึ้น ด้วยเหตุนี้ การประเมินและเสริมสร้างโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศขององค์กรจึงเป็นสิ่งจำเป็นและมีความสำคัญ การทำงานจากระยะไกลทำให้เกิดความท้าทายและช่องโหว่ใหม่ ๆ ทำให้การตรวจสอบเทคโนโลยีสารสนเทศภายในองค์กรเป็นเรื่องสำคัญเร่งด่วน

โดยพื้นฐานแล้ว สิ่งนี้เน้นย้ำถึงบทบาทที่สำคัญของการตรวจสอบด้านเทคโนโลยีสารสนเทศที่ครอบคลุม ด้วยการดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างละเอียด องค์กรต่าง ๆ จึงสามารถระบุและแก้ไขช่องโหว่ในเชิงรุก สนับสนุนมาตรการรักษาความปลอดภัยทางไซเบอร์ รับรองการปฏิบัติตามกฎระเบียบ และปกป้องการดำเนินงานและความต่อเนื่องทางธุรกิจในท้ายที่สุด (ประจิต หาวัตรและศรัณย์ ชูเกียรติ, 2560)

ด้วยเหตุนี้ ผู้วิจัยจึงสนใจที่จะศึกษาปัจจัยสำคัญที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศและนำเสนอแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ เนื่องจากปัจจุบันการศึกษาวิจัยถึงการตรวจสอบด้านเทคโนโลยีสารสนเทศยังมีอยู่อย่างจำกัด และมีการพูดถึงปัจจัยที่ส่งผลให้การตรวจสอบด้านเทคโนโลยีสารสนเทศประสบความสำเร็จค่อนข้างน้อย เห็นได้จากงานวิจัยที่ผู้วิจัยได้นำมาอ้างอิง ที่ได้มีการนำงานวิจัยที่เกี่ยวข้องกับการตรวจสอบบัญชีกับการตรวจสอบภายในเข้ามาศึกษาเพิ่มเติมด้วย

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษาปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

1.2.2 เพื่อนำเสนอแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

1.3 ขอบเขตของการวิจัย

งานวิจัยนี้ศึกษาแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งงานวิจัยนี้เป็นงานวิจัยเชิงปริมาณมุ่งศึกษาค้นคว้าเพื่อศึกษาปัจจัยสำคัญที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยประชากรที่ใช้ในงานวิจัย คือ ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศในประเทศไทย และไม่ทราบจำนวนประชากร

1.4 นิยามศัพท์เฉพาะ

1.4.1 เทคโนโลยีสารสนเทศ (Information Technology: IT) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ (มหาวิทยาลัยราชภัฏรำไพพรรณี, 2564)

1.4.2 การตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Audit: IT Audit) หมายถึง การตรวจสอบควบคุมระบบสารสนเทศที่มีอยู่ของหน่วยงาน เพื่อให้ทราบว่าการควบคุมนั้นๆ มีเพียงพอหรือไม่ (ภาพร ภิยโยดิลกชัย, 2553) หรือหมายถึง กระบวนการรวบรวมและพิจารณาหลักฐานต่าง ๆ เพื่อประเมินว่า ระบบคอมพิวเตอร์ได้รับการออกแบบให้มีความมั่นคงด้านข้อมูล มีการปกป้องทรัพย์สิน ช่วยให้ผู้ใช้สามารถใช้ระบบด้อย่างมีประสิทธิภาพ และตอบสนองวัตถุประสงค์และบรรลุเป้าหมายขององค์กรได้อย่างมีประสิทธิผล (มหาวิทยาลัยราชภัฏรำไพพรรณี, 2564)

1.5 ประโยชน์ที่ได้รับ

1.5.1 การพัฒนากระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ

การวิจัยนี้จะช่วยในการพัฒนากระบวนการและแนวทางที่สามารถปรับปรุงคุณภาพการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยการเน้นปัจจัยสำคัญ เช่น ความเป็นอิสระของผู้ตรวจสอบ ความรู้ทางเทคโนโลยี จรรยาบรรณ และการสนับสนุนจากผู้บริหาร เป็นต้น ซึ่งช่วยให้การดำเนินงานตรวจสอบมีความโปร่งใสและประสิทธิภาพมากยิ่งขึ้น

1.5.2 การพัฒนาแนวทางการตรวจสอบที่สอดคล้องกับมาตรฐานสากล

การวิจัยนี้จะช่วยให้มีการพัฒนาแนวทางที่สอดคล้องกับมาตรฐานการตรวจสอบที่ยอมรับในระดับสากล เช่น การประเมินความเสี่ยง การวางแผนการตรวจสอบอย่างมีประสิทธิภาพ และการวิเคราะห์ความเสี่ยง เพื่อให้การตรวจสอบในด้านเทคโนโลยีสารสนเทศมีความครอบคลุมและถูกต้องตามหลักการที่กำหนด

1.5.3 การสนับสนุนในการสร้างความไว้วางใจระหว่างผู้ตรวจสอบและผู้ถูกตรวจสอบ

การรักษาความเป็นกลางและจรรยาบรรณในการตรวจสอบจะช่วยเพิ่มความไว้วางใจจากผู้ถูกตรวจสอบ และสร้างความน่าเชื่อถือในผลการตรวจสอบ ซึ่งจะมีผลต่อการยอมรับผลการตรวจสอบและการปฏิบัติตามข้อเสนอแนะที่เกิดขึ้นจากการตรวจสอบ

1.5.4 การปรับปรุงระบบการวางแผนการตรวจสอบ

การวางแผนการตรวจสอบที่มีประสิทธิภาพ ซึ่งได้รับการพัฒนาจากการวิจัยนี้ จะช่วยให้สามารถเลือกหน่วยงานและระบบงานที่มีความเสี่ยงสูงมาทำการตรวจสอบก่อน และจะช่วยลดเวลาที่สูญเสียในการตรวจสอบในพื้นที่ที่มีความเสี่ยงต่ำ

1.5.5 การช่วยให้ผู้บริหารสามารถสนับสนุนการตรวจสอบได้อย่างมีประสิทธิภาพ

การศึกษาผลกระทบจากการสนับสนุนของผู้บริหารจะช่วยให้ผู้บริหารเข้าใจถึงความสำคัญของการตรวจสอบด้านเทคโนโลยีสารสนเทศ และสามารถให้ความร่วมมือในการดำเนินงานได้อย่างราบรื่น นอกจากนี้ยังสามารถช่วยในการกำหนดทรัพยากรและสนับสนุนการแก้ไขปัญหาหลังจากผลการตรวจสอบ

1.5.6 การพัฒนาความสำเร็จของการตรวจสอบ

ด้วยการประยุกต์ใช้ปัจจัยที่ได้รับจากการวิจัย เช่น การใช้มาตรฐานการตรวจสอบที่ทันสมัย การมีทักษะทางเทคโนโลยีสารสนเทศที่เหมาะสม และการวางแผนการตรวจสอบอย่างรัดกุม งานวิจัยนี้จะช่วยเพิ่มโอกาสในการประสบความสำเร็จของการตรวจสอบในองค์กร และช่วยลดความเสี่ยงที่อาจเกิดขึ้นจากการตรวจสอบที่ไม่สมบูรณ์

1.5.7 การสร้างพื้นฐานสำหรับการพัฒนาแนวทางปฏิบัติที่ดีในอนาคต

การวิจัยนี้จะช่วยให้สามารถพัฒนาแนวทางการตรวจสอบที่ดียิ่งขึ้นในอนาคต โดยการใช้ผลการวิจัยเป็นฐานในการปรับปรุงขั้นตอนและกระบวนการให้มีความเหมาะสมกับเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การวิจัยนี้ผู้วิจัยได้ศึกษาถึงกรอบแนวคิด ทฤษฎี เอกสาร และงานวิจัยที่เกี่ยวข้องกับการศึกษาเรื่อง “แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ” ซึ่งแบ่งเป็นหัวข้อดังต่อไปนี้

2.1 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2.2 แนวทางปฏิบัติในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

2.3 กฎหมายด้านเทคโนโลยีสารสนเทศ

2.4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

2.5 ปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

2.6 แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

2.1 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ได้ให้คำจำกัดความของเทคโนโลยีสารสนเทศ (IT) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) โดยสรุปได้ดังนี้

เทคโนโลยีสารสนเทศ (Information Technology: IT) การใช้เทคโนโลยีในธุรกิจครอบคลุมข้อมูล ระบบปฏิบัติการ ระบบงาน ฐานข้อมูล ฮาร์ดแวร์ และระบบเครือข่ายสื่อสาร (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2565)

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk: IT Risk) ความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ รวมถึงภัยคุกคามทางไซเบอร์ ซึ่งอาจส่งผลกระทบต่อการดำเนินธุรกิจ ความมั่นคงของข้อมูล และความเชื่อมั่นของตลาดทุน (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2565)

ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security: IT Security) การรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล รวมถึงความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2565

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประกอบธุรกิจขององค์กร สามารถแบ่งออกเป็น 4 ประเภทหลัก (สำนักงาน กลต, ที่ ธ.(ว) 32/2545) ดังนี้

ประเภทที่ 1 Access Risk เป็นความเสี่ยงจากการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจ ซึ่งอาจนำไปสู่การล่วงรู้และใช้ข้อมูลโดยมิชอบ หรือทำให้การปฏิบัติงานไม่มีประสิทธิภาพ

ประเภทที่ 2 Integrity Risk เป็นความเสี่ยงจากความไม่ถูกต้องของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการแก้ไขข้อมูลโดยไม่มีอำนาจ หรือการประมวลผลที่ผิดพลาด

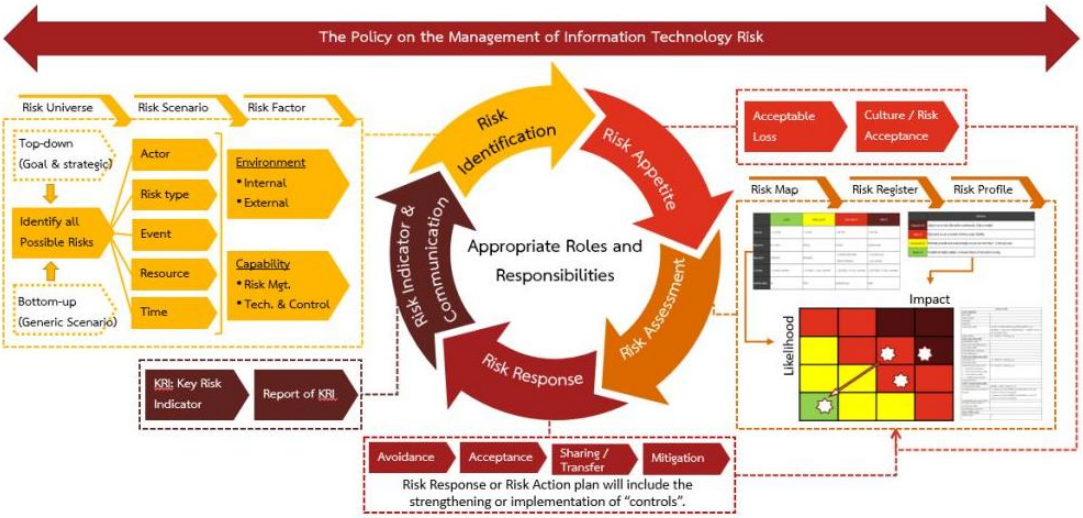
ประเภทที่ 3 Availability Risk เป็นความเสี่ยงจากการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง ซึ่งอาจทำให้การดำเนินธุรกิจหยุดชะงัก

ประเภทที่ 4 Infrastructure Risk เป็นความเสี่ยงจากการที่องค์กรไม่มีการบริหารจัดการเทคโนโลยีสารสนเทศที่ดี รวมถึงไม่มีระบบคอมพิวเตอร์และบุคลากรที่เพียงพอในการสนับสนุนธุรกิจ

2.2 แนวทางปฏิบัติในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (2562) ได้ให้แนวทางปฏิบัติในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ไว้ดังนี้

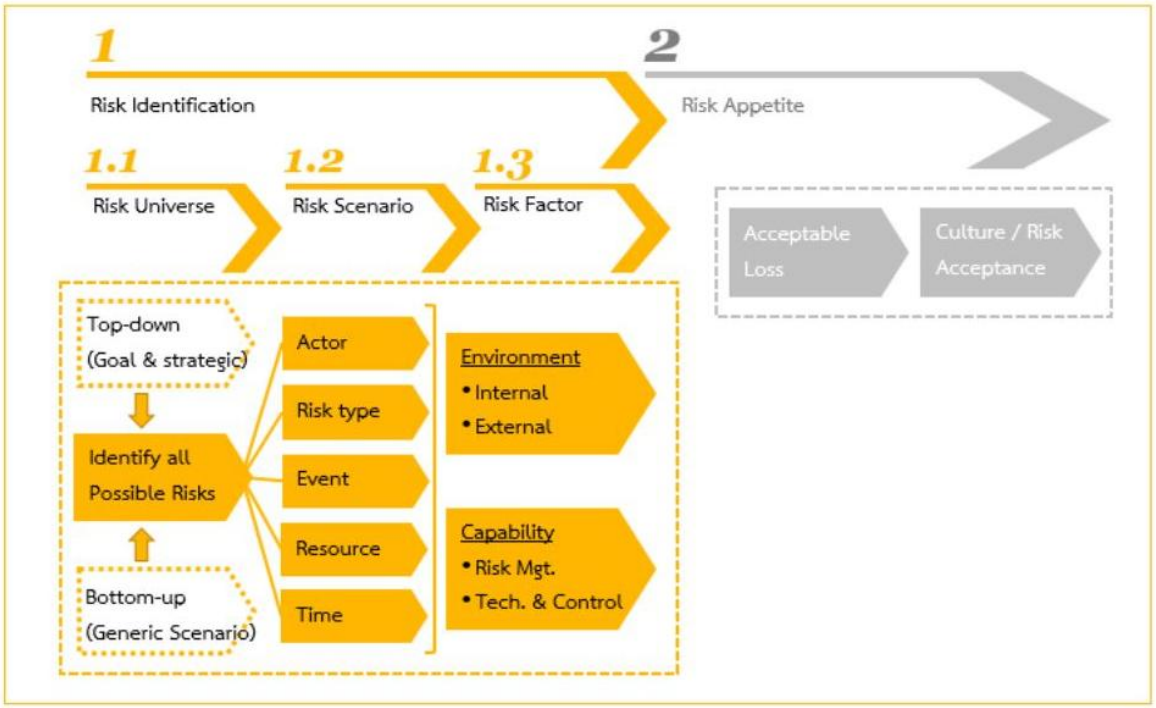
เพื่อให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพ ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยนโยบายนี้ควรได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจ สื่อสารไปยังผู้ที่เกี่ยวข้อง และทบทวนหรือปรับปรุงนโยบายอย่างสม่ำเสมอ นอกจากนี้ควรกำหนดขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายดังกล่าว กระบวนการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศควรดำเนินการอย่างต่อเนื่อง ประกอบด้วยกระบวนการดังสรุปในภาพประกอบที่ 2-1



ภาพที่ 2-1 กรอบการบริการ และจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

(ที่มา : สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2562)

1) การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related Risk Identification) ประกอบด้วย 3 ขั้นตอนย่อย ดังนี้



ภาพที่ 2-2 การระบุความเสี่ยง

(ที่มา : สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2562

ขั้นตอนย่อยที่ 1 ความเสี่ยงที่เป็นไปได้ทั้งหมด (Risk Universe)

การระบุความเสี่ยงที่เป็นไปได้ทั้งหมด (Risk Universe) เริ่มต้นจากการพิจารณาวัตถุประสงค์ของแผนกลยุทธ์ กระบวนการทางธุรกิจ และระบบสารสนเทศที่สนับสนุนกิจกรรมทางธุรกิจ รวมถึงโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง การทำเช่นนี้ช่วยกำหนดขอบเขตในการบริหารความเสี่ยงและทำให้ผู้บริหารเห็นภาพรวมของความเสี่ยงทั้งหมดที่ต้องจัดการ

ขั้นตอนย่อยที่ 2 เหตุการณ์ความเสี่ยง (Risk Scenario)

เหตุการณ์ความเสี่ยง คือ เหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการบรรลุวัตถุประสงค์ของผู้ประกอบธุรกิจ ทั้งในด้านบวกและด้านลบ โดยเหตุการณ์ความเสี่ยงทางเทคโนโลยีสารสนเทศควรระบุครอบคลุมองค์ประกอบดังนี้

องค์ประกอบที่ 1 ผู้กระทำให้เกิดความเสี่ยง (Actor) หมายถึง บุคคล กลุ่มบุคคล หรือองค์กรที่เกี่ยวข้องกับภัยคุกคาม เช่น พนักงาน ลูกจ้าง หุ้นส่วน ผู้ให้บริการภายนอก คู่แข่ง คู่ค้า หรือหน่วยงานกำกับดูแล

องค์ประกอบที่ 2 ประเภทของภัยคุกคาม หรือประเภทของความเสี่ยง (Threat type or Risk type) หมายถึง ลักษณะของความเสี่ยงหรือภัยคุกคาม เช่น ความเสี่ยงจากการปฏิบัติงานบุคลากรภายในและภายนอก หรือข้อผิดพลาดตามธรรมชาติ

องค์ประกอบที่ 3 เหตุการณ์ที่อาจเกิดขึ้น (Event) ตัวอย่างเช่น มีการรั่วไหลของข้อมูลสำคัญ มีการหยุดชะงักของระบบสารสนเทศมีการขโมยหรือสูญหายของทรัพยากรสารสนเทศ การละเมิดกฎระเบียบข้อบังคับต่าง ๆ รวมทั้งการใช้ทรัพยากรสารสนเทศอย่างไม่เหมาะสม

องค์ประกอบที่ 4 สินทรัพย์หรือทรัพยากรที่เกี่ยวข้อง (Asset/Resource) หมายถึง สินทรัพย์หรือทรัพยากรที่ที่ได้รับผลกระทบจากความเสี่ยง เช่น บุคลากร ความสามารถของบุคลากร โครงสร้างองค์กร กระบวนการทางด้านเทคโนโลยีสารสนเทศ ข้อมูล โปรแกรม และระบบงานต่าง ๆ

องค์ประกอบที่ 5 ช่วงเวลา หรือระยะเวลาที่เกิดเหตุการณ์ (Time) อันได้แก่ ความยาวของระยะเวลาของเหตุการณ์ความเสี่ยงช่วงเวลาที่เหตุการณ์ความเสี่ยงอาจเกิดขึ้น โดยอาจรวมถึงระยะเวลาในการตรวจพบเหตุการณ์ความเสี่ยงหรือระยะเวลาที่ผลกระทบจากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้น

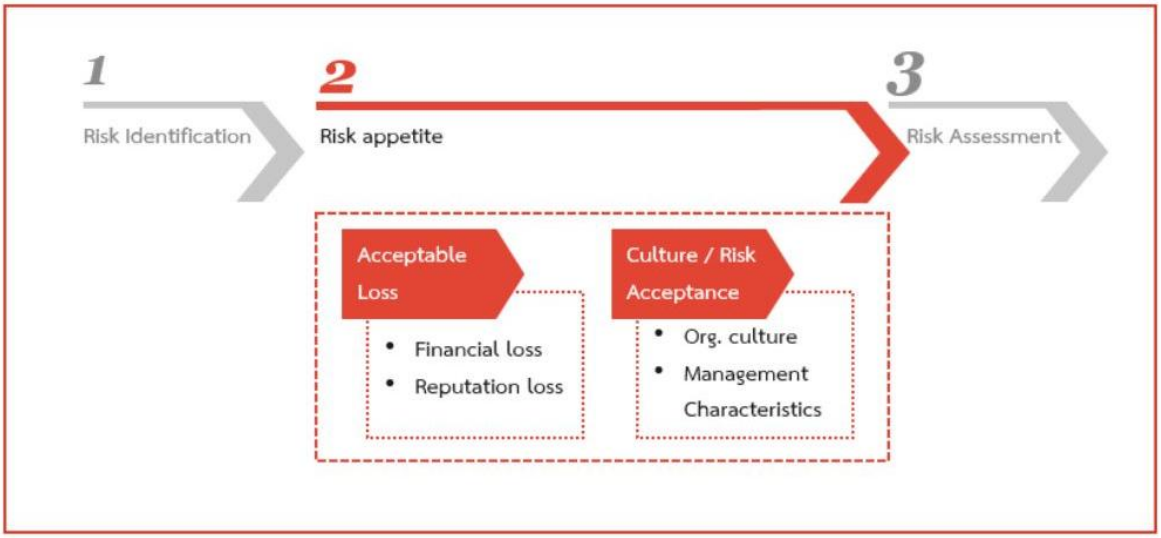
ขั้นตอนย่อยที่ 3 ปัจจัยความเสี่ยง (Risk Factors)

ปัจจัยความเสี่ยง คือ ปัจจัยที่มีผลกระทบต่อความถี่และผลกระทบของเหตุการณ์ความเสี่ยง (Risk Scenario) ซึ่งอาจมีลักษณะที่แตกต่างกัน โดยสามารถจัดประเภทได้ 2 กลุ่ม ได้แก่ กลุ่มที่ 1 สภาพแวดล้อมการดำเนินงานขององค์กร คือ สภาพแวดล้อมหรือเหตุการณ์ที่เพิ่มโอกาสเกิดหรือผลกระทบจากเหตุการณ์ความเสี่ยง โดยสามารถแบ่งเป็น 2 ส่วนหลัก ได้แก่ 1) สภาพแวดล้อมภายนอก และ 2) สภาพแวดล้อมภายใน กลุ่มที่ 2 ความสามารถในการบริหารจัดการทางด้าน

เทคโนโลยีสารสนเทศขององค์กร โดยสามารถแบ่งออกเป็น 2 ส่วน ได้แก่ 1) ความสามารถในการบริหารและจัดการความเสี่ยง และ 2) ความสามารถทางด้านเทคโนโลยีสารสนเทศ และการควบคุมทางด้านเทคโนโลยีสารสนเทศ

2) ความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite)

ความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite) คือ ปริมาณความเสี่ยงที่องค์กรสามารถยอมรับเมื่อมีความเสี่ยงเกิดขึ้น โดยพิจารณาระดับความสูญเสียที่องค์กรสามารถยอมรับได้ ทั้งทางด้านการเงินและชื่อเสียง รวมถึงวัฒนธรรมขององค์กรและระดับการยอมรับความเสี่ยงของผู้บริหาร ซึ่งอาจรวมถึงลักษณะการบริหารด้วย



ภาพที่ 2-3 การกำหนดระดับความเสี่ยงที่ยอมรับได้

(ที่มา : สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2562)

3) การประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (IT Risk Assessment)

จากเหตุการณ์ความเสี่ยงที่ระบุไว้ ผู้ประกอบธุรกิจควรมีกระบวนการในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อประเมินระดับความสำคัญ ควรดำเนินการโดยมีขั้นตอนย่อยดังนี้

ขั้นตอนย่อยที่ 1 ประเมินโอกาสเกิดและผลกระทบที่อาจเกิดขึ้นทั้งในด้านบวกและด้านลบของแต่ละเหตุการณ์ความเสี่ยง ผลการประเมินอาจนำเสนอในรูปแบบของแผนภาพความเสี่ยง (Risk Map) ที่แสดงระดับโอกาสเกิดและผลกระทบ (Risk Scale) ของแต่ละเหตุการณ์ความเสี่ยง จากนั้นจัดทำทะเบียนความเสี่ยง (Risk Register) ซึ่งบรรยายข้อมูลรายละเอียดของความเสี่ยงที่ระบุไว้

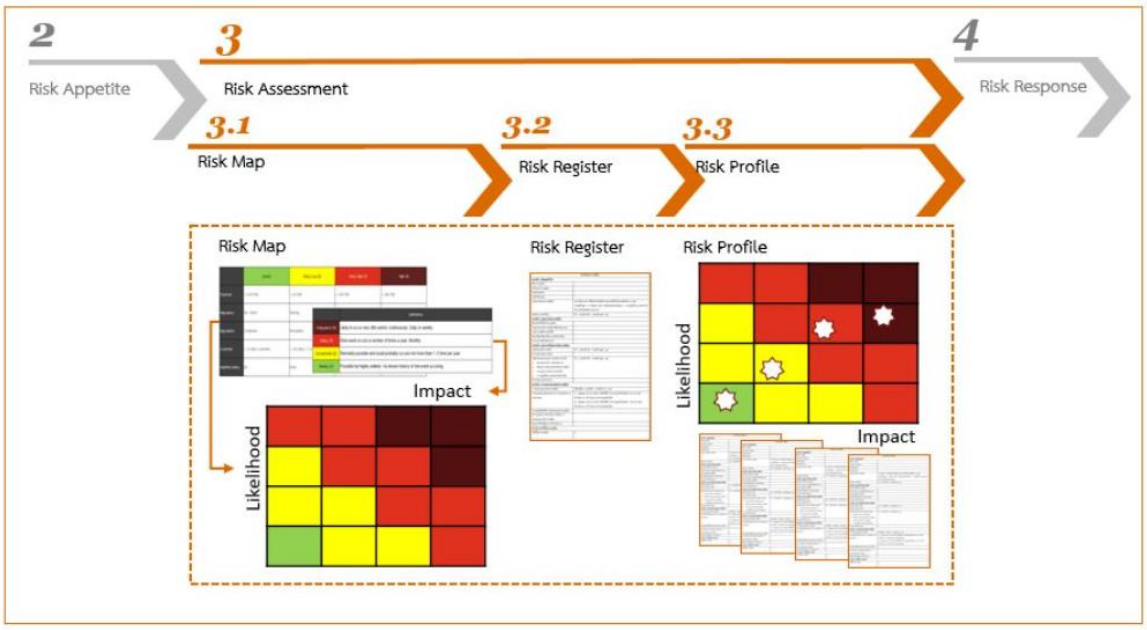
ขั้นตอนย่อยที่ 2 จัดทำโครงร่างของความเสี่ยง (Risk Profile) รวบรวมความเสี่ยงทั้งหมดและแสดงสถานะของความเสี่ยงในปัจจุบัน โดยพิจารณาทุกปัจจัยความเสี่ยงที่เกี่ยวข้อง รวมถึงกำหนดตัวควบคุมและความเสี่ยงที่ยังเหลืออยู่ภายหลังการควบคุม

ขั้นตอนย่อยที่ 3 เปรียบเทียบความเสี่ยงที่ยังเหลืออยู่ภายหลังการควบคุมกับความเสี่ยงที่องค์กรยอมรับได้ หากความเสี่ยงอยู่ในระดับที่เกินกว่าที่องค์กรยอมรับได้ ควรกำหนดวิธีการจัดการกับความเสี่ยงนั้น

ขั้นตอนย่อยที่ 4 วิเคราะห์ต้นทุนและประโยชน์ที่จะได้รับจากการจัดการความเสี่ยงในแต่ละรูปแบบ

ขั้นตอนย่อยที่ 5 ระบุความต้องการในภาพรวมของโครงการหรือระบบงานเพื่อระบุความเสี่ยงและความคาดหวังจากการควบคุมหลักที่ใช้ในการลดความเสี่ยงที่ตอบสนองต่อความต้องการของโครงการหรือระบบงานนั้น ๆ

ขั้นตอนย่อยที่ 6 ประเมินผลการวิเคราะห์ความเสี่ยงก่อนการตัดสินใจดำเนินการบริหารและจัดการความเสี่ยง เพื่อให้มั่นใจว่าการวิเคราะห์สอดคล้องกับความต้องการขององค์กรและการประเมินความเสี่ยงเป็นไปอย่างเหมาะสมและสมเหตุสมผล



ภาพที่ 2-4 การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(ที่มา : สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2562)

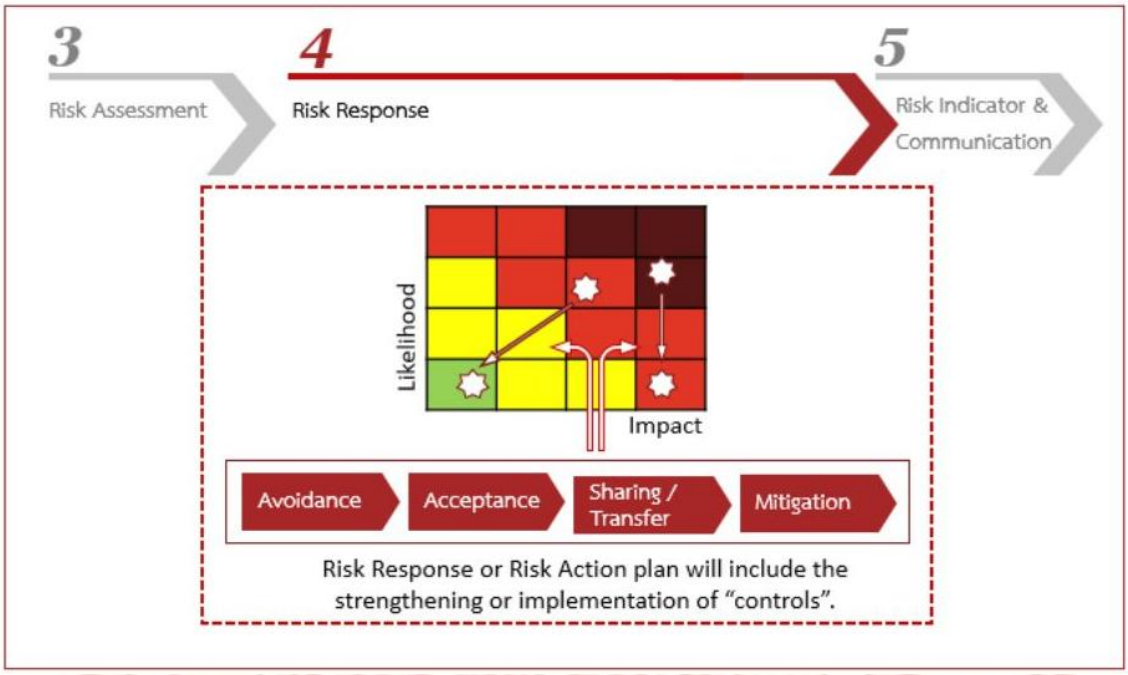
การประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ มีเครื่องมือที่ใช้ในการประเมินความเสี่ยง ดังนี้

เครื่องมือที่ 1 แผนภาพความเสี่ยง (Risk Map) เป็นเครื่องมือที่ใช้ในการประเมินระดับความสำคัญของความเสี่ยงที่ระบุไว้ และเพื่อให้ผู้ที่เกี่ยวข้องในการบริหารและจัดการความเสี่ยงสามารถจัดกลุ่มความเสี่ยงและบริหารจัดการได้อย่างมีประสิทธิผล การประเมินความเสี่ยงควรพิจารณาถึงสองส่วนประกอบหลัก คือ โอกาสเกิดและผลกระทบ ซึ่งเทคนิคในการนำเสนอความเสี่ยงที่นิยมใช้คือการใช้แผนภาพความเสี่ยง (Risk Map) โดยแผนภาพนี้จะช่วยแสดงระดับของโอกาสเกิดและผลกระทบของแต่ละเหตุการณ์ความเสี่ยง ทำให้การตัดสินใจในการจัดการความเสี่ยงมีความแม่นยำและชัดเจนยิ่งขึ้น

เครื่องมือที่ 2 ทะเบียนความเสี่ยง (Risk Register) เป็นเครื่องมือที่จัดขึ้นเพื่อบรรยายรายละเอียดและส่วนประกอบที่เกี่ยวข้องของแต่ละความเสี่ยงที่ระบุไว้ หลังจากจัดทำแผนภาพความเสี่ยงแล้ว ทะเบียนความเสี่ยงประกอบด้วยข้อมูลต่างๆ เช่น เจ้าของความเสี่ยง รายละเอียดเหตุการณ์ความเสี่ยง ผลการวิเคราะห์ความเสี่ยง รายละเอียดการควบคุม หรือกิจกรรมเพื่อตอบสนองหรือบริหารและจัดการความเสี่ยง รวมถึงสถานการณ์ดำเนินงานในปัจจุบัน การจัดทำทะเบียนความเสี่ยงนี้ช่วยให้การติดตามและการบริหารจัดการความเสี่ยงเป็นระบบและมีประสิทธิภาพมากยิ่งขึ้น

เครื่องมือที่ 3 โครงร่างของความเสี่ยง (Risk Profile) เป็นการรวบรวมแผนภาพและทะเบียนความเสี่ยงขององค์กร เพื่อแสดงสถานะปัจจุบันของความเสี่ยงและใช้ในการรายงานผลความเสี่ยง โดยอ้างอิงข้อมูลจากการวิเคราะห์ความเสี่ยงและตัวชี้วัดผลการปฏิบัติงาน ควรดำเนินการในกระบวนการเดียวกับการจัดทำโครงร่างความเสี่ยงของกระบวนการธุรกิจ และปรับปรุงอย่างน้อยปีละ 1 ครั้ง ขึ้นอยู่กับปัจจัยแวดล้อม โดยควรประกอบด้วยปัจจัยเสี่ยง ผลการประเมินความเสี่ยง ข้อมูลความเสียหายในอดีต ตัวชี้วัดผลการปฏิบัติงาน และผลการตรวจสอบล่าสุดที่เกี่ยวข้องกับความเสี่ยง

4) การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (Risk Response) เพื่อการวางแผนการจัดการความเสี่ยงที่เหมาะสมและตอบสนองต่อเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น องค์กรสามารถพิจารณาวิธีการในการรับมือกับความเสี่ยงใน 4 รูปแบบ ประกอบด้วย การหลีกเลี่ยงความเสี่ยง การยอมรับความเสี่ยง การร่วมจัดการหรือการถ่ายโอนความเสี่ยง และการลดความเสี่ยง



ภาพที่ 2-5 แนวทางการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(ที่มา : สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2562)

รูปแบบที่ 1 การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การหลีกเลี่ยงความเสี่ยง คือ การหลีกเลี่ยงกิจกรรมหรือสาเหตุที่อาจก่อให้เกิดความเสี่ยง ซึ่งโดยส่วนมากจะใช้วิธีการนี้ในกรณีที่ไม่มีการจัดการความเสี่ยงที่เหมาะสมในรูปแบบอื่นอีกแล้ว รวมทั้งผลกระทบจากความเสี่ยงนั้นอาจสูงเกินกว่าระดับที่องค์กรยอมรับได้ เช่น การยกเลิกโครงการที่มีความเสี่ยงสูง หรือการเปลี่ยนแปลงกระบวนการทำงานเพื่อลดความเสี่ยงที่อาจเกิดขึ้น

รูปแบบที่ 2 การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับความเสี่ยง คือ การที่องค์กรไม่กำหนดกิจกรรมใด ๆ เพื่อตอบสนองต่อความเสี่ยงที่อาจเกิดขึ้น โดยผู้บริหารยอมรับผลที่อาจเกิดขึ้นจากความเสี่ยงนั้น ๆ ซึ่งโดยส่วนมากจะใช้วิธีการนี้ในกรณีที่ผลกระทบจากความเสี่ยงต่ำกว่าต้นทุนในกิจกรรมที่ใช้บริหารและจัดการความเสี่ยงนั้น ข้อควรระวังในการวางแผนการจัดการความเสี่ยงแบบการยอมรับความเสี่ยง คือการกำหนดผู้ที่สามารถตัดสินใจยอมรับความเสี่ยงนั้น เนื่องจากความเสี่ยงทางด้านเทคโนโลยีสารสนเทศมีผลกระทบต่อการดำเนินงานทางธุรกิจในภาพรวม ดังนั้นองค์กรอาจต้องมีกระบวนการที่ชัดเจนในการระบุระดับของความเสี่ยงที่ยอมรับได้ รวมทั้งผู้ที่สามารถตัดสินใจยอมรับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศในกรณีต่าง ๆ

รูปแบบที่ 3 การร่วมจัดการความเสี่ยง/ถ่ายโอนความเสี่ยง (Risk Sharing/Transfer) การร่วมจัดการความเสี่ยง คือ การลดความถี่ในการเกิดหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น โดยกระจายหรือโอนไปยังบุคคลอื่น เช่น การทำประกันหรือการใช้งานผู้ให้บริการภายนอกในราคาคงที่

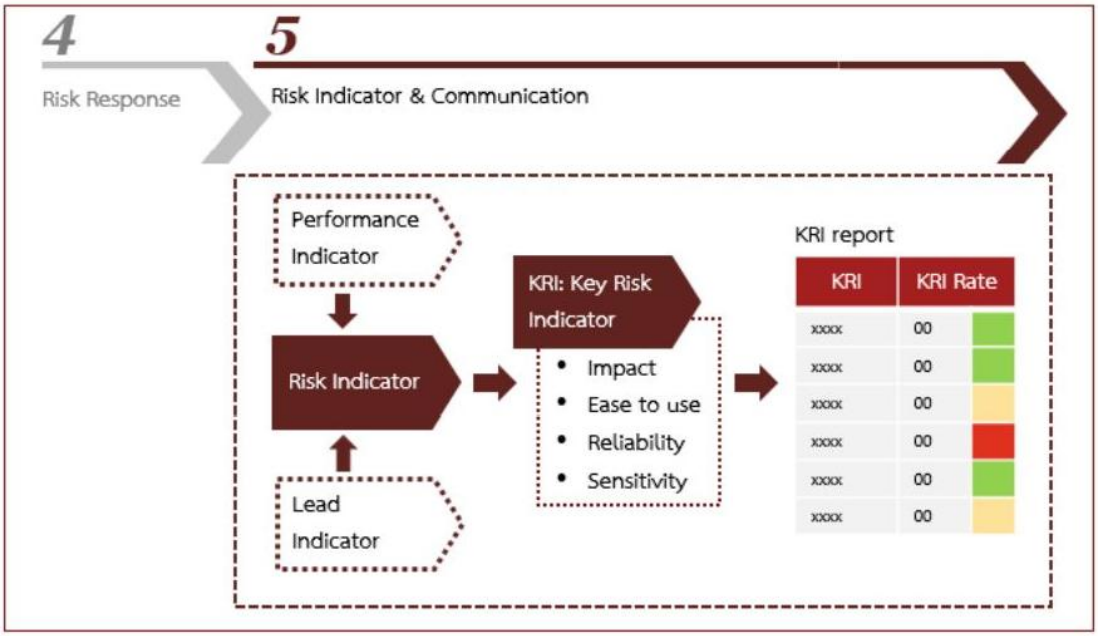
(fixed price) การถ่ายโอนความเสี่ยงนี้สามารถช่วยลดผลกระทบจากความเสี่ยงได้ แต่ไม่สามารถถ่ายโอนความรับผิดชอบจากความเสี่ยง ผู้ประกอบธุรกิจยังคงเป็นผู้มีหน้าที่รับผิดชอบในความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นได้

รูปแบบที่ 4 การลดความเสี่ยง (Risk Mitigation) การลดความเสี่ยงสามารถทำได้โดยการจัดให้มีกิจกรรมการควบคุมเพื่อลดความถี่ในการเกิดหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น โดยอาจทำได้ใน 2 รูปแบบคือ แบบที่ 1 กำหนดให้มีการบริหารและจัดการความเสี่ยงอย่างรัดกุม และแบบที่ 2 มีกิจกรรมการควบคุมเพื่อลดโอกาสเกิดหรือผลกระทบจากความเสี่ยงนั้น ๆ นอกจากนี้ยังอาจรวมถึงกิจกรรมอื่น ๆ ในการลดความเสี่ยง เช่น การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศที่เหมาะสม และการปรับใช้มาตรฐานต่าง ๆ ในการบริหารจัดการทางด้านเทคโนโลยีสารสนเทศ

ผู้ประกอบธุรกิจควรพิจารณาจัดระดับความสำคัญของรายการกิจกรรมเพื่อจัดการความเสี่ยงและเรียงลำดับในการจัดการความเสี่ยงตามระดับความสำคัญ เนื่องจากรายการกิจกรรมเพื่อจัดการความเสี่ยงทั้งหมดอาจใช้ทรัพยากรมากกว่าทรัพยากรที่องค์กรมีอยู่ โดยผู้ประกอบธุรกิจอาจแยกเป็น 3 ระดับความสำคัญ ได้แก่ ความสำคัญสูง ซึ่งเป็นกิจกรรมที่มีประสิทธิภาพและประสิทธิผลสูงในการลดความเสี่ยง หรือเป็นกิจกรรมที่จัดการต่อความเสี่ยงที่มีความสำคัญ ความสำคัญปานกลาง กิจกรรมที่จัดการต่อความเสี่ยงที่สำคัญแต่อาจต้องใช้ทรัพยากรมากหรือดำเนินการได้ยาก หรือเป็นกิจกรรมที่มีประสิทธิภาพและประสิทธิผลที่จัดการกับความเสี่ยงในระดับที่รองลงมา ความสำคัญในระดับนี้จึงควรได้รับการพิจารณาความเหมาะสมจากผู้บริหารอีกครั้ง และ ความสำคัญต่ำ ซึ่งเป็นกิจกรรมที่จัดการต่อความเสี่ยงที่สำคัญน้อย หรือเป็นกิจกรรมที่อาจไม่คุ้มค่าในการดำเนินการ

5) การกำหนดตัวชี้วัดความเสี่ยง (IT Risk Indicator) การติดตาม และรายงานผลการบริหารและจัดการความเสี่ยง (IT Risk Monitoring / Reporting)

ผู้ประกอบธุรกิจควรกำหนดตัวชี้วัดความเสี่ยง (Risk Indicator) เพื่อวัดและติดตามแนวโน้มของความเสี่ยงที่อาจเกิดขึ้น ตัวชี้วัดควรแบ่งเป็นตัวชี้วัดผลการดำเนินงาน (Performance Indicator) สำหรับเหตุการณ์ที่เกิดขึ้นแล้ว และตัวชี้วัดนำ (Lead Indicator) สำหรับการป้องกันเหตุการณ์ความเสี่ยงในอนาคต ตัวชี้วัดที่เลือกควรเชื่อมโยงถึงสาเหตุที่แท้จริงของความเสี่ยง



ภาพที่ 2-6 การกำหนดตัวชี้วัดความเสี่ยง การติดตาม และการรายงานผลการบริหารและจัดการความเสี่ยง
(ที่มา : สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2562)

ผู้ประกอบธุรกิจควรพัฒนาตารางเพื่อเปรียบเทียบตัวชี้วัดความเสี่ยงและจัดทำตัวชี้วัดความเสี่ยงหลัก (Key Risk Indicator) โดยพิจารณาจาก (1) ผลกระทบจากความเสี่ยง (2) ความยากง่ายในการใช้งานตัวชี้วัดความเสี่ยง (3) ความน่าเชื่อถือ (4) การตอบสนองต่อการเปลี่ยนแปลงของความเสี่ยง

2.3 กฎหมายด้านเทคโนโลยีสารสนเทศ

1) พระราชกฤษฎีกา ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 ในเรื่อง พระราชกฤษฎีกามีเรื่องที่เกี่ยวข้อง “หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ.2550” ซึ่งพูดถึงการ ส่งต่อข้อมูลใดๆ ที่เป็นการทำให้ผู้อื่นเสียหาย.... จะมีความผิดทางกฎหมายด้วย

2) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีเนื้อหาที่น่าสนใจในส่วนดังนี้

มาตรา 9 ทำให้เสียหาย ทำลายแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกิน 5 ปีหรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

มาตรา 10 กระทำให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ จนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกิน 5 ปีหรือปรับไม่เกิน 100,000 บาท หรือทั้งจำ

ทั้งปรับ

มาตรา 12 การกระทำความผิดตามมาตรา 9 หรือมาตรา 10

1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

2) กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลหรือระบบคอมพิวเตอร์ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ของสาธารณะ ในทางเศรษฐกิจของประเทศ หรือกระทำต่อข้อมูลหรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

3) การกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

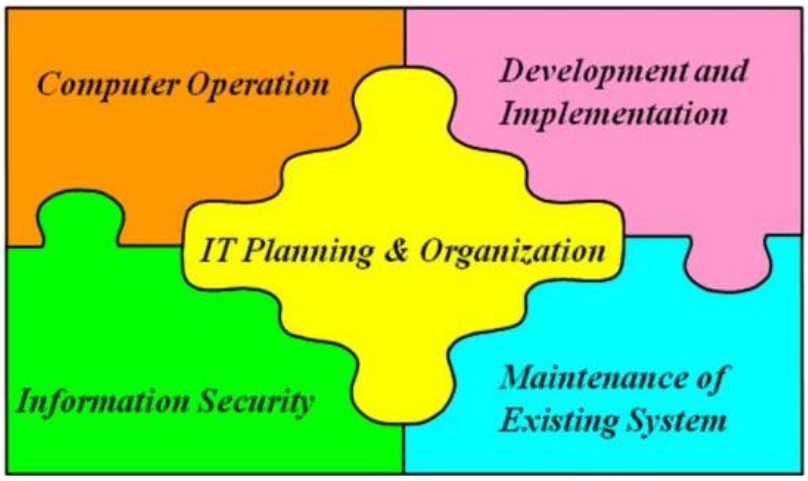
2.4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

การตรวจสอบระบบเทคโนโลยีสารสนเทศเป็นกระบวนการสำคัญในการเก็บรวบรวมและประเมินหลักฐานเพื่อพิจารณาว่าระบบสารสนเทศสามารถบรรลุวัตถุประสงค์หลักได้หรือไม่ ซึ่งวัตถุประสงค์เหล่านี้ได้แก่ การป้องกันสินทรัพย์จากการทุจริตหรือความผิดพลาด การรักษาความถูกต้องของข้อมูล ความมีประสิทธิผลของระบบงาน และความมีประสิทธิภาพในการใช้ทรัพยากร (อภิณห์พร เมธาวัชนานนท์, 2551)

หน่วยงานที่รับผิดชอบการตรวจสอบระบบเทคโนโลยีสารสนเทศควรมีความอิสระจากการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ผู้ตรวจสอบต้องมีความรู้ทางเทคนิคคอมพิวเตอร์อย่างเพียงพอ โดยเฉพาะผู้ที่ทำหน้าที่ตรวจสอบการควบคุมทั่วไปจะต้องมีความรู้เกี่ยวกับการทำงานของระบบจัดการของเครื่องคอมพิวเตอร์ที่ตรวจสอบ ส่วนผู้ตรวจสอบการควบคุมภายในระบบงานต้องมีความรู้พื้นฐานในการออกแบบระบบและการควบคุมภายในของแต่ละระบบงาน (อภิณห์พร เมธาวัชนานนท์, 2551)

การตรวจสอบระบบเทคโนโลยีสารสนเทศ ประกอบด้วย การควบคุมทั่วไป (General Control) และการควบคุมเฉพาะระบบงาน (Application Control)

1) การควบคุมทั่วไป (General Control) หมายถึง การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุม นโยบายและวิธีการในการควบคุมระบบสารสนเทศ (มหาวิทยาลัยราชภัฏรำไพพรรณี, 2564) การควบคุมทั่วไปประกอบด้วย 5 องค์ประกอบ

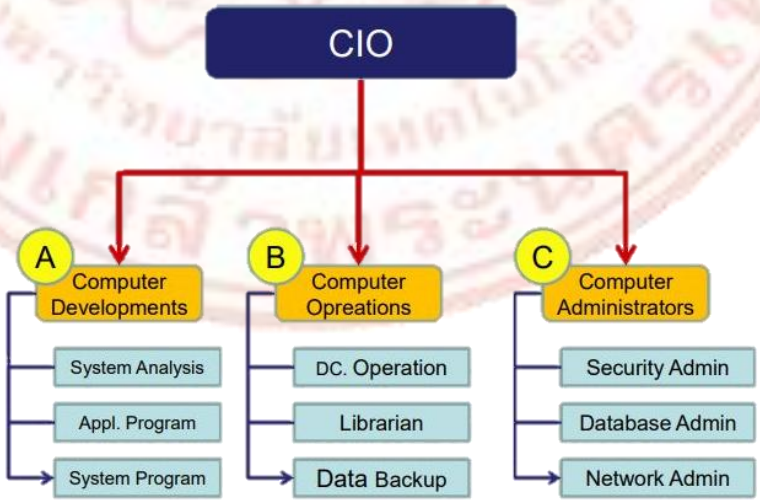


ภาพที่ 2-7 องค์ประกอบของการควบคุมทั่วไป

(ที่มา : สมภพ เตชเสนสกุล)

องค์ประกอบที่ 1 การวางแผนและการควบคุมองค์กรด้านสารสนเทศ (IT Planning and Organization)

การวางแผนด้านสารสนเทศ (IT Planning) มีคณะกรรมการกำกับดูแลด้านสารสนเทศ (IT Steering Committee) ซึ่งมีหน้าที่กลั่นกรองและพัฒนาระบบสารสนเทศให้สามารถสนับสนุนบริษัทได้อย่างเต็มประสิทธิภาพ และวางแผนยุทธศาสตร์ด้านสารสนเทศ (IT Strategic Plan) ซึ่งวางแผนระยะสั้นและระยะยาว พร้อมทั้งมีงบประมาณในการลงทุนด้านสารสนเทศ และการสื่อสารวัตถุประสงค์และติดตามผลอย่างเป็นลายลักษณ์อักษร



ภาพที่ 2-8 การควบคุมองค์กรด้านสารสนเทศ (IT Organization Control)

(ที่มา : สมภพ เตชเสนสกุล)

การควบคุมองค์กรด้านสารสนเทศ (IT Organization Control) คนกลุ่ม A เป็นประเภท Programmer ซึ่งต้องให้ทำงาน Programmer อย่างเดียว ห้ามทำงานที่อื่น โดยเฉพาะงานกลุ่ม B เพราะเป็นงาน Operation โดยตรงของบริษัทต้องแบ่งแยกหน้าที่ระหว่างกลุ่ม A และ B อย่างชัดเจน

องค์ประกอบที่ 2 การควบคุมการพัฒนาและการใช้งาน (Development and Implementation Controls)

ครอบคลุมกระบวนการพัฒนาและปรับใช้ระบบสารสนเทศ รวมถึงการศึกษาความเป็นไปได้ การวิเคราะห์และออกแบบระบบ การสร้างโปรแกรม การทดสอบโปรแกรม การแปลงข้อมูล การติดตั้งระบบ และการตรวจสอบหลังการใช้งาน และตรงตามข้อกำหนดทางธุรกิจ ซึ่งประกอบด้วยขั้นตอนต่อไปนี้

ขั้นตอนที่ 1 การจัดทำข้อกำหนดทางธุรกิจ (Business Requirement) เพื่อรวบรวมและจัดทำเอกสารข้อกำหนดทางธุรกิจที่ชัดเจนและครอบคลุม ซึ่งเกี่ยวข้องกับการทำงานอย่างใกล้ชิดกับผู้มีส่วนได้ส่วนเสียเพื่อทำความเข้าใจความต้องการ วัตถุประสงค์

ขั้นตอนที่ 2 การศึกษาความเป็นไปได้ (Feasibility Study) เพื่อประเมินความเป็นไปได้ทางเทคนิค เศรษฐกิจ การดำเนินงาน และกฎหมาย

ขั้นตอนที่ 3 การวิเคราะห์และออกแบบระบบ (System Analysis and Design) เพื่อกำหนดสถาปัตยกรรมระบบ โครงสร้างข้อมูล เวิร์กโฟลว์ และอินเทอร์เฟซผู้ใช้

ขั้นตอนที่ 4 การสร้างโปรแกรม (Coding Program) ตามข้อกำหนดของระบบ โดยนักพัฒนาต้องแปลการออกแบบเป็นซอฟต์แวร์ปฏิบัติการที่มีมาตรฐานการเขียนโค้ด

ขั้นตอนที่ 5 การทดสอบโปรแกรม (Program Testing) รวมถึงการทดสอบหน่วย (Unit Test) การทดสอบระบบ (System Test) และการทดสอบการยอมรับของผู้ใช้ (User Acceptance Test: UAT) เพื่อยืนยันว่าระบบตรงตามข้อกำหนดของผู้ใช้และสามารถใช้งานได้

ขั้นตอนที่ 6 การแปลงข้อมูล (Data Conversion) หากระบบใหม่เกี่ยวข้องกับการย้ายข้อมูลจากระบบที่มีอยู่ การแปลงข้อมูลถือเป็นสิ่งสำคัญ ขั้นตอนนี้รวมถึงการถ่ายโอน ตรวจสอบ และกระทบยอดข้อมูล (Data Reconciliation) เพื่อความสมบูรณ์ของข้อมูล

ขั้นตอนที่ 7 การติดตั้งระบบ (System Implementation) พร้อมทั้งการจัดทำเอกสารระบบ (System Document) และคู่มือการฝึกอบรม (Training Manual) เพื่อฝึกอบรมผู้ใช้และผู้ดูแลระบบ

ขั้นตอนที่ 8 การตรวจสอบหลังการใช้งาน (Post Implementation Review) เพื่อตรวจสอบประสิทธิภาพของระบบและแก้ไขปัญหาที่เกิดขึ้น

องค์ประกอบที่ 3 การบำรุงรักษาระบบควบคุมที่มีอยู่ (Maintenance of Existing System Control)

องค์ประกอบนี้กล่าวถึงการจัดการการอัปเดตซอฟต์แวร์ แพตช์ และการปรับปรุงระบบอย่างมีประสิทธิภาพ เพื่อให้ระบบที่มีอยู่ยังคงปลอดภัย มีประสิทธิภาพ และสอดคล้องกับข้อกำหนดที่เปลี่ยนแปลงไป

องค์ประกอบที่ 4 การควบคุมความปลอดภัยของข้อมูล (Information Security Control)

การควบคุมความปลอดภัยของข้อมูลเป็นส่วนสำคัญของการควบคุมทั่วไป โดยเกี่ยวข้องกับการประเมินมาตรการขององค์กรเพื่อปกป้องข้อมูลที่ละเอียดอ่อนและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยมีองค์ประกอบย่อยสำคัญดังนี้

องค์ประกอบย่อยที่ 1 นโยบายและขั้นตอนการรักษาความปลอดภัยของสารสนเทศ (IT Security Policy and Procedure) เป็นเอกสารพื้นฐานที่ให้แนวทาง มาตรฐาน และกฎเกณฑ์ในการปกป้องทรัพย์สินด้านสารสนเทศ

องค์ประกอบย่อยที่ 2 การควบคุมการเข้าถึง (User Access Control Feature) ที่ควบคุมการเข้าถึงทรัพยากรสารสนเทศ ระบบ และข้อมูล

องค์ประกอบย่อยที่ 3 แบบฟอร์มและขั้นตอนคำขอของผู้ใช้ (User Request Form and Procedure) แบบฟอร์มและขั้นตอนคำขอของผู้ใช้ใช้เพื่อจัดการคำขอเข้าถึงของผู้ใช้

องค์ประกอบย่อยที่ 4 การบันทึกและการตรวจสอบ (Logging and Monitoring) การบันทึกและการตรวจสอบเกี่ยวข้องกับการรวบรวมและการวิเคราะห์บันทึกข้อมูลของระบบเพื่อตรวจจับและตอบสนองต่อเหตุการณ์ด้านความปลอดภัย

องค์ประกอบย่อยที่ 5 ความปลอดภัยทางด้านกายภาพ (Physical Security) มาตรการรักษาความปลอดภัยทางกายภาพช่วยปกป้องโครงสร้างพื้นฐานทางกายภาพและฮาร์ดแวร์ที่รองรับระบบสารสนเทศ ซึ่งรวมถึงการรักษาความปลอดภัยศูนย์ข้อมูล ห้องเซิร์ฟเวอร์ อุปกรณ์เครือข่าย และส่วนประกอบที่สำคัญอื่นๆ

องค์ประกอบที่ 5 การควบคุมการทำงานของคอมพิวเตอร์ (Computer Operation Control)

การควบคุมการทำงานของคอมพิวเตอร์มุ่งเน้นไปที่การจัดการในแต่ละวันและการตรวจสอบโครงสร้างพื้นฐานด้านสารสนเทศ การควบคุมการทำงานของคอมพิวเตอร์ประกอบด้วย (1) การกำหนดตารางการดำเนินงาน (Operation Schedule) ตารางเวลา และขั้นตอนการควบคุม (Control Procedure) (2) การกำหนดข้อตกลงระดับการให้บริการ (Define Service Level Agreement: SLA) (3)การสำรองข้อมูล (Data Back-up Procedure) และ (4) การกู้คืนจากความล้มเหลวในการดำเนินงาน และการกำหนดแผนการกู้คืนระบบสารสนเทศ (Disaster and Recovery Plan: DRP)

การควบคุมเฉพาะระบบงาน (Application Control) คือ การควบคุมเฉพาะระบบงานเป็นการควบคุมรายงานข้อมูลในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของข้อมูลเป็นแนวทางในการกำหนดขอบเขตการควบคุม (มหาวิทยาลัยราชภัฏรำไพพรรณี, 2564) โดย

วัตถุประสงค์มี 4 ประการ (CAVR) คือ (1) ให้ความมั่นใจในความสมบูรณ์ของข้อมูล (Completeness) (2) ความถูกต้องตรงกันทุกประการของข้อมูล (Accuracy) (3) ความสมเหตุสมผลของข้อมูล (Validity) และ (4) การจำกัดการเข้าถึงข้อมูลและสินทรัพย์ (Restricted Access to Date and Physical Assets)

CAVR ทำได้โดยการควบคุมสิ่งต่างๆ ดังนี้ (1) ข้อมูลนำเข้า (Input Control) ควบคุมวิธีการนำเข้าข้อมูล แหล่งที่มาของข้อมูล และความถูกต้องของข้อมูล (2) การประมวลผล (Processing Control) ควบคุมการประมวลผลให้มีความแม่นยำถูกต้องและครบถ้วนเป็นไปตามหลักเกณฑ์การใช้แฟ้มข้อมูล และ (3) ข้อมูลผลลัพธ์ (Output Control) การกระทบยอดข้อมูลนำเข้าและผลลัพธ์ เพื่อพิสูจน์ความถูกต้องด้วยระบบ Manual ซึ่งเป็นหน้าที่โดยตรงของหน่วยงานควบคุมคุณภาพข้อมูล

2.5 ปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

จากการศึกษาของผู้วิจัยในหัวข้อ ปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ผู้วิจัยศึกษางานวิจัยที่เกี่ยวข้องกับการตรวจสอบภายในและการตรวจสอบบัญชีเพิ่มเติม เนื่องจากผู้วิจัยเล็งเห็นว่า ลักษณะงานในการตรวจสอบด้านเทคโนโลยีสารสนเทศ การตรวจสอบภายใน และการตรวจสอบบัญชี มีความคล้ายคลึงกัน จึงได้นำปัจจัยที่ส่งผลต่อการตรวจสอบภายในและการตรวจสอบบัญชีมานำเสนอร่วมกับปัจจัยที่ส่งผลต่อการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยปัจจัยที่นำเสนอ มีดังนี้

1) ความเป็นอิสระของผู้ตรวจสอบ

ความเป็นอิสระของผู้ตรวจสอบ หมายถึง สภาวะที่ผู้ตรวจสอบสามารถดำเนินกิจกรรมเพื่อทำให้การตรวจสอบเทคโนโลยีสารสนเทศ บรรลุผลโดยปราศจากอคติและปราศจากความเอนเอียง อันเป็นการเอื้อให้ผู้ตรวจสอบ สามารถปฏิบัติงานตามภารกิจด้วยความเชื่อมั่นในงานและไม่มีการลดหย่อนในคุณภาพของงาน ทั้งนี้ ดุลยพินิจของผู้ตรวจสอบในเรื่องที่เกี่ยวข้องกับการตรวจสอบจะต้องไม่อยู่ภายใต้การชักจูง หรือชักนำจากผู้อื่น หรือไม่ถูกแทรกแซงจากปัจจัยภายในหรือภายนอก (สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย, 2554; ISACA, 2014; Havelka & Merhout, 2013; Vaicekauskas & Mackevičius, 2014; ชัชพงศ์ อธิปัญญาวงศ์, 2559) สอดคล้องกับที่ Azhar (2013) และ Abdulahi (2016) กล่าวว่า ความเป็นอิสระนั้นทำให้ผู้สอบทานสามารถสอบทานขั้นตอนการดำเนินงานต่าง ๆ ที่เพื่อแสดงข้อมูลที่แท้จริง และผู้ตรวจสอบภายในควรมีความเป็นอิสระจากเงื่อนไขหรือข้อจำกัดที่คุกคามความเป็นกลาง

จากการศึกษาของ ณภัทร จิตต์เสรี พบว่าความเป็นอิสระของผู้ตรวจสอบภายในส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบ แต่การศึกษาของ ชัชพงศ์ อธิปัญญาวงศ์ (2559) พบว่าความเป็นอิสระของผู้ตรวจสอบภายในไม่ส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบ โดยอาจมีสาเหตุจากความเป็นอิสระของผู้ตรวจสอบ นอกจากจะขึ้นอยู่กับผู้ตรวจสอบแล้วอาจปรับเปลี่ยนไปตามจำนวนบุคลากรหรือขนาดขององค์กร ซึ่งสอดคล้องกับการศึกษาของ อรพรรณ แสงศิวะเวทย์ (2016) ที่ทำให้ทราบเพิ่มเติมว่าความเป็นอิสระของผู้ตรวจสอบภายในจะส่งผลหรือไม่ส่งผลนั้นอาจปรับเปลี่ยนไปตามจำนวนบุคลากรหรือขนาดขององค์กร

2) ความรู้ความสามารถของผู้ตรวจสอบ

ความรู้ด้านเทคโนโลยีสารสนเทศของผู้ตรวจสอบ หมายถึง ความเข้าใจหรือสิ่งที่สั่งสมทางสติปัญญาเฉพาะบุคคลที่ได้มาจากการศึกษา หรือ มาจากประสบการณ์ที่เกี่ยวข้องในด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถเข้าใจและนำมาประยุกต์ใช้ให้เข้ากับลักษณะเฉพาะขององค์กร ตามประเภทและลักษณะของธุรกิจ รวมทั้งวัตถุประสงค์ขององค์กร โดยที่ผู้ตรวจสอบเทคโนโลยีสารสนเทศ ต้องสามารถประเมินกระบวนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับกระบวนการทางธุรกิจ เพื่อนำมาประยุกต์ใช้ให้เข้ากับลักษณะเฉพาะขององค์กร ตามประเภทลักษณะของธุรกิจ และวัตถุประสงค์ขององค์กร (ชัชพงศ์ อธิปัญญาวงศ์, 2559) ตามที่ Havelka and Merhout (2013) กล่าวว่า ระดับความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบ เช่น ระดับความชำนาญด้านเทคโนโลยีสารสนเทศโดยทั่วไป ความเข้าใจในโปรแกรมประยุกต์สำหรับกระบวนการและการปฏิบัติงาน ความเข้าใจในภาษาคอมพิวเตอร์ และความเข้าใจในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการปฏิบัติงาน ส่งผลต่อคุณภาพของกระบวนการตรวจสอบเทคโนโลยีสารสนเทศ เป็นต้น

จากการศึกษาของ สุวรรณี รุ่งจตุรงค์ (2561) พบว่าปัจจัยด้านความรู้ความสามารถของผู้สอบบัญชีมีผลต่อประสิทธิภาพการสอบบัญชี แต่การศึกษาของ ชัชพงศ์ อธิปัญญาวงศ์ (2559) พบว่าความรู้ด้านเทคโนโลยีสารสนเทศของผู้ตรวจสอบ ไม่ส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบ เพราะถึงแม้ว่าผู้ตรวจสอบจะมีความรู้เฉพาะทางซึ่งเกี่ยวข้องกับธุรกิจขององค์กร แต่ความรู้เฉพาะทางที่ผู้ตรวจสอบมีอยู่ก็ไม่อาจทำให้เกิดคุณภาพของการตรวจสอบได้เสมอไป ผู้ตรวจสอบอาจจำเป็นต้องใช้ความรู้เฉพาะทางที่มีร่วมกับการสั่งสมประสบการณ์(Audit Time) และวิจารณญาณในการสังเกตและสงสัยเยี่ยงผู้ประกอบวิชาชีพของผู้ตรวจสอบ (Professional Skepticism) อีกด้วย (Hu, 2015)

3) วุฒิภาวะ ทักษะ และประสบการณ์ของผู้ตรวจสอบ

วุฒิภาวะ ทักษะ และประสบการณ์ของผู้ตรวจสอบ กล่าวได้ว่า หมายถึง ความรู้และความสามารถในการตรวจสอบข้อมูลหลักฐานทางการบัญชีและข้อมูลอื่น ๆ ตามมาตรฐานที่ได้รับการยอมรับโดยทั่วไปในการปฏิบัติงานภาคสนาม (Usman, 2016)

ตลาดหลักทรัพย์แห่งประเทศไทย และสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (2548) กล่าวว่า งานตรวจสอบภายในเป็นวิชาชีพอย่างหนึ่ง ดังนั้น ผู้ตรวจสอบภายในควรมีคุณสมบัติ ที่เหมาะสมและสามารถสนับสนุนให้ปฏิบัติงานเยี่ยงผู้ประกอบวิชาชีพได้ นอกจากคุณสมบัติที่กล่าวไว้ในหัวข้อ “คุณสมบัติตามมาตรฐานการตรวจสอบภายใน” ผู้ตรวจสอบภายในควรต้องมีคุณสมบัติ อื่น ๆ ที่จำเป็น โดยมีรายละเอียดดังนี้

(1) ความสามารถในการนำมาตรฐานการตรวจสอบภายใน กระบวนการ และเทคนิค ต่าง ๆ ที่เกี่ยวข้องกับงานตรวจสอบภายในไปประยุกต์ใช้ในทางปฏิบัติ

(2) ผู้ตรวจสอบภายในที่ปฏิบัติงานตรวจสอบรายงานทางการเงินควรมีความรู้ด้านการ บัญชีเป็นอย่างดี รวมถึงความเข้าใจต่อมาตรฐานการบัญชีและมาตรฐานอื่น ๆ ที่เกี่ยวข้อง

(3) ควรมีความเข้าใจเกี่ยวกับหลักการบริหารจัดการซึ่งจะเป็นประโยชน์อย่างมากต่อผู้ตรวจสอบในการประเมินสาระสำคัญของความแตกต่างระหว่างแนวปฏิบัติที่ดีและแนวปฏิบัติที่ใช้อยู่ในบริษัท เนื่องจากแนวปฏิบัติที่ดีนั้นควรประยุกต์ใช้ให้เหมาะสมกับองค์กรแต่ละแห่ง การเข้าใจหลักการบริหารจะทำให้ผู้ตรวจสอบภายในสามารถให้คำแนะนำที่เป็นประโยชน์ในทางปฏิบัติแก่ผู้บริหารมากยิ่งขึ้น

(4) ควรมีความรู้ทั่วไปในด้านต่าง ๆ ประกอบด้วย การบัญชี เศรษฐศาสตร์ กฎหมาย ธุรกิจกฎหมายภาษีอากร การเงิน และเครื่องมือการบริหาร อย่างไรก็ตาม ผู้ตรวจสอบภายในไม่จำเป็นต้องมีความรู้ในเรื่องเหล่านี้อย่างละเอียด เนื่องจากหากจำเป็นต้องใช้ความรู้ทางด้านนี้ ผู้ตรวจสอบภายในสามารถขอคำแนะนๆหรือบริการจากผู้เชี่ยวชาญเรื่องนี้โดยตรง ดังนั้น ความรู้ที่ผู้ตรวจสอบภายในควรมีอย่างน้อยต้องช่วยให้ผู้ตรวจสอบภายในสามารถระบุปัญหาที่เกิดขึ้นหรือที่อาจจะเกิดขึ้น ซึ่งนำไปสู่การตัดสินใจหาข้อมูลเพิ่มเติม หรือบ่งชี้ความช่วยเหลือที่ต้องการจากผู้เชี่ยวชาญในเรื่องนั้น ๆ

(5) ควรมีความรู้เกี่ยวกับระบบคอมพิวเตอร์ และเทคโนโลยีอย่างเพียงพอ เพื่อบ่งชี้เรื่องที่ควรได้รับการตรวจสอบและกำหนดเรื่องที่ควรขอความช่วยเหลือจากผู้เชี่ยวชาญด้านคอมพิวเตอร์

(6) ควรสามารถพิจารณาใช้เทคโนโลยีในการเพิ่มประสิทธิภาพงานตรวจสอบภายใน เช่น การใช้โปรแกรมการวิเคราะห์ข้อมูล การใช้โปรแกรมประเมินความเสี่ยงโปรแกรม เพื่อปฏิบัติงานตรวจสอบภายใน โปรแกรมเพื่อการบริหารงานตรวจสอบภายใน เป็นต้น

จากการศึกษาของ ชัชพงศ์ อธิปัญญาวงศ์ (2559) พบว่าวุฒิภาวะของผู้ตรวจสอบส่งผลทางบวกต่อ คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ สอดคล้องกับการศึกษาของ สุวรรณี รุ่ง

จตุรงค์ (2561) ซึ่งพบว่าประสบการณ์มีผลต่อประสิทธิภาพการสอบบัญชี ด้านการเรียนรู้ ด้านเทคนิคการปฏิบัติหน้าที่ และด้านทักษะการจัดองค์กรอย่างมีนัยสำคัญ และจากการศึกษาของ ณภัทร จิตต์เสรี (2565) และ อรพรรณ แสงศิวะเวทย์ (2559) พบว่าทักษะของผู้ตรวจสอบภายในส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบภายใน แต่จากการศึกษาของ อรพรรณ แสงศิวะเวทย์ (2559) ทักษะของผู้ตรวจสอบภายในไม่ส่งผลต่อประสิทธิภาพของงานตรวจสอบภายใน และ อัมรา เพียรบูชา พบว่าประสบการณ์ในการทำงานด้านสอบบัญชีแตกต่างกันไม่มีความสัมพันธ์กับการปฏิบัติงานตรวจสอบบัญชีแตกต่างกัน ซึ่งอาจเกิดขึ้นได้จากลักษณะการให้ระดับคะแนนในปัจจัยนี้มีความแตกต่างกันไปตามลักษณะงานตรวจสอบภายในของแต่ละองค์กร

4) จรรยาบรรณและจริยธรรมของผู้ตรวจสอบ

จรรยาบรรณและจริยธรรมของผู้ตรวจสอบเป็นกฎและกฎหมายที่เกี่ยวข้องกับการปฏิบัติงานของผู้ตรวจสอบ เพื่อให้การตรวจสอบเป็นไปตามหลักธรรมาภิบาลและมีความเป็นธรรม ตรงตามรากฐานของอาชีพและกฎหมาย

จากการศึกษาของ ศรุดา โพธิ์พันธุ์ (2561) พบว่าจริยธรรมของผู้ตรวจสอบภายในส่งผลต่อประสิทธิผลของการตรวจสอบภายในซึ่งสอดคลองกับกรมบัญชีกลางที่กล่าวไว้ว่า จริยธรรมของผู้ตรวจสอบภายในเป็นปัจจัยที่ทำให้งานตรวจสอบภายในบรรลุเป้าหมาย แต่จากการศึกษาของ สุวรรณี รุ่งจตุรงค์ (2561) ปัจจัยด้านจรรยาบรรณของผู้สอบบัญชีไม่มีผลต่อประสิทธิภาพการสอบบัญชี

5) มาตรฐานการตรวจสอบ

กรมบัญชีกลาง ได้กล่าวว่า มาตรฐานการตรวจสอบภายใน ประกอบด้วยส่วนสำคัญ 2 ส่วน ดังนี้

ส่วนที่ 1 มาตรฐานด้านคุณสมบัติ เป็นมาตรฐานที่กล่าวถึงลักษณะของหน่วยงานและบุคลากรที่ทำหน้าที่ตรวจสอบภายใน ประกอบด้วย (ศรุดา โพธิ์พันธุ์, 2561)

(1) หน่วยตรวจสอบภายในคนมีการกำหนดวัตถุประสงค์ อำนาจหน้าที่ความรับผิดชอบของงานตรวจสอบภายในอย่างเป็นทางการไว้ในกฎบัตรการตรวจสอบภายใน เพื่อเป็นกรอบอ้างอิงและเป็นแนวทางในการปฏิบัติงานที่สำคัญของหน่วยตรวจสอบภายใน

(2) การกำหนดถึงความเป็นอิสระและความเที่ยงธรรม การปฏิบัติงานตรวจสอบภายในควรมีความเป็นอิสระและผู้ตรวจสอบภายในคนปฏิบัติหน้าที่ด้วยความเที่ยงธรรม ซื่อสัตย์ สุจริตและมีจริยธรรม

(3) การปฏิบัติงานตรวจสอบด้วยความเชี่ยวชาญและความระมัดระวังรอบคอบ ผู้ตรวจสอบภายในควรปฏิบัติหน้าที่ด้วยความเชี่ยวชาญและระมัดระวังรอบคอบเยี่ยงผู้ประกอบวิชาชีพ

(4) การสร้างหลักประกันคุณภาพและการปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง หัวหน้าหน่วยตรวจสอบภายในคนปรับปรุงและรักษาระดับคุณภาพของงานตรวจสอบภายใน โดยมีการปรับปรุงงานตรวจสอบภายในให้ครอบคลุมทุก ๆ ด้านและติดตามดูแลประสิทธิภาพของงานอย่างต่อเนื่อง

ส่วนที่ 2 มาตรฐานด้านการปฏิบัติงาน เป็นมาตรฐานที่กล่าวถึงลักษณะของงานตรวจสอบภายในและบรรทัดฐานที่สามารถใช้ประเมินผลการปฏิบัติงานตรวจสอบภายใน ประกอบด้วย (ศรุดา โพธิ์พันธุ์, 2561)

(1) การบริหารงานตรวจสอบภายใน หัวหน้างานตรวจสอบภายในควรมีการบริหารงานตรวจสอบภายในให้เกิดผลสัมฤทธิอย่างมีประสิทธิภาพ เพื่อให้งานตรวจสอบภายในสามารถสร้างคุณค่าเพิ่มให้กับองค์กร

(2) ลักษณะงานตรวจสอบภายใน งานตรวจสอบภายใน คือ การประเมินเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานขององค์กรให้ถึงเป้าหมายที่วางไว้ และปรับปรุงประสิทธิภาพของการบริหารความเสี่ยงโดยการควบคุมและกำกับดูแล

(3) การวางแผนการปฏิบัติงานตรวจสอบภายใน ผู้ตรวจสอบภายในคนจัดทำแผนการปฏิบัติงานตามภารกิจที่ได้รับมอบหมายทั้งในด้านการให้หลักประกันและการให้คำปรึกษา โดยคนคำนึงถึง วัตถุประสงค์ของงานและวิธีการดำเนินงานตรวจสอบภายใน ความเสี่ยงที่สำคัญที่มีผลกระทบต่อความสำเร็จ ความเพียงพอและความมีประสิทธิภาพของกิจการบริหารความเสี่ยง และระบบการควบคุม และโอกาสในการปรับปรุงกิจกรรมการบริหารความเสี่ยงและระบบการควบคุมภายในให้ดีขึ้น

(4) การปฏิบัติงานตรวจสอบ การสอบภายในควรรวบรวม วิเคราะห์ ประเมิน และบันทึกข้อมูลให้เพียงพอต่อการปฏิบัติงานที่ได้รับมอบหมายให้บรรลุตามวัตถุประสงค์ และหัวหน้าหน่วยงานตรวจสอบภายในควรควบคุมการปฏิบัติงานที่ได้มอบหมายอย่างใกล้ชิด เพื่อให้เกิดความมั่นใจว่าการปฏิบัติงานจะสามารถบรรลุตามวัตถุประสงค์ที่กำหนดไว้อย่างมีคุณภาพ

(5) การรายงานผลการปฏิบัติงาน ผู้ตรวจสอบภายในควรรายงานผลการปฏิบัติงานอย่างทันกาล โดรายงานดังกล่าวประกอบด้วย วัตถุประสงค์ ขอบเขต การสรุปผลการตรวจสอบ ความคิดเห็น ข้อเสนอแนะและแนวทางในการปรับปรุงแก้ไขที่สามารถนำไปปฏิบัติได้ด้วยความถูกต้อง ครบถ้วน ชัดเจน เที่ยงธรรม รัดกุม สร้างสรรค์ และรวดเร็ว รวมทั้งควรเผยแพร่ผลการปฏิบัติงานให้บุคคลที่เกี่ยวข้องและเหมาะสมได้รับทราบ

(6) การติดตามผล หัวหน้าหน่วยงานตรวจสอบภายในควรกำหนดระบบการติดตามผลว่าได้มีการนำข้อเสนอแนะในรายงานผลการปฏิบัติงานไปสู่การปฏิบัติ

(7) การยอมรับสภาพความเสี่ยง หัวหน้าหน่วยงานตรวจสอบภายในควรรายงานเรื่องความเสี่ยงที่อาจก่อให้เกิดความเสียหายแก่องค์กรซึ่งยังไม่ได้รับการแก้ไขหารือให้กับผู้บริหาร

จากการศึกษาของ ศรุดา โพธิ์พันธุ์ (2561) พบว่ามาตรฐานการตรวจสอบส่งส่งผลต่อประสิทธิผลของการตรวจสอบภายใน เนื่องจากผู้ตรวจสอบภายในเป็นส่วนหนึ่งของการตรวจสอบภายใน ดังนั้นจึงต้องมีการกำหนดวัตถุประสงค์ อำนาจหน้าที่ ความรับผิดชอบของงานตรวจสอบภายในอย่างเป็นทางการ เพื่อใช้เป็นกรอบอ้างอิงและเป็นแนวทางปฏิบัติงานที่สำคัญของหน่วยตรวจสอบภายใน

6) การฝึกอบรมและการพัฒนา

การฝึกอบรมและการพัฒนา หมายถึง กระบวนการเรียนรู้ที่เกี่ยวข้องกับการได้มาซึ่ง ความรู้ ทักษะ แนวคิด หลักเกณฑ์ หรือการเปลี่ยนทัศนคติและพฤติกรรม เพื่อเพิ่มประสิทธิภาพการทำงานให้กับบุคลากร ซึ่งเป็นกระบวนการที่ต้องปฏิบัติอย่างต่อเนื่อง โดยบุคลากรจะได้รับความรู้อย่างแท้จริงและทราบถึงแนวทางในการปฏิบัติงานในองค์กรได้ดีขึ้น อีกทั้งในปัจจุบันการฝึกอบรมเป็นสิ่งสำคัญมากในการที่จะเป็นส่วนหนึ่งในการสร้างกำไรให้กับองค์กร ส่วนมากกำหนดให้มีการฝึกอบรมที่เหมาะสมอย่างสม่ำเสมอ ซึ่งวัตถุประสงค์หลักของการฝึกอบรมนั้นเพื่อต้องการพัฒนาทักษะของบุคลากรซึ่งจะส่งผลให้องค์กรมีความสามารถในการทำกำไรได้มากขึ้น (Ameeq, 2013; ณภัทร จิตต์เสรี: อรพรรณ แสงศิวะเวทย์, 2559)

จากการศึกษาของ ณภัทร จิตต์เสรี พบว่าการฝึกอบรมและการพัฒนาส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบภายใน ซึ่งสอดคล้องกับการศึกษาของ อรพรรณ แสงศิวะเวทย์ (2559) พบว่าการฝึกอบรมและพัฒนาส่งผลต่อทักษะของผู้ตรวจสอบภายใน ซึ่งทักษะของผู้ตรวจสอบภายในเป็นปัจจัยหนึ่งที่ส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบภายใน จึงกล่าวได้ว่าการฝึกอบรมและพัฒนาส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบภายใน

7) การสนับสนุนจากผู้บริหาร

การสนับสนุนจากผู้บริหาร หมายถึง ปัจจัยสำคัญที่จำเป็นต่อการช่วยสนับสนุนการพัฒนาความรู้ของบุคลากรในองค์กร การสนับสนุนทางด้านการเงินสำหรับโครงสร้างในด้านความรู้และขอบเขตข่ายทักษะของพนักงานในการนำมาประยุกต์ใช้ แชร์ปรสบการณ์ และรวบรวม (Abdul & Shamyla, 2012) สอดคล้องกับ Dessalegn และ Aderajew (2007) เล็งเห็นว่าปัจจัยนี้ถือเป็นปัจจัยหนึ่งที่ส่งผลต่อกระบวนการปฏิบัติหน้าที่ของที่ปรึกษากระบวนการดำเนินการอย่างชัดเจน ฝ่ายการจัดการได้ทำการติดตามผลการตรวจสอบและข้อเสนอแนะนำที่ถูกเสนอจากการลงพื้นที่ตรวจสอบของผู้สอบทานจะทำให้สามารถระบุประสิทธิผลของการดำเนินงานได้ (ณภัทร จิตต์เสรี)

จากการศึกษาของ Zulktifli, Alagan และ Mohd (2014) พบว่า การสนับสนุนและให้ความเชื่อมั่นในคุณค่าของฝ่ายบริหารส่งผลกระทบให้เกิดความมั่นใจได้ว่างานตรวจสอบภายในจะสามารถดำเนินการได้อย่างมีประสิทธิภาพ จากการศึกษาของ Havelka และ Merhout (2008) พบว่าการสนับสนุน การร่วมมือ และการเข้าใจจากลูกค้า ผู้ถูกตรวจสอบ และผู้บริหารระดับสูง รวมถึงการได้รับการสนับสนุนเพียงพอจากผู้เกี่ยวข้องมีผลต่องานตรวจสอบในหลายด้าน จากการศึกษาของ อรพรรณ แสงศิวะเวทย์ (2559) พบว่าการสนับสนุนจาก ผู้บริหารส่งผลต่อประสิทธิภาพของงานตรวจสอบภายใน และจากการศึกษาของ ณภัทร จิตต์เสรี พบว่าการสนับสนุนจากผู้บริหารส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบภายใน

8) การวางแผนการตรวจสอบ

การวางแผนการตรวจสอบ (บุญศรี กุศเลิศจริยา, 2541) เป็นสิ่งจำเป็นต่อการปฏิบัติงานตรวจสอบที่มีประสิทธิผล เนื่องจากเป็นการกำหนดว่ากิจกรรมใดที่ควรจะตรวจสอบ ควรจะตรวจสอบเมื่อไร ระยะเวลาที่จะตรวจสอบ งบประมาณ ตลอดจนจำนวนผู้ตรวจสอบ เป็นต้น เนื้อหาในการตรวจสอบของแต่ละองค์กรจะแตกต่างกันตามลักษณะการประกอบการ วัตถุประสงค์ และเป้าหมายของแต่ละองค์กร ซึ่งในการวางแผนการตรวจสอบมี 2 ลักษณะ คือ แผนการตรวจสอบระยะยาว (Long-Rang Plan) เป็นแผนที่มีระยะเวลาตั้งแต่ 1 ปีขึ้นไป และ แผนการตรวจสอบระยะสั้นหรือแผนการตรวจสอบประจำปี (Short-Rang Plan) เป็นแผนที่มีระยะเวลา 1 ปีหรือไม่เกิน 1 ปี

จากการศึกษาของ อัมรา เพียรบูชา พบว่าการวางแผนการตรวจสอบบัญชีมีความสัมพันธ์กับการปฏิบัติงานตรวจสอบบัญชีอย่างมีนัยสำคัญ ซึ่งสอดคล้องกับการศึกษาของ บุญศรี กุศเลิศจริยา (2541) พบว่า การวางแผนการตรวจสอบส่งผลต่อความสำเร็จของการตรวจสอบภายใน

9) การวิเคราะห์ความเสี่ยง

การวิเคราะห์ความเสี่ยง หมายถึง การพิจารณาผลกระทบของความไม่แน่นอนของ เหตุการณ์หรือปัจจัยที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศในองค์กรโดยรวม เช่น ความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่าที่อาจเกิดขึ้นโดยเกี่ยวข้องกับระบบสารสนเทศและเทคโนโลยี ต่อวัตถุประสงค์ขององค์กรธุรกิจ ซึ่งแต่เดิมมุมมองการตรวจสอบเป็นเพียงกิจกรรมที่ระบุและประเมินความผลกระทบ ตามแนวทางแบบการตรวจหาข้อผิดพลาดทั่วไป (Cangemi, 2014; Rosário et al, 2012; ชัชพงศ์ อธิปัญญาวงศ์, 2559)

จากการศึกษาของ ชัชพงศ์ อธิปัญญาวงศ์ (2559) การวิเคราะห์ความเสี่ยง ส่งผลต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ ซึ่งสอดคล้องกับ Vaicekauskas และ Mackevičius (2014) และ El-Masry และ Hansen (2007) ได้ระบุว่า การพิจารณาประเมินระดับความเสี่ยงส่งผลต่อการ

วางแผนการตรวจสอบตามแนวความเสี่ยงในการดำเนินงานของผู้รับการตรวจ และยังส่งผลต่อความมีประสิทธิผลของรายงานประเด็นที่พบจากการตรวจสอบ อันเป็นคุณลักษณะหนึ่งของคุณภาพการตรวจสอบ

10) หลักฐานการตรวจสอบ

หลักฐานการตรวจสอบ คือ ข้อมูลที่ผู้ตรวจสอบเก็บรวบรวมเพื่อให้ข้อมูลหรือข้อเท็จจริงเกี่ยวกับกระบวนการทางธุรกิจและการปฏิบัติขององค์กร หลักฐานนี้ใช้ในการประเมินความเสี่ยงและประสิทธิผลของระบบควบคุมและการดำเนินงานขององค์กร การเก็บรวบรวมและการใช้หลักฐานเป็นส่วนสำคัญของกระบวนการตรวจสอบ จากการศึกษาของ อัมรา เพียรบูชา พบว่าหลักฐานการสอบบัญชีที่มีความสัมพันธ์กับการปฏิบัติงานตรวจสอบบัญชีอย่างมีนัยสำคัญ

ตารางที่ 2-1 ตารางสรุปงานวิจัยที่เกี่ยวข้องกับแต่ละปัจจัย

No	งานวิจัยที่เกี่ยวข้อง	ความเป็นอิสระของผู้ตรวจสอบ	ความรู้ความสามารถของผู้ตรวจสอบ	ความเที่ยงธรรม และประสบการณ์ของผู้ตรวจสอบ	จรรยาบรรณและจริยธรรมของผู้ตรวจสอบ	มาตรฐานการตรวจสอบ	การฝึกอบรมและการพัฒนา	การยินยอมจากผู้บริหาร	การวางแผนการตรวจสอบ	การวิเคราะห์ความเสี่ยง	หลักฐานการตรวจสอบ
1	Abdul & Shamyla (2012)	X						X			
2	Abdulahi (2016)	X									
3	Ameeq (2013)						X				
4	Azhar Susanto (2013)	X									
5	Cangemi (2014)									X	
6	Dessalegn & Aderajew (2007)							X			
7	El-Masry & Hansen (2007)									X	
8	Havelka & Merhout (2008)	X	X							X	
9	Havelka & Merhout (2013)	X	X					X			
10	HELIYON (2023)	X						X			
11	Hu (2015)		X								
12	Rosário, Pereira, Silva (2012)									X	
13	Usman (2016)			X							
14	Vaicekauskas & Mackevičius (2014)	X								X	
15	Zulktifli, Alagan, Mohd (2014)							X			
16	แคทรียา เรืองเจริญ (2564)	X	X								
17	ชัชพงศ์ อธิปัญญาวงศ์ (2559)			X						X	
18	ณภัทร จิตต์เสรี	X		X			X	X			
19	บุญศรี กุศเลิศจริยา (2541)								X		
20	ศรุดา โพธิ์พันธุ์ (2561)				X	X					
21	สุวรรณี รุ่งจตุรงค์ (2561)		X	X							
22	อรพรรณ แสงศิวะเวทย์ (2559)	X		X			X	X			
23	อัมรา เพียรบูชา (2557)								X		X

2.6 แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีaaสารสนเทศ

กรมบัญชีกลาง กล่าวไว้ว่า กระบวนการปฏิบัติงานตรวจสอบภายในจำเป็นต้องดำเนินการอย่างเป็นขั้นตอน เพื่อให้ผู้ตรวจสอบภายในสามารถปฏิบัติงานตรวจสอบได้อย่างมั่นใจและได้ผลงานที่มีคุณภาพ โดยขั้นตอนของการปฏิบัติงานตรวจสอบที่สำคัญ ประกอบด้วย 3 ขั้นตอน ดังนี้

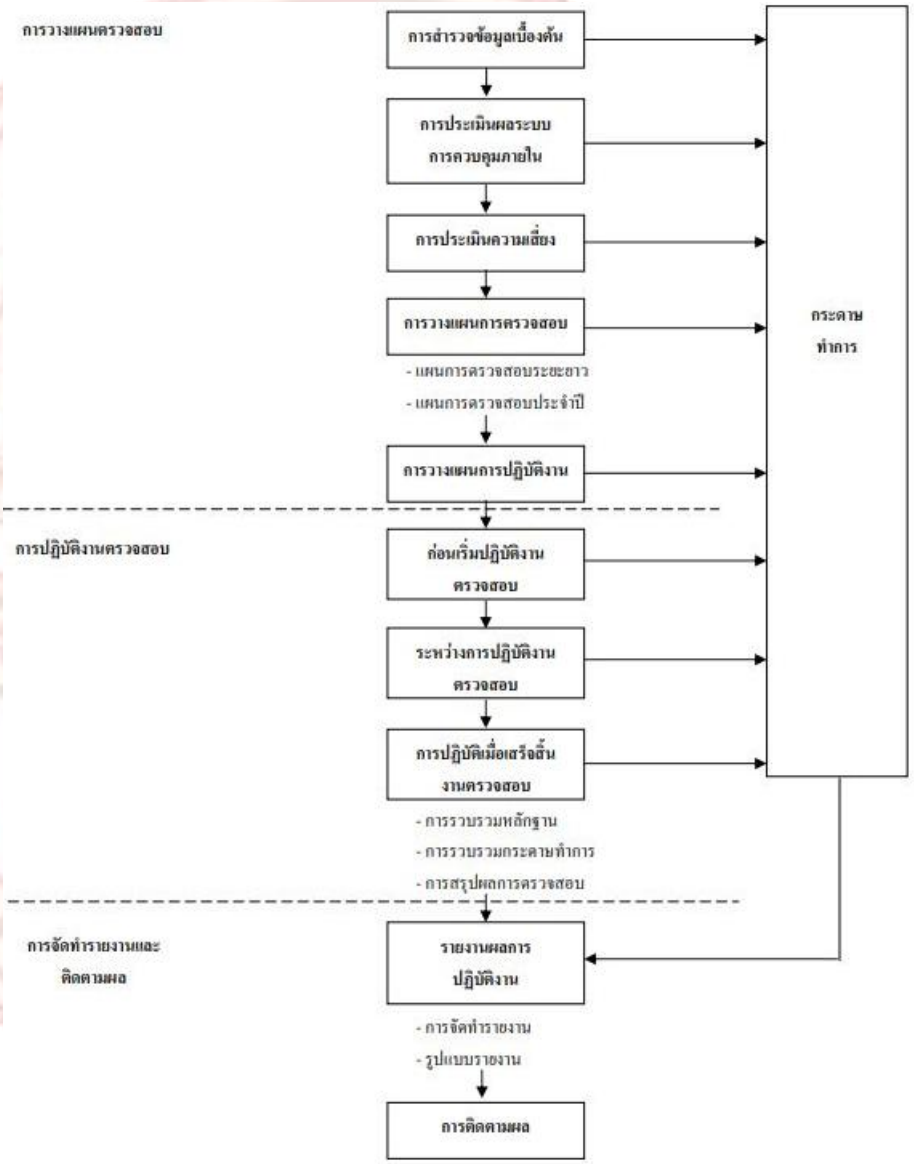
ขั้นตอนที่ 1 การวางแผนตรวจสอบ การวางแผนเป็นการคิดล่วงหน้าก่อนที่จะลงมือปฏิบัติงานจริงว่าจะตรวจสอบเรื่องใด ด้วยวัตถุประสงค์อะไร ที่หน่วยรับตรวจใด ณ เวลาไหน และใช้เวลาตรวจสอบเท่าไร โดยใช้ทรัพยากรที่มีอยู่ คือ บุคลากร งบประมาณ และวัสดุอุปกรณ์อย่างเหมาะสม การวางแผนที่ดีช่วยให้การปฏิบัติงานเป็นไปตามวัตถุประสงค์ภายในระยะเวลา งบประมาณ และอัตรากำลังที่กำหนด ซึ่งการวางแผนตรวจสอบประกอบด้วยเนื้อหาสาระสำคัญ 3 เรื่อง ได้แก่ (1) ประเภทของการวางแผนตรวจสอบ (2) ขั้นตอนของการวางแผนตรวจสอบ และ (3) การเสนอแผนการตรวจสอบ

ขั้นตอนที่ 2 การปฏิบัติงานตรวจสอบ คือ กระบวนการตรวจสอบ สอบทาน และรวบรวมหลักฐานเพื่อวิเคราะห์และประเมินผลการปฏิบัติงานของหน่วยงานต่าง ๆ ว่าเป็นไปตามนโยบาย แผนงาน ระเบียบปฏิบัติขององค์กร รวมทั้งกฎหมายที่เกี่ยวข้องพร้อมทั้งเสนอข้อมูลที่ได้จากการตรวจสอบ และข้อเสนอแนะต่อผู้บริหารเพื่อประกอบการตัดสินใจในการบริหารงาน โดยการปฏิบัติงานตรวจสอบประกอบด้วยสาระสำคัญ 3 เรื่อง ได้แก่ (1) ก่อนเริ่มปฏิบัติงานตรวจสอบ (2) ระหว่างการปฏิบัติงานตรวจสอบ และ (3) การปฏิบัติเมื่อเสร็จสิ้นงานตรวจสอบ

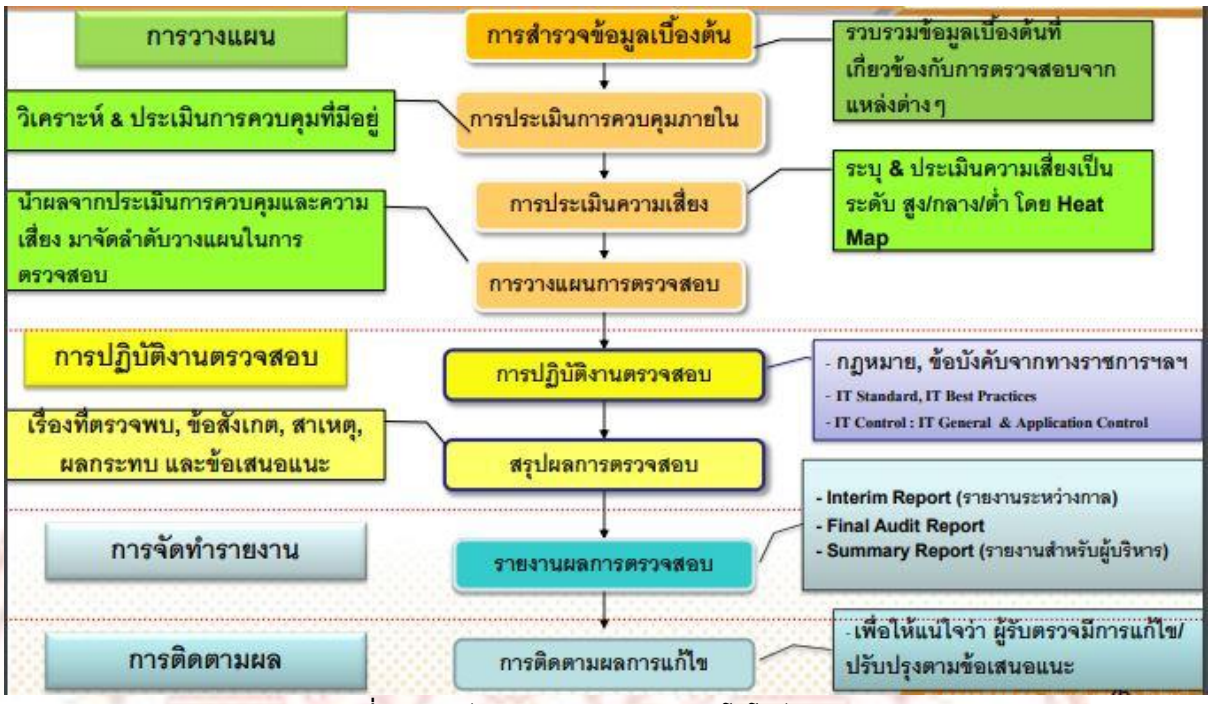
ขั้นตอนที่ 3 การจัดทำรายงานและติดตามผล การจัดทำรายงานเป็นการรายงานผลการปฏิบัติงานให้ผู้บริหารทราบถึงวัตถุประสงค์ ขอบเขต วิธีปฏิบัติงานและผลการตรวจสอบข้อมูลทั้งหมดทุกขั้นตอน สรุปข้อบกพร่องที่ตรวจพบ ประเด็นความเสี่ยงที่สำคัญและการควบคุม รวมทั้งเรื่องอื่น ๆ ที่ผู้บริหารควรทราบ พร้อมข้อเสนอแนะในการแก้ไขปรับปรุง เพื่อเสนอผู้บริหารหรือผู้ที่เกี่ยวข้องพิจารณาสั่งการแก้ไขปรับปรุงต่อไป ซึ่งลักษณะของรายงานผลการปฏิบัติงานที่ดี มีองค์ประกอบดังนี้ (1) ถูกต้อง (Accuracy) (2) ชัดเจน (Clarity) (3) กะทัดรัด (Conciseness) (4) ทันกาล (Timeliness) (5) สร้างสรรค์ (Constructive Criticism) และ (6) จูงใจ (Pursuance)

การติดตามผลเป็นขั้นตอนสุดท้ายของกระบวนการปฏิบัติงานตรวจสอบภายใน ซึ่งถือได้ว่าเป็นขั้นตอนที่สำคัญของการตรวจสอบ เพราะแสดงถึงคุณภาพและประสิทธิผลของงานตรวจสอบว่าผู้รับการตรวจและผู้บริหารได้ปฏิบัติตามข้อเสนอแนะในรายงานการปฏิบัติงานตรวจสอบหรือไม่ และข้อบกพร่องที่พบได้รับการแก้ไขอย่างเหมาะสมแล้วหรือยัง เมื่อผู้ตรวจสอบภายในเสนอรายงานผลการปฏิบัติงานต่อผู้บริหารระดับสูงแล้ว ผู้ตรวจสอบภายในต้องติดตามผลว่าผู้บริหารฯ ได้สั่งการหรือไม่ประการใด และหากสั่งการแล้ว หน่วยรับตรวจดำเนินการตามข้อเสนอแนะของผู้ตรวจสอบ

ภายในที่ผู้บริหารสั่งการหรือไม่ เพื่อให้แน่ใจว่าข้อบกพร่องที่พบได้รับการแก้ไขอย่างเหมาะสม หรือมีปัญหาและอุปสรรคอย่างไร และรายงานผลการติดตามต่อผู้บริหารต่อไป ทั้งนี้ผู้บริหารที่ได้รับทราบแล้วไม่ได้สั่งการแก้ไขตามข้อเสนอแนะ แสดงว่าผู้บริหารยอมรับภาระความเสี่ยงหากเกิดความเสียหายขึ้นในอนาคต



ภาพที่ 2-9 กระบวนการปฏิบัติงานตรวจสอบภายใน (Internal Audit Process)
(ที่มา : กรมบัญชีกลาง)



ภาพที่ 2-10 วิธีการตรวจสอบระบบเทคโนโลยีสารสนเทศ

(ที่มา : สมภพ เตชเสนสกุล)

บทที่ 3
วิธีดำเนินการวิจัย

การศึกษาวิจัยเรื่อง แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยมุ่งศึกษาปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และนำเสนอแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยมีขั้นตอนและวิธีการดำเนินงานวิจัยดังต่อไปนี้

3.1 รูปแบบการวิจัย

3.2 การทบทวน ศึกษาเอกสาร และงานวิจัยที่เกี่ยวข้อง

3.3 ประชากรหรือกลุ่มผู้ให้ข้อมูล

3.4 เครื่องมือที่ใช้ในการวิจัย

3.5 โมเดลการวิจัย

3.6 แหล่งข้อมูลและการเก็บรวบรวมข้อมูล

3.7 การวิเคราะห์ข้อมูล

3.1 รูปแบบการวิจัย

ในการศึกษาวิจัยครั้งนี้ เป็นการวิจัยในรูปแบบการวิจัยเชิงคุณภาพ (Quantitative Research) โดยรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึก (In-depth Interview) ตามที่ได้ทบทวนศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง เพื่อกำหนดกรอบแนวคิดในการศึกษาสมมติฐานงานวิจัย ประชากรหรือผู้ให้สัมภาษณ์ เครื่องมือที่ใช้ในงานวิจัย การวิเคราะห์ข้อมูล และแผนดำเนินงานวิจัย

3.2 การทบทวน ศึกษาเอกสาร และงานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้ทบทวน และศึกษาเอกสารงานวิจัยและข้อมูลที่เกี่ยวข้องกับปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ เช่น การค้นคว้าจากฐานข้อมูล เอกสารวิชาการ และการค้นคว้าข้อมูลจากอินเทอร์เน็ต เพื่อศึกษาข้อมูลเกี่ยวกับการทำการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรวบรวม

ปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ นำมาสู่โมเดลการวิจัยในการศึกษาสมมติฐานงานวิจัย

3.3 ประชากรหรือกลุ่มผู้ให้ข้อมูล

ประชากรหรือกลุ่มผู้ให้ข้อมูลที่ใช้ในงานวิจัย คือ ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศและผู้ตรวจสอบภายในที่มีประสบการณ์ด้านการตรวจสอบด้านเทคโนโลยีสารสนเทศในประเทศไทย จำนวน 6 คน โดยแบ่งเป็น ผู้อำนวยการฝ่ายตรวจสอบด้านเทคโนโลยีสารสนเทศ จำนวน 1 ท่าน ผู้ช่วยผู้จัดการ จำนวน 1 ท่าน ผู้ตรวจสอบภายในอาวุโส จำนวน 1 ท่าน ผู้เชี่ยวชาญสเปเชียลลิสด้านการตรวจสอบภายใน จำนวน 1 ท่าน ผู้ตรวจสอบภายในและตรวจสอบด้านเทคโนโลยีสารสนเทศ จำนวน 2 ท่าน

3.4 เครื่องมือที่ใช้ในการวิจัย

ในการศึกษาวิจัยครั้งนี้เป็นการศึกษาเชิงคุณภาพ เพื่อให้ได้ข้อมูลเกี่ยวกับปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และเนื่องจากมีข้อจำกัดเกี่ยวกับจำนวนประชากรที่ใช้ในงานวิจัย ทางผู้วิจัยจึงใช้การสัมภาษณ์แบบเชิงลึก (In-depth Interview) ด้วยคำถามปลายเปิด โดยเครื่องมือที่ใช้ในการศึกษาวิจัย มีดังนี้

3.4.1) ผู้วิจัย ผู้วิจัยเป็นเครื่องมือสำคัญในการทำหน้าที่เป็นผู้สังเกตการณ์ ตั้งคำถาม จดบันทึก และการวิเคราะห์ข้อมูล แต่เนื่องจากการสัมภาษณ์แบบเชิงลึก เป็นการสื่อสารหรือพูดคุยเพื่อรวบรวมข้อมูลด้านข้อเท็จจริงและข้อมูลด้านความคิดเห็น

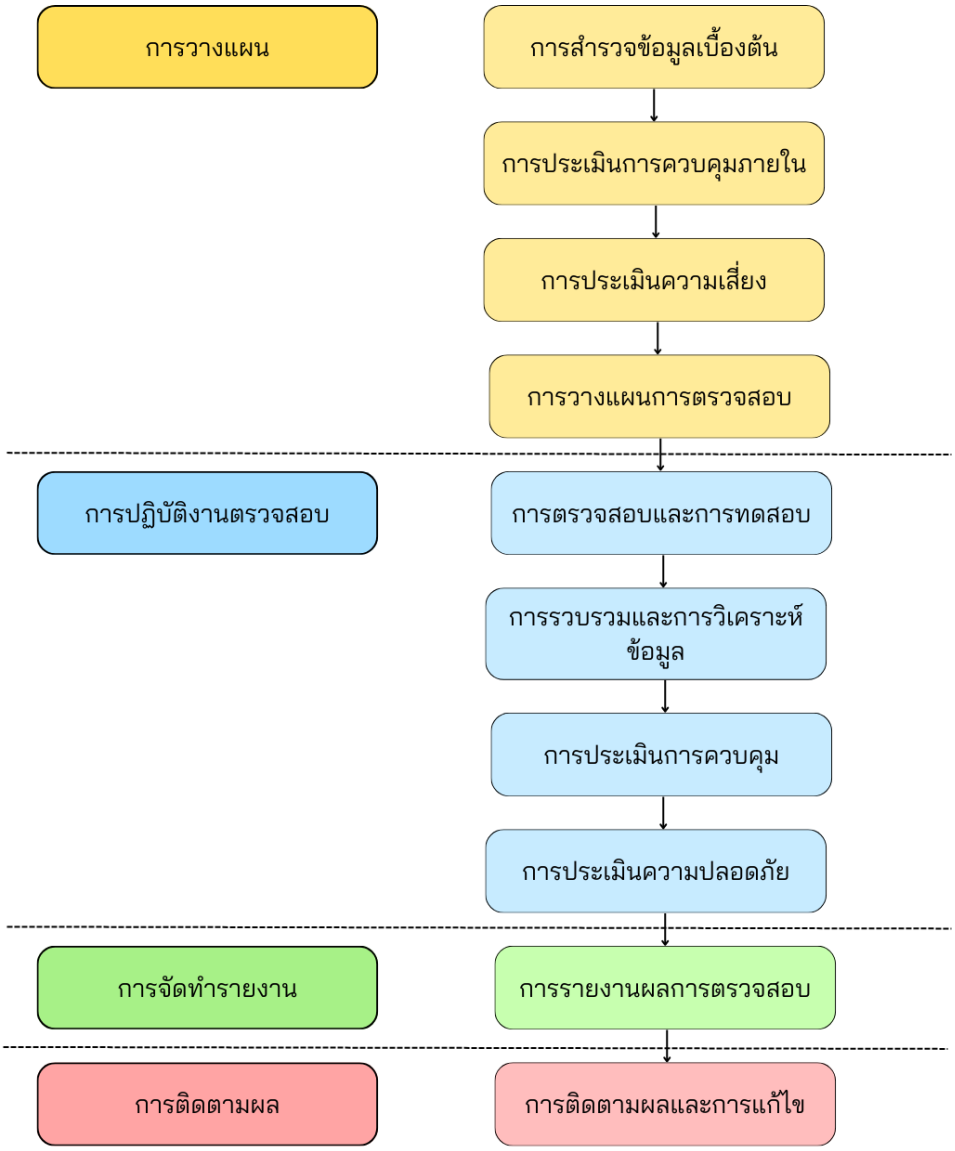
3.4.2) การสัมภาษณ์ ผู้วิจัยได้ใช้การสัมภาษณ์แบบมีโครงสร้าง (Structured Interview) ซึ่งเป็นวิธีการสัมภาษณ์ที่ผู้สัมภาษณ์จัดเตรียมข้อคำถามไว้เป็นชุดคำถามที่สมบูรณ์ครอบคลุมประเด็นที่ต้องการ และทำการสัมภาษณ์หรือซักถามตามประเด็นข้อคำถามที่จัดไว้ ซึ่งการสัมภาษณ์เป็นไปแบบไม่เป็นทางการ (Informal Interview) เพื่อสร้างความเป็นกันเอง และยืดหยุ่นในการตอบคำถามของผู้ให้สัมภาษณ์ โดยผู้วิจัยได้เริ่มสัมภาษณ์จากปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และเมื่อสัมภาษณ์ครบทุกปัจจัย ผู้วิจัยจึงได้สัมภาษณ์ในประเด็นถัดไป คือ

แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยผู้วิจัยได้เปิดโอกาสให้ผู้สัมภาษณ์ได้อธิบายแนวทางตามที่ผู้ให้สัมภาษณ์ปฏิบัติงานอยู่ หรือประสบการณ์ที่ผู้ให้สัมภาษณ์เคยปฏิบัติมาก่อน โดยได้ทำการสัมภาษณ์ทั้งหมด 6 ครั้ง ซึ่งในแต่ละครั้งใช้เวลาในการสัมภาษณ์เฉลี่ยครั้งละ 18 นาที โดยทำการสัมภาษณ์ตั้งแต่วันที่ 4 ตุลาคม พ.ศ.2567 ถึงวันที่ 23 ตุลาคม พ.ศ. 2567

3.4.3) อุปกรณ์ที่ใช้ในการสัมภาษณ์ ผู้วิจัยใช้อุปกรณ์ที่ใช้ในการสัมภาษณ์ ประกอบไปด้วย เครื่องบันทึกเสียง เพื่อบันทึกข้อมูลเสียงในการสนทนาและสัมภาษณ์ระหว่างผู้วิจัยกับผู้ให้สัมภาษณ์ โดยผู้วิจัยได้มีการขออนุญาตผู้ให้สัมภาษณ์ก่อนบันทึกเสียงทุกครั้ง ถ้าหากผู้ให้สัมภาษณ์ไม่ยินยอมในการให้บันทึกเสียง ผู้วิจัยจะไม่ทำการบันทึกเสียง และเปลี่ยนไปใช้อุปกรณ์ถัดไปคือ สมุดจดบันทึกหรือแบบบันทึกข้อมูลในการสัมภาษณ์ เพื่อให้ผู้วิจัยใช้จดบันทึกข้อมูลที่ได้จากการสัมภาษณ์ การสังเกตุ รวมถึงประเด็นความคิดเห็นต่างๆที่ได้จากผู้ให้สัมภาษณ์

3.5 โมเดลการวิจัย

โมเดลแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ



ภาพที่ 3-1 โมเดลแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ผู้วิจัยได้นำโมเดลของสมภพ เตชเสนสกุล นำมาประยุกต์ใช้กับงานวิจัยที่ผู้วิจัยได้ทำการศึกษา ซึ่งประกอบด้วย 4 ขั้นตอนหลัก ดังนี้

ขั้นตอนที่ 1 การวางแผน ขั้นตอนนี้เกี่ยวข้องกับการกำหนดขอบเขตและวัตถุประสงค์ของการตรวจสอบ รวมถึงการระบุระบบ กระบวนการ และการควบคุมที่จะถูกตรวจสอบ ตลอดจนการทำความเข้าใจสภาพแวดล้อมด้านสารสนเทศ ความเสี่ยง และข้อกำหนดด้านกฎระเบียบขององค์กร

ประกอบด้วย 4 ขั้นตอน ดังนี้ (1) การสำรวจข้อมูลเบื้องต้น (2) การประเมินการควบคุมภายใน (3) การประเมินความเสี่ยง และ (4) การวางแผนการตรวจสอบ

ขั้นตอนที่ 2 การปฏิบัติงานตรวจสอบ ทำการตรวจสอบตามแผนงานที่วางไว้ให้ครบทุกขั้นตอน แล้วทำการสรุปผลการตรวจสอบ ซึ่งผลของการตรวจสอบทำให้ระบุถึงข้อบกพร่องที่ตรวจพบ ข้อสังเกตต่าง ๆ สาเหตุของข้อบกพร่องนั้น ผลกระทบที่อาจเกิดขึ้น รวมถึงข้อเสนอแนะที่จะนำเสนอ ประกอบด้วย 4 ขั้นตอน ดังนี้ (1) การตรวจสอบและการทดสอบ (2) การรวบรวมและการวิเคราะห์ข้อมูล (3) การประเมินการควบคุม และ (4) การประเมินความปลอดภัย

ขั้นตอนที่ 3 การจัดทำรายงาน หลังจากดำเนินการตรวจสอบแล้ว ผู้ตรวจสอบจะบันทึกสิ่งที่ค้นพบ รวมถึงจุดอ่อน ช่องโหว่ หรือส่วนที่ไม่ปฏิบัติตามที่ระบุใด ๆ รวมถึงให้คำแนะนำเพื่อแก้ไขปัญหาเหล่านี้และปรับปรุงการกำกับดูแลด้านสารสนเทศและความปลอดภัย และจัดเตรียมรายงานการตรวจสอบโดยละเอียด รายงานนี้เสนอให้กับฝ่ายบริหาร ผู้มีส่วนได้ส่วนเสีย และหน่วยงานกำกับดูแลที่เกี่ยวข้อง

ขั้นตอนที่ 4 การติดตามผล การติดตามผลและการแก้ไข หลังจากดำเนินการตามการเปลี่ยนแปลงที่แนะนำ องค์กรอาจได้รับการตรวจสอบติดตามผลเพื่อประเมินว่ามีการดำเนินการแก้ไขหรือไม่ และแก้ไขปัญหาที่ระบุได้อย่างมีประสิทธิภาพหรือไม่ ขั้นตอนนี้ช่วยให้มั่นใจได้ถึงการปรับปรุงอย่างต่อเนื่องและการปฏิบัติตามคำแนะนำการตรวจสอบด้านสารสนเทศ

3.6 แหล่งข้อมูลและการเก็บรวบรวมข้อมูล

ผู้วิจัยได้ศึกษาและเก็บรวบรวมข้อมูลจากแหล่งข้อมูลต่างๆ ทั้งจากงานวิจัย วารสาร วิทยานิพนธ์ และเว็บไซต์ เพื่อศึกษาและทำความเข้าใจเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ แล้วเลือกวิเคราะห์ประเด็นที่สนใจ โดยผู้วิจัยแบ่งประเภทของข้อมูลตามรูปแบบการเก็บข้อมูลเป็น 2 ประเภท ดังนี้

รูปแบบที่ 1 ข้อมูลปฐมภูมิ (Primary Data) เป็นข้อมูลที่อยู่ในรูปแบบประสบการณ์ของแต่ละบุคคล การเก็บข้อมูลจะรวบรวมด้วยวิธีการสัมภาษณ์แบบเจาะลึกกับผู้ให้สัมภาษณ์ ซึ่งในการเลือกตัวอย่างจะเป็นแบบเฉพาะเจาะจง โดยเป็นการเลือกกลุ่มตัวอย่างแบบเจาะจงเฉพาะผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศในประเทศไทย และการสัมภาษณ์จะใช้การสัมภาษณ์แบบมีโครงสร้าง (Structured Interview) นอกจากนี้ ผู้วิจัยได้ทำการศึกษานำร่องเพื่อใช้เป็นแนวทางในการสร้างกรอบงานวิจัย ตั้งคำถามในการสัมภาษณ์ และวิเคราะห์ผลของข้อมูลที่ได้จากการสัมภาษณ์

สำหรับการกำหนดโครงสร้างของคำถามในการสัมภาษณ์เชิงลึก (In-depth Interview) ผู้วิจัยได้ตั้งคำถามที่จะใช้สัมภาษณ์ 9 คำถาม ประกอบด้วย

คำถามที่ 1 ท่านคิดว่าความเป็นอิสระของผู้ตรวจสอบ ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

คำถามที่ 2 ท่านคิดว่าความรู้ความสามารถของผู้ตรวจสอบ ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

คำถามที่ 3 ท่านคิดว่าวุฒิภาวะ ทักษะ และประสบการณ์ของผู้ตรวจสอบ ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

คำถามที่ 4 ท่านคิดว่าจรรยาบรรณและจริยธรรมของผู้ตรวจสอบ ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

คำถามที่ 5 ท่านคิดว่ามาตรฐานการตรวจสอบ ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

คำถามที่ 6 ท่านคิดว่าการสนับสนุนจากผู้บริหาร ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

คำถามที่ 7 ท่านคิดว่าการวางแผนการตรวจสอบ ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

คำถามที่ 8 ท่านคิดว่าการวิเคราะห์ความเสี่ยง ส่งผลต่อความสำเร็จในการตรวจสอบเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

คำถามที่ 9 ท่านคิดว่าแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศควรเป็นอย่างไร หรือมีขั้นตอนการปฏิติใดบ้าง

การวิจัยครั้งนี้มีวิธีการเก็บรวบรวมข้อมูล ดังนี้

ขั้นตอนที่ 1 การวางแผนการสัมภาษณ์เชิงลึกและกำหนดขั้นตอนในการเก็บรวบรวมข้อมูล เริ่มจากการสรรหาและคัดเลือกผู้ให้สัมภาษณ์ รวมถึงตั้งประเด็นคำถามที่ใช้ในการสัมภาษณ์

ขั้นตอนที่ 2 การสรรหาและคัดเลือกผู้ให้สัมภาษณ์ ผู้วิจัยได้สรรหาผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศในประเทศไทย โดยพิจารณาจากคุณสมบัติที่ตรงกับความต้องการ บุคคลหรือผู้ให้สัมภาษณ์ท่านนั้นสะดวกในการให้ข้อมูล และสามารถนัดเวลาที่เหมาะสมในการสัมภาษณ์

ขั้นตอนที่ 3 การสัมภาษณ์ด้วยตัวผู้วิจัยเอง พร้อมทั้งแนะนำตัว แจ้งวัตถุประสงค์ โดยก่อนที่ผู้วิจัยจะทำการสัมภาษณ์ ผู้วิจัยได้ขออนุญาตใช้เครื่องบันทึกเสียง รวมถึงทำการสอบถามเกี่ยวกับข้อมูลเบื้องต้น ทำความรู้จัก และสร้างความสัมพันธ์อันดีก่อน เพื่อให้เกิดความเชื่อใจและพร้อมที่จะให้ข้อมูลได้อย่างเต็มที่ ก่อนที่จะทำการสัมภาษณ์เชิงลึกต่อไป

ขั้นตอนที่ 4 การสัมภาษณ์เชิงลึกกับผู้ให้สัมภาษณ์ ก่อนการสัมภาษณ์ ผู้วิจัยได้เตรียมตัวและเตรียมคำถามที่ใช้ในการสัมภาษณ์ โดยการหาข้อมูลเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศ ปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งการสัมภาษณ์เป็นไปแบบกันเอง ไม่กดดัน เพื่อสร้างความสบายใจและไม่อึดอัดในการให้ข้อมูลและตอบคำถามของผู้ให้สัมภาษณ์ และเมื่อจบการสัมภาษณ์ผู้วิจัยได้ทำการพูดคุยเกี่ยวกับการทำวิจัยครั้งนี้บ้างเล็กน้อย รวมถึงได้ทำการขอบคุณผู้ให้สัมภาษณ์สำหรับการสละเวลาส่วนตัวมาให้ผู้วิจัยได้ทำการสัมภาษณ์ในครั้งนี้

ขั้นตอนที่ 5 การรวบรวมข้อมูลที่ได้จากการสัมภาษณ์ ผู้วิจัยได้เริ่มถอดคำสัมภาษณ์ของผู้ให้สัมภาษณ์ และสร้างเอกสารของแต่ละคนไว้ จากนั้นผู้วิจัยได้อ่านเอกสารที่ได้จากการถอดคำสัมภาษณ์รวมกับอ่านข้อมูลที่ได้จากการจดบันทึก เพื่อรวบรวมข้อมูลที่เป็นประโยชน์ต่องานวิจัย เพื่อนำไปวิเคราะห์ข้อมูลและสรุปผลการวิจัยต่อไป

ขั้นตอนที่ 6 การวิเคราะห์ข้อมูลและสรุปผลการวิจัยที่ได้จากการสัมภาษณ์ ผู้วิจัยใช้วิธีการจำแนกข้อมูล โดยใช้การวิเคราะห์คำหลักหรือประเด็นหลักที่เกี่ยวข้องกับแต่ละคำถาม จากนั้นสร้างข้อสรุปแบบอุปนัย (Analytic Induction) เพื่อสรุปข้อมูลเพื่อนำมาเชื่อมโยงกับข้อมูลที่ผู้วิจัยได้ทำการศึกษาหรือทบทวนวรรณกรรมมา เพื่อให้ได้ข้อมูลที่สามารถตอบคำถามงานวิจัย และวัตถุประสงค์ของงานวิจัยได้

รูปแบบที่ 2 ข้อมูลทุติยภูมิ เป็นข้อมูลที่ได้จากการที่ผู้วิจัยได้ทำการศึกษาข้อมูลเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศ ปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ จากทั้งการทบทวนวรรณกรรม การค้นคว้าจากหนังสือ บทความ เอกสารทางวิชาการ เว็บไซต์ และงานวิจัยที่เกี่ยวข้อง

3.7 การวิเคราะห์ข้อมูล

ผู้วิจัยจะนำข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก (In-depth Interview) มาวิเคราะห์โดยใช้ระเบียบวิธีเชิงคุณภาพ (Qualitative Methodology) โดยอาศัยวิธีการ วิเคราะห์เนื้อหา (Content Analysis) ซึ่งเป็นกระบวนการวิเคราะห์ข้อมูลที่มุ่งเน้นการตีความเชิงลึกจากข้อความหรือถ้อยคำของผู้ให้ข้อมูล เพื่อระบุประเด็นหลัก รูปแบบ หรือความหมายที่แฝงอยู่ในเนื้อหาการสื่อสาร

ในการดำเนินการ ผู้วิจัยจะเริ่มจากการถอดบทสัมภาษณ์ออกมาเป็นข้อความอย่างละเอียด (Transcription) แล้วทำการอ่านบทสัมภาษณ์ซ้ำหลายรอบ (Repeated Reading) เพื่อทำความเข้าใจและซึมซับข้อมูลเชิงลึก จากนั้นจะทำการแยกแยะคำหลัก (Keywords) หรือประเด็นสำคัญที่สัมพันธ์กับคำถามการวิจัย

การวิเคราะห์ข้อมูลจะอยู่ในลักษณะของการ วิเคราะห์เชิงอุปนัย (Inductive Content Analysis) โดยไม่ยึดติดกับทฤษฎี แต่เปิดโอกาสให้ประเด็นต่าง ๆ ปรากฏขึ้นจากข้อมูลจริง แล้วนำมาจัดกลุ่ม และสร้างข้อสรุปที่สะท้อนความสำคัญของแต่ละปัจจัยตามที่ผู้ให้ข้อมูลสะท้อนผ่านคำพูดของตน

นอกจากนี้ ข้อมูลที่ได้จะถูกอธิบายอย่างมีโครงสร้างในลักษณะการบรรยายเชิงพรรณนา (Narrative Description) โดยผู้วิจัยจะเน้นคุณภาพและน้ำหนักความสำคัญของข้อมูล รวมถึงความสอดคล้องระหว่างคำตอบของผู้ให้ข้อมูลในแต่ละประเด็น เพื่อสังเคราะห์และ ตีความ (Interpretation) ให้เชื่อมโยงกับวัตถุประสงค์ของการวิจัย และแนวคิดหรือทฤษฎีที่เกี่ยวข้อง

ผลลัพธ์ที่ได้จากการวิเคราะห์จะถูกใช้เพื่อจัดทำข้อเสนอแนะในเชิงแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งตอบโจทย์ทั้งวัตถุประสงค์ข้อที่ 1 คือการศึกษาปัจจัยที่ส่งผลต่อความสำเร็จ และข้อที่ 2 คือการเสนอแนวทางปฏิบัติที่เหมาะสมต่อไป

บทที่ 4
ผลการดำเนินการวิจัย

การศึกษาเรื่อง “แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ” มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และนำเสนอแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยใช้วิธีการวิจัยในรูปแบบการวิจัยเชิงคุณภาพ (Quantitative Research) โดยรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศในประเทศไทย จำนวน 6 คน โดยมีผลการดำเนินการวิจัย ดังต่อไปนี้

4.1 ข้อมูลทั่วไปของผู้ให้สัมภาษณ์

4.2 ความเป็นอิสระของผู้ตรวจสอบ

4.3 ความรู้ความสามารถของผู้ตรวจสอบ

4.4 วุฒิภาวะ ทักษะ และประสบการณ์ของผู้ตรวจสอบ

4.5 จรรยาบรรณและจริยธรรมของผู้ตรวจสอบ

4.6 มาตรฐานการตรวจสอบ

4.7 การสนับสนุนจากผู้บริหาร

4.8 การวางแผนการตรวจสอบ

4.9 การวิเคราะห์ความเสี่ยง

4.10 แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

4.1 ข้อมูลทั่วไปของผู้ให้สัมภาษณ์

จากการสัมภาษณ์ข้อมูลทั่วไปของผู้ให้สัมภาษณ์ทั้ง 6 คน พบว่า เป็นผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ และผู้ตรวจสอบภายในที่มีประสบการณ์การตรวจสอบด้านเทคโนโลยีสารสนเทศในประเทศไทย ที่มีประสบการณ์การทำงานตั้งแต่ 2-15 ปี ซึ่งไม่มีใบประกาศนียบัตรด้านการตรวจสอบด้านเทคโนโลยีสารสนเทศ แต่บางคนมีใบประกาศนียบัตรด้านอื่นๆที่เกี่ยวข้องกับการตรวจสอบด้านเทคโนโลยีสาร

4.2 ความเป็นอิสระของผู้ตรวจสอบ

ความเป็นอิสระของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศถือเป็นรากฐานของการตรวจสอบที่มีประสิทธิภาพและน่าเชื่อถือ ผู้ให้สัมภาษณ์ทุกคนเห็นพ้องว่า หากขาดความเป็นอิสระแล้ว ผลการตรวจสอบอาจไม่สะท้อนความเป็นจริงอย่างตรงไปตรงมา โดยเฉพาะเมื่อต้องเผชิญกับแรงกดดันจากผู้มีอำนาจในองค์กร

ผู้ให้สัมภาษณ์คนที่ 1 กล่าวอย่างชัดเจนว่า “ถ้าไม่มีอิสระ ผู้ตรวจสอบจะกลายเป็นเพียงเครื่องมือของผู้บริหาร ผลที่ออกมาก็ไม่เป็นกลาง” ขณะเดียวกัน ผู้ให้สัมภาษณ์คนที่ 5 ชี้ว่า “บางองค์กรผู้ตรวจสอบไม่ได้รายงานต่อคณะกรรมการตรวจสอบโดยตรง ทำให้มีแรงกดดันเรื่องการนำเสนอข้อค้นพบที่อาจกระทบกับผู้บริหาร”

ทั้งนี้ ความอิสระอาจถูกจำกัดจากโครงสร้างการบังคับบัญชาที่ไม่เหมาะสม เช่น ขึ้นตรงกับฝ่ายบริหารที่เป็นผู้รับการตรวจสอบเอง ทำให้เกิดความขัดแย้งทางผลประโยชน์ ดังนั้น การจัดโครงสร้างองค์กรที่เอื้อให้เกิดความเป็นอิสระ เช่น การรายงานต่อคณะกรรมการตรวจสอบ (Audit Committee) โดยตรง จึงเป็นกลไกสำคัญที่ช่วยส่งเสริมความน่าเชื่อถือของผลการตรวจสอบ

4.3 ความรู้ความสามารถของผู้ตรวจสอบ

ความรู้ความสามารถทางเทคโนโลยีของผู้ตรวจสอบเป็นหัวใจสำคัญของการตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีคุณภาพ โดยเฉพาะในยุคที่เทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็ว ผู้ให้สัมภาษณ์ทั้ง 6 คนต่างย้ำถึงความสำคัญของการมีความรู้ทั้งด้านเทคนิค (Technical knowledge) และระบบควบคุมภายใน

ผู้ให้สัมภาษณ์คนที่ 4 ให้ความเห็นว่า “อย่างน้อยต้องเข้าใจเรื่อง general control และ application control ไม่งั้นจะคุยกับฝ่ายไอทีไม่รู้เรื่อง แล้วก็จะพลาดประเด็นสำคัญ” ขณะที่ผู้ให้สัมภาษณ์คนที่ 2 ระบุว่า “การมีความรู้ด้านไอทีโดยตรง จะช่วยให้เรามองเห็นจุดเสี่ยงในระบบที่ซ่อนอยู่ ซึ่งผู้ตรวจสอบทั่วไปอาจมองไม่เห็น”

ความสามารถที่ว่านี้ต้องครอบคลุมทั้งระบบฮาร์ดแวร์ ซอฟต์แวร์ การบริหารจัดการความเสี่ยง รวมถึงความเข้าใจในบริบทธุรกิจขององค์กรด้วย การพัฒนาความรู้ต่อเนื่องจึงเป็นสิ่งจำเป็นสำหรับผู้ตรวจสอบไอทีเพื่อให้สามารถรับมือกับภัยคุกคามและเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็ว

4.4 วุฒิภาวะ ทักษะ และประสบการณ์ของผู้ตรวจสอบ

วุฒิภาวะและประสบการณ์ของผู้ตรวจสอบส่งผลโดยตรงต่อความสามารถในการวิเคราะห์ประเมินความเสี่ยง และสร้างความร่วมมือกับผู้รับการตรวจสอบ โดยเฉพาะในประเด็นที่ละเอียดอ่อน

หรือกระทบต่อความมั่นคงของระบบ ผู้ให้สัมภาษณ์ทุกคนต่างชี้ว่า ความสามารถในการสื่อสารและโน้มน้าวใจเป็นปัจจัยสำคัญที่ช่วยให้งานตรวจสอบราบรื่น

ผู้ให้สัมภาษณ์คนที่ 6 กล่าวว่า “เวลาไปเจอคนที่ไม่ให้ความร่วมมือ ถ้าไม่มีประสบการณ์ เราจะจัดการสถานการณ์แบบนั้นไม่เป็นเลย” อีกทั้ง ผู้ให้สัมภาษณ์คนที่ 3 เน้นว่า “การมีประสบการณ์หลากหลาย จะทำให้ผู้ตรวจสอบมองเห็นภาพรวมและสามารถเสนอแนะแบบที่เหมาะสมกับแต่ละบริบทได้”

ดังนั้น การเสริมสร้างทักษะด้าน soft skill ควบคู่กับความรู้เชิงเทคนิคจึงเป็นสิ่งจำเป็น เช่น ทักษะการเจรจา การตั้งคำถาม การฟังอย่างมีประสิทธิภาพ รวมถึงการควบคุมอารมณ์และการวางตัวอย่างเหมาะสมในการทำงานร่วมกับผู้บริหารระดับสูง

4.5 จรรยาบรรณและจริยธรรมของผู้ตรวจสอบ

จรรยาบรรณและจริยธรรมของผู้ตรวจสอบไม่เพียงแต่เป็นหลักประกันด้านความโปร่งใส แต่ยังส่งผลโดยตรงต่อความไว้วางใจจากผู้ที่เกี่ยวข้องกับกระบวนการตรวจสอบ โดยเฉพาะในประเด็นเกี่ยวกับการรักษาความลับ และความเป็นกลาง

ผู้ให้สัมภาษณ์คนที่ 1 กล่าวไว้ว่า “ข้อมูลที่เราตรวจสอบบางครั้งเป็นข้อมูลที่ละเอียดอ่อนมาก ถ้ารั่วไหลก็มีผลกระทบต่อทั้งองค์กร” ขณะที่ผู้ให้สัมภาษณ์คนที่ 5 ย้ำว่า “ความเป็นกลางต้องมาก่อน ถ้าเราเข้าข้างฝ่ายใดฝ่ายหนึ่ง งานตรวจสอบจะไม่มีความน่าเชื่อถือเลย”

จริยธรรมยังรวมถึงการไม่ใช้ตำแหน่งหน้าที่แสวงหาผลประโยชน์ส่วนตัว รวมถึงการหลีกเลี่ยงความขัดแย้งทางผลประโยชน์ (Conflict of Interest) การปฏิบัติตามหลักจรรยาบรรณของวิชาชีพ เช่น IIA Code of Ethics หรือ ISACA Code of Professional Ethics จึงมีความสำคัญอย่างยิ่งต่อวิชาชีพนี้

4.6 มาตรฐานการตรวจสอบ

มาตรฐานการตรวจสอบช่วยกำหนดกรอบในการทำงานให้มีความเป็นระบบ ถูกต้อง และสามารถอ้างอิงได้เมื่อเกิดข้อโต้แย้ง โดยเฉพาะเมื่อมีการตรวจสอบย้อนกลับจากหน่วยงานภายนอก ผู้ให้สัมภาษณ์ทุกคนเห็นพ้องว่า มาตรฐาน เช่น ISACA, COBIT, และ ISO/IEC 27001 เป็นต้น เป็นเครื่องมือสำคัญที่ช่วยให้ผู้ตรวจสอบทำงานได้อย่างมั่นใจ

ผู้ให้สัมภาษณ์คนที่ 2 ให้ความเห็นว่า “มาตรฐานช่วยให้เรามีแนวทาง ไม่หลุดจากหลักการที่เป็นที่ยอมรับในระดับสากล” อีกทั้ง ผู้ให้สัมภาษณ์คนที่ 4 กล่าวว่า “ถ้าไม่อัปเดตมาตรฐาน ก็จะพลาดประเด็นที่สำคัญ เพราะระบบไอทีมันพัฒนาเร็วมาก”

การนำมาตรฐานมาประยุกต์ใช้อย่างเหมาะสมกับบริบทขององค์กร และการมีระบบติดตามการเปลี่ยนแปลงของมาตรฐาน เป็นสิ่งที่จำเป็นอย่างยิ่งสำหรับการคงไว้ซึ่งคุณภาพของการตรวจสอบ

4.7 การสนับสนุนจากผู้บริหาร

การสนับสนุนจากผู้บริหารเป็นปัจจัยเชิงโครงสร้างที่ส่งผลต่อประสิทธิภาพของกระบวนการตรวจสอบอย่างมีนัยสำคัญ โดยเฉพาะในการขอข้อมูล ความร่วมมือ หรือการดำเนินการตามข้อเสนอแนะ ผู้ให้สัมภาษณ์หลายคนย้ำว่า หากผู้บริหารให้ความสำคัญกับการตรวจสอบ จะส่งผลดีต่อการปฏิบัติงานของทีมตรวจสอบ

ผู้ให้สัมภาษณ์คนที่ 3 ระบุว่า “บางครั้งเราตรวจพบจุดอ่อน ถ้าไม่มีผู้บริหารหนุนหลัง หน่วยงานที่เกี่ยวข้องก็ไม่ทำอะไรเลย” ขณะที่ผู้ให้สัมภาษณ์คนที่ 6 ให้มุมมองว่า “ผู้บริหารต้องเข้าใจว่าการตรวจสอบไม่ใช่การจับผิด แต่เป็นการช่วยให้องค์กรมีระบบที่ดีขึ้น”

การสื่อสารกับผู้บริหารจึงควรทำอย่างสม่ำเสมอ เพื่อสร้างความเข้าใจร่วมกันเกี่ยวกับความเสี่ยง และประโยชน์จากการตรวจสอบ การได้รับการสนับสนุนอย่างต่อเนื่องจะทำให้หน่วยตรวจสอบมีความเข้มแข็งมากขึ้น

4.8 การวางแผนการตรวจสอบ

การวางแผนตรวจสอบที่ดีส่งผลโดยตรงต่อประสิทธิภาพของงานตรวจสอบ ผู้ให้สัมภาษณ์ทุกคนเห็นพ้องว่า การเลือกประเด็นหรือระบบที่มีความเสี่ยงสูงก่อนเป็นสิ่งสำคัญ

ผู้ให้สัมภาษณ์คนที่ 1 กล่าวไว้ว่า “ถ้าไม่มีแผนที่ดี เราอาจไปเสียเวลาตรวจงานที่ไม่มีความเสี่ยงสูง แล้วพลาดจุดสำคัญ”

นอกจากนี้ การวางแผนต้องคำนึงถึงทรัพยากรที่มีอยู่ เช่น จำนวนผู้ตรวจสอบและความสามารถเฉพาะด้านของแต่ละคน เพื่อให้แผนสามารถนำไปปฏิบัติได้จริง แผนที่ดีควรยืดหยุ่นและปรับเปลี่ยนได้หากมีเหตุการณ์ไม่คาดคิดเกิดขึ้น เช่น การโจมตีทางไซเบอร์ และเหตุการณ์ฉุกเฉินด้านระบบสารสนเทศ เป็นต้น

4.9 การวิเคราะห์ความเสี่ยง

การวิเคราะห์ความเสี่ยงถือเป็นเครื่องมือสำคัญที่ช่วยให้การตรวจสอบมุ่งเน้นไปยังประเด็นที่มีผลกระทบสูง ผู้ให้สัมภาษณ์ทุกคนยอมรับว่า การวิเคราะห์ความเสี่ยงเป็นตัวกำหนดทิศทางของแผนตรวจสอบประจำปี

ผู้ให้สัมภาษณ์คนที่ 5 ชี้ว่า “การประเมินความเสี่ยงช่วยให้เรารู้ว่าจะต้องให้ความสำคัญกับระบบไหนก่อน”

โดยการวิเคราะห์ควรครอบคลุมทั้งความเสี่ยงเชิงเทคนิคและเชิงธุรกิจ เช่น ความเสี่ยงด้านความมั่นคงของข้อมูล การเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือผลกระทบต่อภาพลักษณ์องค์กร นอกจากนี้ ยังต้องอาศัยข้อมูลจากหลายแหล่ง เช่น รายงานเหตุการณ์ในอดีต พฤติกรรมของผู้ใช้ระบบ และการเปลี่ยนแปลงทางนโยบายภายนอก

4.10 แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

จากการสัมภาษณ์และการศึกษางานวิจัยที่เกี่ยวข้องเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ พบว่า กระบวนการตรวจสอบที่มีขั้นตอนชัดเจนและการดำเนินงานที่มีความรัดกุมเป็นสิ่งสำคัญ โดยมีแหล่งอ้างอิงที่น่าเชื่อถือสนับสนุนแนวทางการตรวจสอบดังกล่าว เช่น กรมบัญชีกลางและทฤษฎีที่เกี่ยวข้องในด้านการตรวจสอบภายใน ซึ่งกล่าวถึงขั้นตอนที่สำคัญในการตรวจสอบที่ครอบคลุมทั้งการวางแผน การปฏิบัติงานตรวจสอบ และการติดตามผล ดังนั้นจึงสามารถสรุปแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศตามขั้นตอนหลักที่ได้จากการศึกษางานวิจัยและสัมภาษณ์ดังนี้

แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ประกอบด้วย 5 ขั้นตอนหลัก

ขั้นตอนที่ 1 การวิเคราะห์ความเสี่ยง (Risk Assessment) ถือเป็นขั้นตอนแรกที่สำคัญในกระบวนการตรวจสอบ โดยการวิเคราะห์หาความเสี่ยงจะช่วยให้ผู้ตรวจสอบเลือกหน่วยงานหรือระบบงานที่มีความเสี่ยงสูงที่สุดในการตรวจสอบ เพื่อลดความเสี่ยงที่อาจเกิดขึ้น และเพิ่มประสิทธิภาพในการตรวจสอบ

โดยผู้ให้สัมภาษณ์หลายคนเห็นตรงกันว่า การประเมินความเสี่ยงควรเป็นขั้นตอนเริ่มต้นในการตรวจสอบ โดยต้องมีการสำรวจข้อมูลเบื้องต้นและการสัมภาษณ์ผู้ใช้งานระบบก่อนการวางแผนจริง เพื่อให้เข้าใจบริบทของระบบงานหรือโครงการที่จะตรวจ ผู้ให้สัมภาษณ์คนที่ 1 กล่าวว่า “จะต้องมีการประเมินความเสี่ยงก่อน ได้เป็นออดิทยูนิเวิร์สออกมา” ขณะที่ผู้ให้สัมภาษณ์คนที่ 3 ย้ำว่า “ก่อนการแพลนนิ่ง จะมีการพรีลิม เราจะต้องไปสัมภาษณ์เขาก่อนว่า งานอันนั้นคืออะไร” แนวคิดนี้สอดคล้องกับโมเดลของสมภพ เตชเสนสกุล และแนวทางของกรมบัญชีกลางที่เน้นว่า การสำรวจข้อมูลและการประเมินความเสี่ยงเป็นขั้นตอนสำคัญที่สุดในการวางรากฐานการตรวจสอบ

ขั้นตอนการวิเคราะห์ความเสี่ยง ประกอบด้วย 2 ขั้นตอน ดังนี้ (1) การสำรวจข้อมูลเบื้องต้นและการพรีลิม (Pre-Audit) และ (2) การประเมินความเสี่ยง ซึ่งได้รับการยืนยันจากแหล่งงานวิจัยที่กล่าวถึงการประเมินความเสี่ยงเป็นขั้นตอนที่ต้องทำอย่างละเอียดก่อนการดำเนินการตรวจสอบจริง

ขั้นตอนที่ 2 การวางแผน ขั้นตอนนี้เกี่ยวข้องกับการกำหนดขอบเขตและวัตถุประสงค์ของการตรวจสอบ รวมถึงการระบุระบบ กระบวนการ และการควบคุมที่จะถูกตรวจสอบ ตลอดจนการทำความเข้าใจสภาพแวดล้อมด้านสารสนเทศ ความเสี่ยง และข้อกำหนดด้านกฎระเบียบขององค์กร ซึ่งการวางแผนที่ดีนั้นจะช่วยให้กระบวนการตรวจสอบมีทิศทางที่ชัดเจนและสามารถทำได้ภายในเวลาและทรัพยากรที่กำหนดได้

ผู้ให้สัมภาษณ์ส่วนใหญ่กล่าวถึงการกำหนดแผนการตรวจสอบล่วงหน้า โดยมีรายละเอียดชัดเจน เช่น ขอบเขตการตรวจสอบ การสุ่มตัวอย่างข้อมูล และการวางโครงสร้างขั้นตอนที่ต้องดำเนินการ ผู้ให้สัมภาษณ์คนที่ 1 กล่าวว่า “เจาะไปว่าในแผนปีที่จะตรวจสอบ แต่ละองค์กรเราจะตรวจสอบอะไรบ้าง และจะดูข้อมูลพรีแพรดาต้าก่อนลงตรวจจริง” อีกทั้งผู้ให้สัมภาษณ์คนที่ 6 กล่าวว่า “ต้องมีแผนหรือเช็คลิสต์ว่าจะต้องตรวจไรบ้างตามลำดับ หรือตรวจโครงการไหนก่อนหลัง” กรมบัญชีกลางและโมเดลของสมภพต่างก็เน้นว่า การวางแผนควรคำนึงถึงทรัพยากร เวลา และความซับซ้อนของระบบ

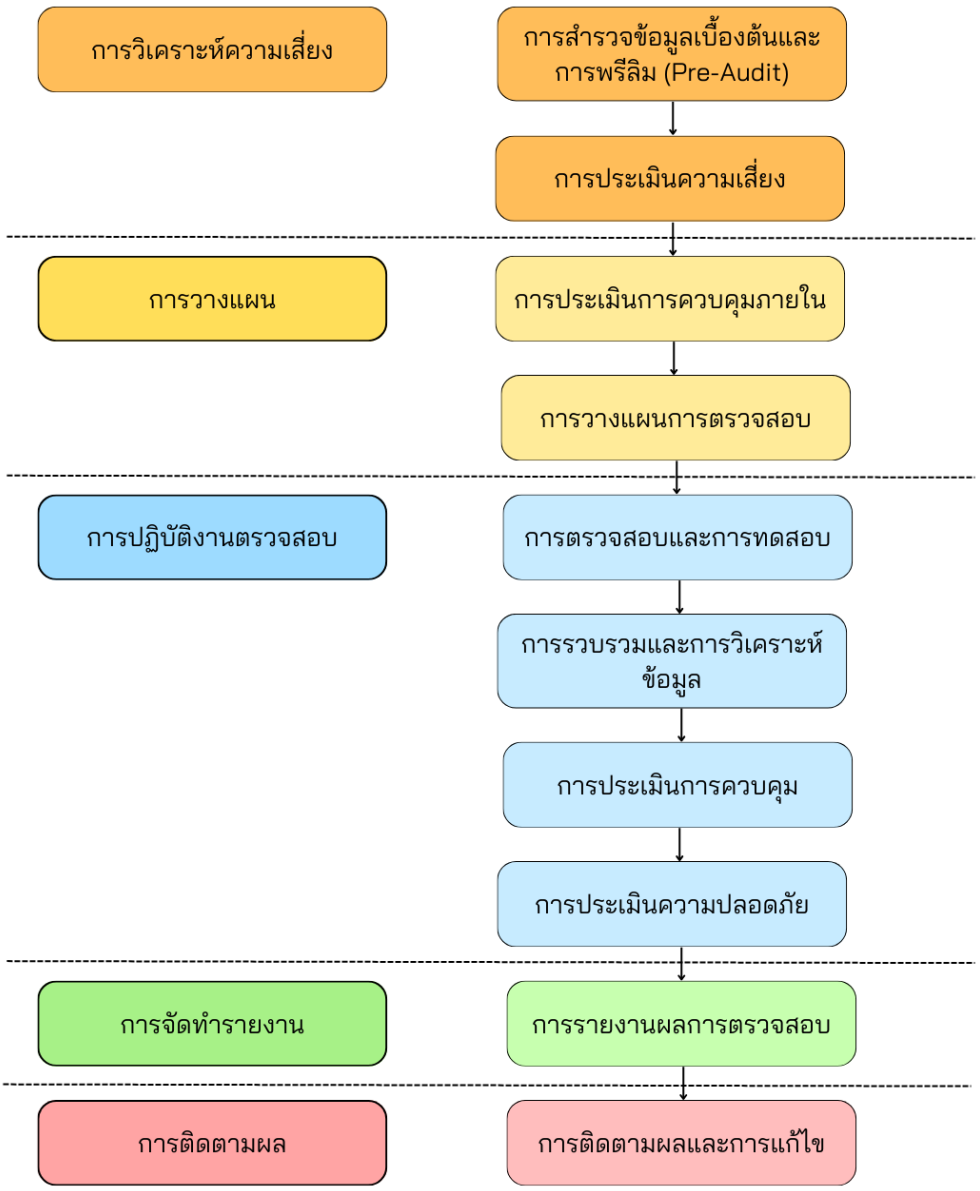
ขั้นตอนการวางแผน ประกอบด้วย 2 ขั้นตอน ดังนี้ (1) การประเมินการควบคุมภายใน และ (2) การวางแผนการตรวจสอบ โดยทฤษฎีของกรมบัญชีกลางได้ย้ำถึงการใช้ทรัพยากรบุคลากรงบประมาณ และเวลาต่าง ๆ อย่างมีประสิทธิภาพเพื่อให้การตรวจสอบสำเร็จลุล่วงไปด้วยดี

ขั้นตอนที่ 3 การปฏิบัติงานตรวจสอบ เมื่อการวางแผนเสร็จสมบูรณ์แล้ว ขั้นตอนถัดไปคือการดำเนินการตรวจสอบตามแผนงานที่วางไว้ให้ครบทุกขั้นตอน โดยจะต้องมีการรวบรวมหลักฐานที่เกี่ยวข้องและการประเมินการควบคุมภายใน รวมถึงการประเมินความปลอดภัยและข้อบกพร่องต่าง ๆ ที่อาจเกิดขึ้น แล้วทำการสรุปผลการตรวจสอบ ซึ่งผลของการตรวจสอบทำให้ระบุถึงข้อบกพร่องที่ตรวจพบ ข้อสังเกตต่าง ๆ สาเหตุของข้อบกพร่องนั้น ผลกระทบที่อาจเกิดขึ้น รวมถึงข้อเสนอแนะที่จะนำเสนอ ซึ่งได้รับการยืนยันจากแนวทางการตรวจสอบที่เกี่ยวข้อง เช่น กรมบัญชีกลาง ซึ่งแนะนำให้ผู้ตรวจสอบรวบรวมข้อมูลที่เกี่ยวข้องและดำเนินการประเมินความเสี่ยงที่อาจเกิดขึ้นระหว่างการตรวจสอบ โดยผู้ให้สัมภาษณ์คนที่ 1 กล่าวว่า “ดูข้อมูลพรีแพรดาต้าก่อนลงตรวจจริงว่ามีข้อมูลอะไรที่เกี่ยวข้องบ้าง เพื่อทำการเลือกสุ่มตัวอย่าง” ขณะที่ผู้ให้สัมภาษณ์คนที่ 4 ระบุว่า “แต่ถ้าเสริม ก่อนที่จะลงตรวจแต่ละครั้งอาจจะต้องวิเคราะห์เพิ่มเติมเพื่อตรวจสอบว่าความเสี่ยงของหน่วยงานนั้นมีการเปลี่ยนแปลงเพิ่มขึ้นหรือน้อยลงไหม”

โดยขั้นตอนการปฏิบัติงานตรวจสอบ ประกอบด้วย 4 ขั้นตอน ดังนี้ (1) การตรวจสอบและการทดสอบ (2) การรวบรวมและการวิเคราะห์ข้อมูล (3) การประเมินการควบคุม และ (4) การประเมินความปลอดภัย

ขั้นตอนที่ 4 การจัดทำรายงาน หลังจากดำเนินการตรวจสอบแล้ว ผู้ตรวจสอบจะบันทึกสิ่งที่ค้นพบ รวมถึงจุดอ่อน ช่องโหว่ หรือส่วนที่ไม่ปฏิบัติตามที่ระบุใด ๆ รวมถึงให้คำแนะนำเพื่อแก้ไขปัญหาเหล่านี้และปรับปรุงการกำกับดูแลด้านสารสนเทศและความปลอดภัย และจัดเตรียมรายงานการตรวจสอบโดยละเอียด เพื่อนำเสนอให้กับฝ่ายบริหาร ผู้มีส่วนได้ส่วนเสีย และหน่วยงานกำกับดูแลที่เกี่ยวข้อง นำไปใช้ในการตัดสินใจ โดยผู้ให้สัมภาษณ์คนที่ 1 กล่าวว่า “เป็นร่างรายงาน เพื่อนำประเด็นไปคอนเฟิร์มกับผู้รับตรวจ ว่าเราพบประเด็นอะไรบ้าง” อีกทั้ง ผู้ให้สัมภาษณ์คนที่ 6 กล่าวว่า “เขียนรายงาน แล้วก็สุดท้ายก็เป็นการติดตามผล” แนวคิดนี้สอดคล้องกับกรมบัญชีกลางที่ได้เสนอว่ารายงานต้องมีความถูกต้อง ชัดเจน และสร้างแรงจูงใจให้เกิดการแก้ไข

ขั้นตอนที่ 5 การติดตามผล การติดตามผลและการแก้ไข หลังจากดำเนินการตามการเปลี่ยนแปลงที่แนะนำ องค์กรอาจได้รับการตรวจสอบติดตามผลเพื่อประเมินว่ามีการดำเนินการแก้ไขหรือไม่ และแก้ไขปัญหาที่ระบุได้อย่างมีประสิทธิภาพหรือไม่ ขั้นตอนนี้ช่วยให้มั่นใจได้ถึงการปรับปรุงอย่างต่อเนื่องและการปฏิบัติตามคำแนะนำการตรวจสอบด้านสารสนเทศ โดยงานวิจัยจากกรมบัญชีกลางที่กล่าวถึงกระบวนการตรวจสอบภายใน 3 ขั้นตอน ได้แก่ การวางแผน การปฏิบัติงานตรวจสอบ และการจัดทำรายงานและติดตามผล โดยมีการเน้นย้ำถึงการใช้ทรัพยากรอย่างเหมาะสมและการติดตามผลอย่างมีประสิทธิภาพเพื่อให้การตรวจสอบประสบความสำเร็จ ซึ่งการติดตามผลเป็นขั้นตอนที่ผู้ให้สัมภาษณ์กล่าวถึงมากที่สุด โดยมองว่าเป็นจุดที่สะท้อนถึงความสำเร็จหรือความล้มเหลวของการตรวจสอบ โดยผู้ให้สัมภาษณ์คนที่ 1 กล่าวว่า “ใช้เวลาในการแก้ไขข้อตรวจพบนั้นนานเท่าไหร่ ใครเป็นผู้รับผิดชอบในการแก้ไข เพื่อนำไปสู่ขั้นตอนการติดตามผล” ขณะที่ผู้ให้สัมภาษณ์คนที่ 2 ย้ำว่า “ถ้าถามว่าอันไหนสำคัญ ก็คือ การติดตามผล”



ภาพที่ 4-1 โมเดลของแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศนั้นมุ่งเน้นไปที่กระบวนการที่มีขั้นตอนชัดเจนและการดำเนินงานที่มีความรัดกุม การวางแผนตรวจสอบ ถือเป็นจุดเริ่มต้นที่สำคัญ เนื่องจากการประเมินความเสี่ยง (Risk Assessment) อย่างละเอียดจะช่วยให้ทีมตรวจสอบสามารถเลือกเน้นตรวจสอบในหน่วยงานหรือระบบงานที่มีความเสี่ยงสูงสุด และลดการตรวจสอบในจุดที่มีความเสี่ยงต่ำหรือไม่สำคัญ นอกจากนี้ยังต้องพิจารณาถึงความสำคัญของทรัพยากร เช่น บุคลากรและเวลาที่ใช้ในการตรวจสอบเพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและบรรลุผลตาม

วัตถุประสงค์ที่ตั้งไว้ การพรีลิมหรือการทำความเข้าใจเบื้องต้นเกี่ยวกับงานที่ต้องตรวจก่อนลงมือจริงก็เป็นส่วนสำคัญที่จะช่วยเสริมความชัดเจนในการวางแผนและทำให้การดำเนินการในขั้นตอนถัดไปมีความมั่นใจมากขึ้น

ในระหว่างขั้นตอนการปฏิบัติงานตรวจสอบ ทีมตรวจสอบจะต้องทำการรวบรวมหลักฐาน ที่เกี่ยวข้อง เพื่อใช้ในการประเมินการปฏิบัติงานและการควบคุมภายในของหน่วยงาน โดยเฉพาะในกรณีที่มีการพิจารณาข้อบกพร่องหรือความเสี่ยงที่อาจมีผลกระทบต่อองค์กร การตรวจสอบนี้จะต้องพิจารณาถึงมาตรฐานการดำเนินงานที่กำหนดไว้และระเบียบปฏิบัติขององค์กร รวมทั้งกฎหมายหรือข้อบังคับที่เกี่ยวข้องเพื่อให้มั่นใจว่าการดำเนินงานนั้นไม่ละเมิดข้อกำหนดหรือสร้างความเสี่ยงด้านการปฏิบัติงานที่อาจส่งผลกระทบในระยะยาว

หลังจากการตรวจสอบเสร็จสิ้นแล้ว การจัดทำรายงานผลการตรวจสอบเป็นกระบวนการที่สำคัญมาก รายงานที่ดีควรมีคุณสมบัติที่ชัดเจน ถูกต้อง และมีการอธิบายผลการตรวจสอบอย่างกระชับเพื่อให้ผู้บริหารสามารถเข้าใจได้ง่ายและนำไปใช้ในการตัดสินใจ การสรุปข้อบกพร่องและการเสนอแนะในการแก้ไขควรเป็นไปอย่างสร้างสรรค์และเป็นประโยชน์ โดยเฉพาะเมื่อพิจารณาถึงการติดตามผลหลังจากที่มีการเสนอแนะการแก้ไขไปแล้ว การติดตามผลจะช่วยให้มั่นใจว่าองค์กรหรือหน่วยงานที่ถูกตรวจสอบได้ดำเนินการตามข้อเสนอแนะอย่างมีประสิทธิภาพ และหากพบอุปสรรคในการดำเนินการ ก็สามารถปรับปรุงหรือขอระยะเวลาเพิ่มเติมได้

ในเชิงปฏิบัติการจากการสัมภาษณ์ พบว่า หลายองค์กรเน้นย้ำถึงความสำคัญของการติดตามผลอย่างต่อเนื่อง ซึ่งมีบทบาทในการยืนยันว่าองค์กรไม่เพียงแค่รับรู้ข้อบกพร่องเท่านั้น แต่ยังสามารถดำเนินการแก้ไขได้อย่างมีประสิทธิภาพและทันเวลาตามกรอบที่กำหนด นอกจากนี้ การสุ่มตัวอย่างข้อมูลและการตรวจสอบตัวอย่างข้อมูลอย่างรอบคอบ เป็นขั้นตอนที่ช่วยลดข้อผิดพลาดและทำให้การตรวจสอบสามารถเจาะลึกไปในจุดสำคัญได้อย่างตรงจุด การมีแผนการตรวจสอบที่เหมาะสมและเช็คลิสต์ที่ชัดเจนทำให้การตรวจสอบสามารถครอบคลุมและไม่ละเลยประเด็นที่สำคัญ

โดยสรุปแล้ว แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศนั้นไม่เพียงแค่เป็นกระบวนการที่มีขั้นตอนที่ชัดเจน แต่ยังต้องมีการประเมินความเสี่ยงที่เหมาะสม วางแผนการตรวจสอบที่แม่นยำ และต้องมีการติดตามผลอย่างต่อเนื่องเพื่อให้การตรวจสอบมีความโปร่งใสและมีประสิทธิภาพสูงสุด ทั้งนี้ทุกขั้นตอนต้องได้รับการประสานงานและสื่อสารกันอย่างดีระหว่างผู้

ตรวจสอบและหน่วยงานที่ถูกตรวจสอบเพื่อให้การดำเนินการเป็นไปตามแผนและผลที่ได้เป็นที่ยอมรับในทุกฝ่าย

4.11 ตัวอย่างการนำแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศประยุกต์ใช้กับการตรวจสอบระบบฐานข้อมูล

ขั้นตอนที่ 1 การวิเคราะห์ความเสี่ยง (Risk Assessment) ประกอบด้วย 2 ขั้นตอน ดังนี้

(1) การสำรวจข้อมูลเบื้องต้นและการพรีลิม (Pre-Audit)

(1.1) ทำการศึกษาเอกสารประกอบระบบ เช่น โครงสร้างฐานข้อมูล (Database Schema) แผนผังระบบ (System Architecture Diagram) นโยบายความปลอดภัยสารสนเทศ (IT Security Policy) และคู่มือการสำรองข้อมูล (Backup and Recovery Procedure) เป็นต้น

(1.2) สัมภาษณ์ผู้ดูแลระบบฐานข้อมูล (DBA) และผู้ใช้งานหลัก เพื่อทำความเข้าใจว่า มีใครเข้าถึงฐานข้อมูลบ้าง ข้อมูลประเภทใดจัดเป็นข้อมูลสำคัญ (Critical Data) และระบบมีมาตรการป้องกันข้อมูลรั่วไหลหรือไม่

(2) การประเมินความเสี่ยง

(2.1) ประเมินความเสี่ยงตามองค์ประกอบ CIA Triad ได้แก่

(2.1.1) สิทธิ์การเข้าถึงข้อมูลและการป้องกันข้อมูลรั่วไหล (Confidentiality)

(2.1.2) ความถูกต้องของข้อมูล (Integrity) เช่น การป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น

(2.1.3) ความสามารถในการเข้าถึงข้อมูลได้ตามต้องการ (Availability)

(2.2) จัดทำตารางวิเคราะห์ความเสี่ยง (Risk Matrix) เพื่อแสดงโอกาสเกิด (Likelihood) × ผลกระทบ (Impact) เช่น “การสำรองข้อมูลไม่สมบูรณ์” ให้เป็นความเสี่ยงระดับสูง พร้อมระบุความเสี่ยงที่ต้องได้รับการตรวจสอบเป็นลำดับแรก เป็นต้น

โดยผลลัพธ์ที่ได้จากการวิเคราะห์ความเสี่ยง (Risk Assessment) คือ รายการความเสี่ยงสำคัญ (Key Risks) เอกสารสรุปตารางวิเคราะห์ความเสี่ยง (Risk Matrix) พร้อมระดับความรุนแรงและแนวทางเบื้องต้นในการลดความเสี่ยง

ขั้นตอนที่ 2 การวางแผน ประกอบด้วย 2 ขั้นตอน ดังนี้

(1) การประเมินการควบคุมภายใน

(1.1) ศึกษามาตรการควบคุมในระบบฐานข้อมูล เช่น การกำหนดสิทธิ์ผู้ใช้ (User Privileges) การจัดเก็บรหัสผ่าน (Password Management) การเข้ารหัสข้อมูล (Data Encryption) และการบันทึกกิจกรรม (Audit Trail / Log Management) เป็นต้น

(1.2) ตรวจสอบการปฏิบัติตามนโยบาย เช่น Password Policy สอดคล้องกับมาตรฐาน ISO/IEC 27001 หรือไม่ และมีการสำรองข้อมูลอัตโนมัติหรือไม่ เป็นต้น

(2) การวางแผนการตรวจสอบ

(2.1) ระบุขอบเขต (Scope) เช่น ตรวจสอบเฉพาะฐานข้อมูล Oracle ของระบบ ERP เป็นต้น

(2.2) กำหนดวัตถุประสงค์ (Objective) เช่น ตรวจสอบการควบคุมสิทธิ์ผู้ใช้ เป็นต้น

(2.3) กำหนดเครื่องมือที่จะใช้ เช่น SQL Query สำหรับดึงข้อมูลผู้ใช้ และ Database Security Scanner เป็นต้น

(2.4) จัดทำตารางแผนตรวจสอบ (Audit Program)

ตารางที่ 4-1 ตารางตัวอย่างตารางแผนตรวจสอบ (Audit Program)

ลำดับ	กิจกรรมการตรวจสอบ	วิธีการตรวจสอบ	ผู้รับผิดชอบ	ระยะเวลา
1	ตรวจสอบสิทธิ์ผู้ใช้	ใช้ SQL ดึงข้อมูลจาก SYS.USER	ผู้ตรวจสอบ	1 วัน
2	ตรวจสอบ Log การเข้าถึง	วิเคราะห์ Audit Trail	ผู้ตรวจสอบ	2 วัน

โดยผลลัพธ์ที่ได้จากขั้นตอนการวางแผน คือ เอกสารแผนการตรวจสอบฐานข้อมูล (Database Audit Plan) รายการควบคุมที่ต้องตรวจสอบ และตารางกิจกรรมและระยะเวลาดำเนินงาน

ขั้นตอนที่ 3 การปฏิบัติงานตรวจสอบ ประกอบด้วย 4 ขั้นตอน ดังนี้

(1) การตรวจสอบและการทดสอบ

(1.1) ทดสอบการควบคุมการเข้าถึง (Access Control Testing) โดยการตรวจสอบสิทธิ์ (Permissions) ของผู้ใช้งานและผู้ดูแลระบบ (DBA) โดยเฉพาะสิทธิ์ระดับสูง (Superuser) เพื่อให้มั่นใจว่าเป็นไปตามหลักการ Need-to-Know ตรวจสอบผ่าน System Tables/Views ใน DBMS

(1.2) ทดสอบความปลอดภัยของการกำหนดค่า (Configuration Security Testing) โดยการตรวจสอบการตั้งค่า DBMS เช่น การกำหนดค่าพารามิเตอร์ความปลอดภัย นโยบายรหัสผ่าน และการปิดบริการที่ไม่จำเป็น

(1.3) ทดสอบกระบวนการสำรองและกู้คืนข้อมูล โดยจำลองสถานการณ์ข้อมูลเสียหาย

(1.4) ตรวจสอบว่า Account ที่ไม่ได้ใช้งานนานเกิน 90 วันถูกระงับหรือไม่

(2) การรวบรวมและการวิเคราะห์ข้อมูล

(2.1) รวบรวมหลักฐาน (Evidence) เช่น บันทึกกิจกรรมการเข้าถึงหรือเปลี่ยนแปลงข้อมูล (Audit Logs/Trail) รายงานการตั้งค่าความปลอดภัย และผลลัพธ์จากการรัน SQL Query เพื่อตรวจสอบสิทธิ์

(2.2) วิเคราะห์ Log เพื่อค้นหากิจกรรมที่น่าสงสัย หรือการเข้าถึงและเปลี่ยนแปลงที่ไม่ได้รับอนุญาต

(3) การประเมินการควบคุม

(3.1) ทดสอบประสิทธิภาพ (Operating Effectiveness Test) โดยทดสอบว่าการควบคุมที่ระบุไว้ในขั้นตอนที่ 2 ทำงานได้อย่างมีประสิทธิผล ตลอดระยะเวลาที่ตรวจสอบ เช่น ตรวจสอบบันทึกการสำรองข้อมูล เพื่อดูว่าการสำรองข้อมูลเป็นไปตามกำหนดเวลาอย่างสม่ำเสมอ เป็นต้น

(3.2) ประเมินว่า การจำกัดสิทธิ์ผู้ใช้งานสอดคล้องกับหลัก Least Privilege หรือไม่

(3.3) ประเมินผลว่า การควบคุมมีประสิทธิภาพในการลดความเสี่ยงหรือไม่

(4) การประเมินความปลอดภัย

(4.1) ตรวจสอบมาตรการ การเข้ารหัสข้อมูล (Encryption) ทั้งข้อมูลที่จัดเก็บ (Data at Rest) และข้อมูลที่ส่งผ่านเครือข่าย (Data in Transit)

(4.2) ตรวจสอบ Patch Version การป้องกันการโจมตี และช่องโหว่ที่ยังไม่ได้รับการแก้ไข

โดยผลลัพธ์ที่ได้จากการปฏิบัติงานตรวจสอบ คือ หลักฐานการตรวจสอบ (Audit Evidence) รายการข้อบกพร่องและจุดควบคุมที่อ่อนแอ และรายงานเบื้องต้น (Preliminary Audit Findings)

ขั้นตอนที่ 4 การจัดทำรายงาน

(1.1) สรุปผลการตรวจสอบในรูปแบบรายงาน โดยมีส่วนประกอบหลัก ได้แก่

(1.1.1) บทสรุปผู้บริหาร (Executive Summary) โดยสรุปภาพรวมของการตรวจสอบ

(1.1.2) วัตถุประสงค์และขอบเขตการตรวจสอบ

(1.1.3) วิธีการตรวจสอบ

(1.1.4) ผลการตรวจสอบและข้อบกพร่อง

(1.1.5) ข้อเสนอแนะในการปรับปรุง เช่น ควรกำหนดนโยบายการเปลี่ยนรหัสผ่านทุก 90 วัน และควรเปิดใช้งาน Database Auditing สำหรับกิจกรรมของผู้ดูแลระบบ

(1.2) นำเสนอผลต่อผู้บริหารและผู้รับผิดชอบ

โดยผลลัพธ์ที่ได้จากการจัดทำรายงาน คือ รายงานผลการตรวจสอบ (Database Audit Report) และเอกสารสรุปข้อบกพร่องและแนวทางแก้ไข

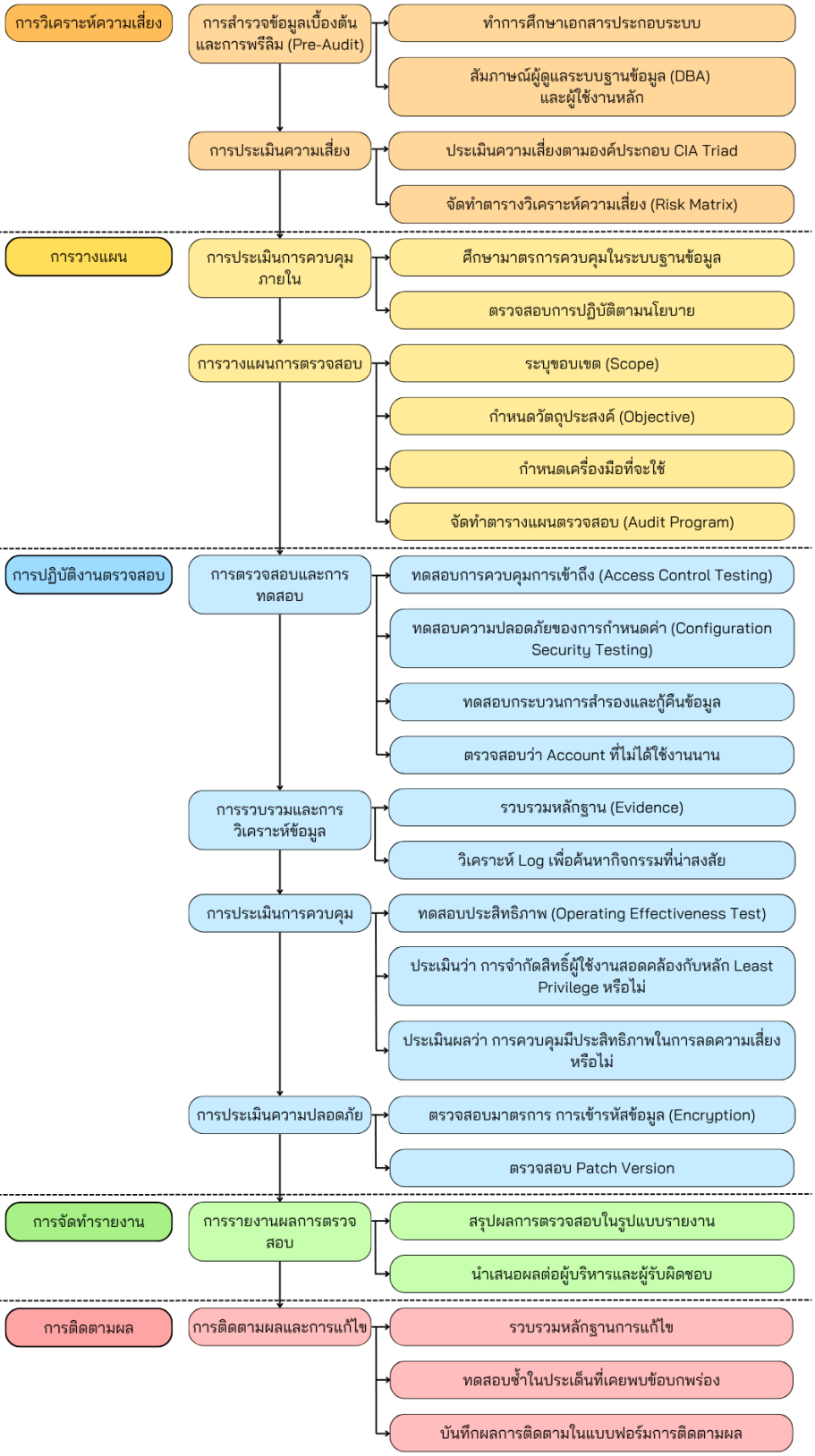
ขั้นตอนที่ 5 การติดตามผล

(1.1) รวบรวมหลักฐานการแก้ไข เช่น นโยบายความปลอดภัยฉบับใหม่ หลักฐานการอัปเดต Patch และ Log การปรับปรุงสิทธิ์ผู้ใช้ เป็นต้น

(1.2) ทดสอบซ้ำในประเด็นที่เคยพบข้อบกพร่อง เพื่อตรวจสอบว่าได้ดำเนินการแก้ไขข้อบกพร่องที่พบภายในกรอบเวลาที่กำหนดแล้วหรือยัง และเพื่อยืนยันว่าข้อบกพร่องได้รับการแก้ไขอย่างมีประสิทธิภาพและไม่ก่อให้เกิดปัญหาใหม่ เช่น เดิมมีผู้ใช้ที่ไม่ได้ล็อกอินเกิน 90 วัน ตรวจสอบใหม่ว่าระบบได้ระงับบัญชีแล้วหรือไม่ เป็นต้น

(1.3) บันทึกผลการติดตามในแบบฟอร์มการติดตามผล

โดยผลลัพธ์ที่ได้จากการติดตามผล คือ รายงานการติดตามผล และสรุปสถานะการแก้ไข เช่น แก้ไขแล้วเสร็จ อยู่ระหว่างดำเนินการ หรือยังไม่ดำเนินการ



ภาพที่ 4-2 โมเดลตัวอย่างการนำแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศประยุกต์ใช้กับการตรวจสอบระบบฐานข้อมูล

บทที่ 5

สรุปผล อภิปรายผล และข้อเสนอแนะ

จากการศึกษาเรื่อง “แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ” มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และนำเสนอแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยใช้วิธีการวิจัยในรูปแบบการวิจัยเชิงคุณภาพ (Quantitative Research) โดยรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศในประเทศไทย จำนวน 6 คน สามารถสรุปผลวิจัย อภิปรายผล และนำเสนอข้อเสนอแนะ ได้ดังนี้

5.1 สรุปผลการวิจัย

5.2 อภิปรายผลการวิจัย

5.3 ข้อจำกัดงานวิจัย

5.4 ข้อเสนอแนะ

5.1 สรุปผลการวิจัย

จากการสัมภาษณ์เชิงลึกกับผู้ให้สัมภาษณ์ทั้ง 6 คน สามารถสรุปผลการวิจัยได้ดังนี้

5.1.1) ข้อมูลทั่วไปของผู้ให้สัมภาษณ์ ผู้ให้สัมภาษณ์ทั้ง 6 คน เป็นผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ และผู้ตรวจสอบภายในที่มีประสบการณ์การตรวจสอบด้านเทคโนโลยีสารสนเทศในประเทศไทย ที่มีประสบการณ์การทำงานตั้งแต่ 2-15 ปี ซึ่งจะเห็นได้ว่า ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศไม่มีใบประกาศนียบัตรด้านการตรวจสอบด้านเทคโนโลยีสารสนเทศ แต่บางคนมีใบประกาศนียบัตรด้านอื่นๆที่เกี่ยวข้องกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ และองค์กรที่ผู้ให้สัมภาษณ์ปฏิบัติงานอยู่ มีความแตกต่างกันบ้างในด้านโครงสร้างขององค์กร แต่จะเห็นได้ว่า ความคิดเห็นของทุกคนมีความคิดเห็นเป็นไปในทางเดียวกัน

5.1.2) ปัจจัยความเป็นอิสระของผู้ตรวจสอบถือเป็นปัจจัยสำคัญที่ส่งผลโดยตรงต่อการดำเนินงานในการตรวจสอบ หากผู้ตรวจสอบไม่สามารถทำงานได้อย่างอิสระ ความคิดเห็นและการ

วิเคราะห์จะถูกบิดเบือนหรือไม่ตรงไปตรงมา ซึ่งอาจส่งผลต่อความน่าเชื่อถือและผลลัพธ์ของการตรวจสอบ ดังที่ผู้ให้สัมภาษณ์บางคนกล่าวถึงว่า ถ้าผู้ตรวจสอบไม่ได้รับความอิสระในการดำเนินงาน ความเสี่ยงในการตรวจสอบอาจไม่สะท้อนความเป็นจริง และผลการตรวจสอบอาจเบี่ยงเบนไปจากข้อเท็จจริง

5.1.3) ปัจจัยด้านความรู้ความสามารถของผู้ตรวจสอบเป็นสิ่งที่สำคัญ เพราะการตรวจสอบด้านเทคโนโลยีสารสนเทศต้องใช้ความเข้าใจในหลายด้าน ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ความเสี่ยง และกระบวนการต่าง ๆ หากผู้ตรวจสอบไม่มีความรู้และทักษะพื้นฐานจะทำให้การตรวจสอบมีข้อผิดพลาดได้ นอกจากนี้ประสบการณ์ในการทำงานและการรู้จักเครื่องมือที่ใช้ในการตรวจสอบก็มีความสำคัญ

5.1.4) ปัจจัยด้านวุฒิภาวะ ทักษะ และประสบการณ์ของผู้ตรวจสอบ การมีประสบการณ์ในการทำงานจะช่วยให้ผู้ตรวจสอบสามารถวิเคราะห์สถานการณ์และปัญหาต่าง ๆ ได้ดียิ่งขึ้น และสามารถแก้ไขปัญหาหรือประเด็นต่าง ๆ ได้อย่างมีประสิทธิภาพ นอกจากนี้ทักษะในการเจรจาและการสื่อสารก็มีความสำคัญในการทำงานร่วมกับผู้ถูกตรวจสอบ โดยเฉพาะในกรณีที่ผู้ถูกตรวจสอบมีความเชี่ยวชาญมากกว่าหรือมีตำแหน่งสูงกว่า

5.1.5) ปัจจัยด้านจรรยาบรรณและจริยธรรมเป็นสิ่งที่สำคัญมากในการทำงานตรวจสอบ โดยเฉพาะเมื่อผู้ตรวจสอบมีการเข้าถึงข้อมูลที่เป็นความลับขององค์กร การปกป้องข้อมูลและรักษาความเป็นกลางในการตัดสินเป็นสิ่งที่ไม่สามารถละเลยได้ การปฏิบัติตามจรรยาบรรณอย่างเคร่งครัดช่วยให้ผลการตรวจสอบมีความน่าเชื่อถือและไม่เกิดการเผยแพร่ข้อมูลที่อาจก่อให้เกิดผลเสียต่อองค์กร

5.1.6) ปัจจัยด้านมาตรฐานการตรวจสอบ การยึดตามมาตรฐานการตรวจสอบที่ชัดเจนและถูกต้องเป็นสิ่งที่สำคัญในการปฏิบัติงานตรวจสอบ หากไม่ปฏิบัติตามมาตรฐานอาจส่งผลให้ผลการตรวจสอบผิดพลาด หรือไม่สามารถอ้างอิงกับมาตรฐานหรือกฎหมายที่เกี่ยวข้องได้ ซึ่งอาจส่งผลเสียต่อองค์กรได้ การใช้มาตรฐานการตรวจสอบที่ทันสมัยและได้รับการปรับปรุงอย่างสม่ำเสมอช่วยให้ผู้ตรวจสอบสามารถประเมินสถานการณ์ได้อย่างถูกต้อง

5.2.7) ปัจจัยการสนับสนุนจากผู้บริหาร การได้รับการสนับสนุนจากผู้บริหารมีผลอย่างมากต่อการดำเนินงานของผู้ตรวจสอบ หากผู้บริหารไม่เข้าใจหรือไม่สนับสนุนกระบวนการตรวจสอบ ผู้ตรวจสอบอาจได้รับข้อมูลที่ไม่ครบถ้วนหรือไม่ได้รับความร่วมมือ ซึ่งอาจส่งผลให้การตรวจสอบไม่

สามารถดำเนินการได้อย่างราบรื่น การสนับสนุนจากผู้บริหารจะช่วยให้การทำงานมีประสิทธิภาพมากขึ้น และผู้ตรวจสอบสามารถทำงานได้ตามแผน

5.2.8) ปัจจัยด้านการวางแผนการตรวจสอบเป็นสิ่งสำคัญที่ช่วยให้การตรวจสอบมีเป้าหมายและทิศทางที่ชัดเจน การวางแผนที่ดีจะช่วยให้ผู้ตรวจสอบสามารถเลือกตรวจสอบส่วนที่มีความเสี่ยงสูงและมีความสำคัญสำหรับองค์กร การประเมินความเสี่ยงและการจัดลำดับความสำคัญในการตรวจสอบเป็นปัจจัยที่ช่วยเพิ่มประสิทธิภาพในการตรวจสอบ

5.2.9) ปัจจัยด้านการวิเคราะห์ความเสี่ยง การวิเคราะห์ความเสี่ยงช่วยให้ผู้ตรวจสอบสามารถเลือกตรวจสอบหน่วยงานหรือระบบที่มีความเสี่ยงสูงได้ และลดความเสี่ยงที่ไม่จำเป็น การประเมินความเสี่ยงอย่างถูกต้องช่วยให้การตรวจสอบมีความหมายและสามารถนำไปสู่การพัฒนาหรือแก้ไขปัญหาได้อย่างตรงจุด

ในภาพรวม ผลการสัมภาษณ์ทั้งหมดแสดงให้เห็นว่าหลายปัจจัยมีผลกระทบต่อความสำเร็จในการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยเฉพาะความเป็นอิสระ ความรู้ความสามารถของผู้ตรวจสอบ และการได้รับการสนับสนุนจากผู้บริหาร ซึ่งถือเป็นสิ่งสำคัญในการทำให้การตรวจสอบเป็นไปได้อย่างมีประสิทธิภาพและตรงไปตรงมา

5.2.10) แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

ผลการวิจัยนี้ได้เสนอแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยการเพิ่มขั้นตอนสำคัญในกระบวนการตรวจสอบที่แตกต่างจากแนวทางเดิมที่กรมบัญชีกลางได้กำหนดไว้ ซึ่งมีการพัฒนาหลักการที่สำคัญคือ การวิเคราะห์ความเสี่ยงก่อนการดำเนินการตรวจสอบจริง และการติดตามผลหลังการตรวจสอบ เพื่อให้มั่นใจว่าองค์กรดำเนินการแก้ไขข้อบกพร่องที่พบได้อย่างมีประสิทธิภาพ

ในกระบวนการวางแผนการตรวจสอบ แนวทางที่กรมบัญชีกลางเน้นการกำหนดขอบเขตและทรัพยากรที่ใช้ในการตรวจสอบอย่างเหมาะสม แต่ผลการวิจัยพบว่า การวิเคราะห์ความเสี่ยงในระยะแรกช่วยให้สามารถจัดลำดับความสำคัญในการตรวจสอบได้ชัดเจน โดยเฉพาะในการเลือกองค์กรที่มีความเสี่ยงสูงมาเป็นลำดับแรก การเพิ่มการวิเคราะห์ความเสี่ยงนี้ทำให้กระบวนการตรวจสอบมีความแม่นยำและสอดคล้องกับความเสี่ยงที่แท้จริงขององค์กร

ในด้านการปฏิบัติงานตรวจสอบ แนวทางเดิมมุ่งเน้นการรวบรวมข้อมูลและการประเมินผลตามระเบียบและนโยบายขององค์กร แต่การวิจัยนี้ได้เพิ่มขั้นตอนของการประเมินความปลอดภัย และ

การประเมินการควบคุมอย่างต่อเนื่อง ซึ่งช่วยให้สามารถระบุปัญหาที่เกิดขึ้นระหว่างการตรวจสอบได้ทันท่วงที และสามารถป้องกันข้อบกพร่องที่อาจจะเกิดขึ้นในอนาคต

ในส่วนของการจัดทำรายงานและการติดตามผล จากการวิจัยพบว่า การติดตามผลหลังการตรวจสอบเป็นขั้นตอนสำคัญที่ไม่เพียงแค่การเสนอรายงานการตรวจสอบไปยังผู้บริหาร แต่ยังต้องติดตามว่าผู้รับการตรวจสอบได้นำข้อเสนอแนะไปปฏิบัติตามหรือไม่ ซึ่งช่วยให้การแก้ไขข้อบกพร่องเป็นไปอย่างมีประสิทธิภาพและต่อเนื่อง

เมื่อเปรียบเทียบกับงานวิจัยที่มีอยู่ แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศที่ได้จากการวิจัยนี้มีความแตกต่างจากแนวทางเดิม โดยเฉพาะในเรื่องการ วิเคราะห์ความเสี่ยง และ การติดตามผล ซึ่งถือเป็นการพัฒนาใหม่ที่ช่วยเพิ่มประสิทธิภาพในการตรวจสอบ ทั้งในการวางแผน ตรวจสอบ และการติดตามผลการแก้ไขข้อบกพร่อง

โดยรวมแล้ว ผลการวิจัยนี้ได้เสนอแนวทางที่ช่วยให้การตรวจสอบด้านเทคโนโลยีสารสนเทศมีความแม่นยำและมีประสิทธิภาพมากยิ่งขึ้น สามารถป้องกันปัญหาที่อาจเกิดขึ้นในอนาคตได้ดีกว่าแนวทางเดิม และช่วยให้องค์กรสามารถบริหารความเสี่ยงได้อย่างมีระบบและต่อเนื่อง

5.2 อภิปรายผลการวิจัย

ผลการวิจัยสะท้อนให้เห็นว่าการตรวจสอบด้านเทคโนโลยีสารสนเทศมีความซับซ้อนและต้องอาศัยปัจจัยเกื้อหนุนหลายด้าน ทั้งปัจจัยที่เกี่ยวข้องกับตัวผู้ตรวจสอบเอง มาตรฐานการตรวจสอบ และบริบทขององค์กร โดยเมื่อพิจารณาเชิงบูรณาการกับทฤษฎีและงานศึกษาที่ผ่านมา พบว่าองค์ประกอบเหล่านี้ล้วนส่งผลโดยตรงต่อคุณภาพและประสิทธิภาพของการตรวจสอบ

ประการแรก ความเป็นอิสระของผู้ตรวจสอบ ถือเป็นรากฐานสำคัญที่ทำให้ผลการตรวจสอบมีความน่าเชื่อถือ ผู้ให้สัมภาษณ์เกือบทั้งหมดเน้นย้ำว่า หากผู้ตรวจสอบขาดอิสระ ไม่สามารถแยกการปฏิบัติงานออกจากอิทธิพลของฝ่ายบริหารหรือผู้ถูกตรวจสอบได้ ผลการตรวจสอบย่อมมีโอกาสบิดเบือนและไม่สะท้อนความเสี่ยงที่แท้จริง ซึ่งสอดคล้องกับ ISACA (2014) และ Havelka & Merhout (2013) ที่ชี้ว่า ความเป็นอิสระทำให้ผู้ตรวจสอบสามารถรายงานข้อเท็จจริงอย่างตรงไปตรงมา อย่างไรก็ตาม ผลการศึกษาในอดีต เช่น ชัชพงศ์ อธิปัญญาวงศ์ (2559) พบว่าความเป็นอิสระอาจไม่ได้ส่งผลต่อประสิทธิภาพเสมอไป แต่ขึ้นกับโครงสร้างและขนาดขององค์กร ซึ่งก็ตรงกับคำ

ให้สัมภาษณ์ที่สะท้อนว่า องค์กรที่ไม่มีสายบังคับบัญชาที่แยกออกจากฝ่ายปฏิบัติจริง ๆ ย่อมทำให้ความอิสระถูกจำกัดและส่งผลต่อคุณภาพงานตรวจสอบ

ประการถัดมา ความรู้ความสามารถด้านเทคโนโลยีของผู้ตรวจสอบ เป็นอีกปัจจัยที่ได้รับการยืนยันจากทั้งข้อมูลเชิงประจักษ์และทฤษฎี ผู้ให้สัมภาษณ์หลายรายกล่าวว่า การตรวจสอบ IT จำเป็นต้องอาศัยความรู้ทั้งด้านฮาร์ดแวร์ ซอฟต์แวร์ การควบคุมความเสี่ยง และการบริหาร IT Service หากผู้ตรวจสอบขาดทักษะเหล่านี้ การประเมินความเสี่ยงและการออกข้อเสนอแนะย่อมไม่ถูกต้อง ตรงกับงานของ Havelka & Merhout (2013) ที่เน้นระดับความรู้เทคโนโลยีและกระบวนการทางธุรกิจเป็นปัจจัยหลักต่อคุณภาพงานตรวจสอบ แม้งานวิจัยของ ชัชพงศ์ (2559) จะโต้แย้งว่าความรู้เพียงอย่างเดียวไม่เพียงพอหากปราศจากประสบการณ์และวิจารณญาณ แต่ก็ไม่อาจปฏิเสธได้ว่าความรู้คือพื้นฐานที่ขาดไม่ได้

นอกจากความรู้แล้ว วุฒิภาวะ ทักษะ และประสบการณ์ ก็เป็นตัวแปรที่ทำให้ผู้ตรวจสอบสามารถประยุกต์ความรู้ไปสู่การปฏิบัติจริงได้อย่างมีประสิทธิภาพ ข้อมูลจากการสัมภาษณ์สะท้อนว่าผู้ตรวจสอบที่มีประสบการณ์มากสามารถระบุปัญหาได้ตรงจุด และใช้ทักษะการสื่อสารเพื่อสร้างความร่วมมือจากผู้รับตรวจได้ดีกว่า ซึ่งสอดคล้องกับการศึกษาของ Usman (2016) ที่ระบุว่า ประสบการณ์ช่วยให้ผู้ตรวจสอบมีความเชี่ยวชาญในการสังเกตและการตัดสินใจ อีกทั้งยังช่วยเสริมสร้างความน่าเชื่อถือเมื่อต้องอธิบายผลการตรวจต่อผู้บริหารหรือบุคลากรที่มีความเชี่ยวชาญสูงในสายงานเทคนิค

ต่อมา จรรยาบรรณและจริยธรรมของผู้ตรวจสอบ เป็นปัจจัยที่ทุกผู้ให้สัมภาษณ์เห็นตรงกันว่าไม่อาจมองข้าม เพราะงานตรวจสอบ IT มักเกี่ยวข้องกับข้อมูลที่มีความอ่อนไหวและเป็นความลับขององค์กร หากขาดจรรยาบรรณอาจนำไปสู่การรั่วไหลของข้อมูลหรือการถูกร้องเรียนว่าขาดความเป็นธรรม งานวิจัยในอดีตต่างยืนยันว่าการคงไว้ซึ่งความเป็นกลาง โปร่งใส และการรักษาความลับเป็นหัวใจสำคัญในการสร้างความไว้วางใจต่อผู้ตรวจสอบ

มาตรฐานการตรวจสอบ ก็มีบทบาทเชิงระบบที่ช่วยกำหนดกรอบและหลักเกณฑ์ที่ชัดเจน ผู้ให้สัมภาษณ์ย้ำว่า การยึดมั่นในมาตรฐาน เช่น ISACA, ISO/IEC 27001 และมาตรฐานภายในประเทศ ช่วยลดข้อผิดพลาดและทำให้การปฏิบัติสอดคล้องกับข้อกำหนดด้านกฎหมาย ซึ่งสอดคล้องกับทฤษฎีที่ว่ามาตรฐานการตรวจสอบทำหน้าที่เป็น “benchmark” ให้ผู้ตรวจสอบสามารถอ้างอิงได้เมื่อมีข้อโต้แย้ง

อีกประเด็นคือ การสนับสนุนจากผู้บริหาร ผู้ให้สัมภาษณ์หลายรายสะท้อนตรงกันว่า หากผู้บริหารไม่เข้าใจหรือไม่เห็นความสำคัญของงานตรวจสอบ จะทำให้ผู้ตรวจสอบไม่ได้รับความร่วมมือและข้อมูลที่จำเป็น งานวิจัยด้าน Internal Control ที่เน้นบทบาทของผู้บริหารระดับสูงที่กำหนดทิศทางและสนับสนุนให้เกิดการควบคุมที่มีประสิทธิภาพ

ขณะเดียวกัน การวางแผนตรวจสอบและการวิเคราะห์ความเสี่ยง ก็เป็นกลไกสำคัญที่ช่วยเพิ่มคุณค่าของงานตรวจสอบ ผู้ให้สัมภาษณ์ยืนยันว่า หากไม่มีการวิเคราะห์ความเสี่ยงที่ครอบคลุม ผู้ตรวจสอบอาจเสียเวลาไปกับการตรวจสอบเรื่องที่ไม่สำคัญ และไม่สามารถสร้างคุณค่าเชิงกลยุทธ์ให้แก่องค์กรได้ ซึ่งสอดคล้องกับงานวิจัยที่ชี้ว่าการประเมินความเสี่ยงที่แม่นยำช่วยให้สามารถจัดลำดับความสำคัญและใช้ทรัพยากรตรวจสอบได้อย่างคุ้มค่า

นอกเหนือจากปัจจัยทั้งแปดแล้ว การวิจัยยังชี้ให้เห็น แนวทางปฏิบัติที่ดีในการตรวจสอบ IT ซึ่งประกอบด้วยการประเมินความเสี่ยง การสร้าง Audit Universe การวางแผน การตรวจสอบภาคสนาม การจัดทำรายงาน และการติดตามผล ผู้ให้สัมภาษณ์บางรายเน้นย้ำถึงขั้นตอนเสริม เช่น การเตรียมข้อมูลล่วงหน้า (Pre-preparation) และการวิเคราะห์การเปลี่ยนแปลงของความเสี่ยงก่อนลงพื้นที่จริง ซึ่งช่วยเพิ่มประสิทธิภาพและความแม่นยำของกระบวนการตรวจสอบ กระบวนการเหล่านี้สอดคล้องกับ ISACA (2014) ที่มุ่งให้การตรวจสอบมีความเป็นระบบ ครบถ้วน และสามารถสร้างคุณค่าจริงต่อองค์กร

กล่าวโดยสรุป งานวิจัยนี้สะท้อนว่าการตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีคุณภาพเกิดจากการผสมผสานของ คุณสมบัติและทักษะส่วนบุคคลของผู้ตรวจสอบ, การใช้มาตรฐานและกรอบการตรวจสอบที่ยอมรับในระดับสากล, การสนับสนุนจากผู้บริหารและบริบทองค์กร, ตลอดจน การยึดมั่นในแนวทางปฏิบัติที่ดีอย่างครบวงจร ผลลัพธ์ดังกล่าวไม่เพียงสอดคล้องกับทฤษฎีและงานวิจัยที่มีอยู่ แต่ยังตอกย้ำว่าการตรวจสอบ IT ในปัจจุบันมิใช่เพียงการตรวจสอบด้านเทคนิคเท่านั้น หากแต่เป็นกระบวนการเชิงกลยุทธ์ที่ต้องการทั้งความรู้ ความเชี่ยวชาญ ความเป็นกลาง และการสนับสนุนเชิงระบบเพื่อสร้างคุณค่าและความยั่งยืนให้แก่องค์กร

5.3 ข้อจำกัดงานวิจัย

เนื่องจากงานตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit) ในประเทศไทยยังไม่เป็นที่แพร่หลายและได้รับความสนใจมากนัก จึงทำให้การศึกษาและการวิจัยในด้านนี้มีจำนวนข้อมูลที่จำกัดและขาดความครอบคลุมในหลาย ๆ ประเด็น ซึ่งเป็นอุปสรรคสำคัญในการพัฒนาแนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit) และการประยุกต์ใช้โมเดลต่าง ๆ ในประเทศไทย เนื่องจากผู้ที่มีความเชี่ยวชาญในด้านนี้ยังมีจำนวนไม่มาก

ในส่วนของปัจจัยที่ยังไม่ครอบคลุมทุกประเด็นนั้น เนื่องจากขาดข้อมูลที่หลากหลายและตัวอย่างจากงานวิจัยหรือการศึกษาที่เกิดขึ้นในประเทศไทย โดยเฉพาะในกรณีที่เกี่ยวข้องกับกระบวนการตรวจสอบในองค์กรต่าง ๆ ซึ่งมีการใช้เทคโนโลยีที่ทันสมัยและระบบสารสนเทศที่มีความซับซ้อนมากขึ้น ความหลากหลายของสถานการณ์ต่าง ๆ ทำให้การพัฒนาผลการศึกษามีข้อจำกัดในการประยุกต์ใช้ในสภาพแวดล้อมที่แตกต่างกัน รวมถึงขาดข้อมูลจากองค์กรที่ทำการตรวจสอบในลักษณะเดียวกัน ซึ่งทำให้ยากที่จะหาแนวทางหรือข้อสรุปที่ครอบคลุมทุกปัจจัยที่เกี่ยวข้อง

อีกปัญหาหนึ่งที่สำคัญคือการหาผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความเชี่ยวชาญในประเทศไทย โดยเฉพาะในภาคธุรกิจที่ไม่ใช่ภาครัฐหรือองค์กรขนาดใหญ่ เนื่องจากในหลายองค์กรยังขาดบุคลากรที่มีทักษะและความรู้เฉพาะด้านการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเต็มที่ นอกจากนี้ยังพบว่าผู้ตรวจสอบที่ทำงานในด้านนี้ส่วนหนึ่งยังไม่มีใบประกอบวิชาชีพที่เกี่ยวข้องกับการตรวจสอบหรือการรับรองความเชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศโดยตรง

5.4 ข้อเสนอแนะ

จากผลการสัมภาษณ์ผู้ให้สัมภาษณ์ในงานวิจัยนี้ ได้ชี้ให้เห็นถึงปัจจัยเพิ่มเติมที่มีผลต่อการดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งนอกเหนือจากการศึกษาในเชิงทฤษฎีแล้ว ปัจจัยที่สำคัญที่ไม่ควรมองข้าม คือ ปัจจัยทางด้านการฝึกอบรมและการพัฒนาทักษะของผู้ตรวจสอบให้ทันต่อการเปลี่ยนแปลงและพัฒนาการของมาตรฐานการตรวจสอบที่มีการอัพเดตและปรับปรุงอยู่เสมอ โดยการฝึกอบรมที่มีประสิทธิภาพจะช่วยเสริมสร้างความเข้าใจและทักษะในการตรวจสอบด้านเทคโนโลยีสารสนเทศให้สามารถตรวจจับความเสี่ยงและปัญหาที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ และยังสามารถปฏิบัติตามมาตรฐานที่เหมาะสมกับการเปลี่ยนแปลงทางเทคโนโลยีได้อย่างถูกต้อง

การฝึกอบรมในเรื่องนี้ไม่เพียงแค่เน้นที่ทฤษฎี แต่ต้องรวมถึงการฝึกปฏิบัติจริงในสถานการณ์ที่หลากหลาย โดยการให้ผู้ตรวจสอบมีโอกาสได้สัมผัสและทำงานในสถานการณ์ที่เกี่ยวข้องกับการตรวจสอบเทคโนโลยีสารสนเทศ เช่น การประเมินความปลอดภัยของระบบ การตรวจสอบกระบวนการควบคุมภายใน และการระบุความเสี่ยงที่เกิดขึ้นจากเทคโนโลยีที่องค์กรใช้ เพื่อให้สามารถประเมินได้อย่างแม่นยำและสอดคล้องกับมาตรฐานต่าง ๆ

นอกจากนี้ ควรให้ความสำคัญกับการศึกษาข้อมูลและเทคโนโลยีที่เกี่ยวข้องอย่างต่อเนื่อง ซึ่งในยุคที่เทคโนโลยีมีการพัฒนาอย่างรวดเร็ว การทำงานของผู้ตรวจสอบจะต้องสามารถเข้าใจเทคโนโลยีที่มีการเปลี่ยนแปลงไปอย่างต่อเนื่อง เช่น ระบบคลาวด์ (Cloud Computing) การใช้ปัญญาประดิษฐ์ (Artificial Intelligence) ในการตรวจสอบ การรักษาความปลอดภัยไซเบอร์ (Cybersecurity) และเทคโนโลยีบล็อกเชน (Blockchain) เป็นต้น โดยเฉพาะการปรับตัวให้เข้ากับเทคโนโลยีใหม่ ๆ ที่องค์กรนำมาใช้ และการศึกษามาตรฐานใหม่ ๆ ที่เกี่ยวข้องกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ

อีกประการที่สำคัญคือการศึกษากระบวนการทำงานที่เกี่ยวข้องกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งไม่ใช่แค่การตรวจสอบด้านเทคนิคและความปลอดภัยเท่านั้น แต่ยังรวมถึงการประเมินความเสี่ยงในกระบวนการทำงานต่าง ๆ เช่น กระบวนการจัดการข้อมูล การควบคุมการเข้าถึงข้อมูล และการรักษาความเป็นส่วนตัวของข้อมูลในระบบเทคโนโลยีสารสนเทศที่องค์กรใช้ โดยการศึกษาผลกระทบที่เกิดจากการทำงานในลักษณะต่าง ๆ จะช่วยให้ผู้ตรวจสอบสามารถทำการประเมินที่มีความครอบคลุมและแม่นยำมากยิ่งขึ้น

ด้วยเหตุนี้ การศึกษาและการฝึกอบรมทั้งในด้านทฤษฎีและการปฏิบัติจริง รวมถึงการติดตามและปรับปรุงการฝึกอบรมเพื่อให้ทันสมัยกับมาตรฐานใหม่ ๆ จึงเป็นสิ่งที่สำคัญมากในการพัฒนาความสามารถของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งจะเป็นปัจจัยในการทำให้การตรวจสอบด้านนี้มีความเข้มแข็งและมีประสิทธิภาพในการป้องกันและจัดการกับความเสี่ยงที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในองค์กร

ดังนั้น ผู้วิจัยจึงขอเสนอให้มีการศึกษาและการฝึกอบรมในประเด็นเหล่านี้ในอนาคต เพื่อเสริมสร้างความสามารถในการตรวจสอบด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพและทันสมัยกับการเปลี่ยนแปลงของเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็วในโลกปัจจุบัน

บรรณานุกรม

ภาษาไทย

กรมบัญชีกลาง. (ม.ป.ป.). *การตรวจสอบภายใน ให้อะไรมากกว่าที่ท่านคิด*. กรุงเทพฯ: กรมบัญชีกลาง.

กรมบัญชีกลาง. (ม.ป.ป.). *แนวปฏิบัติการตรวจสอบภายใน*. กรุงเทพฯ: กรมบัญชีกลาง.

แคทรียา เรืองเจริญ. (2564). ปัจจัยที่ส่งผลกระทบต่อมาตรฐานด้านการปฏิบัติงานการตรวจสอบภายใน ในมุมมองของผู้รับการตรวจสอบ สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. การค้นคว้าอิสระบัญชีมหาบัณฑิต, คณะบัญชี, มหาวิทยาลัยศรีปทุม.

ชัชพงศ์ อธิปัญญาวงศ์. (2559). ปัจจัยที่มีผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT. มหาวิทยาลัยธรรมศาสตร์.

ณภัทร จิตต์เสรี. (ม.ป.ป.). ปัจจัยที่ส่งผลต่อประสิทธิภาพการปฏิบัติงานของการตรวจสอบภายในเขตพื้นที่กรุงเทพมหานคร. คณะบริหารธุรกิจ, มหาวิทยาลัยรามคำแหง.

ตลาดหลักทรัพย์แห่งประเทศไทย และสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย. (2548). แนวทางการตรวจสอบภายใน. กรุงเทพฯ: ตลาดหลักทรัพย์แห่งประเทศไทย.

บุญเกียรติ เดชะวรานนท์. (ม.ป.ป.). การตรวจสอบเทคโนโลยีสารสนเทศ : Information Technology Audit. สืบค้นเมื่อ 5 กันยายน 2566, จาก http://www.bfiia.org

บุญศรี กุศเลิศจริยา. (2541). ปัจจัยที่มีผลต่อความสำเร็จของการตรวจสอบภายในของส่วนราชการ. สาขาวิชาบริหารธุรกิจ, คณะบริหารและจัดการ, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

ประจิต หาวัตรและศรัณย์ ชูเกียรติ. (2560). การตรวจสอบเทคโนโลยีสารสนเทศในมหาวิทยาลัย: การวิเคราะห์เนื้อหาสาระของรายงานการตรวจสอบภายในประจำปี. วรสารวิชาชีพบัญชี. ปีที่ 13. ฉบับที่ 37.

ภาพร ภิยโยดิลกชัย. (2553). การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT. งานค้นคว้าอิสระปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร, มหาวิทยาลัยธุรกิจบัณฑิตย์.

มหาวิทยาลัยราชภัฏรำไพพรรณี. (2564). คู่มือปฏิบัติงานการตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit).

ศรุดา โพธิ์พันธุ์. (2561). ปัจจัยที่มีผลต่อประสิทธิผลของการตรวจสอบภายในในมุมมองของผู้รับการตรวจของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง. งานค้นคว้าอิสระปริญญามหาบัณฑิต สาขาวิชาบริหารธุรกิจ, คณะบริหารและจัดการ, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

สมภพ เตชเสนสกุล. (ม.ป.ป.). แนวทางตรวจสอบระบบเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบระบบเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์. สืบค้นเมื่อ 5 กันยายน 2566, จาก https://www.sepo.go.th

สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย. (2554). มาตรฐานสากลการปฏิบัติงานวิชาชีพตรวจสอบภายใน. กรุงเทพฯ : สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย.

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2562). แนวทางการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (IT Risk Management Practice).

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2565). การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit).

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2565). ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ.

สุวรรณี รุ่งจตุรงค์. (2561). ปัจจัยที่ส่งผลต่อประสิทธิภาพของงานสอบบัญชีของผู้สอบบัญชีรับอนุญาตในเขตกรุงเทพมหานครและปริมณฑล. ผลงานวิจัย, คณะบัญชี, มหาวิทยาลัยศรีปทุม.

อภิณห์พร เมธาวัชนานนท์. (2551). การตรวจสอบเทคโนโลยีสารสนเทศ (เอกสารการสอน). กรุงเทพฯ : คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์.

อรพรรณ แสงศิวะเวทย์. (2559). ปัจจัยที่ส่งผลกระทบต่อประสิทธิภาพของงานตรวจสอบภายใน: มุมมองของผู้ตรวจสอบภายใน. มหาวิทยาลัยธรรมศาสตร์.

อัมรา เพียรบูชา. (2557). ปัจจัยที่ส่งผลกระทบต่อการปฏิบัติงานตรวจสอบบัญชีของ ผู้สอบบัญชีรับอนุญาตในเขตกรุงเทพมหานคร. บัญชีมหาบัณฑิต, บัณฑิตวิทยาลัย, มหาวิทยาลัยศรีปทุม.

ภาษาอังกฤษ

Abdul, H., & Shamyla, A. (2012). Linking top management support and IT infrastructure with organizational performance: Mediating role of knowledge application. Canadian Social Science.

Abdulahi, A. D. (2016). Effects of internal audit practice on organizational performance of remittance companies in Mogadishu-Somalia. Journal of Business Management.

Ameeq, U., & Furqan, H. (2013). Impact of training on employee's development and performance in hotel industry of Lahore Pakistan. Journal of Business Studies Quarterly.

Azhar, S. (2013). Accounting information systems. Lingga Jaya, Bandung.

Cangemi, M. (2014). Performing a strategic risk-based assessment: Integrating data analytics into the audit universe. EDPACS: The EDP Audit, Control & Security Newsletter, 49(5), 1–6.

Dessalegn, G., & Aderajew, W. (2007). Internal audit effectiveness: An Ethiopian public sector case study.

El-Masry, E., & Hansen, K. (2007). Factors affecting auditors' utilization of evidential cues. Managerial Auditing Journal, 23(1), 26–50.

HELIYON. (2023). Examining the critical factors of internal audit effectiveness from internal auditors' perspective: Moderating role of extrinsic rewards. https://doi.org/10.1016/j.heliyon.2023.e20497

Hu, D. (2015). Audit quality and measurement: Towards a comprehensive understanding. Academy of Accounting and Financial Studies Journal, 19(1), 209–222.

ISACA. (2014). ITAF: A professional practices framework for IS audit/assurance (3rd ed.). Rolling Meadows, IL: ISACA.

Merhout, J., & Havelka, D. (2008). Information technology auditing: A value-added IT governance partnership between IT management and audit. Communications of the Association for Information Systems, 23, 463–482.

Rosário, T., Pereira, R., & Silva, M. (2012). Formalization of the IT audit management process. In Proceedings of IEEE the 16th International Enterprise Distributed Object Computing Conference Workshops, 1–10.

Stoel, D., Havelka, D., & Merhout, J. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. International Journal of Accounting Information Systems, 13, 60–79.

Usman. (2016). Effect of independence and competence on the quality of internal audit: Proposing a research framework. International Journal of Scientific & Technology Research, 5.

Vaicekauskas, D., & Mackevičius, J. (2014). Developing a framework for audit quality management in audit firms. Zeszyty Teoretyczne Rachunkowosci, 75(131), 171–193.

Zulikifli, B., Alagan, S., & Mohd, S. I. (2014). Factors that contribute to the effectiveness of internal audit in public sector.

ประวัติผู้เขียน

ชื่อ	นายพชรพล สัตยพงศ์
ชื่อวิทยานิพนธ์	แนวทางปฏิบัติที่ดีในการตรวจสอบด้านเทคโนโลยีสารสนเทศ
สาขาวิชา	วิทยาศาสตร์ข้อมูลเพื่อนวัตกรรม
ประวัติ	ประวัติการศึกษา พ.ศ. 2564 สำเร็จการศึกษาปริญญาตรี วิทยาศาสตรบัณฑิต สาขาวิชาฟิสิกส์อิเล็กทรอนิกส์ มหาวิทยาลัยธรรมศาสตร์ ประวัติการทำงาน พ.ศ. 2567-ปัจจุบัน กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตำแหน่ง พนักงานสนับสนุนด้านการบริหารจัดการข้อมูล