Journal of Digital Business and Social Sciences

Journal homepage: jdbs.rsu.ac.th

Guideline Framework of Information Technology Security System by ISO 27001: 2013 Standard of the Securities and Exchange Commission (SEC)

กรอบโครงร่างความมั่นคงปลอดภัยระบบสารสนเทศ (ISO27001: 2013): กรณีศึกษา สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

Chanakan Arponpong[a], Buarian Soongpol[a*]
ชนกานต์ อาภรณ์พงษ์[a], บัวเรียน สูงพล[a*]

[a]*College of Digital Information Technology, Rangsit University, Thailand*

[*]*Corresponding author: buerian@gmail.com*

Received 24 November 2022; Revised 2 December 2022; Accepted 3 December 2022; Published Online 22 March 2023

Abstract

This research compared the Information Technology System Implementation Guideline of the Securities and Exchange Commission (SEC) with ISO 27001: 2013 Standard because Information Technology nowadays comes into the capital market sector, and there is a digital database that can cause damage in the event of a data leak. The objectives of the research are: (1) To enable organizations in the capital market sector or the stock market to achieve operational efficiency, maintain, improve, and continually develop a security management system for information technology; (2) To ensure that the Information Technology System Implementation Guideline of SEC can guide organization or agencies in the capital market; (3) To support organization management in the Information Technology System. The research prepared a satisfaction assessment form comparing the Information Technology System Implementation Guideline of SEC with ISO 27001 standard for ten respondents from information technology security and safety-related personnel. It was found that the results were generally at a high level of satisfaction, with an average score of 4.40 and a standard deviation of 0.457, which is consistent with the content analysis of information that can improve additional content to meet the ISO 27001 standard better.

Keywords: *Information Technology System; Information Technology Security; ISO 27001 Standard*

Please cite this article as: Arponpong, C., & Soongpol, B. (2023, March). Guideline Framework of Information Technology Security System by ISO 27001: 2013 Standard of the Securities and Exchange Commission (SEC). *Journal of Digital Business and Social Sciences*, *9*(1), JDB011, 1-12.

บทคัดย่อ

งานวิจัยนี้ได้ทำการศึกษาการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) กับมาตรฐาน ISO 27001 เนื่องจากปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทต่อองค์กรในภาคตลาดทุนมากขึ้น และมีฐานข้อมูลที่อยู่ในระบบดิจิทัลซึ่งอาจก่อให้เกิดความเสียหายหากเกิดเหตุการณ์ข้อมูลรั่วไหล งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อให้องค์กรในภาคตลาดทุน หรือตลาดหลักทรัพย์เกิดประสิทธิภาพในการปฏิบัติ รักษา ปรับปรุง และพัฒนาระบบบริหารความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศอย่างต่อเนื่อง และทำให้มั่นใจได้ยิ่งขึ้นว่าแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต มีแนวทางในการแนะนำองค์กรหรือหน่วยงานในภาคตลาดทุนให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศตามมาตรฐานสากลที่พัฒนาขึ้นโดยองค์กรสากล ISO (International Organization for Standardization) ซึ่งได้รับการยอมรับในระดับนานาชาติ
งานวิจัยนี้ได้จัดทำแบบประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001 ของผู้ตอบแบบสอบถามจำนวน 10 คนจากบุคลากรที่ดำเนินการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง พบว่าผลการแปลผลการตอบแบบประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001 โดยรวมอยู่ในระดับมีความพึงพอใจมาก โดยมีคะแนนเฉลี่ย 4.40 และมีค่าเบี่ยงเบนมาตราฐาน 0.457 ซึ่งสอดคล้องกับการวิเคราะห์เนื้อหาของสารสนเทศโดยเนื้อหาของแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. ครอบคลุมตามมาตรฐาน ISO 27001 และสามารถปรับปรุงเนื้อหาเพิ่มเติมเพื่อให้ครบถ้วนตามมาตรฐาน ISO 27001 ได้ดีมากยิ่งขึ้น

คำสำคัญ*: ระบบเทคโนโลยีสารสนเทศ; การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ; มาตรฐาน* ISO 27001

Please cite this article as: Arponpong, C., & Soongpol, B. (2023, March). Guideline Framework of Information Technology Security System by ISO 27001: 2013 Standard of the Securities and Exchange Commission (SEC). *Journal of Digital Business and Social Sciences*, *9*(1), JDB011, 1-12.

1. บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจขององค์กรในภาคตลาดทุนมากขึ้น เนื่องจากเป็นโครงสร้างพื้นฐานที่สำคัญที่รองรับกลยุทธ์ในการดำเนินธุรกิจ ช่วยเพิ่มประสิทธิภาพ ลดต้นทุนในการดำเนินงาน และเพิ่มศักยภาพในการตอบสนองต่อความต้องการของลูกค้าที่ต้องการผลิตภัณฑ์และบริการที่หลากหลายได้อย่างสะดวกและรวดเร็ว และเนื่องด้วยสาเหตุประการนี้ทำให้องค์กรไม่ว่าขนาดเล็ก ขนาดกลาง หรือขนาดใหญ่ ต่างมีฐานข้อมูลของลูกค้าที่อยู่ในระบบดิจิทัลด้วยกันทั้งสิ้น ฉะนั้นความมั่นคงปลอดภัยของข้อมูลสารสนเทศจึงมีความสำคัญและเป็นสิ่งจำเป็นที่ต้องมีในทุกองค์กร เพื่อทำการรวบรวมประมวลผล และจัดเก็บข้อมูลบนคอมพิวเตอร์ และอุปกรณ์อื่น ๆ ที่องค์กรใช้งาน โดยข้อมูลต่าง ๆ เหล่านี้อาจเป็นข้อมูลที่สำคัญมาก เช่น ทรัพย์สินทางปัญญา ข้อมูลทางการเงิน ข้อมูลส่วนบุคคล หรือเป็นข้อมูลสำคัญของหลายประเทศ

สำนักงาน ก.ล.ต. ซึ่งมีบทบาทในการควบคุมดูแลองค์กรในภาคตลาดทุนจึงกำหนดให้ผู้ประกอบธุรกิจ หรือองค์กรต้องจัดให้มีนโยบาย มาตรการ และระบบงาน ในการกำกับดูแลและบริหารจัดการเทคโนโลยีและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยต้องดำเนินการควบคุมดูแล ติดตาม และตรวจสอบให้มีการปฏิบัติตามนโยบาย มาตรการ และระบบงานดังกล่าว ตลอดจนมีการทบทวนความเหมาะสมเป็นประจำ จึงออกประกาศแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางให้หน่วยงาน องค์กรในภาคตลาดทุน หรือตลาดหลักทรัพย์มีระบบบริหารความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศที่ดี

2. วัตถุประสงค์การวิจัย

1. ศึกษามาตรฐาน ISO 27001: 2013 เพื่อนำมาเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

2. เปรียบเทียบผลการศึกษาเพื่อนำมาพัฒนาหรือปรับปรุงแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต)

3. นำเสนอกรอบโครงร่างความมั่นคงปลอดภัยระบบสารสนเทศเพื่อสนับสนุนการบริหารในระดับองค์กร

3. ทบทวนวรรณกรรม

ความมั่นคงปลอดภัยสารสนเทศ

ความมั่นคงปลอดภัยสารสนเทศ คือการป้องกันข้อมูลสารสนเทศ รวมไปถึงอุปกรณ์และองค์ประกอบอื่น ๆ ที่เกี่ยวข้อง เช่น ระบบซอร์ฟแวร์และฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนข้อมูลสารสนเทศนั้นให้อยู่ในสถานะที่มีความปลอดภัย และรอดพ้นจากภัยคุกคามจากทั้งภายในองค์กรและภายนอกองค์กร โดยมีเป้าหมายในการรักษาความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วยคุณสมบัติ 3 ประการ ได้แก่

- ความลับ (Confidentiality) หมายถึง การปกปิดข้อมูลหรือทรัพยากร ที่มีความจำเป็นต้องเก็บรักษาความลับของข้อมูลที่เกิดจากการใช้คอมพิวเตอร์ในด้านที่ละเอียดอ่อน
- ความถูกต้องสมบูรณ์ (Integrity) หมายถึง ความน่าเชื่อถือของข้อมูลหรือทรัพยากร
- ความพร้อมใช้งาน (Availability) หมายถึง ความสามารถในการใช้ข้อมูลหรือทรัพยากรที่ต้องการ

มาตรฐาน ISO 27001: 2013

มาตรฐาน ISO 27001: 2013 เป็นมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศที่พัฒนาขึ้นโดยองค์กรสากล ISO (International Organization for Standardization) ซึ่งได้รับการยอมรับในระดับนานาชาติ โดยมาตรฐาน ISO 27001: 2013 ถูกจัดให้เป็นแนวทางและข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) เพื่อสร้างความมั่นใจถึงความมีประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศขององค์กร

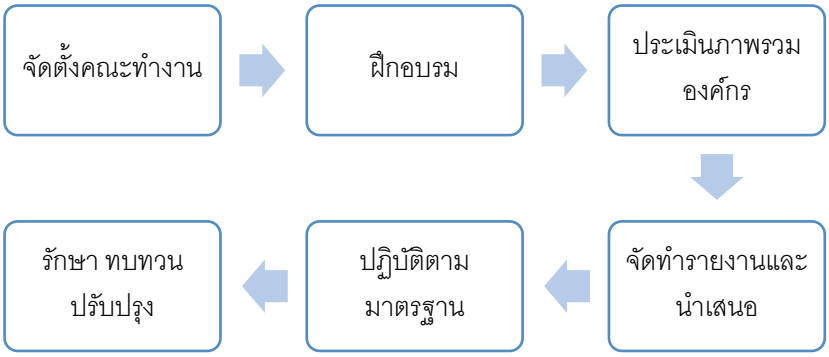
ในมาตรฐาน ISO 27001: 2013 มีเนื้อหาแบ่งออกเป็น 14 หัวข้อใหญ่ (Domain) ซึ่งเป็นข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยในแต่ละข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยจะประกอบไปด้วยวัตถุประสงค์ (Control Objective) และมาตรการ (Control) ในการรักษาความมั่นคงปลอดภัย ตามตารางที่ 1

ตารางที่ 1 รายละเอียดมาตรฐาน ISO 27001: 2013

ข้อ	หัวข้อ	ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย	จำนวนวัตถุประสงค์	จำนวนมาตรการ
1	A.5	นโยบายความมั่นคงปลอดภัยสารสนเทศ	1	2
2	A.6	โครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	2	7
3	A.7	ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล	3	6
4	A.8	การบริหารจัดการทรัพย์สิน	3	10
5	A.9	การควบคุมการเข้าถึง	4	14
6	A.10	การเข้ารหัสข้อมูล	1	2
7	A.11	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	2	15
8	A.12	ความมั่นคงปลอดภัยสำหรับการดำเนินการ	7	14
9	A.13	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล	2	7
10	A.14	การจัดหา การพัฒนา และการบำรุงรักษาระบบ	3	13
11	A.15	ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก	2	5
12	A.16	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	1	7
13	A.17	ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ	2	4

ข้อ	หัวข้อ	ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย	จำนวนวัตถุประสงค์	จำนวนมาตรการ
14	A.18	การปฏิบัติตามข้อกำหนด	2	8

ในประเทศไทยได้ออกกฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติ (พ.ร.บ.) ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และ พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ จึงทำให้องค์กรในประเทศเกิดความตื่นตัวและให้ความสนใจในเรื่องความมั่นคงปลอดภัยสารสนเทศมากขึ้น องค์กรในประเทศไทยเริ่มนำ มาตรฐาน ISO 27001 มาเป็นแนวทางสำหรับพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยแนวทางในการนำมาตรฐาน ISO 27001 มาใช้ในองค์กรนั้น มี 6 ขั้นตอน ตามรูปที่ 2



รูปที่ 2 แนวทางในการนำมาตรฐาน ISO 27001 จำนวน 6 ขั้นตอน

โดยมีรายละเอียด ดังนี้

1.จัดตั้งคณะทำงาน IT Security Steering หรือ IT Security Working Group เพื่อทำการศึกษามาตรฐานอย่างละเอียด

2. จัดฝึกอบรมให้ทีมงานได้ทำความเข้าใจในส่วนของข้อกำหนดของมาตรฐาน ISO 27001 ซึ่งจะทำให้ทีมงานได้เข้าใจแนวทางของการตรวจสอบโดยการนำมาตรฐาน ISO 27001 มาใช้อย่างถูกต้อง

3. จัดทำการประเมินภาพรวมขององค์กรเปรียบเทียบกับมาตรฐาน ISO 27001 โดยใช้เทคนิค Gap Analysis คือการตรวจประเมินเบื้องต้นเพื่อหาความแตกต่างระหว่างระบบที่เป็นอยู่ในปัจจุบันขององค์กร กับมาตรฐานที่ต้องการจะเป็นในอนาคต

4. หลังจากการทำ “Gap Analysis Workshop” แล้วควรมีการจัดทำรายงานและมีการนำเสนอต่อ Board of Director เพื่อที่จะให้ผู้บริหารระดับสูงเกิดความเข้าใจในปัญหาที่เกิดขึ้น

5. ผู้บริหารระดับสูงตัดสินใจให้การสนับสนุนในการปฏิบัติตามมาตรฐาน ISO/IEC 27001 และดำเนินการแก้ไขข้อบกพร่องจากการที่องค์กรยังไม่ได้ปฏิบัติตามมาตรฐานดังกล่าวอย่างเป็นรูปธรรม (Corrective Action)

6. มีการรักษา ทบทวนผลการทำระบบและหาจุดปรับปรุงอย่างต่อเนื่องเพื่อความมีประสิทธิภาพของการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร

แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

สำนักงาน ก.ล.ต. มีบทบาทในการควบคุมและดูแลองค์กรในภาคตลาดทุนจึงได้จัดทำแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ เพื่อกำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีนโยบาย มาตรการ และระบบงานในการกำกับดูแลและบริหารจัดการเทคโนโลยีและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยต้องดำเนินการควบคุมดูแลติดตาม และตรวจสอบให้มีการปฏิบัติตามนโยบาย มาตรการ และระบบงาน ตลอดจนมีการทบทวนความเหมาะสมเป็นประจำ โดยมีแนวทางในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ตามตารางที่ 2

ตารางที่ 2 รายละเอียดแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

ข้อ	หัวข้อ
หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)	
1.1	บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ
1.2	โครงสร้างการกำกับดูแล
1.3	นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT
หมวดที่ 2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)	
2.1	โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (Organization of Information Technology Security)
2.2	การบริหารจัดการบุคลากร และบุคคลภายนอก
2.3	การบริหารจัดการทรัพย์สินด้าน IT (IT Asset Management)
2.4	การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)
2.5	การควบคุมการเข้าถึงข้อมูลและระบบ IT (Access Control)
2.6	การควบคุมการเข้ารหัส (Cryptographic Control)
2.7	การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
2.8	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT Operations Security)
2.9	การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (Communication System Security)
2.10	การบริหารจัดการโครงการด้าน IT (IT Project Management) การจัดหา พัฒนา

ข้อ	หัวข้อ
	และบำรุงรักษาระบบ IT (System Acquisition, Development and Maintenance)
2.11	การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT Incident Management)
2.12	แผนฉุกเฉินด้าน IT (IT Contingency Plan)
หมวดที่ 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)	

4. ระเบียบวิธีการวิจัย

เนื่องจากเป้าหมายของงานวิจัยนี้ คือ เพื่อทำการศึกษาการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ประเทศไทย (สำนักงาน ก.ล.ต.) กับมาตรฐาน ISO 27001 โดยมีวัตถุประสงค์เพื่อให้หน่วยงาน องค์กรในภาคตลาดทุน หรือตลาดหลักทรัพย์เกิดประสิทธิภาพในการปฏิบัติ รักษา ปรับปรุง และพัฒนาระบบบริหารความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศอย่างต่อเนื่อง และทำให้มั่นใจได้ยิ่งขึ้นว่าแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. มีแนวทางในการแนะนำองค์กรหรือหน่วยงานในภาคตลาดทุนให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศตามมาตรฐานสากล ดังนั้น ระเบียบวิธีวิจัยที่เหมาะสม คือ การวิจัยเชิงคุณภาพด้วยวิธีการวิเคราะห์เนื้อหาสาระ (Content Analysis) ของแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต และมาตรฐาน ISO 27001: 2013 ซึ่งมีการวิเคราะห์เนื้อหาของสารสนเทศที่สื่อสารอย่างละเอียดทั้งเนื้อหาที่ปรากฏชัดเจนและเนื้อหาโดยนัย นอกจากนั้นได้ทำแบบประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001 โดยเก็บจากการสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) จากบุคลากรที่ดำเนินการด้านความมั่นคงปลอดภัยในสำนักงาน ก.ล.ต. จำนวน 10 คนเพื่อนำมาหาค่าเฉลี่ยกลุ่มตัวอย่าง (X bar) และค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) ซึ่งมีมาตรวัดตามมาตราส่วนประมาณค่ากำหนดระดับคะแนนในการตอบแบบประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001 จำนวน 5 ระดับ ดังนี้

5 หมายถึง มีความพึงพอใจมากที่สุด

4 หมายถึง มีความพึงพอใจมาก

3 หมายถึง มีความพึงพอใจปานกลาง

2 หมายถึง มีความพึงพอใจมากน้อย

1 หมายถึง มีความพึงพอใจน้อยที่สุด

และมีการแปลความหมายระดับค่าคะแนนเฉลี่ยข้อมูลวัดมาตราส่วนประมาณค่าพิจารณาตามเกณฑ์การวิเคราะห์ ดังนี้

ระดับคะแนนเฉลี่ย 4.50-5.00 หมายถึง มีความพึงพอใจมากที่สุด

ระดับคะแนนเฉลี่ย 3.50 -4.49 หมายถึง มีความพึงพอใจมาก

ระดับคะแนนเฉลี่ย 2.50 -3.49 หมายถึง มีความพึงพอใจปานกลาง

ระดับคะแนนเฉลี่ย 1.50-2.40 หมายถึง มีความพึงพอใจน้อย

ระดับคะแนนเฉลี่ย 1.00 -1.49 หมายถึง มีความพึงพอใจน้อยที่สุด

จากคะแนนดังกล่าวใช้คำนวณค่าเฉลี่ยของตัวแปร เพื่อดูแนวโน้มของระดับความพึงพอใจของผู้ตอบแบบสอบถาม และมีการคำนวณค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) ใช้คำนวณเพื่อวัดการกระจายระดับความพึงพอใจของผู้ตอบแบบสอบถาม

5. ผลการวิจัย

จากการศึกษาแบบประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001 ของผู้ตอบแบบสอบถามจากบุคลากรที่ดำเนินการด้านความมั่นคงปลอดภัยที่เกี่ยวข้องจำนวน 10 คนมีผลที่ได้ ตามตารางที่ 2

ตารางที่ 2 ผลการศึกษาแบบประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001

ข้อ	หัวข้อ	ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย	คะแนนค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	การแปลผล
1	A.5	นโยบายความมั่นคงปลอดภัยสารสนเทศ	4.80	0.421	มากที่สุด
2	A.6	โครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	4.25	0.263	มาก
3	A.7	ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล	4.27	0.644	มาก
4	A.8	การบริหารจัดการทรัพย์สิน	4.47	0.322	มาก
5	A.9	การควบคุมการเข้าถึง	4.40	0.293	มาก
6	A.10	การเข้ารหัสข้อมูล	4.85	0.241	มากที่สุด
7	A.11	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	4.25	0.589	มาก
8	A.12	ความมั่นคงปลอดภัยสำหรับการดำเนินการ	4.80	0.421	มากที่สุด
9	A.13	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล	4.25	0.263	มาก
10	A.14	การจัดหา การพัฒนา และการบำรุงรักษาระบบ	4.27	0.438	มาก

ข้อ	หัวข้อ	ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย	คะแนนค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	การแปลผล
11	A.15	ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก	4.60	0.516	มากที่สุด
12	A.16	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	4.40	0.516	มาก
13	A.17	ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ	4.40	0.966	มาก
14	A.18	การปฏิบัติตามข้อกำหนด	3.60	0.516	มาก
คะแนนเฉลี่ย			4.40	0.457	มาก

จากตารางที่ 2 ผลการแปลการตอบแบบประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001 โดยรวมอยู่ในระดับมีความพึงพอใจมาก โดยมีคะแนนเฉลี่ย 4.40 และมีค่าเบี่ยงเบนมาตราฐาน 0.457 สามารถสรุปหัวข้อที่ได้คะแนนความพึงพอใจ ดังต่อไปนี้

ตารางที่ 3 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่ได้ผลความพึงพอใจมากที่สุด

หัวข้อ	ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย	คะแนนค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน
A.5	นโยบายความมั่นคงปลอดภัยสารสนเทศ	4.80	0.421
A.10	การเข้ารหัสข้อมูล	4.85	0.241
A.12	ความมั่นคงปลอดภัยสำหรับการดำเนินการ	4.80	0.421
A.15	ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก	4.60	0.516

จากตารางที่ 3 ข้อกำหนดที่มีคะแนนค่าเฉลี่ยสูงที่สุด คือ การเข้ารหัสข้อมูล โดยมีคะแนนค่าเฉลี่ย 4.85 และมีค่าเบี่ยงเบนมาตราฐาน 0.241

ตารางที่ 4 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่ได้ผลความพึงพอใจมาก

หัวข้อ	ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย	คะแนนค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน
A.6	โครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	4.25	0.263
A.7	ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล	4.27	0.644
A.8	การบริหารจัดการทรัพย์สิน	4.47	0.322
A.9	การควบคุมการเข้าถึง	4.40	0.293
A.11	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	4.25	0.589
A.13	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล	4.25	0.263
A.14	การจัดหา การพัฒนา และการบำรุงรักษาระบบ	4.27	0.438
A.16	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	4.40	0.516
A.17	ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ	4.40	0.966
A.18	การปฏิบัติตามข้อกำหนด	3.60	0.516

จากตารางที่ 4 ข้อกำหนดที่มีคะแนนค่าเฉลี่ยต่ำที่สุด ได้แก่ การปฏิบัติตามข้อกำหนด โดยมีคะแนนค่าเฉลี่ย 3.60และมีค่าเบี่ยงเบนมาตราฐาน 0.516

6. บทสรุป

จากการศึกษาพบว่าผลการแปลผลการตอบแบบประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001 โดยรวมอยู่ในระดับมีความพึงพอใจมาก โดยมีคะแนนเฉลี่ย 4.40 และมีค่าเบี่ยงเบนมาตราฐาน 0.457

ข้อกำหนดที่มีคะแนนค่าเฉลี่ยสูงที่สุด ได้แก่ การเข้ารหัสข้อมูล โดยมีคะแนนค่าเฉลี่ย 4.85 และมีค่าเบี่ยงเบนมาตราฐานที่ 0.241และยังมีอีก 3 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่ได้ผลความพึงพอใจมากที่สุด ได้แก่ นโยบายความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยสำหรับการดำเนินการ และความสัมพันธ์กับผู้ขายผู้ให้บริการภายนอก ซึ่งสอดคล้องและมีเนื้อหาที่ครอบคลุมและครบถ้วนตามมาตรฐาน ISO 27001

ข้อกำหนดที่มีคะแนนค่าเฉลี่ยต่ำที่สุด ได้แก่ การปฏิบัติตามข้อกำหนด โดยมีคะแนนค่าเฉลี่ย 3.60 และมีค่าเบี่ยงเบนมาตราฐาน 0.516 โดยยังอยู่ในระดับคะแนนเฉลี่ยที่ได้รับความพึงพอใจมาก และยังมีอีก 9 ข้อกำหนดด้านการ

รักษาความมั่นคงปลอดภัยที่ได้ผลความพึงพอใจมากเช่นกัน ได้แก่ โครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล การบริหารจัดการทรัพย์สิน การควบคุมการเข้าถึง ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล การจัดหา การพัฒนา และการบำรุงรักษาระบบ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ ซึ่งสอดคล้องและมีเนื้อหาที่ครอบคลุมตามมาตรฐาน ISO 27001 ทั้งนี้ แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. สามารถปรับปรุงเนื้อหาเพิ่มเติมเพื่อให้ครบถ้วนตามมาตรฐาน ISO 27001 ได้มากขึ้นตามข้อเสนอแนะ ดังนี้

1) การติดต่อหน่วยงานที่มีอำนาจด้านความมั่นคงปลอดภัย การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน หรือกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย และสมาคมวิชาชีพ

2) ด้านความมั่นคงปลอดภัยด้านบุคลากร โดยระบุให้มีหน่วยงานบริหารทรัพยากรบุคคลมีการตรวจสอบประวัติการทำงานย้อนหลังของผู้สมัครตามกฎหมายระเบียบ ข้อบังคับที่เกี่ยวข้อง และมีการกำหนดกระบวนการทางวินัย เพื่อลงโทษหากมีการละเมิดความมั่นคงปลอดภัย

3) เพิ่มขั้นตอนปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูลอย่างเหมาะสม และสอดคล้องกับประเภทของสารสนเทศ

4) มีการระบุการออกแบบสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกเพื่อตอบโจทย์ในการรักษาความมันคงปลอดภัยทางกายภาพ และสามารถใช้งานได้อย่างเหมาะสม

5) เพิ่มขั้นตอนปฏิบัติให้มีการรักษาความปลอดภัยของทรัพย์สินที่นำไปใช้งานนอกองค์กร รวมไปถึงมีการกำหนดมาตรการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ดูแล

6) เพิ่มแนวทางการบริหารจัดการการเปลี่ยนแปลงการให้บริการจากผู้ให้บริการภายนอก

7) ให้ความรู้ด้านการปฏิบัติตามข้อกำหนดทางกฎหมายและสัญญาที่มีผลทางกฎหมาย

8) เพิ่มการแนะนำการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) อย่างเป็นลายลักษณ์อักษร โดยได้รับอนุมัติจากผู้มีอำนาจและเผยแพร่อย่างทั่วถึง และมีการทดสอบมาตรการต่าง ๆ ว่าสามารถใช้งานได้และมีประสิทธิภาพเมื่อเกิดเหตุเสียหายตามระยะเวลาที่กำหนด

9) เพิ่มแนวทางการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Utility Programs)

10) เพิ่มแนวทางการจำกัดและควบคุมการเข้าถึงชุดคำสั่ง (Source Code) ของโปรแกรม

เอกสารอ้างอิง

ชุลีกร นวลสมศรี, และสุทธิศักดิ์ จันทวงษ์โส. (2560). การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013 กรณีศึกษาขององค์กรด้านการบินแห่งหนึ่ง. *วารสารวิจัย มหาวิทยาลัยขอนแก่น (ฉบับบัณฑิตศึกษา), 17*(4), 1-11.

ธนภัทร กิตติวณิชพันธุ์, และอานนท์ ทับเที่ยง. (2561). สมรรถนะของบุคลากรในหน่วยงานราชการด้านความมั่นคงปลอดภัยไซเบอร์ตามข้อกำหนด NIST และมาตรฐาน ISO27001/2013. *วารสาร Engineering Transactions, 21*(1), 7-19.

ประจิต หาวัตร, และศรันย์ ชูเกียรติ. (2560). การตรวจสอบเทคโนโลยีสารสนเทศในมหาวิทยาลัย: การวิเคราะห์เนื้อหาสาระของรายงานการตรวจสอบภายในประจำปี. *วารสารวิชาชีพบัญชี, 13*(37), 5-14.

ภัทราพร โชติมหา. (2561). *การจัดทำแนวทางการตรวจสอบภายในตามมาตรฐาน ISO27001: 2013 กรณีศึกษาการทางพิเศษแห่งประเทศไทย*. วิทยานิพนธ์มหาบัณฑิต. มหาวิทยาลัยศรีปทุม.

วรรษา เปาอินทร์. (2565). การพัฒนาแนวทางปฏิบัติเพื่อพัฒนาความมั่นคงปลอดภัย การป้องกันความลับและความเป็นส่วนตัวของข้อมูลส่วนบุคคล สำหรับโรงพยาบาล. *Journal of the Thai Medical Informatics Association, 8*(1), 1-13.

สุภาพร พรมโส, ปราลี มณีรัตน์, และประสงค์ ปราณีตพลกรัง. (2564). สถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ. *วารสารวิทยาศาสตร์และเทคโนโลยีนายเรืออากาศ, 17*(2), 17 -30.

อนาวิล แก้วสอาด, และณัฐวี อุตกฤษฎ์. (2563). แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร. *วารสารสถาบันวิชาการป้องกันประเทศ*, *12*(1), 1-15.

Abomhara, M., & Geir, M. K. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security, 4*, 65–88. doi:10.13052/jcsm2245-1439.414

Arina, A. (2021). Implementing Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova. In *The 11th International Conference on Electronics, Communications and Computing* (pp. 228-231). Republica Moldova: Technical University of Moldova.

Arina, A., Pavel, N., & Anatolie, A. (2021). Analysis of Security Frameworks Implemented in Hei's. *InterConf, 7*(8), 347-359.

Bouziani, M., Merbah, M., Tiskar, M., Et-Tahir, A., & Chaouch, A. (2022). When can we talk about implementing an Information Security Management System, according to ISO 27001?. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13*(2), 394-401.

Fúska, R. (2022). *Implementation of ISO27001 standard in startups*. Master's thesis. Luleå University of Technology.

Sereepong, P. (2014). *มาตรการ (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001: 2013*. Retrieved from http://www.club27001.com

Ukidve, A., Mantha, S. S., & Reddy, D. N. (2022). Analyzing Mapping of ISO 27001: 2013 Controls for Alignment with Enterprise Risks Management. *Asian Journal of Organic & Medicinal Chemistry, 7*(2), 123-129.

ZERO!. (2020). *3 เสาหลัก CIA (Confidentiality, Iintegrity, Availability)*. Retrieved from https://medium.com/@rungsiman.ksp