การศึกษาเพื่อพัฒนาและปรับปรุงองค์กรให้เป็นมาตรฐาน Annex A ภายใต้มาตรฐาน ISO/IEC27001:2013 สู่มาตรฐาน ISO/IEC27001:2022

A STUDY OF ORGANIZATIONAL IMPROVEMENT RELATED TO ANNEX A STANDARDS UNDER THE STANDARDS ISO/IEC27001:2013 TO ISO/IEC27001:2022

โสพล ภพน้ำ[1]
ผู้ช่วยศาสตราจารย์ ดร.นันทิกา ปริญญาพล [2]

บทคัดย่อ

จากการศึกษาและการทำงานในด้านความปลอดภัยโดยมีมาตรฐาน ISO27001:2013 ใช้ภายในองค์กรทำให้ผู้วิจัยเล็งเห็นว่าในส่วนของข้อกำหนดมีบางข้อที่มีการเปลี่ยนแปลงอยู่ตลอดเวลานั่นคือในส่วนของระบบความปลอดภัยของอุปกรณ์อิเล็กทรอนิกส์ ที่มีความเชื่อมโยงถึงความมั่นใจในการทำงานและความมั่นใจกับลูกค้าในด้านของธุรกิจที่ทำให้เกิดการแข่งขันในธุรกิจ และมาตรฐานความเชื่อมั่นกับลูกค้า จึงได้จัดทำและดำเนินระบบ ISO27001:2013 เพื่อให้มีมาตรฐานสำหรับองค์กรไม่ว่าจะเป็นขนาดเล็ก ขนาดกลาง หรือขนาดใหญ่ ก็สามารถพัฒนาและปรับปรุงองค์กรได้อย่างครอบคลุมตั้งแต่เรื่องคน (Human), Hardware, Software และอื่น ๆ นำสู่การเสนอมาตรการจัดการความมั่นคงปลอดภัยของสารสนเทศ ตาม Annex A ของ ISO 27001:2013 ทั้งหมด 14 ข้อ

เพื่อให้องค์กรทุกขนาดมีแผนในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเป็นไปตามประกาศของคณะกรรมการธุรกรรมอิเล็กทรอนิกส์รวมถึงสอดคล้องกับระบบประเมินคุณภาพรัฐวิสาหกิจ ผู้วิจัยจึงเล็งเห็นความสำคัญของการศึกษาถึงปัจจัยที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยเป็นไปตามประกาศของคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 โดยได้มีการนำเอา

[1] นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยธุจกิจบัณฑิตย์

[2] อาจารย์ที่ปรึกษาสารนิพนธ์

มาตรฐาน ISO/IEC 27001 ซึ่งเป็นมาตรฐานสากลด้าน Information Security Management System มาเป็นกรอบในการดำเนินงาน ในการเข้ารับการรับรองมาตรฐาน ฯ ต่อไป

คำสำคัญ: มาตรฐาน, องค์กร, ความปลอดภัยสารสนเทศ

ABSTRACT

From studying and working in safety with standards ISO27001:2013 used within the organization, the researcher realized that there are some requirements that are constantly changing, namely in the security system of electronic devices. Which is linked to confidence in work and confidence with customers in the area of business that causes competition in business and standards of confidence with customers Therefore, the creation and operation of the system occurred. ISO27001:2013 in order to have standards for organizations, whether small, medium or large, to be able to develop and improve the organization in a comprehensive manner from Human, Hardware, Software and others, leading to the proposal of information security management measures. According to Annex A of ISO 27001:2013, All 14 points

To ensure that organizations of all sizes have plans for information security management in accordance with the announcements of the Electronic Transactions Commission and in accordance with the state enterprise quality assessment system. The researcher therefore recognizes the importance of studying factors related to information security management. In order to have security in accordance with the announcement of the Electronic Transactions Commission. Regarding policies and practices for maintaining information security of government agencies, B.E. 2010, Royal Decree on Secure Methods for Electronic Transactions, B.E. 2010, which has adopted ISO/ IEC 27001, which is an international standard for Information Security Management System, is the framework for operations. in receiving standard certification, etc.

Keywords: Standards, Organization, Information Security

บทนำ

เพื่อให้องค์กรทุกขนาดมีแผนในการบริหารการจัดการความมั่นคงและความปลอดภัยสารสนเทศและเป็นไปตามที่คณะกรรมการธุรกรรมอิเล็กทรอนิกส์ประกาศไว้และสอดคล้องกับระบบประเมินคุณภาพรัฐวิสาหกิจ ผู้วิจัยจึงเล็งเห็นความสำคัญของการศึกษาถึงปัจจัยที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และเพื่อให้มีความมั่นคงปลอดภัยเป็นไปตามประกาศของคณะกรรมการธุรกรรม

อิเล็กทรอนิกส์ เรื่องนโยบายและแนวทางการปฏิบัติในการรักษาความมั่นคงและความปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และพระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 โดยได้มีการนำเอามาตรฐาน ISO/IEC27001 ซึ่งเป็นมาตรฐานสากลด้าน Information Security Management System มาเป็นกรอบในการดำเนินงานในการเข้ารับการรับรองมาตรฐาน ISO/IEC27001 และประเมินว่าในปัจจุบันองค์กรมีความพร้อมในการเข้ารับการรับรองมาตรฐาน ฯ เพียงใด อีกทั้งควรมีการปรับปรุงอย่างไรเพื่อให้องค์กรมีความพร้อมในการเข้ารับการรับรองมาตรฐาน ฯ ต่อไป

วัตถุประสงค์ของงานวิจัย

1. เพื่อศึกษาและตรวจสอบให้องค์กรมีการปรับปรุงมาตรฐานให้มีประสิทธิภาพ และเป็นมาตรฐานในปัจจุบัน ISO27001:2013
2. เพื่อศึกษาและตรวจสอบให้องค์กรมีความพร้อมสำหรับการปรับปรุงมาตรฐานให้มีประสิทธิภาพและเป็นมาตรฐานในปัจจุบัน ISO27001:2022
3. ดำเนินงานสำหรับการปรับเปลี่ยนหรือปรับปรุงในส่วนที่มีเพิ่มเติมมาจากมาตรฐานให้ระบุไว้เพื่อให้ทราบว่าองค์กรมีความพร้อมหรือไม่นำมาใช้งานหรือปรับปรุงยังไง

ประโยชน์ที่คาดว่าจะได้รับ

1. ตรวจสอบองค์กรเพื่อปรับปรุงให้มีความพร้อมสำหรับมาตรฐาน ISO27001:2013
2. วิเคราะห์และประเมินองค์กรสำหรับการปรับปรุงขององค์กรในการเข้ามาตรฐานจาก ISO27001:2013 เป็นมาตรฐาน ISO27001:2022
3. เพื่อทราบถึงปัญหาและข้อผิดพลาดที่เกิดขึ้นภายในองค์กรสำหรับการปรับปรุงให้เข้าสู่มาตรฐาน ISO27001:2022 และปรับปรุงแก้ไขลำดับถัดไป

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

มาตรฐานความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 หรือ Information Security Management System หรือ ISMS เป็นระบบมาตราฐานการจัดการความมั่นคงปลอดภัยของข้อมูล ระบบนี้เกิดขึ้นครั้งแรกโดยสถาบันมาตราฐานแห่งประเทศอังกฤษ (British Standards Institution: BSI) ต่อมาได้ออกมาตราฐานที่เกี่ยวข้องกัน โดยเน้นที่ระบบการจัดการตามแบบวงจรการควบคุมคุณภาพ หรือวงจรเดมมิ่งซึ่งเป็นแนวคิดการพัฒนาคุณภาพงานให้มีความพัฒนาอย่างต่อเนื่องโดยมีชื่อย่อที่เป็นคือ PDCA (Plan, Do, Check, Action) ซึ่งจะทำให้ระบบการจัดการ ความมั่นคง ปลอดภัยของข้อมูล มีความชัดเจนในเชิงปฏิบัติมากขึ้น และสอดคล้องกับระบบ

การจัดการของมาตรฐาน ISO (International Organization for Standardization)โดยระบบนี้มีหลักการเพื่อปกป้อง ข้อมูลที่สำคัญขององค์กรในแง่ของ Confidential (ความลับ) Integrity(ความถูกต้อง) Availability (ความพร้อมใช้) หรือ ที่เราเรียกว่า CIA

ภาพที่ 3.3 แผนการดำเนินงานตามหลัก PDCA

การประเมินความเสี่ยง

การประเมินความเสี่ยงจะแสดงความสัมพันธ์ระหว่างช่องโหว่และผลกระทบที่มีต่อระบบ จากการให้คะแนนแก่ช่องโหว่ และผลกระทบจะทำให้ทราบถึงระดับความเสี่ยงที่อาจเกิดขึ้นโดยทั่วไปการให้คะแนนแก่ช่องโหว่ และผลกระทบจะกระทำโดยเจ้าของระบบซึ่งมีความเข้าใจต่อธุรกิจและความสำคัญของผลกระทบในแต่ละด้าน

ตารางที่ 1 ตารางประเมินความเสี่ยง

ความรุนแรง	คำอธิบาย
Critical	ช่องโหว่ที่สำคัญมีคะแนน CVSS 9.0 – 10.0 พวกเขาสามารถประนีประนอมได้อย่างง่ายดายมัลแวร์หรือการหาประโยชน์ที่เปิดเผยต่อสาธารณะ
High	ช่องโหว่ที่มีความรุนแรงสูงมีคะแนน CVSS อยู่ที่ 7.0 – 8.9 ไม่มีมัลแวร์สาธารณะหรือช่องโหว่ที่เป็นที่รู้จัก

ความรุนแรง	คำอธิบาย
Medium	ช่องโหว่ที่มีความรุนแรงปานกลางมีคะแนน CVSS อยู่ที่ 4.0 – 6.9 และสามารถบรรเทาได้ภายในกรอบเวลาที่ขยายออกไป
Low	ช่องโหว่ที่มีความรุนแรงต่ำถูกกำหนดด้วยคะแนน CVSS 0.1 – 3.9 ช่องโหว่ระดับต่ำบางรายการไม่สามารถบรรเทาได้ง่ายๆ เนื่องจากแอพพลิเคชันและระบบปฏิบัติการปกติ เหล่านี้ควรจัดทำเป็นเอกสารและยกเว้นอย่างถูกต้องหากไม่สามารถแก้ไขได้
Information	ช่องโหว่ของข้อมูลมีคะแนน CVSS ต่ำกว่า 4.0 สิ่งเหล่านี้ถือเป็นความเสี่ยงแต่โดยทั่วไปจะเป็นข้อมูลอ้างอิงสำหรับสถานะและการกำหนดค่าของสินทรัพย์

โดยการแก้ไขช่องโหว่จะเสร็จสิ้นโดยเร็วที่สุดตามแนวทางเหล่านี้

ตารางที่ 2 ตารางระยะเวลาการแก้ไขเมื่อเกิดความเสี่ยง

Device Type	Rating				
	Critical	High	Medium	Low	Information
Internet Facing	30 days	90 days	120 days	180 days	Not Required
Non-Internet Facing	60 days	90 days	120 days	180 days	Not Required
Network Devices	60 days	90 days	120 days	180 days	Not Required

หมายเหตุ: การแก้ไขช่องโหว่ควรตรวจสอบให้แน่ใจว่าเป็นเวอร์ชั่นเสถียรและทดสอบกับสภาพแวดล้อมอื่นที่เกี่ยวข้องไม่ส่งผลกระทบต่อระบบก่อนที่จะนำไปใช้กับสภาพแวดล้อมการผลิต

ขั้นตอนการดำเนินงาน

เมื่อประเมินความเสี่ยงของสารสนเทศ จนทราบว่ามีเรื่องอะไรบ้างที่มีความเสี่ยง ไม่ว่าจะเสี่ยงมากเสี่ยงปานกลางหรือเสี่ยงน้อย ทุกความเสี่ยงต้องมีคำตอบรองรับว่าความเสี่ยงแต่ละระดับจะจัดการอย่างไร โดยทั่วไปความเสี่ยงสูงจะมีการทำแผนงานจัดการความเสี่ยง(Risk Treatment) โดยมีมาตรการต่าง ๆ มาดูแลจัดการโดยการจะทำมาตรฐานของ ISO27001:2013 โดยใช้เกณฑ์ของมาตรฐานต้องเริมดังนี้

1. ศึกษาข้อกำหนด
2. ตั้งทีมงานในการทำระบบ สร้างแผนโครงการ
3. กำหนดขอบข่ายกิจกรรมและอาณาบริเวณ
4. จัดทำรายการกิจกรรม และทรัพย์สินสารสนเทศ
5. ประเมินความเสี่ยง (CIA) จาก
    a. มูลค่าความเสียหาย
    b. ภัยคุกคาม
    c. จุดอ่อน
    d. ความรุนแรง
    e. โอกาสเกิด
6. จัดทำ / กำหนดมาตรการควบคุมความเสี่ยงจาก Annex A
    a. ยอมรับความเสี่ยง
    b. ควบคุมความเสี่ยง
    c. ถ่ายโอนความเสี่ยง
    d. หลีกเลี่ยงความเสี่ยง
7. จัดทำ Statement of Applicability
8. ปฏิบัติตามมาตร การควบคุมความเสี่ยง
9. กำหนดตัวชี้วัด ให้ครบ รอบด้าน
10. วัดผลตามตัวชี้วัด
11. ทำ Internal Audit และ Management Review

ผลการดำเนินงาน

การปรับเปลี่ยนองค์กรให้เป็นไปตามมาตรฐานของ ISO27001:2013 โดยทำตามขั้นตอน วิธีการและใช้เครื่องมือ ที่ได้ศึกษาให้การนำแนวนโยบายดังกล่าวไปปฏิบัติจากการศึกษามาตรฐานต่าง ๆ ของ ISO27001:2013 ประกาศใช้งานในปัจจุบันพบว่าการกำหนดนโยบาย ข้อบังคับ การดูแล การใช้งาน และรูปแบบเอกสารต่าง ๆ ทำให้เห็นว่า Annex A นั่นมีวัตถุประสงค์และเหตุผลต่าง ๆ เพื่อให้สามารถปรับปรุงองค์กรให้มีความปลอดภัยในด้านเทคโนโลยีสารสนเทศตั้งแต่ สถานที่ อุปกรณ์ไฟฟ้า อุปกรณ์อิเล็กทรอนิกส์ และเอกสารต่าง ๆ ที่ผู้ใช้งานหรือองค์กรนั่นเขียนขึ้นมาใช้งานภายใน ภายนอก ลูกค้า รวมถึงพาร์ทเนอร์ขององค์กร ตัวอย่างนโยบายที่นำมาปรับใช้ในองค์กรเช่น

มาตรฐานการเข้ารหัส (Encryption Standard)

วัตถุประสงค์

เพื่อให้ข้อแนะนำในการใช้เทคนิคการเข้ารหัสเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตหรือการปรับเปลี่ยนข้อมูลโดยไม่ได้รับอนุญาต

ขอบเขต

เอกสารนี้ใช้บังคับกับทุกสภาพแวดล้อมของระบบสารสนเทศที่ต้องการดำเนินการเข้ารหัส มีเป้าหมายในการให้ข้อแนะนำในการใช้เทคนิคการเข้ารหัสเพื่อป้องกันการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตและรักษาความถูกต้องของข้อมูล

ระบุไว้ในมาตรฐานว่า

1. Symmetric encryption

ตารางที่ 3 Symmetric encryption

Encryption	1) AES-256

2. Asymmetric encryption (PKI-Public Key Infrastructure)

ตารางที่ 4 Asymmetric encryption

Encryption	1) AES-CBC mode 256 bit 2) RSA-3072 (2048)
Digital Signature	1) ECDSA-256 (Elliptic Curve Digital Signature Algorithm)
Hashing	1) SHA-256
Key Exchange	1) ECDH-256 (Elliptic Curve Diffie-Hellman)

3. Recommended protocol

ตารางที่ 5 Recommended protocol

File transfer	1) SFTP 2) HTTS
Email	1) S/MIME using digital certificates 2) PGP 3) TLS 1.2 or better
Remote-VPN	1) SSLv3 2) IPsec-v2/IPsec-v3 (and key strength refer to no. 1 & 2)
Web application	1) TLS1.2 or better (and key strength refer to no. 1 & 2)

เป็นต้น

สรุปผล และวิเคราะห์

ผลของการศึกษาและปรับปรุงพบว่า สามารถนำแนวทางรักษาความปลอดภัยดังกล่าวไปใช้จัดการความปลอดภัยข้อมูลสารสนเทศในภาพรวมได้อย่างรวดเร็ว สำหรับอุปกรณ์ และระบบที่ติดตั้งใหม่และมีองค์ประกอบคล้ายกันหรือเหมือนกันในการทำงานสามารถนำข้อกำหนดแนวทางปฏิบัติ ช่วยลดเวลาทดสอบและดำเนินการด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ และมีการดำเนินการตามมาตรฐาน ISO27001 ทำให้สามารถพัฒนาและต่อยอดเพื่อรองรับรูปแบบมาตรฐานขั้นต่อไปได้

ข้อจำกัดของการศึกษาและปรับปรุงพบว่าไม่สามารถศึกษาซอฟต์แวร์ต่าง ๆ ที่ติดตั้งใช้งานภายในองค์กรได้อย่างเพียงพอที่จะกำหนดแนวทางรักษาความปลอดภัยสำหรับระบบงาน และมีซอฟต์แวร์จำนวนมากในบางแผนกที่มีการปรับเปลี่ยนการติดตั้งในการใช้งานและถอนการติดตั้งทันทีหลังใช้งาน ข้อจำกัดหรือจุดอ่อนที่สำคัญอีกประการหนึ่ง คือ สินทรัพย์ข้อมูลสารสนเทศที่มีรุ่นผลิตภัณฑ์แตกต่างกันมาก แม้จะเป็นยี่ห้อเดียวกันก็จะไม่สามารถใช้แนวทางรักษาความปลอดภัยข้อมูลสารสนเทศได้ และเลือกประเภทของอุปกรณ์ และระบบไม่เหมาะสม จึงต้องระบุผู้รับรองหรือผู้อนุมัติขึ้นมาเพื่อให้ได้รับการยืนยันว่าเห็นชอบการติดตั้งซอฟต์แวร์นี้

ข้อเสนอแนะ

เอกสารที่สำคัญและมีการพูดถึงบ่อยครั้ง คือ Annex A ที่ใช้ในการตรวจสอบการดำเนินการตามข้อตกลงภายใต้มาตรฐาน ISO/IEC27001 ซึ่งมาตรการควบคุมมีรายละเอียดในการดำเนินการที่ละเอียดอ่อนและเจาะจงไม่ได้ตามที่ต้องการทั้งหมด จึงเห็นควรให้ศึกษาเพื่อนำเอกสาร Annex A มาใช้ให้มีประสิทธิภาพยิ่งขึ้นสำหรับการพัฒนาต่อยอดเพื่อรองรับมาตรฐานฉบับต่อไป

บรรณานุกรม

ภาษาไทย

ภุมวุฒิ วิทวัสสำราญกุล. (2563). *แนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ.* มหาวิทยาลัยธุรกิจบัณฑิตย์, กรุงเทพฯ.

ภาษาต่างประเทศ

Planning for and Implementing ISO27001. (2019). Retrieved from https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001.

Security controls. (2018). Retrieved from https://en.wikipedia.org/wiki/Security_controls.

United States Department of Defense. (2017). *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Washington, D.C.