RESEARCH ARTICLE

Journal of Science Innovation for Sustainable Development
https://ph01.tci-thaijo.org/index.php/JSISD/index

A Gap Analysis of Compliance with Information Security Measures against ISO/IEC 27001:2022 and Technical Vulnerability Assessment Companies A

Rungtawan Prasanit[1], Supawat Seawue[1], Narin Panawas[1,*], Chiraphorn Chomyim[1]

ABSTRACT

This project aimed to evaluate the compliance of information security measures against ISO/IEC 27001:2022 standards and conduct technical vulnerability assessments of the operating system and application programs of Company A. Study user satisfaction with the system, employing a 10-step methodology and utilizing tools such as OpenVAS for vulnerability assessment and a satisfaction assessment questionnaire. The sample group comprises 3 system administrators, selected through a targeted approach. The findings reveal that Objective 1 has been achieved, and overall user satisfaction ratings are good, with an average score of 4.33 and a standard deviation of 0.57.

Keywords: Information security, ISO/IEC standards, Technical vulnerabilities of operating systems

Published Online: 31 May 2024
ISSN: 2730-3829

Rungtawan Prasanit[1]
[1]Faculty of Information Technology, Sripatum University at Chonburi (64704955@chonburi.spu.ac.th)

Supawat Seawue[1]
[1]Faculty of Information Technology, Sripatum University at Chonburi (64709025@chonburi.spu.ac.th)

Narin Panawas[1,*]
[1]Faculty of Information Technology, Sripatum University at Chonburi (narin.pa@chonburi.spu.ac.th)

Chiraphorn Chomyim[1]
[1]Faculty of Information Technology, Sripatum University at Chonburi (chiraphorn.ch @chonburi.spu.ac.th)

[*]*Corresponding Author*

Received date: 21 March 2023
Revised date: 7 May 2024
Accepted date: 16 May 2024

RESEARCH ARTICLE

Journal of Science Innovation for Sustainable Development
https://ph01.tci-thaijo.org/index.php/JSISD/index

การตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 และการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการบริษัท A

รุ้งตะวัน ประสนิท[1], ศุภวัฒน์ แซ่วื้อ[1], นรินทร์ พนาวาส[1,*], จิราภรณ์ ชมยิ้ม[1]

บทคัดย่อ

โครงงานนี้มีวัตถุประสงค์เพื่อ 1) ตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 และการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการและโปรแกรมแอพพลิเคชั่น บริษัท A และ2) ศึกษาความพึงพอใจของผู้ใช้งานระบบ โดยมีวิธีการศึกษา 10 ขั้นตอน เครื่องมือที่ใช้ในการศึกษา ประกอบด้วย OpenVAS และแบบประเมินความพึงพอใจ กลุ่มตัวอย่างที่ใช้ คือกลุ่มผู้ดูแลระบบ จำนวน 3 คน ได้มาด้วยวิธีการแบบเจาะจง ผลการศึกษาพบว่า ตอบวัตถุประสงค์ที่ 1 และผลจากการประเมินความพึงพอใจโดยรวมอยู่ในระดับดี ได้ค่าเฉลี่ยรวมเท่ากับ 4.33 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.57

คำสำคัญ: ความมั่นคงปลอดภัยสารสนเทศ, มาตรฐาน ISO/IEC, ช่องโหว่ทางเทคนิคของระบบปฏิบัติการ

Published Online: 31 พฤษภาคม 2567
ISSN: 2730-3829

รุ้งตะวัน ประสนิท[1]
[1]คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
(64704955@chonburi.spu.ac.th)

ศุภวัฒน์ แซ่วื้อ[1]
[1]คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
(64709025@chonburi.spu.ac.th)

นรินทร์ พนาวาส[1,*]
[1]คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
(narin.pa@chonburi.spu.ac.th)

จิราภรณ์ ชมยิ้ม[1]
[1]คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
(chiraphorn.ch @chonburi.spu.ac.th)

[*]*Corresponding Author*

Recevived date: 21 มีนาคม 2566
Revised date: 7 พฤษภาคม 2567
Accepted date: 16 พฤษภาคม 2567

1. บทนำ

บริษัท A ในนิคมอมตะชลบุรี มีการใช้งานเทคโนโลยีสารสนเทศจำนวนมากเพื่อใช้ในการดำเนินงาน และเป็นบริษัทผู้ผลิตชิ้นส่วนยานยนต์ให้กับบริษัทผู้ผลิตรถยนต์ชั้นนำทั้งในและต่างประเทศ ประกอบกับเทคโนโลยีมีความก้าวหน้าอย่างรวดเร็วก่อให้เกิดความเสี่ยง และภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าองค์กรมีการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่เหมาะสม การตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 และการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการ และโปรแกรมแอปพลิเคชันจะช่วยให้องค์กรมีความตระหนักและทราบถึงช่องโหว่และแนวทางปรับปรุงขององค์กร ทั้งในด้านมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ และช่องโหว่ทางเทคนิคของระบบสารสนเทศ

คณะผู้จัดทำได้จัดทำโครงการตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 และการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการขึ้น เพื่อห้ฝ่ายเทคโนโลยีสารสนเทศได้นำผลลัพธ์จากการดำเนินงานนี้ ไปใช้ในการพัฒนาปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ และแก้ไขช่องโหว่ทางเทคนิคของระบบสารสนเทศ ให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001 ซึ่งเป็นมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สากลให้การยอมรับทั่วโลก รวมถึงสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง ทำให้องค์กรมีความพร้อมในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และตอบสนองต่อสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศได้อย่างเหมาะสม นอกจากนี้ยังช่วยสร้างความเชื่อมั่น และภาพลักษณ์ชื่อเสียงที่ดีต่อลูกค้าและผู้ที่มีส่วนเกี่ยวข้อง และสนับสนุนการปรับปรุงต่อเนื่องของระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

วัตถุประสงค์

1. ตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 และการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการ และโปรแกรมแอปพลิเคชัน บริษัท A ในนิคมอมตะชลบุรี
2. ศึกษาความพึงพอใจของผู้ใช้งานระบบ

2. วิธีการวิจัย

การตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 และการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการ และโปรแกรมแอปพลิเคชัน บริษัท A ในนิคมอมตะ ชลบุรี ภายในระยะเวลา 60 วัน ดัง Figure 1 มีดังนี้

1) แผนการศึกษาเกี่ยวกับการดำเนินงาน

1. ศึกษาบริบทขององค์กรเพื่อให้ทราบถึงลักษณะขององค์กร เช่น ขนาดขององค์กร เป้าหมายในการดำเนินกิจกรรมธุรกิจ โครงสร้างองค์กร และสภาพแวดล้อมภายในและภายนอกองค์กร เป็นต้น ซึ่งจำเป็นในการกำหนดความต้องการในการปรับปรุงความมั่นคงปลอดภัยขององค์กร
2. ศึกษานโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศองค์กร เพื่อตรวจสอบความสอดคล้องของนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรกับมาตรฐาน ISO/IEC 27001
3. ศึกษาระบบสารสนเทศ และระบบเครือข่ายขององค์กร (network diagram, system diagram, site tour, interview) ขั้นตอนการเตรียมความพร้อม และศึกษาโครงสร้างของระบบเครือข่าย และระบบสารสนเทศในองค์กรเพื่อให้เข้าใจถึงทราบถึงสภาพแวดล้อมภายในองค์กร วิเคราะห์ความเป็นไปได้ และความเสี่ยงในการดำเนินงาน

4. จัดทำแผนการดำเนินงาน ศึกษาและจัดเตรียมเครื่องมือสำหรับการดำเนินงาน (audit checklist, vulnerability assessment tool)
5. นำเสนอแผนการดำเนินงานและร่วมกันวางแผนจัดการความเสี่ยงที่อาจเกิดขึ้นระหว่างดำเนินงาน
6. ดำเนินการตรวจประเมินตามแผน
7. รวบรวม และวิเคราะห์ผลการตรวจประเมิน
8. จัดทำรายงานผลตรวจการประเมิน
9. นำเสนอผลการตรวจประเมิน

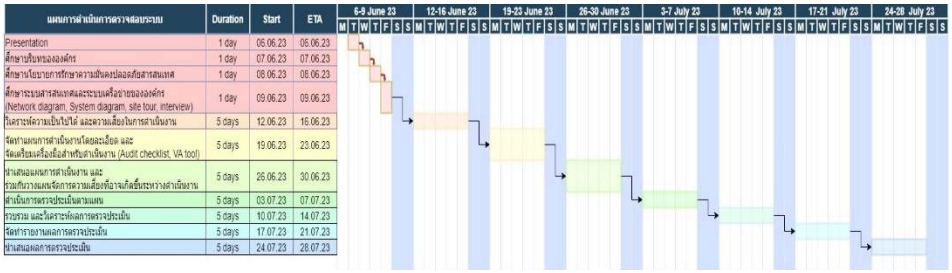

Figure 1 Operational Study Plan

2) การศึกษาทฤษฎีที่เกี่ยวข้องกับงานวิจัย

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่ได้รับการยอมรับในระดับสากล ซึ่งเผยแพร่โดย International Organization for Standardization (ISO) และ International Electrotechnical Commission (IEC) เป็นมาตรฐานสากลที่ได้กำหนดแนวทางดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของหน่วยงาน โดยมีกระบวนการบริหารจัดการสารสนเทศที่มีความสำคัญขององค์กรให้มีความมั่นคงปลอดภัยตามหลัก CIA (ความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ดัง Figure 2 ซึ่งมีแนวทางการปฏิบัติตามขั้นตอนของกระบวนการดังนี้ เริ่มตั้งแต่ทำการวิเคราะห์และประเมินความเสี่ยง เพื่อให้ทราบว่าสารสนเทศใดที่มีความสำคัญต่อการดำเนินธุรกิจขององค์กรโอกาสที่จะเกิดความเสี่ยง และความเสียหายอันส่งผลกระทบต่อการดำเนินธุรกิจขององค์กรจากภัยคุกคามทั้งภายใน และภายนอกองค์กรกับสารสนเทศนั้นมีมากน้อยเพียงใด และมีแนวทางบริหารจัดการในการป้องกันความเสี่ยงดังกล่าว โดยจำเป็นต้องจัดลำดับความสำคัญของความเสี่ยงทั้งหมดที่พบและพิจารณาจัดลำดับความสำคัญ จากนั้นจึงดำเนินตามวงจร P (Plan หรือการวางแผน) D (Do หรือการประยุกต์ใช้หรือ การดำเนินการ) C (Check หรือการตรวจสอบ) A (Action หรือการบำรุงรักษา หรือการปรับปรุง) โดยเริ่มจากจากทำการออกแบบระบบบริหารจัดการ ซึ่งในที่นี่ หมายถึง กระบวนการที่เปรียบเสมือนเป็นเครื่องมือในการรักษาความมั่นคงปลอดภัย รวมถึงการพัฒนาขั้นตอนปฏิบัติเพื่อให้เกิดกระบวนการป้องกันและรักษาความมั่นคงปลอดภัยของสารสนเทศที่ใช้ในการดำเนินธุรกิจขององค์กรอย่างเหมาะสม โดยหลังจากที่ได้ดำเนินการตามระบบที่ได้วางแผนไว้ จากนั้นทำการตรวจสอบการดำเนินงานว่ามีการดำเนินงานครบถ้วนตรงตามวัตถุประสงค์และแผนที่กำหนดไว้ อีกทั้งยังต้องพิจารณาหาจุดอ่อนที่อาจเกิดขึ้นเมื่อได้ข้อมูลครบถ้วน แล้วจึงนำมาพิจารณาทำการบำรุงรักษากระบวนการเดิมที่มีประสิทธิภาพเหมาะสมเพียงพอ และทำการปรับปรุงกระบวนการที่ยังมีจุดอ่อนให้ดีขึ้น เพื่อทำให้ระบบบริหารจัดการที่ประยุกต์ใช้ในองค์กรนั้นมีคุณภาพ ทันสมัย และเหมาะสมอยู่เสมอ (Panawas, 2008)

Journal of Science Innovation for Sustainable Development
https://ph01.tci-thaijo.org/index.php/JSISD/index

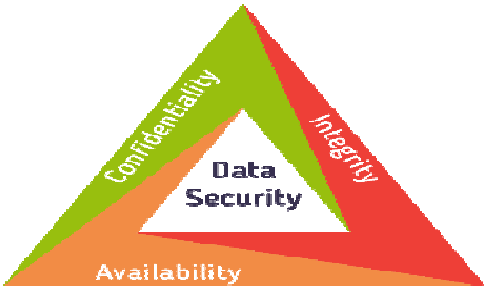

Figure 2 CIA principles

Retrieved from: https://devopedia.org/information-security-principles

โครงสร้างโดยรวมของมาตรฐาน ISO/IEC 27001 เวอร์ชัน 2013 ก่อนได้รับการปรับปรุงแบ่งเนื้อหาออกเป็น 14 หัวข้อใหญ่ (Domain) ซึ่งแต่ละหัวข้อ ประกอบด้วยวัตถุประสงค์จำนวนแตกต่างกัน รวมแล้วจำนวน 35 วัตถุประสงค์ (Control objectives) (ISO27001security, 2022) หลังจากมีการปรับปรุงโครงสร้างใหม่ของมาตรฐาน ISO/IEC 27001 เวอร์ชัน 2022 ได้ปรับปรุงแบ่งเนื้อหาออกเป็น 2 ส่วน คือ ส่วนที่เป็นข้อกำหนดในการจัดตั้ง ดำเนินการ และบำรุงรักษาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และส่วนที่เป็นมาตรการควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศทั้งหมด 93 มาตรการ โดยแบ่งออกเป็น 4 ด้าน ได้แก่ มาตรการด้านองค์กร มาตรการด้านบุคคลากร มาตรการเชิงกายภาพ และมาตรการด้านเทคโนโลยี ดัง Figure 3 นอกจากนี้มาตรฐาน ISO/IEC 27001:2022 จะมุ่งเน้นที่การป้องกัน ตรวจจับ และตอบสนองต่อการโจมตีทางไซเบอร์ (Cyberattack) (Chotimaha, 2018) ควบคู่ไปกับการการปกป้องข้อมูลตามกรอบทำงานของ NIST Cybersecurity Framework (Averyitech, 2021)

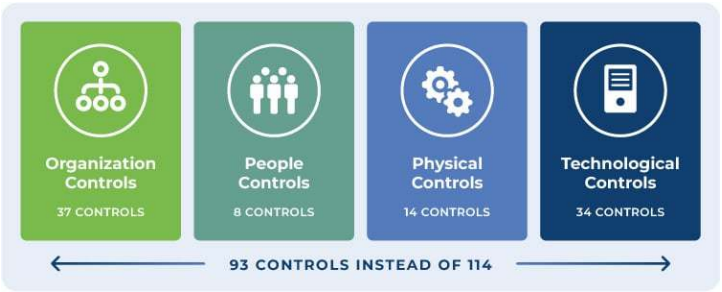

Figure 3 Structure ISO/IEC 27001:2022

Retrieved from: https://www.advantio.com/blog/whats-new-in-iso/iec-27002-2022-updates

NIST Cybersecurity Framework หรือเรียก NIST CSF Version 1.1 เป็น Framework กรอบมาตรฐานสากลที่ทุกองค์สามารถนำมาปรับใช้ให้เหมาะสม เพื่อบริหารระบบโครงสร้างความมั่นคงปลอดภัยสารสนเทศขององค์กร เผยแพร่โดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ของสหรัฐอเมริกา โดยมีวัตถุประสงค์

1) อธิบายมาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบัน
2) อธิบายมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป้าหมาย
3) ระบุและจัดลำดับความสำคัญของโอกาสในการปรับปรุง
4) ประเมินความคืบหน้าไปสู่สถานะเป้าหมาย
5) สื่อสารระหว่างผู้มีส่วนได้ส่วนเสียภายในและภายนอกเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

ซึ่งประเทศไทยนั้นได้มีการนำ NIST Cybersecurity Framework มาเป็นต้นแบบส่วนหนึ่งในการจัดทำ พ.ร.บ .การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 การนำ NIST CSF มาประยุกต์ใช้บริหารความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องดำเนินการ 5 ฟังก์ชันหลัก ดังนี้

1) Identify ระบุและเข้าใจสภาพแวดล้อมของตนเองทรัพย์สินและความเสี่ยงที่มี

2) Protect หาแนวทางที่เหมาะสมในการปกป้องทรัพย์สิน

3) Detect มีการตรวจจับและเฝ้าระวังภัยคุกคามที่อาจจะเกิดขึ้น

4) Response เมื่อพบภัยคุกคามสามารถที่จะตอบสนองได้ทันท่วงที เพื่อลดผลกระทบหรือจำกัดความเสียหายให้อยู่ในวงแคบ

5) Recover สามารถกู้คืนระบบขึ้นมาให้บริการตามปกติได้อย่างรวดเร็วภายใต้งบประมาณและหลักการบริหารความเสี่ยงขององค์กร

การตรวจสอบช่องโหว่ทางเทคนิค (Vulnerability assessment) เป็นกระบวนการตรวจสอบและวิเคราะห์ช่องโหว่ที่อาจเกิดขึ้นในระบบสารสนเทศ หรือ โครงสร้างเครือข่ายขององค์กรที่อาจเกิดขึ้นในระบบสารสนเทศ ซึ่งอาจเป็นช่องโหว่ทางซอฟต์แวร์ เครือข่าย หรือการกำหนดค่าที่ไม่ถูกต้อง ทำให้เกิดความเสี่ยงที่อาจถูกใช้ในการโจมตีระบบเพื่อระบุปัญหาความมั่นคงปลอดภัย และ จุดอ่อนที่อาจถูกโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาตโดยมุ่งหวังในการระบุช่องโหว่ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบและข้อมูลสำคัญขององค์กรโดยกระบวนการ Vulnerability Assessment จะใช้เครื่องมือ Vulnerability Scanning Tool เพื่อตรวจสอบความมั่นคงปลอดภัยระบบเครือข่าย ค้นหาช่องโหว่ที่ใช้งานภายในองค์กร เช่น ระบบปฏิบัติการซอฟต์แวร์ (OS) อุปกรณ์ Network อุปกรณ์ Security เป็นต้น โดยการระบุระดับความรุนแรงของช่องโหว่ เป็นต้น จะอ้างอิงตาม CVE (เว็บไซต์รวบรวมชื่อและคำอธิบายช่องโหว่ ดัง Figure 4 และ CVSS (เว็บไซต์ที่วิเคราะห์การโจมตีช่องโหว่และประเมินคะแนนระดับความรุนแรง ดัง Figure 5 โดยทั้งสองเว็บไซต์อยู่ในการกำกับและความดูแลโดยกระทรวงความมั่นคงแห่งมาตุภูมิของรัฐบาลกลางแห่งประเทศสหรัฐอเมริกา และกำกับดูแลโดยองค์กรไม่แสวงหาผลกำไร MITRE Corporation ขั้นตอนการทำ Vulnerability Assessment ดังนี้

1) Vulnerability Identification Testing ขั้นตอนการร่างลิสต์ช่องโหว่แอปพลิเคชันอย่างครอบคลุม วิเคราะห์ระบบ เพื่อทำการทดสอบความมั่นคงปลอดภัยของแอปพลิเคชัน เซิร์ฟเวอร์ หรือ ระบบต่าง ๆ

2) Vulnerability Analysis การระบุต้นตอสาเหตุ หาจุดกำเนิดช่องโหว่ที่เกิดขึ้นจากในการวิเคราะห์ในขั้นตอนแรก

3) Risk Assessment การจัดลำดับความสำคัญของช่องโหว่ ระบุความร้ายแรงแต่ละช่องโหว่ที่พบ

4) Remediation การพยายามร่วมกันระหว่าง ทีม security ผู้เชี่ยวชาญ security และทีม operator เพื่อกำหนดวิธีการและแนวทางแก้ไขช่องโหว่แต่ละจุด

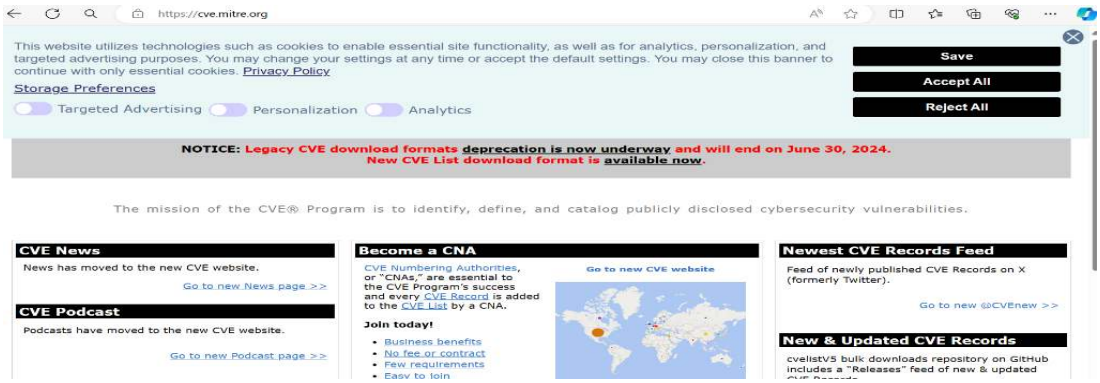

Figure 4 Website Page Common Vulnerabilities and Exposures (CVE)

Retrieved from: https://www.cve.org

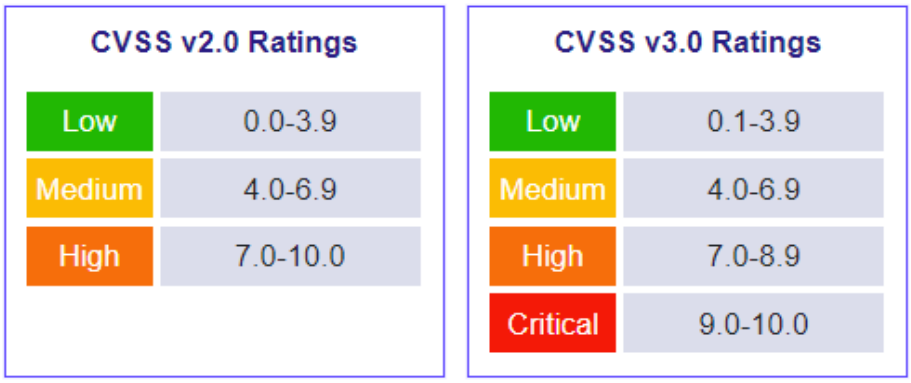

Figure 5 Scoring criteria Common Vulnerability Scoring System (CVSS)

Retrieved from: https://forum.huawei.com/enterprise/en/The-Overview-of-Common-Vulnerability-Scoring-System-CVSS-PART-04/thread/667251190766911488-667213854934970368

3) เครื่องมือที่ใช้ในกระบวนการประเมินช่องโหว่

OpenVAS (Open Vulnerability Assessment System) เป็นโปรแกรมโอเพนซอร์สที่นิยมใช้ในการทดสอบสแกน และ ตรวจสอบระบบเครือข่ายเพื่อค้นหาช่องโหว่ที่เปิดเผย หรือ มีความเสี่ยงต่อความมั่นคงปลอดภัย ดัง Figure 6 โดยสามารถสแกนแบบเครือข่าย และ เครื่องคอมพิวเตอร์รายบุคคล ซึ่งสามารถระบุรายละเอียดเกี่ยวกับช่องโหว่ เช่น ระดับความรุนแรง ข้อมูลการแก้ไขแนะนำ และการสร้างรายงานที่ช่วยในการวิเคราะห์และจัดการช่องโหว่ เป็นต้น โดยการใช้โพรโทคอล ที่มีรูปแบบการส่งข้อมูลแบบเป็นมาตรฐาน OMP (OpenVAS Management Protocol) เพื่อการสื่อสารระหว่างเครื่องมือ OpenVAS Client และ OpenVAS Scanner ทำให้ผู้ใช้สามารถจัดการและ ควบคุมกระบวนการสแกนช่องโหว่ได้ ทำให้ OpenVAS เป็นเครื่องมือที่สำคัญสำหรับผู้ดูแลระบบ และ การรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร (Stefan, 2022)

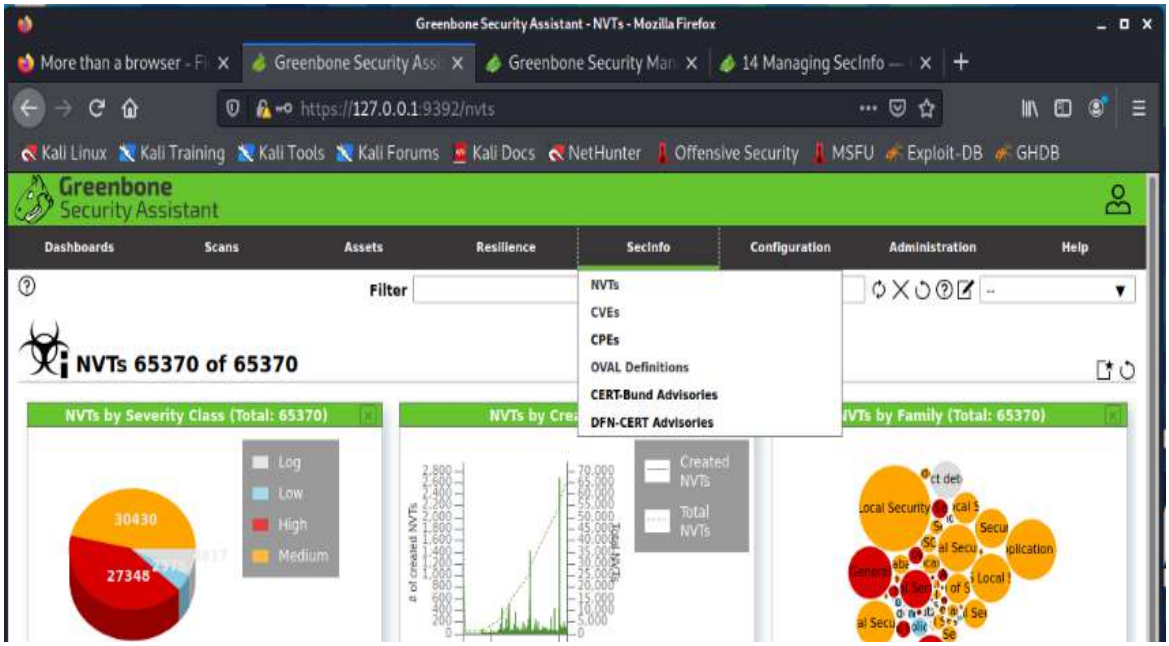

Figure 6 Program screen Open VAS

Retrieved from: https://stafwag.github.io/blog/blog/2021/03/07/openvas-first-scan

3. ผลการวิจัย

การดำเนินการตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 จาก Table 1 และ Figure 7 พบว่ามาตรการด้านองค์กร จำนวน 37 มาตราการ มีระดับความสอดคล้องกับข้อกำหนด เพียง 16% จากการผ่านมาตรฐาน 80% แสดงให้เห็นว่า องค์กรขาดและต้องปรับปรุงมาตรการควบคุมด้านองค์กร เนื่องมาจากองค์กรยังขาดในด้านข้อกำหนดด้านความมั่นคงปลอดภัยข้อมูลที่สำคัญหลายประการ ส่วนที่สำคัญ คือ การกำหนดนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร ซึ่งเป็นส่วนสำคัญในการตรวจประเมิน มาตรการด้านบุคคลากร จำนวน 8 มาตราการ มีระดับความสอดคล้องกับข้อกำหนด 88% ถือว่าผ่านมาตราฐาน เนื่องจากองค์กรมีมาตรการควบคุมด้านบุคคลากรที่มีประสิทธิภาพในระดับสูง องค์กรมีมาตรการควบคุมด้านความมั่นคงปลอดภัยข้อมูลพนักงานที่เหมาะสมและมีประสิทธิภาพ องค์กรควรดำเนินการปรับปรุงระบบ ISMS อย่างต่อเนื่อง เพื่อรักษาระดับประสิทธิภาพ และเพื่อปกป้องข้อมูลสำคัญขององค์กร มาตรการเชิงกายภาพ มาตราการมีระดับความสอดคล้องกับข้อกำหนด 68% อยู่ในเกณฑ์ปานกลาง ที่องค์กรต้องมีมาตรการควบคุมด้านกายภาพที่เพิ่มมากขึ้นในการปกป้องทรัพย์สิน และข้อมูลทางกายภาพ และมาตรการด้านเทคโนโลยี มาตราการมีระดับความสอดคล้องกับข้อกำหนด 57% ถือว่าอยู่ในเกณฑ์ที่ต่ำกว่าเกณฑ์มาตรฐาน โดยองค์กรต้องมีมาตรการควบคุมด้านเทคโนโลยีที่มากเพียงพอในการปกป้องข้อมูลและระบบสารสนเทศ องค์กรควรดำเนินการปรับปรุงมาตรการควบคุมด้านเทคโนโลยีของตนอย่างต่อเนื่องเพื่อรักษาระดับประสิทธิภาพ และเพื่อปกป้องข้อมูลสำคัญขององค์กร

Table 1 The Consistency of Information Security Measures

ISOIEC 27001 Audit	% Compliance	Status) 80 %)
Annex A (A.5) Organizational controls	16	Not Pass
Annex A (A.6) People control	88	Pass
Annex A (A.7) Physical controls	68	Not Pass
Annex A (A.8) Technological controls	57	Not Pass

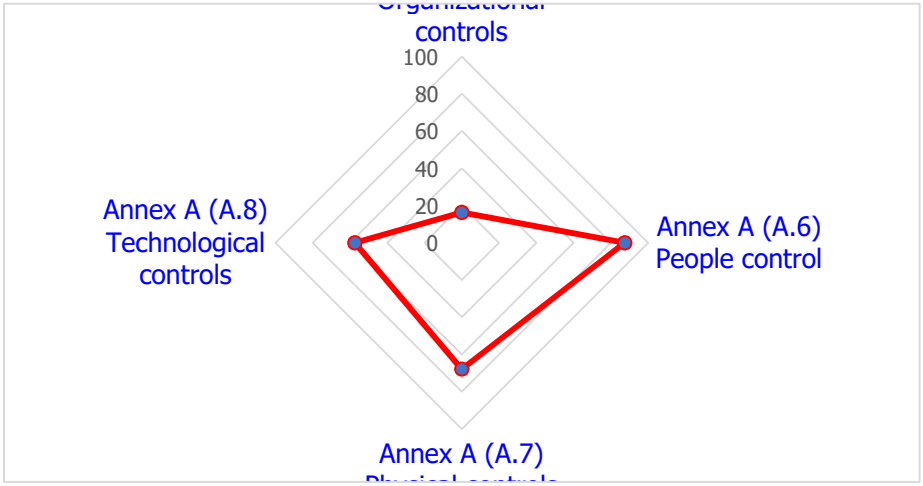

Figure 7 The results of the assessment for compliance with information security measures according to ISO/IEC 27001 standards

จากการดำเนินการตรวจสอบหาช่องโหว่ทางเทคนิคของระบบปฏิบัติการ และโปรแกรมแอปพลิเคชันบนเครื่องแม่ข่าย จำนวน 4 เครื่อง โดยใช้โปรแกรม OpenVAS ในการตรวจสอบ พบว่า เครื่องแม่ข่ายที่ 1 ชื่อ Active Directory เป็นจุดศูนย์กลางในการจัดการ และควบคุมสิทธิ์ในเครือข่ายที่มีความสำคัญในการป้องกันการเข้าถึงที่ไม่

เหมาะสม และการละเมิดความมั่นคงปลอดภัยของข้อมูลในองค์กร เมื่อทำตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการ Active Directory ขององค์กร ได้ค้นพบช่องโหว่ในระดับ "Medium" ที่สำคัญที่สุด คือ เกี่ยวกับการใช้โพรโทคอล SSL/TLS เวอร์ชันเก่าที่ไม่เป็นที่นิยมแล้ว และ ใบรับรองที่ถูกเซ็น ด้วยอัลกอริทึมเซ็น ที่อ่อนแอ หรือไม่เหมาะสม เครื่องแม่ข่ายที่ 2 ชื่อ SQL Server พบว่า มี ช่องโหว่ในระดับ "High" จำนวน 1 รายการ คือ ช่องโหว่ SSL/TLS หมายถึง การรายงานความเสี่ยงจากชุดรหัส (Cipher suites) ที่ใช้ในการเข้ารหัสข้อมูลในระบบ SSL/TLS ที่เป็นเรื่องน่ากังวลมากที่สุด อาจ มีผลกระทบต่อความมั่นคงปลอดภัยของระบบ และ อาจทำให้เกิดช่องโหว่ในการเชื่อมต่อแบบ SSL/TLS ที่ไม่ปลอดภัย ซึ่ง เป็นสิ่งที่ต้องดำเนินการแก้ไขและปรับปรุง เพื่อ เพิ่มความมั่นคงปลอดภัยให้กับระบบในอนาคต เครื่องแม่ข่ายที่ 3 ชื่อ Antivirus Server ขององค์กรได้ค้นพบช่องโหว่ในระดับ "High" ที่มีความเสี่ยงมากที่สุดในส่วนของโปรแกรม Apache HTTP Server Apache Tomcat และ OpenSSL ที่ทำหน้าที่ให้การให้บริการระบบเว็บไซต์ ซึ่งอาจทำให้ระบบอยู่ในสภาวะที่ไม่ปลอดภัยและเสี่ยงต่อการโจมตี และ ขาดความมั่นคงปลอดภัยของข้อมูลในระบบ และสุดท้ายเครื่องแม่ข่ายที่ 4 ชื่อ Alfresco พบช่องโหว่ที่มีความเสี่ยงในระดับ "High" คือ ช่องโหว่ในการเปิดเผยข้อมูลใน /WEB-INF/ ของ Alfresco ช่องโหว่ในการเข้าถึงและโจมตีด้วย Brute Force ช่องโหว่ใน SSL/TLS และช่องโหว่ในระบบจัดการ Webmin ที่มีผลกระทบทำให้สามารถให้ผู้ไม่หวังดีสามารถเข้าใช้งานผ่านหน้าเว็บไซต์ ดัง Figure 8 และ Figure 9 แนวทางในการแก้ไข และ ป้องกันช่องโหว่ เริ่มจากเครื่องแม่ข่าย Alfresco เครื่องแม่ข่าย Antivirus Server เครื่องแม่ข่าย Alfresco เครื่องแม่ข่าย SQL Server และเครื่องแม่ข่าย Active Directory ตามลำดับ พร้อมสร้างความตระหนักให้กับบุคลากรในองค์กรตระหนักถึงการรักษาความมั่งคงปลอดภัยสารสนเทศเพื่อช่วยส่งเสริมให้องค์กรปฏิบัติตามให้สอดคล้องกับมาตรฐาน ISO/IEC 27001 เพื่อเตรียมความพร้อมในการเข้าสู่การตรวจรับมาตรฐาน ISO/IEC 27001 (Harangsee, 2020)

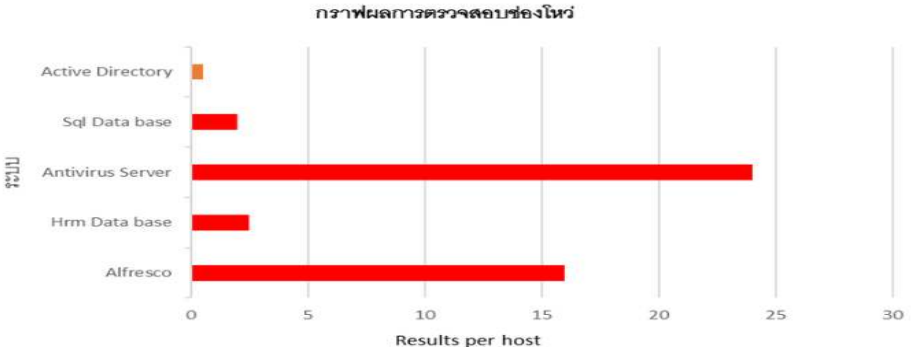

Figure 8 Vulnerability inspection results

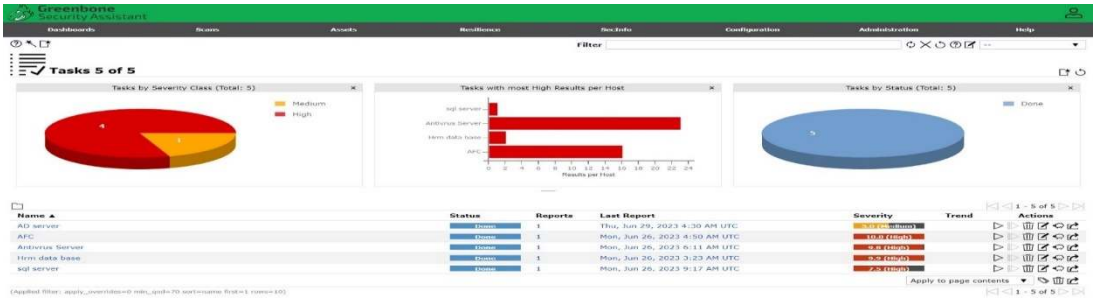

Figure 9 Example of an OpenVAS program screen that lists the Vulnerability Assessment Report

4. สรุปผลการวิจัย

การประเมินผลความพึงจากการตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 และการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการ บริษัท A ผู้ตอบแบบสอบถาม เป็นกลุ่มผู้ดูแลระบบเครือข่าย จำนวน 3 คน คณะผู้จัดทำได้ใช้ แบบสอบถามในการประเมินความพึงพอใจ โดยแบ่งเป็น 5 ระดับ ดังนี้

ระดับ 5 หมายถึง ดีมาก

ระดับ 4 หมายถึง ดี

ระดับ 3 หมายถึง ปานกลาง

ระดับ 2 หมายถึง น้อย

ระดับ 1 หมายถึง ต้องปรับปรุง

กำหนดค่าเฉลี่ยจากการประเมินผลความพึงพอใจ ดังนี้

คะแนน 4.50 - 5.00 หมายถึง ดีมาก

คะแนน 3.50 - 4.49 หมายถึง ดี

คะแนน 2.50 - 3.49 หมายถึง ปานกลาง

คะแนน 1.50 - 2.49 หมายถึง น้อย

คะแนน น้อยกว่า 1.49 หมายถึง ต้องปรับปรุง

Table 2 Results of satisfaction assessment of information technology system inspection guidelines

Satisfaction Evaluation	$\overline{x}$	SD	Quality Level
Standards and Content			
ISO/IEC 27001 Compliant with ISO/IEC 27001 standards	4.33	0.57	Good
Appropriate for the Organization	4.33	0.57	Good
Clear and easy to Understand	4.33	0.57	Good
Implementation			
Can be practically applied to inspection work	4.33	0.57	Good
It can be practically applied to review and control inspection work	4.33	0.57	Good

จาก Table 2 พบว่า ผลการวิเคราะห์ความพึงพอใจ ต่อแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 จากกลุ่มผู้ดูแลระบบเครือข่าย จำนวน 3 คน สามารถสรุปผลความพึงพอใจแต่ละส่วน และสรุปผลความพึงพอใจโดยรวม ดังนี้

ส่วนที่ 1 ความพึงพอใจด้านมาตรฐานและเนื้อหาแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 ได้ค่าเฉลี่ยรวมเท่ากับ 4.33 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.57 สรุปผลการประเมินได้ว่าความพึงพอใจด้านมาตรฐานและเนื้อหาแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 มีคุณภาพอยู่ในระดับดี

ส่วนที่ 2 ความพึงพอใจด้านการประยุกต์แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 ได้ค่าเฉลี่ยรวมเท่ากับ 4.33 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.57 สรุปผลการประเมินได้ว่าความพึงพอใจด้านการประยุกต์แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 มีคุณภาพอยู่ในระดับดี

5. กิตติกรรมประกาศ

ขอขอบคุณคณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี และบริษัท A ในนิคมอมตะชลบุรี ที่อำนวยความสะดวก และช่วยเหลือในการทำวิจัยครั้งนี้

ผลประโยชน์ทับซ้อน

ผู้เขียนขอยืนยันว่างานวิจัยนี้ไม่มีความขัดแย้งทางผลประโยชน์ที่เกี่ยวข้องกับบทความนี้กับบทความอื่น ๆ

REFERENCES

Averyitech. (2021). *NIST cybersecurity framework*. Retrieved from https://www.averyittech.com/NIST_Cybersecurity_Framework

Advantio Ltd. (2023). ISO/IEC 27002:2022. Retrieved from https://www.advantio.com/blog/whats-new-in-iso/iec-27002-2022-updates

Chotimaha, P. (2018). *Guidelines for internal audit according to ISO 27001:2013 standard: A case study of the Expressway Authority of Thailand* (Master's thesis). Sripatum University, Faculty of Information Technology, Information Technology

CVE Program Mission. (2023). Retrieved from https://www.cve.org

Information Security Principles. (2023). Retrieved from https://devopedia.org/information-security-principles

Harangsee, B. (2020). *ISO/IEC 27001:2022 standard Thai version*. Retrieved from https://smartpdpa.gec.co.th/news/6391614101e7e93a1ee6e20a

Huawei Technologies Co., Ltd. (2023). The overview of common vulnerability scoring system. Retrieved from https://forum.huawei.com/enterprise/en/The-Overview-of-Common-Vulnerability-Scoring-System-CVSS-PART-04/thread/667251190766911488-667213854934970368

ISO27001security. (2022). *ISO/IEC 27001:2022*. Retrieved from https://www.iso27001security.com/html/27001.html

OpenVAS on Kali GNU/Linux part 2: First scan. (2023). Retrieved from https://stafwag.github.io/blog/blog/2021/03/07/openvas-first-scan

Panawas, N. (2008). *Security measures on information network systems for organizations*. Retrieved from http://dspace.spu.ac.th/handle/123456789/1016

Stefan. (2022). *Install OpenVAS on Kali Linux – Easy step-by-step tutorial*. Retrieved from https://www.ceos3c.com/security/install-openvas-kali-linux