แนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศ โดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ

ภุมวุฒิ วิทวัสสำราญกุล

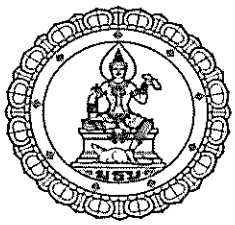
สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมเว็บและการพัฒนาแอปพลิเคชันบนอุปกรณ์พกพา
วิทยาลัยครีเอทีฟ ดีไซน์ แอนด์ เอ็นเตอร์เทนเมนต์เทคโนโลยี
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2563

A Practical Approach to Establish Information Security System using Information Security Management System framework

Poomwoot Vittavassamrankul

Thematic Paper Submitted in Partial Fulfillment of the Requirements for the Degree of Master in Web Engineering and Mobile Application Development, College of Creative Design and Entertainment Technology, Dhurakij Pundit University

2020



ใบรับรองสารนิพนธ์

วิทยาลัยครีเอทีฟดีไซน์ แอนด์ เอ็นเตอร์เทนเมนต์เทคโนโลยี มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา วิทยาศาสตรมหาบัณฑิต

หัวข้อสารนิพนธ์	แนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ
เสนอโดย	ภุมวุฒิ วิทวัสสำราญกุล
สาขาวิชา	วิศวกรรมเว็บและการพัฒนาแอปพลิเคชันบนอุปกรณ์พกพา
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร.วรสิทธิ์ ชูชัยวัฒนา

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบสารนิพนธ์แล้ว

.....ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.วิลาวัลย์ อินทร์ชำนาญ)

.....กรรมการและอาจารย์ที่ปรึกษาสารนิพนธ์

(ผู้ช่วยศาสตราจารย์ ดร.วรสิทธิ์ ชูชัยวัฒนา)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.อรวรรณ อิ่มสมบัติ)

วิทยาลัยครีเอทีฟดีไซน์ แอนด์ เอ็นเตอร์เทนเมนต์เทคโนโลยี

..... คณบดี

(ผู้ช่วยศาสตราจารย์ ดร.วิลาวัลย์ อินทร์ชำนาญ)

วันที่ 26 เดือน พฤษภาคม พ.ศ. 2563

หัวข้อสารนิพนธ์	แนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศ โดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ
ชื่อผู้เขียน	ภุมวุฒิ วิทวัสสำราญกุล
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร. วรสิทธิ์ ชูชัยวัฒนา
สาขาวิชา	วิศวกรรมเว็บและการพัฒนาแอปพลิเคชันบนอุปกรณ์พกพา
ปีการศึกษา	2562

บทคัดย่อ

สำนักงานศาลยุติธรรมอยู่ระหว่างจัดทำแนวนโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศ โดยอ้างอิงจากมาตรฐาน ISO/IEC 27001 และเพื่อพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่ายตามกระบวนการปฏิบัติมาตรฐาน จึงแบ่งกลุ่มอุปกรณ์และระบบตามเกณฑ์คุณสมบัติและการทำงาน พื้นที่การเข้าถึงระบบ งานที่ให้บริการ เป็น 7 ประเภท เลือกตัวแทนของแต่ละประเภทเพื่อศึกษาตามกระบวนการจัดการความปลอดภัยข้อมูลสารสนเทศ และกำหนดแนวทางพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศของระบบแต่ละประเภท ผลสรุปดังนี้

1. ระบบโครงสร้างพื้นฐาน (Infrastructure) ตัวแทนคือ ระบบสำรองไฟฟ้า เน้นการแจ้งเตือน เตรียมความพร้อม และมาตรการตอบสนองกรณีไฟฟ้าดับฉุกเฉิน

2. ระบบบริหารจัดการเครือข่าย (Network Management) ตัวแทนคือ ระบบรักษาความปลอดภัยบนเครือข่ายภายใน (Firewall) เน้นการกำหนด Policy ที่เหมาะสม การเฝ้าระวัง กำหนดขั้นตอนปฏิบัติกรณีฉุกเฉิน

3. ระบบงานที่ให้บริการเฉพาะเครือข่ายภายใน (Internal Service) ตัวแทนคือ ระบบสารบัญอิเล็กทรอนิกส์ เน้นให้บริการที่มีเสถียรภาพ ตอบสนองแก้ไขปัญหารวดเร็ว และเข้าถึงได้เฉพาะเครือข่ายภายใน

4. ระบบงานที่ให้บริการผ่านเครือข่ายภายนอก (External Service) คือ ระบบยื่นและส่งคำคู่ความโดยสื่ออิเล็กทรอนิกส์ (e-Filling) เน้นการตรวจสอบสิทธิ์ ความถูกต้องของข้อมูลและการแก้ไขข้อมูลตามสิทธิ์ที่กำหนด ป้องกันการเข้าถึงและการโจมตีระบบจากผู้ไม่ประสงค์ดีผ่านเครือข่ายภายนอก

5. ระบบงานบริการจากหน่วยงานพันธมิตร (Third party Service) ตัวแทนคือ ระบบจดหมายอิเล็กทรอนิกส์ (e - Mail) จุดเน้นการรักษาความปลอดภัยบัญชีผู้ใช้ การโจมตีแบบ Phishing และ Social Engineering

6. ระบบงานที่ให้บริการเฉพาะ (Specific Service) ตัวแทนคือ ระบบสื่อสารทางไกลผ่านจอภาพ (Video Conference) เน้นการบริหารจัดการใช้งาน การกำหนด Policy และการตรวจสอบความปลอดภัยมีลักษณะเฉพาะ กำหนดมาตรการแก้ไขให้ระบบสามารถกลับมาใช้งานได้อย่างรวดเร็ว

7. เว็บไซต์ (Website) ตัวแทนคือ เว็บไซต์สำนักงานศาลยุติธรรม (www.coj.go.th) จุดเน้นคือ การป้องกันการโจมตีผ่านทาง Browser การตรวจสอบการเปลี่ยนแปลงของหน้าเว็บไซต์

จากการศึกษาพบว่า การใช้กรอบแนวคิดการจัดการความปลอดภัยข้อมูลสารสนเทศเพื่อพัฒนาแนวทางรักษาความปลอดภัยภายในศูนย์ปฏิบัติการเครือข่าย สามารถกำหนดขั้นตอนปฏิบัติสำหรับอุปกรณ์และระบบที่มีคุณสมบัติ และการทำงานคล้ายคลึงกันได้อย่างมีประสิทธิภาพในระดับหนึ่ง ขึ้นอยู่กับการแบ่งประเภทอุปกรณ์ และระบบที่เหมาะสม โดยระบบแต่ละประเภทจะมีข้อแตกต่างกันที่การให้ความสำคัญหรือมุ่งเน้นในกิจกรรมที่เป็นจุดสำคัญหรือจุดวิกฤติ

อย่างไรก็ตามภายหลังดำเนินการตามแนวทางรักษาความปลอดภัยข้อมูลสารสนเทศของสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภทแล้ว จำเป็นต้องดำเนินการตรวจสอบแนวทางรักษาความปลอดภัยจำเพาะสำหรับแต่ละอุปกรณ์และระบบ เพื่อให้การรักษาความปลอดภัยครบถ้วนมีประสิทธิภาพ เนื่องจากระบบประเภทเดียวกันจะมีความแตกต่างกันในรายละเอียด

Thematic Paper Title	A Practical Approach to Establish Information Security System using Information Security Management System framework
Author	Poomwoot Vittavassamrankul
Thematic Paper Advisor	Asst.Prof.Dr. Worasit Choochaiwattana
Academic Program	Web Engineering and Mobile Application Development
Academic Year	2019

ABSTRACT

The Office of the Courts of Justice is in the process of creating an information security policy by referring to the ISO / IEC 27001 standard and developing information security systems within the network operations center in accordance with the standard operating procedures. Therefore, devices and systems classification according to eligibility and operation criteria system access area are divided into 7 categories. The representatives of each category to study according to the information security management process and guidelines for developing information security systems for each type of system is defined. The results are summarized as follows:

1. Infrastructure (Infrastructure): The representative is the power backup system. Focus on notifications Prepare And response measures for emergency power outages

2. Network Management System (Network Management): The representative is the security system on the internal network (Firewall), focusing on defining an appropriate policy, surveillance, and determining emergency procedures.

3. The system that provides services for internal networks (Internal Service): The representatives are the electronic table of contents, focusing on providing a stable service responding and fast problems fixing in the internal network.

4. The system that provides services through an external network (External Service): The representative is a system for submitting and delivering electronic media (e-Filling), focusing

on authentication, data accuracy and correction of rights as specified, and access prevention of attacking systems from malicious parties via the external networks.

5 . Service system from the partner organization (Third Party Service): The representative is the electronic mail system (e - Mail), focusing on the security of user accounts, Phishing attacks and Social Engineering.

6 . The specific service system (Special Service) : The representative is the video conference system, focusing on the management, usage, policy setting, and security checking in particular, fixing corrective action to allow the system quickly restored.

7. Website (Website): The representative is the website of the Office of the Court of Justice (www.coj.go.th), focusing on attacks prevention via the browser and changes detection to the page of the website

The study found that the use of information security management frameworks to develop security guidelines within the network operations center can specify procedures for devices and systems that have similar characteristics and operations with some degree of efficiency depending on the classification of devices and systems that are appropriate by each type of system. There will be differences in the importance of activities that are important or critical.

However, after implementing the security guideline for each type of information assets, it is necessary to conduct inspections of specific security guidelines for each device and system to ensure complete security effective because the same type of systems could have differences in details.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้จัดทำขึ้นตามแนวทางที่ผู้บริหารหน่วยงานมีความประสงค์ที่จะให้บุคลากรมุ่งเน้นศึกษาเรื่องเกี่ยวกับการรักษาความปลอดภัยข้อมูลสารสนเทศ และเนื่องจากการศึกษาโดยมีวัตถุประสงค์ชัดเจนอยู่แล้ว จึงเชื่อแน่ว่าสารนิพนธ์ฉบับนี้จะเป็นประโยชน์แก่ผู้ศึกษาเอง และนำไปปฏิบัติเพื่อเป็นประโยชน์แก่หน่วยงานต่อไป พร้อมกันนี้ขอขอบคุณสำนักงานศาลยุติธรรม หน่วยงานผู้ให้ทุนการศึกษาภายในประเทศ ระดับปริญญาโท ซึ่งถือเป็นส่วนที่สำคัญอย่างยิ่งที่ทำให้มีโอกาสศึกษาต่อเพิ่มเติม

ขอบคุณบุคคลแรก คือ คุณพ่อ คุณแม่ ที่ปลูกฝังให้รักการศึกษา รักการอ่าน ทำให้มีกำลังใจที่จะศึกษาหาความรู้อีกครั้งแม้ว่าจะมีภาระหน้าที่เพิ่มมากขึ้น

ขอขอบคุณ ผู้ช่วยศาสตราจารย์ ดร. วรสิทธิ์ ชูชัยวัฒนา ที่สละเวลาตรวจสอบงานและให้คำปรึกษา แม้ว่าท่านอาจารย์จะไม่ค่อยมีเวลา ขอบคุณอาจารย์ท่านอื่นที่ให้คำแนะนำให้สมบูรณ์ยิ่งขึ้น และที่ขาดไม่ได้ขอขอบคุณเลขาคณะผู้ช่วยติดต่อประสานงาน และตอบคำถามได้ทุกเวลาที่ต้องการ รวมทั้งให้คำแนะนำ ช่วยตรวจสอบรูปแบบเอกสารสารนิพนธ์ให้ออกมาเรียบร้อยดูดีมีชาติตระกูล

ขอขอบคุณ เพื่อนร่วมงานส่วนระบบเครือข่าย สำนักเทคโนโลยีสารสนเทศ สำนักงานศากยุติธรรม ที่สนับสนุนข้อมูลเพื่อนำมาใช้ในการจัดทำสารนิพนธ์นี้ และขอบคุณหัวหน้าส่วนที่เข้าใจกรณีโทรไปแจ้งว่าขอลาป่วยเพื่อการศึกษาเนื่องจากทำงานไม่ทัน

ขอขอบคุณการสนับสนุนจากพ่อแม่พี่น้อง และภรรยา ที่แบกภาระหน้าที่แทนเนื่องจากในช่วงทำการศึกษาพอดีกับการคลอดบุตรคนที่สอง ทำให้เวลาที่จะดำเนินการศึกษาเป็นไปด้วยความยากลำบาก เวลาว่างที่ได้มานั้นมาจากการที่คนในครอบครัวช่วยทำงานแทนในส่วนที่ควรจะเป็นความรับผิดชอบของผู้ศึกษา

อีกหลายท่านที่ยังกล่าวถึงไม่หมดจึงขอขอบคุณรวมไว้ ณ ที่นี้

ภุมวุฒิ วิทวัสสำราญกุล

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

เทคโนโลยีสารสนเทศเข้ามามีบทบาทในการปฏิบัติงานของทุกองค์กรตั้งแต่กิจกรรมพื้นฐาน ไปจนถึงการตัดสินใจของผู้บริหาร ประกอบกับการพัฒนาด้านเทคโนโลยีสารสนเทศ และการสื่อสารมีส่วนช่วยให้การทำงานร่วมกันเป็นไปอย่างมีประสิทธิภาพ ในอีกทางหนึ่งการบุกรุกของผู้ไม่ประสงค์ดีก็มีความซับซ้อน และมีประสิทธิภาพยิ่งขึ้น การรักษาความปลอดภัยข้อมูลสารสนเทศจึงเป็นส่วนที่ต้องพัฒนาควบคู่ไปกับการบริหารจัดการเทคโนโลยีสารสนเทศในการปฏิบัติงาน ปัจจุบันการทำงานร่วมกันในองค์กรมีการดำเนินการอย่างเป็นระบบ และมีความเชื่อมโยงกันอย่างซับซ้อนโดยอาศัยเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยของข้อมูลสารสนเทศจึงประกอบด้วยหลายส่วน มากกว่าเพียงแค่การมีชื่อผู้ใช้และรหัสลับเข้าใช้งาน ระบบยืนยันตัวบุคคล หรือการเข้ารหัสข้อมูล

สำนักงานศาลยุติธรรม โดยสำนักเทคโนโลยีสารสนเทศ อยู่ระหว่างจัดทำแนวนโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศ อย่างไรก็ตามแผนดังกล่าวเป็นแนวนโยบายซึ่งต้องมีแนวปฏิบัติต่อไป ส่วนงานแรกที่ควรนำนโยบายดังกล่าวไปดำเนินการ คือ ศูนย์ปฏิบัติการเครือข่าย สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม เนื่องจากเป็นส่วนให้บริการเครื่องแม่ข่าย และระบบงานแก่หน่วยงานศาลยุติธรรมทั่วประเทศ จึงศึกษากรอบแนวคิดระบบจัดการความปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ซึ่งมีโครงสร้างการทำงานยืดหยุ่น สามารถใช้กรอบแนวคิดกระบวนการจัดการ เช่น PDCA หรือ Six Sigma ในการพัฒนา และปรับใช้มาตรฐานดังกล่าวเป็นแนวทางการรักษาความปลอดภัยข้อมูลสารสนเทศให้สอดคล้องกับแนวนโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศของสำนักงานศาลยุติธรรม

1.2 คำถามงานวิจัย

คำถามในการวิจัย ได้กำหนดไว้ดังนี้

1. การรักษาความปลอดภัยข้อมูลสารสนเทศของศูนย์ปฏิบัติการเครือข่าย สำนักงานศาลยุติธรรม ควรมีข้อกำหนดใดบ้างตามมาตรฐานสากล ISO/IEC 27001

2. สามารถแบ่งประเภทระบบภายในศูนย์ปฏิบัติการเครือข่ายสำนักงานศาลยุติธรรมตามลักษณะการทำงานได้อย่างไรบ้าง เพื่อให้เหมาะสมกับการบริหารจัดการรักษาความปลอดภัยข้อมูลสารสนเทศของระบบแต่ละประเภท

3. ข้อกำหนด เพื่อเป็นแนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศสำหรับระบบแต่ละประเภท ตามข้อ (2) ควรมีข้อปฏิบัติ ลำดับขั้นตอน กระบวนการ และจุดเน้น เพื่อให้เหมาะสมกับระบบแต่ละประเภทอย่างไรบ้าง

4. สามารถนำแนวทางพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศที่ศึกษามาปรับใช้กับระบบภายในศูนย์ปฏิบัติการเครือข่ายได้อย่างไร

1.3 วัตถุประสงค์ของการวิจัย

1. ศึกษาการจัดการความปลอดภัยข้อมูลสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 เพื่อใช้เป็นกรอบการศึกษาแนวปฏิบัติ และข้อกำหนดการรักษาความปลอดภัยข้อมูลสารสนเทศสำหรับอุปกรณ์ และระบบที่ติดตั้งอยู่ในศูนย์ปฏิบัติการเครือข่าย สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม

2. ระบุประเภทของสินทรัพย์ข้อมูลสารสนเทศ เพื่อให้เหมาะแก่การจัดการความปลอดภัยข้อมูลสารสนเทศกับอุปกรณ์ และระบบที่มีคุณสมบัติ และการทำงานเหมือนกัน

3. วิเคราะห์ระบบแต่ละประเภทภายในศูนย์ปฏิบัติการเครือข่าย เพื่อกำหนดแนวทางรักษาความปลอดภัยข้อมูลสารสนเทศที่เหมาะสมกับระบบแต่ละประเภท

4. กำหนดแนวทางพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศ สำหรับอุปกรณ์ และระบบภายในศูนย์ปฏิบัติการเครือข่าย

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับจากการวิจัยนี้คือ

1. สามารถนำแนวทางพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศที่ศึกษา ไปใช้ในการพัฒนาการรักษาความปลอดภัยข้อมูลสารสนเทศของอุปกรณ์ และระบบภายในศูนย์ปฏิบัติการเครือข่าย สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม ได้อย่างเหมาะสม

2. สามารถนำรูปแบบวิธีการศึกษาวิจัยไปใช้ในการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศของหน่วยงานศาลยุติธรรมทั่วประเทศ ซึ่งมีองค์ประกอบของฮาร์ดแวร์ ซอฟต์แวร์ ลักษณะงาน และระดับชั้นการรักษาความปลอดภัยที่แตกต่างกันได้

3. สามารถนำผลการศึกษาวิจัย และข้อเสนอแนะเป็นแนวทางในการศึกษา และพัฒนา เพื่อยกระดับความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่ายให้มีประสิทธิภาพยิ่งขึ้น และเป็นแนวทางในการดำเนินการเพื่อขอใบรับรองตามมาตรฐาน ISO 27001 ต่อไป

บทที่ 2
แนวคิดทฤษฎีและผลงานที่เกี่ยวข้อง

แนวคิดทฤษฎี และผลงานที่เกี่ยวข้อง คือ

2.1 การรักษาความปลอดภัยข้อมูลสารสนเทศพื้นฐาน

2.2 มาตรฐานระบบจัดการความปลอดภัยข้อมูลสารสนเทศ (Information Security Management System : ISMS) ISO 27001:2013

2.3 กระบวนการขับเคลื่อนมาตรฐานระบบจัดการความปลอดภัยข้อมูลสารสนเทศ

2.4 แนวนโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศ สำนักงานศาลยุติธรรม

2.5 การดำเนินการตามมาตรฐาน ISO 27001:2013

2.6 การรักษาความปลอดภัยประเภทของอุปกรณ์ และระบบสารสนเทศ

2.7 การตรวจประเมินภายในความปลอดภัยข้อมูลสารสนเทศ

2.8 การวิเคราะห์ช่องว่างทางศักยภาพ (Gap Analysis)

2.1 การรักษาความปลอดภัยข้อมูลสารสนเทศพื้นฐาน

ลักษณะของสินทรัพย์ข้อมูลสารสนเทศ จากคำจำกัดความของ The National Archives (2011) ประเทศอังกฤษ กล่าวว่าสินทรัพย์ข้อมูลสารสนเทศประกอบด้วย เนื้อหาข้อมูล ข้อกำหนดของข้อมูล และการจัดการข้อมูล เพื่อให้สามารถเข้าใจข้อมูล แบ่งปันข้อมูล ปกป้องข้อมูล และใช้ประโยชน์ข้อมูลได้อย่างมีประสิทธิภาพ สินทรัพย์ข้อมูลสารสนเทศมีมูลค่า (value) ความเสี่ยง (risk) และวงจรชีวิต (life cycle) การจัดการกับสินทรัพย์ข้อมูลสารสนเทศ ให้พิจารณา ดังนี้

1. สามารถค้นข้อมูลได้อย่างไร
2. ใครสามารถเข้าถึงข้อมูลได้ และทำอย่างไร
3. สามารถทำงานกับข้อมูลได้อย่างไร

4. ความเข้าใจเกี่ยวกับข้อมูลดังกล่าวมีอะไรบ้าง

5. ความน่าเชื่อถือข้อมูลอยู่ในระดับใด

ขั้นตอนการประเมินสินทรัพย์ข้อมูลสารสนเทศ โดยจัดทำเอกสารความสัมพันธ์ระหว่างข้อกำหนดการดำเนินงาน และสินทรัพย์ข้อมูลสารสนเทศ และอาจมีการจัดทำทะเบียนสินทรัพย์ข้อมูล (Information Asset Register : IAR)

Examples: Fields on an Information Asset Register	
Description	Brief description of what the asset is More detail on what the components of the asset are
Users	Who created the asset, or where does the asset come from? Who is the Information Asset Owner? Which department holds responsibility for the asset? Who are the stakeholders?
Date	Creation date Date closed (for closed assets) Last date asset register was reviewed/updated
Asset status	Is this asset being actively updated? Has the asset been closed?
Purpose	What part of the business does this asset support? Business risks from or to the asset
Value	What is the value to the business? What would be the cost of replacing the information?
Retention schedule	How long should it be kept in immediate access? What should happen to it when it no longer needs immediate access? What are the disposal requirements?
How do you need to use your asset	How will you **find** the information? Who can **open** the information and how? How do you need to be able to **work with** the information? What do you need to be able to **understand** about your information? To what extent do you need to **prove** your information is what it claims to be?
Risk	What are the risks to the asset? What are the risks to the business from the asset (for example from its loss, corruption or inappropriate access)?

ภาพที่ 2.1 ตัวอย่างข้อมูลทะเบียนสินทรัพย์ข้อมูลสารสนเทศ

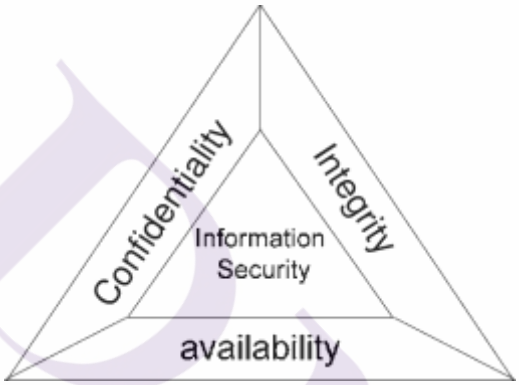
ที่มา : Information Asset Register and Business Requirements Version : 1.2 [online] : เข้าถึง 10 ก.พ. 2562. จาก http://www.nationalarchives.gov.uk/documents/identify-information-assets.pdf

นายจตุชัย แพงจันทร์ (2553, หน้า 8 - 10) กล่าวว่าข้อมูลสารสนเทศที่มีความปลอดภัยต้องมีคุณสมบัติ 3 ประการ คือ ความลับ ความถูกต้อง และความพร้อมใช้งาน เรียกว่า CIA Triad ดังนี้

1. การรักษาความลับ (Confidentiality) หมายถึง การทำให้ข้อมูลสามารถเข้าถึง หรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

2. ความถูกต้อง (Integrity) หมายถึง การรักษาความคงสภาพข้อมูลจากแหล่งที่มาหรือไม่ได้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต

3. ความพร้อมใช้งาน (Availability) หมายถึง การทำให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้เมื่อต้องการ



ภาพที่ 2.2 องค์ประกอบความปลอดภัยข้อมูลสารสนเทศ (CIA)

ที่มา : Information Security Properties (CIA Triad) [online] : เข้าถึง 10 ก.พ. 2562. จาก https://www.researchgate.net/figure/Information-Security-Properties-CIA-Triad_fig1_220121692

เพื่อเป็นแนวทางในการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศแล้ว ควรกล่าวถึงการกระทำที่ก่อให้เกิดความเสียหายต่อความปลอดภัยข้อมูลสารสนเทศ Michael G Solomon and Mike Chapple (2005, pp. 5-7) กล่าวถึงสิ่งที่มีลักษณะตรงข้ามกับ CIA Triad ประกอบด้วยหัวข้อหลัก 3 ประการ คือ Disclosure, Alteration และ Denial เรียกว่า DAD Triad ดังนี้

1. การเปิดเผยข้อมูล (Disclosure) หมายถึง การเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

2. การเปลี่ยนแปลงข้อมูล (Alteration) หมายถึง การเปลี่ยนแปลงข้อมูลโดยไม่ถูกต้อง ทำให้ระบบไม่สามารถรับรองความถูกต้องของข้อมูลได้

3. การปฏิเสธการให้บริการ (Denial) หมายถึง การปฏิเสธการให้บริการแก่ผู้ใช้ที่มีสิทธิ์ใช้งาน กรณีพบได้ทั่ว คือ การโจมตีประเภท DoS attack หรือที่รู้จักกันในชื่อของ DDos : Distributed denial of service

ภาพที่ 2.3 องค์ประกอบภัยคุกคามข้อมูลสารสนเทศ (DAD)

ที่มา : CISSP - the CIA Triad and its opposites [online] : เข้าถึง 10 ก.พ. 2562. จาก https://thorteaches .com/cissp-the-cia-triad-and-its-opposites/

นอกจาก CIA Triad แล้ว นายจตุชัย แพงจันทร์ (2553, หน้า 12 - 13) กล่าวถึงหลักการเกี่ยวกับการรักษาความปลอดภัยข้อมูลสารสนเทศ ดังนี้

1. ความเป็นส่วนตัว (Privacy)
2. การระบุตัวตน (Identification)
3. การพิสูจน์ทราบตัวตน (Authentication)
4. การอนุญาตใช้งาน (Authorization)
5. การตรวจสอบได้ (Accountability)

เมื่อกล่าวถึงการรักษาความปลอดภัยแล้ว ข้อมูลที่สำคัญอีกประการ คือภัยคุกคาม สามารถแบ่งประเภทภัยคุกคามเป็นประเภท คือ ภัยคุกคามจากคนภายในองค์กร ภัยคุกคามจากคน

ภายนอกองค์กร ภัยธรรมชาติ เช่น น้ำท่วม แผ่นดินไหว ไฟไหม้ และภัยคุกคามจากสิ่งแวดล้อมไม่เหมาะสม เช่น น้ำรั่วซึม ฝุ่นละออง สารเคมี อุณหภูมิร้อนเกินไป และความชื้น

นอกจากภัยคุกคามแล้วส่วนประกอบที่สำคัญที่ต้องศึกษาได้แก่ช่องโหว่ของอุปกรณ์และระบบ ช่องโหว่หรือจุดอ่อน (Vulnerability) หมายถึง ช่องทางที่อาจถูกใช้สำหรับโจมตีได้ ถ้าเปรียบกับการรักษาความปลอดภัยทางกายภาพช่องโหว่อาจหมายถึง ประตู หน้าต่างที่ถูกเปิดทิ้งไว้ ส่วนจุดอ่อนหรือช่องโหว่ของระบบคอมพิวเตอร์ และเครือข่ายจะหมายถึง ช่องทางที่ผู้โจมตีสามารถเจาะเข้าระบบหรือเครือข่ายได้ เช่น การเปิดพอร์ต (port) ทิ้งไว้โดยไม่จำเป็น อาจแบ่งประเภทช่องโหว่แบ่งตามหมวดสินทรัพย์ข้อมูลสารสนเทศ ดังนี้

1. ช่องโหว่ด้านฮาร์ดแวร์ (Hardware)
2. ช่องโหว่ด้านซอฟต์แวร์ (Software)
3. ช่องโหว่ด้านเครือข่าย (Network)
4. ช่องโหว่ด้านบุคลากร (Personnel)
5. ช่องโหว่ทางกายภาพ (Physical site)
6. ช่องโหว่ด้านการจัดการ (Organizational)

เมื่อทราบถึงช่องโหว่แล้วสิ่งที่ต้องกระทำก็คือจัดการช่องโหว่เหล่านั้นโดยการประเมินช่องโหว่สินทรัพย์ข้อมูลสารสนเทศ Vulnerability Assessment เป็นกระบวนการ ระบุปริมาณ และจัดลำดับความสำคัญช่องโหว่ Federal Emergency Management Agency (n.d.) กำหนดคำถามเพื่อประเมินช่องโหว่สินทรัพย์ข้อมูลสารสนเทศ ดังนี้

1. สามารถให้คำอธิบายว่าช่องโหว่คืออะไร
2. ให้คำจำกัดความโดยสร้าง
3. ระบุจำนวนหรือระดับความร้ายแรงของช่องโหว่ และการแก้ไขเพื่อบรรเทาภัย
4. ให้คะแนนระดับของช่องโหว่
5. ระบุปัญหาการออกแบบระบบ
6. ประเมินการออกแบบการป้องกันแก้ไขภัยคุกคามแต่ละประเภท และระดับ
7. กำหนดระดับการป้องกันการแก้ไขบรรเทาภัยคุกคามแต่ละประเภท

ขั้นตอนการประเมินช่องโหว่ Kenneth Gonzalez (2018) อธิบายกระบวนการประเมินช่องโหว่ข้อมูลสารสนเทศ ดังนี้

1. การประเมินเบื้องต้น (Initial assessment) ระบุสินทรัพย์ กำหนดความเสี่ยงและค่าวิกฤตสำหรับแต่ละอุปกรณ์ สิ่งสำคัญ คือ การระบุความสำคัญของอุปกรณ์ที่มีในองค์กร และต้องเข้าใจว่าอุปกรณ์ดังกล่าวสามารถเข้าถึงได้โดยสมาชิกหรือเฉพาะผู้ดูแลระบบและผู้ใช้ที่ได้รับการอนุญาต

2. กำหนดคำจำกัดความพื้นฐานของระบบ (System Baseline Definition) ทำความเข้าใจกับปัจจัยเชิงกลยุทธ์และมีความเข้าใจในรายละเอียดที่ชัดเจน ได้แก่ ความเสี่ยง ระดับความเสี่ยงที่ยอมรับได้ แนวทางปฏิบัติ และนโยบายการลดความเสี่ยงสำหรับแต่ละอุปกรณ์ การรักษาความเสี่ยงที่เหลือ การตอบโต้สำหรับแต่ละอุปกรณ์หรือบริการ

3. สแกนช่องโหว่ (Perform the Vulnerability Scan) โดยใช้ข้อกำหนดและนโยบายที่ถูกต้องเหมาะสมในการตรวจสอบหรือสแกนช่องโหว่ ก่อนเริ่มดำเนินการสแกนช่องโหว่ ให้ตรวจสอบข้อกำหนดการปฏิบัติ กฎระเบียบ และลักษณะงานขององค์กร สิ่งสำคัญคือต้องตระหนักถึงบริบท และพิจารณาว่าการสแกนช่องโหว่สามารถดำเนินการทั้งหมดในคราวเดียว หรือต้องแบ่งกลุ่ม

4. สร้างรายงานช่องโหว่ของสินทรัพย์ข้อมูลสารสนเทศ (Vulnerability Assessment Report Creation) โดยให้มีรายละเอียดครบถ้วน และเพิ่มมูลค่าพิเศษด้วยคำแนะนำตามเป้าหมายการประเมินเบื้องต้น รายงานช่องโหว่ของสินทรัพย์ข้อมูลสารสนเทศควรรายงานโดยละเอียด คือ ชื่อของช่องโหว่ วันที่ค้นพบ คะแนนความเสี่ยงของช่องโหว่โดยตรวจสอบจากฐานข้อมูลความเสี่ยง คำอธิบายโดยละเอียดเกี่ยวกับช่องโหว่ รายละเอียดเกี่ยวกับระบบที่ได้รับผลกระทบ รายละเอียดเกี่ยวกับกระบวนการแก้ไขช่องโหว่ และหลักฐานแนวคิด (A Proof of concept : PoC) ของช่องโหว่สำหรับระบบ (หมายถึงให้มีการทดสอบ ตรวจสอบก่อนยืนยันความถูกต้อง)

ตารางที่ 2.1 โอกาสที่จะเกิดการโจมตีจากช่องโหว่

ความเปิดเผย	ความหมาย
High	ช่องโหว่ที่เกิดขึ้นและเป็นที่รู้จักกันอย่างแพร่หลาย มีความเข้าใจในช่องโหว่อย่างมาก มาตรการป้องกันและแก้ไขยังไม่มี
Moderate	ช่องโหว่ที่เกิดขึ้นเป็นที่รู้จักกันแต่ยังไม่แพร่หลาย ความเข้าใจในช่องโหว่ยังไม่เข้าใจอย่างชัดเจน เกี่ยวเนื่องอยู่กับช่องโหว่อื่น ๆ มีมาตรการป้องกันและแก้ไขแต่ยังไม่ดีเพียงพอ
Low	ช่องโหว่อาจเกิดขึ้น แต่ยังไม่เป็นที่รู้จัก เป็นช่องโหว่ที่ขึ้นอยู่กับช่องโหว่อื่นที่มีเกิดขึ้นก่อนหน้าแล้ว มาตรการป้องกันและแก้ไขยังไม่มี

ที่มา : Global Information Assurance Certification Paper [online] : เข้าถึง 10 ก.พ. 2562. จาก https://www.giac.org/paper/gcux/241/public-servers-vulnerability-assessment-report/101868

ตารางที่ 2.2 ระดับความเสียหายที่เกิดจากการโจมตีจากช่องโหว่

ระดับความเสียหาย	ความหมาย
High	ความเสียหายสูง ต้องมีการกำหนดมาตรการป้องกันแก้ไขที่แข็งแกร่ง เมื่อเกิดความเสียหายระบบอาจจะสามารถทำงานต่อไปได้ แต่ต้องปฏิบัติการแก้ไขอย่างเร่งด่วนที่สุดเท่าที่จะเป็นไปได้
Medium	ความเสียหายปานกลาง ต้องมีการกำหนดมาตรการป้องกันแก้ไข และกำหนดแผนปฏิบัติการแก้ไขให้ได้ในระยะเวลาที่สมเหตุสมผล
Low	ความเสียหายต่ำ เจ้าหน้าที่ผู้รับผิดชอบต้องตัดสินใจว่าจะกำหนดมาตรการป้องกันแก้ไข หรือจะยอมรับช่องโหว่ของระบบ

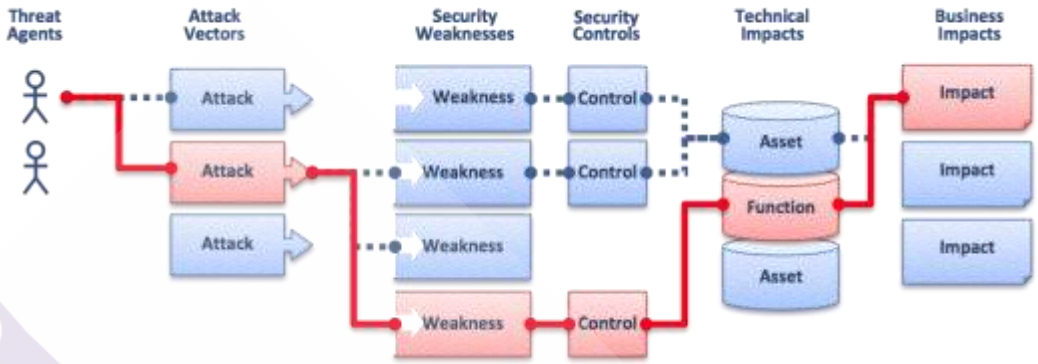
ที่มา : Global Information Assurance Certification Paper [online] : เข้าถึง 10 ก.พ. 2562. จาก https://www.giac.org/paper/gcux/241/public-servers-vulnerability-assessment-report/101868

ภายหลังทราบภัยคุกคามและช่องโหว่แล้วจะดำเนินการประเมินความเสี่ยงเพื่อบริหารจัดการความเสี่ยงนั้น ๆ Michael G Solomon and Mike Chapple (2005, pp. 11 - 13) แสดงขั้นตอนการดำเนินการประเมินความเสี่ยง ดังนี้

1. ระบุข้อมูลสารสนเทศที่มีคุณค่า (Identifying and Valuing Assets) คือ การกำหนดข้อมูลสารสนเทศที่มีคุณค่าขององค์กร และให้คะแนนแก่ข้อมูลสารสนเทศเหล่านั้น มีเทคนิคอยู่ 2 ประการ ได้แก่ การประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Risk Assessment) และการประเมินความเสี่ยงเชิงปริมาณ (Quantitative Risk Assessment) เพื่อตัดสินใจในการกำหนดมาตรการป้องกันความเสียหายที่อาจเกิดขึ้นจากความเสี่ยงต่าง ๆ

2. แยกแยะความเสี่ยงที่อาจเกิดขึ้น (Identifying and Assessing Risks) โดยให้คำอธิบายที่สำคัญ คือ ระบุจุดอ่อนของระบบ ระบุภัยคุกคาม ระบุความเสี่ยงต่อจุดอ่อนและภัยคุกคาม

ขั้นต่อไป คือ การดำเนินการจัดการความเสี่ยง โดยทั่วไปดำเนินการได้ 4 ลักษณะ คือ การหลีกเลี่ยงความเสี่ยง การบรรเทาความเสี่ยง การยอมรับความเสี่ยง และการถ่ายโอนความเสี่ยง ในสภาพการทำงานจริง การเลือกวิธีบริหารจัดการความเสี่ยงไม่มีคำว่าถูกหรือผิดแล้วแต่ความเหมาะสม ในบางครั้งอาจเลือกใช้กระบวนการจัดการบางอย่าง หรือเลือกใช้การจัดการความเสี่ยงหลายข้อร่วมกัน นอกจากการจัดการความเสี่ยงขั้นต้นแล้วยังมีการจัดการความเสี่ยงในรูปแบบอื่น การจัดการความเสี่ยงสำหรับข้อมูลสารสนเทศสำหรับการปฏิบัติเพื่อให้เข้าใจง่าย คือ การป้องกัน (Prevent) ลด (Reduce) ยอมรับ (Accept) การควบคุม (Control) และการโอน (Transfer)



ภาพที่ 2.4 ผลกระทบของช่องโหว่และความเสี่ยงของการถูกโจมตี

ที่มา : Vulnerability (computing) [online] : เข้าถึง 10 ก.พ. 2562. จาก https://commons.wikimedia.org/wiki/File:2010-T10-ArchitectureDiagram.png

เรื่องที่น่าสนใจอีกประการคือการควบคุมความปลอดภัย Security controls (n.d.) อธิบายการควบคุมความปลอดภัย (Security Control) หมายถึง มาตรการป้องกันหรือตอบโต้เพื่อหลีกเลี่ยง ตรวจจับ การบุกรุก หรือลดความเสี่ยง สามารถจำแนกได้หลายเกณฑ์ ตัวอย่างเช่น การแยกตามเวลาที่สัมพันธ์กับเหตุการณ์ด้านความปลอดภัย ได้แก่ การควบคุมเชิงป้องกัน (Preventive controls), การควบคุมตรวจสอบ (Detective controls), การควบคุมแก้ไข (Corrective controls) และการแยกประเภทตามลักษณะของเหตุการณ์ด้านความปลอดภัย ได้แก่ การควบคุมทางกายภาพ (Physical controls), การควบคุมกระบวนการ (Procedure controls), การควบคุมทางเทคนิค (Technical controls), การควบคุมด้านกฎหมายและข้อบังคับ (Legal and regulatory or compliance controls)

2.2 มาตรฐานระบบจัดการความปลอดภัยข้อมูลสารสนเทศ (Information Security Management System : ISMS) ISO 27001:2013

ISO/IEC 27001 (n.d.) กล่าวถึง มาตรฐาน ISO 27001 ว่าพัฒนาโดยองค์การระหว่างประเทศว่าด้วยการกำหนดมาตรฐาน ISO (International Organization for Standardization) เป็นข้อกำหนดสำหรับการพัฒนาระบบจัดการความปลอดภัยสารสนเทศ (Information security management system) เพื่อประสิทธิภาพ และประสิทธิผลของความปลอดภัยข้อมูลสารสนเทศของ

องค์กร ความสอดคล้องตามข้อกำหนดด้านความมั่นคงปลอดภัย และระเบียบข้อบังคับที่เกี่ยวข้อง และพัฒนามาตรฐาน ISO 17799 (Information technology – Security techniques – Code of practices for information security management) ซึ่งเป็นแนวปฏิบัติสำหรับการประเมิน และจัดการความเสี่ยง รวมถึงแนวทางในการควบคุม ตามมาตรฐาน ISO 27001

เพื่อเป็นพื้นฐานการศึกษามาตรฐานที่จึงขออธิบายถึง ISO 27000 ซึ่งเป็นมาตรฐานของระบบคุณภาพในการจัดการความปลอดภัยสำหรับสารสนเทศ หรือ Information Security Management (ISM) ประกอบด้วยมาตรฐานย่อย ดังนี้

ISO 27000 ว่าด้วย ภาพรวม และคำศัพท์ต่างๆที่ใช้ในมาตรฐาน

ISO 27001 ว่าด้วย ความต้องการตามมาตรฐานว่าสิ่งที่จำเป็นต้องดำเนินการนั้นมีเรื่องใดบ้าง

ISO 27002 ว่าด้วย เกณฑ์มาตรฐานในการปฏิบัติ ว่าควรปฏิบัติอย่างไรเพื่อให้เป็นไปตามความต้องการของมาตรฐาน สิ่งใดที่จำเป็นต้องมี และต้องมีในระดับไหน

ISO 27003 ว่าด้วย แนวทางการดำเนินงานตามมาตรฐาน

ISO 27004 ว่าด้วย การวัดประเมินตามมาตรฐาน

ISO 27005 ว่าด้วย การบริหารความเสี่ยงตามมาตรฐาน

ISO 27006 ว่าด้วย แนวทางการปฏิบัติเพื่อให้ได้รับการรับรองตามมาตรฐาน

ISO 27007 ว่าด้วย แนวทางการตรวจประเมินตามมาตรฐานของผู้ตรวจประเมิน

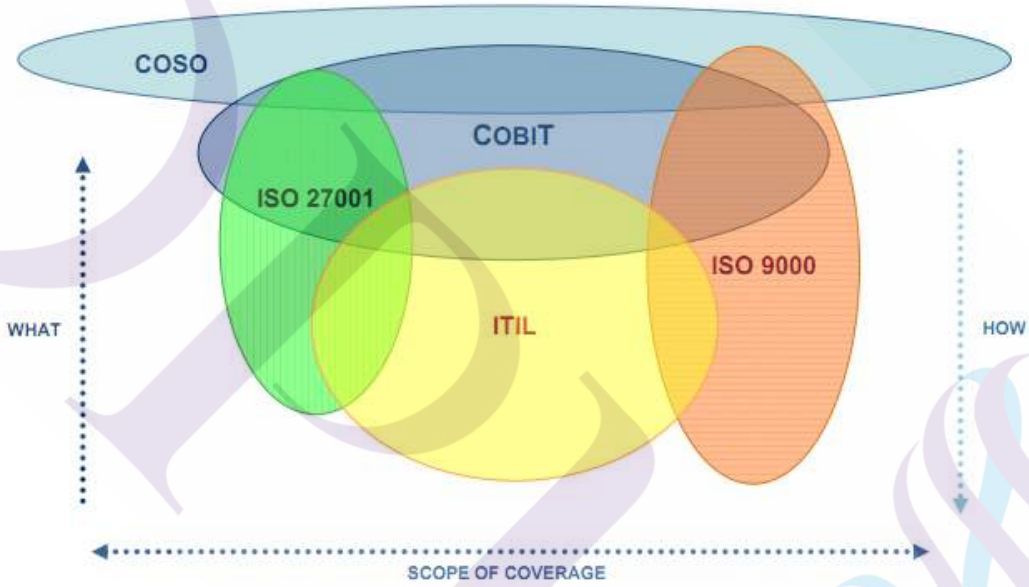
นายจตุชัย แพงจันทร์ (2553, หน้า 31 - 37) แสดงมาตรฐานอื่นที่เกี่ยวข้องอาจใช้เป็นมาตรฐานในการรักษาความปลอดภัยข้อมูลสารสนเทศ คือ

COBIT (Control Objective for Information and Related Technology) เป็นการกำหนดแนวคิด และแนวปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่าง ๆ ประกอบด้วย 4 หัวข้อหลัก (Domain) คือ
การวางแผนและการจัดการองค์กร (PO : Planning and Organization), การจัดหาและการติดตั้งใช้งาน (AI : Acquisition and Implementation), การส่งมอบ และการบริการดูแล (DS : Delivery and Support), การเฝ้าติดตามและประเมินผล (M : Monitor and Evaluate)

ITIL (The Information Technology Infrastructure Library) เป็นหลักการจัดการด้านไอทีในองค์กร มีอีกชื่อหนึ่งว่า IMS (Infrastructure Management Service) ปัจจุบันเป็น ITILv3 ประกอบด้วย 26 กระบวนการ และจัดกลุ่มไว้ 5 กลุ่ม หรือ 5 เล่ม คือ ยุทธศาสตร์งานบริการ (Service Strategy)

การออกแบบงานบริการ (Service Design) การส่งมอบงานบริการ (Service Transition) การปฏิบัติงานบริการ (Service Operation) การปรับปรุงงานบริการอย่างต่อเนื่อง (Continual Service Improvement)

มาตรฐานแต่ละประเภทจะมีข้อมูลบางส่วนที่มีเนื้อหาร่วมกัน และบางส่วนที่แตกต่างกันออกไป หน่วยงานที่มีการนำมาตรฐานอื่นมาใช้อยู่แล้ว หรือมีการดำเนินการตามมาตรฐานใด ๆ บางส่วน จะสามารถนำมาตรฐานดังกล่าวมาใช้ร่วมกันได้ จากมุมมองการนำไปใช้งาน ITIL ถือเป็นมาตรฐานที่ง่ายที่สุดที่จะนำไปใช้ เนื่องจาก ITIL สามารถใช้งานได้บางส่วน และยังไม่มีผลกระทบต่อประสิทธิภาพ



ภาพที่ 2.5 มาตรฐานที่มีเนื้อหาการรักษาความปลอดภัยข้อมูลสารสนเทศร่วมกันบางส่วน

ที่มา : Comparison between COBIT, ITIL and ISO 27001 [online] : เข้าถึง 10 ก.พ. 2562. จาก http://engineer-t.blogspot.com/2016/03/comparison-between-cobit-itil-and-iso.html

ข้อกำหนดของมาตรฐาน ISO 27001 ได้แบ่งเนื้อหาของออกเป็น 2 ส่วน คือ

1. การบริหารจัดการระบบความปลอดภัยข้อมูลสารสนเทศ
2. รายการควบคุม และวัตถุประสงค์ของการควบคุม

ISO/IEC 27001 (n.d.) สรุปข้อกำหนดสำหรับเกณฑ์มาตรฐานระบบคุณภาพ ISO 27001 : 2013 ซึ่งมีอยู่ทั้งหมด 114 หัวข้อควบคุม และ 14 หัวข้อหลัก คือ

Domain ที่ 1 ในมาตรฐานคือหมวด A5 : Information security policies หรือ นโยบายการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

Domain ที่ 2 ในมาตรฐานคือหมวด A6 : How information security is organized เป็นหัวข้อที่ว่าด้วยเรื่อง Organization of Information Security หรือ โครงสร้างพื้นฐานด้านการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

Domain ที่ 3 ในมาตรฐานคือหมวด A7 : Human resources security - controls that are applied before, during, or after employment. เป็นหัวข้อที่ว่าด้วยเรื่อง Human Resource Security หรือ การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคลที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

Domain ที่ 4 ในมาตรฐานคือหมวด A8 : Asset management เป็นหัวข้อที่ว่าด้วยเรื่อง Asset Management หรือ การบริหารจัดการสินทรัพย์ที่เกี่ยวกับสารสนเทศขององค์กร

Domain ที่ 5 ในมาตรฐานคือหมวด A9 : Access controls and managing user access เป็นหัวข้อที่ว่าด้วยเรื่อง Access Control หรือ การควบคุมการเข้าถึงข้อมูลสารสนเทศ

Domain ที่ 6 ในมาตรฐานคือหมวด A10 : Cryptographic technology เป็นหัวข้อที่ว่าด้วยเรื่องการเข้ารหัสและถอดรหัส เพื่อป้องกันข้อมูลสารสนเทศ

Domain ที่ 7 ในมาตรฐานคือหมวด A.11: Physical security of the organization's sites and equipment เป็นหัวข้อที่ว่าด้วยเรื่อง Physical & Environmental Security หรือ การรักษาความมั่นคงปลอดภัยทางกายภาพที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

Domain ที่ 8 ในมาตรฐานคือหมวด A12 : Operational security เป็นหัวข้อว่าด้วยเรื่องข้อปฏิบัติในการรักษาความปลอดภัย

Domain ที่ 9 ในมาตรฐานคือหมวด A.13: Secure communications and data transfer เป็นหัวข้อที่ว่าด้วยเรื่อง Communications & Operations Management หรือ การบริหารจัดการเรื่องการสื่อสารและการปฏิบัติงานที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

Domain ที่ 10 ในมาตรฐานคือหมวด A14 Secure acquisition, development, and support of information systems เป็นหัวข้อที่ว่าด้วยเรื่อง Information Systems Acquisition Development & Maintenance หรือ การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

Domain ที่ 11 ในมาตรฐานคือหมวด A15 : Security for suppliers and third parties เป็นหัวข้อที่ว่าด้วยเรื่องการรักษาความปลอดภัยในการทำงานร่วมกับหน่วยงานภายนอก

Domain ที่ 12 ในมาตรฐานคือหมวด A16 : Incident management เป็นหัวข้อที่ว่าด้วยเรื่อง Information Security Incident Management หรือ การบริหารการเตรียมความพร้อมเพื่อรับเหตุการณ์ที่ไม่คาดฝันที่อาจเกิดขึ้นกับระบบสารสนเทศ

Domain ที่ 13 ในมาตรฐานคือหมวด A17 : Business continuity/disaster recovery (to the extent that it affects information security) เป็นหัวข้อว่าด้วยเรื่อง Business continuity หรือการดำเนินการภายหลังการกู้ระบบจนสามารถใช้งานได้เรียบร้อยแล้ว รวมถึงผลกระทบที่มีต่อข้อมูลสารสนเทศ

Domain ที่ 14 ในมาตรฐานคือหมวด A18 : Compliance - with internal requirements, such as policies, and with external requirements, such as laws. เป็นหัวข้อว่าด้วยเรื่องข้อปฏิบัติเพื่อรักษาความปลอดภัยข้อมูลสารสนเทศ ทั้งนโยบายปฏิบัติภายในหน่วยงาน รวมทั้งกฎหมายระเบียบ ข้อตกลงภายนอก ที่เกี่ยวข้อง

รายละเอียดในแต่ละหัวข้อหลัก (Domain) ประกอบด้วย วัตถุประสงค์ของการควบคุมตามเกณฑ์มาตรฐาน ปัจจุบันมาตรฐาน ISO 27001 : 2013 ประกอบด้วย ข้อกำหนด (controls) 114 ข้อ แบ่งเป็นกลุ่มข้อกำหนด (clauses) 14 ข้อ และเป็นประเภทข้อกำหนด (control categories) 35 ข้อ แต่อย่างไรก็ตามไม่จำเป็นต้องมีการดำเนินงานตามข้อกำหนดทั้งหมด ขึ้นอยู่กับ ลักษณะภารกิจและการวิเคราะห์ผลกระทบทางธุรกิจ หรือ Business Impact Analysis : BIA ของแต่ละองค์กรนั่นเอง

2.3 กระบวนการขับเคลื่อนมาตรฐานระบบจัดการความปลอดภัยข้อมูลสารสนเทศ

นายจตุชัย แพงจันทร์ (2553, หน้า 40 - 41) แสดงกระบวนการขับเคลื่อนมาตรฐานระบบจัดการความปลอดภัยข้อมูลสารสนเทศ หรือการนำไปปฏิบัติ โดยใช้วงจร PDCA (Plan – Do – Check - Action) ดังนี้

ตารางที่ 2.3 ขั้นตอนการปฏิบัติ Plan – Do – Check - Action

Plan : วางแผนจัดทำ ISMS	a) กำหนดขอบเขตการจัดทำ ISMS b) กำหนดนโยบายของ ISMS c) กำหนดรูปแบบ และวิธีการประเมินความเสี่ยง d) ระบุความเสี่ยง e) วิเคราะห์ และประเมินความเสี่ยง f) วิเคราะห์ และประเมินหนทางในการประเมินความเสี่ยง g) กำหนดวัตถุประสงค์ และมาตรการในการควบคุมเพื่อลดความเสี่ยง h) ขออนุมัติผู้บริหารเกี่ยวกับความเสี่ยงที่ไม่มีมาตรการเพื่อควบคุม i) ขออนุมัติผู้บริหารเกี่ยวกับการทำระบบ ISMS j) จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้ ISMS
Do : ดำเนินการตามแผน	a) กำหนดแผนการกำจัดความเสี่ยง ซึ่งประกอบด้วยแนวทางปฏิบัติสำหรับผู้บริหาร ทรัพยากรที่ใช้ ความรับผิดชอบ และลำดับความสำคัญของความเสี่ยง b) ปฏิบัติตามแผนลดความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ c) ดำเนินการตามมาตรการควบคุมที่เลือก เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ d) กำหนดเกณฑ์สำหรับวัดประสิทธิภาพของมาตรการควบคุม e) ฝึกอบรม และกระตุ้นให้ตระหนักเกี่ยวกับการรักษาความปลอดภัย f) บริหารการปฏิบัติการของ ISMS g) บริหารทรัพยากรของ ISMS h) กำหนดขั้นตอนปฏิบัติเพื่อตรวจจับ และตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย

ตารางที่ 2.3 (ต่อ)

Check : เฝ้าระวังและตรวจสอบ	a) เฝ้าระวังและตรวจจับข้อผิดพลาดต่าง ๆ และประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ b) ตรวจพิจารณาว่า ISMS มีประสิทธิภาพเพียงพอหรือไม่ c) วัดประสิทธิภาพของมาตรการที่ใช้ว่าได้ผลหรือไม่ d) ประเมินเป็นประจำว่าความเสี่ยงยังอยู่ในระดับที่ยอมรับได้หรือไม่ e) ตรวจสอบภายใน ISMS f) ตรวจสอบและประเมินว่าระบบ ISMS ทำงานตามขอบเขตที่กำหนดหรือไม่ g) ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดต่างๆ ที่ตรวจพบ h) บันทึกการปฏิบัติ และเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของ ISMS
Act : รักษาและปรับปรุง ISMS	a) ดำเนินการเพิ่มเติมเพื่อปรับปรุง ISMS b) แก้ไขปัญหาที่เกิดขึ้นและป้องกันไม่ให้เกิดขึ้นอีก c) สื่อสารให้ผู้เกี่ยวข้องทราบเกี่ยวกับการปรับปรุงระบบ d) ทำให้แน่ใจว่าการปรับปรุงระบบนั้นบรรลุวัตถุประสงค์ที่ตั้งไว้

2.4 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลยุติธรรม

สำนักงานศาลยุติธรรมเป็นองค์กรอิสระตามรัฐธรรมนูญ ทำหน้าที่เป็นหน่วยงานธุรการของศาลยุติธรรมทั่วประเทศ โดยมีสำนักเทคโนโลยีสารสนเทศกำกับดูแลด้านเทคโนโลยีสารสนเทศ รวมถึงการกำหนดมาตรฐานในการพัฒนาเทคโนโลยีสารสนเทศ ซึ่งสำนักเทคโนโลยีโดยความร่วมมือของสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์กรมหาชน) (สพธอ.) ดำเนินการจัดทำแนวปฏิบัติภายใต้มาตรฐาน ISO 27001 แบ่งข้อกำหนดเป็น 7 หมวด โดยมีรายละเอียด สรุปได้ดังนี้

1. หมวดที่ 1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ โดยมีแนวปฏิบัติ 18 ข้อ คือ

ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ส่วนที่ 2 การบริหารจัดการเข้าถึงของผู้ใช้

ส่วนที่ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ 4 การบริหารจัดการสินทรัพย์

ส่วนที่ 5 การควบคุมการเข้าถึงเครือข่าย

ส่วนที่ 6 การควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน และสารสนเทศ

ส่วนที่ 8 การบริหารจัดการซอฟต์แวร์ และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี

ส่วนที่ 9 การปฏิบัติงานจากภายนอกสำนักงาน

ส่วนที่ 10 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ส่วนที่ 11 การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย

ส่วนที่ 12 การควบคุมจดหมายอิเล็กทรอนิกส์

ส่วนที่ 13 การควบคุมการใช้อินเตอร์เน็ต (Internet)

ส่วนที่ 14 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ส่วนที่ 15 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ส่วนที่ 16 การตรวจจับการบุกรุก

ส่วนที่ 17 การติดตั้งและกำหนดค่าของระบบ

ส่วนที่ 18 การจัดเก็บข้อมูลจารจรคอมพิวเตอร์

2. หมวดที่ 2 การรักษาความปลอดภัยฐานข้อมูล และสำรองข้อมูล แบ่งเป็น

ส่วนที่ 1 การรักษาความปลอดภัยฐานข้อมูล

ส่วนที่ 2 การสำรองข้อมูล

3. หมวดที่ 3 การตรวจสอบ และประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ 1 การตรวจสอบ และประเมินความเสี่ยง

ส่วนที่ 2 ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

4. หมวดที่ 4 การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

5. หมวดที่ 5 การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

6. หมวดที่ 6 การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

7. หมวดที่ 7 หน้าที่และความรับผิดชอบ

2.5 การดำเนินการตามมาตรฐาน ISO 27001:2013

Planning for and Implementing ISO 27001 (2011) แบ่งกระบวนการ ดำเนินการตามมาตรฐาน ดังนี้

2.5.1 งบประมาณในการดำเนินการ การนำมาตรฐาน ISO 27001 ต้องพิจารณาต้นทุนและระยะเวลาของโครงการ โดยต้องพิจารณาค่าใช้จ่าย 4 ประเภท ดังนี้

1. งบประมาณที่ใช้ประกอบด้วย ระบบการจัดการทรัพยากรบุคคล ระบบเทคโนโลยีสารสนเทศ สิ่งอำนวยความสะดวก และระบบรักษาความปลอดภัย

2. การจ้างที่ปรึกษาภายนอกที่มีประสบการณ์ช่วยประหยัดเวลา และค่าใช้จ่ายมีประโยชน์ในระหว่างการตรวจสอบภายใน และทำให้มั่นใจว่าจะได้รับการรับรองมาตรฐานอย่างราบรื่น

3. ค่าใช้จ่ายเพื่อขอใบรับรองตามมาตรฐาน ISO 27001

4. งบประมาณในการดำเนินการ ซึ่งค่าใช้จ่ายเหล่านี้ขึ้นอยู่กับสภาพความมั่นคงปลอดภัยของระบบ IT ภายในองค์กร หากผลจากการประเมินความเสี่ยงหรือการตรวจสอบพบช่องโหว่ในระบบค่าใช้จ่ายในการดำเนินการจะขึ้นอยู่กับแนวทางดำเนินการ โดยเฉลี่ยแล้วใช้เวลาประมาณ 4-9 เดือน ขึ้นอยู่กับมาตรฐานการปฏิบัติงาน และคุณภาพ และการสนับสนุนด้านการจัดการ ขนาดและลักษณะขององค์กร ระดับความมั่นคงและวุฒิภาวะของระบบเทคโนโลยีสารสนเทศภายในองค์กร และเอกสารที่มีอยู่ สำหรับองค์กรที่ปฏิบัติตามกรอบ COBIT, มาตรฐาน

การตรวจสอบ (SAS) No.70 Type I และ Type II, มาตรฐานการรักษาความปลอดภัยข้อมูลการชำระเงินของอุตสาหกรรมการชำระเงิน (PCI DSS), มาตรฐานของสถาบันมาตรฐาน และเทคโนโลยีแห่งชาติ (NIST) หรือบัญญัติกฎหมายของ Sarbanes-Oxley Act ของสหรัฐอเมริกา ซึ่งมีการกำหนดนโยบาย และขั้นตอนการดำเนินการความเสี่ยง วัตถุประสงค์ของการควบคุม และการควบคุมการดำเนินงานบางส่วนอยู่แล้ว สามารถช่วยลดเวลาและค่าใช้จ่ายในการดำเนินโครงการ ISMS ได้อย่างมาก แสดงในภาพที่ 2.6

Figure 2—Time and Cost Savings on Respective PDCA Phases Associated With the IT Initiative

IT Initiative	Ready Information Inventory	Time and Cost Savings on the Following PDCA Phases
COBIT	Policies, procedures, risk assessment, control objectives and controls	Phase 2—Obtain management support. Phase 3—Select the proper scope of implementation. Phase 4—Define a method of risk assessment. Phase 5—Prepare an inventory of information assets to protect, and rank assets according to risk classification based on risk assessment. Phase 6—Manage the risks, and create a risk treatment plan. Phase 7—Set up policies and procedures to control risks. Phase 8—Allocate resources, and train the staff.
SAS 70 Type I and Type II	Policies, procedures, risk control objectives and controls	Phase 6—Manage the risks, and create a risk treatment plan. Phase 7—Set up policies and procedures to control risks.
NIST	Risk assessment, detailed control objectives and controls	Phase 2—Obtain management support. Phase 3—Select the proper scope of implementation. Phase 4—Define a method of risk assessment. Phase 6—Manage the risks, and create a risk treatment plan.
PCI DSS	Detailed control within the PCI DSS framework	Phase 6—Manage the risks, and create a risk treatment plan.

ภาพที่ 2.6 มาตรฐานอื่นที่ตรงกับการดำเนินงานในมาตรฐาน ISO 27001

ที่มา : Figure 2 – Time and Cost Saving on Respective PDCA Phases Associated With the IT Initiative [online] : เข้าถึง 10 ก.พ. 2562. จาก https://www.slideshare.net/YerlinSturdivant/planning-forand-implementing-iso-27001

2.5.2 การวางแผน ISMS ตามมาตรฐาน ISO กระบวนการที่สำคัญ ได้แก่

1. การตรวจสอบภายใน (Internal Audit) ในระหว่างขั้นตอนการวางแผนเบื้องต้น ข้อมูลจากการตรวจสอบภายในจะเป็นประโยชน์สำหรับการพัฒนากลยุทธ์ในการดำเนินงาน

2. ฝ่ายไอทีต้องทุ่มเททรัพยากร และเวลาในการทำกิจกรรมที่เกี่ยวข้องกับการเริ่มต้นกระบวนการตามมาตรฐาน ISO 27001 ข้อมูลรายละเอียดกระบวนการและนโยบายด้านเทคโนโลยี

สารสนเทศขององค์กร และการกำหนดกระบวนการและการควบคุมด้านเทคโนโลยีสารสนเทศที่มีอยู่จะช่วยให้ทำความเข้าใจว่ากระบวนการที่มีอยู่สอดคล้องกับข้อกำหนด หรือไม่

2.5.3 การตัดสินใจ ว่าเมื่อใดและอย่างไรที่จะใช้มาตรฐาน ISO 27001 ขึ้นอยู่กับปัจจัยหลายด้าน ได้แก่ วัตถุประสงค์ และลำดับความสำคัญทางธุรกิจ ระดับวุฒิภาวะของระบบที่มีอยู่ในปัจจุบัน การยอมรับและความตระหนักของผู้ใช้ ความสามารถในการตรวจสอบภายใน ภาระผูกพันตามสัญญา ความต้องการของลูกค้า ความสามารถในการปรับตัว ความยึดมั่นในกระบวนการภายใน ความพยายามในการปฏิบัติตามข้อกำหนดและกฎหมายที่มีอยู่ และโปรแกรมการฝึกอบรมที่มีอยู่

2.5.4 การตรวจสอบ

1. ทบทวนระบบ ISMS อย่างไม่เป็นทางการ รวมถึงตรวจสอบการดำรงอยู่และความครบถ้วนสมบูรณ์ของเอกสารสำคัญ เช่น นโยบายความปลอดภัยขององค์กร แผนการแก้ไขปัญหาความเสี่ยง (RTP) คำชี้แจงการบังคับใช้ (SOA)

2. ทดสอบ ISMS ตามข้อกำหนดที่ระบุไว้ใน ISO 27001 การตรวจสอบรับรองมักจะดำเนินการโดยผู้ตรวจสอบที่ลงทะเบียน

3. ตรวจสอบเป็นระยะเพื่อยืนยันว่าองค์กรยังคงปฏิบัติตามมาตรฐาน การบำรุงรักษาการรับรอง ต้องมีการตรวจสอบการประเมินใหม่เพื่อยืนยันว่า ISMS ยังคงทำงานตามที่ระบุ

2.5.5 ขั้นตอนการดำเนินการ ตามกระบวนการ PDCA

1. ระบุวัตถุประสงค์ของธุรกิจ เป็นขั้นตอนที่ช่วยสนับสนุนด้านการจัดการวัตถุประสงค์หลักมาจากภารกิจ แผนยุทธศาสตร์ และเป้าหมายด้านเทคโนโลยีสารสนเทศขององค์กร โดยระบุ และจัดลำดับความสำคัญของวัตถุประสงค์

2. รับการสนับสนุนด้านการจัดการ ผู้บริหารต้องให้ความสำคัญกับการจัดตั้ง การวางแผน การดำเนินงาน การติดตามตรวจสอบ การบำรุงรักษา และการปรับปรุงระบบรักษาความปลอดภัยข้อมูลสารสนเทศอย่างจริงจัง ต้องมีกิจกรรมเพื่อสร้างความมั่นใจว่ามีทรัพยากรที่เหมาะสมในการทำงานในระบบ ISMS และพนักงานทุกคนที่ได้รับผลกระทบจาก ISMS ต้องรับการฝึกอบรมเพื่อให้มีความสามารถที่เหมาะสมในการปฏิบัติงานที่มีความปลดภัย

3. กำหนดขอบเขต ขอบเขตตามมาตรฐาน ISO 27001 อาจครอบคลุมทุกส่วนหรือบางส่วนขององค์กรก็ได้ การระบุขอบเขตของการดำเนินงานช่วยประหยัดเวลา และงบประมาณขององค์กรได้

4. เขียนนโยบาย ISMS สั้น ๆ พิจารณาเลือกใช้วิธีการที่เหมาะสม

5. กำหนดวิธีการและกลยุทธ์การประเมินความเสี่ยงของคุณ มาตรฐาน ISO 27001 มิได้ระบุวิธีการประเมินความเสี่ยงที่จะใช้ จึงอาจพิจารณาเลือกใช้วิธีการที่เหมาะสม เช่น วิธีการที่จะใช้เพื่อประเมินความเสี่ยงต่อสินทรัพย์ที่ระบุในรายการสินทรัพย์ฯ ความเสี่ยงที่ไม่สามารถรองรับได้ และต้องได้รับการป้องกันหรือบรรเทา การใช้มาตรฐาน NIST Special Publication (SP) 800-30 คู่มือการบริหารความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศ และการจำแนกประเภทสินทรัพย์และการจำแนกประเภทข้อมูลโดยองค์กร

6. สร้างแผนการจัดการความเสี่ยง และดำเนินการจัดการความเสี่ยงตามแผน

7. ตั้งค่านโยบาย และขั้นตอนการควบคุมความเสี่ยง

8. จัดสรรทรัพยากรที่จำเป็น และดำเนินการฝึกอบรมพร้อมโปรแกรมการรับรู้

9. ตรวจสอบ ISMS อย่างระมัดระวัง

10. เตรียมความพร้อมสำหรับการตรวจสอบภายใน

11. ทบทวนการจัดการเป็นระยะ

2.5.6 ระบุระดับผลกระทบต่อสินทรัพย์ข้อมูลสารสนเทศต่อระดับความปลอดภัย กำหนดเป็นสูง ปานกลาง และต่ำ

1. ระบุความเสี่ยง จำแนกประเภทตามความรุนแรง และความเสี่ยง

2. หลังจากระบุความเสี่ยงและระดับของ CIA แล้วให้กำหนดค่าความเสี่ยง

3. จากค่าความเสี่ยงให้พิจารณาว่าความเสี่ยงนั้นยอมรับได้หรือไม่ และควรใช้วิธีใดในการจัดการความเสี่ยง

4. ภายหลังประเมินความเสี่ยงเสร็จสิ้นแล้ว ให้จัดทำรายการสินทรัพย์ข้อมูลสารสนเทศที่มีความเสี่ยงที่ไม่สามารถยอมรับได้และจะต้องมีการควบคุม (รายงานการประเมินความเสี่ยง) ซึ่งระบุถึงมูลค่าความเสี่ยงสำหรับแต่ละสินทรัพย์

2.5.7 จัดการความเสี่ยงและสร้างแผนการบริหารความเสี่ยง

ขั้นตอนต่อไป คือ ทำการวิเคราะห์ช่องว่างด้วยตัวควบคุมตามมาตรฐาน (ดูภาคผนวก A ของ ISO 27001 หรือ ISO 27002) เพื่อสร้าง RTP และ SOA ในส่วนนี้เป็นเอกสารสำคัญที่ต้องได้รับการอนุมัติจากผู้บริหารเกี่ยวกับความเสี่ยงที่เหลืออยู่ โดยดำเนินการดังนี้

1. กำหนดความเสี่ยงที่ยอมรับได้ (ยอมรับ โอน ลด และหลีกเลี่ยง)
2. ระบุการควบคุมการปฏิบัติงาน และการควบคุมด้านต่าง ๆ โดยใช้การวิเคราะห์ช่องว่างทางศักยภาพ (Gap Analysis)
3. กำหนดรายการที่ดำเนินการควบคุม

Figure 5—Risk Treatment Plan

Risk	Explanations of Risk Treatment Categories			
	Reduce	Avoid	Accept	Transfer
Information security risk	Reduce or mitigate the risk; refer to the 133 controls to identify and implement suitable information security controls or the other initiatives in the organization, e.g., ITIL, COBIT.	Avoid the situation that creates the risk by proactive planning, redesigning or reengineering.	Management should acknowledge the residual risk if there is no cost-effective solution.	Is it possible to transfer some or all of the risk to a third party (insurer)?
Risk and Risk Treatment Example With Applicable Controls				
Inappropriately configured firewall rule sets increasing the risk of unauthorized access to critical and/or privileged network resources	Management performs and reviews vulnerability assessments on an annual basis.	Management has defined perimeter security controls, including firewalls and intrusion detection systems.		

ภาพที่ 2.7 คำอธิบายแผนการจัดการความเสี่ยง

ที่มา : Figure 5 – Risk Treatment Plan [online] : เข้าถึง 10 ก.พ. 2562. จาก https://www.slideshare.net/YerlinSturdivant/planning-forand-implementing-iso-27001

4. SOA จะอธิบายถึงวัตถุประสงค์ของการควบคุม ตัวควบคุมที่เลือกจากภาคผนวก A และเหตุผลสำหรับการใช้การควบคุมหรือไม่ใช้การควบคุม

Figure 6—Example SOA for Applicable Controls				
Control Objective	**Control From Annex A of ISO/IEC 270001**	**Adopted or Not Adopted**	**Justification**	**Organization Procedures and Reference**
Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.	10.5.1 Information Backup	Adopted	Management has implemented a strategy for cyclical backup of data and programs.	XXX—Information security policy XXX—Information backup and media protection procedure

ภาพที่ 2.8 ตัวอย่างการใช้มาตรการควบคุมการดำเนินการ

ที่มา : Figure 6 – Example SOA for Applicable Controls [online] : เข้าถึง 10 ก.พ. 2562. จาก https://www.slideshare.net/YerlinSturdivant/planning-forand-implementing-iso-27001

2.5.8 กำหนดนโยบายและขั้นตอนในการควบคุมความเสี่ยง

การควบคุมที่รับรองไว้ใน SOA องค์กรจะต้องมีการแถลงนโยบาย และเอกสารความรับผิดชอบโดยละเอียด เพื่อระบุบทบาทของผู้ใช้ในการปฏิบัติตามนโยบาย และขั้นตอน รายการนโยบายและขั้นตอนที่เกี่ยวข้อง

Figure 7—Referenced Policies and Procedures to Control Risks Example						
ISO 27001:2005 Controls						
Clause	**Section**	**Control/Control Objective**	**Existing Controls**	**Excluded Controls**	**Justification**	**Reference Policies and Procedures**
Information systems acquisition, development and maintenance	12.4	Security of system files	Yes		Best practices	Systems acquisition/ development policy
	12.4.1	Control of operational software				
	12.4.2	Protection of system test data				

ภาพที่ 2.9 ตัวอย่างการกำหนดรายการนโยบายในขั้นตอนควบคุม

ที่มา : Figure 7 – Reference Policies and Procedures to Control Risks Example [online] : เข้าถึง 10 ก.พ. 2562. จาก https://www.slideshare.net/YerlinSturdivant/planning-forand-implementing-iso-27001

2.5.9 จัดสรรทรัพยากร และฝึกอบรมพนักงาน

สิ่งสำคัญประการหนึ่งสำหรับการจัดการ คือ ทรัพยากรเพียงพอในการจัดการ พัฒนา บำรุงรักษา และใช้ระบบ ISMS จึงจำเป็นต้องมีการจัดทำเอกสารตรวจสอบสำหรับทรัพยากรและผู้ฝึกอบรม

2.5.10 ติดตามการดำเนินการของ ISMS

การตรวจสอบภายในเพื่อการติดตาม และทบทวน ประกอบด้วย การทดสอบ การควบคุม และระบุการดำเนินการแก้ไข การป้องกัน เพื่อให้วงจร PDCA สมบูรณ์ ระบุระยะระหว่างการควบคุมกับสภาพการทำงานจริง โดยระบุการควบคุมแก้ไข และการป้องกันที่จำเป็น รวมทั้งจากการปฏิบัติตามระเบียบขององค์กร ขั้นตอนที่สำคัญ คือ การทบทวนการจัดการโครงการ ผลการตรวจสอบ และการทบทวนเป็นระยะ ๆ โดยให้มีการจัดทำเป็นเอกสารรายงาน

2.5.11 เตรียมความพร้อมสำหรับการตรวจสอบรับรอง

การรับรองมาตรฐาน ISO ต้องดำเนินการตรวจสอบภายใน ทบทวนการจัดการและกิจกรรมในกระบวนการ PDCA อย่างครบวงจร รวมถึงมีหลักฐานการดำเนินการตรวจสอบและข้อแนะนำ ผู้ตรวจสอบเบื้องต้นจะตรวจสอบเอกสาร ISMS เพื่อกำหนดขอบเขต และเนื้อหาของ ISMS วัตถุประสงค์ของการสอบทาน และตรวจสอบว่ามีหลักฐานเพียงพอ และมีการสอบทานเอกสารที่ส่งให้ผู้ตรวจสอบมาตรฐาน

2.5.12 ดำเนินการตรวจสอบการประเมินเป็นระยะ ๆ

การตรวจสอบเป็นระยะช่วยยืนยันว่าองค์กรยังคงปฏิบัติตามมาตรฐาน การบำรุงรักษาการรับรองต้องมีการตรวจสอบการประเมินใหม่เป็นระยะ ๆ โดยมีการดำเนินการตามวงจร PDCA และช่วยให้การจัดการ ISMS สามารถรู้ได้ว่าองค์กรมีความคืบหน้าไปเท่าไหร่ และปรับปรุงก้าวหน้าในระดับใด สิ่งนี้มีผลโดยตรงต่อเวลา และค่าใช้จ่ายที่เกี่ยวข้อง

กล่าวโดยสรุป ความสำเร็จที่แท้จริงของ ISO 27001 คือ การจัดวางสิ่งต่าง ๆ ให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ และประสิทธิภาพในการบรรลุวัตถุประสงค์ดังกล่าว องค์กรต้องมีความเข้าใจอย่างละเอียดเกี่ยวกับขั้นตอนการใช้ PDCA หากไม่มีแผนงาน ISO 27001 ที่ได้รับการพัฒนาอย่างดี การนำมาตรฐาน ISO 27001 ไปใช้ จะเป็นการดำเนินการที่ใช้เวลา และเสียค่าใช้จ่ายสูง เพื่อให้บรรลุผลการลงทุนตามแผน (ROI) ต้องพัฒนาแผนการดำเนินงานโดยคำนึงถึงเป้าหมายขั้นสุดท้าย ทั้งนี้ การฝึกอบรม และการตรวจสอบภายในเป็นส่วนสำคัญของการปฏิบัติตามมาตรฐาน ISO 27001

2.6 การรักษาความปลอดภัยสำหรับอุปกรณ์ และระบบสารสนเทศแต่ละประเภท

Vasant Raval and Ashok Fichadia (2007) กล่าวถึงการรักษาความปลอดภัยแต่ละระบบที่จำเป็นต้องมีข้อกำหนด และวิธีการในการรักษาความปลอดภัยที่แตกต่างกัน การแยกการควบคุมความปลอดภัยข้อมูลสารสนเทศตามองค์ประกอบของระบบ ทำให้แยกขั้นตอนปฏิบัติที่เกี่ยวข้องกับแต่ละส่วนงานได้ชัดเจนยิ่งขึ้น

2.6.1 การควบคุมข้อมูลสารสนเทศ และการให้บริการ

1. กำหนดนโยบายและการปฏิบัติ (Security Policy and Practice) เป็นการกำหนดกฎระเบียบ ขั้นตอน อำนาจ ในการเข้าถึงข้อมูล

2. การระบุ และยืนยันตัวตน (Identification and Authentication) เพื่อค้นหาและรับรู้ว่าใครเป็นผู้เข้าถึงข้อมูล

3. การเข้าใช้งาน และกำหนดสิทธิ์ในการใช้งาน (Access and Authorization) เป็นกระบวนการอนุญาตให้ผู้ใช้ที่มีสิทธิ์เข้าใช้งานข้อมูลสารสนเทศและระบบได้ตามสิทธิ์

4. การไหลของข้อมูลสารสนเทศ (Information Flow) เป็นกระบวนการกำหนดเส้นทางของข้อมูลสารสนเทศว่าสามารถผ่านไปยังเส้นทางใดบ้าง จำเป็นต้องเข้ารหัสหรือไม่

5. ความพร้อมในการใช้งาน และความต่อเนื่องในการให้บริการ (Availability and Continuity) เป็นการป้องกันภัยคุกคามต่อข้อมูลสารสนเทศเพื่อให้บริการได้อย่างต่อเนื่อง

6. การบันทึกข้อมูลจราจรทางคอมพิวเตอร์ และเส้นทางสื่อสาร (Logs and Trails) เป็นกระบวนการจัดเก็บข้อมูลว่าเชื่อมต่อจากที่ใด ระบุกระบวนการที่ทำ วันที่และเวลาเข้าออกจากระบบ เพื่อบันทึกพฤติกรรมการเข้าสู่ระบบ

7. การตรวจสอบความเสี่ยง (Risk-Based Audit) เป็นกระบวนการตรวจสอบความเสี่ยงที่อาจเกิดขึ้น ขั้นตอนนี้เป็นส่วนหนึ่งของขั้นตอนการประเมินสินทรัพย์ข้อมูลสารสนเทศ

8. การจัดการเพื่อควบคุมระบบ (Management of Control Systems) เป็นกระบวนการกำหนดขั้นตอนกระบวนวิธีการเพื่อควบคุมระบบ นับตั้งแต่การกำหนดนโยบาย การบังคับใช้นโยบาย การสร้าง และบำรุงรักษาระบบควบคุม และการประเมินการควบคุมว่าสามารถตอบสนองต่อความเสี่ยงได้อย่างเหมาะสมหรือไม่

2.6.2 การควบคุมระบบปฏิบัติการ

1. การยืนยันตัวตน (Authentication)
2. การกำหนดสิทธิ์ (Authorization)
3. ความสัมพันธ์ที่น่าความเชื่อถือ (Trust Relationships)
4. ตารางปฏิบัติงาน (Job Scheduling)
5. ไฟล์ซิสเต็ม (File Systems)
6. ซอฟต์แวร์อัพเดต (Software Update)

2.6.3 การควบคุมแอปพลิเคชัน

แบ่งการควบคุมตามการทำงานของแอปพลิเคชันเป็น 3 ชั้น (tier) คือ Presentation Layer หรือ Presentation tier หมายถึง ส่วนของโปรแกรมที่มีผลกระทบต่อการมองและสัมผัสของผู้ใช้ Business Layer หรือ Business tier เป็นกระบวนการระหว่างทาง โดยรับมาจาก Presentation tier และนำข้อมูลไปดำเนินการตามกระบวนการทางธุรกิจ และ Data Layer หรือ Data tier เป็นกระบวนการของระบบที่เกี่ยวกับการเข้าถึงฐานข้อมูล

จากนั้น แบ่งประเภทแอปพลิเคชันขึ้นอยู่ความสัมพันธ์ระหว่างคอมพิวเตอร์ของผู้ใช้และเครื่องแม่ข่าย โดยแบ่งเป็น Thin client application คอมพิวเตอร์ของผู้ใช้จะมีการทำงานแค่ระดับ Presentation tier อาจเป็นเว็บบราวเซอร์ทำหน้าที่รวบรวมเอาท์พุทและแสดงผลบนจอภาพ ส่วน Business tier และ Data tier ทั้งหมดจะทำงานบนเว็บเซิร์ฟเวอร์ และ Fat client application คอมพิวเตอร์ของผู้ใช้มีการทำงานทั้งระดับ Presentation tier, Business tier มีเพียงส่วน Data tier ที่ทำงานอยู่บนเซิร์ฟเวอร์ การแบ่งแอปพลิเคชันเป็นลำดับชั้นทำให้สามารถแบ่งการพัฒนาแอปพลิเคชันในแต่ละระดับ(tier) ออกจากกัน ง่ายต่อการปรับปรุงแอปพลิเคชันในแต่ละ tier และง่ายต่อการควบคุม

พิจารณาความเสี่ยงในแต่ละ tier และดำเนินการควบคุม เช่น ความเสี่ยงที่มักพบเกิดจากแอปพลิเคชันที่ใช้งานบนเว็บ คือ Boundary Checking ใช้การควบคุม กำหนดให้มีกระบวนการตรวจสอบอินพุทของผู้ใช้ เพื่อป้องกันการโจมตีในรูปแบบดังกล่าวต้องจำกัดข้อมูลนำเข้าให้อยู่ในรูปแบบเฉพาะที่ต้องการ เป็นต้น

สรุปแนวทางควบคุมแอปพลิเคชัน ดังนี้

1. ตรวจสอบอินพุทของผู้ใช้ (Data validation)
2. การยืนยันตัวตนผ่านแอปพลิเคชัน (Application Authentication)
3. เข้ารหัสก่อนส่งไปยังเซิร์ฟเวอร์ (Encrypt)

4. การจัดการเซสชั่น (Session Management)

5. การเปลี่ยนแปลงการควบคุมและการจัดการ (Change Control and Change Management) เพื่อแก้ไขจุดบกพร่องที่ตรวจพบ

6. แบ่งแยกหน้าที่เพื่อไม่ได้ให้บุคลากรเพียงคนเดียวดูแลทุกขั้นตอน ทำให้แน่ใจได้ว่าไม่มีใครคนใดคนหนึ่งทำการเปลี่ยนแปลงที่ก่อให้เกิดความเสียหาย ให้แบ่งขั้นตอนการเปลี่ยนแปลงเป็น 3 ส่วน คือ (1) เปลี่ยนแปลงสิทธิ์ (2) เปลี่ยนแปลงการโปรแกรม (3) เปลี่ยนแปลงการดำเนินการ

2.6.4 การควบคุมฐานข้อมูล

1. ดำเนินการยืนยันตัวตน (Authentication)

2. ปรับเปลี่ยนบัญชีเริ่มต้น (Default Accounts)

3. ควบคุมการทำงานผ่าน Batch Scripts

4. ป้องกันการใช้คำสั่ง Process Listings

5. ไม่ส่งข้อมูล ID และ password ผ่านทาง command line

6. ตรวจสอบไม่ให้มี password hash อยู่ใน registry key

7. ไม่ใช้การยืนยันตัวตนด้วยระบบปฏิบัติการเพื่อเข้าสู่ฐานข้อมูลจากเครื่องคอมพิวเตอร์ภายนอกเครือข่าย

8. ในกรณีกลับกัน ไม่ใช้การเข้าสู่ฐานข้อมูลที่เปิดให้ใช้ระบบจัดการฐานข้อมูล เพื่อมีสิทธิเข้าสู่ระบบปฏิบัติการ

9. ปิดฟังก์ชันทั้งหมด และเปิดใช้งานเฉพาะเท่าที่จำเป็น

10. ตรวจสอบช่องโหว่ที่สำคัญ คือ ขาดการออกแบบสถาปัตยกรรมความปลอดภัยของฐานข้อมูลบนแอปพลิเคชัน หรือการเขียนชุดคำสั่ง SQL ไม่รัดกุม

11. ปิดไม่ให้ใช้งาน Bypassing Application Controls

12. ตรวจสอบการทำงานของ Single sign-on

13. ป้องกัน SQL Injection

2.6.5 การควบคุมการสื่อสาร

1. ตรวจสอบควบคุมโครงสร้างพื้นฐานทางการสื่อสาร

2. ตรวจสอบความจำเป็นในการใช้การควบคุมทางไกล หากไม่มีความจำเป็นให้ปิด port กรณีมีความจำเป็นต้องเปิดให้บริการต้องมีกระบวนการตรวจสอบการยืนยันตัวตน

3. ตรวจสอบการลงชื่อเข้าใช้ระบบ และไม่มีการใช้งานรหัสผ่านตั้งต้น กำหนดให้ระบบป้องกันการเข้าใช้จากผู้บุกรุกเมื่อมีความพยายามเข้าใช้ระบบเกินจำนวนครั้งที่กำหนด

4. ให้ความรู้แก่พนักงาน แจ้งเตือนลูกค้า ตรวจสอบกระบวนการควบคุม และการตรวจสอบ log

5. ตรวจสอบให้การตั้งรหัสไม่ให้สามารถคาดเดาได้โดยง่าย

6. ดำเนินการเข้ารหัสเพื่อป้องกันการเปิดอ่านโดยง่าย

7. ใช้วิธีการแบ่งแยกเครือข่ายทาง logical โดยใช้เทคโนโลยี virtual local area network (VLAN) และ quality of service (QoS)

2.6.6 การควบคุมความปลอดภัยบนระบบเครือข่าย

1. การยืนยันตัวตน 2 ปัจจัย

2. Packet Filtering Firewalls เพื่อตรวจสอบ IP address และ port จาก data packet header ทุกตัว จากนั้นจะทำงานตาม rules ซึ่งได้กำหนดไว้ว่าจะให้ส่งผ่าน (allow) หรือตัดทิ้ง (drop) ข้อมูลสำคัญที่ตรวจสอบได้แก่ Source IP address, Destination IP address, Source port number, Destination port number

3. Stateful Packet Inspection Firewalls การทำงานของ packet filtering firewall เรียกว่าเป็น stateless ซึ่งจะเพิ่มเติมการตรวจสอบโดยนำแพคเก็ตที่นำส่งมาก่อนหน้ามาพิจารณาเปรียบเทียบกับแพคเก็ตที่ได้รับใหม่ ทำให้ทราบว่าเป็น แพคเก็ตใหม่ หรือเป็นส่วนของการเชื่อมต่อเดิม

4. Application-Level Proxy Firewalls เรียกอีกอย่างว่า gateway firewall การทำงานมีความแตกต่างจากสองประเภทที่กล่าวมา เนื่องจากเป็นการทำงานในระดับ application level security ทำงานโดย application proxy program เป็นตัวกลางในการรับส่งข้อมูลจากคอมพิวเตอร์แต่ละเครื่องส่งคำขอมายัง application proxy และรับข้อมูลตอบกลับจาก application proxy มีการยืนยันตัวตนที่มีความปลอดภัย ไม่อนุญาตให้มีการเชื่อมต่อระหว่างผู้ส่ง และผู้รับโดยตรง สามารถทำงานแบบ transparent filtering การกำหนด rule ทำได้ง่าย และสามารถทำการกรองได้อย่างมีประสิทธิภาพ

5. กำหนดนโยบายความปลอดภัย และทบทวนแก้ไขให้เป็นปัจจุบัน

6. การตรวจสอบระบบ และการควบคุมทางเทคนิค เช่น ไม่อนุญาตให้มีการติดตั้งใช้งานโมเด็มที่มีการเชื่อมต่อกับภายนอกเข้าสู่เครือข่ายภายใน

7. กำหนดให้สิทธิน้อยที่สุดเมื่อติดตั้งใช้งาน SNMP สำหรับ service ที่ไม่มีความจำเป็นให้ปิด SNMP ทำการปิดกั้น SNMP จากภายนอก หรือใช้ ingress filtering รวมทั้งให้เปลี่ยนแปลงค่าเริ่มต้นต่าง ๆ

2.6.7 การควบคุมความปลอดภัยบนเว็บไซต์

1. ป้องกันตั้งแต่ระบบปฏิบัติการ โดยตรวจสอบแก้ไขบัญชีผู้ใช้เริ่มต้น ให้กำหนดสิทธิ์น้อยที่สุดในการเข้าถึง (least privilege)

2. Web Server Software เมื่อติดตั้งซอฟต์แวร์เรียบร้อยแล้วจะทำงานด้วย script และ application จำนวนมาก ซึ่งทำให้เกิดความเสี่ยงที่เรียกว่า Web environment เช่น คำสั่งที่ทำให้แสดง code ของ script หรือ application, คำสั่ง error message ที่จะแสดงรายการข้อผิดพลาดให้แก่ผู้ใช้ ผู้บุกรุกสามารถใช้ประโยชน์เพื่อให้ได้รายละเอียดข้อมูลของเว็บไซต์เพื่อหาช่องโหว่อื่น

3. Add on Components การบุกรุกเว็บเซิร์ฟเวอร์มักจะผ่านทาง add on component ที่มีช่องโหว่ เช่น ISAP (Internet Server Application Programming Interface), DLL (Dynamic Link Library) การทำงานของ buffer overflow อยู่ใน ISAPI filter รองรับการทำงานร่วมกับ IPP (Internet Printing Protocol) เป็นช่องทางที่ผู้บุกรุกมักใช้เพื่อแทรกข้อมูลลงใน buffer

4. Input Validation เป็นเทคนิคเพื่อให้แน่ใจว่าการรับ ข้อมูลเข้าสู่ระบบเป็นข้อมูลในรูปแบบตามที่กำหนด ขั้นตอนที่สำคัญเริ่มจากการกำหนดค่าที่ต้องการ เช่น ประเภทข้อมูล ขนาด ความยาวตัวอักษร minimum และmaximum length ตัวอักขระที่ยอมรับให้ใช้งานได้ และกำหนดค่าตัวเลขที่ใช้งาน

5. Cross Site Scripting (XSS) เป็นการโจมตีที่ผู้บุกรุกแทรก code หรือ script ไว้บนเว็บที่จะถูกเรียกใช้ เมื่อผู้ใช้เข้าเว็บไซต์จะมีการเรียก code ที่เป็นอันตรายด้วยเนื่องจากเชื่อถือเว็บไซต์ที่เข้าใช้งาน ความเสี่ยงจากการโจมตีประเภทนี้ นอกจากการแสดงข้อความ pop up อาจมีการสร้าง link เพื่อนำไปยังเว็บไซต์ที่เป็นอันตราย สามารถควบคุมด้วยการตรวจสอบเว็บไซต์ทั้งหมดว่ามีการแสดงข้อมูลอินพุทของผู้ใช้ที่ส่วนใดของเว็บไซต์บ้างดำเนินการตรวจสอบข้อมูลนำเข้าอย่างเข้มงวดโดยทำที่ฝั่ง server side และทดสอบข้อมูลที่อาจเป็นไปได้ทั้งหมด เข้ารหัสข้อมูลนำเข้าจากผู้ใช้เพื่อป้องกันการโจมตีดังกล่าวโดยการแปลงอักขระเป็นรูปแบบ HTML entity encoding เช่น “<” and “>” ให้แปลงเป็น “&lt” and “&gt”

6. Buffer Overflows ปัญหาอาจเกิดจากเว็บไซต์มีการใช้ library ของ third party ซึ่งมีช่องโหว่ด้าน buffer overflow โดยทั่วไปการตรวจสอบ server side validation จะช่วยตรวจสอบ

ขนาดข้อมูลนำเข้าไม่ให้เกิน buffer ตรวจสอบว่าการเขียนโค้ดมีส่วนตรวจสอบ size check และรวมรวมการใช้งาน library ของ third party ให้ตรวจสอบเพื่ออัพเดทได้อย่างรวดเร็วเมื่อมีการปรับปรุง

7. การโจมตีผ่าน SQL code เป็นรูปแบบที่พบมากโดยเฉพาะ web application ที่ต้องมีการเชื่อมต่อกับฐานข้อมูลหลังบ้าน ความเสี่ยงที่สำคัญคือ การ bypass เพื่อควบคุมการยืนยันตัวตน และการใช้เทคนิคต่าง ๆ เพื่อให้ได้ข้อมูลที่มีความสำคัญ หากไม่สามารถปิดการใช้งานได้ให้กำหนดสิทธิในการทำงานน้อยที่สุด และแทนที่การใช้งาน SQL statement ด้วยการใช้ Web application และใช้งาน user define store procedure เนื่องจากการทำงานดังกล่าวต้องการ parameter ที่มีจำนวนเฉพาะทำให้การโจมตีเป็นไปได้ยากขึ้น

8. Error Handling การแสดงข้อความเพื่อแจ้งความผิดพลาดของระบบเมื่อการร้องขอผิดพลาดหรือหมดระยะเวลาเป็นการทำงานที่พบกันได้โดยปกติทั่วไป แต่ผู้บุกรุกสามารถอาศัยข้อความแสดงรายละเอียดต่าง ๆ เพื่อค้นหาช่องโหว่ หรือข้อมูลที่สำคัญ

2.7 การตรวจประเมินภายในความปลอดภัยข้อมูลสารสนเทศ

การตรวจประเมินความปลอดภัยข้อมูลสารสนเทศเป็นขั้นตอนที่สำคัญในกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศ Bill Hayes (2003) ได้อธิบายในเชิงปฏิบัติ สรุปได้ดังนี้

“การตรวจประเมิน” คือ กระบวนการที่องค์กรภายนอกจะทำการตรวจสอบองค์กร และรายงานเป็นลายลักษณ์อักษร วลีที่ว่า “การทดสอบการเจาะ” (penetration test) ที่ใช้สลับกับวลี “การตรวจประเมินความปลอดภัยของคอมพิวเตอร์” (computer security audit) ทั้งสองวลีนี้ไม่ใช่สิ่งเดียวกัน การทดสอบการเจาะ เป็นความพยายามในการค้นหาช่องโหว่ในทรัพยากรที่สำคัญอย่างเช่น ไฟร์วอลล์ หรือเว็บเซิร์ฟเวอร์ ซึ่งนักทดสอบใช้งานจากภายนอกไฟร์วอลล์เพื่อจำลองวิธีการโจมตีโดยแฮกเกอร์ ในทางกลับกันการตรวจประเมินความปลอดภัยของคอมพิวเตอร์ คือ การประเมินทางเทคนิคที่เป็นระบบ และสามารถวัดผลได้ว่า การใช้นโยบายความปลอดภัย (Security Policy) ขององค์กรเป็นอย่างไร

ผู้ตรวจประเมินความปลอดภัยข้อมูลสารสนเทศทำหน้าที่ในการตรวจสอบตั้งแต่การสัมภาษณ์ส่วนบุคคล สแกนช่องโหว่ ตรวจสอบการตั้งค่าระบบปฏิบัติการ วิเคราะห์เครือข่าย และข้อมูลบันทึกเหตุการณ์ประวัติของระบบ โดยมุ่งเน้นความสนใจไปยังนโยบายการรักษาความปลอดภัยซึ่งเป็นรากฐานของกลยุทธ์ด้านความปลอดภัยขององค์กรที่มีประสิทธิภาพ ตัวอย่างคำถามสำคัญ เช่น รหัสผ่านยากต่อการเจาะเป็นอย่างไร มีรายการควบคุมการเข้าถึง (ACLs) บนอุปกรณ์

เครือข่ายเพื่อควบคุมว่าใครสามารถเข้าถึงข้อมูลที่ใช้ร่วมกันได้ หรือไม่ ระบบปฏิบัติการ (Operation System) และแอปพลิเคชัน (Application) มีการปรับปรุงให้เป็นปัจจุบันหรือไม่ เป็นต้น การตอบคำถามเหล่านี้ต้องดำเนินการอย่างเคร่งครัดจริงจัง เพื่อให้สารมารถประเมินความปลอดภัยของข้อมูลที่สำคัญได้อย่างถูกต้อง

การตรวจประเมินความปลอดภัยข้อมูลสารสนเทศ แบ่งได้ 2 ประเภท คือ การตรวจประเมินโดยผู้เชี่ยวชาญภายนอก และการตรวจประเมินโดยบุคลากรภายใน การใช้ผู้ตรวจสอบภายนอกมีข้อดี คือ ผู้ตรวจประเมินมีประสบการณ์ ใช้ชุดซอฟต์แวร์รักษาความปลอดภัยในการสแกนช่องโหว่ ข้อเสียที่สำคัญ คือ ค่าใช้จ่ายสูง และผู้ตรวจประเมินที่มีคุณสมบัติ และประสบการณ์หาได้ยากมาก นอกจากนี้ความสำเร็จของการตรวจสอบขึ้นกับคุณภาพของการสื่อสารที่จัดตั้งขึ้นระหว่างองค์กรกับผู้ตรวจสอบ ทำให้การตรวจสอบภายนอกดูเป็นการกระทำที่หวือหวามากกว่าเป็นการแก้ปัญหาอย่างถาวร

การตรวจสอบภายในโดยบุคลากรภายในเป็นเรื่องง่ายและมีประสิทธิภาพสูง ช่วยให้สามารถรวบรวมข้อมูลพื้นฐานด้านความปลอดภัย และตรวจสอบว่านโยบายในปัจจุบันมีประสิทธิภาพหรือไม่ อย่างไรก็ตามข้อบกพร่อง คือ ผู้ตรวจสอบภายในมักจะขาดประสบการณ์ และเครื่องมือที่จำเป็น ปัญหาดังกล่าวสามารถแก้ไขได้โดยการฝึกอบรมให้กับพนักงาน ข้อดีอีกประการ คือ ราคาถูก และ มีประสิทธิภาพในแง่ของกระบวนการ ไม่รบกวนกระบวนการทำงานที่มีอยู่ภายในบริษัท

ขั้นตอนในการตรวจสอบภายใน สามารถสรุปได้ดังนี้

1. กำหนดขอบเขตของการตรวจสอบ
2. กำหนดภัยคุกคามที่ต้องเผชิญ
3. การคำนวณความเสี่ยง
4. การควบคุมที่จำเป็น

2.8 การวิเคราะห์ช่องว่างทางศักยภาพ (Gap Analysis)

เครื่องมือที่มีความสำคัญอย่างหนึ่งในการวัดระดับของปัญหาในปัจจุบันกับเป้าหมายที่ต้องการไปถึงนั่นคือ การวิเคราะห์ช่องว่างทางศักยภาพ (Gap analysis) เป็นแนวคิด ทฤษฎี และการประยุกต์ใช้กับระบบบริหารงานคุณภาพ โดยเปรียบเทียบประสิทธิภาพของบริษัท ณ ปัจจุบันกับระดับที่ต้องการ หรือสิ่งที่ควรจะเป็น สำหรับการประเมินในมิติต่าง ๆ องค์กรจะอ้างอิงเกณฑ์การ

ประเมินจากมาตรฐานต่าง ๆ เช่น ข้อกำหนดด้านกฎหมาย มาตรฐาน ISO มาตรฐานจากลูกค้า เป็นต้น และเมื่อตรวจพบความแตกต่างหรือ Gap องค์กรจะต้องจัดทำแผนการปรับปรุงเพื่อลดช่องว่างหรือปิดช่องว่างนั้น การวิเคราะห์ช่องว่างสามารถดำเนินการในมุมมองที่แตกต่างกัน เช่น การจัดการองค์กร (เช่น ทรัพยากรมนุษย์) ทิศทางธุรกิจ กระบวนการทางธุรกิจ เทคโนโลยีสารสนเทศ การวิเคราะห์ช่องว่างทางศักยภาพ เป็นเครื่องมือในการจำแนกว่าผลิตภัณฑ์หรือกระบวนการว่าตรงกับความต้องการหรือชุดของความต้องการที่กำหนดเป้าหมายได้ดีเพียงใดสามารถกำหนดเป็นอันดับ คือ “ดี” (Good) “ปานกลาง” (Average) หรือ “แย่” (Poor)

2.8.1 การวิเคราะห์ช่องว่างทางศักยภาพ 3 ขั้นตอน

Gap analysis (n.d.) แสดงการวิเคราะห์ช่องว่างอย่างง่าย 3 ขั้นตอนจาก en.wikipedia.org/wiki/Gap_analysis ดังนี้

1. วิเคราะห์สถานะปัจจุบันขององค์กร เพื่อค้นหาสถานะปัจจุบันโดยการวิเคราะห์อาจรวมถึงข้อมูลเชิงคุณภาพ เช่นกระบวนการ ระเบียบวิธีของทีม และข้อมูลเชิงปริมาณ เช่น จำนวนการโทรติดต่อในแต่ละสัปดาห์ ในทางปฏิบัติจริงกระบวนการวิเคราะห์ช่องว่างควรประเมินทุกสิ่งที่ทำอยู่ในปัจจุบันเพื่อให้มองเห็น “ภาพรวม”

2. ระบุเป้าหมายอุดมการณ์เชิงกลยุทธ์ เช่น ต้องการอยู่ที่ไหน ไม่ควรจะเกิดอะไรขึ้น ต้องมีอะไรที่ไม่เคยมีมาก่อน หรือต้องมีการเปลี่ยนแปลงอย่างไร ที่สำคัญที่สุด คือ ต้องดำเนินการอย่างไรเพื่อไปถึงเป้าหมายที่กำหนด

3. เชื่อมช่องว่าง (ลดช่องว่าง) จากสถานะปัจจุบันไปยังอนาคตในอุดมคติ โดยพิจารณาว่ามีช่องว่างใดบ้าง ปัญหาที่ทำให้ไม่บรรลุเป้าหมาย ดำเนินการหาวิธีแก้ไขปัญหา ทั้งนี้การกำหนดวัตถุประสงค์ที่ชัดเจนช่วยให้มองเห็นได้อย่างชัดเจน ในทางปฏิบัติสามารถเลือกใช้เครื่องมือต่าง ๆ ให้เหมาะสมในการวิเคราะห์ช่องว่างทางศักยภาพ เช่น SWOT analysis, McKinsey 7S Framework, Nadler-Tushman Model

2.8.2 การวิเคราะห์ช่องว่างทางศักยภาพ 5 ขั้นตอน

Amanda Athuraliya (2019) อธิบายแนวทางการวิเคราะห์ช่องว่างทางศักยภาพ เพื่อเป็นแนวทางปฏิบัติ ดังนี้

1. เลือกปัญหา หรือพื้นที่ของปัญหาเพื่อดำเนินการวิเคราะห์

2. กำหนดเป้าหมาย โดยคำนึงถึงความเป็นไปได้ ความสอดคล้องทางธุรกิจ
3. แสดงกระบวนการ และสถานะปัจจุบัน รวบรวมข้อมูลที่จำเป็นทั้งหมด
4. กำหนดสถานะที่ต้องการของธุรกิจและองค์ประกอบที่เกี่ยวข้อง
5. ระบุช่องว่างระหว่าง 2 สถานะ คือ สถานะปัจจุบัน และสถานะที่ต้องการ และดำเนินการเพื่อปิดช่องว่างระหว่าง 2 สถานะดังกล่าว

บทที่ 3
การดำเนินงาน

การพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศศูนย์ปฏิบัติการเครือข่าย สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม เพื่อนำแนวนโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศของสำนักงานศาลยุติธรรม ซึ่งใช้เกณฑ์มาตรฐาน ISO/IEC 27001:2013 ไปดำเนินการในขั้นตอนปฏิบัติ โดยค้นหาขั้นตอน กระบวนการ วิธีการและเครื่องมือ ที่จะทำให้การนำแนวนโยบายดังกล่าวไปปฏิบัติกับอุปกรณ์ และระบบอื่นที่มีความคล้ายคลึงกัน มีขั้นตอนการดำเนินการ ดังนี้

3.1 กำหนดขั้นตอนที่เหมาะสมในการศึกษากระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

3.2 วิเคราะห์การดำเนินการตามขั้นตอนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

3.3 กำหนดแนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ

3.1 กำหนดขั้นตอนที่เหมาะสมในการศึกษากระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

3.1.1 ปรับปรุงขั้นตอนให้เหมาะสมกับการพัฒนากระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

จากแนวคิดทฤษฎีในกระบวนการเพื่อรับรองมาตรฐาน ISMS และบริหารจัดการความปลอดภัยข้อมูลสารสนเทศ โดยดำเนินการตามวงจร PDCA (Plan – Do – Check - Action) ที่ได้แสดงไว้ในบทที่ 2 และศึกษาจากขั้นตอนกระบวนการปฏิบัติต่าง ๆ เพื่อหาแนวทางปฏิบัติที่เหมาะสม

Planning for and Implementing ISO 27001 (2011) กล่าวถึงการดำเนินการตามมาตรฐาน ISO 27001 ตั้งแต่ขั้นตอนงบประมาณไปจนถึงการบริหารจัดการของผู้บริหาร ในที่นี้ให้ความสนใจเฉพาะส่วนที่เกี่ยวกับขั้นตอนปฏิบัติการ ดังนี้

ขั้นตอนดำเนินการ

1. จัดทำนโยบายระบบจัดการความปลอดภัยสำหรับสารสนเทศ
2. กำหนดขอบเขตของระบบจัดการความปลอดภัยสำหรับสารสนเทศ
3. จัดทำขั้นตอน และการควบคุมในการสนับสนุนระบบจัดการความปลอดภัยสำหรับสารสนเทศ
4. เลือกและจัดทำวิธีการประเมินความเสี่ยง
5. จัดทำรายงานการประเมินความเสี่ยง
6. จัดทำแผนการรักษาความเสี่ยง กำหนดขั้นตอนการบันทึกตามระบบบริหารความมั่นคงปลอดภัยสำหรับสารสนเทศ
7. จัดทำบันทึกในระบบจัดการความปลอดภัยสำหรับสารสนเทศ
8. จัดทำ Statement of Applicability (SoA) หรือ เอกสารแสดงมาตรการในมาตรฐาน ISO 27001 ที่องค์กรได้มีการนำมาใช้งาน และเหตุผลของการใช้งาน รวมถึงมาตรการที่ไม่ได้นำมาใช้งาน และเหตุผลที่ไม่ได้ใช้งาน

ข้อกำหนดทางด้านเอกสาร

1. เอกสารแสดงนโยบาย ISMS และวัตถุประสงค์
2. ขอบเขตของ ISMS
3. วิธีการปฏิบัติงาน และการควบคุมเพื่อสนับสนุนต่อ ISMS
4. คำอธิบายเกี่ยวกับวิธีการประเมินความเสี่ยง
5. รายงานการประเมินความเสี่ยง
6. แผนการจัดการความเสี่ยง

7. เอกสารวิธีการปฏิบัติงานที่จำเป็นสำหรับองค์กร เพื่อให้มั่นใจได้ถึงความมีประสิทธิผลในการวางแผน การดำเนินการ และการควบคุมกระบวนการความปลอดภัยข้อมูลสารสนเทศ และอธิบายถึงแนวทางในการวัด ความมีประสิทธิผลของการควบคุม

8. บันทึกที่จำเป็นสำหรับมาตรฐาน

9. เอกสาร Statement of Applicability

รวมถึงขั้นตอนการปฏิบัติเพื่อให้เป็นไปตามมาตรฐาน ISO 27001 แบ่งเป็นขั้นตอน ดังนี้

1. ระบุวัตถุประสงค์ของธุรกิจ
2. รับการสนับสนุนด้านการจัดการ
3. กำหนดขอบเขต
4. เขียนนโยบาย ISMS สั้น ๆ
5. กำหนดวิธีการ และกลยุทธ์การประเมินความเสี่ยง
6. สร้างแผนการจัดการความเสี่ยง และจัดการความเสี่ยงเหล่านั้น
7. ตั้งค่านโยบาย และขั้นตอนการควบคุมความเสี่ยง
8. จัดสรรทรัพยากรที่จำเป็น และดำเนินการฝึกอบรมพร้อมโปรแกรมการรับรู้
9. ตรวจสอบ ISMS อย่างระมัดระวัง
10. เตรียมความพร้อมสำหรับการตรวจสอบภายใน
11. ทบทวนการจัดการเป็นระยะ

จากแนวทางกำหนดขั้นตอนดำเนินการ ISMS ข้างต้น เพื่อให้เหมาะสมและง่ายกับการดำเนินการตามแนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศ โดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ แบ่งขั้นตอนตามแนวทาง PDCA ได้ 4 ขั้นตอน

3.1.1.1 ขั้นเตรียมความพร้อม เทียบได้กับ Plan ของ PDCA เป็นการเตรียมข้อมูล ศึกษาข้อมูล วิเคราะห์ข้อมูล เพื่อรวมรวมข้อมูล และจัดเตรียมเอกสารทั้งหมดที่ต้องใช้งาน ศึกษาสถานะปัจจุบันของอุปกรณ์ และระบบ และข้อมูลที่จะใช้ในการขั้นตอนต่อไป ดังนี้

1. ระบุวัตถุประสงค์ทางธุรกิจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
2. ระบุนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
3. กำหนดขอบเขตของระบบจัดการความปลอดภัยข้อมูลสารสนเทศ
4. ระบุและจัดทำรายการสินทรัพย์ข้อมูลสารสนเทศ
5. กำหนดเกณฑ์ในการแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ
6. กำหนดประเภทสินทรัพย์ข้อมูลสารสนเทศตามคุณสมบัติ และการควบคุม
7. เลือกตัวแทนของสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท
8. ตรวจสอบและกำหนดการปฏิบัติการรักษาความปลอดภัยข้อมูลสารสนเทศแต่ละประเภทที่มีการดำเนินการอยู่ในปัจจุบัน
9. กำหนดรูปแบบและวิธีการประเมินความเสี่ยง
10. ระบุความเสี่ยงที่มีผลต่อข้อมูลสารสนเทศในขอบเขตที่เกี่ยวข้อง
11. วิเคราะห์และประเมินความเสี่ยง
12. กำหนดวัตถุประสงค์ และมาตรการในการควบคุมเพื่อลดความเสี่ยง
13. จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้ ISMS

3.1.1.2 ขั้นดำเนินการ เทียบได้กับ Do ของ PDCA เป็นการนำข้อมูลที่ศึกษาวิเคราะห์จากขั้นตอนเตรียมความพร้อมมากำหนดแผนและปฏิบัติตามแผนแก้ไขความเสี่ยง ดังนี้

1. กำหนดแผนการแก้ไขความเสี่ยงสำหรับอุปกรณ์และระบบที่เป็นตัวแทนของสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท ตามขั้นตอนการบันทึกของระบบการจัดการความปลอดภัยข้อมูลสารสนเทศ ซึ่งประกอบด้วยแนวทางปฏิบัติ ทรัพยากรที่ใช้ ความรับผิดชอบ และลำดับความสำคัญของความเสี่ยง
2. ปฏิบัติตามแผนลดความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ที่วางไว้
3. ดำเนินการตามมาตรการควบคุมที่เลือก เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้
4. กำหนดเกณฑ์สำหรับวัดประสิทธิภาพของมาตรการควบคุม
5. กำหนดขั้นตอนปฏิบัติเพื่อตรวจจับ และตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย
6. จัดทำ Statement of Applicability (SoA)

3.1.1.3 ขั้นทบทวนแก้ไขปรับปรุง เทียบได้กับขั้นตอน Check ของ PDCA เป็นกระบวนการเพื่อตรวจสอบ ประเมิน และแก้ไข ขั้นตอนดำเนินการให้เป็นไปตามแผนหรือระดับการรักษาความปลอดภัยที่กำหนด ดังนี้

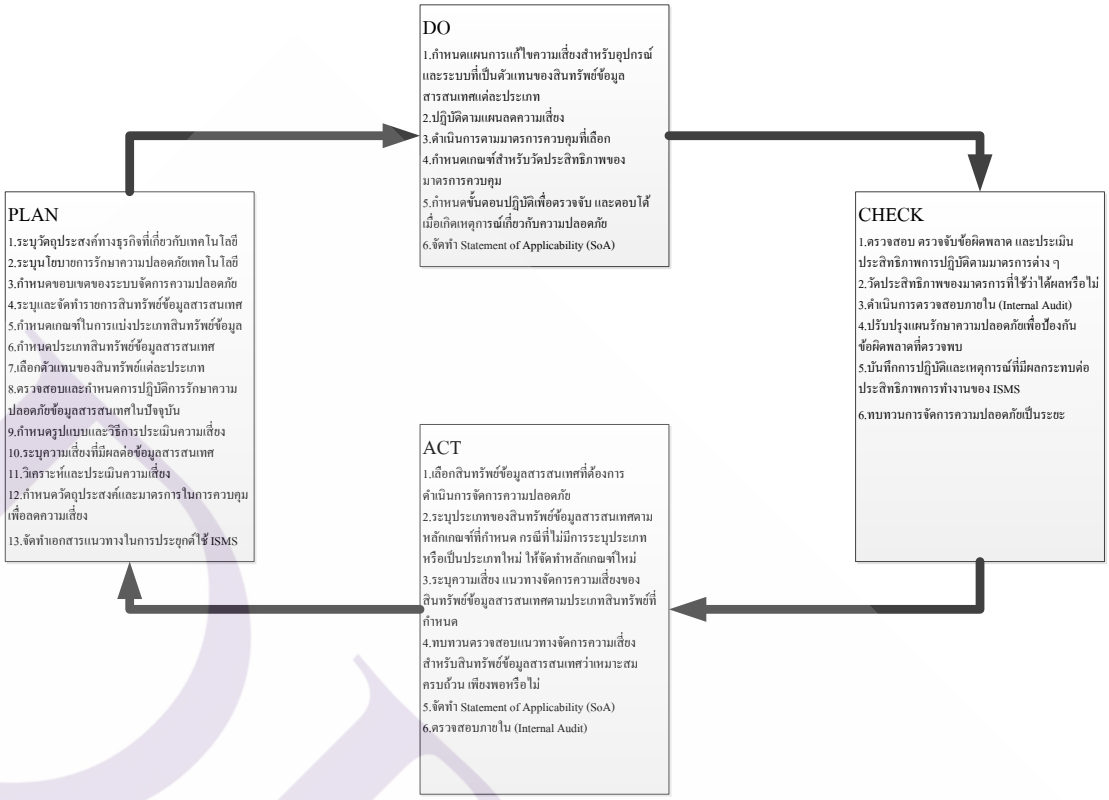
1. ตรวจสอบ ตรวจจับข้อผิดพลาด และประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ
2. วัดประสิทธิภาพของมาตรการที่ใช้ว่าได้ผลหรือไม่
3. ดำเนินการตรวจสอบภายใน (Internal Audit)
4. ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดที่ตรวจพบ
5. บันทึกการปฏิบัติ และเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของ ISMS
6. ทบทวนการจัดการความปลอดภัยเป็นระยะ

3.1.1.4 ขั้นกำหนดแนวทางปฏิบัติ เทียบได้กับขั้นตอน Act ของ PDCA เป็นกระบวนการกำหนดแนวทางรักษาความปลอดภัยข้อมูลสารสนเทศ

1. จัดทำข้อกำหนดที่ชัดเจนในการแบ่งอุปกรณ์ และระบบแต่ละประเภท
2. จัดทำแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศสำหรับอุปกรณ์ และระบบแต่ละประเภท
3. เปรียบเทียบแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศส่วนที่เหมือนกัน และต่างกันของอุปกรณ์
4. นำข้อกำหนดในการรักษาความปลอดภัยข้อมูลสารสนเทศไปปฏิบัติ
5. ทบทวน ตรวจสอบ ความเหมาะสมในการรักษาความปลอดภัยข้อมูลสารสนเทศ

3.1.2 ปฏิบัติตามขั้นตอนการพัฒนากระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

ปฏิบัติตามขั้นตอนที่ได้รับการปรับเปลี่ยนเรียบร้อยแล้ว โดยใช้การดำเนินการแบบ PDCA ทั้งนี้ การดำเนินการดังกล่าวแบ่งออกเป็นการเตรียมความพร้อม การดำเนินการ การตรวจสอบแก้ไข และการนำไปปฏิบัติ ตามแผนภาพดังนี้



ภาพที่ 3.1 แผนผังขั้นตอนการพัฒนากระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

3.2 วิเคราะห์การดำเนินการตามขั้นตอนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

3.2.1 ขั้นเตรียมความพร้อม

3.2.1.1 ระบุวัตถุประสงค์ทางธุรกิจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

สำนักงานศาลยุติธรรมมีการกำหนดแผนยุทธศาสตร์รอบระยะเวลา 5 ปี สำหรับแผนยุทธศาสตร์ปัจจุบัน เป็นแผนยุทธศาสตร์ศาลยุติธรรม พ.ศ. 2561 – 2564 ดังนี้

ตารางที่ 3.1 แผนยุทธศาสตร์ศาลยุติธรรม พ.ศ. 2561 – 2564 โดยย่อ

ยุทธศาสตร์		เป้าประสงค์
J	**Justice for all** ยึดมั่นการอำนวยความยุติธรรมด้วยหลักนิติธรรม	สังคมไทยมีความสงบสุขเรียบร้อย สามัคคีปรองดอง อย่างมั่นคงและยั่งยืน
U	**Uplift and Upload Standard** ยกระดับมาตรฐานระบบงานศาลยุติธรรมสู่ระดับสากล	การอำนวยความยุติธรรมที่มีมาตรฐานในระดับสากลของศาลยุติธรรม
S	**Strong Specialized Court** เพิ่มความเข้มแข็งให้ศาลชำนัญพิเศษและศาลอุทธรณ์คดีชำนัญพิเศษ	ศาลชำนัญพิเศษและศาลอุทธรณ์คดีชำนัญพิเศษมีความเชี่ยวชาญในการพิจารณาพิพากษาคดีชำนัญพิเศษ และมีระบบการอำนวยความยุติธรรมที่สอดคล้องกับลักษณะของแต่ละประเภทคดี
T	**Trusted Pillar** เพิ่มความเชื่อมั่นในศรัทธาในการอำนวยความยุติธรรม	ประชาชนและสังคมศรัทธาและเชื่อมมั่นในกระบวนการอำนวยความยุติธรรมของศาลยุติธรรม
I	**Innovation** พัฒนานวัตกรรมการอำนวยความยุติธรรมของศาลยุติธรรม	การบริหารคดีและการบริหารของศาลยุติธรรมมีความสะดวก รวดเร็ว และเสียค่าใช้จ่ายน้อย
C	**Collaboration** เร่งบูรณาการเครือข่ายด้านการยุติธรรมทั้งภายในประเทศและระหว่างประเทศ	หน่วยงานในกระบวนการยุติธรรมในประเทศและต่างประเทศ รวมถึงองค์การระหว่างประเทศให้การยอมรับและให้ความร่วมมือทางการศาลการยุติธรรมและทางวิชาการ
E	**Excellence Organization** เพิ่มศักยภาพขององค์กรสู่ความเป็นเลิศ	ศาลยุติธรรมมีระบบงานตุลาการ ระบบงานธุรการของศาลยุติธรรม ระบบงานส่งเสริมงานตุลาการ และระบบงานวิชาการ ที่มีขีดสมรรถนะสูงในการสนับสนุนการอำนวยความยุติธรรมให้ดำเนินไปอย่างมีประสิทธิภาพ

สำนักงานศาลยุติธรรมมีการเผยแพร่ แผนยุทธศาสตร์ศาลยุติธรรม พ.ศ. 2561 – 2564 ประจำปีทางเว็บไซต์ https://www.coj.go.th ซึ่งมีการแสดงรายละเอียดตามแผนยุทธศาสตร์แต่ละหัวข้อ ระบุตัวชี้วัด และแนวทางดำเนินการ ซึ่งมีส่วนที่ระบุถึงและมีการใช้งานเทคโนโลยีสารสนเทศหลายลักษณะ

3.2.1.2 ระบุนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

จากวัตถุประสงค์ทางธุรกิจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศใช้เป็นแนวทางในการพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กร และเป็นแนวทางจัดทำนโยบายรักษาความปลอดภัยข้อมูลสารสนเทศ สำหรับข้อมูลนโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศที่ศึกษาได้ดำเนินการร่างแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลยุติธรรมเรียบร้อยแล้ว ตามเอกสารบทที่ 2 แนวคิดทฤษฎีและผลงานที่เกี่ยวข้อง ในหัวข้อ 2.2.3

3.2.1.3 กำหนดขอบเขตของระบบจัดการความปลอดภัยข้อมูลสารสนเทศ

วิธีการกำหนดขอบเขตอาจครอบคลุมทุกส่วนหรือบางส่วนขององค์กร โดยพิจารณาประเด็นต่าง ๆ ที่เกี่ยวข้อง เป็นประโยชน์ และเหมาะสม ดังนี้

1. ระบุพื้นที่
2. สถานที่
3. สินทรัพย์และเทคโนโลยีขององค์กรอะไรบ้างที่จะถูกควบคุม
4. ระบุผู้ให้บริการ
5. ระบุคู่ค้า
6. ระบุหน่วยงานภายนอกที่มีการทำงานร่วมกัน
7. ระบุการพึ่งพาองค์กรอื่น
8. ระบุมาตรฐานด้านกฎระเบียบหรือกฎหมายที่ใช้กับพื้นที่

3.2.1.4 ระบุและจัดทำรายการสินทรัพย์ข้อมูลสารสนเทศ

ก่อนดำเนินการอื่นมีความจำเป็นต้องจัดทำรายการสินทรัพย์ข้อมูลสารสนเทศ โดยให้กำหนดเจ้าของสินทรัพย์และมอบหมายความรับผิดชอบในการปกป้องความลับความสมบูรณ์ และความพร้อมใช้งานของข้อมูล เพื่อให้ตรงตามข้อกำหนด ISO 27001: 2013 ต้องมีการพัฒนาสินทรัพย์ข้อมูลสารสนเทศ (A.8.1.1) เจ้าของทรัพย์สินต้องได้รับการเสนอชื่อ (A.8.1.2) และต้องใช้สินทรัพย์ที่มีการยอมรับ ตามที่กำหนดไว้ (A.8.1.3)

องค์ประกอบรายการสินทรัพย์ข้อมูลสารสนเทศหมายถึงสิ่งต่าง ๆ ดังนี้

ฮาร์ดแวร์ คือ อุปกรณ์และสายสัญญาณ

ซอฟต์แวร์ คือ โปรแกรมทั้งที่มีค่าใช้จ่าย พัฒนาเอง หรือฟรีแวร์

ข้อมูล ไม่ใช่เฉพาะสื่ออิเล็กทรอนิกส์ แต่รวมถึงข้อมูลในรูปแบบอื่น ๆ

โครงสร้างพื้นฐาน คือ อาคาร สำนักงาน ระบบไฟฟ้า ระบบแจ้งเตือนความผิดปกติภายในศูนย์ปฏิบัติการเครือข่าย, เครื่องปรับอากาศ และระบบอื่นที่มีผลต่อความปลอดภัยข้อมูลสารสนเทศ

ทรัพยากรบุคคล คือ บุคลากรด้านเทคโนโลยีสารสนเทศ หรือบุคลาการที่เกี่ยวข้องในการทำงานภายในศูนย์ปฏิบัติการเครือข่าย

บริการ คือ บริการที่มอบให้ผู้ใช้ปลายทาง ในที่นี้จะรวมถึงบริการระบบภายในและบริการจากภายนอก ซึ่งสิ่งเหล่านี้ไม่ใช่สินทรัพย์ในความหมายตรง แต่บริการดังกล่าวจำเป็นต้องมีการควบคุมดังนั้นจึงต้องรวมอยู่ในการจัดการสินทรัพย์ด้วย

3.2.1.5 กำหนดเกณฑ์ในการแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ

เกณฑ์การแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ พิจารณาจากคุณสมบัติที่มีผลต่อการนโยบายและการปฏิบัติเพื่อรักษาความปลอดภัยข้อมูลสารสนเทศ เช่น แบ่งตามพื้นที่การเข้าถึงของเครือข่าย เป็น Internal Zone, External Zone และ DMZ Zone เป็นต้น การใช้เกณฑ์ที่มีความหลากหลายเพื่อหาเกณฑ์ที่เหมาะสมในการแบ่งประเภทของสินทรัพย์ข้อมูลสารสนเทศ เพื่อสามารถนำไปกำหนดกระบวนการรักษาความปลอดภัยสินทรัพย์ข้อมูลสารสนเทศได้โดยง่าย ดังนี้

1. แบ่งตามลักษณะสินทรัพย์
2. แบ่งตามพื้นที่เครือข่ายที่เข้าถึงระบบได้
3. แบ่งตามขอบเขตการทำงานของระบบ
4. แบ่งตามหน้าที่การทำงานของอุปกรณ์และระบบ
5. แบ่งตามความรับผิดชอบดูแลระบบ
6. แบ่งตามระบบปฏิบัติการ
7. แบ่งความเสี่ยงของการโจมตีต่าง ๆ
8. แบ่งตามระดับความสำคัญของการกำหนดสิทธิ์

3.2.1.6 กำหนดประเภทสินทรัพย์ข้อมูลสารสนเทศตามคุณสมบัติและการควบคุม

การกำหนดประเภทสินทรัพย์ข้อมูลสารสนเทศต้องกำหนดให้เหมาะสมกับเกณฑ์ในการแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ คุณสมบัติของอุปกรณ์ และสามารถนำไปกำหนดความเสี่ยงและการควบคุม ตัวอย่างเช่น อุปกรณ์ Firewall เป็นอุปกรณ์ Rack Server ที่มีระบบปฏิบัติการประเภท Linux ความเสี่ยงของอุปกรณ์ประเภทดังกล่าวจึงเป็นช่องโหว่ของการตั้งค่าบัญชีผู้ใช้เริ่มต้น (Default User) ช่องโหว่ของระบบปฏิบัติการของ Linux เช่น Shell Shock และช่องโหว่ของการกำหนด Policy เป็นต้น

3.2.1.7 เลือกตัวแทนของสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท

เนื่องจากการศึกษาสินทรัพย์ข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่ายมีข้อจำกัดด้านความรู้ความเข้าใจระบบ และจำนวนสินทรัพย์ที่มีจำนวนมากและเพิ่มขึ้นตามการขยายตัวขององค์กร การศึกษาจากตัวอย่างของสินทรัพย์แต่ละประเภทจะทำให้ทราบถึงลักษณะเด่นที่แตกต่างกันของคุณสมบัติ รวมไปถึงมาตรการควบคุมสำคัญ จุดเน้น จุดอ่อน ของช่องโหว่ ตัวอย่างเช่น ระบบโครงสร้างพื้นฐานศูนย์ปฏิบัติการเครือข่าย ประกอบด้วยระบบย่อย ๆ ที่ทำงานร่วมกัน สามารถพิจารณาเลือก ระบบสำรองไฟฟ้า เป็นตัวอย่างกรณีศึกษาเนื่องจากเป็นระบบที่มีผลต่อระบบอื่นอย่างชัดเจน และถือเป็นโครงสร้างพื้นฐานของทุกระบบ

3.2.1.8 ตรวจสอบและระบุแนวทางปฏิบัติการรักษาความปลอดภัยสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภทที่มีการดำเนินการอยู่ในปัจจุบัน

บันทึกรายการรักษาความปลอดภัยข้อมูลสารสนเทศที่มีการปฏิบัติงานในปัจจุบันของอุปกรณ์และระบบแต่ละประเภท เพื่อทราบสถานะปัจจุบันของการรักษาความปลอดภัยข้อมูลสารสนเทศ ในที่นี้กรณีที่หน่วยงานมีการใช้งานมาตรฐานใดมาตรฐานหนึ่งอยู่แล้วจะช่วยลดเวลาในการดำเนินการต่าง ๆ เนื่องจากมาตรฐานมีเนื้อหาบางส่วนที่ตรงกัน

3.2.1.9 กำหนดรูปแบบและวิธีการประเมินความเสี่ยง

1. ขั้นตอนการประเมินความเสี่ยง

1.1 เลือกตัวแทนของอุปกรณ์และระบบแต่ละประเภท เพื่อประเมินความเสี่ยง สำหรับอุปกรณ์ที่มีคุณสมบัติ และการกำหนดนโยบายรักษาความปลอดภัยเหมือนหรือใกล้เคียงกัน

1.2 ระบุข้อมูลสารสนเทศที่มีคุณค่า คือ การกำหนดข้อมูลสารสนเทศที่มีคุณค่าขององค์กร และให้คะแนนแก่ข้อมูลสารสนเทศเหล่านั้น มีเทคนิคอยู่ 2 ประการ คือ การ

ประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Risk Assessment) และการประเมินความเสี่ยงเชิงปริมาณ (Quantitative Risk Assessment) จากการศึกษาพบว่าการกำหนดคะแนนแก่ข้อมูลสารสนเทศดังกล่าวในรูปแบบการประเมินความเสี่ยงเชิงคุณภาพมีความเหมาะสมกว่า เนื่องจากเป็นหน่วยงานราชการที่ให้ความสำคัญต่อความน่าเชื่อถือ การปฏิบัติงานด้วยความถูกต้อง มั่นคงมากกว่าผลกำไร หรือผลประโยชน์เชิงตัวเลข

1.3 ประเมินความเสี่ยงที่อาจเกิดขึ้น คือ การกำหนดความเสี่ยงที่อาจเกิดขึ้นต่อข้อมูลสารสนเทศ ดังนี้

1.3.1 Vulnerability ระบุจุดอ่อนหรือช่องโหว่ของระบบ การค้นหาช่องโหว่อาจทำได้โดยโดยปลดหรือบายพาสระบบรักษาความปลอดภัยเพื่อตรวจสอบ พิจารณาด้านต่าง ๆ ดังนี้ ช่องโหว่ด้านฮาร์ดแวร์ (Hardware) ช่องโหว่ด้านซอฟต์แวร์ (Software) ช่องโหว่ด้านเครือข่าย (Network) ช่องโหว่ด้านบุคลากร (Personnel) ช่องโหว่ทางกายภาพ (Physical site) และช่องโหว่ด้านการจัดการ (Organizational)

1.3.2 Treat ระบุภัยคุกคามที่สามารถโจมตีช่องโหว่ของระบบ

1.3.3 Risk ระบุความเสี่ยงต่อช่องโหว่ของระบบและภัยคุกคาม

1.4 แสดงข้อมูลการประเมินความเสี่ยงในรูปแบบตาราง โดยกำหนดคะแนนให้กับโอกาสที่เกิดจากการโจมตีจากช่องโหว่ และระดับความเสียหายหรือผลกระทบที่มีต่อระบบ

2. ตารางประเมินความเสี่ยง

ตารางประเมินความเสี่ยงจะแสดงความสัมพันธ์ระหว่างช่องโหว่และผลกระทบที่มีต่อระบบ จากการให้คะแนนแก่ช่องโหว่ และผลกระทบจะทำให้ทราบถึงระดับความเสี่ยงที่อาจเกิดขึ้น โดยทั่วไปการให้คะแนนแก่ช่องโหว่ และผลกระทบจะกระทำโดยเจ้าของระบบซึ่งมีความเข้าใจต่อธุรกิจและความสำคัญของผลกระทบในแต่ละด้าน

3. ระบุภัยคุกคาม

ภายหลังกำหนดขอบเขตของระบบจัดการความปลอดภัยข้อมูลสารสนเทศให้กำหนดรายการภัยคุกคามจากข้อมูลภัยคุกคามที่หน่วยงานต้องเผชิญ ให้พิจารณาจากประเด็นต่าง ๆ ดังนี้

3.1 รายการภัยคุกคามจากภัยธรรมชาติที่มีโอกาสเกิดขึ้นได้น้อย แต่มีผลกระทบสูง เช่น ไฟไหม้ แผ่นดินไหว น้ำท่วม และพายุ

3.2 รายการช่องโหว่ของอุปกรณ์และระบบแต่ละภายในศูนย์ปฏิบัติการเครือข่าย เช่น อุปกรณ์แบบ Rack Server ติดตั้ง OS ด้วย MS Windows และใช้งานระบบสำนวนคดีศาลชั้นต้นซึ่งมีการพัฒนาด้วย MS Access มีการเปิดการรักษาความปลอดภัยในระดับต่ำสุด เพื่อใช้งาน Macro จึงมีรายการช่องโหว่ของ Rack Server ในรุ่นนั้นๆ ช่องโหว่ของ OS และช่องโหว่ของ Application

3.3 รายการภัยคุกคามจากอุปกรณ์และระบบหลักขัดข้อง เกิดผลกระทบสูงระบบไฟฟ้าขัดข้อง ระบบไฟฟ้าเป็นโครงสร้างพื้นฐานที่สำคัญ เนื่องจากอุปกรณ์ และระบบทำงานโดยใช้ไฟฟ้า

3.3.1 ระบบปรับอากาศขัดข้อง เนื่องจากอุปกรณ์และระบบมีความร้อนสูง เมื่อระบบปรับอากาศขัดข้องจนอุณหภูมิของอุปกรณ์สูงเกินกว่ากำหนด อุปกรณ์จะรีสตาร์ทหรือปิดระบบ ทำให้มีผลกระทบสูง

3.3.2 ไฟร์วอลล์ขัดข้อง กรณีเกิดขัดข้องจนอุปกรณ์หยุดให้บริการจะส่งผลกระทบต่อการใช้งานทั้งระบบ

3.3.3 สวิตช์หลักขัดข้อง เครือข่ายภายในอาคารหรืออุปกรณ์และระบบต้องผ่านมายังสวิตช์หลัก การขัดข้องที่จุดซึ่งเปรียบเสมือนคอขวดจะทำให้อุปกรณ์ และระบบทั้งหมดไม่สามารถให้บริการได้

3.3.4 สวิตช์หลักของผู้ให้บริการเครือข่าย (CAT Telecom) กรณีขัดข้องจะมีผลต่อการใช้เครือข่ายของระบบทั้งหมด

3.4 รายการภัยคุกคามที่เกิดขึ้นบ่อย

3.4.1 การโจมตีจากไวรัส มัลแวร์ และวิธีการอื่น ผ่านอินเทอร์เน็ต ปัจจุบันมีการโจมตีจากภายนอกจำนวนมากทั้งที่สามารถตรวจสอบจากข้อมูลจราจรทางคอมพิวเตอร์ (log) และการโจมตีโดยวิศวกรรมทางสังคม การส่งอีเมล์ปลอม

3.4.2 การโจมตีเพื่อให้ระบบปฏิเสธการให้บริการ (denial of service) เป็นการโจมตีที่ป้องกันได้ยาก และมีผลขัดขวางการให้บริการของอุปกรณ์ และระบบงาน เป็นการโจมตีที่พบได้บ่อยอีกด้วย

3.4.3 เครื่องแม่ข่ายให้บริการหรือระบบงานเกิดปัญหา หรือตอบสนองล่าช้ามีผลต่อการทำงานทำงานของหน่วยงานที่ใช้ฐานข้อมูลหรือระบบร่วมกัน

3.5 รายการภัยคุกคามที่เกิดขึ้นเป็นครั้งคราว และมีผลกระทบรุนแรง

3.5.1 อุปกรณ์ฮาร์ดแวร์ เครื่องแม่ข่าย ฐานข้อมูล อุปกรณ์บันทึกข้อมูล หยุดทำงาน หรือขัดข้องบางส่วน ทำให้ไม่สามารถให้บริการได้ตามปกติ

3.5.2 การเปลี่ยนแปลงหน้าเว็บไซต์สำนักงานศาลยุติธรรม เป็นการกระทำที่ส่งผลต่อความน่าเชื่อถือ และชื่อเสียงขององค์กร สำนักงานศาลยุติธรรมเคยพบเหตุการณ์ดังกล่าวเนื่องจากกรณีการพิจารณาคดีเกาะเต่า เดือนมกราคม พ.ศ. 2558

3.5.3 การโจมตีที่มีนัยยะทางการเมือง เป็นรูปแบบการโจมตีที่มีการประกาศเป็นแคมเปญในช่วงระยะเวลาหนึ่ง ทำให้มีการโจมตีจาก Hacker จำนวนมาก และยากในการระวังป้องกัน ซึ่งจะมีการโจมตีเป็นระลอกแล้วแต่การนัดหมาย

3.5.4 การเข้าถึงฐานข้อมูลในกระบวนการพิจารณาคดี ฐานข้อมูลดังกล่าวเป็นฐานข้อมูลสำคัญซึ่งเป็นหัวใจของการพิจารณาคดี โดยเฉพาะกรณีที่การพิจารณาคดียังไม่มีคำพิพากษาถึงที่สุด การเข้าถึง เปลี่ยนแปลงแก้ไข ลบข้อมูล จึงอาจส่งผลกระทบรุนแรง

3.5.5 การเข้าถึงฐานข้อมูลบุคลากรหน่วยงานศาลยุติธรรม ข้อมูลบุคลากรหน่วยงานศาลยุติธรรมมีการเผยแพร่ข้อมูลบางส่วนทางเว็บไซต์อยู่แล้ว กรณีเข้าถึงข้อมูลที่ไม่พึงประสงค์ เช่น ที่อยู่ หมายเลขโทรศัพท์ เงินเดือน มีผลกระทบที่รุนแรงต่อสวัสดิภาพ และอาจมีผู้ไม่ประสงค์ดีนำข้อมูลไปใช้ปลอมแปลงเพื่อดำเนินธุรกรรมทางการเงิน

3.5.6 การโจมตีของแรนซัมแวร์ (Ransomware) มัลแวร์ดังกล่าวจะเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ กรณีเป็นข้อมูลสำคัญที่จำเป็นต่อการทำงาน และไม่มีระบบสำรองข้อมูล หรือการป้องกันที่ดีเพียงพอ จะส่งผลให้ไม่สามารถทำงานได้ ทั้งนี้ เคยมีการแจ้งของหน่วยงานศาลยุติธรรมโดนโจมตีในลักษณะดังกล่าวมาแล้ว

3.6 รายการภัยคุกคามจากช่องโหว่ของอุปกรณ์และระบบ

Vasant Raval and Ashok Fichadia (2007) กล่าวถึงการรักษาความปลอดภัยที่แตกต่างกัน แยกการควบคุมความปลอดภัยตามองค์ประกอบของระบบ ดังนี้

3.6.1 การควบคุมข้อมูลสารสนเทศ และการให้บริการ (Information and Service)

3.6.2 การควบคุมระบบปฏิบัติการ (Operating system)

3.6.3 การควบคุมแอปพลิเคชัน (Application)

3.6.4 การควบคุมฐานข้อมูล (Database)

3.6.5 การควบคุมการสื่อสาร (Telecommunications)

3.6.6 การควบคุมเครือข่าย (Network)

3.6.7 การควบคุมเว็บไซต์และอินเตอร์เน็ต (Web and Internet)

4. ระบุระดับผลกระทบ

การระบุระดับผลกระทบพิจารณาจากมูลค่า และความเสียหายที่เกิดขึ้นต่ออุปกรณ์และระบบ ดังนี้

4.1 มูลค่าสินทรัพย์ข้อมูลสารสนเทศ ซึ่งหน่วยงานศาลยุติธรรมให้ความสำคัญกับความน่าเชื่อถือ ความถูกต้อง ความมั่นคงปลอดภัย ความเสียหายต่อสินทรัพย์ในแง่ดังกล่าวจึงถือว่าเป็นผลกระทบสูง เช่น การเปลี่ยนแปลงหน้าเว็บไซต์ของสำนักงานศาลยุติธรรม

4.2 ความสามารถในการกู้คืนความเสียหายต่อสินทรัพย์ข้อมูลสารสนเทศ เช่น ข้อมูลถูกโจมตีด้วยแรนซัมแวร์ (Ransomware) และไม่มีการสำรองข้อมูล ทำให้เกิดความเสียหายไม่สามารถกู้คืนได้ เป็นความเสียหายร้ายแรง กรณีมีการสำรองข้อมูลไว้แล้วความเสียหายที่เกิดขึ้นจะถือว่าเป็นความเสียหายระดับต่ำ ในกรณีเดียวกันอุปกรณ์ฮาร์ดแวร์ (Hardware) ที่ยังอยู่ระหว่างรับประกันสามารถเปลี่ยนทดแทนอุปกรณ์ที่เสียหายได้ทันที แต่กรณีที่หมดอายุรับประกันต้องใช้ระยะเวลาในการจัดซื้ออุปกรณ์ทดแทน หากเป็นอุปกรณ์ที่มีอายุการใช้งานนานไม่สามารถหาผลิตภัณฑ์ทดแทนได้ก็อาจเป็นผลกระทบต่อระบบสูง

4.3 ความเสียหายต่อสินทรัพย์ข้อมูลสารสนเทศที่มีผลกระทบต่อการทำงานของหน่วยงานในวงกว้าง เช่น ระบบยื่นส่งคำฟ้องทางอิเล็กทรอนิกส์เกิดขัดข้องมีผลต่อการทำงานของหน่วยงานศาลยุติธรรมทุกหน่วยงานทั่วประเทศ ในขณะที่ระบบห้องสมุดอิเล็กทรอนิกส์ขัดข้องมีผลเฉพาะกับผู้ใช้บริการห้องสมุดอิเล็กทรอนิกส์ และผู้ที่ต้องการศึกษาค้นคว้าเท่านั้น

4.4 ความเสียหายต่อสินทรัพย์ข้อมูลสารสนเทศที่มีผลกระทบต่ออุปกรณ์และระบบอื่นภายในศูนย์ปฏิบัติการเครือข่าย เช่น ระบบไฟฟ้า ระบบปรับอากาศ ที่มีผลกระทบสูงต่อระบบทั้งหมด

5. วิเคราะห์ความเสี่ยง

วิเคราะห์ความเสี่ยงโดยจัดทำในรูปแบบตารางเพื่อระบุระดับความเสี่ยง และนำไปแสดงเป็นรหัสสีเพื่อให้มองเห็นได้ง่าย เช่น สีแดง หมายถึง ความเสี่ยงสูงที่ไม่สามารถยอมรับได้ ต้องดำเนินการตามมาตรการป้องกันแก้ไขความเสี่ยง

6. ระบุความเสี่ยงที่มีผลต่อข้อมูลสารสนเทศในขอบเขตที่เกี่ยวข้อง

การระบุความเสี่ยงที่มีผลต่อข้อมูลสารสนเทศในขอบเขตทั้งหมด จะต้องพิจารณาจากความเสี่ยงที่เกี่ยวข้องทั้งหมด ที่อาจมีผลต่อสินทรัพย์ข้อมูลสารสนเทศ โดยพิจารณาจาก ความเสี่ยงจากภัยธรรมชาติ ความเสี่ยงจากโครงสร้างพื้นฐาน ความเสี่ยงจากฮาร์ดแวร์ ความเสี่ยงจากซอฟต์แวร์ ความเสี่ยงจากกระบวนการปฏิบัติงาน เป็นต้น ตัวอย่างการระบุความเสี่ยง

ตารางที่ 3.2 ตัวอย่างการระบุความเสี่ยงที่เกี่ยวข้อง

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอลล์	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ภัยธรรมชาติ : Natural Disaster							
ไฟไหม้	✓	✓	✓	✓		✓	✓
น้ำท่วม	✓	✓	✓	✓		✓	✓
แผ่นดินไหว	✓	✓	✓	✓		✓	✓
ลมพายุ	✓	✓	✓	✓		✓	✓
ฟ้าผ่า	✓	✓	✓	✓		✓	✓

3.2.1.10 วิเคราะห์ และประเมินความเสี่ยง

ประเมินความเสี่ยงโดยให้คะแนนจากโอกาส และผลกระทบต่อการเกิดความเสี่ยง ตัวอย่างเช่น ความเสี่ยงจากไฟไหม้มีโอกาสเกิดขึ้นในระบบสำรองไฟฟ้าสูงว่าระบบอื่น แต่ความ

เสียหายนั้นจะอยู่ในระดับสูงทุกระบบ ดังนั้น เมื่อกำหนดโอกาสที่จะเกิดไฟไหม้ เท่ากับ 2 ผลกระทบ เท่ากับ 5 จะได้ค่าความเสี่ยง 10 เป็นค่าความเสี่ยง ปานกลาง ใช้สีส้ม ดังตัวอย่าง

ตารางที่ 3.3 ตัวอย่างการประเมินความเสี่ยง

ความเสี่ยง	ระบบสำรองไฟฟ้า		ไฟร์วอลล์		ระบบสารบรรณอิเล็กทรอนิกส์		ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์		ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ		เว็บไซต์สำนักงานตาลยุติธรรม	
ภัยธรรมชาติ : Natural Disaster													
ไฟไหม้	2	5 10	1	5 5	1	5 5	1	5 5		1	5 5	1	5 5
น้ำท่วม	2	5 10	1	5 5	1	5 5	1	5 5		1	5 5	1	5 5
แผ่นดินไหว	1	5 5	1	5 5	1	5 5	1	5 5		1	5 5	1	5 5
ลมพายุ	1	5 5	1	5 5	1	5 5	1	5 5		1	5 5	1	5 5
ฟ้าผ่า	2	5 10	1	5 5	1	5 5	1	5 5		1	5 5	1	5 5

3.2.1.11 กำหนดวัตถุประสงค์และมาตรการในการควบคุมเพื่อลดความเสี่ยง

การกำหนดวัตถุประสงค์และการควบคุมเพื่อจัดการความเสี่ยง สำหรับความเสี่ยงที่ไม่สามารถป้องกัน หรือไม่คุ้มค่าที่จะดำเนินการ อาจใช้การยอรับความเสี่ยง หรือถ่ายโอนความเสี่ยง มาตรการควบคุมอาจแบ่งเป็นประเภทต่าง ๆ เพื่อครอบคลุม ดังนี้

1. มาตรการควบคุมตามเวลาที่สัมพันธ์กับเหตุการณ์

1.1 Preventive controls การควบคุมเชิงป้องกัน ก่อนเกิดเหตุการณ์

1.2 Detective controls การควบคุมตรวจสอบ ขณะเกิดเหตุการณ์

1.3 Corrective controls การควบคุมแก้ไข เมื่อเกิดเหตุการณ์แล้ว

2. มาตรการควบคุมตามลักษณะของเหตุการณ์ด้านความปลอดภัย

2.1 การควบคุมทางกายภาพ (Physical controls)

2.2 การควบคุมกระบวนการ (Procedure controls) เช่น กำหนดกระบวนการตอบสนองเหตุการณ์ การควบคุมดูแล

2.3 การควบคุมทางเทคนิค (Technical controls) เช่น ระบบพิสูจน์ตัวตนผู้ใช้ (login) และการควบคุมการเข้าถึงแบบลอจิคอล (logical access controls) ซอฟต์แวร์ป้องกันไวรัส (antivirus software) และไฟร์วอลล์ (firewall)

2.4 การควบคุมด้านกฎหมายและข้อบังคับ (Legal and regulatory or compliance controls) เช่น กฎหมาย นโยบายความเป็นส่วนตัว และข้อตกลง

3.2.1.11 จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้ ISMS

ภายหลังการเตรียมความพร้อมด้านต่าง ๆ ให้จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้ ISMS เพื่อดำเนินการเป็นลำดับขั้น และตรวจสอบความครบถ้วน

3.2.2 ขั้นดำเนินการ

3.2.2.1 กำหนดแผนการแก้ไขความเสี่ยงสำหรับอุปกรณ์และระบบตัวอย่าง

การกำหนดแผนการแก้ไขความเสี่ยงเป็นการจัดเตรียมกระบวนการเพื่อปฏิบัติตามมาตรการควบคุมที่กำหนดไว้ในขั้นเตรียมความพร้อม โดยต้องมีการระบุประเภทสินทรัพย์ ความเสี่ยง ขั้นตอนดำเนินการ ผู้รับผิดชอบ งบประมาณ

3.2.2.2 ปฏิบัติตามแผนลดความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ที่วางไว้

ดำเนินการตามแผนดำเนินการข้างต้น เพื่อลดความเสี่ยงให้อยู่ในระดับต่ำสุด หรือระดับที่ยอมรับได้ สำหรับการดำเนินตามแผนต้องมีการจัดเรียงลำดับตามความสำคัญของความเสี่ยง และกำหนดระยะเวลาเริ่มต้น ระยะเวลาสิ้นสุดแผน เพื่อจัดเป็นปฏิทินดำเนินการ

3.2.2.3 ดำเนินการตามมาตรการควบคุมที่เลือก เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้

การรักษาความปลอดภัยข้อมูลสารสนเทศไม่จำเป็นต้องใช้มาตรการทุกมาตรการในการดำเนินการ ในขณะเดียวกันมาตรการควบคุมอาจเป็นมาตรการเดียวหรือหลายมาตรการ เพื่อควบคุมให้ความเสี่ยงลดลง ทำให้โอกาสการเกิด และผลกระทบลดลง

3.2.2.4 กำหนดเกณฑ์สำหรับวัดประสิทธิภาพของมาตรการควบคุม

การวัดประสิทธิภาพของมาตรการควบคุมตาม ISMS หมายถึง การตรวจสอบว่ามีการนำเอามาตรการควบคุมตามมาตรฐาน ISO 27001 มาใช้เพียงพอ โดยทั่วไปกำหนดที่ 90 % ของทั้งหมด สามารถใช้การวิเคราะห์ช่องว่างทางศักยภาพ (Gap Analysis) ระหว่างระหว่างมาตรการที่ปฏิบัติ กับเป้าหมายที่คาดหวังว่าขณะนี้อยู่ในระดับใด ซึ่งจะพบจุดที่เป็นช่องโหว่ของระบบที่มีการปฏิบัติต่ำกว่าเกณฑ์เป้าหมาย

สำหรับผู้ศึกษาเห็นว่าการวัดประสิทธิภาพของมาตรการควบคุมควรวัดมาตรการปฏิบัติที่ดำเนินการตามแผนด้วย โดยการเปรียบเทียบค่าความเสี่ยงก่อน และหลังดำเนินการตามมาตรการควบคุมว่ามีความเสี่ยงลดลงหรือไม่

3.2.2.5 กำหนดขั้นตอนปฏิบัติเพื่อตรวจจับ และตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย

เพื่อกำจัดช่องโหว่ที่เป็นไปได้จึงพัฒนาชุดของมาตรการตอบโต้โดยคำนึงถึงประสิทธิภาพสูงสุดและค่าใช้จ่ายต่ำ ปัญหาที่มักเกิดขึ้นในขั้นตอนนี้ คือ กำหนดมาตรการตอบโต้ไม่ครบถ้วนสมบูรณ์ กำหนดมาตรการตอบโต้ไม่ครอบคลุมต่อระบบทั้งหมด ตัวชี้วัดสำหรับมาตรการตอบโต้คำนวณไม่ถูกต้อง กระบวนการปรับปรุงแก้ไขตามมาตรการไม่ถูกต้อง

สำนักเทคโนโลยีสารสนเทศมีการจัดทำขั้นตอนปฏิบัติตอบโต้เหตุการณ์ โดยให้เจ้าของระบบเป็นผู้จัดทำและรวบรวมจัดทำแผนการดำเนินการรักษาความปลอดภัยข้อมูลสารสนเทศ อย่างไรก็ตามเป็นการกำหนดข้อปฏิบัติเฉพาะกรณีวิกฤตเท่านั้น สำหรับการกำหนดขั้นตอนปฏิบัติให้ระบุรายละเอียดเหตุการณ์ การตรวจจับ มาตรการที่กำหนด ทรัพยากรที่ต้องใช้งาน ชื่อเจ้าของระบบ ชื่อผู้ปฏิบัติงาน

3.2.2.6 จัดทำ Statement of Applicability (SoA)

การจัดทำ Statement of Applicability (SoA) หรือ เอกสารแสดงมาตรการในมาตรฐาน ISO 27001 ที่องค์กรได้มีการนำมาใช้งาน และเหตุผลของการใช้งาน รวมถึงมาตรการที่ไม่ได้นำมาใช้งานและเหตุผลที่ไม่ได้ใช้งานด้วย

รายการควบคุมที่ต้องระบุไว้อย่างชัดเจนใน Statement of Applicability (SoA) ดังนี้

A5. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) (2 controls)

A6. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security) (7 controls)

A7. ความมั่นคงปลอดภัยสำหรับบุคลากร (Human Resource Security) (6 controls)

A8. การบริหารจัดการทรัพย์สิน (Asset Management) (10 controls)

A9. การควบคุมการเข้าถึง (Access Control) (14 controls)

A10. การเข้ารหัสข้อมูล (Cryptography) (2 controls)

A11. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security) (15 controls)

A12. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security) (14 controls)

A13. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security) (7 controls)

A14. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance) (13 controls)

A15. ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships) (5 controls)

A16. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) (7 controls)

A17. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) (4 controls)

A18. ความสอดคล้อง (Compliance) (8 controls)

สำหรับกรณีศึกษาการรักษาความปลอดภัยภายในศูนย์ปฏิบัติการเครือข่ายฯ เป็นการศึกษาจากอุปกรณ์ และระบบตัวอย่าง จึงจัดทำ SoA จำนวนเท่ากับระบบตัวอย่างที่ศึกษา เนื่องจากอุปกรณ์และระบบแต่ละประเภทมีความจำเป็นต้องใช้งานมาตรการควบคุมใน SoA แตกต่างกัน

ตารางที่ 3.4 ตัวอย่าง Statement of Applicable (SoA)

ตรวจสอบ	หัวข้อ	หัวเรื่อง	การประยุกต์ใช้	หมายเหตุ
A.11.2 Equipment				
✓	A.11.2.1	Equipment siting and protection	จัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงของภัยคุกคามจากสิ่งแวดล้อม และอันตรายต่างๆ รวมถึงการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต	ติดตั้งในตู้ Rack สำหรับระบบสื่อสารทางไกลผ่านจอภาพโดยเฉพาะ
✓	A.11.2.2	Supporting utilities	กำหนดให้มีการป้องกันการล้ม เหลวของระบบและอุปกรณ์สนับสนุน เช่น ระบบสำรองไฟฟ้า ระบบปรับอากาศ ระบบตรวจจับควัน ฉีดพ่นสารดับเพลิง	ศูนย์ปฏิบัติการเครือข่ายได้ติดตั้งระบบโครงสร้างพื้นฐานอยู่แล้ว
✓	A.11.2.3	Cabling security	กำหนดให้การเดินสายไฟฟ้า สายสื่อสารและสายเคเบิลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาตที่อาจทำให้เกิดอุปสรรคหรือ เสียหาย	การเดินสายภายในตู้ Rack และเข้าสวิตช์ ไม่มีส่วนที่ออกไปนอกห้องศูนย์ปฏิบัติการเครือข่ายฯ

3.2.3 ขั้นทบทวนแก้ไขปรับปรุง

3.2.3.1 ตรวจสอบ ตรวจจับข้อผิดพลาด และประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ

ในกรณีที่เกิดความไม่สอดคล้องตามข้อกำหนดของ ISMS ขึ้น องค์กรต้องดำเนินการเพื่อขจัดสาเหตุเพื่อป้องกันการเกิดซ้ำ ทั้งนี้ ต้องมีการจัดทำเอกสารระเบียบวิธีการปฏิบัติงาน โดยมีรายละเอียด ดังนี้

1. การระบุความไม่สอดคล้องตามข้อกำหนด
2. การพิจารณาสาเหตุของความไม่สอดคล้องตามข้อกำหนด
3. การประเมินถึงความจำเป็นในการดำเนินการ เพื่อให้ความไม่สอดคล้องตามข้อกำหนดไม่เกิดขึ้นซ้ำ
4. การดำเนินการปฏิบัติการแก้ไข
5. การบันทึกผลของการดำเนินการ

6. การทบทวนการปฏิบัติการแก้ไข

3.2.3.2 วัดประสิทธิภาพของมาตรการที่ใช้ว่าได้ผลหรือไม่

ดำเนินการวัดประสิทธิภาพ 2 ส่วน

1. วัดประสิทธิภาพมาตรการตามมาตรฐาน ISO 27001
2. วัดประสิทธิภาพมาตรการปฏิบัติ

3.2.3.3 ดำเนินการตรวจสอบภายใน (Internal Audit)

1. แนวทางการตรวจประเมินความปลอดภัยข้อมูลสารสนเทศ

การตรวจประเมินความปลอดภัยข้อมูลสารสนเทศ แบ่งได้ 2 ประเภท คือ การตรวจประเมินโดยผู้เชี่ยวชาญภายนอก และการตรวจประเมินโดยบุคลากรภายใน มีข้อดีข้อเสีย ดังนี้

1.1 การใช้ผู้ตรวจสอบภายนอก ข้อดีคือ ผู้ตรวจประเมินมีประสบการณ์ใช้ชุดซอฟต์แวร์ในการสแกนช่องโหว่ ข้อเสียที่สำคัญ คือ ค่าใช้จ่ายสูง และผู้ตรวจประเมินที่มีคุณสมบัติและประสบการณ์หาได้ยากมาก นอกจากนี้ความสำเร็จของการตรวจสอบขึ้นกับคุณภาพของการสื่อสารระหว่างองค์กรกับผู้ตรวจสอบ

1.2 การตรวจสอบโดยบุคลากรภายในมีประสิทธิภาพสูง ช่วยให้สามารถรวบรวมข้อมูลพื้นฐานด้านความปลอดภัย และตรวจสอบว่านโยบายในปัจจุบันมีประสิทธิภาพหรือไม่ ข้อบกพร่องคือ ผู้ตรวจสอบภายในมักจะขาดประสบการณ์ และเครื่องมือที่จำเป็น ค่าใช้จ่ายน้อย และมีประสิทธิภาพในแง่ของกระบวนการ ไม่รบกวนกระบวนการทำงานที่มีอยู่ภายในบริษัท ข้อดีที่น่าสนใจ คือ ช่วยให้การรักษาความปลอดภัยข้อมูลภายในหน่วยงานได้รับการพัฒนาขึ้น ดังนี้

1.2.1 สร้างพื้นฐานความปลอดภัยภายในองค์กร

1.2.2 ช่วยให้การบังคับใช้กฎระเบียบ และแนวทางปฏิบัติเกี่ยวกับความปลอดภัยได้รับการนำไปปฏิบัติ การตรวจสอบช่วยให้มั่นใจได้ว่ามาตรการรักษาความปลอดภัย จะได้รับการบังคับใช้ และปฏิบัติตามอย่างทั่วถึง

1.2.3 เข้าใจสถานะที่แท้จริงของความปลอดภัยภายในองค์กรและสามารถกำหนดกลยุทธ์สำหรับอนาคตได้อย่างถูกต้อง

1.2.4 การศึกษาแนวทางรักษาความปลอดภัยข้อมูลสารสนเทศนี้ได้ใช้การประเมินด้วยบุคลากรภายใน เนื่องจากมีความเหมาะสมต่อการปฏิบัติงานในหน่วยงานราชการ และมีผลดีต่อการพัฒนาการรักษาความปลอดภัยข้อมูลสารสนเทศต่อไปในอนาคต

2. วัตถุประสงค์การตรวจประเมินภายใน

การตรวจประเมินภายในมีวัตถุประสงค์เพื่อพิจารณาว่า การกำหนดวัตถุประสงค์การควบคุม การควบคุม กระบวนการ และวิธีการปฏิบัติงานของ ISMS เป็นไปตามข้อกำหนดครบถ้วนหรือไม่ ดังนี้

2.1 สอดคล้องตามข้อกำหนดมาตรฐาน ISO 27001 รวมถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

2.2 สอดคล้องตามข้อกำหนดความปลอดภัยข้อมูลสารสนเทศที่กำหนดไว้

2.3 มีการดำเนินการ และดูแลรักษาอย่างมีประสิทธิผล

2.4 เป็นไปตามเป้าประสงค์ที่ได้คาดหมายไว้

3. องค์ประกอบการตรวจประเมินภายใน

โดยทั่วไปรายการตรวจประเมินภายในจะประกอบด้วย 4 คอลัมน์ ดังนี้

3.1 ส่วนอ้างอิง เช่น หมายเลขข้อของมาตรฐานหรือหมายเลขส่วนของนโยบาย เป็นต้น

3.2 สิ่งที่ต้องค้นหา คือ สิ่งที่เขียน สิ่งที่ตรวจสอบค้นพบในระหว่างการตรวจสอบหลัก

3.3 การปฏิบัติตามกฎ คอลัมน์นี้กรอกข้อมูลในระหว่างการตรวจสอบหลัก และข้อมูลสรุปว่า บริษัท ได้ปฏิบัติตามข้อกำหนดหรือไม่

3.4 ผลการค้นหา คอลัมน์นี้ระบุสิ่งที่ค้นพบระหว่างการตรวจสอบหลัก เช่น ชื่อบุคคลที่อ้างถึง คำพูดหรือข้อมูลที่พวกเขากล่าว เลขอ้างอิง และเนื้อหาของระเบียนที่ตรวจสอบ คำอธิบายเกี่ยวกับอุปกรณ์และระบบ ข้อสังเกตเกี่ยวกับ อุปกรณ์ที่ดำเนินการตรวจสอบ เป็นต้น

3.2.3.4 ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดที่ตรวจพบ

องค์กรต้องกำหนดมาตรการดำเนินการ เพื่อขจัดสาเหตุของความไม่สอดคล้องตามข้อกำหนดของ ISMS ที่อาจเกิดขึ้น โดยต้องมีการจัดทำเอกสารระเบียบการปฏิบัติงาน ดังนี้

1. การระบุถึงความไม่สอดคล้องตามข้อกำหนดที่อาจจะเกิดขึ้น และสาเหตุ

2. การประเมินถึงความจำเป็นในการดำเนินการ เพื่อป้องกันการเกิดขึ้นของความไม่สอดคล้องตามข้อกำหนด

3. การดำเนินการปฏิบัติการป้องกัน

4. การบันทึกผลการดำเนินการ

5. การทบทวนการปฏิบัติการป้องกัน

3.2.3.5 บันทึกการปฏิบัติงานและเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของ ISMS

ภายหลังการประเมินภายในให้ดำเนินการตรวจสอบเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของระบบ เพื่อตรวจสอบการนำมาตรการควบคุมไปปฏิบัติ และบันทึกผลจากการวิเคราะห์

3.2.3.6 ทบทวนการจัดการความปลอดภัยเป็นระยะ

โดยปกติการทบทวนการจัดการความปลอดภัยข้อมูลสารสนเทศจะถูกกำหนดให้เหมาะสมกับสภาพแวดล้อมการทำงาน และปัจจัยด้านเทคโนโลยีสารสนเทศต่าง ๆ สำหรับสำนักงานศาลยุติธรรมได้มีการกำหนดการทบทวนนโยบายปกติทุก 1 ปี ในรอบปีงบประมาณเดือนกันยายน ยกเว้นมีการติดตั้งอุปกรณ์ และระบบใหม่ หรือมีการเปิดศาลใหม่ระหว่างปีจะต้องมีการทบทวนการจัดการความปลอดภัยอีกครั้ง เนื่องจากต้องพิจารณาการทำงานที่เพิ่มเข้ามาใหม่ว่ามีผลต่อการรักษาความปลอดภัยของอุปกรณ์ และระบบอย่างไร เป็นช่วงที่มีการเปลี่ยนแปลงติดตั้งอุปกรณ์ และระบบ รวมถึงมีการเปิดหน่วยงานสาขา

3.2.4 ขั้นกำหนดแนวทางปฏิบัติ

3.2.4.1 จัดทำข้อกำหนดที่ชัดเจนในการแบ่งอุปกรณ์และระบบแต่ละประเภท

การแบ่งประเภทอุปกรณ์และระบบที่ติดตั้งอยู่ในศูนย์ปฏิบัติการเครือข่ายสามารถจัดแบ่งได้ตามกฎเกณฑ์หลายรูปแบบ เพื่อให้เกิดความชัดเจนได้จัดแบ่งเกณฑ์ ดังนี้

1. แบ่งประเภทเป็นฮาร์ดแวร์และซอฟต์แวร์ เนื่องจากกระบวนการควบคุมของฮาร์ดแวร์ และซอฟต์แวร์มีรายละเอียดที่แตกต่างกัน

2. แบ่งประเภทตามคุณสมบัติ และการทำงาน เพื่อพิจารณาใช้มาตรการควบคุม และนโยบายรักษาความปลอดภัยในแนวทางเดียวกัน

3. แบ่งประเภทตามเส้นทางในการเข้าถึงระบบ โดยพิจารณาว่าการเข้าสู่ระบบงานหรือฐานข้อมูลมีการผ่านอุปกรณ์ และระบบใดบ้าง เพื่อดำเนินการควบคุมเป็นชั้น ๆ

4. แบ่งประเภทตามระดับรักษาความปลอดภัย เพื่อพิจารณาว่าอุปกรณ์ และระบบมีการกำหนดการควบคุมความปลอดภัยที่เพียงพอ หรือไม่

3.2.4.2 จัดทำแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศสำหรับอุปกรณ์และระบบแต่ละประเภท

จากกรณีศึกษามีการแบ่งอุปกรณ์และระบบแต่ละประเภท โดยสมมติฐานว่าอุปกรณ์และระบบที่มีคุณสมบัติ การทำงาน องค์ประกอบของระบบต่าง ๆ เหมือนหรือคล้ายคลึงกัน การกำหนดนโยบายรักษาความปลอดภัย และมาตรการควบคุมจะเป็นไปในแนวทางเดียวกัน เพื่อนำมาตรการรักษาความปลอดภัยของสินทรัพย์แต่ละประเภทไปใช้กับสินทรัพย์ประเภทเดียวกัน

3.2.4.3 เปรียบเทียบแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศส่วนที่เหมือนกัน และต่างกัน

ตรวจสอบเปรียบเทียบอุปกรณ์ และระบบที่ใช้แนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศประเภทเดียวกัน เพื่อทบทวนความถูกต้อง ครบถ้วน เหมาะสม และพิจารณากำหนดแนวทางรักษาความปลอดภัยในรายละเอียดปลีกย่อยที่เป็นข้อแตกต่างกัน

ตารางที่ 3.5 ตัวอย่างข้อกำหนดการรักษาความปลอดภัยข้อมูลสารสนเทศตามประเภทระบบ

ลำดับ	สินทรัพย์	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
ระบบงานที่ให้บริการเฉพาะ (Specific Service)						
6	Cisco Meeting Server 1000	■ ฮาร์ดแวร์ Cisco UCS C220 M5 Rack Server ■ ซอฟต์แวร์ OS : Linux Application : Cisco Meeting Management v. 8.3 Database : LDAP ■ Storage : -	DMZ	■ ฐานข้อมูลร่วมกัน ■ เรียกใช้ทรัพยากรระหว่างกันโดยกำหนดความเชื่อถือระหว่างอุปกรณ์ด้วยการแลกเปลี่ยน Certificate	สิทธิ์ผู้ดูแลระบบ /เจ้าของระบบ /หน่วยงาน /สิทธิ์บุคคล	■ กำหนดสิทธิ์ควบคุมการเข้าถึงอย่างจำกัดเฉพาะงานที่ทำ ■ ทบทวนสิทธิ์ผู้ดูแลระบบ 2 ครั้ง/ปี ■ กำหนดความยาวรหัสผู้ดูแลระบบไม่น้อยกว่า 8 อักขระและให้ประกอบด้วยอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และอักขระพิเศษ

ตารางที่ 3.5 (ต่อ)

ลำดับ	สินทรัพย์	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
ระบบงานที่ให้บริการเฉพาะ (Specific Service)						
6	Cisco Meeting Server 1000 (ต่อ)	▪ ให้บริการที่ทำงานเฉพาะด้าน สามารถใช้งานได้จากเครือข่ายภายในและภายนอก		▪		▪ กำหนดให้บันทึกรหัสผ่านแจ้งหัวหน้าส่วนระบบเครือข่ายคอมพิวเตอร์ ▪ ปิดการใช้บัญชีผู้ใช้เริ่มต้นของอุปกรณ์ (Default User) และทดสอบการล๊อกอินด้วยบัญชีเริ่มต้น ▪ เปิดให้ควบคุมระบบได้เฉพาะเครื่องคอมพิวเตอร์ ใน VLAN 23 /2 /15 เท่านั้น

ตารางที่ 3.6 ตัวอย่างข้อกำหนดการรักษาความปลอดภัยข้อมูลสารสนเทศจำเพาะ

ลำดับ	สินทรัพย์	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	ข้อมูลจำเพาะ	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
ระบบงานที่ให้บริการเฉพาะ (Specific Service)						
6	Cisco Meeting Server 1000	▪ ฮาร์ดแวร์ Cisco UCS C220 M5 Rack Server ▪ ซอฟต์แวร์ OS : Linux Application : Cisco Meeting	DMZ	▪ ทำงานร่วมกับ Cisco Business Edition 7000 และ 6000 ▪ Video Standard H.261/H.263 (+, ++)/H.264 AVC (baseline and high profile)/	สิทธิ์ผู้ดูแลระบบ /เจ้าของระบบ /หน่วยงาน /สิทธิ์บุคคล	▪ แนวทางรักษาความปลอดภัยช่องโหว่ฮาร์ดแวร์ ▪ แนวทางรักษาความปลอดภัยช่องโหว่ระบบปฏิบัติการ Linux ▪ แนวทางรักษาความปลอดภัยช่องโหว่

ตารางที่ 3.6 (ต่อ)

ลำดับ	สินทรัพย์	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	ข้อมูลจำเพาะ	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
6	Cisco Meeting Server 1000 (ต่อ)	Management v. 8.3 Database : LDAP ■ Storage : - ■ ให้บริการที่ทำงานเฉพาะด้าน สามารถใช้งานได้จากเครือข่ายภายในและภายนอก		H.264 SVC/ WebM, VP8/ Microsoft RTV/ HTML5/ WebRTC /SIP, H.323, TIP/ BFCP RDP / Far End Camera Control (FECC) ■ Audio Standard AAC-LD /Speex /Opus ■ /G.722, G.722.1, G.722.1c, G.728, G.729a, G.711a/u		Cisco Meeting Management v.8.3 ■ แนวทางรักษาความปลอดภัย LDAP ■ แนวทางรักษาความปลอดภัยการกำหนดความเชื่อถือระหว่างอุปกรณ์ ■ แนวทางรักษาความปลอดภัยโปรโตคอล Video Standard ■ แนวทางรักษาความปลอดภัยโปรโตคอล Audio Standard

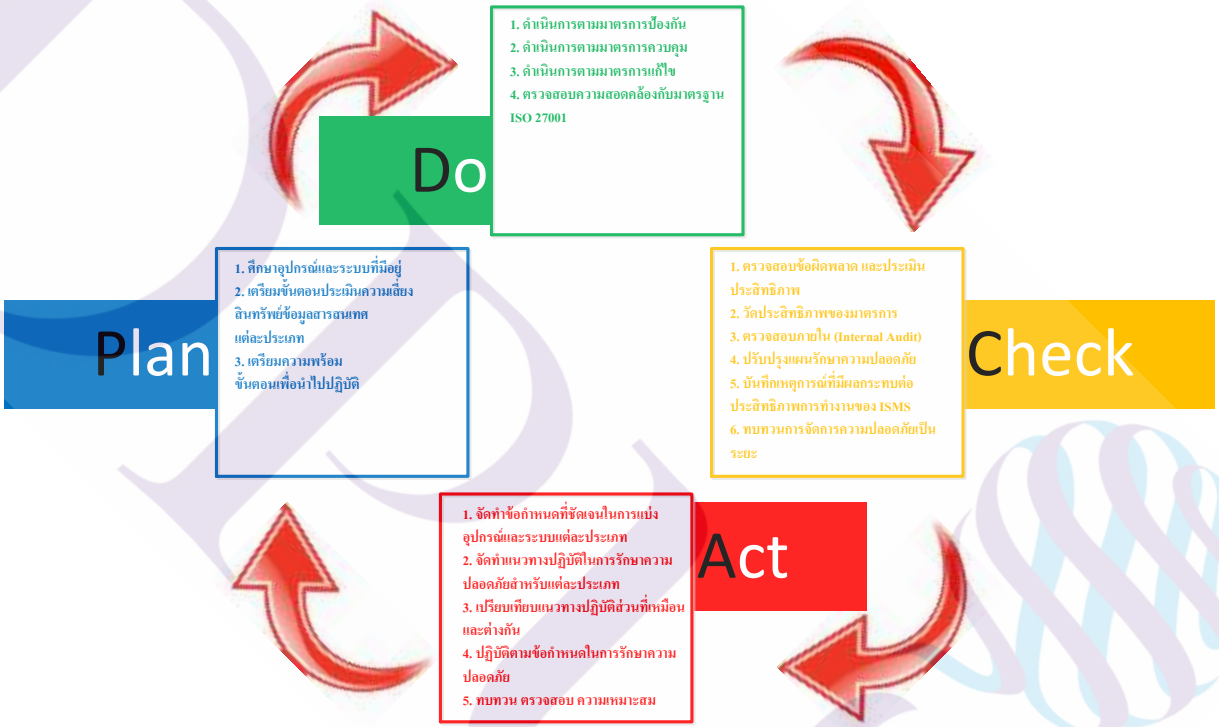
3.2.4.4 ปฏิบัติตามข้อกำหนดในการรักษาความปลอดภัยข้อมูลสารสนเทศ

ปฏิบัติตามข้อกำหนดการรักษาความปลอดภัยข้อมูลสารสนเทศ โดยให้มีการตรวจสอบรายการปฏิบัติในรูปแบบตารางตรวจสอบ

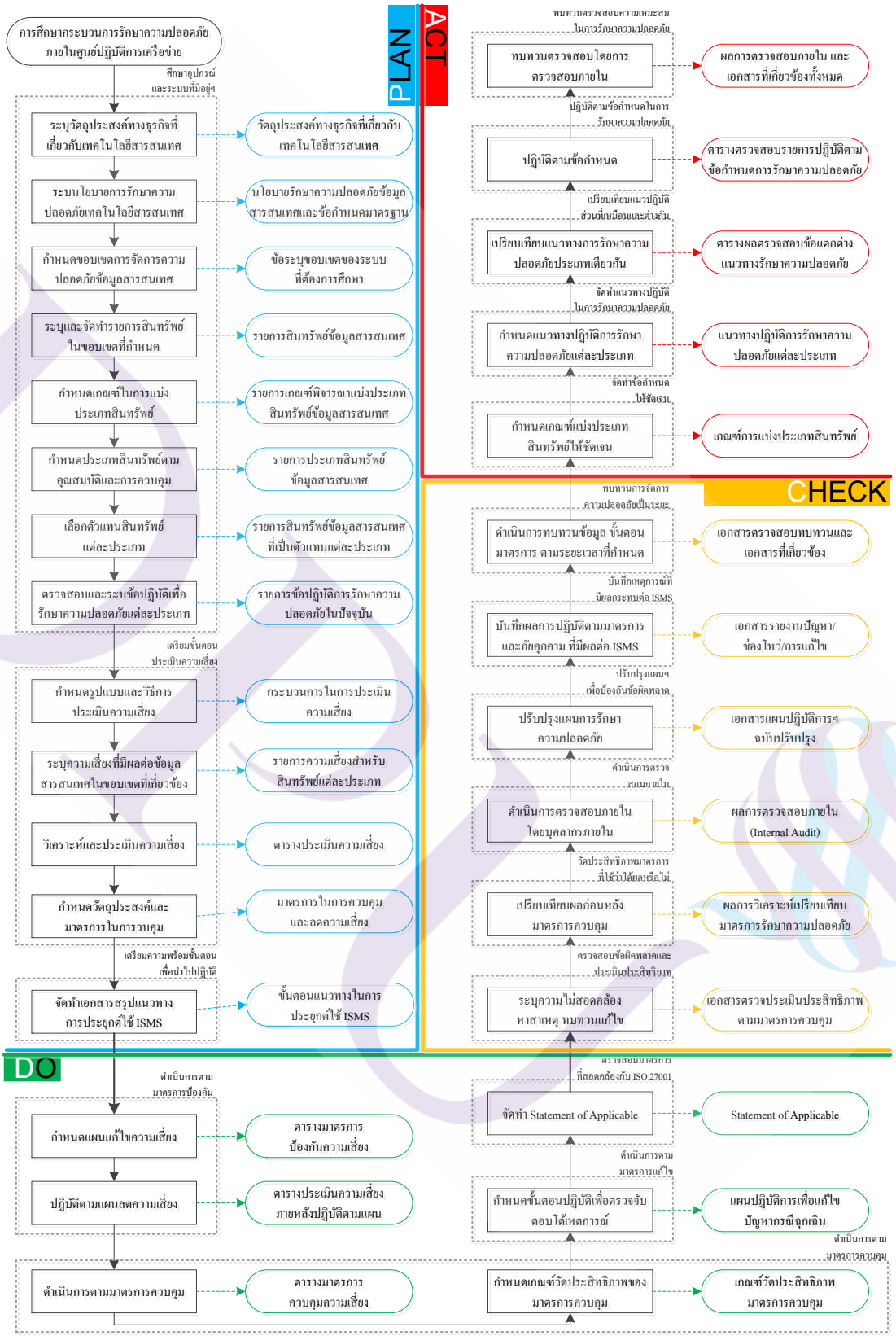
3.2.4.5 ทบทวน ตรวจสอบ ความเหมาะสมในการรักษาความปลอดภัยข้อมูลสารสนเทศ

การทบทวนตรวจสอบความเหมาะสมในการรักษาความปลอดภัยข้อมูลสารสนเทศ เป็นการตรวจสอบภายใน (Internal Audit) ภายหลังดำเนินการตามแนวทางรักษาความปลอดภัยข้อมูลสารสนเทศ เนื่องจากอุปกรณ์และระบบที่มีความเหมือนกันทั้งคุณสมบัติ ลักษณะการใช้งาน อาจมีข้อกำหนดเฉพาะที่แตกต่างกัน เช่น ระดับสิทธิ์ในการเข้าถึงต้องมีการควบคุมเป็นพิเศษ ปริมาณการใช้งาน

3.3 กำหนดแนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ



ภาพที่ 3.2 แนวทางพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศด้วยกระบวนการ PDCA



ภาพที่ 3.3 การดำเนินงานตามกระบวนการพัฒนาระบบรักษาความปลอดภัยในศูนย์ปฏิบัติการเครือข่าย

.

บทที่ 4
ผลการดำเนินงาน

การศึกษาแนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดมาตรฐาน ISO 27001 มีขั้นตอนจำนวนมาก เพื่อแสดงผลการทำงานตามขั้นตอนให้เข้าใจ จึงขอสรุปและยกตัวอย่าง ดังนี้

4.1 ผลการศึกษาขั้นตอนที่เหมาะสมในกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

4.2 ผลการวิเคราะห์การดำเนินงานตามขั้นตอนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

4.3 แนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ

4.1 ผลการศึกษาขั้นตอนที่เหมาะสมในกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

ผู้ศึกษาได้ปรับเปลี่ยนกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศ เพื่อให้เหมาะสมกับการจัดการสินทรัพย์ข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย สำนักเทคโนโลยีสารสนเทศ โดยใช้กระบวนการตามแนวคิด PDCA ดังนี้

ตารางที่ 4.1 ผลการปรับเปลี่ยนขั้นตอนในกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

ขั้นตอน	กิจกรรม	ผลลัพธ์	หมายเหตุ
ขั้นเตรียมความพร้อม : Plan			
1. ศึกษาอุปกรณ์และระบบที่มีอยู่เพื่อทราบสถานะปัจจุบันและความพร้อมในการพัฒนาการจัดการความปลอดภัยข้อมูลสารสนเทศ	1. ระบุวัตถุประสงค์ทางธุรกิจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	วัตถุประสงค์ทางธุรกิจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	เพื่อทราบวัตถุประสงค์ทางธุรกิจที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูลสารสนเทศ
	2. ระบุนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ	นโยบายรักษาความปลอดภัยข้อมูลสารสนเทศและข้อกำหนดมาตรฐานการรักษาความปลอดภัยข้อมูลสารสนเทศที่มีการนำมาใช้งานอยู่ในปัจจุบัน (ถ้ามี)	ศึกษานโยบายที่มีการจัดทำขึ้น หรือข้อกำหนดมาตรฐานที่มีการนำมาใช้ในการรักษาความปลอดภัยข้อมูลสารสนเทศ
	3. กำหนดขอบเขตของระบบจัดการความปลอดภัยข้อมูลสารสนเทศ	ข้อระบุขอบเขตของระบบที่ต้องการศึกษา	เพื่อกำหนดกรอบ ขอบเขตของอุปกรณ์และระบบที่จะดำเนินการจัดการความปลอดภัยข้อมูลสารสนเทศ
	4. ระบุและจัดทำรายการสินทรัพย์ข้อมูลสารสนเทศ ภายในขอบเขตที่กำหนด	รายการสินทรัพย์ข้อมูลสารสนเทศ	เพื่อทราบรายการอุปกรณ์และระบบที่เกี่ยวข้องอย่างครบถ้วน
	5. กำหนดเกณฑ์ในการแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ	รายการเกณฑ์พิจารณาแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ	เพื่อเป็นหลักเกณฑ์ในการพิจารณาแบ่งประเภทสินทรัพย์
	6. กำหนดประเภทสินทรัพย์ข้อมูลสารสนเทศตามคุณสมบัติและการควบคุม	รายการประเภทสินทรัพย์ข้อมูลสารสนเทศ	เพื่อแบ่งกลุ่มสินทรัพย์ข้อมูลสารสนเทศอย่างเหมาะสมตามมาตรการควบคุม
	7. เลือกตัวแทนของสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท	รายการสินทรัพย์ข้อมูลสารสนเทศที่เป็นตัวแทนสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท	เพื่อเป็นตัวแทนสำหรับศึกษาอุปกรณ์และระบบแต่ละประเภท

ตารางที่ 4.1 (ต่อ)

ขั้นตอน	กิจกรรม	ผลลัพธ์	หมายเหตุ
	8. ตรวจสอบและระบุข้อปฏิบัติเพื่อรักษาความปลอดภัยข้อมูลสารสนเทศแต่ละประเภทที่มีการดำเนินการอยู่ในปัจจุบัน	รายการข้อปฏิบัติหรือแนวทางปฏิบัติการรักษาความปลอดภัยข้อมูลสารสนเทศในปัจจุบัน	เพื่อทราบข้อปฏิบัติที่ใช้งานจริง สามารถตรวจสอบความเหมาะสมเพียงพอในการรักษาความปลอดภัยข้อมูลสารสนเทศ
2. เตรียมขั้นตอนประเมินความเสี่ยงสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท เพื่อให้สามารถนำข้อมูลในกระบวนการไปใช้กับอุปกรณ์และระบบที่มีคุณสมบัติลักษณะการทำงานและการกำหนดนโยบายรักษาความปลอดภัยคล้ายคลึงหรือเหมือนกัน	9. กำหนดรูปแบบและวิธีการประเมินความเสี่ยง	กระบวนการในการประเมินความเสี่ยง	เพื่อใช้ในการประเมินความเสี่ยงทั้งหมดในรูปแบบเดียวกัน
	10. ระบุความเสี่ยงที่มีผลต่อข้อมูลสารสนเทศในขอบเขตที่เกี่ยวข้อง	รายการความเสี่ยงสำหรับสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท	เพื่อทราบความเสี่ยงที่เกิดจากสาเหตุต่าง ๆ อย่างครอบคลุมขอบเขตที่ศึกษา
	11. วิเคราะห์และประเมินความเสี่ยง	ตารางประเมินความเสี่ยง	เพื่อทราบระดับความสำคัญความร้ายแรงของความเสี่ยงต่อระบบเทคโนโลยีสารสนเทศ และนำไปใช้ในขั้นตอนจัดการความเสี่ยง
	12. กำหนดวัตถุประสงค์และมาตรการในการควบคุม	มาตรการในการควบคุมและลดความเสี่ยง	เพื่อลดความเสี่ยง เป็นแนวทางปฏิบัติในการจัดการความเสี่ยง
3. เตรียมความพร้อมขั้นตอนเพื่อนำไปปฏิบัติ	13. จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้ ISMS	ขั้นตอนแนวทางในการประยุกต์ใช้ ISMS	เพื่อตรวจสอบแผนการและขั้นตอนการนำไปปฏิบัติ

ตารางที่ 4.1 (ต่อ)

ขั้นตอน	กิจกรรม	ผลลัพธ์	หมายเหตุ
ขั้นดำเนินการ : Do			
1. ดำเนินการตามมาตรการควบคุมเชิงป้องกัน	1. กำหนดแผนการแก้ไขความเสี่ยงสำหรับอุปกรณ์และระบบตัวอย่าง	ตารางมาตรการป้องกันความเสี่ยง	นำข้อมูลการเตรียมขั้นตอนประเมินความเสี่ยงสินทรัพย์ ข้อมูลสารสนเทศ มาใช้ในการกำหนดแผนแก้ไขความเสี่ยง
	2. ปฏิบัติตามแผนลดความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ที่วางไว้	ตารางประเมินความเสี่ยงภายหลังปฏิบัติตามแผนลดความเสี่ยง	ขั้นตอนปฏิบัติ เพื่อลดความเสี่ยง เพื่อให้เห็นถึงผลลัพธ์อาจทำการประเมินความเสี่ยงภายหลังดำเนินการตามแผนลดความเสี่ยงแล้ว
2. ดำเนินการตามมาตรการควบคุมตรวจสอบ	3. ดำเนินการตามมาตรการควบคุมที่เลือก เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้	ตารางมาตรการควบคุมความเสี่ยง	เพื่อตรวจสอบว่าดำเนินการตามมาตรการครบถ้วน ให้มีเอกสารตรวจสอบ
	4. กำหนดเกณฑ์สำหรับวัดประสิทธิภาพของมาตรการควบคุม	เอกสารเกณฑ์วัดประสิทธิภาพของมาตรการควบคุม	เพื่อเป็นเกณฑ์อ้างอิงสำหรับการวัดประสิทธิภาพ
3. ดำเนินการตามมาตรการควบคุมแก้ไข	5. กำหนดขั้นตอนปฏิบัติเพื่อตรวจจับ และตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย	แผนปฏิบัติการเพื่อแก้ไขปัญหากรณีฉุกเฉิน สำหรับอุปกรณ์และระบบ	เพื่อกำหนดขั้นตอนปฏิบัติในกรณีเกิดเหตุการณ์ที่กระทบต่ออุปกรณ์และระบบ
4. ตรวจสอบมาตรการตามข้อตกลงที่สอดคล้องกับมาตรฐาน ISO 27001	6. จัดทำ Statement of Applicability (SoA)	เอกสาร Statement of Applicability (SoA)	เพื่อทราบถึงมาตรการควบคุมที่ถูกนำไปใช้ และไม่ถูกนำไปใช้ พร้อมระบุเหตุผล

ตารางที่ 4.1 (ต่อ)

ขั้นตอน	กิจกรรม	ผลลัพธ์	หมายเหตุ
ขั้นทบทวนแก้ไขปรับปรุง : Check			
1. ตรวจสอบ ตรวจจับข้อผิดพลาด และประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ	1. การระบุความไม่สอดคล้องตามข้อกำหนด 2. การพิจารณาสาเหตุของความไม่สอดคล้องตามข้อกำหนด 3. การประเมินถึงความจำเป็นในการดำเนินการเพื่อให้ความไม่สอดคล้องตามข้อกำหนดไม่เกิดขึ้นซ้ำ 4. การดำเนินการปฏิบัติการแก้ไข 5. การบันทึกผลของการดำเนินการ 6. การทบทวนการปฏิบัติการแก้ไข	เอกสารตรวจประเมินประสิทธิภาพการปฏิบัติตามมาตรการควบคุม	ทบทวนเอกสาร SoA เพื่อตรวจสอบ ประเมินการใช้มาตรการควบคุม ในการรักษาความปลอดภัยข้อมูลสารสนเทศ
2. วัดประสิทธิภาพของมาตรการที่ใช้ว่าได้ผลหรือไม่	เปรียบเทียบผลก่อนและหลังดำเนินการตามมาตรการควบคุม	ผลการวิเคราะห์เปรียบเทียบของมาตรการรักษาความปลอดภัยข้อมูลสารสนเทศก่อนและหลังปรับปรุง	เพื่อทราบถึงประสิทธิภาพของมาตรการว่าถูกต้องเหมาะสม เพียงพอ กับเป้าหมายที่ต้องการหรือไม่
3. ดำเนินการตรวจสอบภายใน (Internal Audit)	ดำเนินการตรวจสอบภายในโดยบุคลากรภายใน	เอกสารผลการตรวจสอบภายใน (Internal Audit)	การตรวจสอบภายในเป็นการตรวจสอบระบบทั้งหมด จะเห็นภาพรวมการทำงาน รวมถึงข้อขัดแย้งในการนำมาตรการควบคุมมาใช้ในการรักษาความปลอดภัย

ตารางที่ 4.1 (ต่อ)

ขั้นตอน	กิจกรรม	ผลลัพธ์	หมายเหตุ
4. ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดที่ตรวจพบ	ปรับปรุงแผนการรักษาความปลอดภัย ภายหลังดำเนินการตรวจสอบภายใน	เอกสารแผนปฏิบัติการรักษาความปลอดภัยข้อมูลสารสนเทศ (ฉบับปรับปรุง)	เพื่อให้แผนมีความถูกต้องเหมาะสม และแก้ไขปัญหาที่พบในกระบวนการตรวจสอบภายใน 1. การระบุถึงความไม่สอดคล้องตามข้อกำหนดที่อาจจะเกิดขึ้น และสาเหตุ 2. การประเมินถึงความจำเป็นในการดำเนินการเพื่อป้องกันการเกิดขึ้นของความไม่สอดคล้องตามข้อกำหนด 3. การดำเนินการปฏิบัติการป้องกัน 4. การบันทึกผลการดำเนินการ 5. การทบทวนการปฏิบัติการป้องกัน
5. บันทึกการปฏิบัติและเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของ ISMS	บันทึกผลการปฏิบัติตามมาตรการควบคุม และเหตุการณ์ภัยคุกคาม ที่มีผลต่อการจัดการความปลอดภัยข้อมูลสารสนเทศ	1. รายงานปัญหาการปฏิบัติตามตามมาตรการรักษาความปลอดภัยข้อมูลสารสนเทศ 2. รายงานการเปลี่ยนแปลงของอุปกรณ์และระบบเทคโนโลยีสารสนเทศ	1. การรักษาความปลอดภัยข้อมูลสารสนเทศด้วยมาตรการควบคุมตามมาตรฐาน ISMS ต้องมีการบันทึก หรือรายงานเพื่อเป็นหลักฐานใช้ตรวจสอบแก้ไขตามขั้นตอน

ตารางที่ 4.1 (ต่อ)

ขั้นตอน	กิจกรรม	ผลลัพธ์	หมายเหตุ
		3. รายงานช่องโหว่และภัยคุกคามที่ยังไม่มีการตรวจสอบ 4. รายงานและการแก้ไขปัญหากรณีฉุกเฉิน 5. รายงานการเปลี่ยนแปลงของข้อกำหนด กฎหมาย และนโยบายรักษาความปลอดภัยข้อมูลสารสนเทศ 6. รายงานการเปลี่ยนแปลงผู้ดูแลระบบ และผู้ใช้	2. บันทึกพื้นที่จุดอ่อน ที่ปฏิบัติตามมาตรการควบคุมไม่เหมาะสม (ทั่วไปหมายถึง การปฏิบัติน้อยกว่า 90%) 3. กำหนดแผนการปรับปรุงสำหรับจุดอ่อนแต่ละจุด โดยให้ทำงานร่วมกับผู้มีส่วนเกี่ยวข้องเพื่อกำหนดวิธีการปรับปรุงการควบคุม 4. กำหนดการประเมินอีกครั้ง กำหนดรอบระยะเวลาเพื่อทบทวนพื้นที่จุดอ่อน เพื่อกำหนดเป้าหมายสำหรับแผนการปรับปรุง
6. ทบทวนการจัดการความปลอดภัยเป็นระยะ	ดำเนินการทบทวนข้อมูล กระบวนการ ขั้นตอน มาตรการ เอกสารควบคุมทั้งหมดตามรอบระยะเวลาที่กำหนด	เอกสารตรวจสอบรายการทบทวนการจัดการความปลอดภัย และ เอกสารที่เกี่ยวข้องทั้งหมด	การทบทวนขึ้นอยู่กับองค์ประกอบด้านเทคโนโลยีสารสนเทศ และระดับการรักษาความปลอดภัย โดยทั่วไปกำหนดระยะเวลา 1 ปี กรณีติดตั้งอุปกรณ์และระบบหรือเปิดศาลใหม่ ให้ทบทวน 2 ช่วงเดือนเมษายน และตุลาคม

ตารางที่ 4.1 (ต่อ)

ขั้นตอน	กิจกรรม	ผลลัพธ์	หมายเหตุ
ขั้นกำหนดแนวทางปฏิบัติ : Act			
1. จัดทำข้อกำหนดที่ชัดเจนในการแบ่งอุปกรณ์และระบบแต่ละประเภท	กำหนดเกณฑ์การแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ และข้อยกเว้นในการนำไปใช้ ที่เหมาะสม	เกณฑ์การแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ	เพื่อให้เกิดความชัดเจน ครอบคลุม และนำไปใช้กำหนดมาตรการควบคุม ได้พิจารณาเกณฑ์ ดังนี้ 1. แบ่งประเภทเป็นฮาร์ดแวร์และซอฟต์แวร์ 2. แบ่งประเภทตามคุณสมบัติและการทำงาน 3. แบ่งประเภทตามเส้นทางในการเข้าถึงระบบ 4. แบ่งประเภทตามระดับรักษาความปลอดภัย
2. จัดทำแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศสำหรับอุปกรณ์และระบบแต่ละประเภท	กำหนดแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศจากการแบ่งอุปกรณ์และระบบแต่ละประเภท	แนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศแต่ละประเภท	เพื่อนำแนวทางปฏิบัติฯ ดังกล่าวไปใช้กับสินทรัพย์ประเภทเดียวกัน

ตารางที่ 4.1 (ต่อ)

ขั้นตอน	กิจกรรม	ผลลัพธ์	หมายเหตุ
3. เปรียบเทียบแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศส่วนที่เหมือนกัน และต่างกัน	ตรวจสอบเปรียบเทียบการใช้แนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศประเภทเดียวกัน และกำหนดส่วนที่เหมือนและแตกต่างของอุปกรณ์	ตารางแสดงผลการตรวจสอบข้อแตกต่างแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศ	เพื่อทบทวนความถูกต้องครบถ้วน เหมาะสม เนื่องจากอุปกรณ์และระบบประเภทเดียวกันอาจมีการสภาพการใช้งาน ความสำคัญของข้อมูล การเข้าถึงระบบอื่น แตกต่างกัน เป็นต้น
4. ปฏิบัติตามข้อกำหนดในการรักษาความปลอดภัยข้อมูลสารสนเทศ	ปฏิบัติตามข้อกำหนดการรักษาความปลอดภัยข้อมูลสารสนเทศ	ตารางตรวจสอบการปฏิบัติตามข้อกำหนดในการรักษาความปลอดภัยข้อมูลสารสนเทศ	เพื่อการนำไปปฏิบัติแต่ละหัวข้อถูกต้องครบถ้วนจึงให้มีการบันทึก และตรวจสอบรายการปฏิบัติด้วย
5. ทบทวน ตรวจสอบความเหมาะสมในการรักษาความปลอดภัยข้อมูลสารสนเทศ	ทบทวนตรวจสอบการดำเนินการรักษาความปลอดภัยข้อมูลสารสนเทศโดยการตรวจสอบภายใน (Internal Audit)	เอกสารที่เกี่ยวข้องทั้งหมด	เพื่อตรวจสอบความเหมาะสม และเพียงพอในการรักษาความปลอดภัย

4.2 ผลการดำเนินงานตามขั้นตอนการรักษาความปลอดภัยข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่าย

ผลการดำเนินงานตามขั้นตอนที่กำหนดในข้อ 4.1 เพื่อให้เข้าใจง่ายจะได้แสดงโครงสร้าง วิธีการปฏิบัติตามลำดับ กระบวนการขั้นตอน และยกตัวอย่าง ดังนี้

4.2.1 ขั้นเตรียมความพร้อม : Plan

4.2.1.1 ศึกษาอุปกรณ์ และระบบที่มีอยู่เพื่อทราบสถานะปัจจุบัน และความพร้อมในการพัฒนาการจัดการความปลอดภัยข้อมูลสารสนเทศ

1. ระบุวัตถุประสงค์ทางธุรกิจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

จากวัตถุประสงค์ทางธุรกิจซึ่งถอดออกมาจากแผนยุทธศาสตร์ศาลยุติธรรม พ.ศ. 2561 – 2564 สรุปวัตถุประสงค์ด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับวัตถุประสงค์ทางธุรกิจ ดังนี้

1.1 ดำเนินการจัดเก็บฐานข้อมูล โดยจัดให้มีช่องทางหรือวิธีการ อุปกรณ์ และระบบ จัดเก็บข้อมูลต่าง ๆ ในรูปแบบฐานข้อมูล เพื่อให้สามารถตรวจสอบ วิเคราะห์ข้อมูล หรือแสดงข้อมูลตามเงื่อนไขการค้นหา

1.2 เผยแพร่ ข้อมูลต่าง ๆ ผ่านช่องทางที่หลากหลาย เพื่อเข้าถึงผู้ใช้ที่มีระดับสิทธิ์แตกต่างกันสามารถเข้าถึงข้อมูลได้เฉพาะสิทธิ์ได้รับ คือ

1.2.1 เผยแพร่ข้อมูลเฉพาะเครือข่ายภายใน ให้สามารถเข้าถึงได้เฉพาะผู้ใช้ภายในหน่วยงานศาลยุติธรรม

12.2. เผยแพร่ข้อมูลระหว่างหน่วยงานที่เชื่อถือได้ เป็นการเผยแพร่ข้อมูลข่าวสารผ่านสื่อต่าง ๆ ระหว่างหน่วยงานในกระบวนยุติธรรมอื่นกับหน่วยงานศาลยุติธรรม

1.2.3 เผยแพร่ข้อมูลทางอินเทอร์เน็ต เป็นการกระจายข้อมูลข่าวสารผ่านสื่อต่าง ๆ ให้แก่สาธารณะ

1.3 ดำเนินการด้านการติดต่อ สื่อสาร โดยจัดให้มีการติดต่อสื่อสารในรูปแบบต่าง ๆ ที่มีความเหมาะสม รองรับการปฏิบัติงานได้อย่างมีประสิทธิภาพ และทั่วถึงไปยังกลุ่มเป้าหมาย

1.4 ดำเนินกระบวนการยุติธรรมภายในหน่วยงานศาลยุติธรรม โดยระบบประชุมทางไกลทางจอภาพ Video Conference ดังนี้

1.4.1 ใช้งาน Video Conference ในกระบวนการพิจารณาคดีระหว่างหน่วยงานศาลยุติธรรม เช่น สืบพยาน อ่านคำพิพากษา ล่ามภาษาต่างประเทศ และผัดฟ้องฝากขังเป็นต้น

1.4.2 ใช้งาน Video Conference เพื่ออำนวยการปฏิบัติงานภายในหน่วยงานศาลยุติธรรม เช่น แถลงนโยบาย ประสานข้อราชการ ประชุม อบรม เป็นต้น

1.4.3 ใช้งาน Video Conference ระหว่างหน่วยงานศาลยุติธรรมและหน่วยงานในกระบวนการยุติธรรมอื่น เช่น ตำรวจ เรือนจำ สถานพินิจและคุ้มครองเด็กและเยาวชน เป็นต้น

1.5 พัฒนาเว็บไซต์เพื่อให้บริการที่สะดวก รวดเร็ว มีประสิทธิภาพ พัฒนา และปรับปรุงเว็บไซต์สำนักงานศาลยุติธรรม และหน่วยงานศาลยุติธรรมเพื่อให้ เข้าถึงข้อมูลได้ง่าย รวดเร็วในการตอบสนอง มีความปลอดภัย และให้บริการครอบคลุมทั่วถึง ดังนี้

1.5.1 Accessibility web เพื่อสามารถให้บริการกลุ่มผู้ใช้ผู้พิการ เช่น พิการทางสายตา ผู้พิการทางหู หรือตาบอดสี สามารถใช้งานเว็บไซต์ได้อย่างมีประสิทธิภาพ

1.5.2 Responsive web เพื่อให้สามารถใช้งานบนอุปกรณ์พกพาขนาดต่าง ๆ ได้อย่างเหมาะสม

1.6 จัดให้มีช่องทางรับข้อมูล ไฟล์เอกสาร จากอินเทอร์เน็ต หรือระบบเพื่อรับข้อมูล ไฟล์เอกสาร หรือไฟล์ในลักษณะอื่นจากเครือข่ายภายนอก อาจมาจากหน่วยงานในกระบวนการยุติธรรมอื่น คู่ความ หรือกลุ่มผู้ใช้ที่ทำงานกับหน่วยงานศาลยุติธรรม

1.7 พัฒนาระบบงานเพื่อให้บริการที่สะดวก รวดเร็ว มีประสิทธิภาพ โดยดำเนินการพัฒนาระบบงานให้สอดคล้องกับการปรับเปลี่ยนกระบวนการทำงานของหน่วยงานศาลยุติธรรมให้เป็นมาตรฐานเดียวกัน มีความสะดวกในการใช้งาน ลดความยุ่งยากซับซ้อนของกระบวนการทำงาน และไม่เกิดการค้างของระบบงาน การคำนวณค่าสถิติหรือการประมวลผลมีความถูกต้องตรวจสอบได้ การให้บริการแก่กลุ่มผู้ใช้ 4 ลักษณะ ได้แก่

1.7.1 เจ้าหน้าที่ของหน่วยงานศาลยุติธรรม และผู้พิพากษา

1.7.2 เจ้าหน้าที่ของหน่วยงานในกระบวนการยุติธรรมอื่น

1.7.3 คู่ความ และผู้มีส่วนได้ส่วนเสียในคดี

1.7.4 ประชาชนทั่วไป

1.8 ใช้งานอุปกรณ์ และระบบเทคโนโลยีสารสนเทศช่วยในการทำงานด้านต่าง ๆ เพิ่มมากขึ้น โดยพัฒนา จัดหาโดยวิธีซื้อหรือเช่า อุปกรณ์ และระบบเทคโนโลยีสารสนเทศเพื่อช่วยในการทำงาน เช่น อุปกรณ์อิเล็กทรอนิกส์สำหรับตรวจสอบหรือจำกัดการเดินทางของบุคคลมาใช้ในการปล่อยชั่วคราว (EM)

1.9 ดำเนินการปรับปรุงอุปกรณ์ และระบบเทคโนโลยีสารสนเทศด้านต่าง ๆ ให้มีประสิทธิภาพยิ่งขึ้น

1.9.1 ปรับปรุงอุปกรณ์ฮาร์ดแวร์ และเครื่องแม่ข่าย ให้มีความทันสมัย รวดเร็ว รองรับการใช้งานที่เพิ่มมากขึ้น และสามารถใช้งานร่วมกับเทคโนโลยีปัจจุบันได้อย่างมีประสิทธิภาพ

1.9.2 ปรับปรุงระบบงาน ที่มีอยู่เดิมหรือพัฒนาทดแทนเพื่อให้รองรับการใช้งานได้อย่างเพียงพอ แก้ไขข้อผิดพลาด ช่องโหว่ เพิ่มความรวดเร็วในกระบวนการทำงานและมีประสิทธิภาพ

1.9.3 ปรับปรุงโครงสร้างพื้นฐาน เครือข่าย อุปกรณ์ โดยจัดหาเพื่อทดแทนของเดิมที่ชำรุด ให้บริการแก่หน่วยงานศาลยุติธรรมที่เพิ่มจำนวนมากขึ้น และปรับปรุงให้มีประสิทธิภาพ ขยายขนาดช่องสัญญาณ (Bandwidth) สามารถตรวจสอบ (Monitoring) กำหนดนโยบาย (Policy) และบริหารจัดการทำงาน (Manage) ได้อย่างมีประสิทธิภาพ

1.9.4 ปรับปรุงการรักษาความปลอดภัยข้อมูลสารสนเทศ เพื่อลดช่องโหว่ และยกระดับการรักษาความปลอดภัยข้อมูลสารสนเทศให้มีประสิทธิภาพ และทันสมัย ให้มีการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) ความพร้อมใช้งาน (Availability)

1.10 นำทรัพยากรข้อมูลสารสนเทศมาใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพการทำงาน

1.10.1 นำฐานข้อมูลมาใช้ในการประมวลผลด้านต่าง ๆ และระบบช่วยตัดสินใจ เช่น ระบบติดตามผล และรายงานการปฏิบัติงานของหน่วยงานศาลยุติธรรมแต่ละแห่ง

1.10.2 ประยุกต์ใช้งาน Video Conference เพื่อเพิ่มประสิทธิภาพและลดค่าใช้จ่าย เช่น นโยบายให้ฝึกอบรมผ่าน Video Conference โดยให้ความรู้ และสนับสนุนให้ใช้งาน Video conference สำหรับงานอื่น ๆ

1.10.3 การดำเนินการตามกระบวนการยุติธรรมโดยใช้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบรับและส่ง คำฟ้อง ระบบคัดถ่ายคำพิพากษา ระบบสืบพยานทางไกลผ่านจอภาพ

2. ระบุนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม โดยความร่วมมือของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้ดำเนินการร่างแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลยุติธรรมเรียบร้อยแล้ว ตามเอกสารบทที่ 2 แนวคิดทฤษฎีและผลงานที่เกี่ยวข้อง ในหัวข้อ 2.2.3 และได้มีการนำไปปฏิบัติอย่างไม่เป็นทางการในบางส่วนแล้ว

3. กำหนดขอบเขตของระบบจัดการความปลอดภัยข้อมูลสารสนเทศ

ตารางที่ 4.2 ขอบเขตการรักษาความปลอดภัยข้อมูลสารสนเทศ

ลำดับ	ขอบเขต	รายละเอียด
1	ระบุพื้นที่	พื้นที่ภายในศูนย์ปฏิบัติการเครือข่ายสำนักเทคโนโลยีสารสนเทศ ทั้งในส่วนของ Server Farm, Battery Room และพื้นที่เก็บของ ซึ่งมีการกั้นแบ่งเป็นส่วนหนึ่งของศูนย์ปฏิบัติการเครือข่าย
2	สถานที่	ศูนย์ปฏิบัติการเครือข่ายสำนักเทคโนโลยีสารสนเทศ ชั้น 4 อาคารศาลอาญา
3	สินทรัพย์และเทคโนโลยีขององค์กรอะไรบ้างที่จะถูกควบคุม	■ โครงสร้างพื้นฐาน ■ ระบบควบคุมและบริหารจัดการเครือข่าย ■ ระบบที่สำนักเทคโนโลยีสารสนเทศเป็นผู้พัฒนาระบบ หรือเป็นผู้ดูแลระบบ หรือเป็นเจ้าของระบบ ■ ระบบที่สำนักงานศาลยุติธรรมจัดซื้อจัดจ้าง หรือไม่ได้เป็นผู้พัฒนาระบบ หรือไม่ได้เป็นเจ้าของระบบ ■ ระบบที่หน่วยงานในสังกัดสำนักงานศาลยุติธรรมขอติดตั้งใช้งานภายในศูนย์ปฏิบัติการเครือข่ายฯ เช่น ศูนย์วิทยบริการ ■ ระบบที่หน่วยงานอื่นติดตั้งไว้เพื่อเชื่อมต่อให้บริการภายในหน่วยงานศาลยุติธรรม เช่น ทะเบียนราษฎร์ ระบบที่ให้บริการระหว่างหน่วยงานพันธมิตร เช่น บริการข้อมูลผ่าน Web Service
4	ระบุผู้ให้บริการ	■ ผู้ให้บริการเครือข่าย : CAT Telecom ■ ผู้ให้บริการโครงสร้างพื้นฐาน : SITEM

ตารางที่ 4.2 (ต่อ)

ลำดับ	ขอบเขต	รายละเอียด
5	ระบุคู่ค้า	■ หน่วยงานสำนัก/กอง ของสำนักงานศาลยุติธรรม ■ หน่วยงานศาลยุติธรรมทั่วประเทศ ■ ผู้บริหารหน่วยงานศาลยุติธรรมผู้บริหารศาลยุติธรรม ■ ผู้บริหารสำนักงานศาลยุติธรรม ■ เจ้าหน้าที่ผู้ใช้งานปฏิบัติงานด้วยระบบงานและบริการของสำนักงานศาลยุติธรรม นักวิชาการคอมพิวเตอร์และพนักงานคอมพิวเตอร์
6	ระบุหน่วยงานภายนอกที่มีการทำงานร่วมกัน	■ สถาบันนิติวิทยาศาสตร์ ■ ตำรวจ สถานีตำรวจภูธร ■ ราชทัณฑ์ เรือนจำ ทัณฑสภาน ■ สถานพินิจ และคุ้มครองเด็กและเยาวชน, ศูนย์ฝึกอบรมเด็กและเยาวชน สำนักงานอัยการจังหวัด ■ ธนาคารกรุงไทย ■ ธนาคารกสิกรไทย ■ ธนาคารไทยพาณิชย์ ■ ธนาคารออมสิน
7	ระบุการพึ่งพาองค์กรอื่น	■ ThaiCERT ■ EDTA ■ DGA ■ MOI
8	ระบุมาตรฐานด้านกฎระเบียบหรือกฎหมายที่ใช้กับพื้นที่	■ ร่างแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลยุติธรรม ■ แผนปฏิบัติการเพื่อแก้ไขปัญหากรณีฉุกเฉิน สำหรับอุปกรณ์และระบบที่อยู่ในความรับผิดชอบของ ส่วนระบบงานฯ ส่วนสนับสนุนฯ และส่วนระบบเครือข่ายฯ

ตารางที่ 4.2 (ต่อ)

ลำดับ	ขอบเขต	รายละเอียด
8	ระบุมาตรฐานด้านกฎระเบียบหรือกฎหมายที่ใช้กับพื้นที่ (ต่อ)	■ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ■ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4. ระบุ และจัดทำรายการสินทรัพย์ข้อมูลสารสนเทศ ภายในขอบเขตที่กำหนด

สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม ได้มีการจัดทำรายการสินทรัพย์ข้อมูลสารสนเทศภายในศูนย์ปฏิบัติการเครือข่ายเรียบร้อยแล้ว โดยจัดทำอยู่ในรูปแบบตาราง Excel และภาพถ่ายประกอบคำอธิบาย ผู้ศึกษาจึงได้ปรับปรุงตารางทะเบียนสินทรัพย์ข้อมูลสารสนเทศเพิ่มข้อมูลในส่วนที่ไม่มีในตารางบันทึกข้อมูล ดังนี้

ตารางที่ 4.3 แบบทะเบียนสินทรัพย์ข้อมูลสารสนเทศ

รายการ	รายละเอียด	หมายเหตุ
ลำดับ	แสดงลำดับสินทรัพย์	0001/0002/0003/0004
สถานะ**	แสดงสถานะอุปกรณ์และระบบ	A = Active = ทำงาน I = Inactive = ปิดระบบ ไม่ทำงาน F = Fix = ซ่อมแซม เปลี่ยนแทน U = Uninstall = รื้อถอน รอส่งคืน สบท
วันที่จัดทำทะเบียน**	บันทึกวันที่จัดทำทะเบียน	วันที่บันทึกรายการสินทรัพย์
ชื่อผู้จัดทำทะเบียน**	ชื่อผู้จัดทำรายละเอียดทะเบียน	ผู้บันทึกรายการสินทรัพย์
สถานที่ติดตั้ง	ระบุสถานที่ติดตั้ง หมายเลขตู้ Rack	ติดตั้งภายในห้องศูนย์ฯ ไม่ระบุตู้ ระบุหมายเลข ตู้ Rack ติดตั้งนอกห้องศูนย์ฯ ภายนอกอาคาร

ตารางที่ 4.3 (ต่อ)

รายการ	รายละเอียด	หมายเหตุ
เลขครุภัณฑ์	หมายเลขครุภัณฑ์ตามที่ สบท กำหนด	เลขครุภัณฑ์จะได้รับต่อเมื่อมีการตรวจรับเรียบร้อยแล้ว รูปแบบ ศย 000000-000-000/0000
ชื่อสินทรัพย์	ใช้ชื่อทางการค้า หรือชื่อเรียกทั่วไป	กรณีชื่อซ้ำกันจะต่อท้ายอุปกรณ์ด้วย IP ตัวท้าย เช่น MCU41 / MCU42
ยี่ห้อ	ระบุยี่ห้อสินทรัพย์	เพื่อติดต่อ ประกันแต่ละแบรนด์
รุ่น	ระบุรุ่น	เพื่อตรวจสอบช่องโหว่ของอุปกรณ์และระบบในรุ่นนั้น
ขนาด	ระบุขนาด	เพื่อคำนวณพื้นที่ติดตั้ง U
หมายเลขเครื่อง	ระบุหมายเลขเครื่อง	เพื่อตรวจสอบกลับ S/N
มูลค่าสินทรัพย์	ระบุมูลค่าสินทรัพย์ด้วยราคา	กรณีไม่สามารถระบุราคาได้ให้ประเมินความเสียหายในกรณีอุปกรณ์และระบบหยุดทำงาน
คำอธิบาย	ระบุวัตถุประสงค์	บรรยายวัตถุประสงค์การใช้งาน เช่น เครื่องแม่ข่ายระบบสารบัญอิเล็กทรอนิกส์ / เครื่องทดสอบระบบ
วันที่ติดตั้ง	ระบุวันที่ทำการติดตั้งอุปกรณ์หรือระบบ	วันที่ติดตั้ง วันที่สร้างไฟล์ วันที่อัพเดต วันที่นำอุปกรณ์ออก
ระบบปฏิบัติการ	ระบุระบบปฏิบัติการ Windows/Linux/VM/etc	แจ้งระบบปฏิบัติการ พร้อมระบุรุ่น กรณีเป็น VM และมีการติดตั้งระบบปฏิบัติการอื่น ให้ระบุครบถ้วน เพื่อระบุช่องโหว่จากระบบปฏิบัติการต่าง ๆ

ตารางที่ 4.3 (ต่อ)

รายการ	รายละเอียด	หมายเหตุ
VLAN	ระบุ VLAN	จัดกลุ่ม VLAN ภายในหน่วยงาน เช่น VLAN 23 ของสำนักเทคโนโลยีสารสนเทศ ซึ่งจะได้รับสิทธิ์ในการเข้าถึงอุปกรณ์และระบบภายในห้องศูนย์ปฏิบัติการเครือข่าย
IP ภายใน	ระบุ IP ภายใน	ทั่วไป 10.xx.xx.xx กรณีเป็น VM ให้ระบุ IP ใน VM ต่อท้ายด้วย เช่น10.xx.xx.xx (10.1.3.xx)
IP สาธารณะ	ระบุ IP สาธารณะ (ถ้ามี)	61.19.239.xxx
ระบบงานที่ให้บริการ**	ระบุระบบงานที่ติดตั้งใช้งาน ระบุอุปกรณ์ที่เรียกใช้งาน	การใช้งานเครื่องแม่ข่ายหรืออุปกรณ์ กรณีมีมากกว่า 1 ระบบ ให้ระบุข้อมูลให้ครบถ้วน แต่เดิมข้อมูลระบบงานจะบันทึกอยู่ในหมายเหตุ
ส่วนหรือหน่วยงานที่ใช้งาน**	ระบุตำแหน่ง ส่วนงาน หน่วยงานที่ใช้งาน หรือระบบงานอื่นที่เรียกใช้งานระบบดังกล่าว	เพื่อทราบว่าอุปกรณ์และระบบมีการใช้จากไหน พิจารณากำหนดสิทธิ์ การเข้าถึงระบบ และตรวจสอบช่องโหว่จากการเรียกใช้งาน
ระบุพื้นที่เข้าถึงเพื่อใช้งาน	ระบุ Zone ที่กำหนดให้ระบบ	Internal Zone External Zone DMZ
วันที่หมดอายุรับประกัน	ระบุวัน เดือน ปี ที่หมดอายุรับประกัน	เพื่อเตรียมความพร้อมกับความเสี่ยงภายหลังหมดประกัน
ระบุเจ้าของสินทรัพย์	ระบุเจ้าของสินทรัพย์ ผู้ดูแลระบบ ผู้สร้างไฟล์ ผู้ได้รับมอบหมาย	ชื่อบุคคล ส่วนงาน หน่วยงาน สำนัก/กอง หน่วยงานศาล หน่วยงานภายนอก

ตารางที่ 4.3 (ต่อ)

รายการ	รายละเอียด	หมายเหตุ
หมายเหตุ	ระบุข้อความอื่น ๆ	คำสั่งพิเศษสำหรับอุปกรณ์และระบบ เช่น อยู่ระหว่างจัดซื้อทดแทน / ให้ปิดการให้บริการจนกว่าจะมีคำสั่งอื่น / ทบทวนความปลอดภัยแล้วให้เปิดบริการได้ โดยแจ้งการเปิด port เพิ่มเติมที่ส่วนระบบเครือข่าย

หมายเหตุ ** รายการที่เพิ่มขึ้นจากรูปแบบบันทึกเดิม

5. กำหนดเกณฑ์ในการแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ

เกณฑ์การแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศตามคุณสมบัติ และการกำหนดมาตรการควบคุม ดังนี้

ตารางที่ 4.4 เกณฑ์การแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ

ลำดับ	เกณฑ์การแบ่งประเภท	ประเภทสินทรัพย์
1	ลักษณะสินทรัพย์	■ Hardware ■ Software ■ People ware ■ Process
2	พื้นที่เครือข่ายที่เข้าถึงระบบได้	■ Internal Zone ■ External Zone ■ DMZ
3	ขอบเขตการทำงานของระบบ	■ ระบบโครงสร้างพื้นฐาน ■ ระบบควบคุมสัญญาณเครือข่าย ■ ระบบที่ให้บริการเฉพาะเครือข่ายภายใน

ตารางที่ 4.4 (ต่อ)

ลำดับ	เกณฑ์การแบ่งประเภท	ประเภทสินทรัพย์
3	ขอบเขตการทำงานของระบบ (ต่อ)	■ ระบบที่ให้บริการผ่านเครือข่ายภายนอก ■ ระบบที่ให้บริการระหว่างหน่วยงานพันธมิตร ■ ระบบที่ใช้บริการของหน่วยงานภายนอก
4	หน้าที่การทำงานของอุปกรณ์และระบบ	■ ระบบไฟฟ้า ■ ระบบปรับอากาศ ■ ระบบล๊อกทางเข้าออก ■ ระบบตรวจจับควัน ■ ระบบตรวจจับความร้อน ■ ระบบตรวจจับน้ำรั่วซึม ■ ระบบพ่นสารดับเพลิง ■ ระบบตรวจจับความเคลื่อนไหวและบันทึกภาพ ■ ระบบแจ้งเตือนทางอีเมล์และ SMS ■ ไฟร์วอล ■ สวิตช์ ■ เครื่องแม่ข่าย ■ อุปกรณ์บันทึกข้อมูล ■ ระบบฐานข้อมูล ■ ระบบงานภายในศาลยุติธรรม ■ ระบบงานที่ใช้งานร่วมหน่วยงานภายนอก ■ ระบบงานที่ให้บริการโดยหน่วยงานอื่น ระบบงานที่ใช้ร่วมกันเฉพาะหน่วยงานพันธมิตร ■ ระบบงานที่ให้บริการเฉพาะ

ตารางที่ 4.4 (ต่อ)

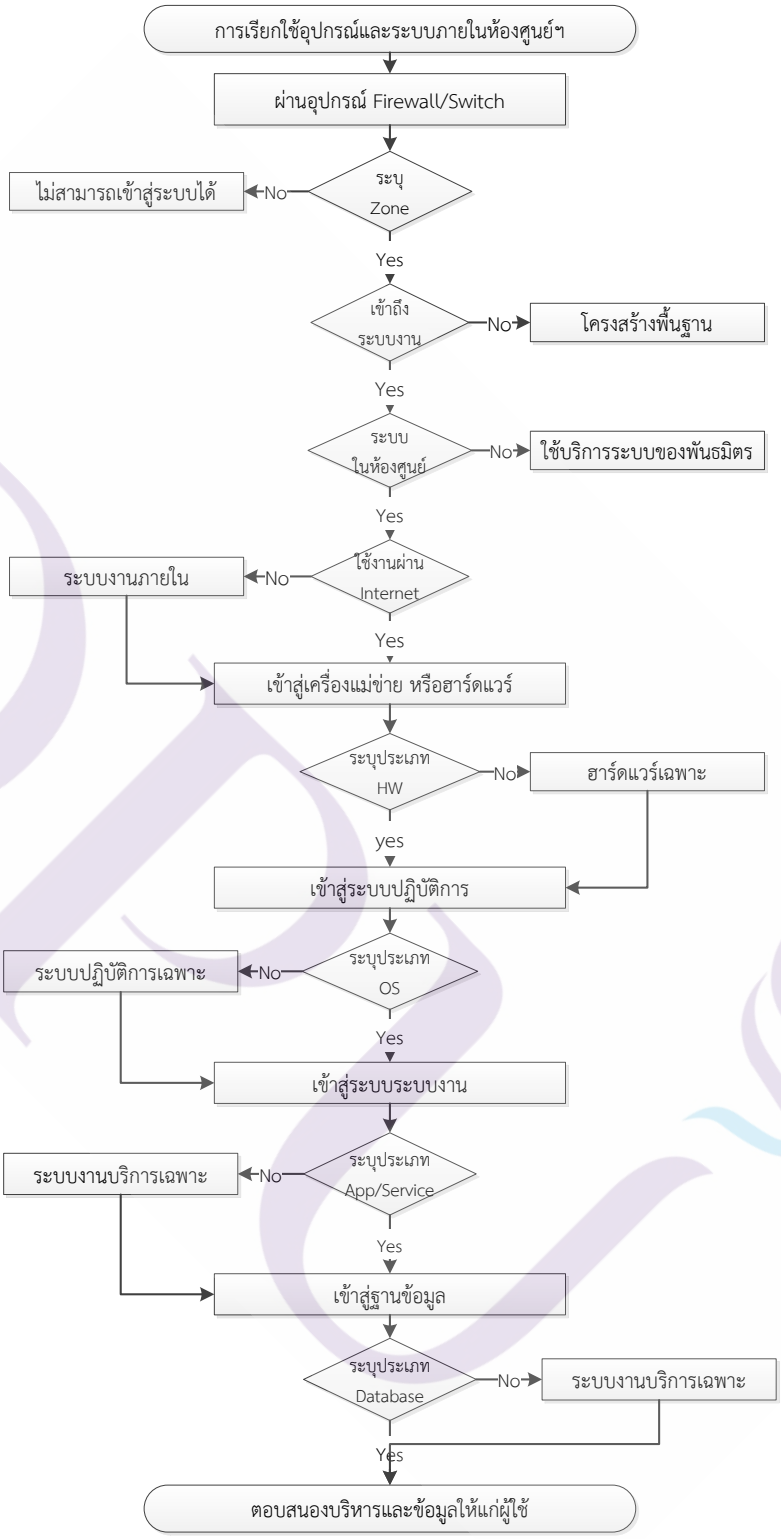
ลำดับ	เกณฑ์การแบ่งประเภท	ประเภทสินทรัพย์
4	หน้าที่การทำงานของอุปกรณ์และระบบ (ต่อ)	▪ เว็บไซต์
5	ความรับผิดชอบดูแลระบบ	▪ ส่วนระบบเครือข่ายเป็นผู้รับผิดชอบดูแลระบบ ▪ ส่วนระบบงานคอมพิวเตอร์เป็นผู้รับผิดชอบดูแลระบบ ▪ ส่วนสนับสนุนและให้บริการระบบงานคอมพิวเตอร์เป็นผู้ดูแลระบบ ▪ หน่วยงานสำนัก/กอง ในสังกัดสำนักงานศาลยุติธรรม เป็นผู้ดูแลระบบ ▪ หน่วยงานศาลยุติธรรมเป็นผู้ดูแลระบบ ▪ หน่วยงานคู่ค้า เป็นผู้ดูแลระบบ
6	ระบบปฏิบัติการ	▪ หน่วยงานผู้ให้บริการเป็นผู้ดูแลระบบ ▪ หน่วยงานบริษัทผู้ขายหรือผู้รับจ้างเป็นผู้ดูแลระบบ Microsoft Windows ▪ Linux ▪ VM ▪ ระบบปฏิบัติการอื่น ๆ
7	ความเสี่ยงของการโจมตีต่าง ๆ	▪ Hacker ▪ Sniffing ▪ Modification ▪ Malware ▪ Social engineering ▪ Phishing ▪ Password guessing ▪ Crytanalysis

ตารางที่ 4.4 (ต่อ)

ลำดับ	เกณฑ์การแบ่งประเภท	ประเภทสินทรัพย์
7	ความเสี่ยงของการโจมตีต่าง ๆ (ต่อ)	■ Macro virus ■ IP spoofing ■ DoS / DDoS ■ Crypter ■ Rootkit ■ Zero-day ■ Zombies ■ โจมตีด้วย Protocol เฉพาะของระบบ
8	ระดับความสำคัญของการกำหนดสิทธิ์	■ สิทธิ์ผู้ดูแลระบบเท่านั้น ■ สิทธิ์เจ้าของระบบ สามารถบริหารจัดการระบบ ขอบเขตจำกัด ■ สิทธิ์ผู้บริหาร ■ สิทธิ์ผู้ปฏิบัติงาน ■ สิทธิ์เฉพาะบุคคล ■ สิทธิ์เฉพาะบุคลากรภายใน ■ สิทธิ์สาธารณะ

6. กำหนดประเภทสินทรัพย์ข้อมูลสารสนเทศตามคุณสมบัติและการควบคุม

เกณฑ์การจัดประเภทสินทรัพย์ มีความหลากหลาย และจำเพาะเจาะจงไม่เหมือนกันในรายละเอียด จึงพิจารณาจากเส้นทางการเข้าถึงข้อมูล เพื่อกำหนดประเภท ดังนี้



ภาพที่ 4.1 แผนผังแสดงจุดตรวจสอบการเข้าถึงอุปกรณ์และระบบภายในศูนย์ปฏิบัติการเครือข่าย

ตารางที่ 4.5 คุณสมบัติตามการแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศ

ลำดับ	ประเภท	คุณสมบัติ	สินทรัพย์ตัวอย่าง
1	โครงสร้างพื้นฐานศูนย์ปฏิบัติการเครือข่าย (Infrastructure)	**ลักษณะสินทรัพย์** Hardware : etc OS : etc Database : etc **หน้าที่การทำงาน** บริหารจัดการโครงสร้างพื้นฐานภายในศูนย์ปฏิบัติการเครือข่าย **พื้นที่เครือข่ายที่เข้าถึง** Internal Zone **ความรับผิดชอบดูแล** ▪ ส่วนระบบเครือข่าย ตรวจสอบความผิดปกติ รายงาน แก้ไขเบื้องต้น ▪ บริษัท SITEM แก้ไขความผิดปกติที่ต้องมีการซ่อมแซม เปลี่ยนทดแทน	1. ระบบสำรองไฟฟ้า 2. ระบบปรับอากาศ 3. ระบบล๊อกด้วยการสแกนลายนิ้วมือและรหัสผ่าน 4. ระบบตรวจจับควัน 5. ระบบตรวจจับความร้อน 6. ระบบตรวจจับน้ำรั่วซึม 7. ระบบพ่นสารดับเพลิง 8. ระบบตรวจจับความเคลื่อนไหวและบันทึกภาพ 9. ระบบแจ้งเตือนทางอีเมล์และ SMS
2	ระบบบริหารจัดการเครือข่าย (Network Management)	**ลักษณะสินทรัพย์** Hardware : Rack Server OS : Linux Database : etc. **หน้าที่การทำงาน** ▪ บริหารจัดการเส้นทางเครือข่าย ▪ ควบคุมนโยบายรักษาความปลอดภัย **พื้นที่เครือข่ายที่เข้าถึง** Internal Zone	1. firewall 2. IPS 3. IDS 4. Switch

ตารางที่ 4.5 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติ	สินทรัพย์ตัวอย่าง
2	ระบบบริหารจัดการเครือข่าย (Network Management) (ต่อ)	**ความรับผิดชอบดูแล** ▪ ส่วนระบบเครือข่ายตรวจสอบความผิดปกติ รายงาน แก้ไขเบื้องต้น ▪ บริษัทผู้รับจ้างแก้ไขความผิดปกติที่ต้องมีการซ่อมแซม เปลี่ยนทดแทน (อยู่ในประกัน ทดแทนทุก 5 ปี)	
3	ระบบงานที่ให้บริการเฉพาะเครือข่ายภายใน (Internal Service)	**ลักษณะสินทรัพย์** Hardware : Rack Server OS : MS Windows/Linux/VM Application : .Net / Java / MS Access Database : MS Access / My SQL / SQL Server / Oracle Storage : NAS **หน้าที่การทำงาน** ▪ ให้บริการระบบที่ใช้งานเฉพาะภายในหน่วยงานศาลยุติธรรม **พื้นที่เครือข่ายที่เข้าถึง** Internal Zone **ความรับผิดชอบดูแล** ▪ ส่วนระบบเครือข่ายเป็นผู้รับผิดชอบดูแลระบบ ▪ ส่วนระบบงานคอมพิวเตอร์เป็นผู้รับผิดชอบดูแลระบบ	1. รายงาน MPLS 2. รายงานการพิจารณาและวินิจฉัยอุทธรณ์และการพิจารณาข้อร้องเรียนเกี่ยวกับการจัดซื้อจัดจ้างฯ 3. รายงานการใช้ประโยชน์ข้อมูลทะเบียนราษฎร 4. ระบบการจัดเก็บและให้บริการคัดสำเนาคำพิพากษาระหว่างศาลทั่วประเทศ 5. ระบบขอย้ายข้าราชการศาลยุติธรรม 6. ระบบพิมพ์สลิปเงินเดือน 7. ระบบรายงานการสืบหาหลักทรัพย์และการผ่อนชำระหนี้ของลูกหนี้ตามคำพิพากษา

ตารางที่ 4.5 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติ	สินทรัพย์ตัวอย่าง
3	ระบบงานที่ให้บริการเฉพาะเครือข่ายภายใน (Internal Service) (ต่อ)	▪ ส่วนสนับสนุนและให้บริการระบบงานคอมพิวเตอร์เป็นผู้ดูแลระบบ ▪ หน่วยงานสำนัก/กอง ในสังกัดสำนักงานศาลยุติธรรม เป็นผู้ดูแลระบบ ▪ หน่วยงานศาลยุติธรรมเป็นผู้ดูแลระบบ ▪ หน่วยงานพันธมิตร เป็นผู้ดูแลระบบ ▪ หน่วยงานบริษัทผู้ขายหรือผู้รับจ้างเป็นผู้ดูแลระบบ	8. ระบบรายงานผลการให้บริการ ข้อมูลข่าวสารของหน่วยงานในสังกัด ฯ 9. ระบบสารบรรณอิเล็กทรอนิกส์ 10. ระบบส่งข้อมูลพัฒนาศักยภาพข้าราชการศาลยุติธรรม (คพ.) 11. รายงานผลการดำเนินงานตามนโยบายประธานศาลฎีกา 12. โปรแกรมข้อมูลบัญชีเงินฝาก 13. โปรแกรมค้นหาข้อมูลทะเบียนนิติบุคคล 14. โปรแกรมฌาปนกิจสงเคราะห์ศาลยุติธรรม 15. โปรแกรมตรวจสอบนายประกันผิดสัญญา 16. โปรแกรมตรวจสอบประวัติการดำเนินคดีของบุคคล 17. โปรแกรมบันทึกข้อมูลเพื่อการตรวจราชการ 18. โปรแกรมพิมพ์หนังสือรับรองการหักภาษี ณ ที่จ่าย 19. โปรแกรมระบบฐานข้อมูลการบังคับคดีผู้ประกัน

ตารางที่ 4.5 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติ	สินทรัพย์ตัวอย่าง
3	ระบบงานที่ให้บริการเฉพาะเครือข่ายภายใน (Internal Service) (ต่อ)		20. โปรแกรมระบบสารสนเทศทรัพยากรบุคคล (DPIS) 21. โปรแกรมรายงานผลการใช้จ่ายเงินสำนักงานศาลยุติธรรม 22. โปรแกรมสำรวจข้อมูลอาคารที่ทำการศาลและบ้านพัก 23. โปรแกรมเผยแพร่คำพิพากษาศาลชั้นต้น 24. ห้องสมุดอิเล็กทรอนิกส์ (รับฝากเซิร์ฟเวอร์ให้บริการ) 25. ระบบค้นหาร่างคำพิพากษาศาลฎีกา (รับฝากเซิร์ฟเวอร์ให้บริการ)
4	ระบบงานที่ให้บริการผ่านเครือข่ายภายนอก (External Service)	**ลักษณะสินทรัพย์** Hardware : Rack Server OS : MS Windows/Linux/VM Application : .Net / Java / MS Access Database : MS Access / My SQL / SQL Server / Oracle Storage : NAS **หน้าที่การทำงาน** ให้บริการระบบที่ใช้งานได้ทั้งเครือข่ายภายในและเครือข่ายภายนอก (อินเทอร์เน็ต)	1. ระบบค้นหาข้อมูลคดี 2. ระบบค้นหาเขตอำนาจศาล 3. ระบบติดตามสำนวนคดี (Tracking System) 4. โปรแกรมคำนวณค่าส่งหมาย 5. ระบบสืบค้นคำพิพากษาศาลชั้นต้น 6. ระบบการส่งเอกสารและประกาศนัดไต่สวน โดยวิธีการโฆษณาทางสื่อฯ (E-Notice System)

ตารางที่ 4.5 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติ	สินทรัพย์ตัวอย่าง
4	ระบบงานที่ให้บริการผ่านเครือข่ายภายนอก (External Service) (ต่อ)	**พื้นที่เครือข่ายที่เข้าถึง** DMZ **ความรับผิดชอบดูแล** ■ ส่วนระบบเครือข่ายเป็นผู้รับผิดชอบดูแลระบบ ■ ส่วนระบบงานคอมพิวเตอร์เป็นผู้รับผิดชอบดูแลระบบ ■ ส่วนสนับสนุนและให้บริการระบบงานคอมพิวเตอร์เป็นผู้ดูแลระบบ ■ หน่วยงานสำนัก/กอง ในสังกัดสำนักงานศาลยุติธรรม เป็นผู้ดูแลระบบ ■ หน่วยงานพันธมิตร เป็นผู้ดูแลระบบ ■ หน่วยงานบริษัทผู้ขายหรือผู้รับจ้างเป็นผู้ดูแลระบบ	7. การยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์ (E - filling) 8. ระบบบริการข้อมูลคดีศาลยุติธรรม (CIOS) 9. ระบบสารสนเทศสำหรับผู้พิพากษา 10. ระบบสมุดโทรศัพท์อิเล็กทรอนิกส์ (E-Phonebook)
5	ระบบงานบริการจากหน่วยงานพันธมิตร (Third party Service)	**ลักษณะสินทรัพย์** Hardware : - OS : - Application : - Database : - Storage : - **หน้าที่การทำงาน** ■ หน่วยงานศาลยุติธรรมใช้ระบบของหน่วยงานพันธมิตร	1. ระบบจดหมายอิเล็กทรอนิกส์ (mail.go.th) 2. ระบบทะเบียนราษฎร์ (dopa)

ตารางที่ 4.5 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติ	สินทรัพย์ตัวอย่าง
5	ระบบงานบริการจากหน่วยงานพันธมิตร (Third party Service) (ต่อ)	**พื้นที่เครือข่ายที่เข้าถึง** Internal Zone สำหรับ dopa DMZ Zone สำหรับ e-Mail **ความรับผิดชอบดูแล** ▪ e – Mail ส่วนระบบเครือข่ายเป็นเจ้าของระบบควบคุมการใช้งานของผู้ใช้และ สพรอ. (DGA) เป็นผู้ดูแลระบบ ▪ dopa ส่วนระบบเครือข่ายเป็นเจ้าของระบบ ควบคุมตรวจสอบการใช้งานของผู้ใช้ และรายงานไปยังมหาดไทย (MOI) เป็นผู้ดูแลระบบ	
6	ระบบงานที่ให้บริการเฉพาะ (Specific Service)	**ลักษณะสินทรัพย์** Hardware : Rack Server OS : MS Windows/Linux/VM Application : etc. Database : My SQL / etc. Storage : NAS **พื้นที่เครือข่ายที่เข้าถึง** Internal สำหรับระบบควบคุม DMZ สำหรับผู้ใช้ **ความรับผิดชอบดูแล** ▪ ส่วนระบบเครือข่ายเป็นผู้ดูแลระบบ ดำเนินการตรวจสอบแก้ไข รายงาน	7. ระบบสื่อสารทางไกลผ่านจอภาพ (Video Conference)

ตารางที่ 4.5 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติ	สินทรัพย์ตัวอย่าง
6	ระบบงานที่ให้บริการเฉพาะ (Specific Service) (ต่อ)	▪ ขอความร่วมมือบริษัทผู้รับจ้างในการแก้ไขปัญหาเนื่องจากไม่มีการต่อ MA	
7	เว็บไซต์ (Website)	**ลักษณะสินทรัพย์** Hardware : Rack Server OS : MS Windows /VM Application : HTML / Java / .NET Database : My SQL Storage : NAS **หน้าที่การทำงาน** ▪ บริการ Web Site หน่วยงานศาลยุติธรรมทั่วประเทศ ▪ บริการ Hosting หน่วยงานศาลยุติธรรมทั่วประเทศ **พื้นที่เครือข่ายที่เข้าถึง** Internal สำหรับระบบควบคุม DMZ สำหรับผู้ใช้ **ความรับผิดชอบดูแล** ▪ ส่วนระบบเครือข่ายเป็นเจ้าของระบบ ▪ บริษัทผู้รับจ้างเป็นผู้ดูแลระบบ เนื่องจากเป็นการจ้างพัฒนา และดูแลด้านความปลอดภัย	1. เว็บไซต์สำนักงานศาลยุติธรรม (www.coj.go.th) 2. เว็บไซต์หน่วยงานสำนัก/กองในสำนักงานศาลยุติธรรม จำนวน 28 หน่วยงาน (ชื่อย่อหน่วยงาน.coj.go.th) 3. เว็บไซต์หน่วยงานศาลยุติธรรมทั่วประเทศ จำนวน 283 หน่วยงาน (ชื่อย่อหน่วยงาน.coj.go.th) 4. เว็บไซต์ชมรมคู่สมรสตุลาการศาลยุติธรรม (ja.coj.go.th) 5. เว็บไซต์สหกรณ์ออมทรัพย์ศาลยุติธรรม (jus.coj.go.th) จัดจ้างพัฒนา และเช่าพื้นที่ hosting ต่อมาย้ายมาอยู่ในศูนย์ฯ 6. เว็บไซต์ศาลฎีกา (www.supremecourt.or.th) จัดจ้างพัฒนา จดทะเบียนโดเมน และเช่าพื้นที่ hosting

7. เลือกตัวแทนของสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท

7.1 ตัวแทนระบบโครงสร้างพื้นฐานศูนย์ปฏิบัติการเครือข่าย (Infrastructure) คือ **ระบบสำรองไฟฟ้า** เนื่องจากเป็นระบบที่มีผลต่อระบบอื่นทั้งหมด

7.2 ตัวแทนระบบบริหารจัดการเครือข่าย (Network Management) คือ **ไฟร์วอลล์** เนื่องจากเป็นด่านหน้าทำหน้าที่กั้นระหว่างเครือข่ายภายในและเครือข่ายภายนอก

7.3 ตัวแทนระบบงานที่ให้บริการเฉพาะเครือข่ายภายใน (Intranet Service) คือ **ระบบสารบรรณอิเล็กทรอนิกส์** เนื่องจากเป็นระบบรับส่งเอกสารราชการที่มีการใช้งานจำนวนมาก

7.4 ตัวแทนระบบงานที่ให้บริการจากเครือข่ายภายนอก (Internet Service) คือ **ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์** (E - filling) เนื่องจากระบบมีความสำคัญและเป็นกระบวนการแรกในการดำเนินกระบวนการยุติธรรม

7.5 ตัวแทนระบบงานที่ใช้บริการหน่วยงานภายนอก (Third party Service) คือ **ระบบจดหมายอิเล็กทรอนิกส์** (e - Mail) เนื่องจากเป็นระบบที่หน่วยงานใช้ในการสื่อสารเป็นหลัก

7.6 ตัวแทนระบบงานที่ให้บริการเฉพาะ (Specific Service) คือ **ระบบสื่อสารทางไกลผ่าน**จอภาพ (Video Conference) เนื่องจากปัจจุบันมีการใช้งานจำนวนมาก

7.7 ตัวแทนเว็บไซต์ของหน่วยงาน (Website) คือ **เว็บไซต์สำนักงานศาลยุติธรรม** เนื่องจากเป็นด่านหน้าให้กับหน่วยงานศาลยุติธรรม

8. ตรวจสอบและระบุข้อปฏิบัติเพื่อรักษาความปลอดภัยข้อมูลสารสนเทศแต่ละประเภทที่มีการดำเนินการอยู่ในปัจจุบัน

ตารางที่ 4.6 ข้อปฏิบัติการรักษาความปลอดภัยข้อมูลสารสนเทศในปัจจุบัน

ประเภท	เลือกตัวแทน	การรักษาความปลอดภัยในปัจจุบัน
1. ระบบโครงสร้างพื้นฐานศูนย์ปฏิบัติการเครือข่าย	ระบบสำรองไฟฟ้า	■ ระบบสำรองไฟฟ้าอยู่ได้นาน 40 นาที ■ ระบบป้องกันไฟฟ้ากระชาก ■ ระบบแจ้งเตือนผ่าน SMS ■ มีการต่อสายไฟฟ้าจากเครื่องกำเนิดไฟฟ้าของอาคาร

ตารางที่ 4.6 (ต่อ)

ประเภท	เลือกตัวแทน	การรักษาความปลอดภัยในปัจจุบัน
1. ระบบโครงสร้างพื้นฐานศูนย์ปฏิบัติการเครือข่าย (ต่อ)	ระบบสำรองไฟฟ้า	■ กรณีไฟฟ้าดับเกินกว่ากำหนด ให้แจ้งเจ้าของระบบดำเนินการปิดระบบ หรือปิดระบบล่วงหน้ากรณีทราบแผนการบำรุงรักษา ■ มีการต่อสัญญา MA เพื่อบำรุงรักษาระบบไฟฟ้าทุกปี ■ กำหนดผู้รับผิดชอบในการเฝ้าระวังกรณีมีการบำรุงรักษาระบบไฟฟ้าอาคารหรือห้องศูนย์ปฏิบัติการเครือข่าย ■ กำหนดผู้รับผิดชอบในการเข้าแก้ไขเมื่อเกิดไฟฟ้าดับกรณีฉุกเฉิน ■ จัดให้มีเวรผู้ทำหน้าที่เฝ้าระวังจำนวน 2 คน โดยใช้เจ้าหน้าที่ส่วนระบบเครือข่ายทั้งหมด ■ บันทึกรายชื่อเจ้าของระบบพร้อมหมายเลขโทรศัพท์ติดต่อกรณีเกิดเหตุขัดข้องกับอุปกรณ์และระบบ เพื่อทราบขั้นตอนดำเนินการ
2. ระบบบริหารจัดการเครือข่าย	ไฟร์วอล	■ ใช้รหัสผ่านระดับ root ขนาด 16 ตัวอักษร ■ ตรวจสอบ log โดยผู้ดูแลระบบทุกวัน ■ ทบทวน Policy ทุก 1 ปี หรือเมื่อมีหน่วยงานศาลเปิดใหม่ ■ กรณีเกิดความผิดปกติของระบบ หรือมีกรณีการตัดสินคดีความที่อาจเป็นสาเหตุให้ตกเป็นเป้าโจมตี จะมีการเฝ้าระวังเพิ่มขึ้น ■ กำหนดอายุรับประกัน 5 ปี ซึ่งจะรวมการอัพเดต Firmware, License และ Signature ต่าง ๆ ■ กำหนดผู้ดูแลระบบ 2 คน

ตารางที่ 4.6 (ต่อ)

ประเภท	เลือกตัวแทน	การรักษาความปลอดภัยในปัจจุบัน
2. ระบบบริหารจัดการเครือข่าย (ต่อ)	ไฟร์วอล	■ กำหนดขั้นตอนเตรียมความพร้อมกรณีอุปกรณ์หยุดการทำงาน หรือชำรุดขัดข้อง ■ เปิดให้สามารถรีโมทควบคุมได้เฉพาะเจ้าหน้าที่ส่วนระบบเครือข่าย ■ เปิดให้ควบคุมผ่าน VPN ได้เฉพาะเจ้าของระบบ ■ มีการต่อสัญญา MA เพื่อบำรุงรักษาระบบไฟฟ้าทุกปี ■ กำหนดผู้รับผิดชอบในการเฝ้าระวังกรณีมีการบำรุงรักษาระบบไฟฟ้าอาคารหรือห้องศูนย์ปฏิบัติการเครือข่าย ■ กำหนดผู้รับผิดชอบในการเข้าแก้ไขเมื่อเกิดไฟฟ้าดับกรณีฉุกเฉิน ■ จัดให้มีเวรผู้ทำหน้าที่เฝ้าระวังจำนวน 2 คน โดยใช้เจ้าหน้าที่ส่วนระบบเครือข่ายทั้งหมด ■ บันทึกรายชื่อเจ้าของระบบพร้อมหมายเลขโทรศัพท์ติดต่อกรณีเกิดเหตุขัดข้องกับอุปกรณ์และระบบ เพื่อทราบขั้นตอนดำเนินการ ■ ใช้รหัสผ่านระดับ root ขนาด 16 ตัวอักษร ■ ตรวจสอบ log โดยผู้ดูแลระบบทุกวัน ■ ทบทวน Policy ทุก 1 ปี หรือเมื่อมีหน่วยงานศาลเปิดใหม่ ■ กรณีเกิดความผิดปกติของระบบ หรือมีกรณีการตัดสินคดีความที่อาจเป็นสาเหตุให้ตกเป็นเป้าโจมตี จะมีการเฝ้าระวังเพิ่มขึ้น ■ กำหนดอายุรับประกัน 5 ปี ซึ่งจะรวมการอัพเดต Firmware, License และ Signature ต่าง ๆ

ตารางที่ 4.6 (ต่อ)

ประเภท	เลือกตัวแทน	การรักษาความปลอดภัยในปัจจุบัน
2. ระบบบริหารจัดการเครือข่าย (ต่อ)	ไฟร์วอล	■ กำหนดผู้ดูแลระบบ 2 คน ■ กำหนดขั้นตอนเตรียมความพร้อมกรณีอุปกรณ์หยุดการทำงาน หรือชำรุดขัดข้อง ■ เปิดให้สามารถรีโมทควบคุมได้เฉพาะเจ้าหน้าที่ส่วนระบบเครือข่าย เปิดให้ควบคุมผ่าน VPN ได้เฉพาะเจ้าของระบบ
3. ระบบงานที่ให้บริการเฉพาะเครือข่ายภายใน	ระบบสารบรรณอิเล็กทรอนิกส์	■ เข้าใช้งานได้เฉพาะเครือข่ายภายใน (Intranet) ■ ใช้รหัสผ่าน ขนาด 8 ตัวอักษร ■ กำหนดสิทธิ์นายทะเบียนและระดับชั้นความลับเอกสารได้ ■ ช่องกรอกข้อมูลทุกช่องมีการตรวจสอบ Null ■ ป้องกันการใส่อักขระพิเศษในช่องกรอกข้อความ ■ กำหนดระยะเวลาสิ้นสุด Session และออกจากระบบเมื่อไม่มีการใช้งาน ในเวลา 3 นาที ■ จัดทำข้อมูลสำรองทุก 1 เดือน ■ กำหนดผู้ดูแลระบบ 1 คน ■ กำหนดขั้นตอนเตรียมความพร้อมกรณีอุปกรณ์หยุดการทำงาน หรือชำรุดขัดข้อง ■ เปิดให้สามารถรีโมทควบคุมได้เฉพาะเจ้าหน้าที่ส่วนระบบงานคอมพิวเตอร์ ■ เปิดให้ควบคุมผ่าน VPN ได้เฉพาะเจ้าของระบบ

ตารางที่ 4.6 (ต่อ)

ประเภท	เลือกตัวแทน	การรักษาความปลอดภัยในปัจจุบัน
4. ระบบงานที่ให้บริการเครือข่ายภายนอก	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์ (E - filling)	■ เข้าใช้งานผ่านเครือข่ายอินเทอร์เน็ต ■ การสมัครตรวจสอบหมายเลขบัตรประจำตัวประชาชนด้วยอัลกอริทึ่มตรวจสอบว่าไม่ใช่เลขสุ่ม ■ ใช้รหัสผ่าน OTP ขนาด 6 ตัวอักษร ■ กำหนดให้เปลี่ยนรหัสเข้าระบบภายหลังล๊อกอินเข้าใช้งานครั้งแรก ■ ป้องกันการใส่อักขระพิเศษในช่องกรอกข้อความ ■ ป้องกันการโจมตีผ่าน Browser ■ จัดทำข้อมูลสำรองทุก 1 วัน ■ กำหนดผู้ดูแลระบบ 2 คน ■ กำหนดขั้นตอนเตรียมความพร้อมกรณีอุปกรณ์หยุดการทำงาน หรือชำรุดขัดข้อง ■ เข้าใช้งานผ่านเครือข่ายอินเทอร์เน็ต ■ การสมัครตรวจสอบหมายเลขบัตรประจำตัวประชาชนด้วยอัลกอริทึ่มตรวจสอบว่าไม่ใช่เลขสุ่ม ■ ใช้รหัสผ่าน OTP ขนาด 6 ตัวอักษร ■ กำหนดให้เปลี่ยนรหัสเข้าระบบภายหลังล๊อกอินเข้าใช้งานครั้งแรก ■ ป้องกันการใส่อักขระพิเศษในช่องกรอกข้อความ ■ ป้องกันการโจมตีผ่าน Browser ■ จัดทำข้อมูลสำรองทุก 1 วัน ■ กำหนดผู้ดูแลระบบ 2 คน ■ กำหนดขั้นตอนเตรียมความพร้อมกรณีอุปกรณ์หยุดการทำงาน หรือชำรุดขัดข้อง

ตารางที่ 4.6 (ต่อ)

ประเภท	เลือกตัวแทน	การรักษาความปลอดภัยในปัจจุบัน
4. ระบบงานที่ให้บริการเครือข่ายภายนอก (ต่อ)	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์ (E - filling)	■ เปิดให้สามารถรีโมทควบคุมได้เฉพาะเจ้าหน้าที่ส่วนระบบงานคอมพิวเตอร์ ■ เปิดให้ควบคุมผ่าน VPN ได้เฉพาะเจ้าของระบบ
5. ระบบงานที่ใช้บริการหน่วยงานภายนอก	ระบบจดหมายอิเล็กทรอนิกส์ (e - Mail)	■ ใช้บริการอีเมล์ของ mail.go.th ตามมติคณะรัฐมนตรี ■ ใช้งานผ่าน https:// ■ กำหนดให้ผู้ใช้ต้องกำหนดรหัสใหม่ในการล๊อกอินครั้งแรก ■ กำหนดรหัสอย่างน้อย 8 ตัวอักษร และรหัสต้องประกอบด้วยตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ ■ สามารถกำหนดการกรอง Spam โดยผู้ใช้ ■ เมื่อมีบัญชีผู้ใช้ทำงานผิดปกติจะถูก Block การทำงานและแจ้งผู้ดูแลระบบของหน่วยงานทางอีเมล์ ■ เมื่อไม่มีการล๊อกอินเข้างานเกินกว่า 1 ปี บัญชีผู้ใช้จะถูกลบออกจากระบบ (ในระเบียบกำหนด 6 เดือน แต่การทำงานจริงให้เวลา 1 ปี) ■ กรณีลืมรหัสผ่านให้สมัครใหม่ผ่านระบบ ■ กำหนดผู้ดูแลระบบเพื่อให้บริการผู้ใช้ของหน่วยงานจำนวน 3 คน (เพิ่ม แก้ไข ลบ จัดกลุ่ม จัดทำรายงาน) ■ กำหนดขั้นตอนเตรียมความพร้อมกรณีอุปกรณ์หยุดการทำงาน หรือชำรุดขัดข้อง ■ กำหนดระดับการเข้าถึงหน้าจอผู้ดูแลระบบเฉพาะเจ้าของระบบ

ตารางที่ 4.6 (ต่อ)

ประเภท	เลือกตัวแทน	การรักษาความปลอดภัยในปัจจุบัน
6. ระบบงานที่ให้บริการเฉพาะ	ระบบสื่อสารทางไกลผ่านจอภาพ (Video Conference)	■ ติดตั้งให้บริการระบบที่ศูนย์ปฏิบัติการเครือข่าย โดยไม่ใช้บริการประชุมทางไกลของหน่วยงานภายนอก (ปัจจุบันยกเว้นให้ใช้ระบบใดก็ได้เพื่อทำงานระหว่างหน่วยงานภายในและหน่วยงานภายนอก) ■ กำหนดให้เปิดการเข้าถึงผ่าน Public IP ระหว่างเวลา 07.00 น. – 17.00 น. ตั้งแต่ พ.ศ. 2558 ■ การเข้าถึงระบบเพื่อควบคุมผ่าน https:// ■ แบ่งระดับผู้ดูแลระบบเป็นหลายระดับ ■ ติดตั้งอุปกรณ์ 2 unit สามารถทำงานต่อเนื่องเมื่อชำรุด ■ จัดเก็บการค่า Configure เพื่อการกู้คืนระบบ ■ จัดให้มีผู้ดูแลระบบจำนวน 4 คน ■ กำหนดขั้นตอนเตรียมความพร้อมกรณีอุปกรณ์หยุดการทำงาน หรือชำรุดขัดข้อง ■ เปิดให้สามารถรีโมทควบคุมได้เฉพาะเจ้าหน้าที่ส่วนระบบเครือข่ายคอมพิวเตอร์ ■ ให้มีการเข้าควบคุมระบบผ่านทางการรีโมทเข้ามายังเครื่องคอมพิวเตอร์ส่วนบุคคลภายในส่วนระบบเครือข่าย ไม่มีการเปิด VPN สำหรับระบบดังกล่าว
7. เว็บไซต์ของหน่วยงาน	เว็บไซต์สำนักงานศาลยุติธรรม	■ การเข้าใช้งานเว็บไซต์ผ่าน ThaiCert ■ จัดจ้างบริษัทเพื่อพัฒนาและดูแลเว็บไซต์โดยเฉพาะ ■ มีการตรวจสอบความผิดปกติของหน้าเว็บไซต์ ■ มีการสำรองข้อมูลเว็บไซต์ทุกวัน ■ จัดให้มีผู้ดูแลระบบจำนวน 2 คน

ตารางที่ 4.6 (ต่อ)

ประเภท	เลือกตัวแทน	การรักษาความปลอดภัยในปัจจุบัน
7. เว็บไซต์ของหน่วยงาน (ต่อ)	เว็บไซต์สำนักงานศาลยุติธรรม	■ กำหนดขั้นตอนเตรียมความพร้อมกรณีอุปกรณ์หยุดทำงาน หรือชำรุดขัดข้อง ■ เปิดให้สามารถรีโมทควบคุมได้เฉพาะเจ้าหน้าที่ส่วนระบบเครือข่ายและบริษัทผู้รับจ้างพัฒนาเว็บไซต์ ■ เปิดให้ควบคุมผ่าน VPN ได้เฉพาะเจ้าของระบบ ■ ป้องกันการโจมตีผ่านทาง Browser

4.2.1.2 เตรียมขั้นตอนประเมินความเสี่ยงสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภท เพื่อให้สามารถนำข้อมูลในกระบวนการไปใช้กับอุปกรณ์ และระบบที่มีคุณสมบัติ ลักษณะการทำงาน และการกำหนดนโยบายรักษาความปลอดภัยคล้ายคลึงหรือเหมือนกัน

1. กำหนดรูปแบบ และวิธีการประเมินความเสี่ยง

การประเมินความเสี่ยงกำหนดวิธีการแบบเมตริกซ์ ด้วยการแทนค่าโอกาส และผลกระทบที่เกิดขึ้นกับอุปกรณ์และระบบ โดยใช้การประเมินเชิงคุณภาพ

ตารางที่ 4.7 โอกาสที่จะเกิดการโจมตี (เชิงปริมาณ)

ระดับโอกาสเกิดความเสี่ยง	โอกาส/ความถี่	คะแนน
สูงมาก	เกิดเป็นประจำ อย่างน้อยเดือนละ 1 ครั้ง	5
สูง	ค่อนข้างบ่อย ปีละ 6 – 10 ครั้ง	4
ปานกลาง	ปานกลาง ปีละ 3 – 5 ครั้ง	3
น้อย	โอกาสเกิดน้อยหรืออย่างมากไม่เกินปีละ 2 ครั้ง	2
น้อยมาก	แทบจะไม่เกิดหรืออย่างมากปีละ 1 ครั้ง	1

ตารางที่ 4.8 โอกาสที่จะเกิดการโจมตี (เชิงคุณภาพ)

สูงมาก (5)	สูง (4)	ปานกลาง (3)	น้อย (2)	น้อยที่สุด (1)
มีโอกาสเกิดขึ้นทุกวัน	เกิดขึ้นทุกเดือน	เกิดขึ้นทุกปี	เกิดขึ้น 2 ปี/ครั้ง	ไม่เคยเกิดขึ้น
ไม่มีการให้ความรู้หรือไม่มีการกำหนดแนวทาง/ข้อปฏิบัติ	มีการให้ความรู้และจัดทำแนวทางปฏิบัติ/ข้อปฏิบัติแก่ผู้ใช้และเจ้าหน้าที่ใหม่	มีการให้ความรู้และจัดทำแนวทางปฏิบัติ/ข้อปฏิบัติแก่ผู้ใช้และเจ้าหน้าที่	มีการให้ความรู้และจัดทำแนวทางปฏิบัติ/แก่ผู้ใช้ และเจ้าหน้าที่ รวมถึงติดตามผลทุกปี	มีการให้ความรู้และจัดทำแนวทางปฏิบัติ/แก่ผู้ใช้ และเจ้าหน้าที่ รวมถึงติดตามผลทุก 3 เดือน

ตารางที่ 4.9 ระดับผลกระทบที่เกิดจากการโจมตี

ระดับผลกระทบ	ระดับคะแนน	รายละเอียด
สูงมาก	5	■ กระทบต่อกระบวนการทำงานทั้งองค์กรหรือบางส่วนเป็นระยะเวลามากกว่า 6 ชั่วโมง ขึ้นไป ■ มูลค่าความเสียหายมากกว่าหรือเท่ากับ 3 แสนบาท ■ กระทบต่อชื่อเสียง และความน่าเชื่อถืออย่างมากทำให้เกิดการต่อต้านต่อสาธารณะ เช่น การชุมนุมประท้วง ■ มีความเกี่ยวข้องกับกฎหมายในแต่ละประเทศ
สูง	4	■ กระทบต่อกระบวนการทำงานทั้งองค์กรหรือบางส่วนเป็นระยะเวลาไม่เกิน 6 ชั่วโมง ■ มูลค่าความเสียหายน้อยกว่า 3 แสนบาท. ■ มีความเกี่ยวข้องกับสัญญากับคู่ค้า หรือลูกค้า

ตารางที่ 4.9 (ต่อ)

ระดับผลกระทบ	ระดับคะแนน	รายละเอียด
สูง (ต่อ)	4	■ กระทบต่อชื่อเสียง และความน่าเชื่อถืออย่างมากทำให้เกิดการคัดค้านต่อสาธารณะ เช่น การเผยแพร่ทางอินเทอร์เน็ตหรือหนังสือพิมพ์
ปานกลาง	3	■ กระทบต่อกระบวนการทำงานทั้งองค์กรหรือบางส่วนเป็นระยะเวลาไม่เกิน 3 ชั่วโมง ขึ้นไป ■ มูลค่าความเสียหายมากกว่าหรือเท่ากับ 1 แสนบาท ■ กระทบต่อชื่อเสียงและความน่าเชื่อถือปานกลางทำให้เกิดการวิจารณ์จากสื่อสาธารณะ เช่น การเผยแพร่ทางอินเทอร์เน็ตหรือหนังสือพิมพ์ ■ มีความเกี่ยวข้องกับข้อบังคับท้องถิ่น หรือข้อตกลงทั่วไป
ต่ำ	2	■ กระทบต่อกระบวนการทำงานทั้งองค์กรหรือบางส่วนเป็นระยะเวลาไม่เกิน 1 ชั่วโมง ■ มูลค่าความเสียหายน้อยกว่า 5 หมื่นบาท ■ กระทบต่อชื่อเสียงและความน่าเชื่อถือ เช่น การร้องเรียน ■ มีความเกี่ยวข้องกับกฎหมายในแต่ละประเทศ
ต่ำมาก	1	■ กระทบต่อกระบวนการทำงานทั้งองค์กรหรือบางส่วนเป็นระยะเวลาไม่เกิน 30 นาที ■ มูลค่าความเสียหายน้อยกว่า 1 หมื่นบาท ■ ไม่กระทบต่อชื่อเสียงและความน่าเชื่อถือ ■ ไม่มีความเกี่ยวข้องกับกฎหมายหรือข้อตกลงใด ๆ

ตารางที่ 4.10 ระดับสีเพื่อระบุคะแนนความเสี่ยง

ระดับ	ความหมาย
สีเขียว	ระดับความเสี่ยงที่องค์กรยอมรับ อาจมีมาตรการป้องกันหรือไม่ก็ได้
สีเหลือง	ระดับความเสี่ยงที่องค์กรยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงมีค่าสูงขึ้นไปยังระดับที่ไม่สามารถยอมรับได้
สีส้ม	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้
สีแดง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และจำเป็นต้องเร่งจัดการความเสี่ยงจนกระทั่งอยู่ในระดับที่สามารถยอมรับได้ในทันที

ตารางที่ 4.11 ความเสี่ยง และความสัมพันธ์ของผลกระทบและโอกาสที่จะเกิดความเสี่ยง

ผลกระทบ						
	สูงมาก	5	10	15	20	25
	สูง	4	8	12	15	16
	ปานกลาง	3	6	9	12	15
	น้อย	2	4	6	8	10
	น้อยมาก	1	2	3	4	5
		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
		โอกาส				

2. ระบุความเสี่ยงที่มีผลต่อข้อมูลสารสนเทศในขอบเขตที่เกี่ยวข้อง

ตารางที่ 4.12 รายการความเสี่ยงที่มีผลกระทบต่ออุปกรณ์และระบบในห้องศูนย์ฯ

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ภัยธรรมชาติ : Natural Disaster							
ไฟไหม้	✓	✓	✓	✓		✓	✓
น้ำท่วม	✓	✓	✓	✓		✓	✓
แผ่นดินไหว	✓	✓	✓	✓		✓	✓
ลมพายุ	✓	✓	✓	✓		✓	✓
ฟ้าผ่า	✓	✓	✓	✓		✓	✓
โครงสร้างพื้นฐานห้องศูนย์ปฏิบัติการฯ : Information Infrastructure							
ระบบสำรองไฟฟ้า	✓	✓	✓	✓		✓	✓
ไฟฟ้าดับจากการบำรุงรักษาไฟฟ้าอาคาร	✓	✓	✓	✓		✓	✓
ไฟฟ้าดับฉุกเฉิน	✓	✓	✓	✓		✓	✓
ไฟกระชาก	✓	✓	✓	✓		✓	✓
เครื่องกำเนิดไฟฟ้าไม่มีความพร้อมใช้งาน	✓	✓	✓	✓		✓	✓
ระบบควบคุมกระแสไฟฟ้าขัดข้อง	✓	✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากเสื่อมสภาพ ชำรุด	✓	✓	✓	✓		✓	✓
กำลังไฟฟ้าไม่เพียงพอติดตั้งอุปกรณ์	✓	✓	✓	✓		✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ระบบปรับอากาศ		✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ		✓	✓	✓		✓	✓
ระบบปล่อยลมเย็นชำรุด		✓	✓	✓		✓	✓
ระบบระบายความร้อนนอกอาคารชำรุด		✓	✓	✓		✓	✓
ระบบควบคุมระบบปรับอากาศชำรุด		✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากเสื่อมสภาพ ชำรุด		✓	✓	✓		✓	✓
ระบบไม่สามารถรักษาอุณหภูมิได้เนื่องจากอากาศภายนอกร้อนมากเกินไป		✓	✓	✓		✓	✓
ระบบล็อกประตูสแกนลายนิ้วมือ รหัสผ่าน หรือบัตรผ่าน	✓	✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ	✓	✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด	✓	✓	✓	✓		✓	✓
ไม่มีกระบวนการกำหนดสิทธิ์	✓	✓	✓	✓		✓	✓
การกำหนดสิทธิ์ไม่เหมาะสมเพียงพอ	✓	✓	✓	✓		✓	✓
ยกเว้นการดำเนินการตามกระบวนการกำหนดสิทธิ์	✓	✓	✓	✓		✓	✓
การกำหนดสิทธิ์ปัจจัยเดียว ด้วยรหัส หรือบัตร	✓	✓	✓	✓		✓	✓
ผู้มีสิทธิ์ตั้งรหัสผ่านที่เดาได้ง่าย	✓	✓	✓	✓		✓	✓
ผู้มีสิทธิ์ลืมรหัสผ่าน	✓	✓	✓	✓		✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
การใช้รหัส หรือบัตร ร่วมกัน	✓	✓	✓	✓		✓	✓
ผู้ไม่มีสิทธิ์นำรหัสหรือบัตรไปใช้เพื่อเข้าสู่พื้นที่	✓	✓	✓	✓		✓	✓
ไฟฟ้าดับประตูปิดอัตโนมัติ	✓	✓	✓	✓		✓	✓
ไฟฟ้าดับประตูเปิดอัตโนมัติ	✓	✓	✓	✓		✓	✓
แบตเตอรี่สำรองระบบควบคุมประตูใช้งานไม่ได้	✓	✓	✓	✓		✓	✓
ระบบตรวจจับควัน							
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ							
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด							
ระบบเตือนตรวจจับไม่ส่งเสียงเตือนเมื่อมีควัน							
ระบบตรวจจับความร้อน							
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ							
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด							
ระบบตรวจจับไม่ส่งเสียงเตือนเมื่อมีความร้อน							
ระบบตรวจจับน้ำรั่วซึม	✓	✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ	✓	✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด	✓	✓	✓	✓		✓	✓
สายเซ็นเซอร์ตรวจจับติดตั้งไม่ครอบคลุมทุกจุด	✓	✓	✓	✓		✓	✓
ระบบไม่แจ้งเตือนเนื่องจากสายเซ็นเซอร์ขาด	✓	✓	✓	✓		✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ระบบเตือนตรวจจับไม่ส่งเสียงเตือนเมื่อมีน้ำรั่วซึม	✓	✓	✓	✓		✓	✓
ระบบพ่นสารดับเพลิง	✓	✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ	✓	✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด	✓	✓	✓	✓		✓	✓
ระบบตรวจจับพ่นสารดับเพลิงเมื่อไม่มีไฟไหม้	✓	✓	✓	✓		✓	✓
ระบบตรวจจับไม่พ่นสารดับเพลิงเมื่อมีไฟไหม้	✓	✓	✓	✓		✓	✓
ระบบพ่นสารดับเพลิงขณะมีการปฏิบัติงานอยู่ภายใน	✓	✓	✓	✓		✓	✓
ระบบตรวจจับความเคลื่อนไหวและบันทึก							
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ							
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด							
ระบบตรวจจับไม่บันทึกเมื่อมีการเคลื่อนไหว							
ผู้ดูแลระบบเข้าสู่ระบบไม่ได้จากความขัดข้อง							
ผู้ดูแลระบบลืมรหัสผ่าน							
ผู้ไม่มีสิทธิ์เข้าถึงระบบจากการรั่วไหลของรหัส							
ไฟล์ภาพเคลื่อนไหวและบันทึกเสียหาย							
ระบบแจ้งเตือนทางอีเมล์และ SMS	✓						
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ	✓						
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด	✓						

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ฮาร์ดแวร์ : Hardware							
ระบบตรวจจับไม่ส่งข้อความ SMS เมื่อมีเหตุการณ์	✓						
ผู้ดูแลระบบเข้าสู่ระบบไม่ได้จากความขัดข้อง	✓						
ผู้ดูแลระบบลืมรหัสผ่าน	✓						
ผู้ไม่มีสิทธิ์เข้าถึงระบบจากการรั่วไหลของรหัส	✓						
ซิมโทรศัพท์ไม่มีเงินทำให้ไม่ทำงาน	✓						
Rack Server		✓	✓	✓		✓	✓
ฮาร์ดแวร์ไม่ทำงานเนื่องจากไฟฟ้าดับ		✓	✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด		✓	✓	✓		✓	✓
ฮาร์ดแวร์ไม่เหมาะกับการใช้งาน เช่น RAM ไม่พอ			✓	✓			
ฮาร์ดแวร์เฉพาะไม่สามารถแก้ไขซ่อมแซมเองได้		✓	✓	✓		✓	✓
ฮาร์ดแวร์มีประวัติการชำรุด		✓	✓	✓		✓	✓
ไม่มีการกำหนดสิทธิ์ให้ผู้ดูแลระบบในระดับต่างกัน		✓	✓	✓		✓	✓
กำหนดสิทธิ์ผู้ดูแลระบบแต่ละระดับไม่เหมาะสม		✓	✓	✓		✓	✓
ผู้ดูแลระบบตั้งรหัสผ่านเดาได้ง่าย		✓	✓	✓		✓	✓
ผู้ดูแลระบบลืมรหัสผ่าน		✓	✓	✓		✓	✓
บัญชีผู้ใช้เริ่มต้นของอุปกรณ์ (Default User)		✓	✓	✓		✓	✓
บัญชีผู้ใช้งานผู้ดูแลระบบรั่วไหล		✓	✓	✓		✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ช่องโหว่ของฮาร์ดแวร์แต่ละรุ่น		✓	✓	✓		✓	✓
IBM				✓			
HP			✓			✓	✓
DELL							
CISCO		✓				✓	
Desktop Server							
DELL							
ECT	✓						
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด	✓						
ฮาร์ดแวร์มีประวัติการชำรุด	✓						
Storage			✓	✓		✓	✓
ฮาร์ดแวร์ไม่ทำงานเนื่องจากไฟฟ้าดับ			✓	✓		✓	✓
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด			✓	✓		✓	✓
ฮาร์ดแวร์ไม่เหมาะกับการใช้งาน เช่น พื้นที่บันทึกข้อมูลไม่เพียงพอ			✓	✓		✓	✓
ฮาร์ดแวร์เฉพาะไม่สามารถแก้ไขซ่อมแซมเองได้			✓	✓		✓	✓
ฮาร์ดแวร์มีประวัติการชำรุด			✓	✓		✓	✓
ไม่มีการกำหนดสิทธิ์ให้ผู้ดูแลระบบในระดับต่างกัน			✓	✓		✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
กำหนดสิทธิ์ผู้ดูแลระบบแต่ละระดับไม่เหมาะสม			✓	✓		✓	✓
ผู้ดูแลระบบตั้งรหัสผ่านเดาได้ง่าย			✓	✓		✓	✓
ผู้ดูแลระบบลืมรหัสผ่าน			✓	✓		✓	✓
บัญชีผู้ใช้เริ่มต้นของอุปกรณ์ (Default User)			✓	✓		✓	✓
บัญชีผู้ใช้งานผู้ดูแลระบบรั่วไหล			✓	✓		✓	✓
ช่องโหว่ของฮาร์ดแวร์แต่ละรุ่น			✓	✓		✓	✓
Fiber Optic Cable		✓	✓	✓	✓	✓	✓
สายขาด สายชำรุด ระหว่างทางจากผู้ให้บริการ		✓	✓	✓	✓	✓	✓
สายขาด สายชำรุด ภายในห้องศูนย์ปฏิบัติการ		✓	✓	✓	✓	✓	✓
การเสียบสายเชื่อมต่อ ไม่ถูกต้อง ไม่สมบูรณ์		✓	✓	✓	✓	✓	✓
RJ45 Cable		✓	✓	✓		✓	✓
สายขาด สายชำรุด		✓	✓	✓		✓	✓
การเชื่อมต่อ ไม่ถูกต้อง ไม่สมบูรณ์		✓	✓	✓		✓	✓
Rack		✓	✓	✓		✓	✓
พัดลมระบายความร้อนไม่ทำงานเนื่องจากไฟฟ้าดับ		✓	✓	✓		✓	✓
พัดลมไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด		✓	✓	✓		✓	✓
ประตูตู้ไม่สามารถล็อกได้ เช่น ล็อกชำรุด กุญแจหัก		✓	✓	✓		✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ประตูตู้เปิดล๊อกไม่ได้ เช่น กุยแจหาย ล๊อกค้าง		✓	✓	✓		✓	✓
PDU (Power Distribute Unit)		✓	✓	✓		✓	✓
ปลั๊กไฟฟ้าไม่ทำงานเนื่องจากไฟฟ้าดับ		✓	✓	✓		✓	✓
ปลั๊กไฟฟ้าไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด		✓	✓	✓		✓	✓
การชำรุดของปลั๊กบางส่วนในราง		✓	✓	✓		✓	✓
ฟิวส์ภายในปลั๊กรางขาดทำให้ปลั๊กไม่จ่ายไฟ		✓	✓	✓		✓	✓
Power Plug		✓	✓	✓		✓	✓
ปลั๊กไฟฟ้าไม่ทำงานเนื่องจากไฟฟ้าดับ		✓	✓	✓		✓	✓
ปลั๊กไฟฟ้าไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด		✓	✓	✓		✓	✓
การติดตั้งปลั๊กหลวมหลุด		✓	✓	✓		✓	✓
ซอฟต์แวร์ : Software							
ระบบปฏิบัติการ : Operating System		✓	✓	✓		✓	✓
ซอฟต์แวร์ไม่ทำงานเนื่องจากปัญหาระบบไฟฟ้า		✓	✓	✓		✓	✓
ซอฟต์แวร์ไม่ทำงานเนื่องจากชำรุดที่ไม่ทราบสาเหตุ		✓	✓	✓		✓	✓
ไม่มีการกำหนดสิทธิ์ให้ผู้ดูแลระบบในระดับต่างกัน		✓	✓	✓		✓	✓
กำหนดสิทธิ์ผู้ดูแลระบบแต่ละระดับไม่เหมาะสม		✓	✓	✓		✓	✓
ผู้ดูแลระบบตั้งรหัสผ่านเดาได้ง่าย		✓	✓	✓		✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ผู้ดูแลระบบลืมรหัสผ่าน		✓	✓	✓		✓	✓
บัญชีผู้ใช้เริ่มต้นของระบบปฏิบัติการ (Default User)		✓	✓	✓		✓	✓
ผู้ไม่มีสิทธิ์สามารถเข้าถึงระบบเนื่องจากรหัสรั่วไหล		✓	✓	✓		✓	✓
การบริหารจัดการกำหนดสิทธิ์ไม่ถูกต้องเหมาะสม		✓	✓	✓		✓	✓
การเข้าถึงระบบด้วยความสัมพันธ์ที่เชื่อถือระหว่างระบบโดยไม่มีการยืนยันหรือกำหนดสิทธิ์อีกครั้ง		✓	✓	✓		✓	✓
ขาดการตรวจสอบการใช้งาน Job Schedule		✓	✓	✓		✓	✓
ผู้ไม่มีสิทธิ์สามารถเข้าถึง File System		✓	✓	✓		✓	✓
ผู้ไม่มีสิทธิ์สามารถเข้าถึง File และ Directory		✓	✓	✓		✓	✓
ขาดการอัพเดทซอฟต์แวร์		✓	✓	✓		✓	✓
ไม่มีระบบสำรองข้อมูล		✓	✓	✓		✓	✓
ไม่มีกระบวนการกู้คืนระบบที่เหมาะสม		✓	✓	✓		✓	✓
ไม่มีการติดตั้งโปรแกรมป้องกันไวรัสหรือมัลแวร์		✓	✓	✓		✓	✓
ช่องโหว่ของระบบปฏิบัติการแต่ละรุ่น		✓	✓	✓		✓	✓
Windows			✓			✓	✓
Linux		✓				✓	
VM (Virtual Machine)				✓		✓	
ETC							

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ระบบงาน : Application			✓	✓			✓
ซอฟต์แวร์ไม่ทำงานเนื่องจากปัญหาระบบไฟฟ้า			✓	✓			✓
ซอฟต์แวร์ไม่ทำงานเนื่องจากชำรุดที่ไม่ทราบสาเหตุ			✓	✓			✓
ไม่มีการกำหนดสิทธิ์ให้ผู้ดูแลระบบในระดับต่างกัน			✓	✓			✓
กำหนดสิทธิ์ผู้ดูแลระบบแต่ละระดับไม่เหมาะสม			✓	✓			✓
ผู้ดูแลระบบตั้งรหัสผ่านเดาได้ง่าย			✓	✓			✓
ผู้ดูแลระบบลืมรหัสผ่าน			✓	✓			✓
บัญชีผู้ใช้เริ่มต้นของระบบงาน (Default User)			✓	✓			✓
ผู้ไม่มีสิทธิ์สามารถเข้าถึงระบบเนื่องจากรหัสรั่วไหล			✓	✓			✓
การบริหารจัดการกำหนดสิทธิ์ไม่ถูกต้องเหมาะสม			✓	✓			✓
การเข้าถึงระบบด้วยความสัมพันธ์ที่เชื่อถือระหว่างระบบ โดยไม่มีการยืนยันหรือกำหนดสิทธิ์อีกครั้ง			✓	✓			✓
ขาดการตรวจสอบการใช้งาน Job Schedule			✓	✓			✓
ขาดการอัพเดทซอฟต์แวร์			✓	✓			✓
ไม่มีระบบสำรองข้อมูล			✓	✓			✓
ไม่มีกระบวนการกู้คืนระบบที่เหมาะสม			✓	✓			✓
ไม่มีการเข้ารหัสการส่งรหัสผ่าน			✓	✓			✓
ไม่มีการเข้ารหัสการส่งข้อมูล			✓	✓			✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ไม่กำหนดความยาวของการรับ Input			✓	✓			✓
ไม่กำหนด Input Validation			✓	✓			✓
ไม่มีการกำหนดเวลาทำงาน Session			✓	✓			✓
ใช้งาน Client Cookies			✓	✓			✓
ขาดการควบคุมการเปลี่ยนแปลง Application			✓	✓			✓
เปิดการเรียกใช้ SQL จาก Address Bar			✓	✓			✓
ช่องโหว่ SQL Injection			✓	✓			✓
ช่องโหว่ LDAP Injection			✓	✓			✓
ขาดการรักษาความปลอดภัยในระดับ Application			✓	✓			✓
ช่องโหว่ของ Development Tool แต่ละรุ่น			✓	✓			✓
.NET			✓	✓			
JAVA							✓
MS Access							
ข้อมูลที่เข้าถึงอาจขัดต่อกฎหมาย โดยเฉพาะ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562			✓	✓			✓
ระบบฐานข้อมูล : Database			✓	✓		✓	✓
ซอฟต์แวร์ไม่ทำงานเนื่องจากปัญหาระบบไฟฟ้า			✓	✓		✓	✓
ซอฟต์แวร์ไม่ทำงานเนื่องจากชำรุดที่ไม่ทราบสาเหตุ			✓	✓		✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ไม่มีการกำหนดสิทธิ์ให้ผู้ดูแลระบบในระดับต่างกัน			✓	✓		✓	✓
กำหนดสิทธิ์ผู้ดูแลระบบแต่ละระดับไม่เหมาะสม			✓	✓		✓	✓
ผู้ดูแลระบบตั้งรหัสผ่านเดาได้ง่าย			✓	✓		✓	✓
ผู้ดูแลระบบลืมรหัสผ่าน			✓	✓		✓	✓
บัญชีผู้ใช้เริ่มต้นของอุปกรณ์ (Default User)			✓	✓		✓	✓
ผู้ไม่มีสิทธิ์สามารถเข้าถึงระบบเนื่องจากรหัสรั่วไหล			✓	✓		✓	✓
การบริหารจัดการกำหนดสิทธิ์ไม่ถูกต้องเหมาะสม			✓	✓		✓	✓
การเข้าถึงระบบด้วยความสัมพันธ์ที่เชื่อถือระหว่างระบบโดยไม่มีการยืนยันหรือกำหนดสิทธิ์อีกครั้ง			✓	✓		✓	✓
ขาดการตรวจสอบการใช้งาน Job Schedule			✓	✓		✓	✓
ขาดการอัพเดทซอฟต์แวร์			✓	✓		✓	✓
ไม่มีระบบสำรองข้อมูล			✓	✓		✓	✓
ไม่มีกระบวนการกู้คืนระบบที่เหมาะสม			✓	✓		✓	✓
ฐานข้อมูลซ้ำซ้อน			✓	✓		✓	✓
ฐานข้อมูลไม่สมบูรณ์			✓	✓		✓	✓
ช่องโหว่ของการใช้โปรแกรมประเภท phpMyAdmin				✓			
ช่องโหว่ของฐานข้อมูลแต่ละรุ่น		✓	✓	✓		✓	✓
MS Access							
My SQL				✓			✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
SQL Server							
Oracle			✓				
LDAP						✓	
etc		✓					
ข้อมูลที่เข้าถึงอาจขัดต่อกฎหมาย โดยเฉพาะ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562							
ระบบที่มีการทำงานเฉพาะ : Special Service						✓	
ระบบไม่ทำงานโดยไม่ทราบสาเหตุ						✓	
การทำงานของระบบด้วยซอฟต์แวร์และฮาร์ดแวร์หลายชุดเชื่อมต่อกัน การชำรุดของส่วนใดส่วนหนึ่งทำให้เกิดข้อขัดข้องการทำงานได้						✓	
การทำงานร่วมกันระหว่างหลายระบบต้องมีการแลกเปลี่ยนรหัสเพื่อยืนยันความเชื่อถือ กรณีรหัสหมดอายุทำให้ระบบไม่ทำงาน						✓	
ผู้ดูแลระบบไม่สามารถบริหารจัดการเชิงลึกได้ เช่น การตั้งค่าเชื่อมโยงระบบทั้งหมด						✓	
การออกแบบมีส่วนคอขวดที่สำคัญ เช่น ฐานข้อมูลผู้ใช้ เมื่อเสียหายระบบจะไม่สามารถทำงานได้ และระบบควบคุมกลางเมื่อชำรุดจะทำให้ระบบย่อยไม่สามารถทำงานร่วมกันได้						✓	

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
การอัพเดทซอฟต์แวร์ทำได้จำกัดผูกติดกับรุ่นของฮาร์ดแวร์						✓	
การทำงานของฟังก์ชั่นต่างๆ มีการเสียค่าใช้จ่าย License แยกเป็นระบบย่อย ทำให้ยากในการขยายระบบ หรือต้องการใช้คุณสมบัติอื่นที่มิได้วางแผนไว้ล่วงหน้า						✓	
ระบบงานเฉพาะมีการใช้ทรัพยากรจำนวนมาก โดยเฉพาะระบบที่ต้องการตอบสนอง Real Time						✓	
บริการระหว่างหน่วยงานพันธมิตร : Third Party Service					✓		
ระบบไม่สามารถใช้งานได้โดยไม่ทราบสาเหตุ					✓		
ระบบไม่สามารถใช้งานได้เนื่องจากการบำรุงรักษาตามระยะเวลาที่กำหนด					✓		
สิทธิ์ผู้ดูแลระบบของหน่วยงานศาลยุติธรรมเป็นระดับผู้ดูแลผู้ใช้ไม่สามารถบริหารจัดการได้					✓		
ผู้ดูแลระบบตั้งรหัสผ่านเดาได้ง่าย					✓		
ผู้ดูแลระบบลืมรหัสผ่าน					✓		
บัญชีผู้ใช้เริ่มต้นของระบบ (Default User)					✓		
ผู้ไม่มีสิทธิ์สามารถเข้าถึงระบบเนื่องจากรหัสรั่วไหล					✓		
ผู้ไม่มีสิทธิ์ทำการแก้ไขบัญชีผู้ใช้ถูก เพิ่ม แก้ไข ลบ					✓		

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ผู้ไม่มีสิทธิ์สามารถเข้าถึงบัญชีผู้ใช้จากการรั่วไหล					✓		
ผู้ไม่มีสิทธิ์เข้าใช้งานบัญชีผู้ใช้					✓		
ผู้ใช้ไม่มีการใช้งานต่อเนื่องเกินกำหนด					✓		
ผู้ใช้ถูกล๊อกระบบชั่วคราวเนื่องจากความผิดปกติ					✓		
ผู้ให้บริการเปลี่ยนแปลงนโยบายรักษาความปลอดภัยบนเครือข่าย หรือ IP โดยไม่แจ้งให้ทราบล่วงหน้า					✓		
ข้อตกลงแลกเปลี่ยนข้อมูลในรูปแบบ Web Service ไม่ชัดเจน เหมาะสม							
ข้อมูลที่เข้าถึงอาจขัดต่อกฎหมาย โดยเฉพาะ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562					✓		
บุคลากร : People ware							
ผู้ดูแลระบบหน่วยงานภายใน	✓	✓	✓	✓	✓	✓	✓
ขาดความรู้ความเข้าใจเชิงเทคนิคและนวัตกรรม	✓	✓	✓	✓	✓	✓	✓
ขาดการฝึกอบรม หรือการฝึกอบรมไม่เหมาะสม	✓	✓	✓	✓	✓	✓	✓
ขาดการถ่ายทอดความรู้	✓	✓	✓	✓	✓	✓	✓
ขาดการควบคุมการใช้สื่อพกพา	✓	✓	✓	✓	✓	✓	✓
ขาดความรู้ในการบำรุงรักษาอุปกรณ์ที่มีความเฉพาะ	✓	✓	✓	✓	✓	✓	✓
ขาดบุคลากรทำงานนอกเวลาราชการ	✓	✓	✓	✓	✓	✓	✓
ผู้ดูแลระบบหน่วยงานพันธมิตร					✓		

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
การแจ้งข้อขัดข้องและติดต่อใช้เวลานาน เนื่องจากให้บริการแก่หน่วยงานหลายแห่ง					✓		
เจ้าหน้าที่รับแจ้งเหตุอย่างเดียว ไม่สามารถให้คำตอบ หรือแก้ปัญหาได้ ต้องรอการประสานกลับอีกครั้ง					✓		
การตอบสนองล่าช้าเกินกว่า 3 ชั่วโมง					✓		
ผู้ดูแลระบบบริษัทผู้ให้บริการ	✓	✓	✓	✓		✓	✓
การแจ้งข้อขัดข้องและติดต่อใช้เวลานาน เนื่องจากให้บริการแก่หน่วยงานหลายแห่ง	✓	✓	✓	✓		✓	✓
ไม่ต่ออายุการบำรุงรักษาระบบ	✓	✓	✓	✓		✓	✓
การตอบสนองล่าช้าเกินกว่า 3 ชั่วโมง	✓	✓	✓	✓		✓	✓
การแก้ไขเปลี่ยนแทนล่าช้าเกินกว่า 24 ชั่วโมง	✓	✓	✓	✓		✓	✓
ผู้ใช้หน่วยงานศาลยุติธรรม			✓	✓	✓	✓	✓
ขาดการตระหนักรู้ด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ			✓	✓	✓	✓	✓
ขาดการฝึกอบรม หรือการฝึกอบรมไม่เหมาะสม			✓	✓	✓	✓	✓
ขาดการถ่ายทอดความรู้			✓	✓	✓	✓	✓
ขาดการควบคุมการใช้สื่อพกพา			✓	✓	✓	✓	✓
การใช้บัญชีผู้ใช้ร่วมกับผู้อื่น โดยเฉพาะระบบงานที่มีการใช้งานภายในหน่วยงาน และอีเมล์			✓	✓	✓	✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบตำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ข้อมูลที่เข้าถึงขัดต่อกฎหมาย พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562				✓	✓	✓	
ผู้ใช้หน่วยงานพันธมิตร				✓		✓	
ขาดเจ้าหน้าที่คอมพิวเตอร์ที่ปฏิบัติงานในพื้นที่มีเฉพาะส่วนกลาง				✓		✓	
ขาดการตระหนักรู้ด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ				✓		✓	
ขาดการฝึกอบรม หรือการฝึกอบรมไม่เหมาะสม				✓		✓	
ขาดการถ่ายทอดความรู้				✓		✓	
ขาดการควบคุมการใช้สื่อพกพา				✓		✓	
ไม่มีบุคลากรทำงานนอกเวลาราชการ				✓		✓	
ข้อมูลที่เข้าถึงขัดต่อกฎหมาย พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562				✓		✓	
ช่องโหว่ของหน่วยงานที่แตกต่างกัน				✓		✓	
สถานีตำรวจภูธร						✓	
เรือนจำ						✓	
ศูนย์ฝึกฯ						✓	
สถานพินิจฯ						✓	
ทัณฑสถานฯ						✓	
สำนักงานอัยการจังหวัด				✓		✓	

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ทนาย				✓		✓	
ผู้ใช้ทั่วไป				✓		✓	
ขาดการตระหนักรู้การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ				✓		✓	
กระบวนการ : Process							
ขาดการฝึกอบรม หรือการฝึกอบรมไม่เหมาะสม				✓		✓	
ขาดการถ่ายทอดความรู้				✓		✓	
ขาดการควบคุมการใช้สื่อพกพา				✓		✓	
การใช้บัญชีผู้ใช้ร่วมกับผู้อื่น				✓		✓	
ข้อมูลที่เข้าถึงขัดต่อกฎหมาย พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562				✓		✓	
การปฏิบัติงานภายในพื้นที่ห้องศูนย์ฯ	✓	✓	✓	✓	✓	✓	✓
กระบวนการควบคุมการเข้าออกไม่มีประสิทธิภาพเพียงพอ	✓	✓	✓	✓	✓	✓	✓
งดเว้นการดำเนินการตามกระบวนการควบคุม	✓	✓	✓	✓	✓	✓	✓
ผู้ไม่มีสิทธิ์เข้าสู่พื้นที่โดยไม่ได้รับอนุญาต	✓	✓	✓	✓	✓	✓	✓
การบันทึกงานที่ปฏิบัติภายในศูนย์ฯ ไม่ละเอียดเพียงพอ	✓	✓	✓	✓	✓	✓	✓
มีผู้เข้าปฏิบัติงานโดยไม่มีเจ้าหน้าที่เข้าควบคุม	✓	✓	✓	✓	✓	✓	✓
ผู้เข้าปฏิบัติงานในห้องศูนย์ฯ นำอุปกรณ์ เข้าติดตั้ง หรือนำออกโดยไม่ได้รับอนุญาต	✓	✓	✓	✓	✓	✓	✓
ผู้เข้าปฏิบัติงานในห้องศูนย์ฯ ทำการคัดลอกข้อมูล โดยไม่ได้รับอนุญาต	✓	✓	✓	✓	✓	✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ระบบไม่ทำงาน ขัดข้อง จากผู้เข้าปฏิบัติงาน เปลี่ยนแปลงการเชื่อมต่อสายสัญญาณ	✓	✓	✓	✓	✓	✓	✓
ระบบโครงสร้างพื้นฐานฯ ชำรุด เสียหาย จากผู้เข้าปฏิบัติงาน	✓	✓	✓	✓	✓	✓	✓
การกำหนดขอบเขตเครือข่าย	✓	✓	✓	✓	✓	✓	✓
ไม่มีการกำหนดขอบเขตเครือข่าย	✓	✓	✓	✓	✓	✓	✓
การกำหนดขอบเขตเครือข่ายที่เข้าถึงไม่เหมาะสม	✓	✓	✓	✓	✓	✓	✓
ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์และระบบที่จำกัดการเข้าถึงเป็นกรณีพิเศษ	✓	✓	✓	✓	✓	✓	✓
การเข้าถึงระบบที่ใช้งานเฉพาะเครือข่ายภายในจากเครือข่ายภายนอกได้	✓	✓	✓				✓
ระบบที่ต้องให้บริการจากเครือข่ายภายนอกขัดข้อง หรือไม่สามารถใช้งานได้ เมื่อใช้งานผ่านเครือข่ายภายใน		✓		✓	✓	✓	✓
การกำหนดเจ้าของระบบ	✓	✓	✓	✓	✓	✓	✓
ไม่มีการกำหนดเจ้าของระบบ	✓	✓	✓	✓	✓	✓	✓
กำหนดเจ้าของระบบไม่เหมาะสม ไม่สามารถตรวจสอบดูแลระบบได้	✓	✓	✓	✓	✓	✓	✓
เจ้าของระบบที่ได้รับการแต่งตั้งมีการโยกย้ายเปลี่ยนตำแหน่งหรือไม่สามารถปฏิบัติหน้าที่ได้	✓	✓	✓	✓	✓	✓	✓
กระบวนการยืนยันตัวตน	✓	✓	✓	✓	✓	✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ไม่มีกระบวนการยืนยันตัวตน	✓	✓	✓	✓	✓	✓	✓
กระบวนการยืนยันตัวตนไม่เหมาะสมเพียงพอ	✓	✓	✓	✓	✓	✓	✓
การกำหนดรหัสผ่านที่ง่ายในการเดา	✓	✓	✓	✓	✓	✓	✓
การกำหนดรหัสผ่านซ้ำกันในระบบต่าง ๆ	✓	✓	✓	✓	✓	✓	✓
ใช้รหัสผ่าน หรือบัตรผ่านร่วมกัน	✓	✓	✓	✓	✓	✓	✓
กระบวนการกำหนดสิทธิ์	✓	✓	✓	✓	✓	✓	✓
ไม่มีการกำหนดสิทธิ์ สามารถเข้าถึงในระดับเดียวกัน	✓	✓	✓	✓	✓	✓	✓
กระบวนการกำหนดสิทธิ์ไม่เพียงพอเหมาะสม	✓	✓	✓	✓	✓	✓	✓
ยกเว้นไม่ทำตามขั้นตอนการกำหนดสิทธิ์	✓	✓	✓	✓	✓	✓	✓
กำหนดสิทธิ์ไม่เหมาะสมกับสิทธิ์ที่ควรได้รับ	✓	✓	✓	✓	✓	✓	✓
กำหนดสิทธิ์ให้สามารถเข้าถึงระบบหนึ่ง ที่อาจเป็นช่องทางเข้าถึงระบบที่ไม่ได้รับสิทธิ์	✓	✓	✓	✓	✓	✓	✓
การเข้าถึงระบบจากเครือข่ายภายใน		✓	✓	✓	✓	✓	✓
ไม่มีกระบวนการควบคุมการเข้าถึงระบบจากเครือข่ายภายใน		✓	✓	✓	✓	✓	✓
กระบวนการควบคุมการเข้าถึงระบบจากเครือข่ายภายใน ไม่เหมาะสมเพียงพอ		✓	✓	✓	✓	✓	✓
ยกเว้นไม่ทำตามกระบวนการควบคุมการเข้าถึงเครือข่ายภายใน		✓	✓	✓	✓	✓	✓
ผู้ไม่มีสิทธิ์สามารถเข้าถึงระบบด้วยเครือข่ายภายใน		✓	✓	✓	✓	✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ผู้ไม่มีสิทธิ์สามารถเข้าถึงระบบผ่าน Access Point ของเครือข่ายภายใน		✓	✓	✓	✓	✓	✓
ผู้มีสิทธิ์ไม่สามารถเข้าถึงระบบด้วยเครือข่ายภายใน		✓	✓	✓	✓	✓	✓
การเข้าถึงระบบจากเครือข่ายภายนอก		✓	✓	✓		✓	✓
ไม่มีกระบวนการควบคุมการเข้าถึงระบบจากเครือข่ายภายนอก		✓	✓	✓		✓	✓
กระบวนการควบคุมการเข้าถึงระบบจากเครือข่ายภายนอกไม่เหมาะสมเพียงพอ		✓	✓	✓		✓	✓
ยกเว้นไม่ทำตามกระบวนการควบคุมการเข้าถึงจากเครือข่ายภายนอก		✓	✓	✓		✓	✓
ผู้ไม่มีสิทธิ์สามารถเข้าถึงระบบจากเครือข่ายภายนอก		✓	✓	✓		✓	✓
ผู้มีสิทธิ์ไม่สามารถเข้าถึงระบบจากเครือข่ายภายนอก		✓	✓	✓		✓	✓
การกำหนดนโยบายรักษาความปลอดภัยบนเครือข่าย		✓	✓	✓	✓	✓	✓
ไม่มีการกำหนด Policy ให้กับอุปกรณ์ (any to any)		✓	✓	✓	✓	✓	✓
กระบวนการกำหนด Policy ไม่เหมาะสม เพียงพอ		✓	✓	✓	✓	✓	✓
มีการเปิด Port ที่ไม่มีการใช้งาน		✓	✓	✓	✓	✓	✓
มีการปิด Port ที่มีการใช้งาน		✓	✓	✓	✓	✓	✓
ไม่มีการจัดการ หรือกำหนด QoS ไม่เหมาะสม		✓	✓	✓	✓	✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
การโจมตีประเภท : Attack							
Hacker		✓	✓	✓	✓	✓	✓
Sniffing		✓	✓	✓	✓	✓	✓
Modification		✓	✓	✓	✓	✓	✓
IP Spoofing		✓	✓	✓	✓	✓	✓
Man-in-the-Middle		✓	✓	✓	✓	✓	✓
Malware		✓	✓	✓	✓	✓	✓
Virus		✓	✓	✓	✓	✓	✓
Worm		✓	✓	✓	✓	✓	✓
Trojan Horse		✓	✓	✓	✓	✓	✓
Adware		✓	✓	✓	✓	✓	✓
Spyware		✓	✓	✓	✓	✓	✓
Ransomware		✓	✓	✓	✓	✓	✓
Backdoor		✓	✓	✓	✓	✓	✓
Crypter		✓	✓	✓	✓	✓	✓
Exploit		✓	✓	✓	✓	✓	✓
Rootkit		✓	✓	✓	✓	✓	✓
Social Engineering		✓	✓	✓	✓	✓	✓

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบปรับปรุงอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
Phishing		✓	✓	✓	✓	✓	✓
Password Guessing		✓	✓	✓	✓	✓	✓
Cryptanalysis		✓	✓	✓	✓	✓	✓
Macro		✓	✓	✓	✓	✓	✓
Zero-day Attack		✓	✓	✓	✓	✓	✓
Zombie		✓	✓	✓	✓	✓	✓

3. วิเคราะห์ และประเมินความเสี่ยง

จากข้อมูลสามารถกำหนดเป็นหัวข้อเพื่อประเมินความเสี่ยง ในที่นี้เห็นว่าการประเมินความเสี่ยงเดียวกันกับสินทรัพย์ข้อมูลสารสนเทศในแต่ละประเภทในหน้าเดียวกันจะช่วยให้สามารถเปรียบเทียบเห็นข้อแตกต่างได้

ตารางที่ 4.13 ตัวอย่างการประเมินความเสี่ยง

ความเสี่ยง	ระบบสำรองไฟฟ้า		ไฟไร้วอล		ระบบสารบรรณอิเล็กทรอนิกส์		ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์		ระบบจดหมายอิเล็กทรอนิกส์		ระบบสื่อสารทางไกลผ่านจอภาพ		เว็บไซต์สำนักงานศาลยุติธรรม	
ภัยธรรมชาติ : Natural Disaster														
ไฟไหม้	2	5 10	1	5 5	1	5 5	1	5 5			1	5 5	1	5 5
น้ำท่วม	2	5 10	1	5 5	1	5 5	1	5 5			1	5 5	1	5 5
แผ่นดินไหว	1	5 5	1	5 5	1	5 5	1	5 5			1	5 5	1	5 5
ลมพายุ	1	5 5	1	5 5	1	5 5	1	5 5			1	5 5	1	5 5
ฟ้าผ่า	2	5 10	1	5 5	1	5 5	1	5 5			1	5 5	1	5 5
โครงสร้างพื้นฐานห้องศูนย์ปฏิบัติการฯ : Information Infrastructure														
ระบบสำรองไฟฟ้า														
ไฟฟ้าดับจากการบำรุงรักษาไฟฟ้าอาคาร	2	4 8	2	5 10	2	5 10	2	5 10			2	5 10	2	5 10
ไฟฟ้าดับฉุกเฉิน	2	5 10	2	5 10	2	5 10	2	5 10			2	5 10	2	5 10
ไฟกระชาก	2	3 6	2	5 10	2	5 10	2	5 10			2	5 10	2	5 10
เครื่องกำเนิดไฟฟ้าไม่มีความพร้อมใช้งาน	2	4 8	2	5 10	2	5 10	2	5 10			2	5 10	2	5 10
ระบบควบคุมกระแสไฟฟ้าขัดข้อง	1	3 3	1	5 5	1	5 5	1	5 5			1	5 5	1	5 5
ระบบไม่ทำงานเนื่องจากเสื่อมสภาพชำรุด	1	5 5	1	5 5	1	5 5	1	5 5			3	5 5	1	5 5

ตารางที่ 4.13 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า		ไฟร์วอล		ระบบสารบรรณอิเล็กทรอนิกส์		ระบบการยืนยันข้องทางระบบรับส่งอิเล็กทรอนิกส์		ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ		เว็บไซต์สำนักงานศาลยุติธรรม	
กำลังไฟฟ้าไม่เพียงพอติดตั้งอุปกรณ์	1	1 1	1	5 5	1	5 5	1	5 5		3	5 15	1	5 5
ระบบปรับอากาศ													
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ			2	5 10	2	5 10	2	5 10		2	5 10	2	5 10
ระบบปล่อยลมเย็นชำรุด			3	4 12	3	4 12	3	4 12		3	4 12	3	4 12
ระบบระบายความร้อนนอกอาคารชำรุด			2	3 6	2	3 6	2	3 6		2	3 6	2	3 6
ระบบควบคุมระบบปรับอากาศชำรุด			1	3 3	1	3 3	1	3 3		1	3 3	1	3 3
ระบบไม่ทำงานเนื่องจากเสื่อมสภาพชำรุด			1	3 3	1	3 3	1	3 3		1	3 3	1	3 3
ระบบไม่สามารถรักษาอุณหภูมิได้เนื่องจากอากาศภายนอกร้อนมากเกินไป			1	3 3	1	3 3	1	3 3		1	3 3	1	3 3
ระบบล็อกประตู													
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ			2	3 6	2	3 6	2	3 6		2	3 6	2	3 6
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด			2	3 6	2	3 6	2	3 6		2	3 6	2	3 6
ไม่มีกระบวนการกำหนดสิทธิ์			1	5 5	1	5 5	1	5 5		1	5 5	1	5 5
การกำหนดสิทธิ์ไม่เหมาะสมเพียงพอ			1	5 5	1	5 5	1	5 5		1	5 5	1	5 5

ตารางที่ 4.13 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า		ไฟร์วอล		ระบบเฝ้าระวังบรรจุอิเล็กทรอนิกส์		ระบบการยืนยันตัวตนระบบรับส่งอิเล็กทรอนิกส์		ระบบลงทะเบียนอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ		เว็บไซต์สำนักงานศาลยุติธรรม	
ยกเว้นการดำเนินการตามกระบวนการกำหนดสิทธิ์			2	5 10	2	5 10	2	5 10		2	5 10	2	5 10
การกำหนดสิทธิ์ปัจจัยเดียว ด้วยรหัส หรือบัตรมีความปลอดภัยไม่เพียงพอ			2	5 10	2	5 10	2	5 10		2	5 10	2	5 10
ผู้มีสิทธิ์ตั้งรหัสผ่านที่เดาได้ง่าย			3	3 9	3	3 9	3	3 9		3	3 9	3	3 9
ผู้มีสิทธิ์ลืมรหัสผ่าน			1	3 3	1	3 3	1	3 3		1	3 3	1	3 3
การใช้รหัส หรือบัตร ร่วมกัน			2	5 10	2	5 10	2	5 10		2	5 10	2	5 10
ผู้ไม่มีสิทธิ์นำรหัสหรือบัตรผู้อื่นไปใช้เพื่อเข้าสู่พื้นที่			1	5 5	1	5 5	1	5 5		1	5 5	1	5 5
ไฟฟ้าดับประตูปิดอัตโนมัติ			2	5 10	2	5 10	2	5 10		2	5 10	2	5 10
ไฟฟ้าดับประตูเปิดอัตโนมัติ			2	5 10	2	5 10	2	5 10		2	5 10	2	5 10
แบตเตอรี่สำรองระบบควบคุมประตูใช้งานไม่ได้			2	5 10	2	5 10	2	5 10		2	5 10	2	5 10
ระบบตรวจจับน้ำรั่วซึม													
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ	3	5 15	3	1 3	3	1 3	3	1 3		3	1 3	3	1 3
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด	2	5 10	2	1 2	2	1 2	2	1 2		2	1 2	2	1 2

ตารางที่ 4.13 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร้ำวอล	ระบบเยาบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ระบบไม่แจ้งเตือนจากสายเซ็นเซอร์ตรวจจับติดตั้งไม่ครอบคลุมทุกจุด	3 / 5 / 15	3 / 1 / 3	3 / 1 / 3	3 / 1 / 3		3 / 1 / 3	3 / 1 / 3
ระบบไม่แจ้งเตือนเนื่องจากสายเซ็นเซอร์ขาด	1 / 5 / 5	1 / 1 / 1	1 / 1 / 1	1 / 1 / 1		1 / 1 / 1	1 / 1 / 1
ระบบเตือนตรวจจับไม่ส่งเสียงเตือนเมื่อมีน้ำรั่วซึม	1 / 5 / 5	1 / 1 / 1	1 / 1 / 1	1 / 1 / 1		1 / 1 / 1	1 / 1 / 1
ระบบพ่นสารดับเพลิง							
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ	2 / 5 / 10	2 / 5 / 10	2 / 5 / 10	2 / 5 / 10		2 / 5 / 10	2 / 5 / 10
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด	1 / 5 / 5	1 / 5 / 5	1 / 5 / 5	1 / 5 / 5		1 / 5 / 5	1 / 5 / 5
ระบบตรวจจับพ่นสารดับเพลิงเมื่อไม่มีไฟไหม้	1 / 5 / 5	1 / 5 / 5	1 / 5 / 5	1 / 5 / 5		1 / 5 / 5	1 / 5 / 5
ระบบตรวจจับไม่พ่นสารดับเพลิงเมื่อมีไฟไหม้	1 / 5 / 5	1 / 5 / 5	1 / 5 / 5	1 / 5 / 5		1 / 5 / 5	1 / 5 / 5
ระบบพ่นสารดับเพลิงขณะมีการปฏิบัติงานอยู่ภายใน	1 / 5 / 5	1 / 5 / 5	1 / 5 / 5	1 / 5 / 5		1 / 5 / 5	1 / 5 / 5
ระบบแจ้งเตือนทางอีเมล์และ SMS							
ระบบไม่ทำงานเนื่องจากไฟฟ้าดับ	2 / 4 / 8						
ระบบไม่ทำงานเนื่องจากเสื่อมสภาพชำรุด	2 / 4 / 8						

ตารางที่ 4.13 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟไร้วอล	ระบบการบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ระบบตรวจจับไม่ส่งข้อความ SMS เมื่อมีเหตุการณ์	3 5 15						
ผู้ดูแลระบบเข้าสู่ระบบไม่ได้จากความขัดข้อง	1 2 2						
ผู้ดูแลระบบลืมรหัสผ่าน	1 2 2						
ผู้ไม่มีสิทธิ์เข้าถึงระบบจากการรั่วไหลของรหัส	1 4 4						
ซิมโทรศัพท์ไม่มีเงินทำให้ไม่ทำงาน	2 4 8						
ฮาร์ดแวร์ : Hardware							
Rack Server							
ฮาร์ดแวร์ไม่ทำงานเนื่องจากไฟฟ้าดับ		2 5 10	2 5 10	2 5 10		2 5 10	2 5 10
ระบบไม่ทำงานเนื่องจากเสื่อมสภาพชำรุด		2 4 8	2 5 10	2 5 10		3 5 15	2 5 10
ฮาร์ดแวร์ไม่เหมาะกับการใช้งาน เช่น RAM ไม่พอ			3 3 9	3 3 9			
ฮาร์ดแวร์เฉพาะไม่สามารถแก้ไขซ่อมแซมเองได้		4 5 20	2 5 10	2 5 10		4 5 20	2 5 10
ฮาร์ดแวร์มีประวัติการชำรุด		2 3 6	2 3 6	2 3 6		4 5 20	1 3 3

ตารางที่ 4.13 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยืนยันตัวตนระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ไม่มีการกำหนดสิทธิ์ให้ผู้ดูแลระบบในระดับต่างกัน		2 5 10	2 5 10	2 5 10		2 5 10	2 5 10
กำหนดสิทธิ์ผู้ดูแลระบบแต่ละระดับไม่เหมาะสม		1 5 10	2 5 10	2 5 10		2 5 10	2 5 10
ผู้ดูแลระบบตั้งรหัสผ่านเดาได้ง่าย		3 5 15	4 4 16	3 4 12		3 4 12	3 4 12
ผู้ดูแลระบบลืมรหัสผ่าน		2 4 8	2 3 6	2 3 6		2 3 6	2 3 6
บัญชีผู้ใช้เริ่มต้นของอุปกรณ์ (Default User)		1 5 5	1 5 5	1 5 5		3 5 15	1 5 5
บัญชีผู้ใช้งานผู้ดูแลระบบรั่วไหล		3 5 15	2 5 10	2 5 10		4 5 20	1 5 5
ช่องโหว่ของฮาร์ดแวร์แต่ละรุ่น		2 5 10	2 5 10	2 4 10		4 5 20	2 5 10
IBM				2 5 10			
HP			2 5 10			2 5 10	2 5 10
DELL							
CISCO	20	2 5 10				2 5 10	

ตารางที่ 4.13 (ต่อ)

ความเสี่ยง	ระบบสำรองไฟฟ้า	ไฟร์วอล	ระบบสารบรรณอิเล็กทรอนิกส์	ระบบการยื่นฟ้องทางระบบรับส่งอิเล็กทรอนิกส์	ระบบจดหมายอิเล็กทรอนิกส์	ระบบสื่อสารทางไกลผ่านจอภาพ	เว็บไซต์สำนักงานศาลยุติธรรม
ECT							
ระบบไม่ทำงานเนื่องจากการเสื่อมสภาพชำรุด	2 5 10						
ฮาร์ดแวร์เฉพาะไม่สามารถแก้ไขซ่อมแซมเองได้	4 5						

จากการวิเคราะห์พบว่า อุปกรณ์ และระบบแต่ละประเภทมีระดับความเสี่ยงแตกต่างกันขึ้นอยู่กับคุณสมบัติ การใช้งาน การเข้าถึงได้จากภายนอก และสภาพอุปกรณ์

4. กำหนดวัตถุประสงค์ และมาตรการในการควบคุม

การจัดการความเสี่ยงอาจแบ่งวัตถุประสงค์ และมาตรการได้เป็น การป้องกัน (Prevent), ลด (Reduce), ยอมรับ (Accept), การควบคุม (Control) และการโอน (Transfer) ความเสี่ยง สำหรับการศึกษานี้เพื่อให้ง่ายแก่การนำไปใช้จึงพิจารณาแบ่งเป็น มาตรการเชิงป้องกัน (Preventive controls) มาตรการควบคุม (Detective controls) มาตรการแก้ไข (Corrective controls) ดังตัวอย่าง

ตารางที่ 4.14 ตัวอย่างวัตถุประสงค์การควบคุมและมาตรการควบคุม

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	วัตถุประสงค์การควบคุม	มาตรการควบคุม
โครงสร้างพื้นฐานห้องศูนย์ปฏิบัติการฯ : Information Infrastructure				
ระบบสำรองไฟฟ้า				
1	ไฟฟ้าดับจากการบำรุงรักษาไฟฟ้าอาคาร	ต่ำ	ป้องกันการเกิดไฟฟ้าดับโดยไม่ทราบล่วงหน้า	▪ ประสานงานการแจ้งเตือนกำหนดการบำรุงรักษาไฟฟ้าประจำปี
			ควบคุมให้มีผลกระทบต่ออุปกรณ์และระบบน้อยที่สุด	▪ เข้าตรวจสอบพื้นที่ติดตั้งระบบไฟฟ้าทุกวัน ▪ กำหนดให้ดำเนินการในวันหยุดราชการ ▪ กำหนดเจ้าหน้าที่เวรเข้าเตรียมความพร้อมระหว่างการบำรุงรักษาไฟฟ้าอาคาร ▪ ตรวจสอบเตรียมความพร้อมอุปกรณ์เครื่องกำเนิดไฟฟ้าที่ติดตั้งบนดาดฟ้า อาคารศาลอาญา
			แก้ไขผลกระทบที่อาจมีต่ออุปกรณ์และระบบ	▪ ประกาศให้ผู้ใช้ระบบทราบทั่วประเทศ ▪ แจ้งผู้ดูแลระบบ เจ้าของระบบ ประเมินระบบตนเอง และให้มอบรหัสควบคุกรณีฉุกเฉินให้แก่เจ้าหน้าที่เวรผู้เข้าปฏิบัติงานในวันหยุด ▪ ปิดอุปกรณ์และระบบที่ไม่จำเป็นต้องใช้ก่อนวันดำเนินการตามแผน 1 วัน
2	ไฟฟ้าดับฉุกเฉิน	ปานกลาง	ป้องกันการเกิดไฟฟ้าดับฉุกเฉิน	▪ แจ้งทางส่วนอาคารสถานที่ ศาลอาญา เพื่อตรวจสอบหม้อแปลงเก่าที่เป็นสาเหตุของไฟฟ้าดับบ่อยครั้ง เพื่อดำเนินการเปลี่ยนแทนแก้ไข
			ควบคุมผลกระทบจากการเกิดไฟฟ้าดับฉุกเฉิน	▪ เข้าตรวจสอบพื้นที่ติดตั้งระบบไฟฟ้าทุกวัน ▪ กำหนดขั้นตอนปฏิบัติงานกรณีฉุกเฉิน เพื่อเข้าดำเนินการกับอุปกรณ์และระบบเมื่อไฟฟ้าดับ ▪ กำหนดเจ้าหน้าที่เวรเพื่อปฏิบัติงานวันหยุด

ตารางที่ 4.14 (ต่อ)

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	วัตถุประสงค์การควบคุม	มาตรการควบคุม
2	ไฟฟ้าดับฉุกเฉิน (ต่อ)	ปานกลาง		■ แจ้งปิดระบบที่ไม่จำเป็นต้องใช้งานเพื่อป้องกันความเสียหายที่อาจเกิดเมื่อระบบสำรองไฟฟ้าไม่สามารถให้บริการได้
		ปานกลาง	แก้ไขความเสียหายที่เกิดจากไฟฟ้าดับฉุกเฉิน	■ ประกาศให้ผู้ใช้ระบบทราบทั่วประเทศ ■ แจ้งผู้ดูแลระบบ เจ้าของระบบ ประเมินระบบตนเอง และให้มอบรหัสควบคุกรณีฉุกเฉินให้แก่เจ้าหน้าที่เวรผู้เข้าปฏิบัติงาน ■ ตรวจสอบอุปกรณ์และระบบที่ได้รับผลกระทบ ภายหลังไฟฟ้าใช้งานได้ ■ กรณีพบปัญหาอุปกรณ์และระบบไม่สามารถทำงานได้ตามปกติให้แจ้งเจ้าของระบบเข้าดำเนินการกู้คืนระบบ ■ แจ้งขอใช้ไฟฟ้าจากเครื่องกำเนิดไฟฟ้าอาคารของศาลอาญา เพื่อจ่ายไฟฟ้าทดแทนการไฟฟ้า
3	ไฟกระชาก	ต่ำ	ป้องกันการเกิดไฟฟ้ากระชาก	■ แจ้งทางส่วนอาคารสถานที่ ศาลอาญา เพื่อตรวจสอบสาเหตุ และแก้ไข
			ควบคุมผลกระทบจากไฟฟ้ากระชาก	■ เข้าตรวจสอบพื้นที่ติดตั้งระบบไฟฟ้าทุกวัน ■ ติดตั้งระบบป้องกันไฟฟ้ากระชากเพิ่มเติมภายในตู้ Rack สำหรับอุปกรณ์และระบบที่มีความอ่อนไหว ■ กำหนดเจ้าหน้าที่เวรเพื่อปฏิบัติงานวันหยุดกรณีได้รับแจ้งเตือนจากระบบ ■ แจ้งปิดระบบที่ไม่จำเป็นต้องใช้งานเพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

ตารางที่ 4.14 (ต่อ)

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	วัตถุประสงค์การควบคุม	มาตรการควบคุม
		ต่ำ	แก้ไขการเกิดไฟฟ้ากระชาก	■ แจ้งผู้ดูแลระบบ เจ้าของระบบ ประเมินระบบตนเอง และให้มอบรหัสควบคุมกรณีฉุกเฉินให้แก่เจ้าหน้าที่เวรผู้เข้าปฏิบัติงาน ■ ตรวจสอบอุปกรณ์และระบบที่ได้รับผลกระทบจากไฟฟ้ากระชากภายหลังไฟฟ้าใช้งานได้ ■ กรณีพบปัญหาอุปกรณ์และระบบไม่สามารถทำงานได้ตามปกติให้แจ้งเจ้าของระบบเข้าดำเนินการกู้คืนระบบ
4	เครื่องกำเนิดไฟฟ้าไม่มีความพร้อมใช้งาน	ต่ำ	ป้องกันการเกิดความไม่พร้อมใช้งานของอุปกรณ์	■ แจ้งให้ส่วนอาคารสถานที่ ศาลอาญาดำเนินการตรวจสอบเตรียมความพร้อมเป็นประจำทุกเดือน ■ ดำเนินการขอทดสอบระบบไฟฟ้าประจำปี การสลับเฟสไฟฟ้า แทนระบบสำรองไฟฟ้า
			ควบคุมผลกระทบกรณีไม่มีความพร้อมใช้งาน	■ เข้าตรวจสอบพื้นที่ติดตั้งระบบไฟฟ้าทุกวัน ■ ติดตั้งระบบสำรองไฟฟ้าเพิ่มเติมภายในตู้ Rack สำหรับอุปกรณ์และระบบที่มีความอ่อนไหว
				■ กำหนดเจ้าหน้าที่เวรเพื่อปฏิบัติงานวันหยุดกรณีได้รับแจ้งเตือนไฟฟ้าดับจากระบบ
			แก้ไขเมื่อไม่สามารถใช้งานเครื่องกำเนิดไฟฟ้าในกรณีจำเป็นได้	■ แจ้งส่วนอาคารสถานที่ ศาลอาญา เข้าตรวจสอบแก้ไข เครื่องกำเนิดไฟฟ้า

ตารางที่ 4.14 (ต่อ)

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	วัตถุประสงค์การควบคุม	มาตรการควบคุม
5	ระบบควบคุมกระแสไฟฟ้าขัดข้อง	ต่ำ	ป้องกันระบบควบคุมกระแสไฟฟ้าขัดข้อง	▪ กำหนดให้มีการบำรุงรักษาระบบควบคุมกระแสไฟฟ้าภายในห้องศูนย์ปฏิบัติการเครือข่าย ปีละ 1 ครั้ง ▪ กรณีพบปัญหากระแสไฟฟ้า แจ้งให้บริษัทผู้ดูแลระบบเข้าตรวจสอบอีกครั้ง
			ควบคุมผลกระทบจากระบบควบคุมกระแสไฟฟ้าขัดข้อง	▪ กรณีระบบควบคุมขัดข้องให้ทำการ Bypass เพื่อใช้งานได้ชั่วคราว
			แก้ไขระบบควบคุมกระแสไฟฟ้าขัดข้อง	▪ แจ้ง SITEM เข้าแก้ไข
6	ระบบไม่ทำงานเนื่องจากเสื่อมสภาพชำรุด	ต่ำ	ป้องกันระบบเสื่อมสภาพชำรุด	▪ กำหนดให้มีการบำรุงรักษา ปีละ 1 ครั้ง ▪ กรณีพบปัญหาแรงดันไฟฟ้าไม่เพียงพอ ให้แจ้งบริษัทเข้าตรวจสอบ
			ควบคุมผลกระทบจากระบบเสื่อมสภาพชำรุด	▪ เมื่อตรวจพบการเสื่อมสภาพชำรุดให้แจ้งเข้าตรวจสอบหาสาเหตุทันที หากปล่อยไว้อาจทำให้อุปกรณ์ที่ทำงานร่วมกันเสื่อมสภาพ
			แก้ไขความเสื่อมสภาพชำรุด	▪ แจ้งบริษัทเข้าดำเนินการแก้ไข

4.2.1.3 เตรียมความพร้อมขั้นตอนเพื่อนำไปปฏิบัติ

ในขั้นตอนนี้เป็นการจัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้ ISMS เพื่อให้เข้าใจและนำไปใช้งานง่ายจึงจัดทำเป็นเอกสารในรูปแบบตาราง

ตารางที่ 4.15 อย่างแนวทางประยุกต์ใช้ ISMS

ตรวจสอบ	มาตรการควบคุมตามขั้นตอนปฏิบัติ	มาตรการควบคุมตามแนวทาง ISMS	ข้อกำหนด
	■ ประสานงานการแจ้งเตือนกำหนดการบำรุงรักษาไฟฟ้าประจำปี	A.6.1.3 Contact with authorities	สำนักเทคโนโลยีสารสนเทศประสานงานให้หน่วยงานศาลอาญาผู้รับผิดชอบดำเนินการบำรุงรักษาไฟฟ้าอาคาร ให้แจ้งกำหนดการบำรุงรักษาและแจ้งเตือนก่อนดำเนินการ
	■ เข้าตรวจสอบพื้นที่ติดตั้งระบบไฟฟ้าทุกวัน	-	
	■ กำหนดให้ดำเนินการในวันหยุดราชการ	-	
	■ กำหนดเจ้าหน้าที่เวรเข้าเตรียมความพร้อมระหว่างการบำรุงรักษาไฟฟ้าอาคาร	A.16.1.5 Response to information security incidents	เจ้าหน้าที่ผู้รับผิดชอบประจำวันซึ่งมีการกำหนดไว้แล้ว เข้าเตรียมความพร้อมเพื่อตอบสนองต่อเหตุการณ์ และดำเนินการตามขั้นตอนควบคุมความเสียหายต่ออุปกรณ์และระบบกรณีเกิดไฟฟ้าดับจากการซ่อมบำรุงไฟฟ้าอาคาร
	■ ตรวจสอบเตรียมความพร้อมอุปกรณ์เครื่องกำเนิดไฟฟ้าที่ติดตั้งบนดาดฟ้าอาคารศาลอาญา	A.6.1.3 Contact with authorities	สำนักเทคโนโลยีสารสนเทศประสานงานให้หน่วยงานศาลอาญาตรวจสอบ เตรียมความพร้อม ทดสอบเครื่องกำเนิดไฟฟ้าอาคารซึ่งอยู่ในความรับผิดชอบของศาลอาญา

4.2.2 ขั้นดำเนินการ : Do

4.2.2.1 ดำเนินการตามมาตรการควบคุมเชิงป้องกัน

มาตรการเชิงป้องกันช่วยให้เหตุการณ์มีโอกาสเกิดขึ้นน้อยลง มีการกำหนดแผนมาตรการควบคุมเชิงป้องกัน และการดำเนินการตามแผน ตัวอย่างแผนแก้ไขความเสี่ยงลักษณะเด่นที่ชัดเจน คือ เป็นการดำเนินการก่อนเหตุการณ์เกิดขึ้น สามารถนำไปปฏิบัติได้ ดังนี้

ตารางที่ 4.16 ตัวอย่างแผนดำเนินการมาตรการป้องกันความเสี่ยง

ลำดับ	ระบบ	ความเสี่ยง	กิจกรรม	แผนดำเนินงาน	ผู้รับผิดชอบ	กำหนดการ
1	ระบบสำรองไฟฟ้า	ไฟฟ้าดับจากการบำรุงรักษาไฟฟ้าอาคาร	ประสานงานการแจ้งเตือนกำหนดการบำรุงรักษาไฟฟ้าประจำปี	1. จัดทำหนังสือถึงผู้อำนวยการสำนักอำนวยการประจำศาลอาญา แจ้งขอทราบแผนบำรุงรักษาไฟฟ้าอาคารของศาลอาญา	นายสิทธิชัย แสงทองจรัสกุล	31 มี.ค. 63
				2. มีหนังสือถึงส่วนอาคารสถานที่ ศาลอาญา สอบถามกำหนดการดับไฟฟ้าเพื่อบำรุงรักษาไฟฟ้าอาคาร และขอความร่วมมือแจ้งให้ทราบล่วงหน้า	นายสิทธิชัย แสงทองจรัสกุล	7 เม.ย. 63
				3. กำหนดเจ้าหน้าที่ส่วนระบบเครือข่าย ฯ ประสานงานกับส่วนอาคารสถานที่ศาลอาญา เพื่อเตรียมความพร้อม	นายวิธาร อัศวมงคลศิริ	31 มี.ค. 63

4.2.2.2 ดำเนินการตามมาตรการควบคุมตรวจสอบ

มาตรการควบคุมตรวจสอบทำให้สามารถทราบเหตุการณ์ เข้าตรวจสอบ และดำเนินการตอบสนองได้อย่างรวดเร็ว การดำเนินการมีการกำหนดแผน และการดำเนินการตามแผน ตัวอย่างดังนี้

ตารางที่ 4.17 ตัวอย่างแผนดำเนินการมาตรการควบคุมความเสี่ยง

ลำดับ	ระบบ	ความเสี่ยง	กิจกรรม	แผนดำเนินงาน	ผู้รับผิดชอบ	กำหนดการ
1	ระบบสำรองไฟฟ้า	ไฟฟ้าดับจากการบำรุงรักษาไฟฟ้าอาคาร	เข้าตรวจสอบพื้นที่ติดตั้งระบบไฟฟ้าทุกวัน	1. กำหนดเจ้าหน้าที่เวรเข้าปฏิบัติการตรวจสอบห้องศูนย์ปฏิบัติการเครือข่ายฯ	หัวหน้าส่วนระบบเครือข่ายคอมพิวเตอร์	31 มี.ค. 63
				2. แจ้งเจ้าหน้าที่ส่วนระบบเครือข่ายฯ ทราบถึงกำหนดเวรเข้าดำเนินการ	นายฐิติเชษฐ์ ดิลกศิลป์	1 เม.ย. 63
				3. เจ้าหน้าที่เวร เข้าตรวจสอบพื้นที่ศูนย์ปฏิบัติการเครือข่ายทุกวัน เวลา 08.30 น. และ 16.00 น. พร้อมทั้งรายงานให้หัวหน้าส่วนระบบเครือข่ายทราบ	รายชื่อเจ้าหน้าที่ทั้งหมด	1 เม.ย. 63

4.2.2.3 ดำเนินการตามมาตรการควบคุมแก้ไข

มาตรการควบคุมแก้ไข อาจแบ่งได้ 2 ประการ ได้แก่ การควบคุมแก้ไขความเสียหายและการกู้คืนระบบ การดำเนินการมีการกำหนดแผน และการดำเนินการตามแผน ตัวอย่างดังนี้

ตารางที่ 4.18 ตัวอย่างแผนดำเนินการมาตรการแก้ไขความเสี่ยง

ลำดับ	ระบบ	ความเสี่ยง	กิจกรรม	แผนดำเนินงาน	ผู้รับผิดชอบ	กำหนดการ
1	ระบบสำรองไฟฟ้า	ไฟฟ้าดับจากการบำรุงรักษาไฟฟ้าอาคาร	แจ้งผู้ดูแลระบบ เจ้าของระบบ ประเมินระบบตนเอง และให้มอบรหัสควบคุมกรณีฉุกเฉินให้แก่เจ้าหน้าที่เวรผู้เข้าปฏิบัติงานในวันหยุด	1. จัดทำรายการเจ้าของระบบที่ติดตั้งระบบภายในศูนย์ พร้อมหมายเลขโทรศัพท์ติดต่อ	นายฐิติเชษฐ์ ดิลกศิลป์	31 มี.ค. 63
				2. เมื่อได้รับแจ้งกรณีไฟฟ้าดับ อยู่ระหว่างใช้ไฟฟ้าจากระบบสำรองไฟฟ้า ให้เจ้าหน้าที่เวรแจ้งเจ้าของระบบ เพื่อประเมินความเสี่ยงของระบบตนเอง และมอบรหัสเข้าสู่ระบบเพื่อปิดระบบตามขั้นตอนแก่เจ้าหน้าที่เวร	รายชื่อเจ้าหน้าที่ทั้งหมด	1 เม.ย. 63
				3. เมื่อระบบสำรองไฟฟ้าแจ้งเตือนเหลือกระแสไฟฟ้า 20% ให้ปิดเครื่องแม่ข่ายและฐานข้อมูลก่อน สำหรับอุปกรณ์สวิตช์ และระบบสื่อสารทางไกลผ่านจอภาพให้ปิดหลังสุด	รายชื่อเจ้าหน้าที่ทั้งหมด	1 เม.ย. 63

4.2.2.4 ตรวจสอบมาตรการตามข้อตกลงที่สอดคล้องกับมาตรฐาน ISO 27001

จัดทำเอกสาร Statement of Applicable (SoA) เพื่อตรวจสอบความสอดคล้องกับการกำหนดมาตรการ และมาตรฐาน ISO 27001 ให้มีการแสดงมาตรการที่ใช้และไม่ใช้ กรณีไม่ใช้งานมาตรการควบคุมให้ระบุเหตุผลด้วย

ตารางที่ 4.19 ตัวอย่างเอกสาร Statement of Applicable (SoA)

ตรวจสอบ	หัวข้อ	หัวเรื่อง	การประยุกต์ใช้	หมายเหตุ
A.5 Information security policies				
A.5.1 Management direction for information security				
✓	A.5.1.1	Policies for information security	จัดทำนโยบายรักษาความปลอดภัยข้อมูลสารสนเทศโดยขออนุมัติจากฝ่ายบริหาร	มีการร่างนโยบายและเสนอผู้บริหารแล้ว แต่ยังไม่มีการประกาศใช้อย่างเป็นทางการ เนื่องจากกระบวนการ ISMS ยังดำเนินการไม่สมบูรณ์
✓	A.5.1.2	Review of the policies for information security	ทบทวนปรับปรุงนโยบายให้มีความทันสมัยและเหมาะสมต่อเทคโนโลยี และนโยบายองค์กร	ทบทวนปรับปรุงนโยบายทุก 5 ปี
A.6 Organization of information security				
A.6.1 Internal organization				
✓	A.6.1.1	Information security roles and responsibilities	ข้อกำหนดวิธีปฏิบัติกรณีฉุกเฉิน	สำนักเทคโนโลยีสารสนเทศได้มอบหมายให้เจ้าของระบบจัดทำข้อกำหนดวิธีปฏิบัติกรณีฉุกเฉินให้ทราบ และปรับปรุงทุก 1 ปี
	A.6.1.2	Segregation of duties		มีการซ้ำซ้อนในหน้าที่ความรับผิดชอบเฉพาะ เครื่องแม่ข่าย ระบบงาน ฐานข้อมูล สำหรับระบบงานภายในเนื่องจากการใช้งานทดสอบโปรแกรม การดำเนินโครงการจัดซื้อแม่ข่ายและส่วนงานนั้น ๆ ดูแลด้วยตัวเองไม่ได้ส่งมอบทั้งหมดมาให้ส่วนระบบเครือข่าย

4.2.3 ขั้นทบทวนแก้ไขปรับปรุง : Check

4.2.3.1 ตรวจสอบ ตรวจจับข้อผิดพลาด และประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ

จากบทที่ 3 กระบวนการตรวจสอบเป็นการพิจารณามาตรการควบคุมที่ปฏิบัติ กับมาตรการควบคุมตามมาตรฐาน ISMS จากนั้นจึงพิจารณาดำเนินการแก้ไข บันทึกผลการดำเนินการ

ตารางที่ 4.20 ตัวอย่างการตรวจสอบข้อผิดพลาดตามมาตรการควบคุม

ลำดับ	ระบบ	ความเสี่ยง	มาตรฐานไม่สอดคล้อง	สาเหตุ	แนะนำแก้ไข
2	ระบบสำรองไฟฟ้า	ไฟฟ้าดับฉุกเฉิน	A.11.2.4 Equipment maintenance	▪ ขาดการตรวจสอบบำรุงรักษาเนื่องจากไม่อยู่ในความรับผิดชอบของสำนักเทคโนโลยีสารสนเทศ เช่น หม้อแปลงไฟฟ้า และเครื่องกำเนิดไฟฟ้า ของศาลอาญา	▪ พิจารณาติดตั้งเครื่องกำเนิดไฟฟ้าสำหรับศูนย์ปฏิบัติการเครือข่าย เพิ่มเติมโดยสำนักเทคโนโลยีสารสนเทศเป็นเจ้าของระบบ
			A.17.2.1 Availability of information processing facilities	▪ ไม่มีการติดตั้งเฟสไฟฟ้าสำรอง ใช้ไฟฟ้าเดียวกันกับของอาคารซึ่งเกิดปัญหาไฟฟ้าดับบ่อยครั้ง	▪ ดำเนินการติดตั้งหม้อแปลงไฟฟ้าและนำเข้ากระแสไฟฟ้าอีกเฟสหนึ่งต่างหาก

4.2.3.2 วัดประสิทธิภาพของมาตรการที่ใช้ว่าได้ผลหรือไม่

การวัดประสิทธิภาพ 2 แบบ คือ ประสิทธิภาพตามมาตรการควบคุมมาตรฐาน และประสิทธิภาพตามมาตรการควบคุมที่ปฏิบัติ ดังตาราง

ตารางที่ 4.21 ตัวอย่างการวัดประสิทธิภาพมาตรการควบคุม

Reference		Compliance Assessment Area		Results	
Check	**Standard**	**Section**	**Initial Assessment Points**	**Findings**	**Status**
	A.5	**Information Security Policies**			
	A.5.1	**Management direction for information security**			
	A.5.1.1	Policies for information security	1. Do Security policies exit? 2. Are all policies approved by management? 3. Are policies properly communicated to employees?	- มีร่างนโยบาย - ผ่านการอนุมัติจากคณะอนุกรรมการฯ - ยังไม่มีการประกาศใช้งานเป็นทางการ	75%

ตารางที่ 4.22 ตัวอย่างการประเมินความเสี่ยงก่อนและหลังปรับปรุง

ลำดับ	ระบบ	ความเสี่ยง	ความเสี่ยงก่อนปรับปรุง		ความเสี่ยงหลังปรับปรุง		หมายเหตุ
1	ระบบสำรองไฟฟ้า	ไฟฟ้าดับฉุกเฉิน	2	5 10	1	3 3	การติดตั้งหม้อแปลงไฟฟ้าและนำเข้ากระแสไฟฟ้าอีกเฟสหนึ่งทำให้โอกาส และผลกระทบลดลง

4.2.3.3 ดำเนินการตรวจสอบภายใน (Internal Audit)

โดยทั่วไปการตรวจสอบจะดำเนินการตามหัวข้อของเกณฑ์มาตรฐาน ซึ่งกรณีศึกษาใช้ ISO 27001 เอกสารที่เกี่ยวข้องสำหรับการตรวจสอบภายในได้แก่

1. ทะเบียนสินทรัพย์ข้อมูลสารสนเทศ
2. กระบวนการทำงานของอุปกรณ์และระบบ
3. รายงานผลการประเมินความเสี่ยง
4. ตรวจสอบเอกสาร Statement of Applicable (SoA)
5. วิเคราะห์บันทึกเหตุการณ์เกิดความผิดปกติของระบบ และหาสาเหตุ
6. ทดสอบด้วยเครื่องมือ Scan Tool ประเภทต่าง ๆ

4.2.3.4 ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดที่ตรวจพบ

ภายหลังดำเนินการตรวจสอบแล้วพบข้อผิดพลาดในกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศ ให้ดำเนินการปรับปรุงแผนป้องกันใหม่ โดยปรับปรุงตามเอกสารแผน และให้มีการบันทึกการปรับปรุง สาเหตุการปรับปรุง วันที่ เวลา และรายละเอียดต่าง ๆ

ตารางที่ 4.23 ตัวอย่างแผนปฏิบัติการรักษาความปลอดภัยข้อมูลสารสนเทศ (ฉบับปรับปรุง)

ลำดับ	ระบบ	ความเสี่ยง	วัตถุประสงค์การควบคุม	มาตรการควบคุม	หมายเหตุ
2	ระบบสำรองไฟฟ้า	ไฟฟ้าดับฉุกเฉิน	ป้องกันการเกิดไฟฟ้าดับฉุกเฉิน	▪ ดำเนินการติดตั้งหม้อแปลงไฟฟ้าและนำเข้ากระแสไฟฟ้าอีกเฟสหนึ่งต่างหาก	▪ **วันที่** 1 เม.ย. 63 ปรับปรุงแผนฯ ▪ **เนื้อหา**ปรับปรุงแผนจากเดิมแจ้งให้ศาลอาญาตรวจสอบเครื่องกำเนิดไฟฟ้าเป็นการดำเนินการติดตั้งหม้อแปลงไฟฟ้าและนำเข้ากระแสไฟฟ้าอีกเฟสหนึ่งต่างหาก ▪ **สาเหตุ**เพื่อให้สอดคล้องตามมาตรฐาน A.17.2.1 ▪ **งบประมาณ** 10,0000 บาท
			ควบคุมผลกระทบจากการเกิดไฟฟ้าดับฉุกเฉิน	▪ เข้าตรวจสอบพื้นที่ติดตั้งระบบไฟฟ้าทุกวัน ▪ กำหนดขั้นตอนปฏิบัติงานกรณีฉุกเฉิน เพื่อเข้าดำเนินการกับอุปกรณ์และระบบเมื่อไฟฟ้าดับ	ไม่มีการแก้ไข

ตารางที่ 4.23 (ต่อ)

ลำดับ	ระบบ	ความเสี่ยง	วัตถุประสงค์การควบคุม	มาตรการควบคุม	หมายเหตุ
2	ระบบสำรองไฟฟ้า (ต่อ)	ไฟฟ้าดับฉุกเฉิน (ต่อ)	ควบคุมผลกระทบจากการเกิดไฟฟ้าดับฉุกเฉิน (ต่อ)	▪ กำหนดเจ้าหน้าที่เวรเพื่อปฏิบัติงานวันหยุดกรณีได้รับแจ้งเตือนจากระบบ ▪ แจ้งปิดระบบที่ไม่จำเป็นต้องใช้งานเพื่อป้องกันความเสียหายที่อาจเกิดเมื่อระบบสำรองไฟฟ้าไม่สามารถให้บริการได้ ▪ ตรวจสอบเตรียมความพร้อมอุปกรณ์เครื่องกำเนิดไฟฟ้าที่ติดตั้งบนดาดฟ้าอาคารศาลอาญา	ไม่มีการแก้ไข
			แก้ไขความเสียหายที่เกิดจากไฟฟ้าดับฉุกเฉิน (ต่อ)	▪ ประกาศให้ผู้ใช้ระบบทราบทั่วประเทศ ▪ แจ้งผู้ดูแลระบบเจ้าของระบบประเมินระบบตนเองและให้มอบรหัสควบคุม	▪ **วันที่** 1 เม.ย. 63 ปรับปรุงแผนฯ ▪ **เนื้อหา**ปรับปรุงแผนจากแจ้งขอใช้เครื่องกำเนิดไฟฟ้าศาลอาญาเป็นการติดตั้งเครื่องกำเนิดไฟฟ้าสำหรับศูนย์ปฏิบัติการเครือข่าย โดยสำนักเทคโนโลยีสารสนเทศเป็นเจ้าของระบบ

ตารางที่ 4.23 (ต่อ)

ลำดับ	ระบบ	ความเสี่ยง	วัตถุประสงค์การควบคุม	มาตรการควบคุม	หมายเหตุ
2	ระบบสำรองไฟฟ้า (ต่อ)	ไฟฟ้าดับฉุกเฉิน (ต่อ)	แก้ไขความเสียหายที่เกิดจากไฟฟ้าดับฉุกเฉิน (ต่อ)	กรณีฉุกเฉินให้แก่เจ้าหน้าที่เวรผู้เข้าปฏิบัติงาน ▪ ตรวจสอบอุปกรณ์และระบบที่ได้รับผลกระทบจากไฟฟ้าดับฉุกเฉินภายหลังไฟฟ้าใช้งานได้ ▪ กรณีพบปัญหาอุปกรณ์และระบบไม่สามารถทำงานได้ตามปกติให้แจ้งเจ้าของระบบเข้าดำเนินการกู้คืนระบบ ▪ ติดตั้งเครื่องกำเนิดไฟฟ้าสำหรับศูนย์ปฏิบัติการเครือข่ายเพิ่มเติม โดยสำนักเทคโนโลยีสารสนเทศเป็นเจ้าของระบบ	▪ **สาเหตุ**เพื่อให้สอดคล้องตามมาตรฐาน A.11.2.4 ▪ **งบประมาณ** 10,0000 บาท

4.2.3.5 บันทึกการปฏิบัติ และเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของ ISMS

เมื่อเกิดเหตุการณ์ให้ทำการบันทึกไว้ เช่นเดียวกับการบันทึก log บนคอมพิวเตอร์ เพื่อให้สามารถนำมาใช้โดยง่ายให้บันทึกแยกสำหรับแต่ละอุปกรณ์ และระบบ เนื้อหาการบันทึกประกอบด้วย วันเดือนปี เวลา เหตุการณ์ความเสียหาย อุปกรณ์และระบบที่เกี่ยวข้อง ระบุ IP ของอุปกรณ์ ระบุการทำงานและโปรโตคอลที่พบ ชื่อผู้บันทึก

1. ระบุบันทึกพื้นที่จุดอ่อน ที่ปฏิบัติตามมาตรการควบคุมไม่เหมาะสม (โดยทั่วไปหมายถึง การปฏิบัติน้อยกว่า 90%)

2. กำหนดแผนการปรับปรุงสำหรับจุดอ่อนแต่ละจุด โดยให้ทำงานร่วมกับผู้มีส่วนเกี่ยวข้องเพื่อกำหนดวิธีการปรับปรุงการควบคุม

3. กำหนดการประเมินอีกครั้ง กำหนดรอบระยะเวลาเพื่อทบทวนพื้นที่จุดอ่อน เพื่อกำหนดเป้าหมายสำหรับแผนการปรับปรุง

4.2.3.6 ทบทวนการจัดการความปลอดภัยเป็นระยะ

กำหนดรอบระยะเวลาการทบทวนให้เหมาะสมกับการดำเนินธุรกิจ มีกำหนดวันที่ดำเนินการชัดเจน กิจกรรมทบทวนการจัดการความปลอดภัยให้ดำเนินการตั้งแต่ต้น โดยตรวจสอบนโยบาย รายการสินทรัพย์ข้อมูลสารสนเทศ รายการความเสี่ยง บันทึกเหตุการณ์ประวัติ ซึ่งอาจมีการเปลี่ยนแปลง

สำหรับอุปกรณ์และระบบภายในศูนย์ปฏิบัติการเครือข่ายฯ มีกำหนดดำเนินการทบทวน ดังนี้

1. วัตถุประสงค์ทางธุรกิจ ทบทวนทุก 5 ปี ตามรอบระยะเวลานโยบายสำนักงานศาลยุติธรรม

2. นโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศ ทบทวนทุก 2 ปี ตามรอบระยะเวลาการดำรงตำแหน่งของผู้พิพากษาผู้ดำรงตำแหน่งประจำสำนัก

3. การตรวจสอบทะเบียนสินทรัพย์ข้อมูลสารสนเทศ และข้อมูลอื่น ๆ ทบทวนทุก 1 ปี ยกเว้นกรณีมีการติดตั้งอุปกรณ์และระบบเพิ่มเติม หรือปรับปรุงระบบใหม่ ให้ดำเนินการทบทวนเพื่อวางแผนติดตั้งระบบ

4.2.4 ขั้นกำหนดแนวทางปฏิบัติ : Act

4.2.4.1 จัดทำข้อกำหนดที่ชัดเจนในการแบ่งอุปกรณ์และระบบแต่ละประเภท

จากการศึกษาพบว่าอุปกรณ์ Hardware และ Software จะมีความสัมพันธ์ที่ไม่สามารถแบ่งแยกกันชัดเจน ดังนั้นจึงกำหนดเกณฑ์ในการแบ่งประเภทอุปกรณ์และระบบ ดังนี้

1. แบ่งประเภทตามคุณสมบัติและการทำงาน เช่น โครงสร้างพื้นฐาน สวิตช์ ไฟร์วอลล์ เครื่องแม่ข่ายระบบงาน เครื่องแม่ข่ายฐานข้อมูล อุปกรณ์บันทึกข้อมูล ซึ่งอุปกรณ์เหล่านี้จะมีคุณสมบัติ การทำงาน ช่องโหว่ และการจัดการแบบเดียวกัน

2. แบ่งประเภทตามพื้นที่การเข้าถึง กำหนด Zone ให้แก่อุปกรณ์และระบบ ซึ่งจะแบ่งเป็นระบบงานภายใน ระบบงานภายนอก ระบบงานที่ใช้ได้ทั้งภายในและภายนอก

3. แบ่งประเภทตามงานที่ให้บริการร่วมกัน เช่น ระบบสารบัญอิเล็กทรอนิกส์ มีการใช้งานเครื่องแม่ข่าย Windows 1 ตัว ฐานข้อมูล VM 1 ตัว และ NAS เพื่อบันทึกข้อมูล 1 ตัว นับเป็น 3 ระบบ แต่เมื่อกล่าวถึงระบบสารบัญอิเล็กทรอนิกส์จะหมายถึง ทั้ง 3 ระบบนี้รวมเข้าด้วยกัน การพิจารณากำหนดสิทธิ์การเข้าถึง กำหนดนโยบายรักษาความปลอดภัย ต้องมีความสอดคล้องกัน

4. แบ่งประเภทสิทธิ์ที่สามารถเข้าถึงอุปกรณ์ เช่น อุปกรณ์ไฟร์วอลล์ และสวิตช์ มีการกำหนดสิทธิ์สำหรับผู้ดูแลระบบ และสิทธิ์เจ้าของระบบเท่านั้น

4.2.4.2 จัดทำแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศสำหรับอุปกรณ์และระบบแต่ละประเภท

ตารางที่ 4.24 แนวปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศสำหรับอุปกรณ์และระบบแต่ละประเภท

ลำดับ	ประเภท	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
1	โครงสร้างพื้นฐานศูนย์ปฏิบัติการเครือข่าย (Infrastructure)	■ ฮาร์ดแวร์ต่างกัน ■ ซอฟต์แวร์ต่างกัน ■ ทำงานควบคุมสภาพแวดล้อมในห้องศูนย์	Internal Zone	■ ทุกระบบแจ้งเตือนผ่าน SMS ■ ระบบฉีดพ่นสารดับเพลิงทำงานร่วมกับระบบตรวจจับควัน และระบบ	สิทธิ์ผู้ดูแลระบบ	■ ตรวจสอบประเมินความเสี่ยงแต่ละระบบแยกจากกัน ■ กำหนดมาตรการควบคุมเชิงป้องกันด้วยการตรวจสอบ

ตารางที่ 4.24 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
1	โครงสร้างพื้นฐานศูนย์ปฏิบัติการเครือข่าย (Infrastructure) (ต่อ)	ปฏิบัติการ	Internal Zone	■ ตรวจจับความร้อน	สิทธิ์ผู้ดูแลระบบ	■ กำหนดมาตรการควบคุมด้วยการเตรียมการล่วงหน้า ■ กำหนดมาตรการแก้ไขด้วยการให้มีระบบสำรอง กำหนดข้อปฏิบัติกรณีฉุกเฉิน และแจ้งบริษัทเข้าดำเนินการแก้ไข ■ กำหนดให้มีเจ้าหน้าที่เวรเข้าตรวจสอบระบบเป็นประจำทุกวัน
2	ระบบบริหารจัดการเครือข่าย (Network Management)	■ ฮาร์ดแวร์ Rack Server ■ ซอฟต์แวร์ OS : Linux ■ ทำงานควบคุมเส้นทางเครือข่าย	Internal Zone	■ กำหนด IP /VLAN /Policy ร่วมกัน	สิทธิ์ผู้ดูแลระบบ	■ ตรวจสอบประเมินความเสี่ยงแต่ละระบบมีความคล้ายคลึงกัน สามารถลอกการตั้งค่าอุปกรณ์ไปใช้อีกเครื่องหนึ่ง แล้วแก้ไขให้เหมาะสมอีกครั้ง ■ กำหนดมาตรการควบคุมเชิงป้องกันด้วยการตรวจสอบประจำวัน ■ กำหนดมาตรการควบคุมด้วยการกำหนด Policy

ตารางที่ 4.24 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
2	ระบบบริหารจัดการเครือข่าย (Network Management) (ต่อ)					■ กำหนดมาตรการแก้ไขด้วยการให้มีระบบสำรอง กำหนดข้อปฏิบัติกรณีฉุกเฉิน และแจ้งบริษัทเข้าแก้ไข
3	ระบบงานที่ให้บริการเฉพาะเครือข่ายภายใน (Internal Service)	■ ฮาร์ดแวร์ Rack Server ■ ซอฟต์แวร์ OS : Windows /Linux/VM Application : .NET/Java /MS Access Database : MS Access / My SQL / SQL Server / Oracle ■ Storage : NAS ■ ให้บริการระบบงานเฉพาะที่ใช้งานจากเครือข่ายภายใน	Internal Zone	■ ฮาร์ดแวร์ใช้ร่วมกันบางระบบ ■ ระบบปฏิบัติการร่วมกัน ■ การทำงานของระบบร่วมกัน ■ ฐานข้อมูลร่วมกัน	สิทธิ์ผู้ดูแลระบบ /เจ้าของระบบ /ผู้บริหาร / ผู้ปฏิบัติงาน /บุคลากรภายในหน่วยงาน/ สิทธิ์บุคคล	■ ตรวจสอบประเมินความเสี่ยงด้านฮาร์ดแวร์ / ซอฟต์แวร์ยี่ห้อรุ่นเดียวกันเหมือนกัน สามารถลอกการตั้งค่าอุปกรณ์ไปใช้อีกเครื่องหนึ่ง แล้วแก้ไขให้เหมาะสม ■ กำหนดมาตรการควบคุมเชิงป้องกันด้วยการตรวจสอบประจำวัน และปิดกั้นการเข้าถึงจากภายนอก ■ กำหนดมาตรการควบคุมด้วยการกำหนด Policy ■ กำหนดมาตรการแก้ไขด้วยการให้มีระบบสำรอง กำหนดข้อปฏิบัติกรณีฉุกเฉิน และแจ้งบริษัทเข้าแก้ไข

ตารางที่ 4.24 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
4	ระบบงานที่ให้บริการผ่านเครือข่ายภายนอก (External Service)	■ ฮาร์ดแวร์ Rack Server ■ ซอฟต์แวร์ OS : Windows /Linux/VM Application : .NET/Java Database : MS Access / My SQL / SQL Server / Oracle ■ Storage : NAS ■ ให้บริการระบบงานที่สามารถใช้งานจากเครือข่ายภายในและภายนอก	DMZ	■ ฮาร์ดแวร์ใช้ร่วมกันบางระบบ ■ ระบบปฏิบัติการร่วมกัน ■ การทำงานของระบบร่วมกัน ■ ฐานข้อมูลร่วมกัน	สิทธิ์ผู้ดูแลระบบ /เจ้าของระบบ /ผู้บริหาร / ผู้ปฏิบัติงาน /บุคลากรภายในหน่วยงาน/ สิทธิ์บุคคล	■ ตรวจสอบประเมินความเสี่ยงด้านฮาร์ดแวร์ / ซอฟต์แวร์ยี่ห้อรุ่นเดียวกันเหมือนกัน สามารถลอกการตั้งค่าอุปกรณ์ไปใช้อีกเครื่องหนึ่ง แล้วแก้ไขให้เหมาะสมอีกครั้ง ■ กำหนดมาตรการควบคุมเชิงป้องกันด้วยการตรวจสอบประจำวัน และเปิดให้เข้าใช้เฉพาะที่จำเป็น ■ กำหนดมาตรการควบคุมด้วยการกำหนด Policy ■ กำหนดมาตรการแก้ไขด้วยการให้มีระบบสำรอง กำหนดข้อปฏิบัติกรณีฉุกเฉิน และแจ้งบริษัทเข้าแก้ไข

ตารางที่ 4.24 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
5	ระบบงานบริการจากหน่วยงานพันธมิตร (Third party Service)	■ ใช้บริการระบบงานของหน่วยงานพันธมิตร	DMZ		สิทธิ์ผู้ดูแลระบบ/เจ้าของระบบ /สิทธิ์ผู้ปฏิบัติงาน /สิทธิ์บุคคล	■ ตรวจสอบประเมินความเสี่ยงด้านการใช้งานและการโจมตีจาก malware/ phishing/ social engineering ■ กำหนดมาตรการควบคุมเชิงป้องกันด้วยมาตรการสมัครขอใช้งานมีการยืนยันจากผู้บังคับบัญชา และให้เปลี่ยนรหัสผ่านใหม่ในครั้งแรกที่ล๊อกอิน ■ กำหนดมาตรการควบคุมด้วยการล๊อกบัญชีที่ทำงานผิดปกติ ■ กำหนดมาตรการแก้ไขด้วย กำหนดข้อปฏิบัติกรณีฉุกเฉิน และแจ้ง DGA

ตารางที่ 4.24 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
6	ระบบงานที่ให้บริการเฉพาะ (Specific Service)	■ ฮาร์ดแวร์ Rack Server ■ ซอฟต์แวร์ OS : Windows /Linux/VM Application : Conference Application Database : LDAP ■ Storage : NAS ■ ให้บริการระบบงานที่ทำงานเฉพาะด้าน สามารถใช้งานได้จากเครือข่ายภายในและภายนอก	DMZ	■ ฮาร์ดแวร์ใช้งานร่วมกันเฉพาะ VM ■ ฐานข้อมูลร่วมกัน LDAP	สิทธิ์ผู้ดูแลระบบ /เจ้าของระบบ /หน่วยงาน /สิทธิ์บุคคล	■ ตรวจสอบประเมินความเสี่ยงด้านฮาร์ดแวร์ / ซอฟต์แวร์ยี่ห้อรุ่นเดียวกันเหมือนกัน สามารถลอกการตั้งค่าอุปกรณ์ไปใช้อีกเครื่องหนึ่ง แล้วแก้ไขให้เหมาะสมอีกครั้ง ■ กำหนดมาตรการควบคุมเชิงป้องกันด้วยการตรวจสอบประจำวัน และเปิดให้เข้าใช้เฉพาะที่จำเป็น ■ กำหนดมาตรการควบคุมด้วยการจำกัดให้เข้าใช้จากภายนอกระหว่างเวลา 07.00 – 17.00 น. ■ กำหนดมาตรการแก้ไขด้วยการให้มีระบบสำรอง กำหนดข้อปฏิบัติกรณีฉุกเฉิน และแจ้งบริษัทเข้าแก้ไข

ตารางที่ 4.24 (ต่อ)

ลำดับ	ประเภท	คุณสมบัติและการทำงาน	พื้นที่เข้าถึง	บริการร่วมกัน	กำหนดสิทธิ์	แนวทางปฏิบัติในการรักษาความปลอดภัย
7	เว็บไซต์ (Website)	■ ฮาร์ดแวร์ Rack Server ■ ซอฟต์แวร์ OS : Windows/VM Application : .NET /Java Database : My SQL ■ Storage : NAS ■ ให้บริการระบบงานที่ทำงานเฉพาะด้าน สามารถใช้งานได้จากเครือข่ายภายในและภายนอก ■ ให้บริการเว็บไซต์ โฮสติ้ง จดโดเมน	DMZ	■ ฮาร์ดแวร์ใช้งานร่วมกันเฉพาะ VM ■ ฐานข้อมูลร่วมกัน	สิทธิ์ผู้ดูแลระบบ /เจ้าของระบบ /หน่วยงาน /สาธารณะ	■ ตรวจสอบประเมินความเสี่ยงการโจมตีผ่านเว็บไซต์ ■ กำหนดมาตรการควบคุมเชิงป้องกันด้วยการตรวจสอบประจำวัน และเปิดให้เข้าใช้เฉพาะที่จำเป็น และตรวจสอบการรับข้อมูลเข้า กำหนด session time ■ กำหนดมาตรการควบคุมด้วยการตั้งแม่ข่ายต่างหาก ■ กำหนดมาตรการแก้ไขด้วยการให้มีระบบสำรอง กำหนดข้อปฏิบัติกรณีฉุกเฉิน และแจ้งบริษัทเข้าแก้ไข

4.2.4.3 เปรียบเทียบแนวทางปฏิบัติในการรักษาความปลอดภัยข้อมูลสารสนเทศส่วนที่เหมือนกัน และต่างกัน

การเปรียบเทียบแนวทางปฏิบัติที่แตกต่างกันมี 2 ลักษณะ คือ

1. เปรียบเทียบระหว่างระบบประเภทแต่ละประเภท พบว่ามีช่องโหว่ จุดอ่อน และความเสี่ยงที่แตกต่างกัน วิธีการควบคุมแตกต่างกันตามคุณสมบัติ และลักษณะการทำงาน

2. เปรียบเทียบระหว่างระบบประเภทเดียวกัน พบว่าระบบประเภทเดียวกันมีข้อแตกต่างกันที่ฮาร์ดแวร์ ระบบปฏิบัติการ ระบบงาน ฐานข้อมูล การตั้งค่า โปรโตคอล พอร์ต และการกำหนดสิทธิ์ให้แต่ละระบบ

4.2.4.4 ปฏิบัติตามข้อกำหนดในการรักษาความปลอดภัยข้อมูลสารสนเทศ

ขั้นตอนปฏิบัติตามข้อกำหนดในการรักษาความปลอดภัยข้อมูลสารสนเทศขั้นตอนนี้หมายถึง การปฏิบัติตามข้อกำหนด 2 ระดับ คือ

1. ข้อกำหนดการรักษาความปลอดภัยข้อมูลสารสนเทศทั่วไป สำหรับอุปกรณ์และระบบประเภทนี้ ซึ่งได้มีการกำหนดไว้ในขั้นตอนก่อนหน้า

2. ข้อกำหนดการรักษาความปลอดภัยข้อมูลสารสนเทศที่เกี่ยวกับช่องโหว่เฉพาะตัวของรุ่น ฮาร์ดแวร์ ระบบปฏิบัติการ ระบบงาน ฐานข้อมูล เว็บไซต์ การกำหนดสิทธิ์ และความเชื่อถือที่กำหนดให้ระหว่างระบบที่มีการเรียกใช้

4.2.4.5 ทบทวน ตรวจสอบ ความเหมาะสมในการรักษาความปลอดภัยข้อมูลสารสนเทศ

การทบทวนตรวจสอบการรักษาความปลอดภัยข้อมูลสารสนเทศ โดยทั่วไปกระทำใน 3 ลักษณะ คือ

1. การตรวจสอบโดยวิเคราะห์ตามขั้นตอนการรักษาความปลอดภัย

2. การตรวจสอบโดยการทดสอบใช้งานจริง โดยเฉพาะการใช้งานจากเครือข่ายภายนอก และการใช้งานร่วมกับระบบงานอื่นที่อาจมีการเรียกใช้ในลักษณะที่มิได้กำหนดไว้

3. การตรวจสอบโดยการใช้ Scan tool ต่าง ๆ

4.3 แนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ

จากการศึกษาการดำเนินการตามกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศและปรับเปลี่ยนขั้นตอนให้เหมาะสมกับการดำเนินการภายในศูนย์ปฏิบัติการเครือข่าย สามารถกำหนดแนวทางในการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดมาตรฐาน ISO 27001 ดังนี้

4.3.1 ระบุประเภทของสินทรัพย์ข้อมูลสารสนเทศ

การระบุประเภทสินทรัพย์ข้อมูลสารสนเทศเป็นไปตามความเหมาะสมของแต่ละพื้นที่ โดยพิจารณาจากคุณสมบัติ หน้าที่การทำงานของระบบ การกำหนด Zone และระดับสิทธิ์ที่ต้องกำหนดให้กับระบบ

4.3.2 ดำเนินการรักษาความปลอดภัยข้อมูลสารเทศที่เหมาะสมกับอุปกรณ์และระบบแต่ละประเภท

เมื่อระบุประเภทของสินทรัพย์ข้อมูลสารสนเทศแล้ว สามารถระบุความเสี่ยงได้จากตารางความเสี่ยงแบ่งตามประเภทสินทรัพย์ และระบุความเสี่ยงจำเพาะของอุปกรณ์ และระบบ ซึ่งมีความแตกต่างกัน พิจารณาจากฮาร์ดแวร์ ระบบปฏิบัติการ ระบบงาน ฐานข้อมูล ระดับการกำหนดสิทธิ์ จากนั้นประเมินความเสี่ยง กำหนดมาตรการป้องกัน ควบคุม และแก้ไขความเสี่ยง ดำเนินการตรวจสอบปรับปรุง รวมทั้งกำหนดมาตรการตามมาตรฐาน ISO 27001

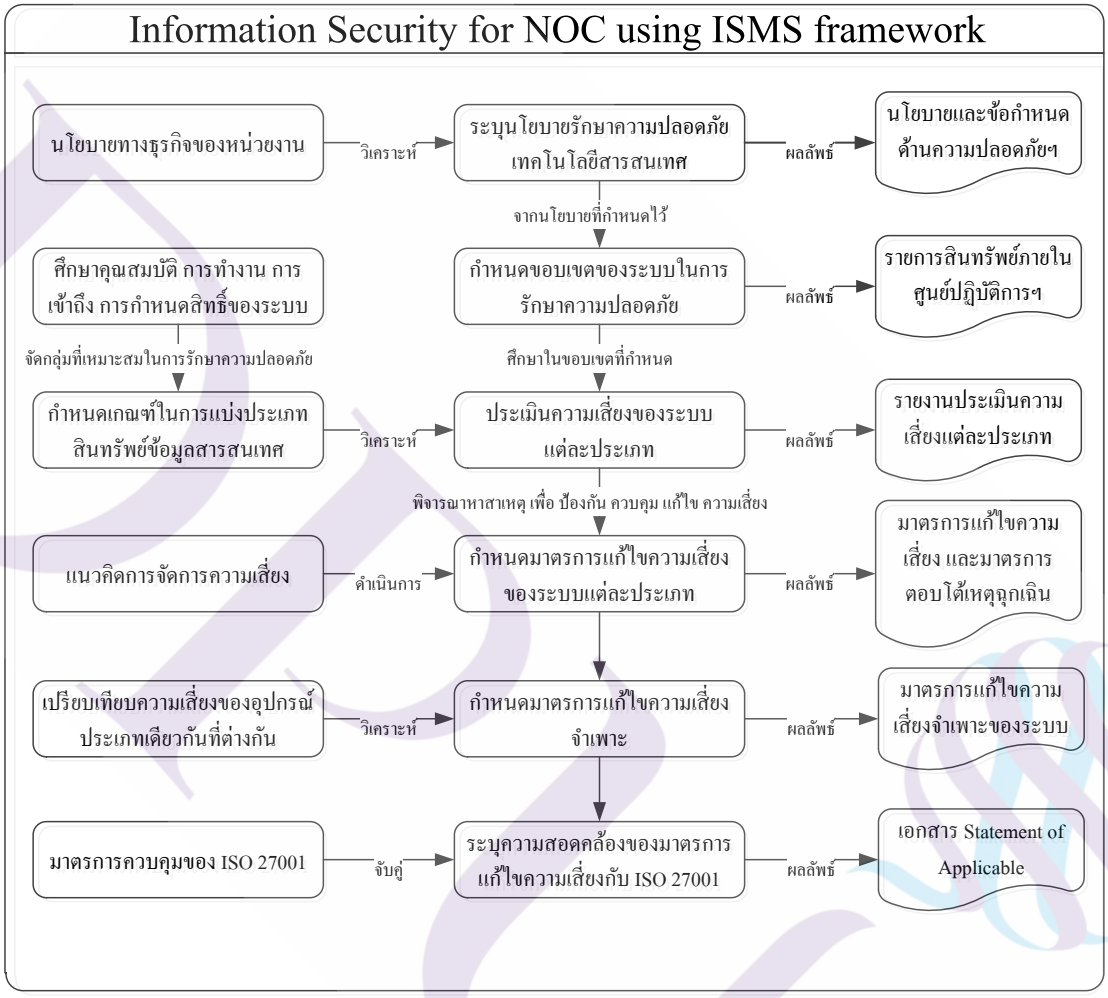
4.3.3 จัดทำเอกสาร Statement of Applicable (SoA)

การจัดทำเอกสารในขั้นตอนนี้เป็นการตรวจสอบว่ามีการปฏิบัติของมาตรการควบคุมตามมาตรฐานครบถ้วนหรือไม่สำหรับแต่ละอุปกรณ์

4.3.4 ดำเนินการตรวจสอบภายใน (Internal Audit)

การตรวจสอบภายในเป็นกระบวนเพื่อตรวจสอบตลอดทั้งระบบ เพื่อตรวจทานผลการดำเนินการตามมาตรการรักษาความปลอดภัย แบ่งเป็นขั้นตอนได้ดังนี้ ทบทวนรายละเอียดสินทรัพย์ข้อมูลสารสนเทศ, การตรวจสอบข้อกำหนดตามมาตรการควบคุม (Compliance testing), การตรวจสอบผลจากการปฏิบัติตามข้อกำหนด (Substantive testing), การตรวจวัดข้อผิดพลาดจากกลุ่มตัวอย่าง (Sampling) และจัดทำเอกสารและรายงาน (Report)

จากผลการศึกษาข้อปฏิบัติ กระบวนการ ข้อกำหนด และมาตรการรักษาความปลอดภัยต่าง ๆ สามารถสรุปแผนผังความสัมพันธ์ระหว่างกระบวนการดำเนินงานกับการนำกรอบแนวคิดการรักษาความปลอดภัยข้อมูลสารสนเทศมาใช้ในการรักษาความปลอดภัยศูนย์ปฏิบัติการเครือข่าย



ภาพที่ 4.2 แผนผังแสดงแนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ สำหรับห้องศูนย์ปฏิบัติการเครือข่าย

บทที่ 5
สรุปผลการดำเนินงาน

สรุปผลการศึกษา และทดสอบวิเคราะห์เบื้องต้นพบว่าสามารถนำไปใช้เป็นแนวทางปฏิบัติในกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศได้ โดยมีข้อจำกัด และเงื่อนไข จึงขอสรุปผลและข้อแนะนำ ดังนี้

5.1 สรุปผล และวิเคราะห์

5.1.1 ผลการศึกษาวิเคราะห์พบว่าการใช้กรอบแนวคิดการจัดการความปลอดภัยข้อมูลสารสนเทศเพื่อพัฒนาแนวทางรักษาความปลอดภัยภายในศูนย์ปฏิบัติการเครือข่าย สามารถกำหนดแนวทางขั้นตอนปฏิบัติสำหรับอุปกรณ์ และระบบที่มีคุณสมบัติและการทำงานคล้ายคลึงกันได้อย่างมีประสิทธิภาพในระดับหนึ่ง โดยการแบ่งประเภทอุปกรณ์และระบบที่เหมาะสมมีความสำคัญอย่างมากในการดำเนินการ อย่างไรก็ตามภายหลังดำเนินการตามแนวทางรักษาความปลอดภัยข้อมูลสารสนเทศของสินทรัพย์ข้อมูลสารสนเทศแต่ละประเภทแล้ว ต้องดำเนินการตรวจสอบแนวทางรักษาความปลอดภัยจำเพาะสำหรับแต่ละอุปกรณ์และระบบ ซึ่งจะมีข้อแตกต่างกันในรายละเอียด เพื่อให้การรักษาความปลอดภัยครบถ้วน มีประสิทธิภาพ

5.1.2 แนวทางรักษาความปลอดภัยข้อมูลสารสนเทศสำหรับสินทรัพย์ประเภทเดียวกันที่ใช้ร่วมกัน เช่น กระบวนการเข้าออกศูนย์ปฏิบัติการเครือข่าย การควบคุมโครงสร้างพื้นฐาน การควบคุมการใช้งานสื่อพกพา ช่องโหว่ของอุปกรณ์ และระบบประเภทเดียวกัน การกำหนดนโยบายรักษาความปลอดภัยบนเครือข่าย (Policy) การกำหนด IP และ VLAN ให้กับสินทรัพย์ข้อมูลประเภทเดียวกัน เป็นต้น สำหรับการรักษาความปลอดภัยข้อมูลสารสนเทศจำเพาะ เกิดจากช่องโหว่ของฮาร์ดแวร์ ระบบปฏิบัติการ ระบบงาน ฐานข้อมูล เฉพาะรุ่น นอกจากนี้ยังเกี่ยวข้องกับการปรับแต่งการทำงานของอุปกรณ์และระบบแต่ละประเภทซึ่งอาจมีการกระทบต่อการทำงาน จำเป็นต้องกำหนดนโยบายรักษาความปลอดภัยบนเครือข่ายที่แตกต่างกัน หรือบางครั้งปิดระบบรักษาความปลอดภัยของระบบปฏิบัติการเพื่อให้ระบบงานสามารถใช้งานได้

5.1.3 ข้อดีของการศึกษาพบว่า สามารถนำแนวทางรักษาความปลอดภัยดังกล่าวไปใช้จัดการความปลอดภัยข้อมูลสารสนเทศในภาพรวมได้อย่างรวดเร็ว สำหรับอุปกรณ์ และระบบที่ติดตั้งใหม่ และมีองค์ประกอบคล้ายคลึงหรือเหมือนกันในการทำงานสามารถนำข้อกำหนดแนวทางปฏิบัติไปใช้ได้ทันที ช่วยลดเวลาทดสอบ และดำเนินการด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ และมีการดำเนินการตามมาตรฐาน ISO 27001 ทำให้สามารถพัฒนาเพื่อขอใบรับรองได้อีกทางหนึ่ง

5.1.4 ข้อจำกัดของการศึกษาพบว่าไม่สามารถศึกษาซอฟต์แวร์ต่าง ๆ ที่ติดตั้งใช้งานภายในศูนย์ปฏิบัติการเครือข่ายฯ ได้อย่างเพียงพอที่จะกำหนดแนวทางรักษาความปลอดภัยสำหรับระบบงาน เนื่องจากหน่วยงานราชการมีการพัฒนาซอฟต์แวร์ที่ไม่เป็นไปตามกระบวนการมาตรฐาน และมีซอฟต์แวร์จำนวนมาก จึงกำหนดแนวทางรักษาความปลอดภัยทั่วไปสำหรับซอฟต์แวร์ ข้อจำกัดหรือจุดอ่อนที่สำคัญอีกประการหนึ่ง คือ สินทรัพย์ข้อมูลสารสนเทศที่มีรุ่นผลิตภัณฑ์แตกต่างกันมาก แม้จะเป็นยี่ห้อเดียวกันก็จะไม่สามารถใช้แนวทางรักษาความปลอดภัยข้อมูลสารสนเทศได้ เนื่องจากความแตกต่างของเทคโนโลยี และการนำแนวทางการรักษาความปลอดภัยแต่ละประเภทไปใช้อาจเกิดข้อผิดพลาดเนื่องจากการกำหนด และเลือกประเภทของอุปกรณ์ และระบบไม่เหมาะสม

เนื่องจากใช้มาตรฐาน ISO 27001 ในการศึกษาจึงมีความครอบคลุมระบบทั้งหมด แต่อาจขาดความลึกซึ้งเพื่อตัดสินใจว่าการรักษาความปลอดภัยข้อมูลสารสนเทศดังกล่าวเหมาะสมเพียงพอ หรือไม่

5.2 ปัญหา และอุปสรรค

5.2.1 การศึกษาโดยใช้ข้อมูลของสินทรัพย์ข้อมูลสารสนเทศภายในศูนย์ปฏิบัติงานเครือข่าย ซึ่งมีความอ่อนไหว และวัฒนธรรมองค์กรเกี่ยวกับกฎหมายที่มีการกำหนดโดยพฤตินัยไว้ว่า ถ้ายังไม่มีกฎระเบียบรองรับ หรือผ่านการพิจารณาของคณะกรรมการแล้วจะให้ยุติไว้ก่อน การขอข้อมูลเพื่อใช้ในการศึกษา และเผยแพร่จึงเป็นเรื่องยาก จึงขาดข้อมูลบางส่วน

5.2.2 การรักษาความปลอดภัยข้อมูลสารสนเทศเป็นเรื่องที่ซับซ้อน ไม่สามารถดำเนินการโดยมีความรู้เกี่ยวกับมาตรฐานการรักษาความปลอดภัยข้อมูลสารสนเทศเพียงอย่างเดียว ทั้งนี้ การนำไปใช้งานจริงต้องอาศัยทักษะการบริหารจัดการมากพอ ๆ กับกระบวนการรักษาความปลอดภัย

5.2.3 มาตรฐาน ISO 27001 เป็นมาตรฐานที่มีต้นฉบับภาษาอังกฤษ กำหนดขั้นตอนดำเนินการการศึกษาค้นคว้า และนำไปปฏิบัติต้องมีประสบการณ์ในการรักษาความปลอดภัยข้อมูลสารสนเทศในระดับหนึ่ง มิเช่นนั้นอาจเข้าใจคลาดเคลื่อน

5.2.4 การนำกระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศไปทดสอบใช้งานกับอุปกรณ์และระบบจะไม่ได้รับความร่วมมือ เพราะนอกจากเป็นความเสี่ยงแก่เจ้าของระบบแล้ว ยังพบว่าการเข้าใจระบบไม่เพียงพอจะทำให้การดำเนินการตามกระบวนการรักษาความปลอดภัยอาจขัดขวางการทำงานของระบบตามปกติ จึงสามารถทดสอบกับอุปกรณ์ และระบบที่ผู้ศึกษาเป็นเจ้าของระบบเท่านั้น

5.3 ข้อเสนอแนะในการศึกษาขั้นต่อไป

5.3.1 ควรศึกษาเกณฑ์การแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศเพื่อให้มีประสิทธิภาพในการนำไปปฏิบัติ จากการศึกษาพบว่าการแบ่งประเภทอุปกรณ์ และระบบโดยมีรายละเอียดที่เพียงพอเหมาะสมจะลดกระบวนการจัดการความปลอดภัยข้อมูลสารสนเทศจำเพาะของอุปกรณ์และระบบ เช่น เครื่องแม่ข่าย ยี่ห้อ HP รุ่น X ระบบปฏิบัติการ Y สำหรับติดตั้งระบบงานภายใน นอกจากนี้ยังเหมาะสมกับหน่วยงานที่มักมีการจัดซื้อทดแทนเป็นคราว ๆ โดยมียี่ห้อ รุ่น เดียวกัน

5.3.2 จากการศึกษาพบว่าการแบ่งประเภทสินทรัพย์ข้อมูลสารสนเทศตามระดับการรักษาความปลอดภัย และกำหนดแนวทางปฏิบัติตามระดับชั้นการรักษาความปลอดภัย จะได้แนวทางปฏิบัติต่ออุปกรณ์ และระบบในการรักษาความปลอดภัยที่เป็นมาตรฐานปฏิบัติ และจะทำให้การดำเนินการในแต่ละระบบเป็นไปในแนวทางเดียวกัน

5.3.3 เอกสารที่สำคัญและมีการพูดถึงบ่อยครั้ง คือ Statement of Applicable ใช้ในการตรวจสอบการดำเนินการตามข้อตกลงมาตรฐาน ซึ่งมาตรการควบคุมมีรายละเอียดในการดำเนินการมากกว่าการตรวจสอบว่ามีการดำเนินการหรือไม่ จึงเห็นควรให้ศึกษาเพื่อนำเอกสาร SoA มาใช้ให้มีประสิทธิภาพยิ่งขึ้น

5.3.4 จากการศึกษาพบว่าการนำไปปฏิบัติอาจมีปัญหาอุปสรรคต่าง ๆ จึงเห็นควรให้ดำเนินการศึกษาการปฏิบัติกับอุปกรณ์ประเภทใดประเภทหนึ่งจนจบกระบวนการ เพื่อทราบการดำเนินการครบถ้วนทุกขั้นตอน และสามารถนำไปปรับใช้กับการดำเนินการในส่วนอื่น ในที่นี้พิจารณาเห็นว่าระบบสื่อสารทางไกลผ่านจอภาพ มีการทำงานด้วยโปรโตคอลเฉพาะ การจัดเส้นทางเครือข่ายแยกออกจากระบบงานอื่น และมีการวางแผนที่จะติดตั้งไฟร์วอลล์ต่างหากให้แก่ระบบดังกล่าว จึงเห็นว่าเหมาะสมที่จะกำหนดเป็นกรณีศึกษาต่อไป

5.3.5 จากการศึกษากระบวนการรักษาความปลอดภัยข้อมูลสารสนเทศ พบว่าการรักษาความปลอดภัยมีลักษณะเหมือนเครื่องกีดขวางเป็นชั้น ๆ ตามลำดับขั้นตอน และมีระดับการรักษาความปลอดภัย ระดับชั้นความลับ การศึกษาการรักษาความปลอดภัยในแต่ละชั้นจะช่วยให้สามารถเลือกใช้วิธีการรักษาความปลอดภัยในแต่ละระดับชั้นเป็นไปอย่างเหมาะสม

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

คณะอนุกรรมการเทคโนโลยีสารสนเทศสำนักงานศาลยุติธรรม (2561). *แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลยุติธรรม*. กรุงเทพฯ: สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม.

จตุชัย แพงจันทร์. (2553). *Master in security 2nd edition*. นนทบุรี: ไอ ดี ซี พรีเมียร์.

ภาษาต่างประเทศ

Amanda Athuraliya (2019). *5 Gap Analysis Tools to Identify and Close the Gaps in Your Business*. Retrieved Feb 10, 2019, from https://creately.com/blog/diagrams/gap-analysis-tools/

Bill Hayes (2003). *Conducting a Security Audit: An Introductory Overview*. Retrieved Feb 10, 2019, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=e3b7729b-8d2c-4c95871e-8c08e4cac1f1&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Department of Veterans Affairs, Federal Emergency Management Agency. (2017). *Step 3 : Vulnerability Assessment*. Retrieved Feb 10, 2019, from https://www.fema.gov/media-library-data/20130726-1524-20490-7825/fema452_step3.pdf

Gap analysis (2014). Retrieved Feb 10, 2019, from https://en.wikipedia.org/wiki/Gap_analysis.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements*. Retrieved Feb 10, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO/IEC 27001. (2014). Retrieved Feb 10, 2019, from https://en.wikipedia.org/wiki/ISO/IEC_27001

Kenneth, G. (2018). *A Step-By-Step Guide to Vulnerability Assessment.* Retrieved Feb 10, 2019, from https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/

Michael G.,S., & Mike,C. (2009). *Information Security Illuminated.* Missisauga, CA: Jones and Bartlett Publishers.

Planning for and Implementing ISO 27001. (2011). Retrieved Feb 10, 2019, from https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001

Security controls. (2018). Retrieved Feb 10, 2019, from https://en.wikipedia.org/wiki/Security_controls

The Information Policy Team, The National Archives. (2011). *Identifying Information Assets and Business Requirements*. Retrieved Feb 10, 2019, from https://www.nationalarchives.gov.uk/documents/identify-information-assets.pdf

Vasant Raval and Ashok Fichadia (2007). *RISKS, CONTROLS, AND SECURITY Concepts and Spplications.* Hoboken, NJ: Don Fowley Publishers.

ประวัติผู้เขียน

ชื่อ-นามสกุล	ภุมวุฒิ วิทวัสสำราญกุล
ประวัติการศึกษา	ปีการศึกษา 2543 สำเร็จการศึกษาระดับปริญญาตรี สาขาวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยรังสิต
ตำแหน่ง และสถานที่ทำงานปัจจุบัน	นักวิชาการคอมพิวเตอร์ชำนาญการ ส่วนระบบเครือข่ายคอมพิวเตอร์ สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม