วารสาร Mahidol R2R e-Journal ปีที่ 10 ฉบับที่ 1 ประจำเดือนมกราคม-เมษายน 2566
Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

ความสำคัญของมาตรฐาน ISO/IEC27001 และระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศในโรงพยาบาล

The Importance of ISO/IEC27001 Standard and Hospital Information Security Management System

จุฑามาศ อยู่เจริญ[1*] และ กิตติศักดิ์ แก้วบุตรดี[1]
CHUTHAMAT YUCHAREON[1*] and KITTISAK KAEWBOODDEE[1]

บทคัดย่อ

ในปัจจุบันได้มีการนำระบบสารสนเทศเข้ามาใช้ในการดำเนินธุรกิจต่าง ๆ เพื่อเพิ่มประสิทธิภาพในการทำงาน ความรวดเร็วในการให้บริการ รวมถึงความถูกต้องแม่นยำต่าง ๆ ของข้อมูล แต่การใช้ระบบสารสนเทศมักพบปัญหาในหลาย ๆ ด้าน เช่น ด้านความมั่นคงปลอดภัยของระบบ, ความมั่นคงปลอดภัยของข้อมูล หรือเสถียรภาพของระบบโครงสร้างพื้นฐานของระบบสารสนเทศ ดังนั้น การกำหนดนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศจึงมีความสำคัญอย่างยิ่งในการควบคุมความเสี่ยงที่อาจจะเกิดขึ้น เช่น ระบบสารสนเทศเพื่อการบริหารจัดการโรงพยาบาล เป็นระบบที่มีความสำคัญที่สุดในการให้บริการแก่ผู้ป่วยที่มารับการรักษาพยาบาลที่โรงพยาบาลศิริราช ดังนั้นการจัดหาเพื่อทำให้ระบบสามารถทำงานได้ตลอดเวลา เช่น การจัดการแหล่งจ่ายไฟฟ้าหลักที่ได้มาตรฐาน หรือแหล่งจ่ายไฟฟ้าสำรองแก่ศูนย์ข้อมูล (Data Center)

การจัดตั้งสถานที่เก็บข้อมูลไว้สำหรับกู้คืนข้อมูลเมื่อเกิดภัยพิบัติ (Disaster Recovery Site) เพื่อรองรับสถานการณ์ฉุกเฉินทำให้ระบบสามารถกลับมาให้บริการแก่ผู้ป่วยได้อย่างรวดเร็วอีกครั้ง เป็นต้น การจัดการบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลธุรกิจที่ดี ซึ่งได้มีการนำระบบการจัดการความเสี่ยงด้านระบบสารสนเทศมาใช้ทั้งในหน่วยงานธุรกิจของภาครัฐและเอกชน อีกทั้ง มาตรฐาน ISO ได้ถูกกำหนดและควบคุมโดยองค์การนานาชาติเพื่อเป็นระบบมาตรฐานสากล มาตรฐาน ISO/IEC27001 เป็นแนวทางเกี่ยวกับความเสี่ยงด้านระบบสารสนเทศเพื่อการกำหนดนโยบายและกระบวนการทำงานต่าง ๆ รวมทั้งการควบคุมที่เหมาะสมในการบริหารความเสี่ยง

ในธุรกิจโรงพยาบาล ระบบสารสนเทศถูกพัฒนาขึ้นเพื่อใช้ในการรวบรวมและจัดเก็บข้อมูลจากแหล่งต่าง ๆ ซึ่งโรงพยาบาลหลายแห่งได้มีการนำระบบสารสนเทศทางการแพทย์ (Medical Informatics) เข้ามาประยุกต์ใช้ เพื่อเพิ่มขีดความสามารถโดยมีการเชื่อมโยงฐานข้อมูลต่าง ๆ เข้าด้วยกัน เช่น เวชระเบียนผู้ป่วย ประวัติการรักษาหรือการใช้ยา เป็นต้น ดังนั้นข้อมูลระบบสารสนเทศของโรงพยาบาลจึงมีความสำคัญอย่างยิ่ง เพื่อป้องกันไม่ให้เกิดภัยคุกคามต่อระบบสารสนเทศ การจัดทำแนวทางในการจัดการควบคุมความมั่นคงปลอดภัยระบบสารสนเทศจึงเป็นเรื่องจำเป็นของโรงพยาบาล เพื่อให้ระบบมีเสถียรภาพด้านความมั่นคงปลอดภัยในด้านของข้อมูล และความน่าเชื่อถือของระบบ จึงได้ดำเนินการด้านนโยบายด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือ ISO/IEC27001 ซึ่งรวมไปถึงด้านความมั่นคงปลอดภัยของข้อมูล และสารสนเทศที่เกี่ยวข้อง มาเป็นวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่มีประสิทธิภาพสำหรับโรงพยาบาล

คำสำคัญ : ระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศในโรงพยาบาล, มาตรฐาน ISO/IEC27001, การบริหารจัดการความเสี่ยง

[1*] ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล

[1*]Siriraj Information Technology Department ,Faculty of Medicine Siriraj Hospital, Mahidol University

[1*] Corresponding Author: chuthamat.yuj@mahidol.edu

วารสาร Mahidol R2R e-Journal ปีที่ 10 ฉบับที่ 1 ประจำเดือนมกราคม-เมษายน 2566
Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

Abstract

At present, the information system has been used in various business operations to increase work efficiency, speed of service including the accuracy of the information. However, the use of information technology often encounters problems in many areas, such as security systems, data security, or stability of the infrastructure of information systems. Therefore, the security policy of information technology is very important in controlling the risk, such as information technology systems for hospital management. It is the most important system in providing services to patients at Siriraj Hospital. The organization should make the hospital system and infrastructure always highly available, such as the main power supply or backup power supply to the data center made with the standard. To establishing the Disaster Recovery Site (DR Site) to support emergency situations which allow the system to recover quickly. Risk management is an important strategic tool for good business governance principles. This has implemented risk management systems for information in both public and private business units, and the ISO standard has been defined and controlled by international organizations to be an international standard system. The ISO/IEC27001 standard is a guideline for information risk for policy-making and work processes including the appropriate controls for risk management.

In the hospital business, information systems were developed to be used to collect and store information from various sources. Hospitals applied electronic medical records (Medical Informatics) to increase capacity by linking various databases together such as patient medical records, treatment history, or medication, etc. So, hospital information systems are extremely important. Establishing guidelines for managing information security controls are necessary for the hospital in order to provide the system to be more stable and secure in terms of information security and system reliability. Therefore, we have implemented an information security management system (ISO/IEC27001), which includes information security and related information. This will lead to an effective security management system for the hospital.

Keywords: Information Security Management System in hospital, ISO/IEC27001 standard, Risk management

บทนำ

ปัจจุบันการรักษาความปลอดภัยของข้อมูลในองค์กรเป็นประเด็นที่สำคัญ ซึ่งแต่ละหน่วยงานมีความจำเป็นต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัยของข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญต่าง ๆ ขององค์กร ซึ่งการใช้ระบบสารสนเทศดังกล่าวนี้มักพบปัญหาในหลาย ๆ ด้าน เช่น ด้านความมั่นคงปลอดภัยของระบบ ดังนั้น การกำหนดนโยบายด้านความมั่นคงปลอดภัยทางระบบสารสนเทศจึงมีความสำคัญอย่างยิ่งในการควบคุมความเสี่ยงต่าง ๆ การจัดการบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลธุรกิจที่ดี ซึ่งได้มีการนำระบบการจัดการความเสี่ยงสารสนเทศมาใช้ทั้งในหน่วยงานธุรกิจของภาครัฐและเอกชน อีกทั้ง

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

มาตรฐาน ISO ได้ถูกกำหนดและควบคุมโดยองค์การนานาชาติเพื่อเป็นระบบมาตรฐานสากล มาตรฐาน ISO/IEC27001 เป็นแนวทางเกี่ยวกับความเสี่ยงด้านสารสนเทศเพื่อการกำหนดนโยบายและกระบวนการทำงานต่าง ๆ รวมทั้งการควบคุมที่เหมาะสมในการบริหารความเสี่ยง (International Organization for Standardization, [ISO], 2018)

ในการดำเนินงานของคณะแพทยศาสตร์ศิริราชพยาบาล ได้มีการพัฒนาระบบสารสนเทศขึ้นเพื่อใช้ในการเชื่อข้อมูล, เก็บรวบรวมข้อมูลที่มีความสำคัญต่าง ๆ เช่น เชื่อมต่อข้อมูลจากสำนักทะเบียนราษฎร์, ข้อมูลการรักษาพยาบาลผู้ป่วย, ข้อมูลการศึกษา และข้อมูลการวิจัยต่าง ๆ ตามพันธกิจของคณะแพทยศาสตร์ศิริราชพยาบาล ซึ่งโรงพยาบาลหลายแห่งไม่เพียงแต่คณะแพทยศาสตร์ศิริราชพยาบาลก็ได้มีการนำระบบสารสนเทศทางการแพทย์ (Electronics Medical Records) เข้ามาประยุกต์ใช้ เพื่อเพิ่มขีดความสามารถโดยมีการเชื่อมโยงฐานข้อมูลต่าง ๆ เข้าด้วยกัน เช่น เวชระเบียนผู้ป่วย ประวัติการรักษาหรือการใช้ยา เป็นต้น ดังนั้นระบบสารสนเทศของโรงพยาบาลจึงมีความสำคัญเป็นอย่างยิ่ง จึงต้องมีการควบคุมและป้องกันให้มีความมั่นคงปลอดภัยอยู่เสมอ เพื่อป้องกันไม่ให้เกิดภัยคุกคามต่อระบบสารสนเทศ การจัดทำแนวทางในการจัดการควบคุมความปลอดภัยระบบสารสนเทศจึงเป็นเรื่องจำเป็นของโรงพยาบาลทุกแห่ง เพื่อให้ระบบมีเสถียรภาพด้านความมั่นคงปลอดภัยของข้อมูล และมีกรอบนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อประโยชน์สูงสุดของทั้งผู้รับบริการและผู้ให้บริการ โดยการนำมาตรฐาน ISO/IEC27001 มาเป็นวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่มีประสิทธิภาพ

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) หรือ ISO/IEC27001 คือ มาตรการในการรักษาความปลอดภัยระบบสารสนเทศ ซึ่งเป็นหัวใจหลักในการบริหารจัดการระบบสารสนเทศขององค์กร และได้มีการนำมาตรการดังกล่าวมาใช้เป็นมาตรฐานในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศอย่างแพร่หลาย (กิตติศักดิ์ แก้วบุตรดี และ อัจฉรา กิจเดช, 2562) รวมถึงในธุรกิจโรงพยาบาลทั้งของภาครัฐและเอกชน เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศของโรงพยาบาลให้อยู่ในระดับมาตรฐานสากล และลดผลกระทบจากความเสียหายที่อาจเกิดขึ้นหากมีการโจมตีระบบสารสนเทศของโรงพยาบาล รวมถึงยังสามารถใช้เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของโรงพยาบาลด้วย และยังสามารถสร้างความเชื่อถือให้แก่ผู้รับบริการ ทำให้โรงพยาบาลมีมาตรฐานในระดับสากล

ความสำคัญของการจัดการความมั่นคงปลอดภัยสารสนเทศในโรงพยาบาล

ความมั่นคงปลอดภัยสารสนเทศถือเป็นเรื่องที่มีความสำคัญเป็นอันดับต้น ๆ ขององค์กรโดยเฉพาะในธุรกิจโรงพยาบาล เนื่องจากข้อมูลต่าง ๆ เช่น ข้อมูลผู้ป่วย ข้อมูลการรักษา ข้อมูลทางการเงิน ข้อมูลของการบริการต่าง ๆ ถือเป็นทรัพย์สินที่มีค่ามหาศาล ในปัจจุบันภัยคุกคามทางคอมพิวเตอร์มีการพัฒนารูปแบบการโจมตีที่รวดเร็วและหลากหลายมากขึ้น ซึ่งก่อให้เกิดผลกระทบต่อความมั่นคงและการเสถียรภาพการดำเนินงานขององค์กร ดังนั้นการกำหนดแนวทางในการบริหารจัดการเกี่ยวกับความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรจึงเป็นที่สำคัญ เช่น การบริหารจัดการความเสี่ยง กระบวนการทำงานอย่างเป็นระบบและสอดคล้องกับมาตรฐานสากล โดยมีการบริหารจัดการและติดตามผลความเสี่ยงอย่างต่อเนื่อง รวมถึงการตระหนักและให้ความสำคัญในด้านการป้องกันความเสี่ยงที่จะเกิดขึ้นกับข้อมูล ซึ่งการที่องค์กรมีสารสนเทศที่ดี (Good

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

Information) ทั้งความถูกต้องสมบูรณ์ และความชัดเจน อาจต้องคำนึงถึงการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security) ด้วย รวมถึงการรักษาความปลอดภัยในคอมพิวเตอร์ส่วนบุคคล ระบบฐานข้อมูลและเครือข่ายการสื่อสารข้อมูล การวิเคราะห์ความเสี่ยง การป้องกันทางกายภาพ ประเด็นด้านกฎหมาย จรรยาบรรณและความตระหนักด้านความปลอดภัยในระบบคอมพิวเตอร์ (กิตติศักดิ์ แก้วบุตรดี และอัจฉรา กิจเดช, 2561)

ปัจจุบันการใช้ประโยชน์จากระบบสารสนเทศในทางการแพทย์ได้มีการเปลี่ยนแปลงเป็นอย่างมาก โรงพยาบาลต่าง ๆ เริ่มมีการใช้ระบบสารสนเทศมาประยุกต์ใช้กับข้อมูลผู้ป่วย การตรวจทางห้องปฏิบัติการ รวมถึงการดูข้อมูลหัตถการทางการแพทย์ ซึ่งการเปลี่ยนแปลงดังกล่าวส่งผลให้เสถียรภาพและความปลอดภัยของระบบสารสนเทศโรงพยาบาลมีความสำคัญเป็นอย่างมาก เพราะระบบสารสนเทศได้ถูกนำมาใช้กับการตรวจวินิจฉัย และการวางแผนการรักษาคนไข้ ต่างจากในอดีตที่ใช้ในการคิดเงิน พิมพ์ใบเสร็จและจัดซื้อเท่านั้น การที่ระบบสารสนเทศของโรงพยาบาลขัดข้องไม่ว่าจะด้วยสาเหตุอันใดก็ตามเพียง 1 วัน ก็อาจจะส่งผลกระทบต่อชีวิตและความปลอดภัยของผู้ป่วยเป็นจำนวนมาก และทางโรงพยาบาลไม่อาจจะปฏิเสธความรับผิดชอบได้ รวมถึงอาจส่งผลกระทบต่อความเชื่อมั่นของสาธารณชนในความปลอดภัยของระบบกับการให้บริการทางการแพทย์ในระดับประเทศได้

ความเสี่ยงของระบบสารสนเทศ เป็นความเสี่ยงที่เกิดจากองค์กรได้นำระบบสารสนเทศมาใช้ในการขับเคลื่อนและดำเนินงานอย่างกว้างขวาง ระบบสารสนเทศจึงกลายเป็นโครงสร้างพื้นฐานของการดำเนินธุรกิจและการทำธุรกรรมต่าง ๆ ขององค์กร ดังนั้นการนำระบบสารสนเทศมาใช้ในองค์กรจึงมีความสำคัญต่อองค์กรอย่างมาก จนอาจกล่าวได้ว่า IT Risk คือ Business Risk นั่นเอง (จิตตกานต์ บุญศิริทิวัตถ์ และ โกวิท รพีพิศาล, 2560)

ภัยคุกคามระบบสารสนเทศ คือสิ่งที่ก่อให้เกิดอันตรายต่อทรัพยากรคอมพิวเตอร์ ซึ่งผู้ใช้คอมพิวเตอร์เป็นผู้ที่ทำให้เกิดความเสียหายของข้อมูล ไม่ว่าจะเป็นส่วนใดส่วนหนึ่งหรือทั้งหมดของข้อมูล เมื่อข้อมูลนั้นถูกคุกคามโดยไม่ได้มีการป้องกันที่รัดกุม จะเป็นสาเหตุให้ข้อมูลนั้นเกิดการเสียหาย จากการโจมตีของกลุ่มที่ไม่หวังดี เช่น จากบุคคลภายในองค์กร หรือกลุ่มเจาะระบบ (Hacker) อย่างไรก็ตาม หากมีการจัดการข้อมูลที่ดี ทำให้ข้อมูลปลอดภัยรัดกุมอยู่เสมอ ภัยต่าง ๆ ก็ไม่สามารถที่จะทำให้ข้อมูลเสียหายได้ (ศราวุฒิ จันทะคัด, 2554; University of South Carolina Board of Trustees, Division of Information Technology, 2014)

การจัดการความเสี่ยงของระบบสารสนเทศในโรงพยาบาล การจัดการความเสี่ยงของระบบสารสนเทศทั้งหน่วยงานธุรกิจและหน่วยงานของรัฐจำนวนมากอาจจะมองข้ามการจัดการปัญหาเรื่องความปลอดภัยของข้อมูล เนื่องจากเป็นงานที่มีเทคนิคค่อนข้างซับซ้อน อย่างไรก็ตาม การจัดการความเสี่ยงของระบบสารสนเทศเป็นสิ่งที่จำเป็นต่อองค์กร ดังนั้นองค์กรต้องสร้างความมั่นคงปลอดภัยในระบบสารสนเทศให้มีความเสี่ยงน้อยที่สุด โดยกำหนดมาตรการรักษาความปลอดภัยขององค์กร โดยเฉพาะอย่างยิ่งองค์กรต่าง ๆ ที่ต้องสามารถปรับตัวและตอบรับกับสภาพปัจจุบันที่มีการเปลี่ยนแปลงอย่างรวดเร็วอยู่เสมอ หากระบบสารสนเทศขององค์กรถูกโจมตีไม่ว่าทางตรงหรือทางอ้อม จะทำให้เกิดผลเสียต่อองค์กรและการดำเนินงานต่าง ๆ ได้ เช่นหากข้อมูลรั่วไหลองค์กรอาจจะถูกฟ้องร้อง และถูกเรียกค่าเสียหายจากเจ้าของข้อมูลได้ หรือถ้าถูกมัลแวร์โจมตี ซึ่งมัลแวร์เป็นซอฟต์แวร์ที่เจตนาออกแบบมาเพื่อสร้างความเสียหายให้กับคอมพิวเตอร์แม่ข่าย, เครื่องคอมพิวเตอร์ลูกข่าย หรือเครือข่ายคอมพิวเตอร์ เป็นต้น โดยเฉพาะอย่างยิ่ง

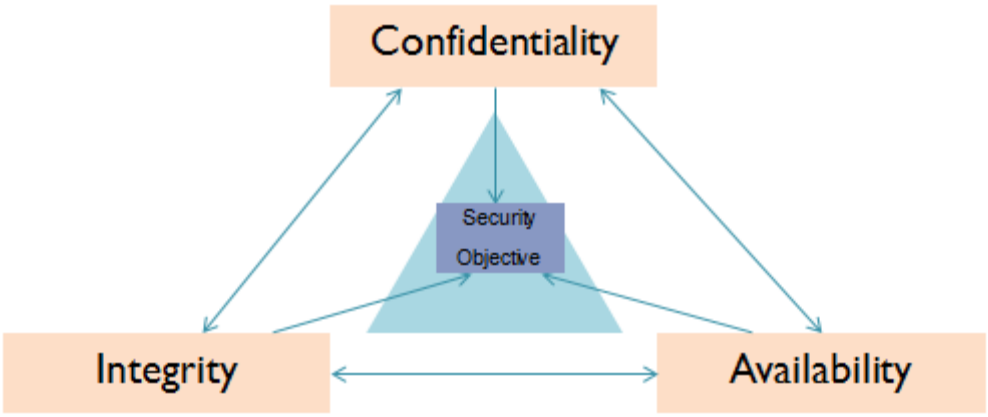
Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

สถานการณ์ในปัจจุบัน ความถูกต้องและความรวดเร็วของข้อมูลข่าวสารมีความสำคัญมากสำหรับการบริการทางการแพทย์ เพื่อที่จะตอบสนองความต้องการของผู้ที่มารับบริการได้อย่างสะดวกและรวดเร็วมากขึ้น ดังนั้นเพื่อให้มีความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร จึงควรมีนโยบายรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรเพื่อนำมาใช้ในการบริหารงาน ให้เกิดเสถียรภาพและภาพลักษณ์ความเชื่อมั่นที่ดีต่อองค์กร มีการรักษาความปลอดภัยข้อมูลของธุรกิจ ที่มีผลกระทบกับค่าใช้จ่ายหากธุรกิจต้องหยุดชะงัก

ระบบสารสนเทศโรงพยาบาล ถูกพัฒนาขึ้นเพื่อรวบรวมและจัดเก็บข้อมูลจากแหล่งข้อมูลต่าง ๆ ทั้งภายในและภายนอกโรงพยาบาลอย่างมีหลักเกณฑ์ ตามกฎ ระเบียบ ข้อบังคับและมาตรฐานของระบบรับรองคุณภาพต่าง ๆ เพื่อนำมาประกอบผลและจัดรูปแบบให้ได้สารสนเทศที่ช่วยสนับสนุนการทำงานและการตัดสินใจในด้านต่าง ๆ ของผู้บริหาร เพื่อให้การดำเนินงานของโรงพยาบาลเป็นไปอย่างมีประสิทธิภาพทำให้บุคลากรสามารถปฏิบัติงานได้สะดวกและรวดเร็ว มีเวลาในการให้บริการผู้ป่วยมากขึ้น รวมถึงมีเวลาในการพัฒนาคุณภาพบริการให้ดีขึ้น

องค์ประกอบของความมั่นคงปลอดภัยสารสนเทศ

ความมั่นคงปลอดภัยของสารสนเทศนั้นมีองค์ประกอบด้วยกัน 3 ประการ คือ ความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ทรัพย์สิน (Asset) ที่มีความมั่นคงปลอดภัยต้องประกอบด้วยองค์ประกอบทั้งสามอย่าง ไม่ว่าทรัพย์สินนั้นจะเป็นสิ่งที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย หรือทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูล เป็นต้น (Al-Zahawi, 2019) ดังภาพที่ 1



ภาพที่ 1 องค์ประกอบของความมั่นคงปลอดภัยสารสนเทศ

ความลับ (Confidentiality) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการรักษาความลับของของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้สามารถเข้าถึงและเข้าใจความหมายได้เฉพาะผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้น ๆ การรักษาความลับให้กับข้อมูลเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ หลักการสำคัญของการรักษาความลับคือ ผู้ที่มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถ

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

เข้าถึงข้อมูลได้ ระบบรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีประสิทธิภาพ ต้องมีมาตรการตรวจสอบสิทธิก่อนเข้าถึง เพื่อยืนยันให้แน่ใจก่อนว่าผู้ที่ร้องขอมีสิทธิหรือได้รับอนุญาตให้เข้าถึงสารสนเทศ หรือระบบงานนั้นได้ กลไกพื้นฐานที่คุ้นเคยกันเป็นอย่างดี คือการใช้รหัสผ่าน (Password) ในการพิสูจน์ตัวตนและสิทธิที่ได้รับอนุญาต นอกจากมาตรของการตรวจสอบสิทธิ การกำหนดชั้นความลับเป็นระดับต่าง ๆ ตามความสำคัญก็สามารถช่วยให้การบริหารจัดการมีประสิทธิภาพมากขึ้น ตัวอย่างเช่น การควบคุมเอกสารคุณภาพของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลได้มีการกำหนดชั้นความลับของสารสนเทศออกเป็น 4 ระดับ ประกอบด้วย ระดับชั้นความลับสุดยอด (Top Secret) ระดับชั้นความลับ (Secret) ระดับชั้นข้อมูลสำหรับใช้ภายในองค์กร (Internal Use) และระดับชั้นสารธารณะ (Public) ชั้นความลับต่าง ๆ นี้จะต้องมีเกณฑ์พิจารณาที่ชัดเจน ว่าสารสนเทศลักษณะใดอยู่ในชั้นความลับใดที่กำหนดไว้ พร้อมทั้งกำหนดแนวทางการระบุชั้นความลับ การจัดเก็บ และการสื่อสารข้อมูลสารสนเทศในแต่ละชั้นความลับอย่างชัดเจน มาตรการทางเทคนิคที่ใช้ในการปกป้องความลับ เช่น การเข้ารหัส (Encryption) ก็สามารถนำมาใช้เพิ่มความแข็งแกร่งให้กับมาตรการปกป้องสารสนเทศที่ต้องการมาตรการดูแลอย่างเข้มงวดได้ ทั้งนี้การรักษาความลับที่เป็นการรักษาความมั่นคงปลอดภัยของสารสนเทศในภาคธุรกิจก็ให้ความสำคัญกับการรักษาความลับทางธุรกิจ ประชาชนทั่วไปก็ต้องการปกป้องข้อมูลส่วนตัวตามสิทธิขั้นพื้นฐานเช่นเดียวกัน จากข่าวการละเมิดมาตรการป้องกันของระบบคอมพิวเตอร์เข้าไปเจาะระบบทั้งในประเทศและต่างประเทศ แสดงให้เห็นว่ามาตรการที่มีอยู่นั้นยังมีจุดอ่อนที่ผู้ไม่ประสงค์ดีที่มีความรู้บุกรุกผ่านช่องโหว่ดังกล่าว

ความถูกต้องสมบูรณ์ (Integrity) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการตรวจสอบความครบถ้วนสมบูรณ์ของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความถูกต้องสมบูรณ์และสามารถตรวจสอบความครบถ้วนสมบูรณ์นั้นได้ เช่น หากมีการแก้ไขไฟล์ที่ถูกสร้างขึ้นแล้วมีการส่งผ่านไฟล์นั้นเข้าสู่เครือข่ายคอมพิวเตอร์ ผู้ที่เกี่ยวข้องจะต้องสามารถตรวจสอบได้ว่าไฟล์นั้นว่าถูกแก้ไขเปลี่ยนแปลงไประหว่างการส่งผ่านช่องทางการสื่อสารหรือไม่ การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ (Integrity) เป็นสิ่งสำคัญที่จะสะท้อนถึงความน่าเชื่อถือของสารสนเทศนั้น ๆ ในเชิงหลักการระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใด ๆ ต่อข้อมูลนั้น ซึ่งข้อมูลต่าง ๆ ล้วนมีความสำคัญมากเพราะสามารถใช้เป็นหลักฐานในการพิสูจน์สิ่งต่าง ๆ หากมองในแง่ความมั่นคงปลอดภัยของสารสนเทศแล้ว ข้อมูลนี้จำเป็นต้องได้รับการปกป้องดูแลความถูกต้องสมบูรณ์และความน่าเชื่อถือ หากข้อมูลถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดีย่อมส่งผลเสียต่อเจ้าของข้อมูลอย่างหลีกเลี่ยงไม่ได้ ตัวอย่างเช่น ข้อมูลผู้ป่วย หรือข้อมูลที่สำคัญที่เกี่ยวข้องกับการรักษาพยาบาลของผู้ป่วย หลังจากที่นำเข้าระบบแล้ว จะต้องไม่ถูกแก้ไขหรือปรับปรุงโดยผู้ที่ไม่ได้รับอนุญาต เป็นต้น

ความพร้อมใช้งาน (Availability) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการรักษาความพร้อมใช้ของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความพร้อมใช้อยู่เสมอ ทำให้ผู้ใช้ที่มีสิทธิ์เข้าถึงและใช้งานทรัพยากรสารสนเทศนั้น ๆ สามารถเข้าใช้งานได้ เช่น ลูกค้าสามารถเข้าถึงและใช้งานบริการนั้นได้เสมอ และอาจหมายรวมถึงเจ้าหน้าที่ที่เกี่ยวข้องสามารถเข้าถึงและบริหารจัดการซอฟต์แวร์นั้นได้ เป็นต้น อุปสรรคที่บั่นทอนความพร้อมใช้งานของระบบคอมพิวเตอร์จำแนกได้ 2 แบบ คือ 1) การที่ระบบ

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

คอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service) 2) ระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of data processing capability) ระบบคอมพิวเตอร์ปฏิเสธการให้บริการอาจเกิดจากการกระทำของผู้ใช้ระบบ ผู้บุกรุกที่มีเจตนาร้าย หรือเกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหวทำให้ระบบคอมพิวเตอร์เสียหาย ตัวอย่างการเตรียมความพร้อมเพื่อรับมือกับเหตุการณ์ที่ไม่อาจคาดคิดของฝ่ายสารสนเทศคณะแพทยศาสตร์ศิริราชพยาบาลได้ตระหนักถึงภัยคุกคามต่างๆ มีการจัดเตรียมแผนกู้คืนจากความเสียหาย (Disaster Recovery Plan) ไว้รองรับ และซักซ้อมเพื่อเตรียมความพร้อมรับมือกับเหตุการณ์ที่ไม่อาจคากคิดอยู่เป็นประจำทุกปี โดยมีการจำลองเหตุการณ์ๆ เช่น ระบบคอมพิวเตอร์ และระบบเครือข่ายที่ให้บริการผู้ป่วยไม่สามารถใช้งานได้ รวมไปถึงการซักซ้อมสำหรับเหตุการณ์ไฟไหม้ศูนย์ข้อมูลซึ่งเป็นหัวใจหลักของการให้บริการระบบสารสนเทศก็ถูกทดสอบด้วยเช่นกัน

ISO/IEC27001 (Information Security Management System ISMS) คืออะไร และจำเป็นอย่างไรกับโรงพยาบาล

ISO/IEC27001:Information Security Management System หรือ ISMS เป็นมาตรฐานสากลที่กล่าวถึง มาตรฐานของระบบบริหารจัดการเพื่อความมั่นคงปลอดภัยของข้อมูล โดยจุดประสงค์ของมาตรฐานเพื่อจะทำให้องค์กรสามารถบริหารจัดการทางด้านความปลอดภัยได้อย่างมีระบบเหมาะสมต่อการดำเนินธุรกิจขององค์กร โดยที่องค์กรต้องทำการวิเคราะห์ความเสี่ยงของระบบจากภัยคุกคามและจุดอ่อนต่าง ๆ ในระบบ จากนั้นจึงวิเคราะห์เพื่อเลือกแนวทางการควบคุมและป้องกันสารสนเทศต่าง ๆ อย่างเหมาะสม โดยในตัวมาตรฐานก็จะมีแนวทางที่เรียกว่า Code of Practice ให้ใช้งานเพื่อควบคุมความเสี่ยงต่าง ๆ ขณะเดียวกันมาตรฐานนี้ก็ยังกำหนดให้องค์กรจะต้องควบคุมดูแลระบบการรักษาความมั่นคงปลอดภัย และกลไกในการพัฒนาอย่างต่อเนื่องด้วย ISO/IEC27001 เป็นมาตรฐานที่ดีที่สุดในการจัดการด้านระบบการรักษาความปลอดภัยข้อมูลองค์กร มาตรฐานนี้สามารถสร้างกลยุทธ์และกำหนดทิศทางสำหรับการประเมิน การวัดค่าและการป้องกันการคุกคามจากภายนอกโดยผ่านกระบวนการจัดการความเสี่ยงของมาตรฐานได้ ในขณะที่การนำระบบ ISMS ไปปฏิบัตินั้นจะมีความแตกต่างกันไปในแต่ละองค์กร แต่มีหลักการพื้นฐานของ ISMS ที่ทุกองค์กรจะต้องปฏิบัติตามเพื่อให้เกิดประสิทธิภาพในการปกป้องทรัพย์สินสารสนเทศขององค์กร ขั้นตอนแรกของการดำเนินการระบบ ISMS อย่างประสบผลสำเร็จ คือ การทำให้ผู้มีส่วนได้เสียที่สำคัญ (key stakeholders) ตระหนักถึงความจำเป็นของการรักษาความปลอดภัยของข้อมูล เพราะหากไม่ได้รับความร่วมมือจากผู้ที่เกี่ยวข้องทั้งหมดขององค์กร ซึ่งล้วนแต่เป็นผู้ที่ต้องปฏิบัติตาม ตรวจสอบและกำกับดูแล และการคงรักษาระบบ ISMS เป็นเรื่องยากที่จะประสบความสำเร็จในการให้ได้มาและรักษาไว้ซึ่งการได้รับการรับรองมาตรฐาน ISMS (กิตติศักดิ์ แก้วบุตรดี และ อัจฉรา กิจเดช, 2562) ดังภาพที่ 2

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

ภาพที่ 2 ISO/IEC27001 Compliance Steps

เพื่อให้ระบบ ISMS ขององค์กรมีประสิทธิผล องค์กรนั้น ๆ ต้องทำการวิเคราะห์ความจำเป็นด้านการรักษาความปลอดภัยสำหรับแต่ละทรัพย์สินสารสนเทศ และนำการควบคุมที่เหมาะสมต่าง ๆ มาใช้เพื่อให้สามารถเก็บรักษาสินทรัพย์ดังกล่าวไว้ได้อย่างปลอดภัย สินทรัพย์สารเทศทั้งหมดไม่สามารถที่จะใช้วิธีการควบคุมเดียวกันได้ เพราะข้อมูลของแต่ละองค์กรมีรูปแบบ และขนาดที่แตกต่างกัน การควบคุมเพื่อการรักษาความปลอดภัยของข้อมูลก็เช่นเดียวกันที่ย่อมต้องแตกต่างกันตามความเหมาะสม การนำระบบ ISMS มาปฏิบัตินั้นไม่ได้เป็นโครงการที่มีระยะเวลาคงที่ตายตัว เพื่อให้องค์กรปลอดภัยจากภัยคุกคามทางข้อมูลต่าง ๆ ระบบ ISMS จำเป็นที่จะต้องเติบโตและพัฒนาอย่างต่อเนื่องเพื่อสนองตอบต่อสภาพทางเทคนิคที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ด้วยเหตุนี้ การประเมินซ้ำอย่างต่อเนื่องของระบบการจัดการความปลอดภัยของข้อมูลจึงเป็นสิ่งที่ต้องทำอย่างขาดไม่ได้ การทดสอบและการประเมินระบบ ISMS ที่บ่อยครั้ง ช่วยให้องค์กรสามารถที่จะรู้ได้ว่าข้อมูลต่าง ๆ ของพวกเขานั้นยังคงได้รับการปกป้องเป็นอย่างดี หรือจำเป็นต้องมีการปรับเปลี่ยนแก้ไขใด ๆ หรือไม่

จากข้อมูลดังกล่าว ISO/ IEC27001: Information Security Management System หรือ ISMS จึงถือเป็นมาตรฐานในการบริหารจัดการเพื่อความมั่นคงปลอดภัยของข้อมูลในโรงพยาบาลได้อย่างเหมาะสม โดยเฉพาะอย่างยิ่งสถานการณ์ในปัจจุบัน ความถูกต้องและความรวดเร็วของข้อมูลมีความสำคัญมากสำหรับการบริการทางการแพทย์ ซึ่งความเสี่ยงด้านระบบสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย ส่งกระทบต่อการรักษาผู้ป่วย ทำให้ข้อมูลผิดพลาดไม่ถูกต้องตรงกัน ข้อมูลที่สำคัญไม่อยู่ระบบ ข้อมูลที่จำเป็นและ

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

สำคัญไปถึงผู้ป่วยหรือผู้ให้บริการล่าช้า จนทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย อีกทั้งความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วยเป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศของโรงพยาบาล หรือใช้ข้อมูลต่าง ๆ ของโรงพยาบาลเกินกว่าสิทธิ์ของตนเอง และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้ หรือความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติ หรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น รวมไปถึงความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านระบบสารสนเทศ อีกทั้งเรื่องของการลดผลกระทบจากความเสียหายที่อาจเกิดขึ้นหากมีการโจมตีระบบสารสนเทศของโรงพยาบาล ดังนั้นโรงพยาบาลหรือองค์กรต่าง ๆ จึงต้องการมาตรฐานที่สามารถจัดการกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

องค์ประกอบที่ก่อให้เกิดความสำเร็จของการดำเนินงานระบบ ISO/IEC27001

การตรวจประเมินภายใน (Internal Audit ISO/IEC27001) เป็นกิจกรรมที่จัดการระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System: ISMS) การตรวจสอบภายในเป็นหัวใจสำคัญของการกำกับดูแลกิจการที่ดี และมีบทบาทสำคัญในการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจสอบภายในเป็นเครื่องมือสำคัญในการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ โดยผู้ตรวจสอบภายในสามารถรายงานเกี่ยวกับประเด็นการประเมินความเสี่ยงที่มีความสำคัญ และรายงานสิ่งที่ต้องปรับปรุงภายในองค์กรให้ผู้บริหารทราบถึงความเสี่ยงต่าง ๆ ให้ผู้บริหารสามารถรับรู้ถึงทิศทางการบริหารจัดการองค์กร นอกจากนี้ผู้ตรวจสอบภายในยังมีส่วนเป็นอย่างมากในการช่วยการปรับปรุงระบบการควบคุมภายในความสำคัญดังที่กล่าวมานี้ทำให้ทีมผู้ตรวจสอบภายในสามารถเป็นที่ปรึกษาในองค์กร และเป็นเครื่องมือสำหรับกระตุ้นการปรับปรุงแนวทางการปฏิบัติงานขององค์กรได้เป็นอย่างดี (Pedneault, 2009) ISO/IEC27001 มีภาพรวมของการวางแผนแบ่งเป็น 7 ขั้นตอนดังนี้

1. เตรียมบุคลากรที่จะทำหน้าที่เป็นผู้ตรวจประเมินภายใน (Internal auditor ISO/IEC27001) โดยผู้ตรวจประเมินเหล่านี้จะต้องมีความรู้และเข้าใจในข้อกำหนด (Requirements) ของ ISO/IEC27001 ว่าแต่ละข้อกำหนดมีเจตนารมณ์อย่างไร และควรจะดูหลักฐานอะไรเพื่อยืนยันว่าได้ปฏิบัติตามข้อกำหนดเหล่านั้น

2. กำหนดช่วงเวลาที่จะทำการตรวจประเมินประเมินภายในไว้ล่วงหน้า โดยส่วนใหญ่นิยมตรวจปีละ 2 ครั้ง และมีการแจ้งกำหนดการตรวจประเมิน (Audit Schedule) ล่วงหน้าไปยังหน่วยงานที่อยู่ภายในขอบเขต (Scope) ของการทำระบบ เพื่อให้หน่วยงานได้รับทราบและเตรียมตัว เตรียมข้อมูลไว้รับการตรวจประเมินภายใน

3. กำหนดขอบเขตของการตรวจประเมิน โดยกำหนดเป็นพื้นที่หน่วยงาน หรือระบบงานให้ชัดเจน เพื่อจะได้วางแผนตรวจประเมินโดยพิจารณาถึงขนาดและความซับซ้อนของระบบงานหรือหน่วยงานที่ไปตรวจ รวมถึงการจัดเวลาและผู้ตรวจประเมินที่มีทักษะและความสามารถตรงกับภาระกิจได้อย่างเหมาะสม

4. หากเป็นการตรวจประเมินภายในครั้งแรก ควรนำ Gap Analysis ISO/IEC27001 มาเป็นแนวทางการวางแผน ให้กำหนดสิ่งที่รายงาน Gap Analysis โดยระบุว่าสิ่งใดที่ยังไม่ได้ทำหรือยังไม่มี เช่น ยังไม่มีนโยบายความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษร เป็นต้น

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

5. ถ้าเป็นการตรวจประเมินภายในครั้งที่ 2 เป็นต้นไป การวางแผนตรวจประเมินภายในควรดูผลของการตรวจประเมิน ครั้งที่ผ่านมาประกอบ เพื่อให้ทราบถึงปัญหาอุปสรรค เช่น ในแผนให้เวลามากหรือน้อยเกินไป ผู้ตรวจถามตรงประเด็นหรือไม่ ฯลฯ นอกจากนี้ให้ตรวจสอบว่าการตรวจประเมินภายในครั้งที่ผ่านมาพบข้อบกพร่องที่หน่วยงานใดหรือจุดใดมากที่สุด เพื่อจะได้ตรวจสอบว่าหน่วยงานดังกล่าวได้แก้ปัญหาเหล่านั้นหรือยัง เป็นต้น

6. วางแผนการตรวจประเมินภายใน (Internal Audit) โดยพิจารณาว่าแต่ละหน่วยงานจะถูกตรวจข้อกำหนด ISO/IEC27001ใด จุดสำคัญคือผู้ที่วางแผนจะต้องเข้าใจในข้อกำหนด และบริบทของหน่วยงานที่ถูกตรวจ ผลที่ได้คือวางแผนตรวจประเมินภายในได้ครอบคลุม ครบถ้วนและกำหนดเวลาได้เหมาะสม

7. เมื่อจัดทำแผนการตรวจประเมินภายใน (Internal audit ISO/IEC27001) แล้ว ให้เสนอตัวแทนฝ่ายบริหาร (Management Representative) พิจารณาและแนะนำให้เสนอต่อ Top Management ลงนามในแผนให้มีผลบังคับใช้อย่างเป็นทางการ

การประเมินความเสี่ยง (Risk Assessment) เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ในการดำเนินงาน รวมทั้งการจัดทำแผนบริหารจัดการความเสี่ยง ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลได้ทำการประเมินความเสี่ยงประจำปีทั้งหมด 6 ด้าน ประกอบไปด้วย 1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) 2. ความเสี่ยงด้านการปฏิบัติงาน (Operation Risk) 3. ความเสี่ยงด้านการเงิน (Financial Risk) 4. ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ/กฎหมาย (Compliance Risk) และ 5. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) โดยมีการกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งโดยทั่วไปองค์กรทางสารสนเทศที่เกี่ยวกับการแพทย์จะมีขั้นตอนหรือกระบวนการบริหารความเสี่ยง 6 ขั้นตอน (โรงพยาบาลแพร่, 2562) ดังนี้

1. การระบุความเสี่ยง (Risk identification) เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยง โดยต้องคำนึงถึงความเสี่ยงที่มีสาเหตุมาจากปัจจัยทั้งภายในและภายนอก ปัจจัยเหล่านี้มีผลกระทบต่อวัตถุประสงค์และเป้าหมายขององค์กรหรือผลการปฏิบัติงานทั้งในระดับองค์กรและระดับกิจกรรม ในการระบุปัจจัยเสี่ยงจะต้องพิจารณาว่ามีเหตุการณ์ใดหรือกิจกรรมใดของกระบวนการปฏิบัติงานที่อาจเกิดความผิดพลาดความเสียหายและไม่บรรลุวัตถุประสงค์ที่กำหนด รวมทั้งมีทรัพย์สินใดที่จำเป็นต้องได้รับการดูแลป้องกันรักษา ดังนั้นสิ่งจำเป็นคือความเข้าใจใน ความหมายของ “ความเสี่ยง (Risk)” “ปัจจัยเสี่ยง (Risk Factor)” และ “ประเภทความเสี่ยง” ก่อนที่จะดำเนินการระบุความเสี่ยงได้อย่างเหมาะสม

2. การประมาณความเสี่ยง (Risk estimation) เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดอุบัติการณ์ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงใดและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาส ที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง

3. การประเมินค่าความเสี่ยง (Risk evaluation) จะพิจารณาปัจจัยจากขั้นตอนที่ผ่านมา ได้แก่ โอกาสภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับ

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

ความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

4. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting) จะทำให้สามารถสามารถจัดลำดับความสำคัญของความเสี่ยงด้านระบบสารสนเทศและดำเนินการบริหารจัดการความเสี่ยงต่อไปได้อย่างมีประสิทธิภาพ

5. การจัดการความเสี่ยง (Risk management) เป็นกระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลงหรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยงมีหลายวิธีดังนี้ 1) การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่เกิดขึ้น เนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง 2) การลด/การควบคุมความเสี่ยง (Risk Reduction) เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่เพื่อลดโอกาสที่จะเกิด หรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้ 3) การกระจายความเสี่ยง หรือการถ่ายโอนความเสี่ยง (Risk Sharing) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้ผู้อื่นช่วยแบ่งความรับผิดชอบไป 4) เลี่ยงความเสี่ยง (Risk Avoidance) เป็นการจัดการความเสี่ยงที่อยู่ในระดับสูงมากและหน่วยงานไม่อาจยอมรับได้จึงต้องตัดสินใจยกเลิกโครงการ/กิจกรรมนั้น

6. การจัดทำแผนปฏิบัติการบริหารความเสี่ยงด้านระบบสารสนเทศ (Risk Treatment Plan: RTP) จากการจัดการความเสี่ยง สามารถนำมาจัดทำแผนปฏิบัติบริหารความเสี่ยง และควบคุมระบบสารสนเทศและการสื่อสาร โดยที่การควบคุม (Control) เป็นการกำหนดนโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ 1) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยง และข้อผิดพลาดตั้งแต่แรก 2) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว 3) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ 4) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องหรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

สรุป

จากข้อมูลดังกล่าว ในองค์กรโดยเฉพาะโรงพยาบาลที่ระบบสารสนเทศถูกพัฒนาขึ้นเพื่อใช้ในการรวบรวมและจัดเก็บข้อมูลนั้น ระบบสารสนเทศของโรงพยาบาลจึงมีความสำคัญอย่างยิ่ง เพื่อป้องกันไม่ให้เกิดภัยคุกคามต่อระบบสารสนเทศ การจัดทำแนวทางในการจัดการควบคุมความปลอดภัยระบบสารสนเทศจึงถือเป็นเรื่องจำเป็น รวมไปถึงการตรวจประเมินภายในเป็นกลไกสำคัญที่จะทำให้การบริหารจัดการองค์กรเกิดความโปร่งใส ตรวจสอบได้ สนับสนุนให้มีกระบวนการกำกับดูแลที่ดี ทำให้เกิดความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรม เพื่อให้ระบบมีเสถียรภาพด้านความมั่นคงปลอดภัยของข้อมูล และมีกรอบนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อประโยชน์สูงสุดของทั้งผู้รับบริการและผู้ให้บริการ โดยการนำมาตรฐาน ISO/IEC27001 มาเป็นวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่มีประสิทธิภาพ

ข้อเสนอแนะ

การบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศและการจัดการบริหารความเสี่ยง นอกจากจะเป็นสิ่งที่จำเป็นแล้ว ประเด็นเรื่องกฎหมายก็เป็นสิ่งหนึ่งที่สำคัญในการบริหารจัดการความมั่นคงปลอดภัย

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

โดยเฉพาะสารสนเทศในโรงพยาบาล ดังนั้นการดำเนินการต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ควรยึดตามหลักกฎหมายของประเทศ และปฏิบัติให้สอดคล้องตามที่กฎหมายบัญญัติ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับองค์กรมีความมั่นคงปลอดภัย มีประสิทธิภาพ และเชื่อถือได้

กิตติกรรมประกาศ

บทความทางวิชาการฉบับนี้สามารถสำเร็จสมบูรณ์ได้เนื่องจากการสนับสนุนของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ที่ตระหนักถึงความสำคัญของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในโรงพยาบาล และได้ให้โอกาสผู้เขียนในการปฏิบัติหน้าที่ผู้ตรวจประเมินภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC27001) คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล รวมถึงคำแนะนำ และการให้ความช่วยเหลือจากบุคคลต่าง ๆ ผู้เขียนจึงขอกล่าวแสดงความขอบคุณมา ณ ที่นี้

เอกสารอ้างอิง

กิตติศักดิ์ แก้วบุตรดี และ อัจฉรา กิจเดช. (2561). บทบาทและความสำคัญของผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ. *วารสาร Mahidol R2R e-Journal. 5*(2), 21-34.

_____. (2562). ความมั่นคงปลอดภัยระบบสารสนเทศ (ISO27001: 2013) – มิติใหม่ของการบริหารจัดการโรงพยาบาล. *วารสาร Mahidol R2R e-Journal. 8*(2), 26-37.

จิตตกานต์ บุญศิริทิวัตถ์ และ โกวิท รพีพิศาล. (2560). การพัฒนาแนวทางในการจัดการความมั่นคงความปลอดภัยระบบสารสนเทศที่เหมาะสมของโรงพยาบาลเอกชนในกรุงเทพมหานคร. *รังสิตสารสนเทศ. 23*(1), 61-91.

จตุชัย แพงจันทร์. (2555). *Master in Security* (2nd ed.). ไอดีซี พรีเมียร์.

โรงพยาบาลแพร่. (2562, พฤศจิกายน). *การบริหารจัดการความเสี่ยง (Risk Management) ด้านเทคโนโลยีสารสนเทศโรงพยาบาลแพร่ ปี 2562*. http://www.phraehospital.go.th/webinternal/medicalinformatics/images/page/file/20111815364CI8Y1.PDF

ศราวุฒิ จันทะคัด. (2554). *การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษา: บริษัทแซนด์แอนด์ซอยล์อุตสาหกรรม จำกัด* [สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ]. http://203.188.27.107/thesis/Thesis_2554/082%20Management%20of%20Computer%20Network%20and%20Security%20A%20Case%20Study%20of%20Sand%20And%20Soil%20Industry%20Co.,Ltd.pdf.

สำนักงานปลัดกระทรวงศึกษาธิการ. (2559). *แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ.* ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. https://ops.moe.go.th/wpcontent/uploads/2017/08/policy- ict.pdf.

Al-Zahawi, O. S. (2019). *Information Security Handbook for ISO 27001 Controls*. Helsinki, Finland: UR academy.

International Organization for Standardization. (2018). *About ISO.* https://www.iso.org/about-us.html

Received: August 20, 2020, Revised: October 29, 2021 , Accepted: November 9, 2021
http://doi.org/10.14456/jmu

International Organization for Standardization. (2018). *ISO Survey of certifications to management system standards*. https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1.

R Moeller, R. (2016). *Brink's Modern Internal Auditing: A Common Body of Knowledge*. (7th ed.). John Wiley & Sons, Inc.

Pedneault, S. (2009). *Techniques and Strategies for Understanding Fraud*. (3rd ed.). John Wiley & Sons, Inc.

Pemble, E. I. M. W., & Goucher, W. F. (2018). The CIO's Guide to Information Security Incident Management. Auerbach Publications.

Salomon, D. (2010). Elements of computer security. Springer Science & Business Media.

University of South Carolina Board of Trustees. (2014). *Information Technology Security.* https://www.uts.sc.edu/itsecurity/threats.shtml.