วารสาร Mahidol R2R e-Journal ปีที่ 8 ฉบับที่ 2 ประจำเดือนพฤษภาคม-สิงหาคม 2564
Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

การตรวจประเมินภายในตามข้อกำหนดมาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ

Internal audits in accordance with the international standard requirements for information security management systems.

นภสินธุ์ บุญมาก[1*] และ เลอพงศ์ แก้วอินทร์[1]
NAPHASIN BOONMAK[1*] and LERPONG KAEWIN[1]

บทคัดย่อ

ความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้นและเข้ามามีบทบาทมากมายในองค์กรต่างๆ ทั้งภาครัฐและภาคเอกชน ซึ่งองค์กรต่างๆ มีข้อมูลที่มีความสำคัญ และข้อมูลที่เป็นความลับขององค์กร ส่งผลให้ความต้องการในการดูแลความมั่นคงปลอดภัยของสารสนเทศเพิ่มสูงขึ้น เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่างๆ ที่สามารถบุกรุกโจมตีข้อมูลขององค์กร

มาตรฐาน ISO/IEC 27001 คือ มาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ได้ถูกนำมาใช้เป็นมาตรฐานในการดำเนินงานขององค์กรต่างๆ เพื่อให้เกิดประสิทธิภาพในการปกป้องทรัพย์สินสารสนเทศขององค์กร และให้การดำเนินงานขององค์กรสอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับ และข้อกำหนดต่างๆ ที่เกี่ยวข้อง โดยหลักการพื้นฐานประการหนึ่งของมาตรฐาน ISO/IEC 27001 คือ การตรวจประเมินภายใน (Internal Audits) ซึ่งการตรวจประเมินภายในเป็นการให้หลักประกันอย่างเที่ยงธรรมและการให้คำปรึกษาอย่างเป็นอิสระ เพิ่มคุณค่าและปรับปรุงการปฏิบัติงานขององค์กรให้ดีขึ้น การตรวจประเมินภายในช่วยให้องค์กรบรรลุถึงเป้าหมายที่วางไว้ ด้วยการประเมินและปรับปรุงประสิทธิภาพของกระบวนการบริหารความเสี่ยง การควบคุมและการกำกับดูแลอย่างเป็นระบบและเป็นระเบียบ

ดังนั้นผู้ตรวจประเมินภายในที่จะดำเนินการตรวจประเมินภายในตามมาตรฐาน ISO/IEC 27001 ต้องมีความรู้ในเรื่องข้อกำหนดมาตรฐาน (Requirements) และมาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยสารสนเทศของ ISO/IEC 27001:2013 และขั้นตอนการตรวจประเมินภายในตามข้อกำหนดมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ

คำสำคัญ: การตรวจประเมินภายใน; ระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ;
ข้อกำหนดมาตรฐาน ISO/IEC 27001:2013

[1*] ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล

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

[*] Corresponding Author: napasin.boo@mahidol.ac.th

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

Abstract

Currently, the advancement of information technology become backbones in various organizations. There are important information and confidential information about the organization which affecting increased demand for information security from various forms of threats that can attack an organization's information. ISO/ IEC 27001 is an international standard for Information Security Management System (ISMS). The ISO/IEC 27001 has been applied as a standard in operations of various organizations in order to be effective in protecting the information assets of the organization and ensure that the operations of the organization comply with the laws, rules, regulations and various requirements. Internal audit is the basic principles of the ISO/ IEC 27001, conducting internal audits is guaranteeing along with independent consulting. The internal audit becomes enrichment and improves the operations of the organization. In addition, an internal audit helps the organization achieve the goals, onward to evaluating and improving the efficiency of the risk management process Systematic and orderly control and supervision.

The internal auditors will be conducting internal audits in accordance with requirements and controls with ISO/ IEC 27001: 2013 standard. The internal auditor exceptional skills and knowledge in internal audit procedures.

Keywords: Internal audits; Information Security Management System; ISO/IEC 27001:2013

บทนำ

หากพิจารณาเหตุการณ์ที่เกิดขึ้นในปัจจุบันและข่าวรอบโลกจะเห็นได้ว่ามีการกระทำผิดด้านเทคโนโลยีสารสนเทศเพิ่มมากขึ้น ตัวอย่างเช่น เมื่อวันที่ 15 สิงหาคม 2562 ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT หรือไทยเซิร์ต) ตรวจพบว่าข้อมูลส่วนตัวของคนไทยปรากฏอยู่ในระบบฐานข้อมูลในต่างประเทศซึ่งมีความคาบเกี่ยวกับเว็บไซต์การพนัน โดยพบข้อมูลรั่วไหลทั้งสิ้นประมาณ 41 ล้านรายการ และเป็นข้อมูลการทำธุรกรรมของคนไทยที่ทำรายการผ่านเว็บไซต์การพนันดังกล่าวถึงจำนวนประมาณ 3.3 ล้านรายการ รวมทั้งมีข้อมูลส่วนตัวของคนไทย เช่น ชื่อ, นามสกุล, หมายเลขโทรศัพท์, วันเกิด, หมายเลขบัตรประจำตัวประชาชน และหมายเลขบัญชีธนาคารรั่วไหลด้วย นอกจากนี้นักวิจัยด้านความมั่นคงปลอดภัยจาก RedDrip Team ได้เผยแพร่รายงานบทวิเคราะห์การโจมตีโดยกลุ่มที่ถูกเรียกว่า OceanLotus ซึ่งเป็นกลุ่มแฮกเกอร์ที่คาดว่าได้รับการสนับสนุนจากรัฐบาลของบางประเทศ โดยก่อนหน้านี้กลุ่มดังกล่าวเคยก่อเหตุปฏิบัติการโจมตีแบบ Advance Persistent Threat (APT) เพื่อขโมยข้อมูลสำคัญโดยเฉพาะข้อมูลด้านข่าวกรองจากหน่วยงานระดับสูงในประเทศจีนและประเทศในแถบเอเชียตะวันออกเฉียงใต้มาแล้ว หากย้อนกลับไปเมื่อวันที่ 28 กันยายน 2561 มีแถลงการณ์จากเฟซบุ๊ก (Facebook) กรณีตรวจพบการรั่วไหลของข้อมูลผู้ใช้งานกว่า 50 ล้านรายทั่วโลก ซึ่งถูกแฮกเกอร์เจาะระบบผ่านช่องโหว่ของแพลตฟอร์ม ทำให้เฟซบุ๊กต้องทำการรีเซตระบบ Access Tokens ของผู้ใช้งานเพื่อป้องกันผลกระทบที่อาจเกิดขึ้น ส่งผลให้ผู้ใช้งานกว่า 90 ล้านบัญชีถูกบังคับให้ออกจากระบบเพื่อให้เข้าสู่ระบบใหม่อีกครั้ง นอกจากนี้การโจรกรรมข้อมูลส่วนบุคคล หรือการขโมยข้อมูลส่วนบุคคลของผู้อื่นไปใช้ฉ้อโกงหรือก่ออาชญากรรมอื่น ๆ เช่น นำ

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

ข้อมูลของผู้อื่นไปใช้ทำบัตรเครดิต กู้เงิน หรือเปิดบัญชีใหม่ เป็นต้น ซึ่งเหตุการณ์ต่าง ๆ เหล่านี้ได้สะท้อนให้เห็นถึงความเสี่ยงที่เกี่ยวข้องความปลอดภัยของข้อมูล

มาตรฐาน ISO/IEC 27001 คือ มาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management Systems: ISMS) จะช่วยให้กิจกรรมทางธุรกิจต่อเนื่องไม่สะดุด ช่วยป้องกันกระบวนการทางธุรกิจจากภัยร้ายแรงต่างๆ เช่น แผ่นดินไหว วาตภัย อุทกภัย ฯลฯ และความเสียหายของระบบข้อมูล โดยครอบคลุมทุกกลุ่มอุตสาหกรรมและทุกกลุ่มธุรกิจ มาตรฐาน ISO/IEC 27001 ให้ต้นแบบสำหรับการประเมินความเสี่ยง การออกแบบด้านการรักษาความปลอดภัยและการนำไปปฏิบัติ รวมถึงการบริหารจัดการความปลอดภัยของข้อมูล โดยมาตรฐาน ISO/IEC 27001 เป็นมาตรฐานสากลเพียงมาตรฐานเดียวที่สามารถตรวจประเมินได้สำหรับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ โดยมาตรฐาน ISO/IEC 27001 จะให้การรับรองว่าองค์กรได้ดำเนินงานโดยสอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับ และข้อกำหนดตามสัญญาอันเกี่ยวเนื่องกับข้อมูลสำคัญ ซึ่งเป็นการพิสูจน์ให้เห็นว่าองค์กรได้มีการดำเนินการตามขั้นตอนที่จำเป็นเพื่อปกป้องข้อมูลที่สำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต เมื่อองค์กรนำมาตรฐาน ISO/IEC 27001 ไปปฏิบัตินั้นจะแตกต่างกันไปในแต่ละองค์กร แต่มีหลักการพื้นฐานของมาตรฐาน ISO/IEC 27001 ที่ทุกองค์กรจะต้องปฏิบัติตามเพื่อให้เกิดประสิทธิภาพในการปกป้องทรัพย์สินสารสนเทศขององค์กร คือ การตรวจประเมินภายใน (Internal Audits) ซึ่งการตรวจประเมินภายในเป็นกิจกรรมบังคับสำหรับองค์กรที่จัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System: ISMS) ซึ่งการตรวจประเมินภายในเป็นการให้ความเชื่อมั่น (Assurance) และการให้คำปรึกษา (Consulting) อย่างเที่ยงธรรมและเป็นอิสระ เพื่อเพิ่มคุณค่าและปรับปรุงการดำเนินงานขององค์กร และช่วยให้องค์กรบรรลุถึงเป้าหมายที่วางไว้

ความสำคัญของมาตรฐาน ISO/IEC 27001

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานด้านการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศที่ผ่านการระดมสมอง อภิปราย และโหวตรับรองโดยประเทศที่เป็นสมาชิก นอกจากนี้ในกระบวนการพัฒนามาตรฐานระดับสากลได้เปิดโอกาสให้ตัวแทนของแต่ละประเทศ องค์กรวิชาชีพได้เข้ามามีส่วนร่วม โดยมีเป้าหมายเพื่อให้เกิดการยอมรับในระดับสากล ซึ่งองค์กร International Organization for Standardization หรือ ISO เป็นหน่วยงานที่ให้กำเนิด ISO/IEC 27001 โดยมีการใช้งานเวอร์ชันแรก คือ ISO/IEC 27001:2005 ประกาศใช้งานครั้งแรกเมื่อปี พ.ศ.2550 หลังจากประกาศใช้ก็ได้รับความสนใจจากองค์กรทั้งภาครัฐและเอกชนทั่วโลกนำมาใช้งานและขอการรับรอง (Certification) สำหรับเวอร์ชันล่าสุดของมาตรฐาน ISO/IEC 27001 คือ ISO/IEC 27001:2013 ประกาศเมื่อ 1 ตุลาคม พ.ศ.2556 มาตรฐาน ISO/IEC 27001 ออกแบบมาให้ใช้ได้กับหน่วยราชการ สถาบันการศึกษา องค์กรประเภทธุรกิจต่างๆ สามารถนำมาปฏิบัติได้เหมือนกันทั้งองค์กรขนาดเล็กและองค์กรขนาดใหญ่ โดยพื้นฐานความมั่งคงปลอดภัยของสารสนเทศจะครอบคลุมถึงเรื่องการใช้งานเทคโนโลยีสารสนเทศ เรื่องกฎระเบียบขององค์กร เรื่องการปฏิบัติงานของบุคลากร เรื่องจัดซื้อจัดจ้าง เรื่องสมรรถนะของบุคลากร เรื่องการควบคุมผู้ให้บริการภายนอก เรื่องการปฏิบัติตามกฎหมายที่เกี่ยวข้อง แม้ว่าองค์กรจะนำระบบไอทีล้ำเลิศแค่ไหนเข้ามาใช้งานภายในองค์กร แต่ถ้าไม่มีกฎระเบียบควบคุมการปฏิบัติงานที่ชัดเจนเกี่ยวกับการใช้งานเทคโนโลยีสารสนเทศ ไม่มีการอบรมให้ความรู้แก่และสร้างความตระหนักถึงความสำคัญของใช้งานเทคโนโลยีสารสนเทศให้แก่บุคลากรขององค์กร และไม่มีการควบคุมผู้ให้บริการภายนอกในการใช้งานเทคโนโลยีสารสนเทศขององค์กรที่ดีพอ องค์กรนั้นก็จะดำเนินกิจกรรมด้วยความยากลำบาก บุคลากรนำทรัพยากรไปกับเรื่องที่ไม่สมควรและหลายคนทำผิดกฎหมาย เช่น บุคลากรใช้คอมพิวเตอร์ขององค์กรโหลดหนังและแชร์ไฟล์ที่ละเมิดลิขสิทธิ์ บุคลากรนำข้อมูลที่เป็นความลับของ

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

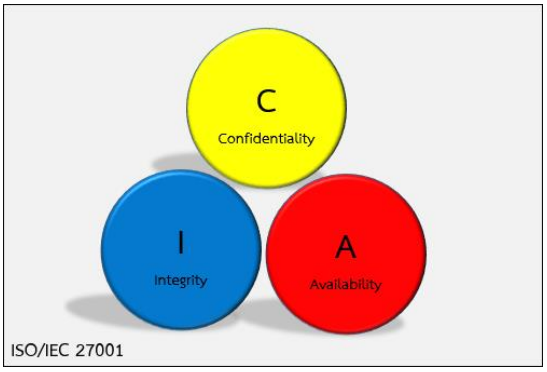
องค์กรไปเผยแพร่ หรือข้อมูลสำคัญรั่วไหล เหตุการณ์เหล่านี้เสี่ยงต่อการละเมิดกฎหมายและเสี่ยงต่อสร้างความเสียหายต่อองค์กรอย่างแน่นอน (ปริญญ์ เสรีพงศ์, 2557)

หัวใจสำคัญของระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วยปัจจัยพื้นฐานหลัก 3 ปัจจัย คือ ข้อมูลส่วนตัวและข้อมูลสำคัญขององค์กร การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ และการบริหารระบบป้องกันความมั่นคงปลอดภัยของข้อมูล

1. ข้อมูลส่วนตัว ข้อมูลสำคัญขององค์กร การรักษาความมั่นคงปลอดภัยของสารสนเทศไม่ให้ถูกขโมย ลักลอบนำไปใช้ ดัดแปลง หรือทำให้เกิดข้อผิดพลาดอื่นใด ซึ่งสำหรับหลายหน่วยงานอาจเป็นอันตรายระดับวิกฤติได้ ซึ่งข้อมูลนี้ไม่เพียงเฉพาะข้อมูลสำคัญขององค์กรแต่ยังรวมถึงข้อมูลส่วนตัวของลูกค้าหรือบุคคลที่สามที่เกี่ยวข้องอื่นๆ ด้วย

2. การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ ซึ่งปัจจุบันมีการคำนึงถึงการตั้งศูนย์สำรองข้อมูล และดำเนินการกู้คืนระบบภายหลังภัยพิบัติ (Disaster Recovery Center: DRC) ซึ่งมีความสำคัญมากในหลายธุรกิจ เช่น ธุรกิจการเงิน หรือบริการด้านสุขภาพเพราะข้อมูลเหล่านั้นมีความสำคัญต่อความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง (Business Continuity)

3. การบริหารระบบป้องกันความมั่นคงปลอดภัยของข้อมูล มีองค์ประกอบในการพิจารณาความมั่นคงปลอดภัยของระบบสารสนเทศ 3 ประเด็นหลัก คือ ความลับของข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) ดังรูปที่ 1



รูปที่ 1 องค์ประกอบในการพิจารณา ISMS

มาตรฐาน ISO/IEC 27001 ใช้แนวทางของวงจรการควบคุมคุณภาพ (Deming Cycle) หรือ PDCA (Plan-Do-Check-Act) ซึ่งถูกคิดค้นโดยวอล์ทเตอร์ ชิวฮาร์ท (Walter Shewhart) ผู้บุกเบิกการใช้สถิติสำหรับวงการอุตสาหกรรม และต่อมาเอดวาร์ด เดมมิ่ง (Edwards W. Deming) ได้ใช้วงจรนี้เป็นเครื่องมือสำหรับการปรับปรุงกระบวนการทำงานของพนักงานภายในโรงงาน และพนักงานในโรงงานได้นำวิธีการ PDCA ช่วยค้นหาปัญหาอุปสรรคในแต่ละขั้นตอนการผลิตให้ดีขึ้น ส่งผลให้วงจรการควบคุมคุณภาพเริ่มเป็นที่รู้จักกันมากขึ้น สำหรับมาตรฐาน ISO/IEC 27001 เน้นเรื่องข้อมูลสารสนเทศ และการวางแนวทางการบริหารให้เกิดความมั่นคงปลอดภัยโดยผ่านกระบวนการตั้งแต่การตั้งเป้าหมาย (Goal Setting) ซึ่งถือเป็นจุดเริ่มต้นสำคัญของการลงมือทำในเรื่องใดเรื่องหนึ่ง เพราะการมีเป้าหมาย หมายถึงการที่องค์กรรู้ว่าองค์กรต้องการอะไร องค์กรจะเดินทางไปในทิศทางใด ยิ่งถ้ารู้ได้ว่าทำไมองค์กรถึงต้องไป และยิ่งมองเห็นภาพขององค์กรเมื่อไปถึงเป้าหมายนั้นชัดเจนมากเท่าไร ยิ่งเกิดแรงกระตุ้นให้บุคลากรขององค์กรอยากออกเดินทางไปสู่เป้าหมายนั้นโดยเร็ว ซึ่งแนวคิดนี้สามารถประยุกต์ใช้ในการดำเนินงานตามมาตรฐาน ISO/IEC 27001 ได้เป็นอย่างดี โดยหลักการของ PDCA (บูรณะศักดิ์, 2551) มีดังนี้

- การวางแผนงาน (Plan) เมื่อองค์กรตั้งเป้าหมายแล้ว สิ่งแรกที่องค์กรต้องดำเนินการ คือ การนำ

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

เป้าหมายมากำหนดรายละเอียดต่างๆ ตัวอย่างเช่น สิ่งที่ต้องทำโดยเรียงตามลำดับความสำคัญ รายละเอียดของสิ่งที่ต้องทำแต่ละขั้นตอน ปัจจัยต่างๆ ที่ต้องใช้ ระยะเวลาเริ่ม-สิ้นสุด บุคคลหรือทีมงานที่เกี่ยวข้องในแต่ละขั้นตอน และที่สำคัญที่สุด คือ ตัวชี้วัดผล (Key Performance Indicator: KPI) โดยแผนงานเป็นตัวกำหนดวิธีการทำงาน และกำหนดระยะเวลาในการดำเนินงานว่าจะบรรลุเป้าหมายเมื่อไหร่ ดังนั้นตัวชี้วัดจึงเป็นตัวที่จะคอยบอกว่าวิธีการที่องค์กรเลือกใช้นั้นถูกต้องหรือไม่ เร็ว-ช้าอย่างไร ทรัพยากรที่ใช้ไปเป็นไปตามแผนหรือเกินกว่าที่กำหนดไว้ เพื่อที่จะได้ปรับแผนหรือวิธีได้อย่างทันท่วงที

- การลงมือปฏิบัติ (Do) เมื่อวางแผนและกำหนดวิธีการดำเนินการเสร็จแล้ว ขั้นตอนต่อไปคือการลงมือปฏิบัติตามแผนงานและวิธีการที่กำหนดไว้อย่างมีวินัยและเคร่งครัด ทักษะการบริหารจัดการต่างๆ จะถูกนำมาใช้ในการลงมือปฏิบัติ เช่น การบริหารเวลาให้ได้ตามแผน การประชุมเพื่อตรวจสอบความคืบหน้า การมอบหมายงานเพื่อแบ่งงานให้บุคลากรที่เกี่ยวข้อง เป็นต้น
- การตรวจสอบ (Check) ภายหลังจากที่ลงมือปฏิบัติไปได้ระยะหนึ่ง องค์กรต้องเริ่มทำการตรวจสอบความคืบหน้าของสิ่งที่ลงมือปฏิบัติว่าเป็นไปตามแผนงานหรือไม่ โดยเปรียบเทียบผลการปฏิบัติงานกับตัวชี้วัดที่กำหนดไว้ ถ้าจุดที่ตรวจสอบได้ผลลัพธ์ตามตัวชี้วัดที่ตั้งไว้หรือดีกว่าแสดงว่าวิธีการที่เลือกใช้นั้นถูกต้อง และสามารถดำเนินการต่อให้แล้วเสร็จได้ตามแผนงานที่วางไว้ แต่ถ้าตรวจสอบออกมาแล้วผลปรากฏว่าสิ่งที่ลงมือปฏิบัติไปนั้นต่ำกว่าตัวชี้วัดที่ตั้ง ถือเป็นสัญญาณเตือนว่ามีความผิดปกติบางอย่างเกี่ยวกับแผนงานหรือวิธีการที่กำหนดไว้ในตอนแรก และอาจส่งผลให้ไม่สามารถดำเนินการต่อให้เสร็จทันตามแผนงานที่กำหนดไว้
- การปรับปรุง (Action) เมื่อตรวจสอบพบว่าไม่สามารถดำเนินการต่อให้เสร็จทันตามแผนงานที่กำหนดไว้ การปรับปรุงเป็นการปรับเปลี่ยนวิธีการหรือทรัพยากรบางอย่างเพื่อทำให้ผลลัพธ์กลับมาอยู่ในแผนงาน และระยะเวลาตามที่กำหนดไว้ในครั้งแรก ซึ่งกระบวนการปรับปรุงเริ่มจากการวิเคราะห์หาสาเหตุที่ทำให้ผลลัพธ์ไม่เป็นไปตามที่วางแผนหรือกำหนดไว้ โดยตรวจสอบว่าเกิดจากองค์ประกอบหรือปัจจัยภายใน/ภายนอกใดบ้าง จากนั้นจึงนำมากำหนดมาตรการแก้ไข ปรับปรุงต่อไปเพื่อให้กิจกรรมต่างๆ สามารถดำเนินการต่อให้แล้วเสร็จได้ตามแผนงานที่วางไว้ สำหรับกรณีที่สามารถดำเนินการต่อให้แล้วเสร็จได้ตามแผนงานที่วางไว้ หากองค์กรมุ่งเน้นประสิทธิภาพผลงานขององค์กร เรียนรู้จากความผิดพลาดต่างต่อเนื่อง สามารถนำการปรับปรุงกระบวนการหรือปรับเปลี่ยนกระบวนการอย่างต่อเนื่องมาใช้ได้เช่นกัน

หลักการของ PDCA ไม่ใช่เพียงแค่ทำให้องค์กรบรรลุเป้าหมายตามที่ตั้งไว้เท่านั้น องค์กรยังสามารถใช้หลักการ PDCA เพื่อการดำเนินกิจกรรมอย่างต่อเนื่องได้ด้วยการยกระดับของเป้าหมายให้สูงขึ้น และเริ่มกำหนดแผนงานและวิธีการที่เหมาะสมที่จะนำพาองค์กรไปสู่เป้าหมายที่สูงขึ้น แล้วจึงเริ่มเข้าสู่วงจร PDCA อีกครั้งเพื่อการปรับปรุงและพัฒนาให้เกิดการทำงานอย่างต่อเนื่อง (Continuous Improvement) ภายในองค์กร ส่งผลให้องค์กรตอบสนองความพึงพอใจของลูกค้า มุ่งเน้นจำกัดการสูญเสียทรัพยากร หรือจำกัดงานที่ไม่ก่อให้เกิดคุณค่า (Non-value added work) ภายในองค์กรได้อีกด้วย (วชิราพร, 2552) ดังรูปที่ 2

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

รูปที่ 2 วงจรการบริหารงานคุณภาพ (Deming Cycle)

ประโยชน์ของมาตรฐาน ISO/IEC 27001

ประโยชน์ของการได้รับการรับรองโดยบุคคลที่ 3 ตามมาตรฐาน ISO/IEC 27001 (Perry, 2018) มีมากมายทั้งสำหรับองค์กรและผู้มีส่วนได้เสียขององค์กร (Stakeholder) ดังนี้

1. การได้รับการรับรองมาตรฐาน ISO/IEC 27001 จะช่วยเพิ่มความน่าเชื่อถือขององค์กรด้วยความครบถ้วนสมบูรณ์ของข้อมูลและระบบต่างๆ ขององค์กร

2. การได้รับการรับรองมาตรฐาน ISO/IEC 27001 เป็นสร้างความมั่นใจให้กับซัพพลายเออร์ ลูกค้าและผู้มีส่วนได้เสียอื่นๆ ว่า องค์กรได้มีการดำเนินมาตรการที่จำเป็นเพื่อปกป้องข้อมูลขององค์กร นอกจากให้ความอุ่นใจให้กับลูกค้าปัจจุบันขององค์กรแล้ว การได้รับการรับรองมาตรฐาน ISO/IEC 27001 ยังสามารถช่วยท่านในการดึงดูดลูกค้าใหม่ที่ใส่ใจในเรื่องการรักษาความปลอดภัย

3. การได้รับการรับรองมาตรฐาน ISO/IEC 27001 ยังสามารถช่วยเสริมสร้างความรู้สึกเกี่ยวกับการรักษาความลับทั่วทั้งองค์กรได้อีกด้วยซึ่งเป็นเรื่องที่สำคัญอย่างมาก เพราะข้อมูลที่สำคัญไม่ได้ถูกเก็บไว้เฉพาะในเซิร์ฟเวอร์และฮาร์ดไดรฟ์เท่านั้น แต่ข้อมูลที่สำคัญสามารถถูกเข้าถึงและจดจำได้โดยบุคคล/พนักงานในองค์กรเองอีกด้วย

4. การได้รับการรับรองมาตรฐาน ISO/IEC 27001 สามารถเปลี่ยนวัฒนธรรมองค์กรได้ ทำให้เป็นสิ่งหนึ่งที่สร้างมูลค่าให้กับข้อมูลส่วนตัวขององค์กร

มาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISO/IEC 27001:2013) ประกอบด้วย 2 ส่วน คือ ข้อกำหนดมาตรฐาน (Requirements) ISO/IEC 27001:2013 และมาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001:2013 โดยมีรายละเอียดดังนี้

ข้อกำหนดมาตรฐาน ISO/IEC 27001:2013

มาตรฐานสากล ISO 27001: 2013 ได้กำหนดให้องค์กรหรือหน่วยงานดำเนินการควบคุมความมั่นคงปลอดภัยของสารสนเทศออกเป็นหมวดหมู่ต่างๆ ทั้งสิ้น 7 หมวด (ปริญญ์, 2556) ดังนี้

1. บริบทขององค์กร (Context of the organization)

มาตรฐานสากล ISO 27001:2013 กำหนดให้องค์กรดำเนินการทบทวน และกำหนดวัตถุประสงค์ขององค์กรที่มีต่อการจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยการรวบรวมความต้องการและความคาดหวังจากผู้ที่เกี่ยวข้องกับองค์กรทั้งหมด เพื่อนำมาใช้ในการกำหนดขอบเขตการดำเนินงาน ตลอดจนการความต้องการและความคาดหวังดังกล่าวไปใช้ในการกำหนดนโยบายด้านความมั่งคงปลอดภัยของสารสนเทศขององค์กร

1.1 ทำความเข้าใจองค์กรและบริบทขององค์กร โดยระบุประเด็นภายใน (Internal issues) เช่น ระเบียบ ข้อบังคับ กฎเกณฑ์ต่างๆ ที่ปฏิบัติอยู่ภายในองค์กร และประเด็นภายนอก (External issues) เช่น พระราชบัญญัติ กฎหมาย นโยบายจากหน่วยงานที่เกี่ยวข้องกับองค์กรมาใช้พิจารณาในการวางระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศให้ครอบคลุมอย่างเหมาะสมไม่ตกหล่นประเด็นสำคัญ

1.2 กำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง โดยองค์กรจะต้องรู้ว่าใครคือผู้เกี่ยวข้อง (Interested parties) และผู้เกี่ยวข้องเหล่านั้นมีความต้องการและมีความคาดหวังอะไร (needs and expectations) จากองค์กร ระบบงานใดมีความสำคัญ เพราะเป็นงานที่เกี่ยวข้องกับการส่งมอบสินค้าหรือบริการ

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

ให้กับผู้เกี่ยวข้อง ซึ่งบริบทขององค์กรเป็นข้อมูลสำคัญในการกำหนดขอบเขต (Scope) ขอบการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศขององค์กร

1.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องพิจารณาถึงข้อกำหนดและความต้องการของผู้เกี่ยวข้อง ซึ่งในส่วนดังกล่าวเป็นเงื่อนไขสำคัญที่องค์กรต้องทำความเข้าใจและกำหนดขอบเขตให้เหมาะสมและเพียงพอคือไม่กำหนดขอบเขตเล็กเกินไปจนตกหล่นผู้เกี่ยวข้อง หรือขอบเขตกว้างเกินกว่าความสามารถในการบริหารจัดการส่งผลให้ระบบขาดประสิทธิภาพ

1.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยองค์กรต้องดำเนินการกำหนดนโยบาย จัดทำเอกสารที่เกี่ยวข้อง เพื่อนำไปปฏิบัติและรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ รวมถึงปรับปรุงอย่างต่อเนื่องและสอดคล้องตามข้อกำหนดของ ISO/IEC 27001:2013 Information Security Management System

2. ภาวะผู้นำ (Leadership)

มาตรฐานสากล ISO 27001:2013 ได้กำหนดให้ผู้บริหารขององค์กรจะต้องให้ความสำคัญในเรื่องการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และดำเนินการกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการกำหนดบทบาท หน้าที่และความรับผิดชอบให้กับบุคลากรขององค์กร

2.1 ภาวะผู้นำและการให้ความสำคัญ ผู้บริหารระดับสูงขององค์กรต้องแสดงให้เห็นถึงภาวะผู้นำและให้ความสำคัญต่อระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ โดยการแสดงออกถึงวิสัยทัศน์ พันธกิจ แผนกลยุทธ์ขององค์กรที่นำมาปฏิบัติให้สอดคล้องกับกฎเกณฑ์ระเบียบปฏิบัติต่างๆ ทั้งภายในและภายนอกองค์กร

2.2 นโยบาย ผู้บริหารระดับสูงต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับจุดประสงค์ขององค์กรและสอดคล้องกับข้อกำหนดตามมาตรฐานสากล ISO 27001:2013

2.3 บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ ผู้บริหารระดับสูงขององค์กรจะต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยของสารสนเทศให้แก่บุคลากรภายในองค์กรอย่างชัดเจน

3. การวางแผน (Planning)

มาตรฐานสากล ISO 27001:2013 ได้กำหนดให้องค์กรดำเนินการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ และบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร โดยองค์กรต้องวางแผนบริหารความเสี่ยงและหาวิธีการควบคุมหรือจัดการความเสี่ยงให้เกิดประสิทธิภาพ

3.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส องค์กรจะต้องวางแผนงานสำหรับระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ จะต้องพิจารณาถึงบริบทขององค์กร พิจารณาความเสี่ยงที่เกี่ยวข้องจากนั้นวางแนวทางจัดการอย่างเหมาะสม (สุวันต์นา, 2562)

3.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ องค์กรต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Objectives) และแผนการบรรลุวัตถุประสงค์ โดยวัตถุประสงค์นี้จะต้องวัดผลได้ และสอดคล้องกับนโยบายความมั่นคงปลอดภัยของสารสนเทศขององค์กร

4. การสนับสนุน (Support)

มาตรฐานสากล ISO 27001:2013 ได้กำหนดให้องค์กรและผู้บริหารระดับสูงขององค์กรให้การสนับสนุนด้านต่างๆ เรื่องการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมุ่งเน้นในประเด็นต่างๆ ที่ต้องให้การสนับสนุน 5 ประเด็น คือ

4.1 ทรัพยากร การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศให้ประสบความสำเร็จนั้นองค์กรจำเป็นต้องมีทรัพยากรต่างๆ เพียงพอและเหมาะสม ซึ่งทรัพยากรประกอบด้วย บุคลากร เวลา งบประมาณ และการสนับสนุนจากผู้บริหารอย่างเป็นรูปธรรม

4.2 สมรรถนะ การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศนั้น บุคลากรที่มีส่วนร่วมในการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศจะต้องมีความรู้ความสามารถ

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

ซึ่งต้องมีการให้ความรู้ที่ตรงกับภาระหน้าที่เพื่อให้บุคลากรสามารถปฏิบัติได้อย่างถูกต้อง เช่น การบริหารความเสี่ยง การจัดการความเสี่ยง และการตรวจประเมินภายใน เป็นต้น

4.3 การสร้างความตระหนัก การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศนั้น องค์กรจะต้องสร้างความตระหนักให้กับบุคลากรทุกคนขององค์กรในด้านความมั่นคงปลอดภัยของสารสนเทศ เพราะหากบุคลกรมีความตระหนักที่เพียงพอ ย่อมจะลดความเสี่ยงได้โดยปริยาย เช่น การจัดชั้นความลับและการควบคุมการเข้าถึงข้อมูลและสารสนเทศภายในองค์กร การใช้รหัสผ่านที่มีความซับซ้อน การเข้าใจและปฏิบัติตามกฎ ระเบียบ ข้อบังคับด้านเทคโนโลยีสารสนเทศขององค์กรอย่างเคร่งครัด เป็นต้น

4.4 การสื่อสาร องค์กรต้องดำเนินการสื่อสารกับบุคคลต่างๆ ที่เกี่ยวข้องกับองค์กร เพื่อให้ความรู้ข่าวสารที่เป็นประโยชน์ ซึ่งเป็นวิธีในการสร้างความตระหนักที่ได้ผลดี โดยองค์กรจะต้องดำเนินการสื่อสารกับบุคลากรทั้งการสื่อสารภายในองค์กร (Internal Communication) และการสื่อสารภายนอกองค์กร (External Communication)

4.5 เอกสารสารสนเทศ การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศเอกสารต่างๆ ภายในองค์กรมีความจำเป็นในการทำงานร่วมกัน เพื่อให้เกิดความชัดเจนแก่ผู้ปฏิบัติและผู้ตรวจสอบ (Auditor) ซึ่งมาตรฐาน ISO27001:2013 กำหนดให้องค์กรดำเนินการควบคุมเอกสารต่างๆ ตั้งแต่เริ่มจัดทำเอกสาร การนำเอกสารไปใช้งาน ตลอดจนการทำลายเอกสารเมื่อสิ้นสุดการใช้งาน ซึ่งจะต้องผ่านการจัดทำโดยผู้ที่มีความรู้ มีผู้ทบทวน และมีการอนุมัติก่อนจะนำไปใช้งาน

5. การดำเนินการ (Operation)

มาตรฐานสากล ISO 27001:2013 ได้กำหนดให้องค์กรดำเนินการบริหารความเสี่ยง (ปริญญ์, 2557) ในการปฏิบัติงาน เพื่อควบคุมความมั่นคงปลอดภัยของสารสนเทศตามขั้นตอนการบริหารความเสี่ยง และมีการจัดการกับความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

5.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม โดยองค์กรต้องควบคุมให้บุคลากรภายในองค์กรปฏิบัติตามแผนจัดการความเสี่ยง

5.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรจะต้องดำเนินการประเมินความเสี่ยงเป็นระยะ ไม่ใช่ทำครั้งเดียวจบ เพราะเมื่อเวลาผ่านไปก็จะมีความเสี่ยงใหม่เกิดขึ้นมา ไม่ว่าจะเป็นความเสี่ยงจากเทคโนโลยีใหม่ๆ หรือสภาพแวดล้อมสังคมและการเมือง

5.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรจะต้องดำเนินการจัดการความเสี่ยงที่จัดทำขึ้นภายหลังการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ โดยกำหนดรายละเอียด ขั้นตอนวิธีการต่างๆ เพื่อนำไปปฏิบัติให้ได้ผลลัพธ์ตามที่กำหนดไว้ให้สอดคล้องกับมาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001:2013

6. การประเมินประสิทธิภาพและประสิทธิผล (Performance Evaluation)

มาตรฐานสากล ISO 27001:2013 ได้กำหนดให้องค์กรดำเนินการประเมินประสิทธิภาพและประสิทธิผลในการดำเนินงานด้านความมั่นคงปลอดภัยของสารสนเทศขององค์กร ดังนี้

6.1 การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน องค์กรต้องดำเนินการการเฝ้าระวัง (Monitor) การวัดผล (Measure) การวิเคราะห์ (Analyze) และการประเมิน (Evaluate) ระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยการดำเนินการดังกล่าวจะทำให้องค์กรรู้ได้ว่าผลลัพธ์เป็นไปตามที่วางแผนหรือไม่อย่างไร

6.2 การตรวจประเมินภายใน องค์กรต้องจัดให้มีการตรวจประเมินภายใน (Internal Audit) ซึ่งการตรวจประเมินภายในเป็นเครื่องมือสำคัญที่ทำให้รู้ว่าระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศที่องค์กรจัดทำขึ้นมานั้น มีความสมบูรณ์ จัดทำครบถ้วนตามข้อกำหนดมีการนำไปปฏิบัติหรือไม่ และได้ผลลัพธ์เป็นอย่างไร

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

ตรวจสอบความเข้าใจ การปฏิบัติและเอกสารบันทึกที่เกี่ยวข้อง

6.3 การทบทวนของผู้บริหาร องค์กรต้องจัดให้มีการประชุมเพื่อรายงานผลของการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศต่อผู้บริหารระดับสูง (Top Management) โดยรายงานถึงการเปลี่ยนแปลงทั้งภายในและการเปลี่ยนแปลงทั้งภายนอกที่มีผลกระทบต่อระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ รายงานผลการประเมินความเสี่ยงและการจัดการความเสี่ยง รายงานผลการเฝ้าระวังด้านความปลอดภัยของสารสนเทศ (Information Security) รายงานผลการตรวจประเมินภายใน (Internal Audit) และข้อบกพร่องจากการตรวจประเมินภายใน เป็นต้น

7. การปรับปรุง (Improvement)

การตรวจประเมินภายใน (Internal Audit) จะพบข้อบกพร่องจากการตรวจประเมินภายในซึ่งเกิดจากการปฏิบัติงานต่างๆ ไม่สอดคล้องกับเกณฑ์ ระเบียบปฏิบัติ หรือวิธีปฏิบัติงานที่องค์กำหนดไว้ มาตรฐานสากล ISO 27001:2013 ได้กำหนดให้องค์กรดำเนินการจัดการและแก้ไขความไม่สอดคล้อง และกำหนดให้มีการดำเนินการปรับปรุงและอย่างต่อเนื่อง ดังนี้

7.1 ความไม่สอดคล้องและการดำเนินการแก้ไข การระบุความไม่สอดคล้อง (Nonconformity) และการแก้ไขความไม่สอดคล้อง (Corrective Action) ต้องดำเนินการอย่างเป็นระบบ และกำหนดให้มีผู้รับผิดชอบและมีบันทึกที่เป็นลายลักษณ์อักษรเกี่ยวกับความไม่สอดคล้องและแนวทางการแก้ไข

7.2 การปรับปรุงอย่างต่อเนื่อง มาตรฐานสากล ISO 27001:2013 กำหนดให้องค์กรปรับปรุงระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศให้มีความเหมาะสม เพียงพอ และมีการปรับปรุงอย่างต่อเนื่อง

มาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001:2013 (Annex A)

มาตรฐานสากล ISO/IEC 27001:2013 ได้กำหนดวัตถุประสงค์ของมาตรการควบคุม (Control Objectives) และมาตรการควบคุม (Controls) ที่ขึ้นทะเบียนอยู่ใน Table A.1 เหมือนมาตรการควบคุมที่อยู่มาตรฐานสากล ISO/IEC 27001:2013 ข้อกำหนด 5 ถึง 18 ในข้อกำหนด 6.1.3 (Sriprapar, 2562) ดังนี้

1. Annex A.5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) โดยมีวัตถุประสงค์เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนดของกฎหมาย ระเบียบ ข้อบังคับ และข้อกำหนดทางธุรกิจต่างๆ ที่เกี่ยวข้อง

2. Annex A.6 โครงสร้างความมั่นคงปลอดภัยของสารสนเทศ (Organization of Information Security) โดยมีวัตถุประสงค์เพื่อสร้างกรอบในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีการจัดโครงสร้างในการควบคุมการลงมือปฏิบัติงาน และการปฏิบัติงานของบุคลากรภายในองค์กร รวมถึงการรักษาความมั่นคงปลอดภัยสารสนเทศในการปฏิบัติงานจากระยะไกล (Teleworking) และการใช้งานอุปกรณ์พกพา (Mobile Device)

3. Annex A.7 ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security) โดยมีวัตถุประสงค์เพื่อให้บุคลากรและผู้ที่ทำสัญญาจ้างเข้าใจบทบาทและหน้าที่ความรับผิดชอบของตนเองเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศขององค์กร ตั้งแต่เริ่มต้นสรรหา ขณะปฏิบัติงาน จนถึงการสิ้นสุดการจ้างงาน

4. Annex A.8 การบริหารจัดการทรัพย์สิน (Asset Management) โดยมีวัตถุประสงค์เพื่อให้มีการระบุทรัพย์สินขององค์กร และมีการบริหารจัดการทรัพย์สินให้มีความมั่นคงปลอดภัยของสารสนเทศอย่างเหมาะสม ตั้งเริ่มต้นนำทรัพย์สินเข้ามาใช้งานภายในองค์กร การกำหนดระดับความสำคัญของข้อมูลและสารสนเทศ การจัดเก็บข้อมูลและสารสนเทศ การเปลี่ยนแปลง การลบ และการทำลายทรัพย์สิน ตลอดจนการเผยแพร่ข้อมูลและสารสนเทศขององค์กร

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

5. Annex A.9 การควบคุมการเข้าถึง (Access Control) โดยมีวัตถุประสงค์เพื่อจำกัดการเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ และควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและข้อมูลสารสนเทศโดยไม่ได้รับการอนุญาต

6. Annex A.10 การเข้ารหัสข้อมูล (Cryptography) โดยมีวัตถุประสงค์เพื่อกำหนดให้ข้อมูลและสารสนเทศมีการเข้ารหัสข้อมูลเป็นไปอย่างเหมาะสมต่อการนำไปใช้งานตามระดับความสำคัญของข้อมูลและสารสนเทศ ตลอดจนป้องกันไม่ให้มีการเปลี่ยนแปลง ปลอมแปลง หรือบิดเบือนข้อมูลและสารสนเทศ

7. Annex A.11 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) โดยมีวัตถุประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และป้องกันการขโมย หรือป้องกันความเสียหาย การแทรกแซงการทำงานที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

8. Annex A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security) โดยมีวัตถุประสงค์เพื่อให้การปฏิบัติงานต่างๆ และการปฏิบัติงานร่วมกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการถูกโจมตีจากผู้ไม่ประสงค์ดีหรือโปรแกรมไม่ประสงค์ดี การบริหารจัดการช่องโหว่ทางต่างๆ ทั้งด้านฮาร์ดแวร์ ซอฟต์แวร์ และเครือข่ายคอมพิวเตอร์ ตลอดจนการป้องกันความสูญหายของข้อมูลสารสนเทศ และมีการบันทึกการเฝ้าระวังหรือบันทึกเหตุการณ์ หรือหลักฐานต่างๆ จากการดำเนินการต่างๆ

9. Annex A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security) โดยมีวัตถุประสงค์เพื่อสร้างความมั่นใจว่าข้อมูลและสารสนเทศบนเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศต่างๆ ได้รับการป้องกันระหว่างการถ่ายโอนไปยังหน่วยภายในองค์กร และหน่วยงานภายนอกองค์กร รวมถึงการไม่เปิดเผยความลับ ซึ่งสะท้อนให้เห็นถึงความต้องการขององค์กรในการปกป้องข้อมูลและสารสนเทศอย่างเหมาะสม

10. Annex A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance) โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศตลอดวงจรชีวิตของการพัฒนาระบบสารสนเทศให้มีการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม

11. Annex A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships) โดยมีวัตถุประสงค์เพื่อให้มีกาป้องกันทรัพยท์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก และรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

12. Annex A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) โดยมีวัตถุประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลสำหรับการบริหารจัดการเหตุขัดข้อง (Incident Management) ให้มีความมั่นคงปลอดภัยของสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนของความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

13. Annex A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management) โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าข้อมูลและสารสนเทศมีความพร้อมใช้ ซึ่งองค์กรมีการบริหารจัดการให้ธุรกิจดำเนินการได้อย่างต่อเนื่อง มีการเตรียมอุปกรณ์ประมวลผลสารสนเทศ บุคลากรและสิ่งต่างๆ ที่เกี่ยวข้องกับดำเนินการทางธุรกิจ

14. Annex A.18 ความสอดคล้อง (Compliance) โดยมีวัตถุประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันทางกฎหมาย ระเบียบ ข้อบังคับ หรือสัญญาจ้างที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

การตรวจประเมินภายในตามข้อกำหนดมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ

คณะแพทยศาสตร์ศิริราชพยาบาลได้รับรองมาตรฐาน ISO/IEC 27001:2013 ผู้บริหารของคณะฯ ได้เล็งเห็นถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศ โดยมอบหมายให้ฝ่ายสารสนเทศเป็นหน่วยงานหลักในการดำเนินกิจกรรมต่างๆ ด้านความมั่นคงปลอดภัยสารสนเทศ กิจกรรมหนึ่งซึ่งถือเป็นหัวใจสำคัญในการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ คือ การตรวจประเมินภายในตามมาตรฐานสากล ISO/IEC 27001:2013 ฝ่ายสารสนเทศดำเนินการแต่งตั้งผู้ตรวจประเมินภายใน และจัดให้มีการตรวจประเมินตามมาตรฐานสากล ISO/IEC 27001:2013 ปีละ 1 ครั้ง ซึ่งการดำเนินกิจกรรมจะยึดหลักปฏิบัติตาม 9 ขั้นตอนดังนี้

ขั้นตอนที่ 1 การเตรียมบุคลากรที่จะทำหน้าที่เป็นผู้ตรวจประเมินภายใน

ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลได้กำหนดบทบาทและมอบหมายหน้าที่ให้กับบุคลากรที่จะปฏิบัติหน้าที่เป็นผู้ตรวจประเมินภายใน (Internal Auditor) โดยผู้ตรวจประเมินภายในต้องมีจริยธรรมของผู้ตรวจประเมินโดยใช้หลักการตรวจประเมิน 6 ประการ คือ ความซื่อสัตย์สุจริต (Integrity), การนำเสนออย่างเป็นธรรม (Fair Presentation), การปฏิบัติงานด้วยความเอาใจใส่อย่างมืออาชีพ (Due Professional Care), การรักษาความลับ (Confidentiality), ความเป็นอิสระ (Independence) และวิธีการที่เน้นหลักฐาน (Evidence-based Approach) และส่งผู้ตรวจประเมินภายในเข้าอบรมให้มีความรู้และความเข้าใจในข้อกำหนดและมาตรการควบคุมของมาตรฐานสากล ISO/IEC 27001:2013 โดยยึดแนวทางการตรวจประเมินซึ่งเป็นหัวใจสำคัญของการตรวจประเมินภายใน 3 เรื่อง (ALshbiel, 2017) คือ

- เกณฑ์การตรวจประเมิน (Audit Criteria) คือ กฎ ระเบียบปฏิบัติ วิธีปฏิบัติงาน ตลอดจนคู่มือการปฏิบัติการที่ซึ่งเขียนขึ้นให้สอดคล้องกับข้อกำหนดและมาตรการควบคุมของมาตรฐานสากล ISO/IEC 27001:2013
- หลักฐานการตรวจประเมิน (Audit Evidence) คือ บันทึก ข้อเท็จจริง หรือข้อมูลต่างๆ ที่ได้จากการสัมภาษณ์ การสังเกต การตรวจสอบจากเอกสาร คู่มือ และแบบฟอร์มของขั้นตอนการปฏิบัติงาน
- สิ่งที่ตรวจพบจากการตรวจประเมิน (Audit Finding) คือ ผลการประเมินหลักฐานการตรวจประเมินที่เก็บรวบรวมได้และเปรียบเทียบกับเกณฑ์การตรวจประเมิน

ขั้นตอนที่ 2 การกำหนดขอบเขตของการตรวจประเมิน

ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศต้องกำหนดพื้นที่ หน่วยงาน หรือระบบงานที่จะดำเนินการตรวจประเมินภายในให้ชัดเจน เพื่อใช้ในการวางแผนตรวจประเมินภายใน โดยพิจารณาถึงขนาดและความซับซ้อนของระบบงานหรือหน่วยงานที่ไปตรวจ รวมถึงการจัดตารางเวลาและผู้ตรวจประเมินภายในที่มีทักษะและความสามารถตรงกับภาระกิจในการตรวจประเมินได้อย่างเหมาะสม

ขั้นตอนที่ 3 การกำหนดช่วงเวลาที่จะทำการตรวจประเมิน

ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลกำหนดให้มีการตรวจประเมินภายในปีละ 1 ครั้ง โดยผู้ตรวจประเมินภายในของฝ่ายสารสนเทศจะแจ้งกำหนดการตรวจประเมิน (Audit Schedule) ล่วงหน้าอย่างน้อย 1 เดือน เพื่อให้ผู้รับการตรวจประเมิน หรือหน่วยงานทราบและเตรียมตัว เตรียมข้อมูลไว้รับการตรวจประเมิน

ขั้นตอนที่ 4 การพิจารณาแนวทางการตรวจประเมิน

การตรวจประเมินภายในครั้งแรก ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลนำรายงานการวิเคราะห์ช่องว่าง (Gap Analysis) ISO/IEC 27001:2013 มาใช้เป็นแนวทางการวางแผนการตรวจประเมิน โดยให้ตรวจสอบจากสิ่งที่ปรากฏในรายงานการวิเคราะห์ช่องว่างที่ระบุว่ายังไม่ได้ทำ หรือยังไม่มี เช่น ยังไม่มีนโยบายความมั่นคงปลอดภัยของสารสนเทศ

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

เป็นลายลักษณ์อักษร เมื่อเข้าทำการตรวจประเมินจะมุ่งเน้นตรวจหานโยบายความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษร หรือกรณีระบุว่ามีแล้วผู้ตรวจประเมินภายในตรวจสอบว่ายังปฏิบัติตามหรือรักษาอยู่ได้หรือไม่

สำหรับการตรวจประเมินในครั้งถัดไปแนะนำให้ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลใช้รายงานการตรวจประเมินจากครั้งก่อนหน้าเพื่อตรวจสอบว่ามีปัญหาหรืออุปสรรคอะไรในการตรวจประเมินครั้งก่อนหน้า เพื่อดูว่าการตรวจประเมินคราวก่อนพบข้อบกพร่องที่หน่วยงานใดมากที่สุดและนำมาใช้ในการจัดทำรายการตรวจประเมิน

ขั้นตอนที่ 5 การวางแผนการตรวจประเมินภายใน

ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล พิจารณาว่าแต่ละหน่วยงานจะถูกตรวจข้อกำหนดและมาตรการควบคุมของมาตรฐาน ISO/IEC 27001:2013 ใดบ้าง จุดที่สำคัญ คือ ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลจะต้องวางแผนการตรวจประเมินภายในให้ตรงกับบริบทของหน่วยงานที่รับการตรวจประเมิน และมีการนำเสนอแผนการตรวจประเมินภายในอย่างเป็นทางการต่อคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Committee) โดยผู้ตรวจประเมินภายในมีการทบทวนแผนการตรวจประเมินภายในและพิจารณาถึงปัจจัยต่อไปนี้ (Russell, 2007)

- ผลลัพธ์และแนวโน้มจากการเฝ้าติดตามแผนงานการตรวจประเมิน
- ความสอดคล้องกับขั้นตอนการดำเนินการของแผนงานการตรวจประเมิน
- ความต้องการและความคาดหวังที่เกิดขึ้นของผู้มีส่วนได้เสีย
- บันทึกเกี่ยวกับแผนงานการตรวจประเมิน
- วิธีการทางเลือกหรือวิธีการใหม่ของการตรวจประเมิน
- ประสิทธิผลของมาตรการจัดการความเสี่ยงที่เกี่ยวเนื่องกับแผนงานการตรวจประเมิน
- ประเด็นการรักษาความลับและความปลอดภัยของข้อมูลเกี่ยวกับแผนงานการตรวจประเมิน
- รายงานผลการทบทวนแผนงานการตรวจประเมินให้แก่ผู้บริหารสูงสุด

ขั้นตอนที่ 6 การดำเนินการตรวจประเมินภายใน

ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล เริ่มการประชุมโดยผู้นำการตรวจประเมิน (Lead Auditor) ดำเนินการยืนยันขอบเขตของการตรวจประเมินภายในและแผนการตรวจประเมินภายใน และแนะนำตัวคณะผู้ตรวจประเมินภายใน องค์กรควรจัดการประชุมเปิดร่วมกับฝ่ายบริหารของผู้รับการตรวจประเมินภายใน

ระหว่างการตรวจประเมินผู้ตรวจประเมินภายในรวบรวมและทวนสอบข้อมูลที่เกี่ยวข้องกับวัตถุประสงค์ขอบข่าย และเกณฑ์การตรวจประเมิน รวมทั้งข้อมูลเกี่ยวกับจุดเชื่อมโยงระหว่างหน่วยงาน กิจกรรม และกระบวนการโดยเครื่องมือการสุ่มตัวอย่าง และเก็บรวบรวมเพื่อใช้เป็นหลักฐานการตรวจประเมิน ผู้ตรวจประเมินภายในบันทึกหลักฐานการตรวจประเมินซึ่งนำไปสู่สิ่งที่พบจากการตรวจประเมินโดยรวบรวมข้อมูลต่างๆ จากการสัมภาษณ์ การสังเกต และการทบทวนเอกสารที่เกี่ยวข้อง นอกจากนี้ในระหว่างการตรวจประเมินผู้ตรวจประเมินภายในมีการพบปะหารือกันเป็นระยะๆ เพื่อแลกเปลี่ยนข้อมูล ประเมินความคืบหน้าของการตรวจประเมิน และมอบหมายงานใหม่ระหว่างสมาชิกของคณะผู้ตรวจประเมินภายใน

ในการตรวจประเมินผู้ตรวจประเมินภายในจะดำเนินการประเมินผลหลักฐานการตรวจประเมิน (Audit Evidence) โดยเทียบกับเกณฑ์การตรวจประเมิน (Audit Criteria) เพื่อตัดสินสิ่งที่พบจากการตรวจประเมิน สิ่งที่พบจากการตรวจประเมินสามารถระบุเป็นความสอดคล้องหรือความไม่สอดคล้องกับเกณฑ์การตรวจประเมิน และแนวปฏิบัติที่ดีพร้อมหลักฐานสนับสนุน โอกาสเพื่อการปรับปรุงและข้อเสนอแนะสำหรับผู้รับการตรวจประเมิน สำหรับการบันทึกความไม่สอดคล้องและหลักฐานการตรวจประเมินที่

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

นำมาสนับสนุนความไม่สอดคล้องอาจแบ่งเป็นประเภทต่างๆ โดยผู้ตรวจประเมินภายในจะทบทวนความไม่สอดคล้องร่วมกับผู้รับการตรวจประเมินเพื่อยอมรับว่าหลักฐานการตรวจประเมินมีความถูกต้องและความไม่สอดคล้องเป็นที่เข้าใจตรงกันระหว่างผู้รับการตรวจประเมินและผู้ตรวจประเมินภายใน

เมื่อเสร็จสิ้นการตรวจประเมินในแต่ละวันผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลจะประชุมหารือร่วมกันเพื่อจัดทำข้อสรุปจากการตรวจประเมิน จัดทำข้อแนะนำ โดยระบุไว้ในแผนการตรวจประเมิน ซึ่งข้อสรุปจากการตรวจประเมินสามารถนำไปสู่ข้อแนะนำเพื่อการปรับปรุง หรือกิจกรรมการตรวจประเมินในอนาคต

ขั้นตอนที่ 7 การดำเนินการในการประชุมปิด

ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลนำเสนอสิ่งที่พบจากการตรวจประเมินและข้อสรุปจากการตรวจประเมินให้ฝ่ายผู้บริหารของฝ่ายสารสนเทศ และผู้รับการตรวจประเมินตลอดจนบุคคลที่รับผิดชอบได้ทราบถึงผลการตรวจประเมินภายใน โดยผู้รับการตรวจประเมินจะดำเนินการกำหนดกรอบระยะเวลาสำหรับแผนการปฏิบัติการแก้ไขสิ่งที่พบจากการตรวจประเมิน (Corrective Action Plan) ซึ่งผู้ตรวจประเมินภายในแจ้งวิธีการรายงานผลการตรวจประเมินและระยะเวลาในการรายงานผลการตรวจประเมินให้ฝ่ายบริหารของผู้รับการตรวจประเมินทราบ

ขั้นตอนที่ 8 การจัดเตรียมและจัดส่งรายงานการตรวจประเมิน

ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลจัดทำรายงานผลการตรวจประเมินภายในและจัดส่งรายงานการตรวจประเมินภายในตามระยะเวลาที่ตกลงไว้ ซึ่งกรณีล่าช้าผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลจะแจ้งเหตุผลให้ผู้รับการตรวจประเมิน กรณีที่พบความไม่สอดคล้องตามข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013 ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลจะดำเนินการออกใบการร้องขอให้ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลดำเนินการแก้ไขข้อบกพร่องหรือความไม่สอดคล้องตามข้อกำหนดที่เกิดขึ้น (Corrective Action Request: CAR)

ขั้นตอนที่ 9 การตรวจติดตามผลการแก้ไขข้อบกพร่อง

เมื่อฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลได้รับรายงานผลการตรวจประเมินภายในตามข้อกำหนดมาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ ขั้นตอนต่อไปการปฏิบัติการแก้ไขข้อบกพร่อง ซึ่งเจ้าหน้าที่และบุคลากรที่เกี่ยวข้องจะร่วมกันปฏิบัติการแก้ไขข้อบกพร่อง โดยมีการระดมสมอง (Brain Storm) เพื่อรวบรวมความคิดเห็นอย่างเป็นระบบของผู้ที่มีส่วนเกี่ยวข้อง โดยใช้แผนภูมิก้างปลา (Fish Bone Diagram) ซึ่งใช้สาเหตุหลักพื้นฐานทั่วไป 6 M ได้แก่ Man, Materials, Machine, Method, Management และ Measure

เมื่อทราบสาเหตุของความบกพร่องที่แท้จริงและครบถ้วนทุกสาเหตุของความบกพร่องแล้ว ก็เข้ามาสู่กระบวนการในการปฏิบัติการแก้ไขตามสาเหตุที่แท้จริง โดยจัดทำแผนการปฏิบัติการแก้ไขสิ่งที่พบจากการตรวจประเมินซึ่งจะกำหนดกิจกรรม วิธีการ ผู้รับผิดชอบ ระยะเวลา หรือสถานที่สำหรับการปฏิบัติ จากนั้นจะตอบกลับลงในใบการร้องขอให้ดำเนินการแก้ไขข้อบกพร่อง หรือความไม่สอดคล้องตามข้อกำหนดที่เกิดขึ้นส่งกลับไปยังผู้ตรวจประเมินภายใน และดำเนินกิจกรรมตามแผนการปฏิบัติการแก้ไขสิ่งที่พบจากการตรวจประเมินที่ระบุไว้ขยายผลไปสู่พื้นที่ กระบวนการ กิจกรรม ที่พบความไม่สอดคล้องที่เกิดขึ้นเพื่อไม่ให้ปัญหาดังกล่าวกลับมาเกิดซ้ำอีก และกำหนดมาตรฐาน วิธีการ หรือระยะเวลามาติดตามความคืบหน้า ของการนำไปปฏิบัติให้ต่อเนื่อง หรือกำหนดเป็นมาตรฐานในการทำงานอย่างถาวร

ผู้ตรวจประเมินภายในของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลจะดำเนินการตรวจติดตามผลการแก้ไขข้อบกพร่องขึ้นตามกรอบเวลาที่ตกลงไว้ และผู้รับการตรวจประเมินจะแจ้งสถานะของการดำเนินการให้บุคคลที่บริหารแผนงานการตรวจประเมินและผู้ตรวจประเมิน

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

ภายในให้ทราบตามความเหมาะสม และนำไปทวนสอบในการประเมินครั้งถัดไป

ปัจจัยสำคัญที่ช่วยส่งเสริมให้การตรวจประเมินภายในด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างมีประสิทธิภาพ คือ ผู้ตรวจประเมินภายในต้องมีความรู้และทักษะในการตรวจประเมินโดยใช้คำถามนำทางเพื่อค้นหาหลักฐานการตรวจประเมิน (Audit Evidence) และมีความรู้ความเข้าใจในข้อกำหนดของ ISO/IEC 27001:2013 รวมถึงนโยบาย ระเบียบปฏิบัติ วิธีปฏิบัติงานขององค์กรเพื่อใช้เป็นเกณฑ์การตรวจประเมิน (Audit Criteria) จากนั้นผู้ตรวจประเมินภายในจะพิจารณาหลักฐานการตรวจประเมินเปรียบเทียบกับเกณฑ์การตรวจประเมินว่าสิ่งที่ตรวจพบจากการตรวจประเมิน (Audit Finding) เช่น ขั้นตอนการปฏิบัติงาน คู่มือปฏิบัติงาน ตลอดจนแบบฟอร์มที่เกี่ยวข้องในการปฏิบัติงานนั้นๆ บุคลากรภายในหน่วยงานนำไปปฏิบัติสอดคล้องหรือไม่สอดคล้องกับข้อกำหนด ของ ISO/IEC 27001:2013 หรือสิ่งที่หน่วยงานกำหนดไว้ หากตรวจพบการปฏิบัติที่ไม่สอดคล้องกับข้อกำหนดและสิ่งที่หน่วยงานกำหนดไว้ ผู้ตรวจประเมินภายในจะจัดทำรายงานผลการตรวจประเมินภายในตามมาตรฐานสากล ISO/IEC 27001:2013 เพื่อนำเสนอต่อผู้บริหารของฝ่ายสารสนเทศ, บุคลากรของคณะฯ และผู้บริหารคณะฯ ให้ทราบและหาแนวทางในการดำเนินการแก้ไขต่อไป

นอกจากนี้ระหว่างกิจกรรมการตรวจประเมินภายในสิ่งหนึ่งที่ผู้ตรวจประเมินภายในและผู้รับการตรวจประเมินจะต้องคำนึงถึงและต้องปฏิบัติ คือ ให้เกียรติซึ่งกันและกัน และต้องตัดบทบาทหน้าที่ของเพื่อนร่วมงานออกไป ทั้งนี้เพื่อให้การตรวจประเมินภายตามมาตรฐานสากล ISO/IEC 27001:2013 มีอิสระในการทำงาน มีความโปร่งใส ไม่มีอคติในการตรวจประเมิน และไม่ถูกครอบงำโดยบุคคลใดบุคคลหนึ่ง สำหรับผู้นำการตรวจประเมิน (Lead Auditor) จะต้องควบคุมสถานการณ์และบรรยากาศของการตรวจประเมินเพื่อให้กิจกรรมการตรวจประเมินภายในดำเนินไปอย่างเรียบร้อย ไม่มีปัญหา หรืออุปสรรคต่าง ๆ ที่อาจเกิดขึ้น และยังเป็นการป้องกันการเกิดข้อพิพาท หรือเหตุการณ์ไม่พึงประสงค์อันจะส่งผลกระทบต่อการตรวจประเมินภายใน และการปฏิบัติงานอื่น ๆ ที่ต้องปฏิบัติร่วมกันในบทบาทหน้าที่ปกติ สิ่งหนึ่งที่ฝ่ายสารสนเทศคณะแพทยศาสตร์ศิริราชพยาบาลได้ตระหนักถึงและเห็นความสำคัญคือ การจัดตั้งทีมขึ้นมาเพื่อตรวจสอบกระบวนการทำงานของตรวจประเมินภายใน ทั้งนี้เพื่อเป็นกระจกเงาสะท้อนให้เห็นถึงการปฏิบัติหน้าที่ของตรวจประเมินภายใน ซึ่งจะเป็นการเพิ่มประสิทธิภาพในการตรวจประเมินภายในให้ดียิ่งขึ้น โดยมุ่งเน้นกระบวนการปฏิบัติงานที่มีการปรับปรุงและพัฒนาอย่างต่อเนื่องตามหลักการของ PDCA

สรุป

การตรวจประเมินภายในตามข้อกำหนดมาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศเป็นกิจกรรมบังคับสำหรับหน่วยงานต้องดำเนินการ โดยองค์กรหรือหน่วยงานต้องกำหนดและมอบหมายหน้าที่ให้กับบุคลากรที่จะปฏิบัติหน้าที่เป็นผู้ตรวจประเมินภายในต้องมีความรู้และความเข้าใจในข้อกำหนดมาตรฐาน (Requirements) และมาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 และดำเนินการตรวจประเมินเพื่อตรวจสอบการปฏิบัติงานให้สอดคล้องกับกฎ ระเบียบปฏิบัติ วิธีปฏิบัติงาน ตลอดจนคู่มือการปฏิบัติการที่องค์กรหรือหน่วยงานนั้นๆ จัดทำขึ้น ซึ่งข้อมูลจะได้จากการสัมภาษณ์ การสังเกต การตรวจสอบจากบันทึก ข้อเท็จจริง เอกสารคู่มือ และแบบฟอร์มของขั้นตอนการปฏิบัติงาน โดยยึดหลักสำคัญของการตรวจประเมินภายในตามข้อกำหนดมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ คือ พิจารณาจากหลักฐานการตรวจประเมิน (Audit Evidence) เปรียบเทียบกับเกณฑ์การตรวจประเมิน (Audit Criteria) และสิ่งที่ตรวจพบจากการตรวจประเมิน (Audit Finding) ปฏิบัติได้สอดคล้องหรือไม่สอดคล้องกับเกณฑ์การตรวจประเมิน

ข้อเสนอแนะ

Received: November 11, 2019, Revised: August 17,2020 , Accepted: September 11 2020
http://doi.org/

ผู้ตรวจประเมินภายในต้องดำเนินการการตรวจประเมินภายในตามข้อกำหนดมาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศอย่างน้อยปีละ 1 ครั้ง และวางแผนการตรวจประเมินให้ครอบคลุมทุกกระบวนการในการปฏิบัติงานโดยพิจารณาจากขอบเขตที่องค์กรกำหนดไว้ และผู้ตรวจประเมินภายในสามารถตรวจประเมินโดยลงลึกในรายละเอียดของการตรวจประเมินได้ตามเกณฑ์ปฏิบัติที่ระบุไว้ใน ISO 27002 (Information technology - Security techniques - Code of practice for information security management)

เอกสารอ้างอิง

บูรณะศักดิ์ มาดหมาย. (2551). การปรับปรุงอย่างต่อเนื่องตามแบบ PDCA. สืบค้นเมื่อ 5 กันยายน 2562, จาก http://inf.ocs.ku.ac.th/document/pdf/Kaizen_PDCA.pdf

ปริญญ์ เสรีพงศ์. (2556). 7 ขั้นตอนวางแผนตรวจประเมินภายใน (Internal Audit) ISO 27001:2013, สืบค้นเมื่อ 2 กันยายน 2562, จาก http://www.club27001.com/2014/12/7-Steps-to-planning-ISO-27001-2013-Audit-Plan.html

ปริญญ์ เสรีพงศ์. (2556). มาตรการ (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001:2013, สืบค้นเมื่อ 2 กันยายน 2562, จาก http://www.club27001.com/2014/02/ISO-27001-2013-Controls-requirement.html

ปริญญ์ เสรีพงศ์. (2557). รีวิว ISO 27001 : 2013 - ตอนที่1 พื้นฐานความมั่นคงปลอดภัยของสารสนเทศ. [เว็บบล็อก]. สืบค้นเมื่อ 6 พฤศจิกายน 2562, จาก http://www.club27001.com/2014/01/review-iso27001-2013-part1.html

ปริญญ์ เสรีพงศ์. (2557). รีวิว ISO 27001 :2013 - ตอนที่2 ความสำคัญของการประเมินความเสี่ยงสารสนเทศ. [เว็บบล็อก]. สืบค้นเมื่อ 6 พฤศจิกายน 2562, จาก http://www.club27001.com/2014/01/review-iso27001-2013-part1.html

วชิราพร ปัญญาพินิจนุกุร. (2552). มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001 และ ISO/IEC 17799 ฉบับประเทศไทย. [เว็บบล็อก]. สืบค้นเมื่อ 6 พฤศจิกายน 2562, จาก http://oknation.nationtv.tv/blog/weblog/2009/02/27/entry-4

สุวันต์นา เสมอเนตร. (2562). การพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC). วารสารวิชาการสาธารณสุข, 28(1), 117-132.

ALshbiel, S.O. (2017). Internal Auditing Effectiveness Success Model: A Study on Jordanian Industrial Firms. Al al-Bayt University, Jordan.

Perry L. Johnson. (2018). ISO 27001, สืบค้นเมื่อ 2 กันยายน 2562, จาก http://www.pjrthailand.com/standards/iso-27001

Russell, J.P. (2007). The Internal Auditing Pocket Guide, Second Edition: Preparing, Performing, Reporting, and Follow-up. 2nd Ed. Milwaukee, WI: ASQ Quality Press.

Sriprapar Ngamhongtong. (2562). อะไรเปลี่ยนไปใน ISO/IEC 27001 เวอร์ชั่นใหม่. สืบค้นเมื่อวันที่ 6 พฤศจิกายน 2562, จาก https://www.isotoyou.com/index.php/article/447-iso27001-dis-what-change.html