วารสาร Mahidol R2R e-Journal ปีที่ 8 ฉบับที่ 2 ประจำเดือนพฤษภาคม-สิงหาคม 2564
Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

องค์กรกับการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ
Organization and Information Technology Risk Assessment

สมหทัย จารุพิมล[1*] และ นภสินธุ์ บุญมาก[1]
SOMHATAI JARUPIMON[1*] and NAPHASIN BOONMAK[2]

บทคัดย่อ

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นกระบวนการทำงานในการป้องกันข้อมูลสารสนเทศที่เป็นความลับ มีความสำคัญ และป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามทางเทคโนโลยีสารสนเทศที่สามารถบุกรุกโจมตีข้อมูลสารสนเทศขององค์กร ซึ่งการประเมินความเสี่ยงในเรื่องนี้เป็นแนวทางในการช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กรอีกแนวทางหนึ่ง โดยการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศมุ่งเน้นการปกป้องข้อมูลสารสนเทศ 3 ประการ ได้แก่ ความลับ, ความถูกต้อง และความพร้อมใช้งาน เพื่อให้บรรลุการปกป้องข้อมูลสารสนเทศดังกล่าว องค์กรต้องประเมินความเสี่ยงในด้านการเข้าถึงข้อมูลสารสนเทศ, ความถูกต้อง ความครบถ้วนของข้อมูลสารสนเทศ, ความพร้อมใช้ของข้อมูลสารสนเทศและการบริหารจัดการด้านเทคโนโลยีสารสนเทศ รวมถึงการประเมินความเสี่ยงด้านอื่น ๆ ที่เกี่ยวข้องและมีผลกระทบต่อการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งทางตรงและทางอ้อม โดยใช้กระบวนการบริหารความเสี่ยงทั้ง 6 ขั้นตอน

ดังนั้นหากองค์กรดำเนินการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศควบคู่กับการประเมินความเสี่ยงในเรื่องอื่น ๆ จะช่วยให้สินทรัพย์ขององค์กรให้รอดพ้นจากความเสี่ยงทั่ว ๆ ไป และความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอีกด้วย และเพื่อให้การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศสำเร็จลุล่วงตามเป้าหมายที่กำหนดไว้ องค์กรต้องให้ความสำคัญและมอบหมายให้ผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ และฝ่ายบริหารขององค์กรให้การสนับสนุนทรัพยากรที่จำเป็น เหมาะสมและได้มาตรฐาน ตลอดจนการสื่อสารภายในองค์กร และการสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และการใช้งานข้อมูลสารสนเทศให้กับบุคลากรทุกระดับภายในองค์กร

คำสำคัญ: การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ; การบริหารความเสี่ยง; การประเมินความเสี่ยง; การจัดการความเสี่ยง

1* ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล
1 Siriraj Information Technology Department, Faculty of Medicine Siriraj Hospital, Mahidol University
* Corresponding Author: somhatai.jar@mahidol.ac.th

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

Abstract

Information technology risk assessment is a process to protect confidential information that is important and prevent damage that may occur from information technology threats that can invade the organization's information. The risk assessment in this regard is another way to help support the success of the organization's mission. The information technology risk assessment focuses on protecting information in 3 areas, including confidentiality, accuracy, and availability. To achieve the protection of the said information the organization must assess the risk of access to information, accuracy and completeness of information, availability of information and management of information technology. Including other risk assessments related and affecting the assessment of information technology risks, both directly and indirectly by using the risk management process in all 6 steps.

Therefore, if the organization conducts a risk assessment and manages information technology risks together with other risk assessments will help the organization's assets escape the general risks and risks associated with information technology. To complete the risk assessment of information technology in accordance with the set goals. Corporate executives must give priority and assign information technology experts to operate and support necessary, appropriate and standardized resources. Including the need to communicate within the organization to raise awareness about information security and use of information to personnel at all levels within the organization.

Keywords: Information technology risk assessment; Risk management; Risk assessment; Risk Treatment

บทนำ

การเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศในปัจจุบันเกิดขึ้นอย่างรวดเร็ว ส่งผลให้องค์กรต่าง ๆ ไม่ว่าจะเป็นหน่วยงานภาครัฐ หรือภาคเอกชนต้องเผชิญกับความไม่แน่นอน การเปลี่ยนแปลงที่เกิดขึ้นทำให้องค์กรต้องมีการปรับตัวรับมือกับการเปลี่ยนแปลงอยู่ตลอดเวลาเพื่อจะทำให้องค์กรสามารถดำเนินงานตามวิสัยทัศน์ นโยบาย แผน ยุทธศาสตร์ กลยุทธ์ ได้ตรงตามเป้าหมาย หรือวัตถุประสงค์ที่องค์กรได้กำหนดไว้ การนำการบริหารความเสี่ยง (Risk Management) มาใช้เพื่อหามาตรการหรือวิธีการลดผลกระทบและโอกาสที่อาจก่อให้เกิดความเสียหายขึ้น นอกจากนี้องค์กรส่วนใหญ่มุ่งหวังที่จะนำระบบสารสนเทศและเทคโนโลยีสารสนเทศเข้าไปช่วยในการปฏิบัติงานให้มีความสะดวก รวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น แต่การนำเทคโนโลยีสารสนเทศมาใช้ย่อมมีความเสี่ยงหลายประการด้วยกัน ดังนั้นนอกจากการบริหารความเสี่ยงในเรื่องทั่ว ๆ ไปแล้ว องค์กรต้องให้ความสำคัญกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเช่นกัน

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ กระบวนการการทำงานที่ช่วยให้องค์กรสามารถสร้างความสมดุลของต้นทุนเชิงเศรษฐศาสตร์และการดำเนินธุรกิจ ระหว่างมาตรการในการป้องกันและการบรรลุผลสำเร็จของพันธกิจ ด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจ

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

ขององค์กร ด้วยเหตุนี้การวางแผนและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงเป็นเรื่องสำคัญของแต่ละองค์กร และควรมีการเตรียมการที่ดี หากองค์กรไม่มีการบริหารจัดการและรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ อาจส่งผลกระทบต่อการดำเนินงานและสร้างความเสียหายต่อองค์กรได้ทั้งในด้านการพัฒนาองค์กร การพัฒนาบุคลากร ความคุ้มค่าทางงบประมาณ

ดังนั้นการประเมินความเสี่ยงและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงต้องมีทั้งการวางแผน การประเมินทั้งโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น และสามารถประเมินเป็นเชิงปริมาณหรือเชิงคุณภาพได้และการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศย่อมเป็นหลักประกันอีกทางหนึ่งที่สร้างความเชื่อมั่นได้ว่าการดำเนินงานต่าง ๆ ขององค์กรนั้นเป็นไปตามวัตถุประสงค์ เนื่องจากการประเมินความเสี่ยงเป็นการวิเคราะห์และคาดการณ์สิ่งที่จะเกิดขึ้นในอนาคตได้ครอบคลุมทุกแง่มุมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ทำให้องค์กรมีการวางแผนป้องกัน ตลอดจนหาแนวทางในการบริหารจัดการเพื่อลดความเสียหายที่จะเกิดขึ้นได้

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง โอกาสที่จะเกิดเหตุการณ์หรือโอกาสเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใดใดที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงินและการบริหาร โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสเกิด (Likelihood) ขึ้นของเหตุการณ์นั้น ๆ ซึ่งความเสี่ยงจำแนกได้เป็น 4 ลักษณะ คือ

- ความเสี่ยงด้านกลยุทธ์
- ความเสี่ยงทางด้านการเงิน
- ความเสี่ยงทางด้านการปฏิบัติงาน
- ความเสี่ยงทางด้านกฎหมาย และข้อกำหนดผูกพันองค์กร

ปัจจัยความเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงซึ่งทำให้ไม่บรรลุวัตถุประสงค์ที่องค์กรหรือหน่วยงานกำหนดไว้ โดยต้องระบุได้ว่าเหตุการณ์นั้นจะเกิดที่ไหน เกิดขึ้นเมื่อใด จะเกิดขึ้นได้อย่างไร และทำไมถึงเกิดขึ้น ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อใช้ในการวิเคราะห์และกำหนดมาตรการลดความเสี่ยงได้อย่างถูกต้อง ที่มาของปัจจัยความเสี่ยงสามารถพิจารณาได้ 2 ช่องทาง (จิรพร สุเมธีประสิทธิ์, 2554) คือ

- ปัจจัยภายนอกองค์กร เช่น เศรษฐกิจ สังคม การเมือง กฎหมาย ฯลฯ
- ปัจจัยภายในองค์กร เช่น กฎระเบียบข้อบังคับ ระบบการทำงาน ประสบการณ์ของบุคลากรภายในองค์กร ฯลฯ

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และระดับของความเสี่ยง โดยการประเมินจากโอกาสเกิด (Likelihood) และผลกระทบ (Impact) ซึ่งเมื่อประเมินความเสี่ยงเสร็จแล้วจะทำให้องค์กรทราบถึงระดับของความเสี่ยง (Degree of Risk) โดยองค์กรจะนำผลการประเมินความเสี่ยงไปบริหารจัดการความเสี่ยงต่อไป

โอกาสเกิด (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง โดยแต่ละองค์กรจะกำหนดเกณฑ์ของระดับโอกาสเกิดความเสี่ยงเป็นระดับต่าง ๆ เช่น โอกาสเกิดสูงมาก โอกาสเกิดสูง โอกาสเกิดปานกลาง โอกาสเกิดน้อย และโอกาสเกิดน้อยมาก และกำหนดนิยามของระดับโอกาสเกิดแต่ละระดับให้ชัดเจน

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

ผลกระทบ (Impact) หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง แต่ละองค์กรจะกำหนดระดับผลกระทบในแต่ละด้านแตกต่างกัน เช่น ผลกระทบด้านประสิทธิผล ผลกระทบด้านมูลค่าทางการเงิน ผลกระทบด้านชื่อเสียงและภาพลักษณ์ขององค์กร ผลกระทบด้านความปลอดภัยของชีวิตบุคลากร เป็นต้น นอกจากนี้แต่ละองค์กรต้องกำหนดนิยามของระดับผลกระทบที่เกิดขึ้นในแต่ละด้านให้ชัดเจน

ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสเกิดและผลกระทบของแต่ละปัจจัยเสี่ยง โดยแต่ละองค์กรจะมีกำหนดเกณฑ์การยอมรับความเสี่ยงแตกต่างกัน เช่น บางองค์กรแบ่งระดับของความเสี่ยงเป็น 5 ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก ในขณะที่บางองค์กรแบ่งระดับของความเสี่ยงเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และน้อย ซึ่งขึ้นอยู่กับบริบทของแต่องค์กร (กรธัช อยู่สุข, 2553)

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการดำเนินงานขององค์กรที่เป็นระบบและต่อเนื่อง และเมื่อนำมาประยุกต์ใช้ร่วมกับแนวคิดการบริหารงานคุณภาพ PDCA หรือ Plan-Do-Check-Act (บูรณะศักดิ์ มาดหมาย, 2551) เพื่อช่วยลดโอกาสเกิดเหตุการณ์ความเสี่ยงหรือลดผลกระทบที่จะสร้างความเสียหายให้องค์กรได้ในอนาคต โดยการบริหารความเสี่ยงนั้น องค์กรจะต้องบริหารความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ หรือควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กรเป็นสำคัญ ซึ่งการบริหารความเสี่ยงจะมีวิธีการจัดการความเสี่ยงหลายวิธีดังนี้

- การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่เกิดขึ้น เนื่องจากองค์กรพิจารณาวิธีการจัดการความเสี่ยงแล้วพบว่าไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง หรืออยู่ในวิสัยที่องค์กรนั้นยอมรับได้
- การลดความเสี่ยง หรือการควบคุมความเสี่ยง (Risk Reduction) เป็นวิธีการหาทางป้องกัน การปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่เพื่อลดโอกาสที่จะเกิด หรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้
- การกระจายความเสี่ยง หรือการถ่ายโอนความเสี่ยง (Risk Transfer) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้บุคคลอื่นที่มิใช่บริษัทประกันโดยสัญญา หรือการถ่ายโอนความเสี่ยงไปให้บริษัทประกันภัยตามรูปแบบและเงื่อนไขที่องค์กรต้องการให้ช่วยแบ่งความรับผิดชอบไป
- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการจัดการความเสี่ยงที่น่าจะเป็นวิธีสุดท้ายที่ได้รับการพิจารณา โดยความเสี่ยงอยู่ในระดับสูงมากและองค์กรไม่อาจยอมรับได้ จึงต้องตัดสินใจหลีกเลี่ยง หรือยกเลิกโครงการ/กิจกรรมนั้น

การควบคุม (Control) หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ

- การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยง และข้อผิดพลาดตั้งแต่แรก
- การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว
- การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

- การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องหรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

กระบวนการบริหารความเสี่ยง

แนวปฏิบัติสำหรับกระบวนการบริหารความเสี่ยงโดยทั่วไปที่หลายองค์กรเลือกใช้ จะยึดหลักเกณฑ์และแนวทางการบริหารความเสี่ยงตามมาตรฐาน ISO 31000 (Risk Management) มีขั้นตอนการดำเนินงาน 6 ขั้นตอน (เกียรติพงษ์ อุดมธนะธีระ,2561) ดังนี้

1. การกำหนดวัตถุประสงค์ (Establish the context)

การกำหนดวัตถุประสงค์และเป้าหมายการดำเนินงานต้องกำหนดให้สอดคล้องกับวิสัยทัศน์ พันธกิจขององค์กร โดยยึดหลัก 5 ประการ คือ มีความชัดเจน (Specific), สามารถวัดผลได้ (Measurable), สามารถปฏิบัติได้ (Achievable), มีความสมเหตุสมผล (Reasonable) และมีกรอบเวลา (Time constrained) ในการดำเนินงาน

2. การระบุความเสี่ยง (Risk Identification)

การระบุเหตุการณ์หรือโอกาสเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใดใดที่มีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร ซึ่งเหตุการณ์นั้นอาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน หรืออาจเกิดขึ้นในอนาคต

3. การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงต้องพิจารณาโอกาสเกิด ความถี่ของเหตุการณ์ที่จะเกิด และผลกระทบต่อองค์กรในด้านต่าง ๆ จากนั้นจัดระดับของความเสี่ยงโดยเปรียบเทียบกับเกณฑ์ที่องค์กรกำหนดไว้ โดยองค์กรสามารถประเมินความเสี่ยงได้หลากหลายวิธี ซึ่งแนวทางที่ใช้ในการวิเคราะห์ความเสี่ยงที่นิยมใช้กันในปัจจุบัน มีอยู่ 2 วิธี ดังนี้

3.1 การวิเคราะห์ความเสี่ยงตามทรัพย์สิน (Asset-Based Risk Assessment) เป็นการประเมินความเสี่ยงที่เกิดขึ้นกับทรัพย์สินขององค์กรโดยตรง ซึ่งประกอบด้วยขั้นตอนหลักๆ คือ

- จัดทำทะเบียนทรัพย์สิน (Inventory of Asset) เพื่อระบุทรัพย์สินสารสนเทศที่สำคัญที่ต้องได้รับการปกป้อง
- พิจารณาถึงภัยคุกคาม (Threat) ที่อาจทำอันตรายต่อทรัพย์สินสารสนเทศ และจุดอ่อน (Vulnerability) ในตัวทรัพย์สิน กระบวนการ หรือมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่อาจเป็นช่องทางให้ภัยคุกคามเหล่านั้นเข้าทำอันตรายต่อทรัพย์สินได้
- ประเมินระดับผลกระทบ (Impact) ต่อองค์กร และโอกาส (Probability) ที่จะเกิดเหตุการณ์ความเสี่ยงขึ้น
- กำหนดระดับของความเสี่ยงตามเกณฑ์ที่องค์กรกำหนดไว้

3.2 การวิเคราะห์ความเสี่ยงตามเหตุการณ์ (Scenario- Based Risk Assessment) เป็นการประเมินความเสี่ยงโดยอาศัยประสบการณ์หรือเหตุการณ์ที่เกิดขึ้นในอดีตเป็นข้อมูลพื้นฐาน หรืออาศัยสถานการณ์ที่หลากหลายที่จะนำไปใช้เป็นข้อมูลในการสร้างการแจกแจงของความเสี่ยงที่อาจเกิดขึ้น เพื่อหาเหตุการณ์หรือสถานการณ์ที่มีความน่าจะเป็นมากที่สุด และหาเหตุการณ์หรือสถานการณ์ที่เลวร้ายที่สุดที่อาจเกิดขึ้นกับองค์กรได้ในอนาคต (จริญญา จันทร์ปาน, 2558)

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

4. การประเมินความเสี่ยง (Risk Evaluation)

เมื่อวิเคราะห์ความเสี่ยงเรียบร้อยแล้ว ขั้นตอนต่อไปคือการประเมินความเสี่ยงโดยพิจารณาจากระดับของความเสี่ยงและจัดลำดับความสำคัญของความเสี่ยงที่จะส่งผลกระทบต่อองค์กรตามกฎเกณฑ์ที่แต่ละองค์กรกำหนดไว้ ซึ่งความเสี่ยงที่องค์กรสามารถยอมรับได้ต้องจัดทำเป็นรายงานและนำเสนอต่อผู้บริหารขององค์กรให้ทราบและหาวิธีดำเนินการกรณีเหตุการณ์ความเสี่ยงนั้น ๆ เกิดขึ้น สำหรับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้จะต้องดำเนินการจัดการความเสี่ยงต่อไป

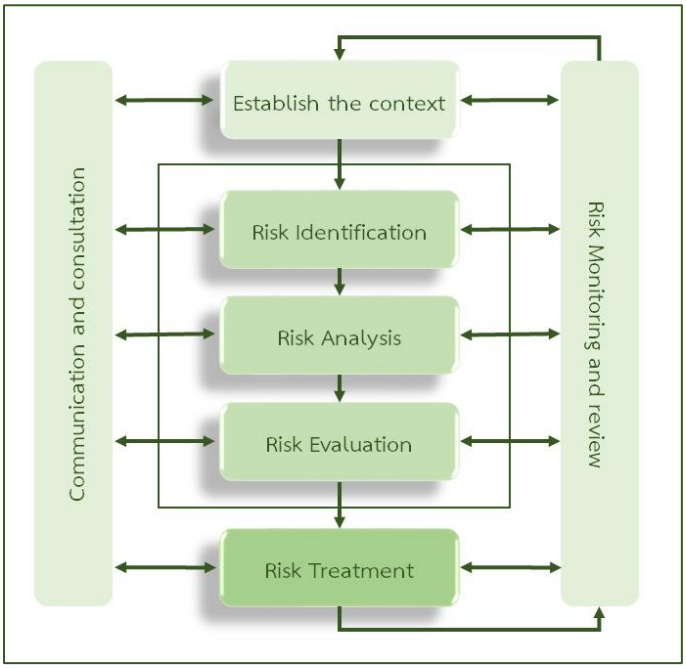
5. การจัดการความเสี่ยง (Risk Treatment)

หลังจากการประเมินความเสี่ยงจะต้องมีการรายงานความเสี่ยงให้ผู้บริหารองค์กรได้ทราบ และเลือกแนวทางในการจัดการความเสี่ยงโดยประเมินจากปัจจัย 2 ประการ คือ ความคุ้มค่าของต้นทุนที่จะต้องใช้ในการบริหารจัดการและผลตอบแทนที่จะได้รับกลับคืนมายังองค์กร และความเป็นไปได้ของประสิทธิผลและความสำเร็จในการบริหารจัดการความเสี่ยงนั้น เมื่อเลือกแนวทางในการจัดการความเสี่ยงได้แล้วจะต้องดำเนินการจัดทำแผนจัดการความเสี่ยง (Risk Treatment Plan: RTP) เพื่อใช้เป็นหลักในการดำเนินงานจัดการความเสี่ยงต่อไป

นอกจากนี้องค์กรต้องตระหนักอยู่เสมอว่าไม่มีความเสี่ยงใดที่ถูกจัดการแล้วจะหมดไป ดังนั้นแนวทางในการจัดการความเสี่ยงที่องค์กรสามารถนำมาใช้ในการปฏิบัติได้ คือ ลดความเสี่ยงให้อยู่ในระดับที่องค์กรสามารถยอมรับได้ ทั้งนี้การลดความเสี่ยงลงสามารถปฏิบัติได้ 2 แนวทาง คือ ลดโอกาสเกิดเหตุการณ์ความเสี่ยง หรือลดผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงนั้น ๆ

6. การเฝ้าสังเกตและทบทวนความเสี่ยง (Risk Monitoring and review)

การเฝ้าสังเกตและทบทวนความเสี่ยง เป็นการติดตามผลการปฏิบัติงานตามแผนจัดการความเสี่ยงขององค์กรเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีประสิทธิภาพ มีความเหมาะสม และเมื่อเสร็จสิ้นกิจกรรมตามแผนจัดการความเสี่ยง องค์กรต้องประเมินความเสี่ยงในเรื่องนั้น ๆ ซ้ำอีกครั้งเพื่อตรวจสอบให้มั่นใจว่าความเสี่ยงที่ได้รับการบริหารจัดการไปแล้วนั้นลดลงอยู่ในเกณฑ์ที่องค์กรยอมรับได้ โดยการประเมินความเสี่ยงซ้ำอีกครั้งภายหลังการจัดการความเสี่ยงเรียกว่า “ความเสี่ยงคงเหลือ (Residual risk reporting) ดังภาพที่ 1



ภาพที่ 1 กระบวนการบริหารความเสี่ยง

ความสำคัญของการบริหารความเสี่ยง

การบริหารความเสี่ยงมีความสำคัญในการดำเนินงานและบุคลากรทุกคนขององค์กร การบริหารความเสี่ยงช่วยให้องค์กรประสบความสำเร็จในผลประกอบการและบรรลุเป้าหมายการทำกำไร การป้องกันความสูญเสียของทรัพยากร ช่วยทำให้มั่นใจถึงการรายงานที่มีประสิทธิภาพ การปฏิบัติที่ถูกต้องตามกฎหมาย กฎระเบียบ และกฎเกณฑ์ต่าง ๆ ขององค์กร

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

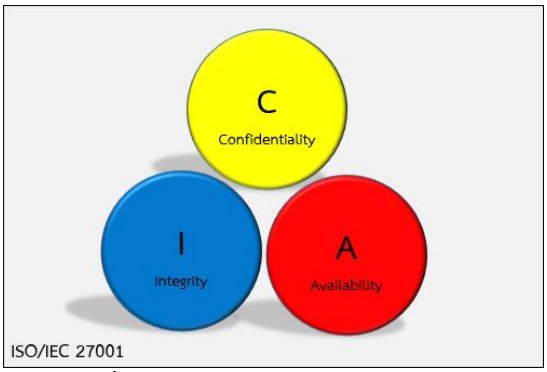
การหลีกเลี่ยงการเสื่อมเสียชื่อเสียงและผลลัพธ์อื่น ๆ อันไม่พึงประสงค์ที่ตามมา โดยรวมแล้วการจัดการความเสี่ยงขององค์กรจะช่วยให้องค์กรทั่วไปดำเนินไปในทิศทางที่ต้องการได้อย่างเหมาะสม และสามารถบรรลุวัตถุประสงค์ขององค์กรที่กำหนดไว้ได้เป็นอย่างดี (ขนิษฐา ชัยรัตนาวรรณ, 2011)

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศมีความหลากหลายเพิ่มมากขึ้นและเข้ามามีบทบาทมากมายในองค์กรต่าง ๆ ทั้งภาครัฐและภาคเอกชน ซึ่งองค์กรต่าง ๆ มีข้อมูลที่มีความสำคัญ และข้อมูลที่เป็นความลับขององค์กร ส่งผลให้ความต้องการในการดูแลความมั่นคงปลอดภัยของสารสนเทศเพิ่มสูงขึ้น เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่าง ๆ ที่สามารถบุกรุกโจมตีข้อมูลขององค์กร มาตรฐาน ISO/IEC 27001 คือ มาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ได้ถูกนำมาใช้เป็นมาตรฐานในการดำเนินงานขององค์กรต่าง ๆ เพื่อให้เกิดประสิทธิภาพในการปกป้องทรัพย์สินสารสนเทศขององค์กร และให้การดำเนินงานขององค์กรสอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับ และข้อกำหนดต่าง ๆ ที่เกี่ยวข้อง (ชุลีกร นวลสมศรี, 2017)

การประเมินความเสี่ยงด้านสารสนเทศ (Information Security Risk Assessment) นับได้ว่าเป็นหัวใจสำคัญของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO27001 (วชิราพร ปัญญา-พินิจนุกูร, 2552) นั่นคือ หากองค์กรประเมินความเสี่ยงไม่ถูกต้อง หรือไม่ครอบคลุมจะทำให้การจัดการความเสี่ยงที่ตามมานั้นแก้ปัญหาไม่ตรงจุด และไม่ครอบคลุมตามไปด้วย มาตรฐาน ISO 27001 มุ่งเน้นการปกป้องข้อมูลสารสนเทศ 3 ประการ (เมธา สุวรรณสาร, 2562) ดังภาพที่ 2 ดังนี้

- ความลับ (Confidential) คือ การปกป้องข้อมูลสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ และมีการกำหนดชั้นความลับของข้อมูลสารสนเทศเพื่อกำหนดเป็นแนวทางในการให้สิทธิ์กับผู้ใช้งานของแต่ละองค์กร
- ความถูกต้องสมบูรณ์ (Integrity) คือ การปกป้องข้อมูลสารสนเทศให้มีความถูกต้องสมบูรณ์ ไม่ให้ถูกแก้ไขเปลี่ยนแปลง หรือผิดไปจากความเป็นจริง
- ความพร้อมใช้งาน (Availability) คือ การปกป้องข้อมูลสารสนเทศ และสร้างความเชื่อมั่นว่าผู้ใช้งานหรือผู้เกี่ยวข้องสามารถใช้งานข้อมูลสารสนเทศได้ตลอดเวลาเมื่อต้องการใช้งาน



ภาพที่ 2 การปกป้องข้อมูลสารสนเทศ 3 ประการของมาตรฐาน ISO 27001

องค์กรสามารถนำการปกป้องข้อมูลสารสนเทศทั้ง 3 ประการนี้มาประยุกต์ใช้ร่วมกับการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ แต่จะปกป้องเข้มงวดมากหรือน้อยขึ้นอยู่กับความเสี่ยงของแต่ละองค์กรที่ประเมินได้ โดยหลักการคือ ข้อมูลใดที่เสี่ยงสูงย่อมต้องมีมาตรการปกป้องเข้มงวดกว่าข้อมูลที่มีความเสี่ยงต่ำ

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ องค์กรควรพิจารณากระบวนการทำงานด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศ 4 ด้าน (ปริญญ์ เสรีพงศ์, 2557) ดังนี้

1. ความเสี่ยงด้านการเข้าถึงข้อมูล (Access Risk) เป็นการประเมินความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูลและระบบสารสนเทศโดยบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงที่บุคคลที่มีหน้าที่เกี่ยวข้องแต่ไม่สามารถเข้าถึงข้อมูลและระบบสารสนเทศได้ องค์กรต้องมีมาตรการควบคุมการเข้าถึงข้อมูลสารสนเทศที่รอบคอบและรัดกุม มิเช่นนั้นบุคคลที่ไม่เกี่ยวข้องอาจนำข้อมูลสารสนเทศขององค์กรไปแสวงหาประโยชน์โดยมิชอบ หรือข้อมูลสารสนเทศเหล่านั้นอาจถูกเปลี่ยนแปลงแก้ไขได้

2. ความเสี่ยงด้านความถูกต้องและครบถ้วนของข้อมูลสารสนเทศ (Integrity Risk) เป็นการประเมินความเสี่ยงเกี่ยวกับการควบคุมและตรวจสอบเพื่อให้มั่นใจว่าการบันทึก การประมวลผล และการแสดงผลข้อมูลสารสนเทศมีความถูกต้องครบถ้วน รวมถึงการควบคุมเกี่ยวกับการพัฒนา แก้ไข หรือเปลี่ยนแปลงระบบสารสนเทศอีกด้วย

3. ความเสี่ยงด้านความพร้อมใช้ของข้อมูลสารสนเทศ (Availability Risk) เป็นการประเมินความเสี่ยงเกี่ยวกับการบริหารจัดการให้ระบบสารสนเทศและข้อมูลสารสนเทศมีความพร้อมใช้งาน สามารถใช้งานได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการ เช่น การสำรองข้อมูล การกู้คืนข้อมูล การบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Management: BCM) เป็นต้น

4. ความเสี่ยงด้านการบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Infrastructure Risk) เป็นการประเมินความเสี่ยงเกี่ยวกับการบริหารจัดการด้านเทคโนโลยีสารสนเทศในภาพรวมให้แก่ผู้ใช้งานอย่างเหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจขององค์กรนั้น ๆ เช่น นโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ระเบียบปฏิบัติขั้นตอนการปฏิบัติงาน การบริหารงานทรัพยากรบุคคล การฝึกอบรม และการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากรภายในองค์กร และบุคลากรที่เข้ามาปฏิบัติงานร่วมกับองค์กร

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่องค์กรพิจารณากระบวนการทำงานด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศ 4 ด้านแล้ว ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารขององค์กรมิได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจ ดังนั้นองค์กรควรพิจารณาว่าข้อมูลสารสนเทศใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของข้อมูล และจัดเตรียมข้อมูลดังกล่าวให้พร้อม เพื่อประโยชน์ในการดำเนินงานของหน่วยงาน

นอกจากนี้ยังมีความเสี่ยงด้านอื่น ๆ ที่เกี่ยวข้อง หรือมีผลกระทบต่อการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งทางตรงและทางอ้อมอีก 4 ด้าน ดังนี้

1. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม เป็นการประเมินความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติสิ่งแวดล้อมที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น ระบบภายในศูนย์ข้อมูล (Data Center) ขององค์กร ต้องพิจารณาเกี่ยวกับระบบปรับอากาศ ระบบควบคุมความชื้น ระบบดับเพลิง เป็นต้น ในเรื่องของนโยบายการเข้าถึงข้อมูลสารสนเทศ การนำข้อมูลสารสนเทศไปใช้ การควบคุมการแลกเปลี่ยนข้อมูล พื้นที่การทำงานและความปลอดภัยในการทำงานของบุคลากรก็เป็นอีกประเด็นหนึ่งที่องค์กรต้องให้ความสำคัญและนำมาประเมินความเสี่ยงด้วย

2. ความเสี่ยงด้านบุคลากร เป็นการประเมินความเสี่ยงที่เกิดจากบุคลากรขององค์กรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงการวางแผนการตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากร / บุคคลที่มีส่วนเกี่ยวข้องกับการ

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

ดำเนินการที่เกี่ยวข้องกับข้อมูลสารสนเทศทุกคนอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความตระหนัก มีความรู้และความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ตลอดจนบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ความเสี่ยงด้านบุคลากรเป็นความเสี่ยงหนึ่งที่สำคัญ ดังนั้นองค์กรจึงควรมีแนวทางและการวางแผนที่กำกับดูแลการบริหารจัดการและควบคุมความเสี่ยงบุคลากรขององค์กรทุกระดับอย่างจริงจัง

3. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ เป็นการประเมินความเสี่ยงที่เกิดจากความผิดพลาด ช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ ไม่ว่าจะเป็นความเสี่ยงที่เกิดจากการทำงานผิดพลาดของอุปกรณ์ ช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ เป็นต้น นอกจากนี้ยังมีช่องโหว่ที่เกิดขึ้นจากการพัฒนาระบบสารสนเทศขึ้นมาใช้เองของแต่ละองค์กร ซึ่งสิ่งเหล่านี้แต่ละองค์กรต้องดำเนินการประเมินความเสี่ยงและจัดการความเสี่ยงเหล่านี้ด้วย

4. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ เป็นการประเมินความเสี่ยงที่เกิดขึ้นจากระบบการทำงานต่าง ๆ ในการจัดทำและพัฒนาระบบสารสนเทศ รวมถึงโปรแกรมประยุกต์อื่น ๆ ที่ใช้ประกอบการใช้งานโปรแกรมหรือระบบสารสนเทศที่พัฒนาขึ้น เช่น การใช้งานโปรแกรมไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม การเปลี่ยนแปลงชุดคำสั่งหรือซอร์สโค้ดโดยผู้ไม่หวังดี เป็นต้น

5. ความเสี่ยงด้านระบบเครือข่าย เป็นการประเมินความเสี่ยงหรือเหตุการณ์ หรือภัยต่าง ๆ ที่เกิดขึ้นกับระบบเครือข่ายขององค์กรทั้งระบบอินทราเน็ต (Intranet) และอินเตอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้านกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงด้านระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่าง ๆ การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย

6. ความเสี่ยงด้านข้อมูลสารสนเทศ เป็นการประเมินความเสี่ยงที่เกิดขึ้นกับข้อมูลในฐานข้อมูลต่าง ๆ ของระบบสารสนเทศภายในองค์กร อาจมีผู้บุกรุกทำให้ข้อมูลสารสนเทศถูกทำลาย หรือการโจรกรรมข้อมูลสารสนเทศที่สำคัญ การลักลอบเข้ามาแก้ไขหรือเปลี่ยนแปลงข้อมูล ความเสี่ยงเหล่านี้ล้วนมีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูลสารสนเทศ ดังนั้นองค์กรต้องให้ความสำคัญในการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงให้ครอบคลุมด้านข้อมูลสารสนเทศด้วย

คณะแพทยศาสตร์ศิริราชพยาบาลกับการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล เป็นองค์กรหนึ่งที่ได้รับการรับรองมาตรฐาน ISO/IEC 27001:2013 (Information Security Management System: ISMS) เมื่อปี พ.ศ. 2560 โดยกิจกรรมที่สำคัญของมาตรฐาน ISO/IEC 27001:2013 คือ การดำเนินการเพื่อจัดการความเสี่ยงและโอกาสเกิดซึ่งมุ่งเน้นการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศควบคู่ไปกับการประเมินความเสี่ยงจากการปฏิบัติงานทั่วไป การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นการระบุความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของข้อมูล เช่น ความลับของข้อมูล ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูล เป็นต้น ซึ่งคณะแพทยศาสตร์ศิริราชพยาบาลเป็นองค์กรหนึ่งที่ขับเคลื่อนพันธกิจขององค์กรโดยใช้เทคโนโลยีสารสนเทศเป็นโครงสร้างพื้นฐานที่สำคัญ ไม่ว่าจะเป็นในด้านการศึกษา ด้านวิชาการ ด้านการวิจัย และด้านการบริการผู้ป่วย ต่างก็ใช้เทคโนโลยีสารสนเทศทั้งสิ้น ด้วยเหตุนี้การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงเป็นหัวใจสำคัญของคณะแพทยศาสตร์ศิริราชพยาบาล

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

ฝ่ายสารสนเทศเป็นหน่วยงานสังกัดสำนักงานคณบดี คณะแพทยศาสตร์ศิริราชพยาบาลที่ได้รับมอบหมายให้บริหารจัดการและควบคุมดูแลในเรื่องของเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ด้วยเหตุนี้ฝ่ายสารสนเทศจึงให้ความสำคัญในเรื่องดังกล่าว และนำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเข้าไปเป็นส่วนหนึ่งของการประเมินความเสี่ยงตั้งแต่ปี พ.ศ.2561 เป็นต้นมา สำหรับการประเมินความเสี่ยงของฝ่ายสารสนเทศเลือกวิธีการวิเคราะห์ความเสี่ยงตามเหตุการณ์ (Scenario-based Risk Assessment) โดยกำหนดให้ดำเนินการประเมินความเสี่ยงปีละ 1 ครั้ง ซึ่งฝ่ายสารสนเทศมอบหมายให้ทีมบริหารจัดการคุณภาพ (Quality Management) รวบรวมและประสานงานในการดำเนินการบริหารความเสี่ยงของฝ่ายสารสนเทศ ดังนั้นเพื่อให้การบริหารจัดการความเสี่ยงครอบคลุมในทุกส่วนการปฏิบัติงานของฝ่ายสารสนเทศและเป็นการเปิดโอกาสให้บุคลากรของฝ่ายสารสนเทศมีส่วนร่วมในกิจกรรมนี้ ทีมบริหารจัดการคุณภาพจึงดำเนินการประเมินความเสี่ยงโดยมอบหมายให้แต่ละทีมในงานต่าง ๆ ซึ่งอยู่ในสังกัดของฝ่ายสารสนเทศดำเนินการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงานในส่วนงานที่แต่ละทีมรับผิดชอบ ซึ่งเมื่อแต่ละทีมประเมินความเสี่ยงได้แล้ว จะส่งแบบประเมินความเสี่ยงมาให้กับทีมบริหารจัดการคุณภาพเพื่อรวบรวมและกำหนดรหัสเหตุการณ์ความเสี่ยง ประจำปี เพื่อใช้ในการดำเนินการติดตามการบริหารความเสี่ยงต่อไป นอกจากการประเมินความเสี่ยงปีละ 1 ครั้งตามรอบของกิจกรรมการบริหารความเสี่ยงของฝ่ายสารสนเทศแล้ว หากแต่ละทีมพบความเสี่ยงเพิ่มเติมจากการปฏิบัติงานระหว่างปี แต่ละทีมสามารถประเมินความเสี่ยงเพิ่มเติมและรวบรวมส่งให้ทีมบริหารจัดการคุณภาพได้ตลอดทั้งปี ทั้งนี้เพื่อให้มั่นใจได้ว่าทุกความเสี่ยงที่พบในการปฏิบัติงานรวมถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศจะได้รับการบริหารจัดการอย่างครอบคลุม ครบถ้วนและมีประสิทธิภาพ

สำหรับการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เพิ่มเข้ามาในการประเมินความเสี่ยงของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลนั้น ยึดตามกระบวนการบริหารความเสี่ยง ดังนี้

ขั้นตอนการระบุความเสี่ยง

บุคลากรในแต่ละทีมของงานต่าง ๆ ภายใต้สังกัดของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล จะดำเนินการระบุความเสี่ยงตามเหตุการณ์ที่อาจเกิดขึ้นกับทรัพย์สินและสารสนเทศของฝ่ายสารสนเทศ โดยพิจารณาจากปัจจัยต่าง ๆ ที่อาจส่งผลให้เกิดความเสียหายต่อทรัพย์สินและสารสนเทศ หรือปัจจัยที่อาจก่อให้เกิดการสูญหาย ความถูกต้อง และความพร้อมใช้งานของข้อมูลสารสนเทศ เช่น ระบบสารสนเทศสำหรับการให้บริการผู้ป่วยเกิดหยุดชะงักอันเนื่องมาจากฮาร์ดดิสก์ของเครื่องแม่ข่ายที่ให้บริการฐานข้อมูลผู้ป่วยเสียหายจากกระแสไฟฟ้ากระชาก, ระบบคอมพิวเตอร์และเครื่องแม่ข่ายคอมพิวเตอร์ ณ ศูนย์สำรองไม่สามารถให้บริการได้ อันเนื่องมาจากระบบปรับอากาศไม่เพียงพอต่อการใช้งาน และ ข้อมูลสำคัญของคณะฯ ถูกเปลี่ยนแปลงหรือสูญหายโดยบุคลากรที่สิ้นสุดสัญญาจ้างหรือลาออกจากคณะฯ อันเนื่องมาจากการถอดถอนสิทธิ์การเข้าถึงล่าช้าหรือการไม่สอบทานบัญชีรายชื่อผู้ใช้งานระบบสารสนเทศ เป็นต้น

ขั้นตอนการวิเคราะห์ความเสี่ยง

เมื่อบุคลากรในแต่ละทีมสามารถระบุความเสี่ยงได้แล้ว ขั้นตอนต่อไปคือ การวิเคราะห์ความเสี่ยง ซึ่งการวิเคราะห์ความเสี่ยงจะประกอบด้วยการพิจารณากลุ่มทรัพย์สินที่ได้รับผลกระทบ หน่วยงานที่ได้รับผลกระทบ ช่องโหว่ที่อาจทำให้เกิดเหตุการณ์ ภัยคุกคาม ประเภทของภัยคุกคาม ตลอดจนบุคคลหรือผู้ที่ทำให้เกิดความเสียหาย ระดับผลกระทบที่จะเกิดขึ้น

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

และระดับโอกาสเกิดของความเสี่ยง นอกจากนี้แต่ละทีมต้องพิจารณาถึงกิจกรรมหรือมาตรการควบคุมที่ใช้อยู่ในปัจจุบันซึ่งเป็นมาตรการในการดูแล ป้องกัน หรือแก้ไขไม่ให้ความเสี่ยงนั้น ๆ เกิดขึ้นได้ รวมถึงการพิจารณาถึงผลกระทบด้านเทคโนโลยีสารสนเทศทั้ง 3 ด้าน อันได้แก่ ความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งาน

ตัวอย่างเช่น ความเสี่ยงในส่วนของข้อมูลสำคัญของคณะฯ ถูกเปลี่ยนแปลงหรือสูญหายโดยบุคลากรที่สิ้นสุดสัญญาจ้างหรือลาออกจากคณะฯ อันเนื่องมาจากการถอดถอนสิทธิ์การเข้าถึงล่าช้าหรือการไม่สอบทานบัญชีรายชื่อผู้ใช้งานระบบสารสนเทศ หากพิจารณาปัจจัยและข้อมูลต่าง ๆ ตามขั้นตอนการวิเคราะห์ความเสี่ยงของฝ่ายสารสนเทศจะสามารถพิจารณาและระบุข้อมูลในส่วนต่าง ๆ ดังนี้

- กลุ่มทรัพย์สินที่ได้รับผลกระทบ ได้แก่ ข้อมูลที่จัดเก็บอยู่ในฐานข้อมูลภายในศูนย์ข้อมูล (Data Center) ของคณะแพทยศาสตร์ศิริราชพยาบาล
- หน่วยงานที่ได้รับผลกระทบ ได้แก่ คลินิก, หอผู้ป่วย และหน่วยงานที่เกี่ยวข้องกับการให้บริการผู้ป่วย
- ช่องโหว่ที่อาจทำให้เกิดเหตุการณ์ ได้แก่ การจัดการบัญชีรายชื่อผู้ใช้งานระบบสารสนเทศ
- ภัยคุกคาม ได้แก่ บุคคลเข้าไปลบ เปลี่ยนแปลง หรือแก้ไขข้อมูล
- ประเภทของภัยคุกคาม ได้แก่ ภัยคุกคามที่เกิดขึ้นโดยเจตนา หรือภัยคุกคามที่เกิดขึ้นโดยไม่เจตนา ซึ่งในกรณีนี้ถือว่าเป็นภัยคุกคามที่เกิดขึ้นโดยเจตนา
- บุคคลหรือผู้ที่ทำให้เกิดความเสียหาย ได้แก่ บุคลากรที่สิ้นสุดสัญญาจ้างหรือลาออก หรือเกษียณอายุราชการ
- ระดับผลกระทบ เมื่อพิจารณาตามเกณฑ์ของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล อยู่ที่ระดับสูงมาก (ระดับ 5) ซึ่งเป็นผลกระทบที่รุนแรงที่สุด
- ระดับโอกาสเกิด เมื่อพิจารณาจากสถิติของการลาออก การสิ้นสุดสัญญาจ้างย้อนหลังกลับไป 1 ปี พบว่ามีระดับโอกาสเกิดอยู่ที่ระดับปานกลาง (ระดับ 3) โดยตรวจสอบพบว่าโอกาสที่บุคลากรลาออก หรือสิ้นสุดสัญญาจ้าง แต่ไม่ได้รับการนำออกจากบัญชีรายชื่อผู้ใช้ระบบสารสนเทศเฉลี่ยอยู่ที่ 1-12 ครั้งต่อปี
- มาตรการควบคุม ได้แก่ การสอบทานบัญชีรายชื่อผู้ใช้งานระบบสารสนเทศปีละ 1 ครั้ง
- ผลกระทบด้านเทคโนโลยีสารสนเทศ ได้แก่ ความถูกต้องสมบูรณ์ ซึ่งหากบุคลากรที่ลาออก หรือสิ้นสุดสัญญาจ้างไปแล้ว แต่ยังสามารถเข้าใช้งานระบบสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลได้ อาจจะเข้าไปดำเนินการแก้ไขข้อมูล หรือเปลี่ยนแปลงข้อมูลให้ผิดไปจากความเป็นจริง

ขั้นตอนการประเมินความเสี่ยง

เมื่อวิเคราะห์ความเสี่ยงเรียบร้อยแล้ว บุคลากรในแต่ละทีมจะดำเนินการประเมินความเสี่ยง ซึ่งพิจารณาระดับของความเสี่ยง โดยเปรียบเทียบกับตารางแสดงระดับความเสี่ยงของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลที่กำหนดไว้ ดังตารางที่ 1 ดังนี้

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

ระดับผลกระทบ (Impact)						
	5	1x5	2x5	3x5	4x5	5x5
	4	1x4	2x4	3x4	4x4	5x4
	3	1x3	2x3	3x3	4x3	5x3
	2	1x2	2x2	3x2	4x2	5x2
	1	1x1	2x1	3x1	4x1	5x1
		1	2	3	4	5
		ระดับโอกาสเกิด (Likelihood)				

ตารางที่ 1 ตารางแสดงระดับความเสี่ยงของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล

หากพิจารณาจากระดับผลกระทบ และระดับโอกาสเกิดจากการวิเคราะห์ความเสี่ยงในส่วนของข้อมูลสำคัญของคณะฯ ถูกเปลี่ยนแปลงหรือสูญหายโดยบุคลากรที่สิ้นสุดสัญญาจ้างหรือลาออกจากคณะฯ อันเนื่องมาจากการถอดถอนสิทธิ์การเข้าถึงล่าช้าหรือการไม่สอบทานบัญชีรายชื่อผู้ใช้งานระบบสารสนเทศ พบว่าระดับโอกาสเกิดอยู่ที่ระดับ 3 และระดับผลกระทบอยู่ที่ระดับ 5 ดังนั้นระดับความเสี่ยงของความเสี่ยงในส่วนของข้อมูลสำคัญของคณะฯ ถูกเปลี่ยนแปลงหรือสูญหายโดยบุคลากรที่สิ้นสุดสัญญาจ้างหรือลาออกจากคณะฯ อันเนื่องมาจากการถอดถอนสิทธิ์การเข้าถึงล่าช้าหรือการไม่สอบทานบัญชีรายชื่อผู้ใช้งานระบบสารสนเทศจะอยู่ที่ช่อง 3X5 ซึ่งตกอยู่ในโซนสีแดง ซึ่งตามเกณฑ์ของคณะแพทยศาสตร์ศิริราชพยาบาล และเกณฑ์ของมหาวิทยาลัยมหิดลจะกำหนดให้หน่วยงานต้องดำเนินการจัดการความเสี่ยง โดยเลือกวิธีในการจัดการความเสี่ยงด้วยการลดความเสี่ยง

จากนั้นบุคลากรในแต่ละทีมจะดำเนินการจัดลำดับความสำคัญของเหตุการณ์ความเสี่ยงที่ประเมินได้ทั้งหมด โดยพิจารณาจากตารางแสดงระดับความเสี่ยงของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลที่กำหนดไว้ ซึ่งหากเหตุการณ์ความเสี่ยงตกอยู่โซนสีแดงและโซนสีส้ม จะต้องดำเนินการจัดการความเสี่ยงทันที

ขั้นตอนการจัดการความเสี่ยง

หลังจากการประเมินความเสี่ยงในส่วนของข้อมูลสำคัญของคณะฯ ถูกเปลี่ยนแปลงหรือสูญหายโดยบุคลากรที่สิ้นสุดสัญญาจ้างหรือลาออกจากคณะฯ อันเนื่องมาจากการถอดถอนสิทธิ์การเข้าถึงล่าช้าหรือการไม่สอบทานบัญชีรายชื่อผู้ใช้งานระบบสารสนเทศเรียบร้อยแล้ว ขั้นตอนต่อไปบุคลากรในแต่ละทีมจะดำเนินการคิดแผนจัดการความเสี่ยง (Risk Treatment Plan: RTP) ซึ่งกิจกรรมที่จะนำมาใช้ในการจัดการความเสี่ยงสามารถเลือกปฏิบัติได้ 2 แนวทาง คือ กิจกรรมที่จัดทำขึ้นเพื่อลดโอกาสเกิดเหตุการณ์ความเสี่ยง หรือกิจกรรมที่จัดทำขึ้นเพื่อลดผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยง ซึ่งความเสี่ยงในส่วนของข้อมูลสำคัญของคณะฯ ถูกเปลี่ยนแปลงหรือสูญหายโดยบุคลากรที่สิ้นสุดสัญญาจ้างหรือลาออกจากคณะฯ อันเนื่องมาจากการถอดถอนสิทธิ์การเข้าถึงล่าช้าหรือการไม่สอบทานบัญชีรายชื่อผู้ใช้งานระบบสารสนเทศนั้น ได้เสนอแผนจัดการความเสี่ยง 2 แผน ได้แก่ แผนระยะยาวจะดำเนินการปรับเปลี่ยนรหัสผู้ใช้งานระบบสารสนเทศด้วยการยืนยันตัวตนด้วยระบบแอคทีฟไดเรคทอรี่ (Active Directory: AD) ซึ่งระบบ AD จะได้รับข้อมูลจากระบบ SAP โมดูล HR ของคณะแพทยศาสตร์ศิริราชพยาบาลวันละ 1 ครั้ง เพื่อนำไปปรับปรุงข้อมูลในระบบ AD ซึ่งหากปรับเปลี่ยนรหัสผู้ใช้งานระบบสารสนเทศด้วยการยืนยันตัวตนด้วยระบบ AD ก็จะเป็นการปรับปรุงบัญชีรายชื่อผู้ใช้งานให้เป็นปัจจุบันอย่างสม่ำเสมอ แต่ยังมีช่องโหว่ของการดำเนินการตามแผนระยะยาว จึงได้คิดการดำเนินการงานเป็นแผนระยะสั้นขึ้นมาอีก 1 แผน ซึ่งแผนระยะสั้นจะดำเนินการเพิ่มความถี่ในการสอบทานสิทธิ์การเข้าถึงระบบสารสนเทศ และสิทธิ์การใช้งานระบบสารสนเทศเป็นปีละ 2 ครั้ง เมื่อได้แผนจัดการความเสี่ยงมาแล้ว แต่ละทีมจะรวบรวมข้อมูลต่าง ๆ กรอกลงในแบบฟอร์มการประเมินความเสี่ยงส่งให้กับทีมบริหารจัดการคุณภาพ

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

ทีมบริหารจัดการคุณภาพจะรวบรวมความเสี่ยงที่ได้รับการประเมินจากทีมต่าง ๆ และนำมาจัดกลุ่มความเสี่ยง สรุปเป็นรายงานความเสี่ยงเพื่อนำเสนอให้ผู้บริหารของฝ่ายสารสนเทศได้ทราบ และเลือกแนวทางในการจัดการความเสี่ยงโดยประเมินจากปัจจัย 2 ประการ คือ ความคุ้มค่าของต้นทุนที่จะต้องใช้ในการบริหารจัดการและผลตอบแทนที่จะได้รับกลับคืนมายังฝ่ายสารสนเทศ และความเป็นไปได้ของประสิทธิผลและความสำเร็จในการบริหารจัดการความเสี่ยงนั้น เมื่อผู้บริหารของฝ่ายสารสนเทศเลือกแนวทางในการจัดการความเสี่ยงได้แล้วจะต้องดำเนินการมอบหมายผู้รับผิดชอบ (เมธา สุวรรณสาร, 2562) ของแผนจัดการความเสี่ยงในแต่ละแผนเพื่อนำไปดำเนินการจัดการความเสี่ยงต่อไป ซึ่งผู้เกี่ยวข้องจะตระหนักอยู่เสมอว่า “ไม่มีความเสี่ยงใดที่ถูกจัดการแล้วจะหมดไป” แต่แผนจัดการความเสี่ยงจะต้องสามารถ “ลดความเสี่ยงให้อยู่ในระดับที่องค์กรสามารถยอมรับได้”

ขั้นตอนการเฝ้าสังเกตและทบทวนความเสี่ยง

ทีมบริหารจัดการคุณภาพ ฝ่ายสารสนเทศจะดำเนินการรวบรวมแผนจัดการความเสี่ยงและรายชื่อผู้รับผิดชอบแต่ละแผนจัดการความเสี่ยง จากนั้นจะนำข้อมูลมาจัดทำเป็นกิจกรรมการเฝ้าสังเกต/ติดตามและตรวจสอบความก้าวหน้าในการดำเนินกิจกรรมตามแผนจัดการความเสี่ยง (Risk Treatment Plan Tracking: RTP Tracking) เดือนละ 2 ครั้ง เพื่อนำเสนอให้ผู้บริหารของฝ่ายสารสนเทศทราบ โดยแผนจัดการความเสี่ยงใดที่ดำเนินการเสร็จสิ้นแล้วก็จะมีการวิเคราะห์และประเมินระดับความเสี่ยงคงเหลือ (Residual Risk) เพื่อให้มั่นใจว่าแผนจัดการความเสี่ยงมีประสิทธิภาพ มีความเหมาะสม และมั่นใจว่าความเสี่ยงที่ได้รับการจัดการไปแล้วนั้นลดลงอยู่ในเกณฑ์ที่ฝ่ายสารสนเทศคณะแพทยศาสตร์ศิริราชพยาบาลยอมรับได้

นอกจากนี้ทีมบริหารจัดการคุณภาพยังเฝ้าติดตามการดำเนินการกิจกรรมต่าง ๆ สำหรับแผนจัดการความเสี่ยงที่อยู่ระหว่างการดำเนินการ เพื่อแจ้งให้ผู้บริหารของฝ่ายสารสนเทศทราบถึงความคืบหน้าในการดำเนินงาน ตลอดจนปัญหาและอุปสรรคต่าง ๆ ที่เกิดขึ้น ทั้งนี้หากพบปัญหาหรืออุปสรรคในการดำเนินงาน ผู้บริหารของฝ่ายสารสนเทศจะให้คำปรึกษาและให้ความช่วยเหลือเพื่อให้กิจกรรมต่าง ๆ ลุล่วงตามวัตถุประสงค์ของแผนจัดการความเสี่ยงนั้น ๆ ต่อไป

สรุป

การประเมินความเสี่ยงและการบริหารจัดการความเสี่ยงขององค์กรมีบทบาทสำคัญในการดำเนินธุรกิจขององค์กรในปัจจุบันและในอนาคต นอกจากนี้องค์กรต้องให้ความสำคัญในการปกป้องข้อมูลสารสนเทศด้วยการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งถือว่าเป็นสินทรัพย์ขององค์กรให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงในแต่ละด้านควรจัดให้อยู่ในความรับผิดชอบหลักของผู้ที่มีความรู้และความสามารถในเรื่องนั้น ๆ สำหรับการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ องค์กรควรมอบหมายผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศเป็นผู้บริหารจัดการ และฝ่ายบริหารขององค์กรต้องให้การสนับสนุนทรัพยากรที่จำเป็น เหมาะสมและได้มาตรฐาน เพื่อปกป้องค์กรจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้การสื่อสารภายในองค์กร และการสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และการใช้งานข้อมูลสารสนเทศให้กับบุคลากรทุกระดับภายในองค์กร ก็มีส่วนสำคัญเช่นกันที่จะทำให้บรรลุผลสำเร็จ หรือจุดมุ่งหมายขององค์กร

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

ข้อเสนอแนะ

ผลการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเป็นตัวกำหนดว่าจะต้องทำแผนจัดการความเสี่ยง (Risk Treatment Plan) เพื่อจัดการความเสี่ยงอะไรบ้าง โดยแผนจัดการความเสี่ยงเป็นกิจกรรมหนึ่งที่มีความสำคัญและนำมาใช้ในการเฝ้าสังเกต ติดตามผลการจัดการความเสี่ยง และทบทวนความเสี่ยงที่เหลืออยู่ นอกจากนี้ประเด็นเรื่องกฎหมายก็เป็นหัวข้อหนึ่งที่สำคัญในการประเมินความเสี่ยง หากประเมินความเสี่ยงแล้วพบว่าเป็นเรื่องผิดกฎหมาย ซึ่งถือว่ามีความเสี่ยงในระดับสูง องค์กรต้องรีบแก้ไขโดยด่วน

เอกสารอ้างอิง

กรธัช อยู่สุข.(2553). การจัดการความเสี่ยง (Risk Management) สำหรับองค์กร Episode 1. สืบค้นเมื่อ 13 มกราคม 2563, จาก https://www.gotoknow.org/posts/364878.

เกียรติพงษ์ อุดมธนะธีระ. (2561). Risk Management Principles and Guidelines ISO 31000: 2009. สืบค้นเมื่อ 14 มกราคม 2563, จาก https://www.iok2u.com/index.php/article/e-book/196-iso-31000-2009-risk management-principles-and-guidelines-iso-31000-2009.

ขนิษฐา ชัยรัตนาวรรณ. (2011), การบริหารความเสี่ยงสากล ISO 31000 กับระบบการศึกษาของไทย. Veridian E-Journal Su. Vol.4 No.1 May – August 2011, 419 – 434.

จริญญา จันทร์ปาน. (2558). Scenario-Based Risk Assessment เหมาะสมหรือไม่กับองค์กรของท่าน. สืบค้นเมื่อ 14 มกราคม 2563, จาก https://www.techtalkthai.com/is-scenario-based-risk-assessment-suitable-for- your-company.

จิรพร สุเมธีประสิทธิ์. (2554). Scenario-Based Risk Assessment การค้นหาและประเมินความเสี่ยงบนสมมติฐานของฉากทัศน์. สืบค้นเมื่อ 14 มกราคม 2563, จาก https://chirapon.wordpress.com.

จิรพร สุเมธีประสิทธิ์. (2554). มารู้จักมาตรฐานการบริหารความเสี่ยงระดับสากลกัน. สืบค้นเมื่อ 14 มกราคม 2563, จาก http://web.kmutt.ac.th/internal-audit/news/detail.php?ID=2618

ชุลีกร นวลสมศรี. (2017). การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO 27001:2013. สืบค้นเมื่อ 14 มกราคม 2563, จาก https://www.tcithaijo.org/index.php/gskku/article/view/102213

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

ปริญญ์ เสรีพงศ์. (2557). รีวิว ISO 27001 :2013 – ตอนที่ 2 ความสำคัญของการประเมินความเสี่ยงสารสนเทศ. [เว็บบล็อก]. สืบค้นเมื่อ 6 พฤศจิกายน 2562, จาก http://www.club27001.com/2014/01/review-iso27001-2013- part1.html

เมธา สุวรรณสาร. (2562). ความมั่นคงปลอดภัยไซเบอร์กับปัจจัยเอื้อที่ก่อให้เกิดความสำเร็จแบบ

Received: January 20,2020, Revised : August 14,2020, Accepted: September 11,2020
http://doi.org/

บูรณาการประโยชน์ของการจัดการความเสี่ยง. สืบค้นเมื่อ 14 มกราคม 2563, จาก http://www.itgthailand.com

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