KKU RESEARCH JOURNAL (GRADUATE STUDY)
Vol. 17 NO. 4: October-December 2017

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013 กรณีศึกษาขององค์กรด้านการบินแห่งหนึ่ง

Risk Assessment in Information Technology and Communication under the ISO27001:2013 Standard A Case Study of Aviation Organization

ชุลีกร นวลสมศรี (Chuleekorn Nuansomsri)[1]* ดร.สุทธิศักดิ์ จันทวงษ์โส (Dr. Suttisak Jantavongso)**

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ (1) ระบุและประเมินความเสี่ยง (2) นำเสนอแนวทางในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013 ขององค์กรกรณีศึกษา วิธีดำเนินการวิจัยเป็นแบบเชิงสำรวจ โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากพนักงานขององค์กรกรณีศึกษา จำนวน 137 ท่าน วิเคราะห์ข้อมูลโดยใช้สถิติเชิงบรรยายค่าร้อยละ และสถิติในการประเมินความเสี่ยง คือ ค่าโอกาสในการเกิดความเสี่ยงและค่าผลกระทบที่จะเกิดความเสี่ยง ผลการวิจัยพบว่า องค์กรกรณีศึกษามีความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่อยู่ในระดับสูงมี 6 ด้าน ดังนี้ (1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (2) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (3) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (4) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (5) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม และ (6) การบริการจัดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ การวิจัยนี้ส่งผลให้ให้องค์กรมีแนวทางในการกำหนดนโยบายและนำแนวทางไปใช้ในบริหารจัดการความเสี่ยงทั้ง 6 ด้านอย่างเหมาะสม รวมไปถึงการปรับปรุงและพัฒนากระบวนการจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้ได้มาตรฐานในระดับสากล

ABSTRACT

The objectives of this research were (1) to identify and assess risks; and (2) to develop a risk management plan on Information Technology and Communications (ICTs) risks under the ISO 27001:2013 standard for an aviation organization. This research applied a qualitative research methodology using questionnaires as a tool to collect data. 137 officials, working at a case study organization, were participated. The descriptive statistics were used to describe the data found in this research. The risk assessment was explained in the form of risk opportunities and the projected impacts from those risks. The findings revealed that a case study organization had the high risks on ICT in 6 areas, namely: (1) Information Security Policy, (2) Operations Security, (3) Information Security Aspects of Business Continuity Management (BCM), (4) Human Resource (HR) Security, (5) Physical and Environmental Security, and (6) Information Security Incident Management (ISIM). Finally, a risk management plan was developed in 6 domains to guide the ICT risk management.

คำสำคัญ: การประเมินความเสี่ยง แผนบริหารความเสี่ยง มาตรฐาน ISO27001:2013

Keywords: Risk assessment, Risk plan, ISO27001:2013

---

[1] *Correspondent author: chuleekorn.n@rsu.ac.th*

** อาจารย์ สาขาวิชาระบบสารสนเทศวิสาหกิจ วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต*

*** ผู้ช่วยศาสตราจารย์ สาขาวิชาระบบสารสนเทศวิสาหกิจ วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต*

บทนำ

เทคโนโลยีสารสนเทศและการสื่อสาร (Information Communication and Technology: ICT) ได้เข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตของมนุษย์ โดยเฉพาะการประกอบธุรกิจในยุคปัจจุบันที่มีการแข่งขันกันสูงและมีการเปลี่ยนแปลงอย่างรวดเร็ว ICT เป็นโครงสร้างพื้นฐานที่สำคัญที่ใช้ในการรองรับกลยุทธ์และกระบวนการดำเนินธุรกิจต่างๆ [1] และเป็นสิ่งที่จำเป็นสำหรับการบริหารงานในสมัยใหม่อย่างหลีกเลี่ยงไม่ได้ ไม่ว่าจะเป็นการนำอุปกรณ์คอมพิวเตอร์เข้ามาช่วยในการปฏิบัติงาน การติดต่อสื่อสาร การจัดเก็บข้อมูลที่สำคัญขององค์กร รวมไปถึงการประมวลผลข้อมูลต่างๆ เพื่อใช้ในการประกอบการตัดสินใจของผู้บริหารที่ต้องการสารสนเทศที่มีคุณภาพ หลายครั้งการแพ้-ชนะในการแข่งขันขององค์กรขึ้นอยู่กับความสามารถในการบริหารจัดการข้อมูลเพื่อให้เกิดความได้เปรียบในการแข่งขัน ปรากฏการณ์เช่นนี้ส่งผลให้แนวโน้มของการดำเนินธุรกิจและความอยู่รอดขององค์กรมีความจำเป็นที่จะต้องพึ่งพาระบบสารสนเทศ ระบบสารสนเทศจึงกลายเป็นทรัพยากรที่มีคุณค่ายิ่งขององค์กรที่จะต้องให้ความสำคัญและมีการจัดสรรงบประมาณในการพัฒนา ปรับปรุง และดูแลรักษาอยู่อย่างสม่ำเสมอ

เมื่อระบบสารสนเทศมีความสำคัญกับองค์กร การดูแลรักษาความมั่นคงและปลอดภัยก็ย่อมมากขึ้นตามลำดับ เนื่องจากระบบสารสนเทศมีความเสี่ยงจากภัยคุกคามต่างๆ ซึ่งจากรายงานแนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ปี 2016 โดย The Information Security Forum (ISF) ได้ระบุทิศทางเชิงลบด้านความมั่นคงปลอดภัยทาง ไซเบอร์ (Cyber) ยังคงต่อเนื่องใน 3 ประเด็น ได้แก่ (1) ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป (2) ความเชื่อมั่นในระบบหรือโซลูชั่น (Solution) การรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่ (3) ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ดังนั้น องค์กรต่างๆ ทั่วโลกจึงต้องปรับกระบวนทัศน์ให้มีความสามารถในการปรับตัวเพื่อรองรับการเปลี่ยนแปลง และผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามไซเบอร์ในรูปแบบใหม่ [2]

การบริหารความเสี่ยง (Risk Management) เป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี [3] เป็นกลไกสำคัญที่ช่วยสนับสนุนให้องค์กรบรรลุวัตถุประสงค์และผลักดันให้องค์กรมีผลการดำเนินที่เป็นเลิศ (High Performance Public Organization) ช่วยให้การบริหารงาน การวางแผน การตัดสินใจ รวมไปถึงการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพ ลดการสูญเสียโอกาสที่จะทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศ [4]

องค์กรกรณีศึกษา (องค์กรด้านการบินแห่งหนึ่งในประเทศไทย) ได้กำหนดยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศมาใช้ในการบริหารงาน การปฏิบัติงานในรูปแบบบูรณาการเพื่อให้องค์กรมีความทันสมัย ใช้นวัตกรรมใหม่ๆ ในการให้บริการแก่ลูกค้าด้วยความสะดวก รวดเร็ว ถูกต้อง และปลอดภัย อันจะนำไปสู่การเป็นบริษัทขนาดใหญ่ของภูมิภาคเอเชียตะวันออกเฉียงใต้ แต่ภายใต้สภาะการดำเนินงานของทุกองค์กรล้วนแล้วแต่มีความเสี่ยง นั่นก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงมีความจำเป็นอย่างยิ่งที่จะต้องบริหารจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ [5] เพื่อเป็นสร้างความมั่นใจในการดำเนินธุรกิจให้สามารถตอบสนองและสนับสนุนการดำเนินขององค์กรอย่างต่อเนื่องและมีประสิทธิภาพ

ในขณะเดียวกันอุตสาหกรรมการบินในประเทศไทยมีการขยายตัวอย่างต่อเนื่อง ด้วยภาวะความต้องการในการเดินทางที่สะดวกรวดเร็วขึ้น การตอบสนองด้านการท่องเที่ยว การประกอบธุรกิจด้านการค้าระหว่างประเทศ และที่สำคัญประเทศไทยเป็นประเทศสมาชิกประชาคมเศรษฐกิจอาเซียน ที่มีการติดต่อค้าขาย การเจรจา การศึกษา แรงงาน การดำเนินกิจกรรมต่างๆ ระหว่างประเทศสมาชิก 10 ประเทศ ประเทศไทยมีความประสงค์ที่จะเป็นประเทศศูนย์กลาง

ด้านการขนส่งทางอากาศของอาเซียน ดังนั้น ประเทศไทยจึงต้องเตรียมความพร้อมในด้านสนามบิน เครื่องมือและองค์ประกอบด้านการบิน และบุคลากรด้านธุรกิจการบิน ในการนำพาธุรกิจด้านการบินของประเทศไทยพัฒนาให้ก้าวหน้าและทันสมัย [6]

จากความสำคัญดังกล่าว ผู้วิจัยจึงได้ศึกษา วิเคราะห์ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรกรณีศึกษา ภายใต้มาตรฐาน ISO27001:2013 เพื่อนำข้อมูลที่ได้มาใช้เป็นแนวทางในการวางแผนป้องกันโอกาสที่จะเกิดความเสี่ยงในการดำเนินงาน ตลอดจนใช้ในการวิเคราะห์ ปรับปรุงกระบวนการทำงานที่ส่งผลกระทบโดยตรงต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร และยกระดับมาตรฐานการทำงานขององค์กรให้มีศักยภาพในการแข่งขันและนำไปสู่การปฏิบัติที่ดี (Best Practices) และบรรลุวัตถุประสงค์ขององค์กรขององค์กรกรณีศึกษา

โจทย์วิจัย/ปัญหาวิจัย

1. องค์กรกรณีศึกษามีความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับใด
2. องค์กรกรณีศึกษามีแนวทางในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างไร

วัตถุประสงค์การวิจัย

1. เพื่อระบุและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013 ขององค์กรกรณีศึกษา
2. เพื่อนำเสนอแนวทางในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013 ขององค์กรกรณีศึกษา

วรรณกรรมที่เกี่ยวข้อง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงินและการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์ [7]

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง [7]

มาตรฐาน ISO27001:2013 เป็นมาตรฐานที่พัฒนาขึ้นโดย ISO (International Organization for Standardization) โดยเป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) เพื่อสร้างความมั่นใจถึงความมีประสิทธิผลและประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศขององค์กร รวมถึงการดำเนินการที่สอดคล้องตามข้อกำหนดด้านระบบความมั่นคงปลอดภัยทั้งของลูกค้า ข้อกฎหมาย และระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้องด้วย โดยแนวทางในการรักษาความมั่นคงปลอดภัยของ

ข้อมูลนั้นจะมีโครงสร้างที่เรียกว่า Plan-Do-Check-Act ซึ่งประกอบไปด้วยขั้นตอน การวางแผน (Plan) การลงมือทำ (Do) การตรวจสอบ (Check) และการปรับปรุงแก้ไข้ (Act) [8] ดังภาพที่ 1

มาตรฐาน ISO/IEC 17799 กล่าวถึงเรื่องของวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่หน่วยจัดทำมาตรการที่กำหนดเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001:2013 เป็นกรอบด้านการควบคุมระบบความปลอดภัยข้อมูล ซึ่งแบ่งรายการควบคุม (Controls) ออกเป็น 14 หัวข้อหลัก ดังนี้ (1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (4) การบริหารจัดการทรัพย์สิน (5) การควบคุมการเข้าถึง (6) การเข้ารหัสข้อมูล (7) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (10) การจัดหา การพัฒนา และบำรุงระบบสารสนเทศ (11) ความสัมพันธ์กับผู้ให้บริการภายนอก (12) การบริการจัดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (13) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (14) ความสอดคล้อง [10-11]

ผู้วิจัยได้ศึกษางานวิจัยที่เกี่ยวข้อง พบว่าองค์กรต่างๆ ทั้งภาครัฐและเอกชนได้ตระหนักถึงความสำคัญของการดูแลรักษาความมั่นคงและปลอดภัยทางเทคโนโลยีสารสนเทศ ได้มีการศึกษาและพัฒนานโยบายด้านความมั่นคงปลอดภัยภายใต้มาตรฐาน ISO27001 และการบริหารความเสี่ยง อาทิ กรณีศึกษา สถานศึกษาระดับพื้นฐาน [8] บริษัท เบทาโกร จำกัด (มหาชน) [9] โรงพยาบาลคลองใหญ่จังหวัดตราด [12] มหาวิทยาลัยกรุงเทพ [13] บริษัท อีวาตาร์ อินเทอมีเดีย [14] บริษัท ฟูจิตสึ ซีสเต็ม บีสซีเนส [15] บริษัท เอ็นอีซี คอร์ปอเรชั่น ประเทศไทย จำกัด [16] ศูนย์พัฒนาและบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพระนคร [17]

วิธีดำเนินการวิจัย

ประชากรที่ใช้ในการศึกษา ได้แก่ พนักงานขององค์กรกรณีศึกษาในสายงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 137 คน

ตัวแปรที่ใช้ในการศึกษา

ตัวแปรต้น ได้แก่ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013 (Annex A) 14 ด้าน ได้แก่ (1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (4) การบริหารจัดการทรัพย์สิน (5) การควบคุมการเข้าถึง (6) การเข้ารหัสข้อมูล (7) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (10) การจัดหา การพัฒนา และบำรุงระบบสารสนเทศ (11) ความสัมพันธ์กับผู้ให้บริการภายนอก (12) การบริการจัดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (13) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (14) ความสอดคล้อง [10-11]

ตัวแปรตาม ได้แก่ ระดับความเสี่ยงและแนวทางการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013

เครื่องมือในการศึกษาครั้งนี้ คือ “แบบสอบถาม” ซึ่งประกอบไปด้วย 2 ตอน คือ

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ได้แก่ เพศ อายุ ระดับการศึกษา และประสบการณ์ทำงาน จำนวน 4 ข้อ

ตอนที่ 2 การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013 ขององค์กรกรณีศึกษา จำนวน 133 ข้อ แบบสอบถามได้ผ่านการตรวจสอบคุณภาพของเครื่องมือโดยการตรวจสอบความตรงเชิงเนื้อหา (Content Validity) ความครอบคลุมของเนื้อหา และลักษณะของแบบสอบถามจากผู้เชี่ยวชาญจำนวน 3 ท่าน แบบสอบถามได้ถูกนำไปทดลองใช้กับพนักงานขององค์กรกรณีศึกษา (Pilot Test) จำนวน 30 ท่าน เพื่อหาค่าความเชื่อมั่นด้วยค่าสัมประสิทธิ์แอลฟา (α) ปรากฏว่าแบบสอบถามที่สร้างขึ้นมีค่า α เท่ากับ 0.90 แสดงว่าแบบสอบถามที่สร้างขึ้นมีค่าความเชื่อมั่นอยู่ในระดับสูง [18]

การเก็บรวบรวมข้อมูล

ผู้วิจัยใช้วิธีการเก็บรวบรวมข้อมูล โดยการแจกแบบสอบถามแก่พนักงานองค์กรกรณีศึกษา ระหว่างวันที่ 15 มกราคม 2560 ถึง 15 มีนาคม 2560

การวิเคราะห์ข้อมูลและสถิติที่ใช้

โอกาสในการเกิดความเสี่ยง (Likelihood) คือ การประเมินโอกาสในการเกิดความเสี่ยงนั้นๆ ซึ่งระดับคะแนนโอกาสในการเกิดความเสี่ยงจะแบ่งออกเป็น 5 ระดับจากมากไปหาน้อย (สูงมาก สูง ปานกลาง น้อย น้อยมาก) ดังตารางที่ 1

ระดับความรุนแรงของผลกระทบที่เกิดขึ้นจากความเสี่ยง (Impact) คือ การประเมินค่าระดับความรุนแรงของผลกระทบของเหตุการณ์ที่มีความเสี่ยงโดยพิจารณาจากทรัพย์สินและประสิทธิภาพการทำงานขององค์กรกรณีศึกษา ซึ่งระดับความรุนแรงของผลกระทบของความเสี่ยงจากมากไปหาน้อย ดังตารางที่ 2

ระดับของความเสี่ยงโดยรวม (Risk Exposure) คือ ผลลัพธ์ที่ได้จากการพิจารณาความสัมพันธ์ระหว่างโอกาสในการเกิดความเสี่ยงและระดับความรุนแรงของผลกระทบที่เกิดขึ้นจากความเสี่ยง ดังภาพที่ 2

จากแผนผังประเมินระดับความเสี่ยงโดยรวม (Risk Assessment Matrix) ให้นำรายการความเสี่ยงของแต่ละระดับความเสี่ยงมาจัดเรียงลำดับ (Risk Ranking) แล้วนำมาวิเคราะห์เปรียบเทียบกับเกณฑ์ความสามารถในการยอมรับความเสี่ยงตามการจำแนกระดับความเสี่ยงโดยรวมทั้งหมด 4 ระดับ ได้แก่ สูงมาก สูง ปานกลาง และ ต่ำ ดังตารางที่ 3

ผลการวิจัย

สถานภาพเบื้องต้นของผู้ตอบแบบสอบถาม พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง คิดเป็นร้อยละ 54.95 อายุอยู่ในช่วง 30-39 ปี คิดเป็นร้อยละ 46.65 การศึกษาระดับสูงสุด คือ ระดับปริญญาตรี คิดเป็นร้อยละ 79.28 และมีประสบการณ์การทำงานระหว่าง 6-10 ปี คิดเป็นร้อยละ 37.84

องค์กรกรณีศึกษา มีความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับสูง 6 ด้าน ได้แก่ (1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (2) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (3) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (4) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (5) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม และ (6) การบริการจัดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ นอกจากนั้นยังพบว่ามีความเสี่ยงอยู่ระดับปานกลาง 8 ด้าน ได้แก่ (1) ความมั่นคงปลอดภัยสารสนเทศ (2) การบริหารจัดการทรัพย์สิน (3) การควบคุมการเข้าถึง (4) การเข้ารหัสข้อมูล (5) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (6) การจัดหา การพัฒนา และบำรุงระบบสารสนเทศ (7) ความสัมพันธ์กับผู้ให้บริการภายนอก (8) ความสอดคล้อง ดังตารางที่ 4

สำหรับความเสี่ยงที่พบอยู่ในระดับสูงนั้น องค์กรไม่สามารถยอมรับได้ ดังนั้น จะต้องพิจารณาหาแนวทางในการบริหารจัดการความเสี่ยงให้ลดลงและอยู่ในระดับที่องค์กรสามารถยอมรับได้ ส่วนความเสี่ยงในระดับปานกลางจะต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้

แนวทางในการบริหารจัดการความเสี่ยง

จากผลการวิจัยสามารถสรุปแนวทางในการบริหารจัดการความเสี่ยงได้ 6 แนวทาง ดังตารางที่ 5

อภิปรายผล

จากผลการประเมินความเสี่ยงขององค์กรณีศึกษา พบว่า นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) มีความเสี่ยงอยู่ในระดับที่สูงสุดที่สุด ซึ่งสอดคล้องกับ การพัฒนานโยบายด้านความปลอดภัยภายใต้มาตรฐาน ISO27001 และการบริหารความเสี่ยง มหาวิทยาลัยกรุงเทพ [13] และการศึกษาแนวทางการพัฒนานโยบายความมั่นคงปลอดภัยสารสนเทศภายในองค์กร กรณีศึกษา บริษัท เอ็นอีซี คอร์ปอเรชั่น ประเทศไทย จำกัด [16] การมีนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่ชัดเจนจะสร้างความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศเพื่อการดำเนินงานขององค์กรได้อย่างมีประสิทธิภาพและประสิทธิผล และผลจากการวิเคราะห์ข้อมูลประเมินความเสี่ยง แสดงให้เห็นค่าระดับคะแนนของความเสี่ยงซึ่งสะท้อนให้เห็นค่าระดับคะแนนที่แตกต่างกัน ทำให้องค์กรกรณีศึกษาทราบว่า ความเสี่ยงในด้านใดที่ควรได้รับการบริหารจัดการอย่างเร่งด่วนก่อน สามารถวางแผนเพื่อกำหนดแนวทางการปฏิบัติในการป้องกันและควบคุมความเสี่ยง กำหนดระยะเวลา และผู้รับผิดชอบได้อย่างมีคุณภาพ

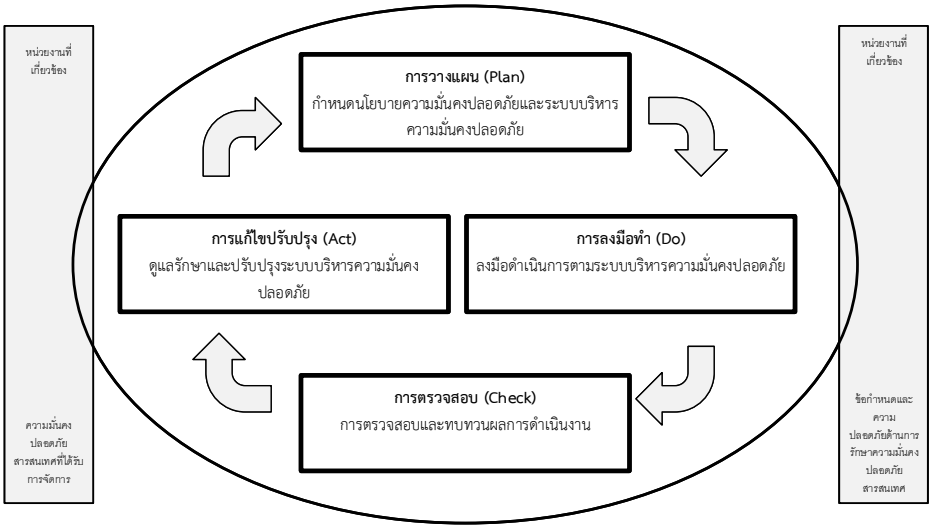
ข้อเสนอแนะ

1. นำแผนบริหารความเสี่ยงที่ได้ เข้าที่ประชุมเสนอให้ผู้บริหารพิจารณาเพื่อนำไปใช้จริง ทั้งนี้จัดตั้งคณะกรรมการเพื่อดำเนินการตรวจสอบความถูกต้องและประเมินความเป็นไปได้ในการดำเนินการตามแนวทางต่างๆ ที่ได้ระบุไว้ในแผน
2. การประกาศให้นำแผนฯ ไปใช้อย่างเป็นทางการและมีกลไกกำกับติดตามรายงานผลเป็นระยะ เพื่อให้สามารถวัดได้ว่าระบบบริหารความเสี่ยงขององค์กรกรณีศึกษาดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผลและเป็นไปตามเป้าหมายหรือไม่

เอกสารอ้างอิง

1. IT Best Practices Report [Internet]. 2014. Retrieved February, 2016, from https://goo.gl/tzm1DY
2. Threat Horizon 2016 – On the Edge of Trust [Internet]. 2016. Retrieved January, 2016, from https://www.acisonline.net/?p=5040&lang=th. Thai.
3. Risk Management Plan for Ministry of Agriculture and Cooperatives 2015-16. [Internet]. 2015. Retrieved January, 2016, from https://www.opsmoac.go.th/download/article/article_20160818095340.pdf. Thai.
4. Risk Management Plan for Chandrakasem Rajabhat University. [Internet]. 2015. Retrieved January, 2016, from http://teacher.chandra.ac.th/audit/images/Paper/Risk_plan2558_2559_new.pdf. Thai

5. IT Risk Management for Department of Medical Services. [Internet]. 2010. Retrieved January, 2016, from http://www.dms.moph.go.th/dmsweb/pmqa/dmsict-risk.pdf. Thai.
6. Annual Report of Airports of Thailand Public Company Limited 2015 [Internet]. 2015. Retrieved January, 2016, from http://cdn.airportthai.co.th/pdf/AOT_AR_PDF-th.pdf. Thai.
7. Risk Management Plan of Ministry of Digital Economy and Society 2014 [Internet]. 2014. Retrieved January, 2016, from http://www.mict.go.th/assets/portals/1/files/download/24_6_2557_s.pdf. Thai.
8. Nutthida S. Development of Guidelines for Secure Use of Information Technology in Basic Education Institutes based on ISO/IEC 27001 Standard. [MSIT thesis]. Bangkok: Sripatum University; 2012. Thai.
9. Worawuth C. The Development of Security Framework for Data Center a Case Study of Betagro Co. Ltd. [MSIT thesis]. Bangkok: Sripatum University; 2012. Thai.
10. Humphreys E. Information Security Management System Standards. Datenschutz und Datensicherheit. 2011, 35(1): 7-11.
11. Humphreys T. State-of-the-art Information Security Management Systems with ISO/IEC 27001, ISO Management Systems. 2005, 6(1): 15-18.
12. Rungarun N, Vipa J. The Development of Information Security Management for Access Control Based on ISO/IEC 27001:2013 for Klongyai Hospital Trat Province. Proceeding of the 4th STOU Graduate Research Conference; 2014; Nov 26-27; Nonthaburi, Thailand.
13. Nattawut V. Developing Security Policy Under standard ISO27001 and Risk management for Bangkok University. [MSNE thesis]. Phathumthani: Mahanakorn University of Technology; 2011. Thai.
14. Monsicha T. Developing Security Policy Under ISO 27001 Standard Case Study for Evatar intermedia. [MSNE thesis]. Phathumthani: Mahanakorn University of Technology; 2015. Thai.
15. Panuwat S. Developing Security Policy Under ISO27001 Standard Case Study for Fujitsu Systems Business (Thailand) Ltd. [MSNE thesis]. Phathumthani: Mahanakorn University of Technology; 2012. Thai.
16. Phumin P. Development of Information Technology Security Policy by Applying ISO/IEC 27001 Related to Computer Crime Act 2550: A Case Study of NEC Corporation (Thailand) Ltd. [MTT thesis]. Phathumthani: Thammasat University; 2009. Thai.
17. Paisan C. Development of Information Systems Security According to ISO 27001 Case Study for Information Technology Development and Service Center, Phranakhon Rajabhat University [MSIT thesis]. Phathumthani: Mahanakorn University of Technology; 2014. Thai.
18. Teera K. Evaluating the Quality of Research Tools. Knowledge Exchange Workshop on Quantitative research techniques; 2016; Jun 19; Burapha University, Chonburi, Thailand. Thai.
19. Berg HP. Risk management: Procedures, methods and experiences. Risk Management. 2010, 1: 79-95.
20. Ministry of Natural Resources and Environment 2012-2016 ICT Master Plan. [Internet]. Retrieved January, 2016, from http://www.mnre.go.th/ewt_dl_link.php?nid=10727. Thai.
21. Risk Management Plan for ICT 2015-16 [Internet]. 2015. Retrieved January, 2016, from http://www.dede.go.th/download/files/cio0002.pdf. Thai.



ภาพที่ 1 PCDA สำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ [8-9]

ตารางที่ 1 ระดับคะแนนโอกาสในการเกิดความเสี่ยง [19-21]

ระดับ	โอกาสในการเกิด	คำอธิบาย
5	สูงมาก	ความถี่ที่อาจเกิดขึ้นภายใน 1 เดือนต่อครั้งหรือมากกว่า หรือมีโอกาสเกิดขึ้นบ่อยครั้งหรือเป็นประจำ
4	สูง	ความถี่ที่อาจเกิดขึ้นตั้งแต่ 2-4 เดือนต่อครั้งหรือมากกว่า หรือมีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	ความถี่ที่อาจเกิดขึ้นตั้งแต่ 5-7 เดือนต่อครั้งหรือมากกว่า หรือมีโอกาสเกิดบ้างบางครั้ง
2	น้อย	ความถี่ที่อาจเกิดขึ้นตั้งแต่ 8-10 เดือนต่อครั้งหรือมากกว่า หรือมีโอกาสเกิดขึ้นบ้างแต่น้อยมาก
1	น้อยมาก	ความถี่ที่อาจเกิดขึ้นตั้งแต่ 11 เดือนถึง 1 ปีต่อครั้งหรือมากกว่า หรือมีโอกาสเกิดได้เฉพาะสถานการณ์ผิดปกติเท่านั้น หรือมีโอกาสเกิดขึ้นบ้างหรือแทบจะไม่เกิดขึ้นเลย

ตารางที่ 2 ระดับคะแนนความรุนแรงของผลกระทบที่จะเกิดขึ้นจากความเสี่ยง [19-21]

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

ระดับความเสี่ยงโดยรวม = โอกาสที่จะเกิดความเสี่ยง x ผลกระทบที่เกิดขึ้นจากความเสี่ยง

ผลกระทบที่เกิดขึ้นจากความเสี่ยง						
สูงมาก	(5)	5 (5x1)	10 (5x2)	15 (5x3)	20 (5x4)	25 (5x5)
สูง	(4)	4 (4x1)	8 (4x2)	12 (4x3)	16 (4x4)	20 (4x5)
ปานกลาง	(3)	3 (3x1)	6 (3x2)	9 (3x3)	12 (3x4)	15 (3x5)
น้อย	(2)	2 (2x1)	4 (2x2)	6 (2x3)	8 (2x4)	10 (2x5)
น้อยมาก	(1)	1 (1x1)	2 (1x2)	3 (1x3)	4 (1x4)	5 (1x5)
		(1) น้อยมาก	(2) น้อย	(3) ปานกลาง	(4) สูง	(5) สูงมาก

โอกาสที่จะเกิดความเสี่ยง

ภาพที่ 2 แผนผังประเมินระดับความเสี่ยงโดยรวม (Risk Assessment Matrix)

ตารางที่ 3 เปรียบเทียบระดับความเสี่ยงกับเกณฑ์ความสามารถในการยอมรับความเสี่ยง [20-21]

ความเสี่ยงโดยรวม	ผลลัพธ์ โอกาสในการเกิด x ผลกระทบ	รายละเอียดความเสี่ยง	เกณฑ์การยอมรับ
■	16.50 – 25.00 = สูงมาก	มีโอกาสที่จะเกิดความเสี่ยงสูงมาก หรือหากเกิดความเสี่ยงขึ้นจะส่งผลกระทบต่อระบบงานที่สำคัญทั้งหมด	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
■	10.50 – 16.49 = สูง	มีโอกาสที่จะเกิดความเสี่ยงสูง หรือหากเกิดความเสี่ยงขึ้นจะส่งผลกระทบต่อระบบงานบางส่วน	ระดับไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่รับได้
■	5.50 – 10.49 = ปานกลาง	มีโอกาสที่จะเกิดความเสี่ยง หรือหากเกิดความเสี่ยงขึ้นจะส่งผลกระทบต่อระบบงานเพียงเล็กน้อย	ระดับที่พอยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
■	1.00 – 5.49 = ต่ำ	มีโอกาสที่จะเกิดความเสี่ยงต่ำหรือหากเกิดความเสี่ยงขึ้นจะไม่ส่งผลกระทบกับระบบงาน	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

ตารางที่ 4 ตารางสรุปผลการประเมินความเสี่ยงขององค์กรกรณีศึกษา

ความเสี่ยง	ความเสี่ยงโดยรวม	แปลความ		แนวทางการบริหารจัดการความเสี่ยง	
		สูง	ปานกลาง	จัดการความเสี่ยงให้ลดลง	ควบคุมความเสี่ยง
1. นโยบายความมั่นคงปลอดภัยสารสนเทศ	14.40	✓		✓	
2. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ	10.08		✓		✓
3. ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล	11.56	✓		✓	
4. การบริหารจัดการทรัพย์สิน	9.00		✓	✓	✓
5. การควบคุมการเข้าถึง	8.98		✓	✓	✓
6. การเข้ารหัสข้อมูล	8.59		✓	✓	✓
7. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	11.25	✓		✓	
8. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน	13.65	✓		✓	
9. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล	7.56		✓		✓
10. การจัดหา การพัฒนา และบำรุงระบบสารสนเทศ	6.75		✓		✓
11. ความสัมพันธ์กับผู้ให้บริการภายนอก	6.20		✓		✓
12. การบริการจัดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	10.80	✓		✓	
13. ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ	12.38	✓			
14. ความสอดคล้อง	5.90		✓		✓

ตารางที่ 5 แนวทางในการบริหารจัดการความเสี่ยง

ความเสี่ยง	แนวทางในการบริหารจัดการความเสี่ยง
นโยบายความมั่นคงปลอดภัยสารสนเทศ	องค์กรจะต้องกำหนดมีโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศที่เป็นลายลักษณ์อักษร เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยเกี่ยวกับระบบสารสนเทศขององค์กรที่ตอบสนองต่อพันธกิจและนโยบายขององค์กร โดยนโยบายจะต้องได้รับการอนุมัติจากผู้บริหารก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ
ความมั่นคงปลอดภัยสำหรับการดำเนินงาน	องค์กรจะต้องกำหนดให้ผู้ดูแลระบบมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย
ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ	องค์กรจะต้องกำหนดแนวทางการดำเนินงานในสถานการณ์ฉุกเฉิน มีการจัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยทั้งในส่วนของแผน Business Continuity Plan (BCP) และแผน Disaster Recovery Plan (DRP) เพื่อให้หน่วยงานมีความสามารถในการให้บริการอย่างต่อเนื่องได้
ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล	องค์กรจะต้องกำหนดนโยบายความปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล ดังนี้ (1) บุคลากรภายในองค์กร หรือหน่วยงานภายนอกที่องค์กรว่าจ้างจะต้องปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยขององค์กรอย่างเคร่งครัด (2) ตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหาร หรือบุคลากรโดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน (3) กำหนดวินัยเพื่อลงโทษบุคลากรที่ฝ่าฝืนหรือละเมิดข้อตกลงด้านความมั่นคงปลอดภัยด้านสารสนเทศภายในองค์กร (4) ผู้ดูแลระบบต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน
ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	องค์กรควรมีการติดตั้งระบบป้องกันอัคคีภัย เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้อย่างทันท่วงที
การบริการจัดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	องค์กรควรมีการตั้งคณะกรรมการพิจารณามูลค่าความเสียหายและปริมาณความถี่จากบุกรุกเข้าระบบ โดยการบันทึกเหตุการณ์ที่เกิดขึ้น สาเหตุที่เกิดขึ้น ปริมาณความถี่ มูลค่าความเสียหายที่หน่วยงานได้รับ และรายงานให้กับผู้บริหารทราบเป็นระยะ