สภาพปัญหา การประเมิน และการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของวิสาหกิจขนาดกลางและขนาดย่อมในอำเภอหนองแค จังหวัดสระบุรี*

Problems, Assessment and Management of Information Technology Risks in Small and Medium Enterprises (SMEs), Nong. Khae District, Saraburi Province

เอกชัย ประเสริฐวงษ์**

วศิณ ชูประยูร***

*วิทยานิพนธ์หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมดิจิทัลและเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต

**นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมดิจิทัลและเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต, E-mail: p_akachai@hotmail.com

***ผู้ช่วยศาสตราจารย์ สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมดิจิทัลและเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต, E-mail: vasin@rsu.ac.th

ได้รับบทความ: 11 ก.พ. 62 / แก้ไขปรับปรุง: 11 ต.ค. 62 / อนุมัติให้ตีพิมพ์: 17 พ.ย. 62 / เผยแพร่ออนไลน์: 19 ธ.ค. 62

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหา ประเมิน และพัฒนาแนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศของผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อมในอำเภอหนองแค จังหวัดสระบุรี ประยุกต์มาตรฐาน ISO:IEC 27001 เป็นพื้นฐานความคิดในการพัฒนากรอบการวิจัย ใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากผู้ประกอบการดังกล่าว จำนวน 200 บริษัท ใช้สถิติการวิเคราะห์ถดถอยเชิงเส้นแบบพหุและการวิเคราะห์ถดถอยโลจิสติกในการทดสอบสมมติฐาน ผลวิจัยพบว่า ผู้ประการส่วนใหญ่ประสบปัญหาเกี่ยวกับการจัดการความเสี่ยงในด้านข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร และเครือข่าย ในระดับมากทุกด้าน มีโอกาสที่จะเกิดความเสี่ยงระดับมากในด้านการถูกโจมตีและเปลี่ยนแปลงข้อมูลการเงิน/บัญชีของบริษัท และการใช้ข้อมูลรายงานทางบัญชีในการระบุ

ปัญหาที่เกิดขึ้นในการดำเนินธุรกิจของบริษัท และพบว่ามีความน่าจะเป็นที่ความเสี่ยงด้านการขาดการประเมินความเสี่ยงในการใช้อุปกรณ์สำรองข้อมูลที่ไม่ถูกต้อง และการขาดการประเมินความเสี่ยงในการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์แวดล้อมของพนักงาน จะมีผลกระทบต่อการดำเนินธุรกิจของบริษัทในระดับมาก ผลการทดสอบสมมติฐานชี้ให้เห็นว่าสภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศมีอิทธิพลต่อโอกาสและผลกระทบของความเสี่ยงต่อการดำเนินธุรกิจได้โมเดลอิทธิพล จำนวน 26 โมเดล และสภาพปัญหาดังกล่าว รวมทั้งโอกาสและผลกระทบของความเสี่ยง ล้วนมีความน่าจะเป็นที่จะส่งผลต่อแนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศทั้ง 5 ด้าน คือ การลดความเสี่ยง การโอนย้ายความเสี่ยง การหลีกเลี่ยงความเสี่ยง และการคงไว้ซึ่งความเสี่ยง ได้โมเดลความน่าจะเป็นจำนวน 47 โมเดล

คำสำคัญ: สภาพปัญหาความเสี่ยงเทคโนโลยีสารสนเทศ การประเมินความเสี่ยงเทคโนโลยีสารสนเทศ การจัดการความเสี่ยงเทคโนโลยีสารสนเทศ ISO/IEC 27001

Abstract

This research aimed to study the problems, assess and develop information technology risk management approaches of small and medium enterprises (SMEs) in Nong Khae District, Saraburi Province. The ISO standards/ IEC 27001 was applied as a conceptual fundamental for developing a research framework. The questionnaires were used as a tool to gather data from the 200 SMEs. Multiple linear regression analysis and logistic regression analysis ere used for hypothesis test. The study found that most of the SMEs experienced problems with risk management in terms of data, hardware, software, personnel and networks at a high level. There were high opportunities at high risk of being attacked and changing financial/accounting data of the companies would be occurred in the SMEs; including the use of accounting report data to identify problems in the business operations of the company. The study also resulted that there were probabilities of a lack of assessment in the use of inappropriate backup devices and

computer equipment and its peripherals of employees; which would affect the business performance of the SMEs at a high level. The hypothesis test indicated that the information technology risk management problems had an influence on the opportunities and impacts of the risks to the business performance. The test obtained 26 influencing models. The information technology risk management problems, including the opportunities and impacts of the risks, all of which are likely to affect the information technology risk management approaches in 5 areas: risk reduction, risk sharing, risk avoidance, and risk retention. The test generated the 47 probability models.

Keywords: IT Risk, IT Risk Assessment, IT Risk Management, ISO/IEC 27001

ความเป็นมาและความสำคัญของปัญหา

เทคโนโลยีเปลี่ยนแปลงโลก หรือ Disruptive Technology และ การเข้าร่วมประชาคมเศรษฐกิจอาเซียน (ASEAN Economics Community—AEC) ทำให้ผู้ประกอบการ SMEs ในประเทศไทยหันมาให้ความสำคัญกับการพัฒนาทักษะการใช้เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเป็นเครื่องมือในการดำเนินธุรกิจให้ประสบผลสำเร็จแบบไร้พรมแดน ด้วยการลงทุนไปพร้อมๆ กับการจัดการกับความเสี่ยงด้านเทคโนโลยีสารสนเทศและที่เกี่ยวข้องที่อาจเกิดขึ้น อาทิ การแพร่กระจายของไวรัสและมัลแวร์ ความแตกต่างระหว่างรุ่นของซอฟต์แวร์ การทำงานตามมาตรฐานของตนโดยไม่อิงมาตรฐานสากล ความผิดพลาดของระบบเครือข่ายจากการให้บริการภายนอก การขาดทักษะและความรู้เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของผู้ประกอบการ การขาดการจัดการสภาพปัญหาความเสี่ยงจากภายในและภายนอกต่อระบบสารสนเทศที่มีความอ่อนไหว การขาดองค์รู้/ข้อมูลข่าวสาร และการป้องกันความเสี่ยงที่อาจเกิดขึ้นในอนาคต ซึ่งจะส่งผลกระทบต่อระบบสารสนเทศของผู้ประกอบการ

จากการศึกษานำร่อง (Pilot Study) ด้วยการสัมภาษณ์ผู้ประกอบการ SMEs ในอำเภอหนองแค จังหวัดสระบุรี จำนวนหนึ่ง พบว่าผู้ประกอบการเหล่านี้ประสบปัญหาเช่นเดียวกันกับที่กล่าวแล้วข้างต้น จากสภาพปัญหาดังกล่าวนี้ผู้วิจัยจึงประสงค์จะศึกษาการจัดการความเสี่ยงของ SMEs ในอำเภอหนองแค

จังหวัดสระบุรี เพื่อนำผลการวิจัยไปเป็นองค์ความรู้พื้นฐานในการจัดการความเสี่ยงเทคโนโลยีสารสนเทศของผู้ประกอบการ SMEs ในพื้นที่ดังกล่าวเพื่อให้ผู้ประกอบการตระหนัก เข้าใจ พัฒนา และปรับปรุงกระบวนการจัดการความเสี่ยงสารสนเทศตามกรอบมาตรฐานสากล ISO/IEC 27001: 2013 รวมทั้งสามารถประยุกต์ใช้กรอบมาตรฐานดังกล่าวในการจัดการความเสี่ยงเหล่านั้น และสามารถบูรณาการเข้ากับสภาพแวดล้อมและปัญหาของ SMEs ในทุกมิติ ในขณะเดียวกัน รัฐบาลได้กำหนดยุทธศาสตร์ชาติด้วยกลไกที่เรียกว่า ประเทศไทย 4.0 (Thailand 4.0) ซึ่งกลไกนี้มีมาตรฐานการจัดการความเสี่ยงที่ชัดเจน สามารถระบุแยกแยะ วิเคราะห์ ดำเนินการจัดการความเสี่ยงที่มีผลกระทบต่อการดำเนินงานของ SMEs ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์การวิจัย

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหา การประเมิน และการจัดการความเสี่ยงเทคโนโลยีสารสนเทศของผู้ประกอบการ SMEs ในอำเภอหนองแค จังหวัดสระบุรี

แนวคิดและทฤษฎีพื้นฐานการวิจัย

แนวคิดและทฤษฎีที่เป็นพื้นฐานของการวิจัยในครั้งนี้ ได้แก่ ความมั่นคงปลอดภัยสารสนเทศ 3 มิติ หรือเรียกโดยย่อว่า CIA ประกอบด้วย ความลับของสารสนเทศ (C: Confidentiality) เป็นการรักษาความลับของข้อมูลด้วยการให้สิทธิเข้าถึงข้อมูลได้เฉพาะผู้ได้รับอนุญาตเท่านั้น สถานประกอบการอาจจัดลำดับขั้นการเข้าถึงข้อมูลด้วยการระบุตัวตนเป็นเบื้องต้น และข้อมูลในระบบสารสนเทศต้องมีความถูกต้องแม่นยำตรงกันทั้งฝ่ายผู้ส่งและผู้รับ (I: Integrity) ข้อมูลจะไม่สามารถแก้ไขได้ในระหว่างเส้นทางการส่งผ่านโดยบุคคลใดบุคคลหนึ่ง ตลอดจนถึงความพร้อมใช้ (A: Availability) ของระบบสารสนเทศที่อุดมพร้อมด้วยศักยภาพของข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร และเครือข่าย ที่ปฏิบัติการได้ทันทีตลอดเวลา ปราศจากความผิดพลาดและความล้มเหลวในขณะใช้งาน (King, 2017)

แนวคิดและทฤษฎีที่เป็นพื้นฐานของการวิจัยอีกประการหนึ่ง คือ ISO/IEC 27001:2013 (International Organization for Standardization and International Electrotechnical Commission

[ISO/IEC], 2013); Shojaie, Federrath, & Saberi (2014) ซึ่งเป็นกรอบมาตรฐานว่าด้วยข้อกำหนดสำหรับการบำรุงรักษาและการพัฒนาระบบการจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่องภายในบริบทองค์กร เป็นข้อกำหนดสำหรับการประเมินและรักษาความเสี่ยงด้านความปลอดภัยข้อมูลที่ปรับให้เหมาะสมกับความต้องการขององค์กรใน 5 มิติ คือ ก) ข้อมูล ข) ฮาร์ดแวร์ ค) ซอฟต์แวร์ ง) บุคลากร และ จ) เครือข่าย แบ่งเป็น 2 ส่วน คือ 1) ระบบจัดการความมั่นคงปลอดภัย และ 2) มาตรการจัดการความมั่นคงปลอดภัย 14 มาตรการ

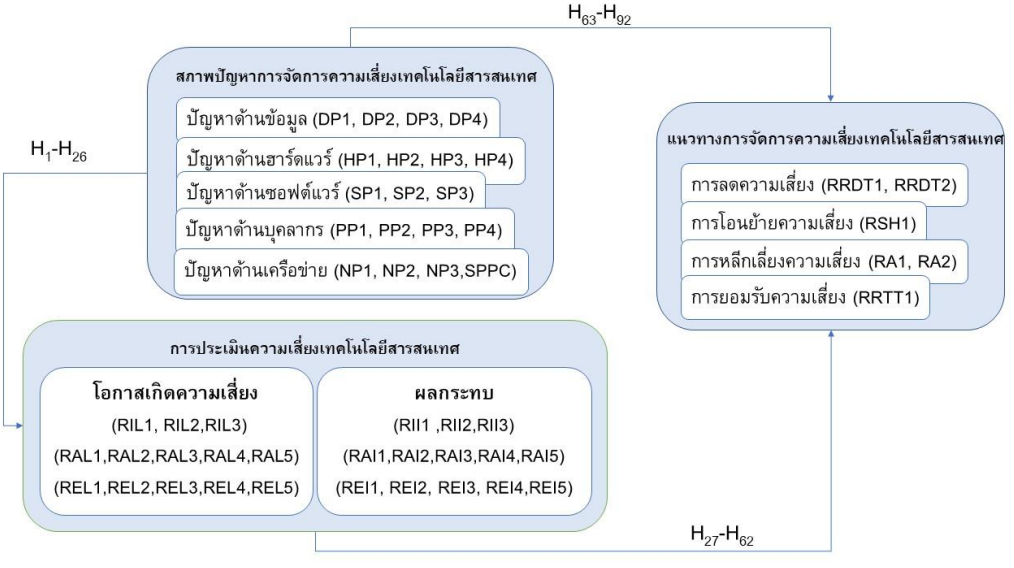
มาตรการทั้ง 14 ด้าน ได้แก่ 1) การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ 2) การจัดระบบความมั่นคงปลอดภัยสารสนเทศ 3) การมีกระบวนการความมั่นคงปลอดภัยในทรัพยากรมนุษย์ (การตรวจสอบประวัติพนักงาน การกำหนดเงื่อนไขความรับผิดชอบตามสัญญาจ้างการบริการภายนอก) 4) การจัดการสินทรัพย์ 5) การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศภายในองค์กร 6) การเข้ารหัสข้อมูล 7) การจัดการความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม 8) การกำหนดขั้นตอนการปฏิบัติงานและหน้าที่รับผิดชอบเพื่อลดความเสี่ยงจากการเปลี่ยนแปลงสภาพแวดล้อม โปรแกรมไม่พึงประสงค์ ช่องโหว่ทางเทคนิค และการสำรองข้อมูล 9) การจัดการความมั่นคงปลอดภัยในการสื่อสารข้อมูล 10) การจัดหา/การพัฒนา/การบำรุงรักษาระบบ 11) การจัดการความสัมพันธ์กับผู้ให้บริการภายนอก 12) การจัดการอุบัติการณ์ความมั่นคงปลอดภัยสารสนเทศ 13) การกำหนดทิศทางความมั่นคงปลอดภัยสารสนเทศของการจัดการความต่อเนื่องทางธุรกิจ และ 14) การปฏิบัติตามระเบียบข้อบังคับนโยบายต่างๆ ภายในองค์กรที่สอดคล้องกับกฎหมาย และสัญญาจัดซื้อจัดจ้าง เพื่อลดความเสี่ยงและข้อพิพาทที่เกิดขึ้นเกี่ยวกับกรรมสิทธิ์ซอฟต์แวร์และทรัพย์สินทางปัญญา จึงอาจกล่าวได้ว่า ISO/IEC 27001: 2013 เป็นกรอบมาตรฐานการบ่งชี้ความเสี่ยง การวิเคราะห์ความเสี่ยง และการตรวจสอบความเสี่ยง

การจัดการความเสี่ยงตามกรอบมาตรฐาน ISO/IEC 27001:2013 ประกอบด้วย กระบวนการ*ลดความเสี่ยง* (ลดความถี่ในการเกิดความเสี่ยง เช่น การอัปเดตซอฟต์แวร์ การป้องกันบุคคลภายนอกเข้าถึงอุปกรณ์ การจัดพื้นที่เฉพาะสำหรับอุปกรณ์สำคัญเพื่อป้องกันปัญหาทางกายภาพ การอบรมผู้ปฏิบัติงานและผู้มีส่วนเกี่ยวข้องตระหนักต่อภัยคุกคาม) กระบวนการถ่ายโอนความเสี่ยง (ทำสัญญาโอนความเสี่ยงให้ผู้เชี่ยวชาญภายนอกเป็นผู้รับผิดชอบทั้งในด้านฮาร์ดแวร์และซอฟต์แวร์) กระบวนการหลีกเลี่ยงความเสี่ยง (จัดการปัญหาก่อนเกิดเหตุการณ์ เช่น ปิดระบบเชื่อมต่ออุปกรณ์คอมพิวเตอร์ ปรับเปลี่ยนระบบปฏิบัติการ

ที่ไม่สามารถอัปเดตได้อีก เนื่องจากมีช่องโหว่ที่อาชญากรไซเบอร์สามารถโจมตีได้ง่าย และถ้าจะอัปเดตหรือแก้ไขจะมีค่าใช้จ่ายสูง) และกระบวนการยอมรับความเสี่ยง (ยอมรับความเสี่ยงที่มีความถี่ในการเกิดต่ำและมีผลกระทบต่อองค์กรเพียงเล็กน้อย ไม่มีความสูญเสียในวงกว้าง แต่ต้องเฝ้าติดตามการเปลี่ยนแปลงโดยไม่ต้องดำเนินการใดๆ) (Ernawati, Suhardi, & Nugroho, 2012; ISO/IEC, 2013)

กรอบแนวคิดของการวิจัย

จากการทบทวนแนวคิดและทฤษฎีที่เกี่ยวข้องข้างต้น ผู้วิจัยจึงกำหนดกรอบแนวคิดในการวิจัยครั้งนี้ดังนี้



รูปที่ 1 กรอบแนวคิดของการวิจัย

จากกรอบการวิจัย อธิบายรายละเอียดเกี่ยวกับตัวแปรดังนี้

ปัญหาด้านข้อมูล (Data Problem)	
DP1	การสำรองข้อมูลผิดพลาดอันเนื่องมาจากพนักงานใช้ขั้นตอนวิธีที่ไม่ถูกต้อง
DP2	การเข้มงวดพนักงานในการจัดการสิทธิการเข้าถึงข้อมูล
DP3	การป้องกันการโจมตีข้อมูลจากไวรัสและมัลแวร์
DP4	การเกิดความผิดพลาดในการจัดเก็บอัปเดตและทำลายข้อมูลผิดวิธี
ปัญหาด้านฮาร์ดแวร์ (Hardware Problem)	
HP1	พื้นที่ไม่เพียงพอต่อการติดตั้งอุปกรณ์สำคัญสำหรับระบบสารสนเทศ
HP2	การละเลยในการตรวจสอบความพร้อมใช้งานของอุปกรณ์อย่างสม่ำเสมอ
HP3	การนำอุปกรณ์เชื่อมต่อส่วนบุคคลมาเชื่อมต่อระบบโดยไม่ตรวจสอบไวรัสและมัลแวร์
HP4	ความต่อเนื่องในการอัปเดตปรับปรุงโปรแกรมของฮาร์ดแวร์
ปัญหาด้านซอฟต์แวร์ (Software Problem)	
SP1	การดาวน์โหลดซอฟต์แวร์และระบบปฏิบัติการที่ผิดกฎหมายมาใช้ในระบบโดยไม่ได้รับอนุญาต
SP2	การขาดความต่อเนื่องในการอัปเดตระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องกับการทำงาน
SP3	การขาดการอัปเดตปรับปรุงรุ่นซอฟต์แวร์ป้องกันไวรัสและมัลแวร์อย่างสม่ำเสมอ
ปัญหาด้านบุคลากร (Personnel Problem)	
PP1	พนักงานไม่มีความรู้ความเข้าใจที่ถูกต้องเกี่ยวกับไวรัสและมัลแวร์
PP2	การขาดความรู้ความเข้าใจในการใช้งานคอมพิวเตอร์ของพนักงาน

PP3	การควบคุมเข้มงวดในการใช้รหัสผ่านในการเข้าถึงระบบสารสนเทศ
PP4	การจัดอบรมให้ความรู้การใช้งานอุปกรณ์คอมพิวเตอร์อย่างถูกต้องปลอดภัย
ปัญหาด้านเครือข่าย (Network Problem)	
NP1	การเกิดเหตุเครือข่ายหยุดทำงานและพนักงานไม่สามารถจัดการปัญหาได้
NP2	การขาดการควบคุมป้องกันบุคคลภายนอกเข้าถึงเครือข่ายของบริษัท
NP3	การที่ผู้ให้บริการอินเทอร์เน็ตไม่มีการแจ้งล่วงหน้าในการซ่อมแซมเครือข่าย
Solution to Prevent Problem to Confidence	
SPPC	การขาดการหาแนวทางการป้องปัญหาที่จะกระทบเครือข่าย เช่น ไฟไหม้ น้ำท่วม และการป้องกันทรัพย์จากบุคคลภายในและภายนอก
โอกาสเกิดความเสี่ยง (Likelihood)	
RIL1	การไม่ทราบที่มาของปัญหาและสาเหตุที่ทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ตามปกติ
RIL2	การให้ความสำคัญในการประชุมเพื่อระบุปัญหาและสาเหตุของระบบสารสนเทศที่ส่งผลต่อการดำเนินธุรกิจ
RIL3	การใช้ข้อมูลรายงานทางบัญชีในการระบุปัญหาที่เกิดขึ้นในการดำเนินธุรกิจของบริษัท
RAL1	การขาดการวิเคราะห์สภาพปัญหาการติดไวรัสและมัลแวร์ในอุปกรณ์คอมพิวเตอร์และเครือข่ายของบริษัท
RAL2	การขาดการวิเคราะห์ถึงปัญหาที่ทำให้อุปกรณ์คอมพิวเตอร์และเครือข่ายของบริษัทประมวลผลล่าช้าและผิดพลาด
RAL3	การขาดการวิเคราะห์และพัฒนาแนวทางการแก้ไขปัญหาการใช้งานระบบปฏิบัติการต่างรุ่นในบริษัท

RAL4	การขาดการศึกษาและวิเคราะห์ปัญหาที่เกิดขึ้นจากการใช้ข้อมูลบริษัทบนสื่อสังคมออนไลน์
RAL5	การขาดการวิเคราะห์และพัฒนาแนวทางแก้ไขปัญหาในกรณีที่ผู้ให้บริการอินเทอร์เน็ตภายนอกหยุดให้บริการชั่วคราวเพื่อปรับปรุงแก้ไขระบบ
REL1	การขาดการประเมินความเสี่ยงจากผู้ไม่ประสงค์ดีโจมตีและเปลี่ยนแปลงข้อมูลการเงิน/บัญชีของบริษัท
REL2	การไม่ทราบข้อมูลข่าวสารทันสมัยด้านเทคโนโลยีสารสนเทศ ทำให้บริษัทไม่สามารถปรับปรุงระบบให้ทันตามความก้าวหน้าดังกล่าว จึงมีความเสี่ยงที่จะถูกโจมตีจากภายนอก
REL3	การขาดการประเมินความเสี่ยงในการใช้อุปกรณ์สำรองข้อมูลที่ถูกต้อง
REL4	การขาดการประเมินความเสี่ยงในการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์แวดล้อมของพนักงานในบริษัท
REL5	การขาดการประเมินความเสี่ยงจากความผิดพลาดของพนักงานที่ปฏิบัติการบนระบบเครือข่ายบริษัท
ผลกระทบ (Impact)	
RII1	ระดับผลกระทบของการไม่ทราบที่มาของปัญหาและสาเหตุที่ไม่สามารถใช้งานระบบสารสนเทศได้ตามปกติ
RII2	ระดับผลกระทบของการขาดการให้ความสำคัญในการประชุมเพื่อระบุปัญหาและสาเหตุของระบบสารสนเทศที่ส่งผลกระทบต่อการดำเนินธุรกิจ
RII3	ระดับผลกระทบของการขาดการใช้ข้อมูลรายงานทางบัญชีในการระบุปัญหาที่เกิดขึ้นส่งผลต่อการดำเนินธุรกิจของบริษัท
RAI1	ระดับผลกระทบของการขาดการวิเคราะห์สภาพปัญหาการติดไวรัสและมัลแวร์ที่ส่งผลต่ออุปกรณ์คอมพิวเตอร์และเครือข่ายของบริษัท

RAI2	ระดับผลกระทบของการขาดการวิเคราะห์ถึงปัญหาส่งผลต่ออุปกรณ์คอมพิวเตอร์และเครือข่ายของบริษัททำให้เกิดการประมวลล่าช้าและผิดพลาด
RAI3	ระดับผลกระทบของการขาดการวิเคราะห์และพัฒนาแนวทางการแก้ไขปัญหาส่งผลต่อการใช้งานระบบปฏิบัติการต่างรุ่นในบริษัท
RAI4	ระดับผลกระทบของการขาดการศึกษาและวิเคราะห์ปัญหาที่เกิดขึ้นส่งผลต่อการใช้ข้อมูลบริษัทบนสื่อสังคมออนไลน์
RAI5	ระดับผลกระทบของการขาดการวิเคราะห์และพัฒนาแนวทางแก้ไขปัญหา ในกรณีที่ผู้ให้บริการอินเทอร์เน็ตภายนอกแจ้งหยุดให้บริการชั่วคราวเพื่อบำรุงรักษาระบบ
REI1	ระดับผลกระทบการขาดการประเมินความเสี่ยงจากผู้ไม่ประสงค์ดีโจมตีส่งผลต่อการเปลี่ยนแปลงข้อมูลการเงิน/บัญชีของบริษัท
REI2	ระดับผลกระทบของการไม่ทราบข้อมูลข่าวสารทันสมัยด้านไอที ส่งผลกระทบต่อบริษัทไม่สามารถปรับปรุงระบบให้ทันตามความก้าวหน้าดังกล่าว จึงมีความเสี่ยงที่จะถูกโจมตีจากภายนอก
REI3	ระดับผลกระทบของการขาดการประเมินความเสี่ยงส่งผลกระทบต่อการใช้อุปกรณ์สำรองข้อมูลที่ไม่ถูกต้อง
REI4	ระดับผลกระทบของการขาดการประเมินความเสี่ยงในการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์แวดล้อมของพนักงานที่ส่งผลต่อการดำเนินธุรกิจ
REI5	ระดับผลกระทบของการขาดการประเมินความเสี่ยงจากความผิดพลาดของพนักงานที่ส่งผลต่อการปฏิบัติงานเกี่ยวข้องกับระบบเครือข่าย
การลดความเสี่ยง (Risk Reduction)	
RRDT1	การออกคำสั่งห้ามพนักงานนำอุปกรณ์ส่วนตัวเชื่อมต่อกับระบบคอมพิวเตอร์ในบริษัท

RRDT2	การใช้กฎระเบียบบังคับพนักงานให้ใช้รหัสผ่านเข้าถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย
การโอนย้ายความเสี่ยง (Risk Sharing)	
RSH1	การให้ผู้เชี่ยวชาญภายนอกจัดการแก้ไขปัญหาอุปกรณ์คอมพิวเตอร์และเครือข่าย
การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)	
RA1	การปรับปรุงแก้ไขอุปกรณ์คอมพิวเตอร์และเครือข่ายให้ปลอดภัยจากภัยคุกคามภายนอก
RA2	การติดตามข่าวสารทันสมัยด้านความก้าวหน้าของเทคโนโลยีสารสนเทศและนำมาปรับปรุงอุปกรณ์คอมพิวเตอร์และเครือข่ายของบริษัทให้ทันตามความก้าวหน้าดังกล่าว
การคงไว้ซึ่งความเสี่ยง (Risk Retention)	
RRTT1	การยอมรับปัญหาและความเสี่ยงที่ส่งผลกระทบต่อการใช้ข้อมูล อุปกรณ์ คอมพิวเตอร์ ซอฟต์แวร์ และเครือข่าย ในการปฏิบัติงานของพนักงานในบริษัท

ระเบียบวิธีวิจัย

ก) ประชากรและกลุ่มตัวอย่าง

ประชากรการวิจัยครั้งนี้คือ ผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อมในอำเภอหนองแค จังหวัดสระบุรี จำนวน 398 แห่ง (กรมโรงงานอุตสาหกรรม, 2560) ผู้วิจัยกำหนดกลุ่มตัวอย่างด้วยการใช้สูตรคำนวณของ Yamane (1973) ได้ขนาดกลุ่มตัวอย่างจำนวน 200 บริษัท

ข) เครื่องมือสำหรับการวิจัย

ผู้วิจัยพัฒนาแบบสอบถามเป็นเครื่องมือเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง ในแบบสอบถามประกอบด้วย 4 ตอน คือ ตอนที่ 1 ภูมิหลังของผู้ประกอบการ SMEs ในอำเภอหนองแค จังหวัดสระบุรี ตอนที่ 2 สภาพปัญหาความเสี่ยงเทคโนโลยีสารสนเทศ ตอนที่ 3 การประเมินโอกาสเกิดความเสี่ยงและผลกระทบ

ต่อเทคโนโลยีสารสนเทศ และตอนที่ 4 แนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ โดยแบ่งระดับคำตอบออกเป็น 5 ระดับ (5 = ระดับมากที่สุด 4 = ระดับมาก 3 = ระดับปานกลาง 2 = ระดับน้อย 1 = ระดับน้อยที่สุด) ตามมาตรวัดของลิเคิร์ท (Likert, 1932)

ค) การตรวจสอบคุณภาพเครื่องมือวิจัย

ผู้วิจัยทดสอบความเที่ยงตรงเชิงโครงสร้าง (Construct Validity) และเชิงเนื้อหา (Content Validity) ของแบบสอบถาม โดยผู้ทรงคุณวุฒิจำนวน 5 ท่าน ได้ให้ความอนุเคราะห์ตรวจสอบความเที่ยงตรงดังกล่าว จากนั้นนำมาคำนวณหาค่าดัชนีความสอดคล้อง (Indexes of Item-Objective Congruence หรือ IOC) ได้ค่าเท่ากับ 0.83 ซึ่งเป็นค่าที่บ่งชี้ว่าแบบสอบถามมีความเที่ยงตรงทั้งในเชิงโครงสร้างและเนื้อหาในระดับสูง (ค่าเกินกว่าค่ามาตรฐาน .50) จากนั้นได้นำแบบสอบถามไปทดลองใช้กับกลุ่มตัวอย่างจำนวน 30 บริษัท แล้วนำไปคำนวณหาค่าเชื่อมั่น (Reliability) ด้วยการคำนวณหาค่าสัมประสิทธิอัลฟาของครอนบัค (Cronbach, 1951) ได้ค่าสัมประสิทธิอัลฟาเท่ากับ .966 หมายความว่าชุดแบบสอบถามนี้มีค่าความเชื่อมั่นในระดับสูง สามารถนำไปใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างได้

ง) การเก็บรวบรวมข้อมูลและการวิเคราะห์ข้อมูล

ผู้วิจัยใช้เทคนิคการสุ่มตัวอย่างโดยใช้หลักความน่าจะเป็น (Probability Random Sampling) และสุ่มตัวอย่างแบบเป็นระบบ (Systematic Random Sampling) ด้วยการกำหนดสุ่มหมายเลขบริษัททั้ง 398 แห่ง แล้วแบ่งประชากรออกเป็นช่วงๆ ละ 5 ลำดับเท่าๆ กัน จากนั้นสุ่มเลือกหน่วยแรก ส่วนหน่วยต่อๆ ไปนับจากช่วงที่กำหนดไว้จนครบ 200 บริษัท จากนั้นแจกแบบสอบถามไปยังกลุ่มตัวอย่างด้วยการนำส่งด้วยตัวเอง ส่งผ่านระบบ Google Form และ แนบลิงค์ Google Form ไว้ในจดหมายอิเล็กทรอนิกส์เพื่อส่งไปยังกลุ่มตัวอย่าง ได้รับแบบสอบถามคืนจำนวน 200 ฉบับ (ร้อยละ 100.00) ข้อมูลที่ได้จากแบบสอบถามผู้วิจัยนำไปวิเคราะห์ด้วยเทคนิคทางสถิติใน 2 กลุ่มสถิติ คือ ก) สถิติพรรณนา ได้แก่ การคำนวณค่าร้อยละ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน และ ข) สถิติอ้างอิง ได้แก่ การวิเคราะห์การถดถอยเชิงเส้นแบบพหุ (Multiple Linear Regression) เพื่อทดสอบสมมติฐานที่ 1-26 และการวิเคราะห์ความถดถอยโลจิสติก (Logistic Regression) เพื่อทดสอบสมมติฐานที่ 27-92

การวิเคราะห์ผลการวิจัย

ในการวิจัยครั้งนี้ ผู้ตอบแบบสอบถามคือผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อมที่ดำเนินธุรกิจในอำเภอหนองแค จังหวัดสระบุรี ซึ่งนับจากนี้ไปตลอดทั้งบทความ จะเรียกว่า “ผู้ประกอบการ” ส่วนใหญ่ (ร้อยละ 77.00) เป็นผู้ประกอบการกิจการผลิตสินค้า จดทะเบียนธุรกิจในรูปแบบบริษัทจำกัด (ร้อยละ 68.00) ดำเนินธุรกิจมาแล้วมากกว่า 15 ปี (ร้อยละ 38.50) มีทุนจดทะเบียนมากกว่า 10 ล้านบาท (ร้อยละ 46.50) และมีพนักงานมากกว่า 30 คน (ร้อยละ 38.00) ผู้วิจัยนำเสนอข้อค้นพบจากการวิจัยตามแนววัตถุประสงค์ ดังนี้

(1) สภาพปัญหาการจัดการความเสี่ยง

1.1 *ด้านข้อมูล:* ผู้ประกอบการระบุว่าการเกิดความผิดพลาดในการจัดเก็บ อัปเดต และทำลายข้อมูลผิดวิธี (DP4) และการสำรองข้อมูลผิดพลาดอันเนื่องมาจากพนักงานใช้ขั้นตอนวิธีที่ไม่ถูกต้อง (DP1) เป็นสภาพปัญหาที่ผู้ประกอบการประสบบ่อยครั้งในระดับมาก ($\bar{X}$= 3.80, S.D.= 1.22 และ $\bar{X}$= 3.58, S.D.= 1.36 ตามลำดับ)

1.2 *ด้านฮาร์ดแวร์*: ผู้ประกอบการส่วนใหญ่เห็นว่าการมีพื้นที่ไม่เพียงพอต่อการติดตั้งอุปกรณ์สำคัญสำหรับระบบสารสนเทศ (HP1) และความต่อเนื่องในการอัปเดตปรับปรุงโปรแกรมของฮาร์ดแวร์ (HP4) เป็นปัญหาในระดับมากของบริษัท ($\bar{X}$= 3.84, S.D.= 1.22 และ $\bar{X}$=3.76, S.D.= 1.32 ตามลำดับ)

1.3 *ด้านซอฟต์แวร์:* ผู้ประกอบการระบุว่าการดาวน์โหลดซอฟต์แวร์และระบบปฏิบัติการที่ผิดกฎหมายมาใช้ในระบบโดยไม่ได้รับอนุญาต (SP1) รวมทั้งการขาดการอัปเดตปรับปรุงรุ่นซอฟต์แวร์ป้องกันไวรัสและมัลแวร์อย่างสม่ำเสมอ (SP3) เป็นปัญหาในระดับมากของบริษัท ($\bar{X}$= 3.96, S.D.= 1.24 และ $\bar{X}$=3.91, S.D.= 1.22 ตามลำดับ)

1.4 *ด้านบุคลากร:* การควบคุมเข้มงวดในการใช้รหัสผ่านในการเข้าถึงระบบสารสนเทศ (PP3) การจัดอบรมให้ความรู้การใช้งานอุปกรณ์คอมพิวเตอร์อย่างถูกต้องปลอดภัย (PP4) เป็นอีก 2 สภาพปัญหาสำคัญเกี่ยวกับบุคลากร ที่บริษัทต้องทุ่มเทความพยายามในการจัดการ ($\bar{X}$= 3.86, S.D.= 1.28 และ $\bar{X}$= 3.65, S.D.= 1.25 ตามลำดับ)

1.5 *ด้านเครือข่าย:* การขาดการควบคุมป้องกันบุคคลภายนอกเข้าถึงเครือข่ายของบริษัท (NP2) และ การที่ผู้ให้บริการอินเทอร์เน็ตไม่มีการแจ้งล่วงหน้าในการซ่อมแซมเครือข่าย (NP3) ($\bar{X}$= 3.87, S.D.= 1.17 และ $\bar{X}$= 3.60, S.D.= 1.24 ตามลำดับ)

(2) ผลการประเมินความเสี่ยงเทคโนโลยีสารสนเทศ

2.1 *โอกาสเกิดความเสี่ยง:* ผลการประเมินชี้ว่าผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อมมีโอกาสที่จะถูกโจมตีและเปลี่ยนแปลงข้อมูลการเงิน/บัญชีของบริษัท เพราะไม่เคยประเมินความเสี่ยงจากผู้ไม่ประสงค์ดีภายนอก (REL1) ($\bar{X}$= 3.89, S.D.= 1.34) และยังชี้ว่า มีความเสี่ยงจากการใช้ข้อมูลรายงานทางบัญชีในการระบุปัญหาที่เกิดขึ้นในการดำเนินธุรกิจของบริษัท (RIL3) ($\bar{X}$= 3.88, S.D.= 1.25) รวมถึงความเสี่ยงจากการขาดการใช้ข้อมูลรายงานทางบัญชีในการระบุปัญหาที่เกิดขึ้น ซึ่งส่งผลต่อการดำเนินธุรกิจของบริษัท (RII3) ($\bar{X}$= 3.70, S.D.= 1.34) และมีความเสี่ยงจากการขาดการวิเคราะห์และพัฒนาแนวทางการแก้ไขปัญหาซึ่งมักส่งผลต่อการใช้งานระบบปฏิบัติการต่างรุ่นในบริษัท (RAI3) ($\bar{X}$= 3.68, S.D.= 1.37)

2.2 ผลกระทบของความเสี่ยง: ระดับผลกระทบของการขาดการประเมินความเสี่ยงส่งผลกระทบต่อการใช้อุปกรณ์สำรองข้อมูลที่ไม่ถูกต้อง (REI3) และ ระดับผลกระทบของการขาดการประเมินความเสี่ยงในการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์แวดล้อมของพนักงานที่ส่งผลต่อการดำเนินธุรกิจ (REI4) ($\bar{X}$= 3.73, S.D.= 1.36 และ ($\bar{X}$= 3.70, S.D.= 1.32)

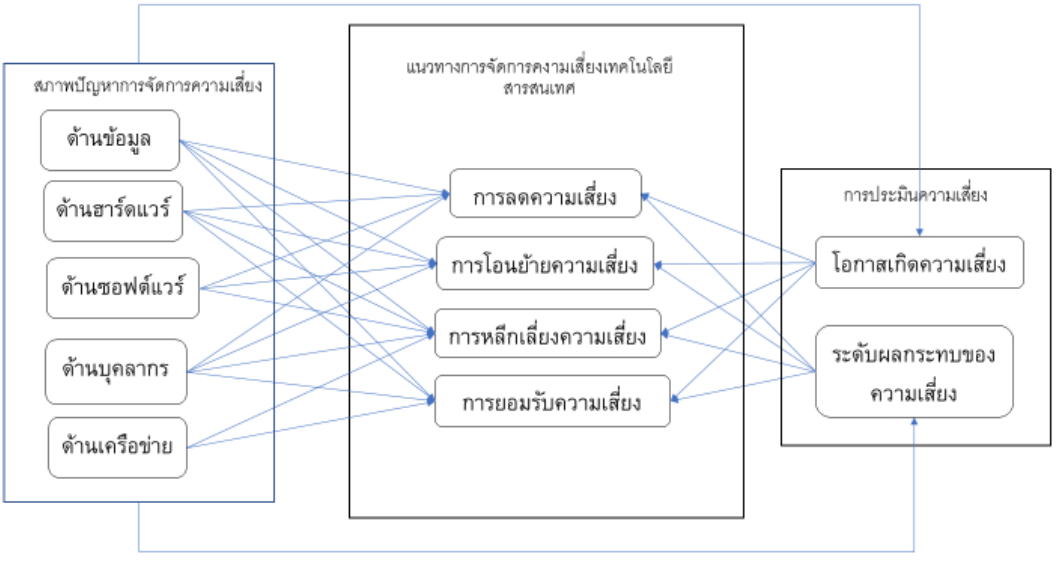
(3) แนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

ผู้ประกอบการส่วนใหญ่เห็นด้วยในระดับมากในการกำหนดแนวทางการจัดการความเสี่ยงใน 4 แนวทาง ก) การใช้กฎระเบียบบังคับพนักงานให้ใช้รหัสผ่านเข้าถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย (RRDT2) ($\bar{X}$= 4.11, S.D.= 1.13) ข) การออกคำสั่งห้ามพนักงานนำอุปกรณ์ส่วนตัวเชื่อมต่อกับระบบคอมพิวเตอร์ในบริษัท (RRDT1) ($\bar{X}$= 2.04, S.D.= 1.19) ค) การปรับปรุงแก้ไขอุปกรณ์คอมพิวเตอร์และเครือข่ายให้ปลอดภัยจากภัยคุกคามภายนอก (RA1) ($\bar{X}$= 4.18, S.D.= 0.99) และ ง) การติดตามข่าวสารทันสมัยด้านความก้าวหน้าของเทคโนโลยีสารสนเทศและนำมาปรับปรุงอุปกรณ์คอมพิวเตอร์และเครือข่ายของบริษัทให้ทันตามความก้าวหน้าดังกล่าว (RA2) ($\bar{X}$= 4.07, S.D.= 1.06)

(4) ผลการทดสอบสมมติฐาน

ผู้วิจัยได้ทดสอบ 92 สมมติฐานตามกรอบการวิจัยในรูปที่ 1 พบว่า ยอมรับ 73 สมมติฐาน และปฏิเสธ 19 สมมติฐาน ทำให้ได้โมเดลอิทธิพลของสภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศต่อโอกาสและผลกระทบของความเสี่ยงต่อการดำเนินธุรกิจ จำนวน 26 โมเดล และพบว่าสภาพปัญหาโอกาส และผลกระทบของความเสี่ยง มีความน่าจะเป็นที่จะส่งผลต่อแนวทางการจัดการความเสี่ยง

เทคโนโลยีสารสนเทศทั้ง 4 ด้าน คือ การลดความเสี่ยง การโอนย้ายความเสี่ยง การหลีกเลี่ยงความเสี่ยง และการคงไว้ซึ่งความเสี่ยง ได้โมเดลความน่าจะเป็นจำนวน 47 โมเดล ผู้วิจัยได้นำผลการทดสอบนี้พัฒนาเป็นแผนภาพดังรูปที่ 2



รูปที่ 2 เส้นทางอิทธิและความน่าจะเป็นของสภาพปัญหาการจัดการความเสี่ยงและการประเมินความเสี่ยงต่อแนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

จากรูปข้างต้น สรุปได้ว่าสภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศทั้ง 5 มิติ มีอิทธิพลต่อ โอกาสในการเกิดความเสี่ยงในทุกด้าน ที่โดดเด่นคือในด้านการไม่ทราบที่มาของปัญหาและสาเหตุที่ทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ตามปกติ (RIL1) การขาดการวิเคราะห์เพื่อพัฒนาแนวทางของระบบปฏิบัติการต่างรุ่น (RAL3) และการละเลยจากการประเมินความเสี่ยงการใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์แวดล้อม (REL4) นอกจากนี้ สภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศทั้ง 5 มิติ ยังมีอิทธิพลต่อผลกระทบจากความเสี่ยงในทุกด้านเช่นเดียวกัน โดยเฉพาะอย่างยิ่งในด้านการขาดการใช้รายงานทางบัญชีเพื่อระบุปัญหาของระบบสารสนเทศ (RII2) การไม่วิเคราะห์การใช้ข้อมูลบริษัทบนสื่อสังคมออนไลน์ (RAI4) และการไม่ทราบข้อมูลทันสมัยด้านเทคโนโลยีสารสนเทศทำให้บริษัทไม่สามารถปรับปรุงระบบให้ทันตามความก้าวหน้าของเทคโนโลยี (REI2)

ในรูปที่ 2 ยังแสดงให้เห็นถึงความน่าจะเป็นที่สภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ โอกาสเกิดความเสี่ยง และระดับผลกระทบของความเสี่ยง จะส่งผลต่อการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในทุกมิติ ยกเว้นสภาพปัญหาด้านซอฟต์แวร์และเครือข่ายที่มีความน่าจะเป็นต่อการจัดการความเสี่ยงเทคโนโลยีสารสนเทศไม่ครบทุกด้าน กล่าวคือ สภาพปัญหาด้านซอฟต์แวร์มีผลต่อการจัดการความเสี่ยงในด้านการลด โอนย้าย และหลีกเลี่ยงความเสี่ยง ส่วนสภาพปัญหาด้านเครือข่ายมีผลต่อการจัดการความเสี่ยงในด้านการหลีกเลี่ยงและการยอมรับความเสี่ยง

การอภิปรายผลการวิจัย

จากผลการทดสอบสมมติฐานดังกล่าว พบปัจจัยที่มีอิทธิพลและความน่าจะเป็นของเหตุการณ์ความเสี่ยงเทคโนโลยีสารสนเทศ ผู้วิจัยอภิปรายผลการทดสอบสมมติฐานโดยจำแนกเป็น 3 ส่วน ดังนี้

1) สภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

จากผลการทดสอบสมมติฐานชี้ให้เห็นว่า สภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ ส่งผลต่อโอกาสเกิดความเสี่ยงในด้าน ก) การดาวน์โหลดซอฟต์แวร์และระบบปฏิบัติการที่ผิดกฎหมายมาใช้ในระบบโดยไม่ได้รับอนุญาต (SP1) ซึ่งสอดคล้องกับงานวิจัยของ Shojaie, Federrath, & Saberi (2014) ที่ชี้ว่าองค์กรขนาดเล็กมักมีความเสี่ยงดังกล่าว และเป็นสาเหตุของความล้มเหลวด้านความมั่นคงปลอดภัยขององค์กร ข) ความเสี่ยงในด้านการควบคุมอย่างเข้มงวดในการใช้รหัสผ่านเพื่อเข้าถึงระบบสารสนเทศ (PP3) สอดคล้องกับวิจัยของธันวัฒน์ นามอ่อนตา, และวศิณ ชูประยูร (2561) ที่ระบุว่าการถูกโจมตีหรือติดไวรัสนั้นเกิดจากความไม่ตระหนักและไม่ใส่ใจจนมีผลกระทบต่อระบบข้อมูลเพียงเพราะการขาดความเข้มงวดการใช้รหัสผ่านที่เป็นระบบและปลอดภัย ค) การขาดการป้องกันการโจมตีข้อมูลจากไวรัสและมัลแวร์ (DP3) ข้อค้นพบนี้สอดคล้องกับงานวิจัยของ Cho, Chung, & Kuo (2016) ที่อธิบายว่าช่องโหว่และปัญหาต่างๆ เกิดจากความล้มเหลวของมนุษย์ที่ขาดความตระหนักถึงความเสี่ยงความมั่นคงปลอดภัย

นอกจากนี้ สภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศยังมีผลต่อผลกระทบความเสี่ยงเทคโนโลยีสารสนเทศในด้าน ก) การมีพื้นที่ไม่เพียงพอต่อการติดตั้งอุปกรณ์สำคัญสำหรับระบบ

สารสนเทศ (HP1) ซึ่งสอดคล้องกับงานวิจัยของ Javaid, & Iqbal (2017) ที่อธิบายว่าวิสาหกิจขนาดกลางและขนาดย่อมไม่สามารถจัดการความเสี่ยงได้เนื่องจากคลาดแคลนงบประมาณและทรัพยากรที่จำเป็นตามมาตรฐานการประเมินความเสี่ยง ISO/IEC 31000 ข) การขาดการควบคุมป้องกันบุคคลภายนอกเข้าถึงเครือข่าย (NP2) สอดคล้องกับงานวิจัยของ Bilbao, & Bilbao (2013) ที่อธิบายว่าการติดต่อมอบหมายผู้ให้บริการภายนอกดำเนินการแก้ไขระบบสารสนเทศต้องมีหลักเกณฑ์ควบคุมตามนโยบายองค์กร เพื่อลดความเสี่ยงและผลกระทบระบบทางเครือข่ายและทางกายภาพตามมาตรฐาน ISO/IEC 31000 และ ค) พนักงานไม่มีความรู้ความเข้าใจที่ถูกต้องเกี่ยวกับไวรัสและมัลแวร์ (PP1) สอดคล้องกับงานวิจัยของ Wu, Guo, Lin, & Li (2015) ที่ระบุว่าต้องอบรมให้ความรู้ความเข้าใจและติดตามประเมินผลด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศแก่พนักงาน

2) โอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงเทคโนโลยีสารสนเทศ

ผลการทดสอบสมมติฐานเผยให้เห็นว่าโอกาสเกิดความเสี่ยงเทคโนโลยีสารสนเทศมีความน่าจะเป็นที่จะส่งผลต่อแนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ อาทิ โอกาสในด้าน ก) การขาดการวิเคราะห์และพัฒนาแนวทางแก้ไขปัญหาการใช้งานระบบปฏิบัติการต่างรุ่น (RAL3) ข้อค้นพบนี้สอดคล้องกับผลการวิจัยของ Shojaie, Federrath, & Saberi (2014) ที่อธิบายว่าองค์กรต้องประเมินการใช้งานฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้องตามโครงสร้างขององค์กร และควบคุมการใช้งานระบบสารสนเทศ ข) การไม่ทราบที่มาของปัญหาและสาเหตุที่ทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ตามปกติ (RIL1) ซึ่งตรงกับผลการวิจัยของ King (2017) ที่ชี้ว่าองค์กรขนาดเล็กมักประสบกับโอกาสที่จะเกิดความเสี่ยงเช่นเดียวกันนี้ และเสนอแนะว่าองค์กรขนาดเล็กควรวิเคราะห์ ประเมิน และระบุความเสี่ยงภายนอกและภายในองค์กร เพื่อลดช่องว่างของความเสี่ยง ค) การขาดการประเมินความเสี่ยงในการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์แวดล้อมของพนักงานในบริษัท (REL4) ตรงกับข้อค้นพบของ Mahopo, Abdullah, & Mujinga (2015) ที่ระบุว่าในการบริหารความเสี่ยงองค์กรต้องวิเคราะห์ประสิทธิภาพควบคู่กับวิธีการปฏิบัติงาน จะทำให้พนักงานเข้าใจถึงกระบวนการปฏิบัติงาน และร่วมมือกันป้องกันปัญหาจากสภาพแวดล้อมที่จะส่งผลกระทบต่อการปฏิบัติงาน ง) การไม่ทราบข้อมูลข่าวสารทันสมัยด้านเทคโนโลยีสารสนเทศ ทำให้บริษัทไม่สามารถปรับปรุงระบบให้ทันตามความก้าวหน้า มีความเสี่ยงที่จะถูกโจมตี (REL2) สอดคล้องกับงานวิจัยของ Bilbao, & Bilbao (2013) ที่อธิบายว่าองค์กรต้องมีการระบุความเสี่ยงจากแหล่งข้อมูลข่าวสารภายนอก และวิเคราะห์ทรัพย์สินที่เกี่ยวข้อง เพื่อดูแนวโน้มของภัยคุกคาม รวมถึง

ตรวจสอบจำนวนครั้งที่เกิดความผิดพลาดเพื่อนำไปสู่การปรับปรุง จ) การขาดการประเมินความเสี่ยงในการใช้อุปกรณ์สำรองข้อมูลที่ถูกต้อง (REL3) สอดคล้องกับข้อค้นพบจากงานวิจัยของ King (2017) ที่ระบุว่าองค์กรขนาดเล็กต้องประเมินความเสี่ยงเกี่ยวกับระบบข้อมูลให้มีความพร้อมใช้ และถูกต้องตลอดเวลา เพราะมีข้อมูลการเงินจำนวนมาก ดังนั้นจึงต้องมีกลไกปกป้องชัดเจนเพื่อลดความเสียหาย และ ฉ) การขาดการประเมินความเสี่ยงจากความผิดพลาดของพนักงานที่ปฏิบัติการบนระบบเครือข่ายบริษัท (REL5) สอดคล้องกับงานวิจัยของชัยญามล เลิศสงคราม (2552) ที่ว่าความผิดพลาดเกิดจากการขาดความรู้ความเข้าใจของพนักงาน เพราะฉะนั้นองค์กรจึงควรกำหนดนโยบายการเข้าถึงเครือข่ายจากบุคคลภายในและภายนอก รวมทั้งจัดการความเสี่ยงการเข้าออกห้องควบคุมระบบเครือข่ายตามมาตรฐานการปฏิบัติงาน สอดคล้องกับนโยบายและกฎหมายที่เกี่ยวข้อง

นอกจากนี้ การทดสอบสมมติฐานยังชี้ให้เห็นว่า ผลกระทบความเสี่ยงเทคโนโลยีสารสนเทศมีความน่าจะเป็นที่จะส่งผลต่อแนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ ได้แก่ ก) การขาดการประเมินความเสี่ยงจากการใช้งานคอมพิวเตอร์และอุปกรณ์แวดล้อมของผู้ปฏิบัติงานส่งผลกระทบต่อการดำเนินธุรกิจ (REI4) สอดคล้องกับผลการวิจัยของ Wijanarka (2014) ที่ว่าแนวทางการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศต้องมีการวางแผน ตรวจสอบและประเมินสภาพแวดล้อมของกระบวนการปฏิบัติงานเพื่อลดความเสี่ยงที่มีโอกาสเกิดและผลกระทบต่อการสนับสนุนด้านสารสนเทศ ข) การขาดการวิเคราะห์ถึงปัญหาส่งผลกระทบต่ออุปกรณ์คอมพิวเตอร์และเครือข่ายทำให้เกิดการประมวลผลล่าช้าและผิดพลาด (RAI2) ตรงกับข้อค้นพบในงานวิจัยของ Cho, Chung, & Kuo (2016) ที่ชี้ว่าการวิเคราะห์ปัญหาและปฏิบัติตามมาตรฐานการบังคับควบคุมดูแลด้านความปลอดภัยไซเบอร์ และความผิดพลาดของผู้ปฏิบัติงานส่งผลต่อการประมวลผลข้อมูลระบบในสารสนเทศ ค) การขาดการศึกษาวิเคราะห์ปัญหาการใช้ข้อมูลบนสื่อสังคมออนไลน์ (RAI4) สอดคล้องกับข้อค้นพบของชัยญามล เลิศสงคราม (2552) ที่ว่าต้องไม่ละเลยที่จะตรวจสอบความมั่นคงปลอดภัยในการใช้ข้อมูลจากเว็บไซต์ต่างๆ รวมทั้งต้องระมัดระวังในการโพสต์ข้อความบนสื่อสังคมออนไลน์ เพราะอาจส่งผลกระทบต่อภาพลักษณ์องค์กร ง) การขาดการวิเคราะห์พัฒนาแนวทางการแก้ไขปัญหาที่มีผลกระทบต่อการใช้งานระบบปฏิบัติการต่างรุ่นในองค์กร (RAI3) ซึ่งมีผลต่อความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับงานวิจัยของ Smet, & Mayer (2016) ที่อธิบายว่าการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต้องมีการตัดสินใจลงทุนเปลี่ยนแปลงเทคโนโลยี

สารสนเทศให้ทันสมัยและมีความมั่นคงปลอดภัย จ) การไม่ทราบที่มาของปัญหาและสาเหตุที่ส่งผลกระทบต่อการไม่สามารถใช้งานระบบสารสนเทศได้ตามปกติ (RII1) สอดคล้องกับงานวิจัยของลภัสวัฒน์ ศุภผลกุลนันทร์ (2559) ที่ระบุว่าปัญหาส่วนใหญ่ของผู้ประกอบการและผู้ปฏิบัติงานคือการขาดองค์กรความรู้การแก้ไขปัญหาระบบสารสนเทศรวมถึงการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สามารถใช้งานได้อย่างถูกต้องและมีประสิทธิภาพ ฉ) การขาดใช้ข้อมูลรายงานทางบัญชีในการระบุปัญหาและสาเหตุที่เกิดขึ้นส่งผลกระทบต่อการดำเนินธุรกิจ (RII3) ซึ่งสอดคล้องกับงานวิจัยของ Shojaie, Federrath, & Saberi (2014) ที่อธิบายเพิ่มเติมว่าการค้นหาสาเหตุความเสี่ยงเทคโนโลยีสารสนเทศจะต้องวิเคราะห์ข้อมูลจากรายงานหรือตัวเลขต่างๆ

3) แนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

จากผลการทดสอบสมมติฐานยังพบอีกว่ามีสภาพปัญหาความเสี่ยงเทคโนโลยีสารสนเทศหลายด้านมี ความน่าจะเป็นที่จะส่งผลต่อแนวทางการจัดการเหตุการณ์ความเสี่ยงเทคโนโลยีสารสนเทศได้แก่ปัญหาเกี่ยวกับ ก) การเข้มงวดผู้ปฏิบัติงานในการจัดการสิทธิการเข้าถึงข้อมูล (DP2) สอดคล้องกับวิจัยของ Smet, & Mayer (2016) ที่ชี้ว่าองค์กรต้องจัดการความเสี่ยงแบบบูรณาการ เพื่อให้ปฏิบัติตามกฎระเบียบว่าด้วยการจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ข) การละเลยในการตรวจสอบความพร้อมใช้งานของอุปกรณ์อย่างสม่ำเสมอ (HP2) สอดคล้องกับข้อค้นพบของ Wijanarka (2014) ที่ระบุว่าองค์กรต้องสนับสนุนให้ความสำคัญต่อการบำรุงรักษาระบบสารสนเทศเพื่อลดผลกระทบเชิงลบของเหตุการณ์ภัยคุกคามที่สามารถหลีกเลี่ยงได้โดยใช้วงจร PDCA ตามมาตรฐาน ISO/IEC 31000 ค) พนักงานไม่มีความรู้ความเข้าใจที่ถูกต้องเกี่ยวกับไวรัสและมัลแวร์ (PP1) ตรงกับงานวิจัยของจิตตกานต์ บุญศิริทิวัตถ์, และโกวิท รพีพิศาล (2560) ที่อธิบายว่าการหลีกเลี่ยงความเสี่ยงที่ดีคือการอบรมผู้ที่เกี่ยวข้องให้ความรู้เพื่อให้สามารถใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพ ง) การสำรองข้อมูลผิดพลาดจากผู้ปฏิบัติงานใช้ขั้นตอนวิธีการที่ไม่ถูกต้อง (DP1) ตรงกับข้อค้นพบของ Williams (2014) ที่ชี้ว่ามาตรฐานและข้อกำหนดต่างๆ ใน ISO/IEC 27001:2013 เป็นแนวทางควบคุมผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยข้อมูลในการลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ จ) การขาดความต่อเนื่องในการ อัปเดตระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องกับการปฏิบัติงาน (SP2) สอดคล้องกับวิจัยของ Javaid, & Iqbal (2017) ที่ชี้ว่าความเสี่ยงส่วนใหญ่เกิดจากความผิดพลาดของระบบและอุปกรณ์ที่มีช่องโหว่ส่งผลให้แฮกเกอร์สามารถโจมตีได้โดยง่าย ดังนั้น องค์กรจึงควรใช้แนวทางการจัดการความเสี่ยงตามมาตรฐาน ISO/IEC

31000 โดยประยุกต์ใช้กับการเปลี่ยนแปลงภัยคุกคาม ฉ) การควบคุมเข้มงวดในการใช้รหัสผ่านเข้าถึงระบบสารสนเทศ (PP3) สอดคล้องกับข้อค้นพบของ Wu, Guo, Lin, & Li (2015) ที่อธิบายว่าข้อมูลเป็นทรัพย์สินเชิงพาณิชย์ต้องมีการควบคุมการเข้าถึงข้อมูลในระบบสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ว่าด้วยการรักษาความมั่นคงปลอดภัยข้อมูล ช) การจัดอบรมให้ความรู้การใช้งานอุปกรณ์คอมพิวเตอร์อย่างถูกต้องปลอดภัย (PP4) ตรงกับผลการวิจัยของ Ernawati, Suhardi, & Nugroho (2012) ที่ชี้ว่าการแก้ไขปัญหาของความไม่แน่นอนทั่วไปในการปฏิบัติงานควรพิจารณาปัจจัยด้านความสามารถของมนุษย์และทำการปรับปรุงเพิ่มประสิทธิภาพขององค์กรตามกระบวนการ ISO/IEC 31000 ซ) การขาดการอัปเดตปรับปรุงรุ่นซอฟต์แวร์ป้องกันไวรัสและมัลแวร์อย่างสม่ำเสมอ (SP3) สอดคล้องกับงานวิจัยของวรัญญาภรณ์ สิริพิพัฒนพร, และสมชาย นำประเสริฐชัย (2558) ที่ว่าองค์กรควรนำมาตรฐาน ISO/IEC 27001:2013 มาปรับใช้เพื่อลดความเสี่ยง ปรับปรุงข้อผิดพลาด หรือช่องโหว่จากซอฟต์แวร์ ฌ) ความต่อเนื่องในการอัปเดตปรับปรุงโปรแกรมของฮาร์ดแวร์ (HP4) ตรงกับงานวิจัยของวีรคุปต์ คงเจริญ (2558) ที่ว่าการป้องกันและการปรับปรุงระบบอย่างต่อเนื่องเป็นกรอบบริหารความเสี่ยงระดับกลยุทธ์ เพื่อจัดการความเสี่ยงภายในและภายนอกองค์กร เพื่อลดโอกาสที่จะเกิดและผลกระทบที่จะตามมา และเพื่อเป็นการปกป้องระบบสารสนเทศ ญ) การนำอุปกรณ์ส่วนตัวเชื่อมต่อระบบโดยไม่ตรวจสอบไวรัสและมัลแวร์ (HP3) สอดคล้องกับงานวิจัยของ Alebrahim, Hatebur, & Goeke (2014) ที่อธิบายว่าองค์กรควรวิเคราะห์เพื่อป้องกันความเสี่ยงจากภัยคุกคามการติดไวรัสและมัลแวร์ต่อทรัพย์สินที่เป็นข้อมูลในระบบตามมาตรฐาน ISO/IEC 27001:2013 และ ฎ) การละเลยในการตรวจสอบความพร้อมใช้งานของอุปกรณ์อย่างสม่ำเสมอ (HP2) สอดคล้องกับงานวิจัยของ Talib, Khelifi, & Ugurlu (2012) ที่ระบุว่าองค์กรควรตรวจสอบทั้งภายในและภายนอกในเชิงลึกเกี่ยวกับกระบวนการและความพร้อมใช้ของเทคโนโลยีสารสนเทศให้มีการพัฒนาต่อเนื่องอย่างมีประสิทธิภาพ จากข้อค้นพบข้างต้นสามารถสรุปได้ว่า ทรัพยากรมนุษย์มีความน่าจะเป็นที่จะส่งผลต่อแนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศของผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อมในอำเภอหนองแค จังหวัดสระบุรี ซึ่งผู้ประกอบการควรเร่งปรับปรุงระบบสารสนเทศให้มีความถูกต้อง ทันสมัย และพร้อมใช้ ชี้ให้พนักงานได้ตระหนัก รับรู้ มีความรู้ความเข้าใจ เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และร่วมกันพัฒนาแนวทางที่ดีที่สุดในการจัดการความเสี่ยงดังกล่าว

เอกสารอ้างอิง

กรมโรงงานอุตสาหกรรม. (2560). *ข้อมูลโรงงานแยกตามพื้นที่.* สืบค้น 31 ตุลาคม 2560, จาก http://www2.diw.go.th/factory/ tumbol.asp.

จิตตกานต์ บุญศิริทิวัตถ์, และโกวิท รพีพิศาล. (2560). การพัฒนาแนวทางในการจัดการความมั่นคงความปลอดภัยระบบสารสนเทศ ที่เหมาะสมของโรงพยาบาลเอกชนในกรุงเทพมหานคร. *วารสารรังสิตสารสนเทศ,* 23 (1). สืบค้น 31 ตุลาคม 2560, จาก http://library.rsu.ac.th/journal/ journal/31/article/108.

ชัยญามล เลิศสงคราม. (2552). *การศึกษาและการจัดการแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารด้วยมาตรฐาน ISO/IEC 27001: กรณีศึกษามหาวิทยาลัยราชภัฏสวนดุสิต* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์.

ธันวัฒน์ นามอ่อนตา, และวศิณ ชูประยูร. (2561). ตัวแบบการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย. *วารสารรังสิตสารสนเทศ, 24*(1). สืบค้น 31 ตุลาคม 2560, จาก http://library.rsu. ac.th/journal/ journal/33/article/122.

ลภัสวัฒน์ ศุภผลกุลนันทร์. (2559). การจัดการเทคโนโลยีสารสนเทศของธุรกิจขนาดกลางและขนาดย่อมกับการเข้าสู่ประชาคมอาเซียน: หลักฐานเชิงประจักษ์จากกลุ่มธุรกิจอุตสาหกรรมในภาคใต้ของประเทศไทย. *วารสาร RMUTL Journal of Humanities and Social Sciences. 4*(2). สืบค้น 31 ตุลาคม 2560, จาก http://tci- thaijo.orgindex. phpbalajhssarticleview7551360831.

วรัญญาภรณ์ สิริพิพัฒนพร, และสมชาย นำประเสริฐชัย. (2558) การวิเคราะห์และแนวทางจัดการ ความเสี่ยงด้านไอทีของหน่วยงานภาครัฐ. *วิศวกรรมสาร มก*, *28*(93). สืบค้น 31 ตุลาคม 2560, จาก https://www.tci-thaijo.org/index.php/kuengj/article/view/79154.

วีรคุปต์ คงเจริญ. (2558). *การนำมาตรฐาน ITIL v.3 มาประยุกต์ใช้ในการบริหารจัดการการให้บริการด้านเทคโนโลยีสารสนเทศ* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพฯ: มหาวิทยาลัยเทคโนโลยีมหานคร.

Alebrahim, A., Hatebur, D., & Goeke, L. (2014). Pattern-based and ISO 27001 compliant risk analysis for cloud systems. In *IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)* (pp.42-47). Retrieved November 17, 2017, from https://www.uni-due.de/imperia/md/content/swe/papers/2014espre.pdf.

Bilbao, A., & Bilbao, E. (2013). Measuring security. In *2013 47th International Carnahan Conference on Security Technology (ICCST)* (pp.1-5). Medellin, Colombia: IEEE. doi: 10.1109/CCST.2013. 6922054

Cho, C. S., Chung, W. H., & Kuo, S. Y. (2016). Cyberphysical security and dependability analysis of digital control systems in nuclear power plants. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 46*(3), 356-369. doi:10.1109/TSMC .2015.2452897.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika,* 16(3), 297-334.

Ernawati, T., Suhardi, D., & Nugroho. R (2012). IT risk management framework based on ISO 31000:2009. In *2012 International Conference on System Engineering and Technology (ICSET)* (pp.1-8). Bandung : IEEE. doi: 10.1109/ICSEngT.2012.6339352

International Organization for Standardization and International Electrotechnical Commission [ISO/IEC]. (2013). *International standard ISO/IEC27001: Information technology—security techniques—information security management systems—Requirements* (2nd ed). Geneva, Switzerland : ISO copyright office.

Javaid, M. I. & Iqbal, M. M. W. (2017). A comprehensive people process and technology (PPT) application model for information system (IS) risk management in small medium enterprises (SME). In *2017 International Conference on Communication Technologies (ComTech)* (pp.78-90). Rawalpindi, Pakistan : IEEE. doi: 10.1109/COMTECH.2017.8065754.

King, K. E. (2017). *Examine the relationship between information technology governance, control objectives for information and related technologies, ISO 27001/27002, and risk management* (Doctoral Dissertation). Retrieved from ProQuest Dissertations and Theses database. (ProQuest No. 10256918)

Likert, R. (1932). A technique for measurement of attitudes. *Archives of Psychology*, 140, 5-55.

Mahopo, B., Abdullah, H., & Mujinga, M. (2015). A formal qualitative risk management approach for IT security. Paper presented at the *2015 Information Security for South Africa (ISSA)*. Retrieved November 17, 2017, from https://www.researchgate.net/ publication/308734082_A_formal_qualitative_isk_management_approach_for_IT_sec urity. doi: 10.1109/ISSA.2015.7335053

Shojaie, B., Federrath, H., & Saberi, I. (2014). Evaluating the effectiveness of ISO 27001: 2013 based on annex A. *Workshop on Frontiers in Availability, Reliability and Security (FARES 2014)*. Organized by University of Fribourg of Swizerland. Retrieved November 17, 2017, from https://svs.informatik.uni-hamburg.de/ publications/2014/ ShFS 2014 -Annex-A-Paper-FARES2014.pdf

Smet, D. D., & Mayer, N. (2016). Integration of it governance and security risk management: A systematic literature review. *In the 2016 International Conference on Information Society (i-Society)* (pp. 143-148). doi: 10.1109/i-Society.2016.7854200

Talib, M. A., Khelifi, A., & Ugurlu, T. (2012). Using ISO 27001 in teaching information security. *IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society*, Montreal, QC, 2012 (pp. 3149-3153). doi: 10.1109/IECON.2012.6389 395

Wijanarka, H. (2014). IT risk management to support the realization of IT value in public organizations. *2014 International Conference on ICT For Smart Society (ICISS)* (pp.113-117). Bandung,Indonesia : IEEE. doi: 10.1109/ICTSS.2014.

Williams, K. L. (2014). *Cyber security governance - a view of selected organizations within the U.S. Department of Defense* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3634751).

Wu, S. M., Guo, D., Lin, W. T., & Li, M.-H. (2015). Web-based analytic hierarchy process (AHP) assessment model for information security policy of commercial banks. *Proceedings of BESSH-2015, 24*(3), 13-18. Retrieved November 17, 2017, from http://www. academicfora .com/wp-content/uploads-2016/01/BCS-1215/132.

Yamane, T. (1973). *Statistics: an introductory analysis.* New York: Harper & Row