การพัฒนาแผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย

A Development of Operational Plan on Information Technology Risk Management, Directorate of Joint Communication, Royal Thai Armed Forces Headquarters

บทความวิจัย

ชาญชัย ประมูลเฉโก[1] และ วศิณ ชูประยูร[2]
Chanchai Pramoolchego and Vasin Chooprayoon
สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยรังสิต จ.ปทุมธานี ประเทศไทย 12000
Program in Management of Information Technology, Graduate School, Rangsit University, Pathumthani, Thailand 12000
E-mail: chanchai.pr.rtarf@gmail.com[1] and E-mail: vasin@rsu.ac.th[2]

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาความคิดเห็นของกำลังพลกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย เกี่ยวกับกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ 2) พัฒนา (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร และ 3) พิจารณา (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร การวิจัยครั้งนี้เป็นการวิจัยทั้งเชิงปริมาณและคุณภาพ ใช้กรอบมาตรฐาน ISO/IEC 27001: 2013 เป็นทฤษฎีหลักในการออกแบบการวิจัย ใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างที่เป็นกำลังพลทั่วไป จำนวน 321 คน ได้แบบสอบถามกลับคืนครบ (ร้อยละ 100)

---

[1] นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมเทคโนโลยีดิจิทัล มหาวิทยาลัยรังสิต
Student of Master of Science in Information Technology Management, College of Digital Innovation Technology Rangsit University

[2] อาจารย์ที่ปรึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมเทคโนโลยีดิจิทัล มหาวิทยาลัยรังสิต
Assistant Professor Master of Science in Information Technology Management, College of Digital Innovation Technology Rangsit University

วันที่รับบทความ: 14 ต.ค.64 วันที่แก้ไขบทความ: 8 พ.ย.64 วันที่ตอบรับบทความ: 16 พ.ย.64

และใช้แบบสัมภาษณ์เป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากฝ่ายบริหาร และฝ่ายอำนวยการของกรมการสื่อสารทหาร จำนวน 5 คน สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ 1) สถิติเชิงพรรณนา (ร้อยละ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน) และ 2) การวิเคราะห์การถดถอยเชิงเส้นแบบพหุ ส่วนกระบวนการวิเคราะห์ข้อมูลจากการสัมภาษณ์นำข้อมูลมาวิเคราะห์เปรียบเทียบเพื่อจำแนกความคิดเห็นต่างและความคิดเห็นเหมือนในแต่ละประเด็น ผลการวิจัยพบว่า กำลังพลส่วนใหญ่มีความต้องการมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในระดับมาก เช่นเดียวกันกับผลการทดสอบสมมติฐานพบว่า ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีอิทธิพลต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศที่ขนาดอิทธิพล (R2) อยู่ระหว่าง 0.491-0.933 และมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในบริบทปัจจุบัน มีอิทธิพลต่อความต้องการแผนความเสี่ยงเทคโนโลยีสารสนเทศที่ขนาดอิทธิพล (R2) อยู่ระหว่าง 0.195-0.933 ทำให้ได้สมการอิทธิพล จำนวน 28 สมการ ผลจากการทดสอบสมมติฐานดังกล่าว คือ สารสนเทศที่เป็นข้อมูลขั้นต้นในการพัฒนาเป็น (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย จากนั้นนำเข้าสู่กระบวนการสนทนากลุ่มเพื่อให้ผู้ทรงคุณวุฒิพิจารณาให้ความเห็นชอบโดย (ร่าง) แผนฯ ดังกล่าว ได้ผ่านการพิจารณาเห็นชอบจากผู้ทรงคุณวุฒิของกรมการสื่อสารทหาร จำนวน 11 คน

คำสำคัญ: การบริหารความเสี่ยงเทคโนโลยีสารสนเทศ, แผนปฏิบัติการความเสี่ยงเทคโนโลยีสารสนเทศ, กองบัญชาการกองทัพไทย

Abstract

The objectives of this research were 1) to study the opinions of the personnel of the Directorate of Joint Communications on the information technology risk management process, 2) to develop a draft action plan for the information technology risk management process, and 3) to consider the draft of "The Action Plan for Managing Information Technology Risks" of the Directorate of Joint Communications. This research used both quantitative and qualitative research approaches. The main theory in research design is the ISO/IEC 27001:2013 standard framework. Three hundred and twenty-one personnel who are the research respondents completed and returned the questionnaires (100.00%). In terms of the qualitative approach, the semi-structured interview was used to gather information from five executives, including the Director of the Directorate of Joint Communications. The statistics used in the empirical data analysis were 1) descriptive (percentage, mean, and standard deviation) and 2) multiple linear regression analysis. The authors comparatively analyzed the interviewers' qualitative data and classified the opinions on each issue into 2 groups; similar opinions and different opinions. The study revealed that most of the respondents need a high level of information security managerial measures. The hypothesis test found that the

management system of information security has influenced information security managerial measures with the effect size (R2) between 0.491-0.933. Moreover, the information security managerial measures in the current context have affected the need for information technology risk plans with the effect size (R2) between 0.195-0.933. The hypothesis test also generated 28 influence equations. The research findings become the primary information for developing the draft of action plan for the information technology risk management process of the Directorate of Joint Communications, Royal Thai Armed Forces Headquarters. Then the information will be taken into consideration by the experts in a discussion group to get an approval. However, the draft was already approved by 11 experts of the Directorate of Joint Communications.

Keywords: IT Risk Management, IT Risk Action Plan, Royal Thai Armed Forces Headquarters

ความเป็นมาและความสำคัญของปัญหา

กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย (สส.ทหาร) ได้อนุวัตระบบสารสนเทศ/เทคโนโลยีสารสนเทศและที่เกี่ยวข้องมาตั้งแต่ก่อตั้ง สส.ทหาร เทคโนโลยีสารสนเทศและที่เกี่ยวข้องที่ สส.ทหาร ยังคงใช้อยู่ประกอบด้วย เทคโนโลยีสารสนเทศที่อำนวยอรรถประโยชน์ให้แก่ สส.ทหาร ในด้านการปฏิบัติงานทั่วไป การติดต่อสื่อสารและรับส่งข้อมูลทั้งภายในและภายนอก การบริหารงานภายใน การรับ-ส่งข่าวสาร การให้บริการเทคโนโลยีสารสนเทศให้แก่หน่วยขึ้นตรงต่าง ๆ ของกองบัญชาการกองทัพไทย รวมถึงเหล่าทัพต่าง ๆ การอำนวยความสะดวกในการปฏิบัติงานประจำวันของกำลังพลใน สส.ทหาร รวมถึงเป็นฝ่ายอำนวยการด้านวิทยาการให้แก่กองบัญชาการกองทัพไทย เพื่อพัฒนาสมรรถนะกำลังพลทุกระดับให้สามารถปฏิบัติงานโดยใช้เทคโนโลยีดังกล่าวในการเพิ่มพูนผลิตภาพ (Productivity) อย่างต่อเนื่อง

จากการทบทวนประวัติการอนุวัตเทคโนโลยีดังกล่าว รวมทั้งทบทวนเอกสารและงานวิจัยที่เกี่ยวข้องของ สส.ทหาร พบว่า มีการใช้เทคโนโลยีแบบสุ่มเสี่ยงให้เกิดความเสียหาย ขาดความมั่นคงปลอดภัย ไม่พัฒนาความตระหนักรู้และให้ความรู้แก่กำลังพลของ สส.ทหาร ในการใช้เทคโนโลยีสารสนเทศที่ถูกต้อง ปลอดภัย ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการปฏิบัติงานได้อย่างเต็มที่ อีกทั้งกำลังพลบางส่วนขาดความใส่ใจต่อเทคโนโลยีสารสนเทศที่นำมาใช้ ปัจจุบัน สส.ทหาร มีการจัดทำแผนปฏิบัติการเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทย พ.ศ.2562-2564 และแผนปฏิบัติการเทคโนโลยีสารสนเทศและการสื่อสาร กองบัญชาการกองทัพไทย พ.ศ.2562-2564 เพื่อช่วยในการพัฒนากำลังพล การพัฒนาโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล การพัฒนาและประยุกต์ใช้ระบบสารสนเทศ การปรับปรุงโครงสร้าง กฎ ระเบียบ คำสั่ง ให้รองรับการทำงานที่ใช้เทคโนโลยีดิจิทัล และความร่วมมือกับหน่วยงานอื่น แต่ที่สำคัญที่สุดก็คือ สส.ทหาร ยังไม่มีแผนงานอย่างเป็นทางการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้เทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย มีความมั่นคงปลอดภัย มีมาตรฐานในการปกป้องหน่วยงานจากความเสียหาย

ที่อาจเกิดขึ้นได้จากความเสี่ยง ดังนั้น เพื่อให้การดำเนินงานตามภารกิจของหน่วยงานบรรลุตามวัตถุประสงค์ ทั้งในมิติการป้องกันสินทรัพย์กายภาพของหน่วยงาน เทคโนโลยีสารสนเทศ รวมถึงการปกป้องงานตามภารกิจของหน่วยงานให้รอดพ้นจากความเสี่ยงที่เกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร จึงจำเป็นอย่างยิ่งที่องค์กรทั้งภาครัฐและเอกชนจะต้องตระหนักรู้ถึงการบริหารความเสี่ยงดังกล่าวอย่างจริงจังด้วยแนวปฏิบัติที่ดี (Best Practices) และเป็นมาตรฐานสากล

สส.ทหาร เป็นหน่วยงานความมั่นคงภาครัฐ มีพันธกิจสำคัญคือ การประสานแผนด้านสื่อสารอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศร่วมกับเหล่าทัพและส่วนราชการอื่น ๆ ที่เกี่ยวข้อง เพื่อสนับสนุนการปฏิบัติการทางทหาร การปฏิบัติการด้านการสื่อสารอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศ ระบบโทรคมนาคมทหาร การสงครามอิเล็กทรอนิกส์ การรักษาความปลอดภัยทางการสื่อสารและสารสนเทศ การสนับสนุนระบบการควบคุมบังคับบัญชาของกองทัพไทย รวมถึงการบริหารจัดการคลื่นความถี่ในกิจการโทรคมนาคมทหาร กิจการวิทยุกระจายเสียงและวิทยุโทรทัศน์ของกองทัพไทยเป็นหน่วยวิทยาการสายสื่อสารของกองบัญชาการกองทัพไทย และสนับสนุนการส่งกำลังบำรุงสิ่งอุปกรณ์สายสื่อสาร พันธกิจเหล่านี้ ล้วนปฏิบัติการบนฐานของระบบ Extranet และ Intranet ซึ่งมีอัตราความเสี่ยงที่จะถูกผู้ไม่ประสงค์ดีเข้ามาก่อการในลักษณะอาชญากรรมไซเบอร์ ทำให้ได้รับความเสียหายจากการถูกโจมตีด้วยไวรัสคอมพิวเตอร์ บุคลากรภายใน ระบบไฟฟ้า อัคคีภัย และปัจจัยอื่น ๆ ทั้งภายในและภายนอก ซึ่งล้วนส่งผลกระทบต่อการดำเนินงานของหน่วย ความเสี่ยงที่เกิดขึ้นอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม

ด้วยเหตุนี้ ผู้วิจัยจึงประสงค์จะค้นหาคำตอบในมุมมองความคิดเห็นของกำลังพล กรมการสื่อสารทหาร รวมถึงความคิดเห็นของฝ่ายบริหารและฝ่ายอำนวยการเกี่ยวกับมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในบริบทปัจจุบัน และความต้องการมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ ตามกรอบมาตรฐาน International Organization for Standardization and International Electrotehnical Commission (ISO/IEC, 2013) เพื่อนำคำตอบที่ได้ไปพัฒนาเป็น (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีของ สส.ทหาร อันจะส่งผลให้เกิดประโยชน์สูงสุดและลดความเสียหายที่จะเกิดขึ้นในอนาคตกับ สส.ทหาร

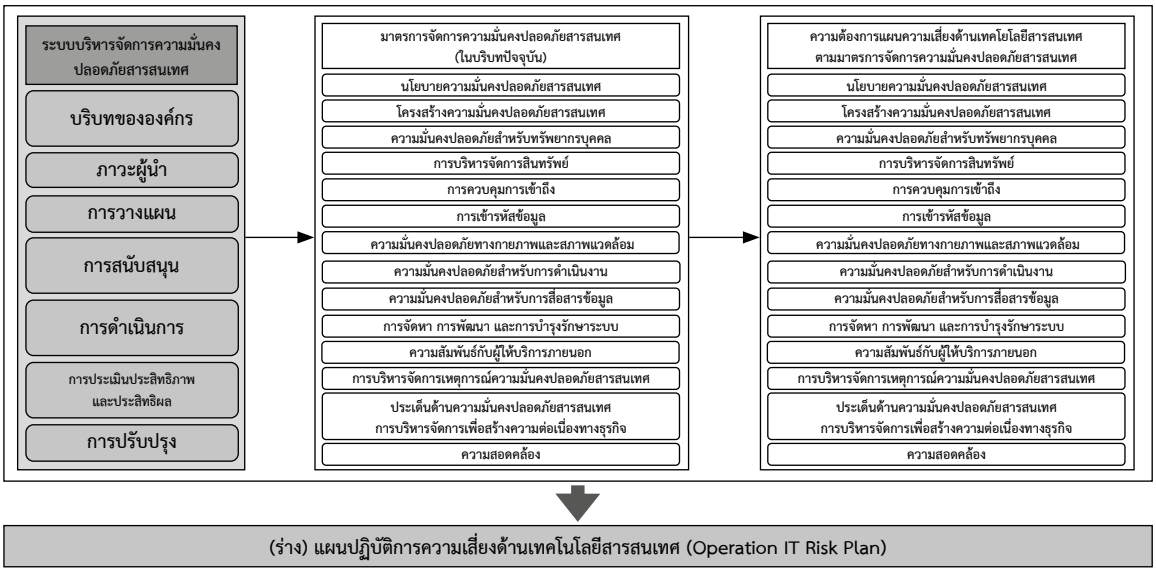
วัตถุประสงค์การวิจัย

การวิจัยนี้มีวัตถุประสงค์เพื่อ

1. ศึกษาความคิดเห็นของกำลังพล สส.ทหาร เกี่ยวกับกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2. พัฒนา (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย
3. พิจารณา (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย โดยผู้ทรงคุณวุฒิ สส.ทหาร จำนวน 11 ท่าน

กรอบการวิจัย

ผู้วิจัยได้พัฒนากรอบแนวคิดการวิจัยในครั้งนี้ด้วยการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องกับกรอบมาตรฐาน ISO/IEC 27001: 2013 ในส่วนที่เป็นระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ ได้กรอบการวิจัยดังภาพ



ภาพ กรอบแนวคิดการวิจัย

สมมติฐานการวิจัย

ประกอบด้วย 2 กลุ่มสมมติฐานหลัก จำนวนรวมทั้งสิ้น 28 สมมติฐาน จำแนกเป็น 2 กลุ่ม ดังนี้

สมมติฐานหลักกลุ่มที่ 1 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีอิทธิพลต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย 14 สมมติฐานย่อย

สมมติฐานหลักกลุ่มที่ 2 มาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในบริบทปัจจุบัน ของ สส.ทหาร มีอิทธิพลต่อความต้องการแผนความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประกอบด้วย 14 สมมติฐานย่อย

วิธีดำเนินการวิจัย

1. ประชากรและกลุ่มตัวอย่าง

การวิจัยครั้งนี้แบ่งประชากรและกลุ่มตัวอย่างในการวิจัยออกเป็น 2 กลุ่ม คือ กลุ่มของการรวบรวมข้อมูลในเชิงปริมาณ และกลุ่มของการรวบรวมข้อมูลในเชิงคุณภาพ

1.1 กลุ่มเชิงปริมาณ คือ กำลังพลของ สส.ทหาร ทุกหน่วยขึ้นตรง ทั้งในส่วนกลาง และส่วนภูมิภาคที่ผ่านกระบวนการคำนวณจากสูตรของเครซี่และมอร์แกน (Krejcie and Morgan, 1970) โดยกำหนดระดับความเชื่อมั่นที่ร้อยละ 95 และค่าความคลาดเคลื่อนที่ ร้อยละ ±5 โดยแทนค่าในสูตรของ Krejcie and Morgan

$$n = \frac{X^2\, Np\,(1\text{-}p)}{e^2(N\text{-}1) + X^2 p(1\text{-}p)}$$

เมื่อ n = ขนาดของกลุ่มตัวอย่าง

N = จำนวนประชากรทั้งหมด

e = ระดับความคลาดเคลื่อนของการสุ่มตัวอย่างที่ยอมรับได้เป็น 0.05 (ค่าความเชื่อมั่นที่ร้อยละ 95)

X^2 = ค่าไคสแควร์ที่ df เท่ากับ 1 และระดับความเชื่อมั่นร้อยละ 95 (X^2 = 3.841)

p = สัดส่วนของลักษณะที่สนใจในประชากร (ถ้าไม่ทราบให้กำหนด p = 0.5)

ทำการแทนค่า

โดยที่ N = 1,944 ในสูตรของ Krejcie and Morgan

$$n = \frac{3.841 \times 1,944 \times 0.5 \times 0.5}{(0.05)^2 \times (1,944 - 1) + 3.841 \times 0.5 \times 0.5}$$

n = 320.867 (ประมาณ 321 คน)

ค่าจำนวนกลุ่มตัวอย่างที่ได้จากการแทนค่าลงในสูตร คือ 320.867 (ประมาณ 321 คน) ซึ่งได้มาจากจำนวนกำลังพลของ สส.ทหาร จำนวน 1,944 คน สรุปได้ว่าผู้วิจัยต้องใช้กลุ่มตัวอย่างทั้งสิ้น 321 คน

1.2 กลุ่มเชิงคุณภาพ คือ

1.2.1 การสัมภาษณ์เชิงลึก ผู้บริหารระดับสูงและฝ่ายอำนวยการ สส.ทหาร จำนวน 5 คน ประกอบด้วย 1) เจ้ากรมการสื่อสารทหาร 2) รองเจ้ากรมการสื่อสารทหาร 3) ผู้อำนวยการสำนักแผนและอำนวยการสื่อสาร กรมการสื่อสารทหาร 4) ผู้อำนวยการศูนย์การโทรคมนาคมทหาร กรมการสื่อสารทหาร 5) ผู้อำนวยการกองแผนและวิศวกรรม ศูนย์การโทรคมนาคมทหาร

1.2.2 ผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ ผู้มีประสบการณ์เกี่ยวกับการบริหารความเสี่ยง จำนวน 11 คน ประกอบด้วย 1) รองเจ้ากรมการสื่อสารทหาร 2) ผู้แทนสำนักแผนและอำนวยการสื่อสาร 3) ผู้อำนวยการกองแผนและวิศวกรรม ศูนย์การโทรคมนาคมทหาร 4) ผู้อำนวยการกองแผนและวิศวกรรม ศูนย์เทคโนโลยีสารสนเทศทหาร 5) ผู้ช่วยผู้อำนวยการกองควบคุมระบบ ศูนย์การโทรคมนาคมทหาร 6) ผู้ช่วยผู้อำนวยการกองการโทรคมนาคมทหาร ศูนย์การโทรคมนาคมทหาร 7) หัวหน้าแผนกวิศวกรรมระบบกองแผนและวิศวกรรม ศูนย์การโทรคมนาคมทหาร 8) หัวหน้าแผนกควบคุมระบบ กองควบคุมระบบโทรคมนาคม ศูนย์การโทรคมนาคมทหาร 9) นายทหารวิเคราะห์และพัฒนาระบบ แผนกสารสนเทศและการสื่อสารข้อมูล กองควบคุมระบบโทรคมนาคม ศูนย์การโทรคมนาคมทหาร 10) นายทหารควบคุมระบบ แผนกควบคุมระบบ กองควบคุมระบบโทรคมนาคม ศูนย์การโทรคมนาคมทหาร 11) ผู้แทนกองพันทหารสื่อสาร กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย เข้าร่วมสนทนากลุ่ม (Focus Group) เพื่อพิจารณา (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือวิจัยประกอบด้วย 3 ลักษณะ คือ

1. แบบสอบถามเพื่อใช้สำรวจความคิดเห็นของกำลังพลของ สส.ทหาร ประกอบด้วย 4 ตอน คือ 1) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ สส.ทหาร ในบริบทปัจจุบัน 2) มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศของ สส.ทหาร ในบริบทปัจจุบัน 3) ความต้องการแผนความเสี่ยงด้านเทคโนโลยีสารสนเทศ สส.ทหาร และ 4) ภูมิหลังผู้ตอบแบบสอบถาม สส.ทหาร จำนวนรวมทั้งสิ้น 96 ข้อ โดยการแจกแบบสอบถามแบบออนไลน์

2. แบบสัมภาษณ์กึ่งโครงสร้าง เพื่อใช้บันทึกมุมมองของผู้บริหารระดับสูงและฝ่ายอำนวยการของ สส.ทหาร เกี่ยวกับสถานภาพการดำเนินงานตามแนวทางกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สส.ทหาร ในบริบทปัจจุบัน ความต้องการมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อนำไปสู่การพัฒนาเป็นแผนบริหารความเสี่ยงที่เหมาะสมกับ สส.ทหาร และความคิดเห็นอื่น ๆ เกี่ยวกับการดำเนินการจัดทำ (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร

3. แบบบันทึกการให้ความเห็นชอบ (ร่าง) แผนฯ เพื่อบันทึกความคิดเห็นเกี่ยวกับ (ร่าง) แผนฯ จากผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ ผู้มีประสบการณ์เกี่ยวกับการบริหารความเสี่ยง ในแบบบันทึกประกอบด้วยประเด็นของแผนปฏิบัติการความเสี่ยงจำนวน 14 แผนย่อย การให้ความเห็นชอบและข้อเสนอแนะเกี่ยวกับแผนปฏิบัติการความเสี่ยงในแต่ละแผนฯ

การตรวจสอบคุณภาพเครื่องมือการวิจัย

ผู้วิจัยได้ส่งเครื่องมือวิจัยประเภทที่ 1 ไปให้ผู้ทรงคุณวุฒิจำนวน 5 ท่าน ตรวจสอบความเที่ยง (Validity) ทั้งในเชิงโครงสร้างและเนื้อหา จากนั้นได้นำผลจากการตรวจของผู้ทรงคุณวุฒิมาคำนวณหาค่าดัชนีความเที่ยงตรงเชิงเนื้อหา (Content Validity Index: CVI) ได้ค่า CVI เท่ากับ 0.926 ซึ่งสามารถนำไปใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลภาคสนามได้ ส่วนเครื่องมือประเภทที่ 2 และ 3 ผู้วิจัยขอความอนุเคราะห์ผู้ทรงคุณวุฒิจากวิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต จำนวน 3 ท่าน ได้พิจารณาประเมินคุณภาพ ผลจากการประเมินบ่งชี้ว่าเป็นแบบเก็บข้อมูลเชิงคุณภาพที่มีศักยภาพ

การวิเคราะห์ข้อมูล

1. การวิเคราะห์ข้อมูลเชิงปริมาณ

1.1 สถิติเชิงพรรณนา ได้แก่ สถิติคำนวณค่าร้อยละ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน

1.2 สถิติอ้างอิง ได้แก่ การวิเคราะห์การถดถอยเชิงเส้นแบบพหุ (Multiple Linear Regression) ด้วยการตรวจสอบความสัมพันธ์ภายในตัวเองของข้อมูล (Autocorrelation) โดยพิจารณาค่า Durbin-Watson มีการตรวจสอบสภาวะร่วมของตัวแปรอิสระ (Multicollinearity) และตรวจสอบความคลาดเคลื่อนที่เกิดจากการพยากรณ์ โดยพิจารณาจากค่าสูงสุดและค่าต่ำสุดของค่า ZResidual ที่ตกอยู่ระหว่าง ±3 ทั้งยังตรวจสอบการแจกแจงของความเคลื่อนที่เกิดจากการพยากรณ์ และการตรวจสอบความแปรปรวนของความคลาดเคลื่อนโดยพิจารณาการกระจายของค่า ZResidual เหนือและใต้ระดับ 0.0 มีขนาดเท่ากันเป็นแนวสี่เหลี่ยมผืนผ้า พร้อมกันนี้ยังได้ตรวจสอบความสัมพันธ์เชิงเส้นระหว่างระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศกับมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) และมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) กับความต้องการมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้วยการวิเคราะห์ความแปรปรวนทางเดียว

2. การวิเคราะห์ข้อมูลเชิงคุณภาพ

2.1 ข้อมูลจากแบบสัมภาษณ์กึ่งโครงสร้าง ผู้วิจัยวิเคราะห์เปรียบเทียบความคิดเห็นของผู้บริหารระดับสูงและฝ่ายอำนวยการ สส.ทหาร ทั้ง 5 ท่าน จำแนกเป็นความคิดเห็นต่างและความคิดเห็นเหมือนในแต่ละประเด็น แล้วนำเสนอผลการวิเคราะห์เชิงเปรียบเทียบในรูปแบบการพรรณนาภาพรวม

2.2 ข้อมูลจากแบบบันทึกการให้ความเห็นชอบ (ร่าง) แผนฯ ผู้วิจัยได้จัดทำและแจกจ่าย (ร่าง) แผนฯ ให้กับผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ และผู้มีประสบการณ์ที่เกี่ยวข้องพิจารณาให้ความเห็นชอบ โดยได้นำความคิดเห็นและข้อเสนอแนะที่ได้รับจากผู้ทรงคุณวุฒิ มาปรับปรุงให้เป็น (ร่าง) แผนฯ ฉบับสมบูรณ์

ผลการวิจัย

ผู้วิจัยนำเสนอผลการวิจัยโดยจำแนกเป็น 2 แนวทาง ดังนี้

1. ผลการวิจัยเชิงปริมาณ มีข้อค้นพบที่น่าสนใจ ดังนี้

1.1 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ กำลังพลส่วนใหญ่ชี้ว่า สส.ทหาร มีการบริหารจัดการในระดับน้อยในประเด็นการสร้างความตระหนักเรื่องนโยบายความมั่นคงปลอดภัยสารสนเทศ และมีการบริหารจัดการในระดับน้อยที่สุดในการกำหนดแผนปฏิบัติเพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

1.2 มาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) กำลังพลส่วนใหญ่เห็นว่า สส.ทหาร มีมาตรการในการจัดการความมั่นคงปลอดภัยสารสนเทศในระดับน้อย และเห็นว่าการควบคุมการเข้าถึงในปัจจุบัน สส.ทหาร มีมาตรการในการจัดการในระดับมาก ส่วนการควบคุมการเข้าถึงเครือข่ายของผู้ใช้งาน (สิทธิในการเข้าถึง) นโยบายควบคุมการเข้าถึง การกำหนดสิทธิการเข้าถึงเป็นลายลักษณ์อักษร การควบคุมการเข้าถึงระบบด้วยขั้นตอนที่มีความมั่นคงปลอดภัย และการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน ด้วยการพิสูจน์ตัวตน มีมาตรการในการจัดการในระดับมากที่สุด

1.3 ความต้องการแผนความเสี่ยงด้านเทคโนโลยีสารสนเทศตามมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ ผลการวิจัยชี้ให้เห็นว่า กำลังพลส่วนใหญ่มีความต้องการในระดับมากที่สุด ประกอบด้วยประเด็นความต้องการให้องค์กร กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับวัตถุประสงค์ขององค์กร มีการกำหนดโครงสร้างภายในองค์กร บทบาทหน้าที่ความรับผิดชอบอย่างชัดเจน กำหนดพื้นที่ที่ต้องการ การรักษาความมั่นคงปลอดภัย โดยอนุญาตเฉพาะผู้ที่มีส่วนเกี่ยวข้องมีการบริหารจัดการความมั่นคงปลอดภัยของเครือข่ายเพื่อป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ และเตรียมการอุปกรณ์ประมวลผลสำรอง ให้มีความพร้อมใช้

1.4 ผลการทดสอบสมมติฐาน จำนวน 28 สมมติฐาน ด้วยการวิเคราะห์ถดถอยเชิงเส้นแบบพหุ พบว่า

1.4.1 การตรวจสอบความสัมพันธ์ภายในตัวเองของข้อมูล (Autocorrelation) ด้วยการพิจารณาค่า Durbin-Watson พบว่ามีค่าอยู่ระหว่าง 1.5-2.5 แสดงว่าข้อมูลไม่มีความสัมพันธ์ภายในตัวเองในทุกสมมติฐาน

1.4.2 การตรวจสอบสภาวะร่วมของตัวแปรอิสระ (Multicollinearity) พบว่า ตัวแปรอิสระในการทดสอบทั้ง 28 สมมติฐาน ไม่มีสภาวะร่วม พิจารณาจากค่าไอเก้น (Eigenvalue) ที่ไม่เข้าใกล้ศูนย์ และค่า Condition Index น้อย

1.4.3 การตรวจสอบความคลาดเคลื่อนที่เกิดจากการพยากรณ์ พบว่ามีความคลาดเคลื่อนในการพยากรณ์น้อย พิจารณาจากค่าสูงสุดและค่าต่ำสุดของค่า ZResidual ที่ตกอยู่ระหว่าง ±3 และค่าเฉลี่ยความคลาดเคลื่อนเท่ากับ 0.0

1.4.4 การตรวจสอบการแจกแจงของความคลาดเคลื่อนที่เกิดจากการพยากรณ์ พบว่ามีการแจกแจงปกติ พิจารณาจากค่าความน่าจะเป็นของข้อมูลเรียงเป็นแนวทแยงเส้นตรง

1.4.5 การตรวจความแปรปรวนของความคลาดเคลื่อนที่เกิดจากการพยากรณ์ พบว่ามีความแปรปรวนคงที่ทั้ง 28 สมมติฐาน พิจารณาจากการกระจายของค่า ZResidual เหนือ และใต้ระดับ 0.0 มีขนาดเท่ากัน เป็นแนวสี่เหลี่ยมผืนผ้า

1.4.6 การตรวจสอบความสัมพันธ์เชิงเส้นระหว่างระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศกับมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) และมาตรการจัดการความมั่นคง

ปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) กับความต้องการมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้วยการวิเคราะห์ความแปรปรวนทางเดียว (One-Way ANOVA) พบว่า มีความสัมพันธ์กันเชิงเส้นตรง อย่างมีนัยสำคัญทางสถิติที่ 0.05

ผลการทดสอบสมมติฐาน ทำให้ได้ (ก) สมการอิทธิพลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในบริบทปัจจุบัน จำนวน 14 สมการ มีขนาดอิทธิพลระหว่างร้อยละ 49.1-93.3 และ (ข) สมการอิทธิพลของมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในบริบทปัจจุบัน ต่อความต้องการแผนความเสี่ยงเทคโนโลยีสารสนเทศ จำนวน 14 สมการ มีขนาดอิทธิพลระหว่างร้อยละ 19.5-93.3 ผู้วิจัยได้นำตัวแปรที่ปรากฏในสมการไปพัฒนาเป็นประเด็นในการ (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สส.ทหาร ตัวอย่างตัวแปรที่โดดเด่นจากสมการที่นำไปพัฒนาเป็นร่างแผนฯ ได้แก่ ตัวแปรการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ความเข้าใจองค์กรและบริบทที่เกี่ยวข้อง และการสนับสนุนทรัพยากรที่จำเป็น ยังมีตัวแปรความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคลทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และหลังจากจ้างงาน ตัวแปรการกำหนดทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และการบริหารจัดการการเข้าถึงของผู้ใช้งาน รวมถึงการป้องกันโปรแกรมไม่ประสงค์ดี และการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย

2. ผลการวิจัยเชิงคุณภาพ มีข้อค้นพบ ดังนี้

2.1 ผลการสัมภาษณ์กึ่งโครงสร้างพบว่า ผู้บริหารระดับสูง และฝ่ายอำนวยการ สส.ทหาร สะท้อนมุมมองเกี่ยวกับกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

2.1.1 สส.ทหาร เตรียมความพร้อมที่จะดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดตั้งศูนย์คอมพิวเตอร์สำรอง และให้สามารถกู้คืนข้อมูลให้กลับมาใช้งานได้ภายใน 24 ชั่วโมง หากเกิดการโจมตี และได้เตรียมพร้อมด้านกำลังพลให้มีความรู้ในเรื่องสารสนเทศ หรือเรื่องที่เกี่ยวข้องผ่านหลักสูตรต่าง ๆ ทั้งหลักสูตรตามแนวทางรับราชการ หลักสูตรเพิ่มพูนความรู้จากภายนอก หรือส่งเสริมให้ได้เข้ารับการศึกษาจากสถานศึกษานอกกระทรวงกลาโหม

2.1.2 ผู้บัญชาการทหารสูงสุดได้มอบนโยบายเกี่ยวกับมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ โดยแต่งตั้งคณะทำงานรับผิดชอบ มีผู้บัญชาการทหารสูงสุด เป็น CEO (Chief Executive Officer) และรองหัวหน้าส่วนราชการเป็น CIO (Chief Information Officer) ของหน่วย และมี CISO (Chief Information Security Officer) รับผิดชอบการบริหารจัดการข้อมูล เจ้ากรมการสื่อสารทหารเป็นผู้รับผิดชอบ จัดหาสารสนเทศ กำหนดให้คณะกรรมการเทคโนโลยีสารสนเทศ (คณะกรรมการ ICT) เป็นผู้พิจารณา และส่งผลการพิจารณาให้กับเสนาธิการทหาร

2.1.3 สส.ทหาร มีอุปกรณ์ Fire Wall เป็นอุปกรณ์ป้องกันภัยคุกคามในขั้นต้น กำหนดให้กำลังพลทุกคนต้องมีการพิสูจน์ตัวตน (Authentication) ก่อนเข้าใช้งานทุกครั้ง มีอุปกรณ์บันทึกการเข้าใช้งาน (Log file) ตลอดเวลา กำหนดให้แบ่งพื้นที่เป็นเขตหวงห้ามเด็ดขาด และเขตหวงห้ามเฉพาะ ในพื้นที่ที่มีเครื่องมือติดตั้ง กำหนดสิทธิ์ในการเข้าถึงเฉพาะบุคคลที่มีส่วนเกี่ยวข้องหรือรับผิดชอบโดยตรงเท่านั้น มีการกำหนดพื้นที่ที่ต้องควบคุมการเข้า-ออก เฝ้าระวังติดตาม (Monitor) ระบบงานต่าง ๆ รวมถึงมีระบบ Call Center ให้ความช่วยเหลือผู้ใช้งาน

ที่มีปัญหาหรือเกิดข้อขัดข้องในระหว่างการใช้งาน นอกจากนี้ยังพิจารณาประเด็นความมั่นคงปลอดภัยไซเบอร์ร่วมด้วย โดยศูนย์ไซเบอร์ทหารเข้ามามีส่วนร่วมในการตรวจสอบและให้คำแนะนำในการปฏิบัติ

2.2 จากข้อมูลการวิจัยเชิงปริมาณและข้อมูลจากการสัมภาษณ์ผู้บริหารระดับสูง ในประเด็นมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศของ สส.ทหาร ในบริบทปัจจุบันและความต้องการมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศของ สส.ทหาร ตามกรอบมาตรฐาน ISO/IEC 27001: 2013 โดยนำผลการวิเคราะห์ข้อมูลที่ได้นำมาจัดทำเป็น (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงตามกรอบมาตรฐาน ISO/IEC 27001: 2013 ทั้ง 14 ประเด็น ประกอบด้วย 1) นโยบายความมั่นคงปลอดภัยสารสนเทศ 2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ 3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล 4) การบริหารจัดการสินทรัพย์ 5) การควบคุมการเข้าถึง 6) การเข้ารหัสข้อมูล 7) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม 8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน 9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล 10) การจัดหา การพัฒนา และการบำรุงรักษาระบบ 11) ความสัมพันธ์กับผู้ให้บริการภายนอก 12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ 13) ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ 14) ความสอดคล้อง ให้ผู้ทรงคุณวุฒิพิจารณาก่อนนำเข้าสู่การสนทนากลุ่ม ซึ่งผลการสนทนากลุ่ม (Focus Group) พบว่า ผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ และผู้มีส่วนเกี่ยวข้องกับการบริหารจัดการความเสี่ยงทั้ง 11 คน ให้ความเห็นชอบ (ร่าง) แผนฯ ทั้ง 14 แผนย่อย โดยทั้ง 11 คน ได้ลงชื่อรับรองการให้ความเห็นชอบในแบบบันทึกการให้ความเห็นชอบ (ร่าง) แผนฯ เพื่อเสนอขออนุมัติใช้ต่อไป

สรุปและอภิปรายผล

สรุป

จากผลการวิจัยนำมาสรุปความคิดเห็นของกำลังพล สส.ทหาร เกี่ยวกับกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำลังพลส่วนใหญ่ชี้ว่า สส.ทหาร มีการบริหารจัดการในระดับน้อย ส่วนมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) ของ สส.ทหาร กำลังพล สส.ทหาร เห็นว่ามีมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในระดับน้อย และเห็นว่าการควบคุมการเข้าถึงในปัจจุบันมีการดำเนินการในระดับมากถึงมากที่สุด โดยเฉพาะในเรื่องการควบคุมการเข้าถึงเครือข่ายของผู้ใช้งานที่มีการกำหนดสิทธิในการเข้าถึงที่กำหนดเป็นหน้าที่ความรับผิดชอบของผู้ใช้งาน ด้วยการพิสูจน์ตัวตน ส่วนความต้องการแผนความเสี่ยงด้านเทคโนโลยีสารสนเทศตามมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศตามกรอบมาตรฐาน ISO/IEC 27001: 2013 ชี้ให้เห็นว่า กำลังพลส่วนใหญ่มีความต้องการในระดับมากที่สุด โดยต้องการให้องค์การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับวัตถุประสงค์ขององค์กร กำหนดโครงสร้างภายในและบทบาทหน้าที่ความรับผิดชอบที่ชัดเจน รวมถึงกำหนดพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยสารสนเทศ พร้อมทั้งต้องมีการเตรียมการอุปกรณ์ประมวลผลสำรองให้มีความพร้อมใช้ด้วย

จากผลการวิจัยดังกล่าวข้างต้น ผู้วิจัยได้นำมาสรุปข้อค้นพบจากการวิจัยในแต่ละประเด็นพิจารณานำเข้าสู่การประยุกต์ใช้ผลการวิจัย จัดทำ (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมการสื่อสารทหาร ประกอบไปด้วย 14 แผนย่อย ตามมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ โดยในแต่ละแผนยังได้กำหนดตัวชี้วัดในการดำเนินการ ดังนี้

1. แผนปฏิบัติการด้านนโยบายความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย การทำความเข้าใจองค์กรและบริบทองค์กร โดยจัดให้มีแผนเพื่อจัดการความเสี่ยงในด้านต่าง ๆ รวมถึงการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศและการทำความเข้าใจนโยบายกับกำลังพล สส.ทหาร

2. แผนปฏิบัติการด้านโครงสร้างความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย การกำหนดกรอบและประยุกต์ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อระบุขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศทั้งภายในและภายนอกองค์กร กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในทุกระดับ กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดโครงสร้างความมั่นคงปลอดภัยสารสนเทศ

3. แผนปฏิบัติการด้านความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล ได้แก่ ประเด็นการปฏิบัติการ ดังนี้ การกำหนดทรัพยากรที่จำเป็น สำหรับการดำเนินการและการปรับปรุงอย่างต่อเนื่อง จัดทำข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ตรวจสอบประเมินผลและทบทวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรตามระยะเวลาที่กำหนด กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล

4. แผนปฏิบัติการด้านการบริหารจัดการทรัพย์สิน ได้แก่ ประเด็นการปฏิบัติการในด้านการกำหนดผู้ที่เกี่ยวข้องและความต้องการของผู้เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีกระบวนการที่เหมาะสมในการดำเนินการควบคุมแก้ไข เพื่อไม่ให้เกิดซ้ำ กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดการบริหารจัดการสินทรัพย์

5. แผนปฏิบัติการด้านการควบคุมการเข้าถึง ประกอบด้วย การจัดทำข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ กำหนดขั้นตอนในการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เฝ้าระวัง วัดผล วิเคราะห์และการประเมินการทำงานด้านความมั่นคงปลอดภัยสารสนเทศ กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการควบคุมการเข้าถึง

6. แผนปฏิบัติการด้านการเข้ารหัสข้อมูล ได้แก่ กิจกรรมในด้าน กำหนดกรอบและประยุกต์ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีกระบวนการที่เหมาะสมเพื่อตอบสนองต่อความไม่สอดคล้อง และดำเนินการควบคุมแก้ไข เพื่อไม่ให้เกิดซ้ำ กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดการเข้ารหัสข้อมูล

7. แผนปฏิบัติการด้านความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม ประกอบด้วย การกำหนดการสื่อสารเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศให้ทราบทั้งองค์กร และต้องปฏิบัติตามแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

8. แผนปฏิบัติการด้านความมั่นคงปลอดภัยสำหรับการดำเนินการ ได้แก่ กิจกรรมในด้านการกำหนดการปฏิบัติบำรุงรักษา และปรับปรุงอย่างต่อเนื่องต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ที่สอดคล้องกับข้อกำหนดตามมาตรฐาน กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดความมั่นคงปลอดภัยสำหรับการดำเนินงาน

9. แผนปฏิบัติการด้านความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล ประกอบด้วย การปฏิบัติการในด้านการกำหนดการสื่อสารเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศให้ทราบทั้งองค์กร และกำหนดขั้นตอนการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในช่วงเวลาตามแผน กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

10. แผนปฏิบัติการด้านการจัดหา การพัฒนาและการบำรุงรักษาระบบ ได้แก่ การดำเนินการในด้านการทบทวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรตามระยะเวลาที่กำหนดไว้ และต้องปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดการจัดหา พัฒนา และดูแลระบบสารสนเทศ

11. แผนปฏิบัติการด้านความสัมพันธ์กับผู้ให้บริการภายนอก ประกอบด้วย การกำหนดกรอบและประยุกต์ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อระบุขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศทั้งภายในและภายนอกองค์กร กำหนดขั้นตอนในการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในช่วงเวลาตามแผน กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดความสัมพันธ์กับผู้ให้บริการภายนอก

12. แผนปฏิบัติการด้านการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ได้แก่ การกำหนดทรัพยากรที่จำเป็น สำหรับการดำเนินการและการปรับปรุงอย่างต่อเนื่องและมีการกำหนดขั้นตอนในการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

13. แผนปฏิบัติการประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ ประกอบด้วย การดำเนินงานในด้านการกำหนดทรัพยากรที่จำเป็น กำหนดขั้นตอนในการดำเนินการประเมินความเสี่ยงและต้องปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ

14. แผนปฏิบัติการด้านความสอดคล้อง ประกอบด้วย กิจกรรมการกำหนดขั้นตอนในการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และมีการทบทวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรตามระยะเวลาที่กำหนด กำหนดตัวชี้วัดสำหรับแผน คือ ระดับความสำเร็จในการกำหนดความสอดคล้อง

อภิปรายผล

การอภิปรายผล ประกอบด้วย 2 ส่วน ดังนี้

1. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จากการวิจัยพบว่าปัจจัยระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีอิทธิพลต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) สอดคล้องกับข้อค้นพบจากงานวิจัยของ รักษิต สุทธิพงษ์ และคณะ (2557) ที่ชี้ว่า การปฏิบัติงานด้านการบริหารความเสี่ยงขององค์กรในระดับน้อยใน 8 ด้าน ต่อไปนี้ คือ 1) สภาพแวดล้อมภายใน 2) วัตถุประสงค์ 3) การระบุความเสี่ยง 4) การประเมินความเสี่ยง 5) การตอบสนองต่อความเสี่ยง 6) ด้านกิจกรรมการควบคุม 7) สารสนเทศและการสื่อสาร และ 8) การติดตามประเมินผลจะส่งผลให้องค์กรมีความเสี่ยงสูง และสอดคล้องกับงานวิจัยของ

ไกรลาศ สิทธิยะ (2558) ที่ศึกษาและอธิบายว่าแนวทางความมั่นคงปลอดภัยสารสนเทศของวิสาหกิจขนาดกลางและขนาดย่อมด้านเครือข่ายไร้สายต้องมีการคำนึงถึงการรักษาความปลอดภัย โดยพิจารณาจากมาตรฐาน ISO/IEC 27001 เพื่อป้องกันข้อมูลทางการเงิน และทางบัญชีเสียหายและเกิดจากการติดไวรัสและมัลแวร์ และการควบคุมการเข้าถึงเฉพาะผู้มีสิทธิ์เข้าถึงระบบสารสนเทศ จำเป็นต้องมีการกำหนดนโยบาย และผู้รับผิดชอบต่อขั้นตอนในการปฏิบัติงาน ทั้งนี้ยังสอดคล้องกับงานวิจัยของ ธันวัฒน์ นามอ่อนตา และ วศิณ ชูประยูร (2561) ที่ศึกษาระดับอิทธิพลของพฤติกรรมปัจจุบันที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศของข้าราชการกองบัญชาการกองทัพไทย ต่อปัญหาและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และระดับอิทธิพลของสภาพปัญหาต่อแนวปฏิบัติดังกล่าว เพื่อนำมาพัฒนาแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับบริบทกองบัญชาการกองทัพไทย ซึ่งพบว่า แนวปฏิบัติที่มีความเหมาะสมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทยควรประกอบด้วย 4 ด้านสำคัญ คือ 1) กำหนดตัวบุคคลอย่างชัดเจนในการเข้าถึงข้อมูลชั้นความลับของหน่วยงาน 2) เข้มงวดในการใช้ระบบพิสูจน์บุคคลก่อนเข้าใช้งานระบบสารสนเทศ 3) จัดให้มีแหล่งเก็บสำรองข้อมูลที่สำคัญขององค์กรและกำหนดให้มีหน่วยงานที่รับผิดชอบโดยเฉพาะ 4) ใช้ผลิตภัณฑ์ซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ และยังสอดคล้องกับงานวิจัยของ Smet and Mayer (2016) ที่ศึกษาการกำกับดูแลแบบบูรณาการความเสี่ยงที่เป็นการปฏิบัติตามกฎ ระเบียบภายในองค์กร การปฏิบัติดังกล่าว องค์กรต้องมีจริยธรรมและสอดคล้องกับความต้องการทางด้านนโยบายภายในซึ่งเป็นความรับผิดชอบของผู้ที่เกี่ยวข้อง เพราะมีความสัมพันธ์กับการบริหารการจัดการความเสี่ยงในองค์กร การสร้างกฎเกณฑ์ต่าง ๆ เป็นมาตรการจัดการความเสี่ยงด้านโครงสร้างเทคโนโลยีสารสนเทศ เพื่อให้เกิดแนวคิดที่มีประสิทธิภาพของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศขององค์กร และยังสอดคล้องกับงานวิจัยของ King (2017) ที่ศึกษาและอธิบายความเสี่ยงในมุมมองเชิงบวกที่มุ่งเน้นองค์กรขนาดเล็กและขนาดกลางที่อยู่ในทวีปอเมริกา โดยใช้กรอบ ISO/IEC 27001: 2013 ที่สามารถแสดงให้เห็นการกำกับดูแลด้านเทคโนโลยีสารสนเทศเพื่อปกปิดข้อบกพร่องของกระบวนการทำงานซึ่งเป็นแนวทางที่ดีที่สุด โดยมุ่งเน้นประสิทธิภาพในการจัดการความเสี่ยงเทคโนโลยีสารสนเทศจากการเติบโตขององค์กรที่มีการประยุกต์ใช้ทรัพย์สินด้านเทคโนโลยีอย่างมีประสิทธิภาพก่อให้เกิดความต่อเนื่องทางธุรกิจ โดยกระบวนการการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เริ่มต้นของขั้นตอนการประเมินความเสี่ยง ระบุความเสี่ยงภายนอก และภายในองค์กรและความสามารถขององค์กรจากภัยคุกคามที่มีผลกระทบด้วยการลดความเสี่ยงแต่ละประเภทโดยการทดสอบการถดถอยเชิงเส้นเพื่อหาความสัมพันธ์เชิงบวกและยังสอดคล้องกับงานวิจัยของ Velasco, Ullauri, Luis, and Jacome (2018) ที่ศึกษาประโยชน์ของการใช้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013 ในอุตสาหกรรมการผลิตของประเทศเอกวาดอร์ โดยใช้วงจร Deming ที่เป็นกระบวนการ PDCA (Plan-Do-Check-Act) สำหรับการวิจัย ตามโครงสร้างของมาตรฐาน ISO/IEC 27001: 2013 พบว่า หลังจากที่ได้ดำเนินการบริหารจัดการองค์กรให้เป็นไปตามกระบวนการ PDCA ทำให้การใช้ระบบรักษาความปลอดภัยของข้อมูลสำหรับอุตสาหกรรมการผลิตของบริษัท ตัดสินใจใช้

มาตรฐาน ISO/IEC 27001: 2013 ในกระบวนการผลิตของบริษัท มาตรฐานนี้เป็นหนึ่งในรูปแบบที่เหมาะสมที่สุดของแนวปฏิบัติที่ดีที่สุดและแนวทางด้านความปลอดภัยเพื่อสร้างชุดของกลยุทธ์และการควบคุมที่รับรองข้อมูลและผลประโยชน์ ซึ่งบริษัทได้นำมาใช้สำหรับการบริหารความเสี่ยง ช่วยให้เกิดการปรับปรุงอย่างต่อเนื่อง

2. มาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) จากการศึกษาวิจัย พบว่าปัจจัยระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศประกอบด้วย 35 ตัวแปร ที่มีอิทธิพลต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ (ในบริบทปัจจุบัน) ซึ่งสอดคล้องกับงานวิจัยของ จิตตกานต์ บุญศิริทิวัตถ์ และโกวิท รพีพิศาล (2560) ที่ศึกษาและอธิบายการพัฒนาแนวทางในการจัดการความมั่นคงปลอดภัยระบบสารสนเทศที่เหมาะสมของโรงพยาบาลเอกชนในกรุงเทพมหานครภายใต้การควบคุมที่เพิ่มเข้ามาใหม่ใน ISO/IEC 27001: 2013 จาก ISO/IEC 27001: 2005 ทั้งในมุมมองของผู้ใช้ระบบและนักพัฒนาระบบ เพื่อพัฒนาแนวทางในการควบคุมความปลอดภัยของระบบสารสนเทศในโรงพยาบาล โดยเสนอแนวทางปฏิบัติสำหรับโรงพยาบาล 11 ด้าน คือ 1) การควบคุมความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ 2) การควบคุมการจำกัดการติดตั้งซอฟต์แวร์ 3) การควบคุมนโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก 4) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก 5) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ 6) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ 7) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ 8) นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย 9) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย 10) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย 11) การทดสอบด้านความมั่นคงปลอดภัยของระบบ ยังสอดคล้องกับงานวิจัยของ เอกชัย ประเสริฐวงษ์ และวศิณ ชูประยูร (2562) ที่ศึกษาและอธิบายถึงสภาพปัญหาการประเมิน และการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของวิสาหกิจขนาดกลางและขนาดย่อมในอำเภอหนองแค จังหวัดสระบุรี โดยอ้างอิงตามกรอบมาตรฐาน ISO/IEC 27001: 2013 ใน 5 มิติ คือ ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร และเครือข่าย และกรอบมาตรฐาน ISO/IEC 31000 ที่เป็นผู้ประกอบการ SMEs ในเขตอำเภอหนองแค จังหวัดสระบุรี จำนวน 200 บริษัท พบว่าสภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศด้านข้อมูล เกิดความผิดพลาดในการจัดเก็บ อัพเดท และการทำลายข้อมูล ด้านฮาร์ดแวร์ พื้นที่ไม่เพียงพอต่อการติดตั้งอุปกรณ์ ด้านซอฟต์แวร์ การดาวน์โหลดซอฟต์แวร์และระบบปฏิบัติการที่ผิดกฎหมายมาใช้ในระบบโดยไม่ได้รับอนุญาต ด้านบุคลากร ขาดการควบคุมและความเข้มงวดในการใช้รหัสผ่านในการเข้าถึงระบบสารสนเทศ ด้านเครือข่ายขาดการควบคุมป้องกัน บุคคลภายนอกเข้าถึงเครือข่ายขององค์กร สอดคล้องกับงานวิจัยของ Alebrahim, Hatebur and Goeke (2014) ที่ศึกษาและอธิบายการวิเคราะห์ความเสี่ยงของระบบคลาวด์และการให้บริการระบบคลาวด์ที่สอดคล้องกับมาตรฐาน ISO/IEC 27001: 2013 โดยใช้แนวคิดทั่วไปสำหรับการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลในองค์กร ในภาคผนวกของมาตรฐาน ISO/IEC 27001: 2013 ในการบรรลุความปลอดภัยของข้อมูลโดยนำเสนอวิธีการที่มีโครงสร้างและรูปแบบที่ใช้ในการวิเคราะห์ความเสี่ยงสำหรับระบบคลาวด์คอมพิวติ้ง เพื่อนำมากำหนดขอบเขตของระบบการจัดการ

ความปลอดภัยของข้อมูล (Information Security Management Systems: ISMS) รูปแบบการคุกคาม รูปแบบความต้องการด้านความปลอดภัยเพื่อกำหนดข้อกำหนดด้านความปลอดภัย โดยนำเสนอการวิเคราะห์ความเสี่ยงตามรูปแบบที่เริ่มจากการกำหนดขอบเขตของระบบการจัดการความปลอดภัยของข้อมูล ระบุขอบเขตก่อนเริ่มการวิเคราะห์ความเสี่ยง ต่อมาจึงวิเคราะห์และระบุสินทรัพย์ที่อยู่ในขอบเขตสำหรับระบบการจัดการความปลอดภัยของข้อมูล ระบุความรับผิดชอบของสินทรัพย์ วิเคราะห์ถึงภัยคุกคามที่จะมีต่อสินทรัพย์ รวมถึงช่องโหว่ที่อาจถูกโจมตีจากภัยคุกคาม และสอดคล้องกับงานวิจัยของ Setiawan, Mukhoyyaroh, and Fauzi (2014) ได้ทำการตรวจสอบระบบสารสนเทศโรงพยาบาลโดยใช้มาตรฐาน ISO/IEC 27001: 2013 กรณีศึกษาใน RSU PKU Muhammadiyah Bantul พบว่า ผู้บริหารของ RSU Muhammadiyah Bantul ไม่ได้ทำการฝึกอบรมอย่างเป็นทางการเกี่ยวกับการจัดการสินทรัพย์โดยขาดการตรวจสอบสินทรัพย์ที่ไม่ได้ดำเนินการเป็นประจำ ดำเนินการเป็นระยะ ส่วนผลการตรวจสอบความปลอดภัยทางกายภาพและสิ่งแวดล้อม มีการปฏิบัติตามขั้นตอนของการรักษาความปลอดภัยทางกายภาพและสิ่งแวดล้อมที่ได้กำหนดไว้โดยองค์กร และยังสอดคล้องกับงานวิจัยของ Lopes, Guarda, and Oliveira (2019) ที่ศึกษาการดำเนินการตามมาตรฐาน ISO/IEC 27001: 2013 ในฐานะที่เป็นผู้อำนวยความสะดวกในการปฏิบัติตามข้อกำหนดการป้องกันข้อมูลทั่วไป โดยพบว่าการดำเนินงานขององค์กรตามข้อกำหนดดังกล่าว องค์กรควรจะเห็นบริบทของการบรรลุเป้าหมายทางธุรกิจ มีความจำเป็นอย่างยิ่งที่จะต้องเน้นย้ำถึงประโยชน์ที่องค์กรจะได้รับในการเพิ่มคุณค่ากับธุรกิจโดยนำข้อกำหนดการป้องกันข้อมูลทั่วไปมาเป็นเครื่องมือสำหรับการสร้างความได้เปรียบเชิงกลยุทธ์บนพื้นฐานของความไว้วางใจระหว่างองค์กร พนักงาน ลูกค้า และคู่ค้า โดยข้อกำหนดการป้องกันข้อมูลทั่วไปส่งเสริมให้ใช้การรับรองมาตรฐาน ISO/IEC 27001: 2013 เพื่อแสดงให้เห็นว่าองค์กรกำลังจัดการความปลอดภัยของข้อมูลตามแนวปฏิบัติที่ได้มาตรฐานในระดับสากล

ข้อเสนอแนะในการวิจัยครั้งต่อไป

1. การวิจัย การพัฒนาแผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สส.ทหาร ในครั้งต่อไปนั้น ควรมีการวิเคราะห์จำแนกกลุ่ม (Discriminant Analysis) เพื่อจำแนกปัจจัย ว่ามีปัจจัยใดบ้าง ที่มีอิทธิพลต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ

2. อาจมีการนำสถิติ การวิเคราะห์องค์ประกอบ (Factor Analysis) เพื่อลดจำนวนตัวแปร โดยการรวมตัวแปรหลาย ๆ ตัวให้อยู่ในองค์ประกอบเดียวกัน องค์ประกอบที่ได้ถือเป็นตัวแปรใหม่ ที่สามารถหาค่าข้อมูลขององค์ประกอบที่สร้างขึ้นได้ เรียกว่า Factor Score สามารถนำองค์ประกอบดังกล่าวไปเป็นตัวแปรสำหรับการวิเคราะห์ทางสถิติต่อไป ใช้ในการแก้ปัญหาอันเนื่องมาจากการที่ตัวแปรอิสระของเทคนิค การวิเคราะห์สมการความถดถอยมีความสัมพันธ์กัน (Multicollinearity)

3. ควรให้มีการขยายขอบเขตการศึกษากระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามกรอบมาตรฐาน ISO/IEC 27001: 2013 ให้ครอบคลุมทุกหน่วยทั้งกองบัญชาการกองทัพไทย

เอกสารอ้างอิง

ไกรลาศ สิทธิยะ. (2558). แนวทางในการวางนโยบายความมั่นคงปลอดภัยทางสารสนเทศสำหรับวิสาหกิจขนาดกลางและขนาดเล็กด้านระบบเครือข่ายไร้สาย. *วารสารวิชาการมหาวิทยาลัยฟาร์อีสเทอร์น, 23*(1), 54-63. สืบค้นจาก http://www.tci-thaijo.org/39036-Article Text-88921-1-10-20150830

จิตตกานต์ บุญศิริทิวัตถ์ และโกวิท รพีพิศาล. (2560). การพัฒนาแนวทางในการจัดการความมั่นคงความปลอดภัยระบบสารสนเทศ ที่เหมาะสมของโรงพยาบาลเอกชนในกรุงเทพมหานคร. *วารสารรังสิตสารสนเทศ, 23*(1), 61-91. สืบค้นจาก http://rilj.rsu.ac.th/journal/31/article/108

ธันวัฒน์ นามอ่อนตา และวศิณ ชูประยูร. (2561). ตัวแบบการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย. *วารสารรังสิตสารสนเทศ, 24*(1), 6-20. สืบค้นจาก http://rilj.rsu.ac.th/download/article/122

รักษิต สุทธิพงษ์. และคณะ (2557). รูปแบบการบริหารความเสี่ยงทางการกีฬาและนันทนาการในโรงเรียนสาธิตสังกัดสำนักงานคณะกรรมการการอุดมศึกษา. *วารสารศึกษาศาสตร์ มหาวิทยาลัยนเรศวร, 16*(4), 55-70. สืบค้นจาก https://so06.tci-thaijo.org/index.php/edujournal_nu/article/view/21942

เอกชัย ประเสริฐวงษ์ และวศิณ ชูประยูร. (2562). สภาพปัญหา การประเมิน และการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของวิสาหกิจขนาดกลางและขนาดย่อมในอำเภอหนองแค จังหวัดสระบุรี. *วารสารรังสิตสารสนเทศ, 26*(2), 6-29. สืบค้นจาก http://rilj.rsu.ac.th/download/article/203

Alebrahim, A., Hatebur D., & Goeke, L. (2014). Pattern-based and ISO 27001 compliant risk analysis for cloud systems. *IEEE Workshop on evolving security and privacy requirements engineering (ESPRE),* 42-47.

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.

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).

Krejcie, R. V., and Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement, 30*(3), 607-610.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator. *Journal of information systems engineering & management, 4*(2), 1-8.

Setiawan, H., Mukhoyyaroh, K. I., & Fauzi, M. D. (2014). Hospital Information System Audit Using The ISO 27001 Standard (Case Study In RSU PKU Muhammadiyah Bantul). *International Journal on Informatics for Development, 3*(1), 32-35.

Smet, D. D., and Mayer, N. (2016). Integration of IT governance and security risk management: A systematic literature review. *International conference on information society (i-Society),* 143-148.

Velasco, J., Ullauri, R., Luis, P., & Jacome, B. (2018). Benefits of implementing an ISMS according to the ISO 27001 standard in the Ecuadorian manufacturing industry. *International conference on information systems and computer science (INCISCOS),* 294-300.