การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ศิวกร รัตติโชติ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรบัญชีมหาบัณฑิต
สาขาวิชาการบัญชี วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี
มหาวิทยาลัยธุรกิจบัณฑิตย์
ปีการศึกษา 2565

A STUDY OF INFORMATION SECURITY MANAGEMENT COMPONENTS IN THE FACULTY OF MEDICINE SIRIRAJ HOSPITAL

SIWAKORN RATTICHOT

A Thematic Paper Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Accountancy Program
Department of College of Innovative Business and Accountancy,
Dhurakij Pundit University
Academic Year 2022

ใบรับรองสารนิพนธ์

วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา บัญชีมหาบัณฑิต

หัวข้อสารนิพนธ์ การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

เสนอโดย ศิวกร รัตติโชติ

สาขาวิชา บัญชีมหาบัณฑิต

อาจารย์ที่ปรึกษาสารนิพนธ์ ดร.ณัฐพัชร์ นวลมณีฐิติ

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบสารนิพนธ์แล้ว

.....ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ศิริเดช คำสุพรหม)

.....กรรมการและอาจารย์ที่ปรึกษาสารนิพนธ์

(ดร.ณัฐพัชร์ นวลมณีฐิติ)

..... กรรมการ

(ดร. เปรมารัช วิลาลัย)

วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชีรับรองแล้ว

..... คณบดีวิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี

(ผู้ช่วยศาสตราจารย์ ดร.ศิริเดช คำสุพรหม)

วันที่ 31 เดือน ก.ค. พ.ศ. 2566

หัวข้อวิทยานิพนธ์	การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล
ชื่อผู้เขียน	ศิวกร รัตติโชติ
อาจารย์ที่ปรึกษา	ดร. ณัฐพัชร์ นวลมณีฐิติ
หลักสูตร	บัญชีมหาบัณฑิต (สาขาวิชาการบัญชี)
ปีการศึกษา	2565

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาองค์ประกอบของการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ซึ่งเป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้แบบสอบถาม (Questionnaire) เป็นเครื่องมือกับกลุ่มตัวอย่างครั้งนี้ คือ บุคลากรจากแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล จำนวน 400 ราย ซึ่งได้มาจากการสุ่มตัวอย่างแบบอย่างง่าย (Simple random sampling) สถิติที่ใช้ในการวิเคราะห์ข้อมูล คือ การวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis) โดยทำการวิเคราะห์องค์ประกอบหลักสำคัญ (Principal Component Analysis: PC) และใช้การหมุนแกนแบบมุมฉาก (Orthogonal Rotation) ด้วยวิธีแวริแมกซ์ (Varimax Method)

ผลการวิจัย พบว่า การวิเคราะห์องค์ประกอบของการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิรราชพยาบาล จากตัวแปร 15 ตัวชี้วัด มีค่าสถิติของไคเซอร์ - ไมเยอร์ - โอลคิน (KMO) มีค่าเท่ากับ 0.938 และ ค่าสถิติไค - สแควร์ (χ^2) ที่ใช้ในการทดสอบมีค่าเท่ากับ 25997.82 ได้ทำการสกัดองค์ประกอบได้องค์ประกอบทั้งหมด 4 องค์ประกอบ มีพิสัยของค่าไอแกน (Eigen value) มากกว่า 1 โดยอยู่ระหว่าง 23.048 – 1.197 และมีค่าความแปรปรวนรวม (Cummulative) ของตัวแปรทั้งหมดได้ร้อยละ 80.03 ประกอบไปด้วยองค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัย และองค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ โดยแต่ละองค์ประกอบสามารถอธิบายความแปรปรวนได้ร้อยละ 65.85, 5.94, 4.82 และ 3.42 ตามลำดับ จากผลการวิจัยพบว่า องค์ประกอบที่ 1 มีร้อยละความแปรปรวนมากที่สุด แสดงว่าส่งผลต่อการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทย์ศาสตร์ศิริราชพยาบาล มากที่สุด

คำสำคัญ: การบริหารจัดการความมั่นคงปลอดภัย, สารสนเทศ, คณะแพทยศาสตร์ศิริราชพยาบาล

ณัฐพัชร์ นวลมณี

ThesisTitle	A Study of Information Security Management Components in the Faculty of Medicine Siriraj Hospital
Author	Siwakorn Rattichot
Thesis Advisor	Nattapat Nuanmaneethiti Ph.D.
Department	Master of Accounting Program
Academic Year	2022

Abstract

The objective of this research was to study the components of information security management at the Faculty of Medicine, Siriraj Hospital. A quantitative approach was employed for the study, with a questionnaire used for data collection. The sample group consisted of personnel from various departments of the Faculty of Medicine, Siriraj Hospital, totaling 400 individuals selected through simple random sampling. Data were analyzed using Exploratory Factor Analysis, specifically Principal Component Analysis (PCA) and the Varimax Method with Orthogonal Rotation.

Research findings revealed that an analysis of the components of information security management at the Faculty of Medicine, Siriraj Hospital, incorporating 15 variables, yielded a Kaiser-Meyer-Olkin (KMO) statistic of 0.938 and a chi-square statistic with a value of 25997.82. Following factor extraction, a total of four components were identified with eigenvalues greater than 1, ranging from 23.048 to 1.197. The cumulative variance of all variables was 80.03%. These components included: Component 1 - Supervision and Management of Information Security; Component 2 - Operation and Maintenance of Information Security Management Systems; Component 3 - Development and Business Continuity Management of Information Security; and Component 4 - Strategic Policy and Management of Information Security. Each component explained variances of 65.85%, 5.94%, 4.82%, and 3.42%, respectively. Based on the research results, Component 1 had the highest variance, indicating it had the most significant impact on the management of information security at the Faculty of Medicine, Siriraj Hospital.

Keywords: Security Management, Information, Faculty of Medicine, Siriraj Hospital

ศิวกร รัตติโชติ

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้ สำเร็จลุล่วงได้ด้วยความอนุเคราะห์ และความกรุณาช่วยเหลืออย่างยิ่งจาก ดร. ณัฐพัชร์ นวลมณีฐิติ อาจารย์ที่ปรึกษาสารนิพนธ์ที่ให้ความใจใส่ในการให้คำปรึกษา ความรู้ และคำแนะนำอื่น ๆ ที่เป็นประโยชน์กับสารนิพนธ์ฉบับนี้ ตลอดจนการตรวจ และแก้ไขข้อบกพร่อง รวมถึงคำชี้แนะแก่ผู้วิจัยด้วยดีตลอดมา จนทำให้สารนิพนธ์ฉบับนี้สำเร็จด้วยดี รวมทั้งขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. ศิริเดช คำสุพรหม ผู้ช่วยศาสตราจารย์ ดร.รัชดาภรณ์ เสมาขันธ์ ดร.เปรมารัช วิลาลัย และ ดร.อริสรา ธานีรณานนท์ กรรมการสอบสารนิพนธ์ที่ได้กรุณาให้ข้อเสนอแนะในการปรับปรุงเพื่อให้สารนิพนธ์ฉบับนี้สมบูรณ์ยิ่งขึ้น ตลอดจนคณาจารย์ เพื่อนร่วมรุ่น และเจ้าหน้าที่วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์ทุกท่านที่ให้ความสะดวกด้านอำนวยการ และประสานงานในการทำสารนิพนธ์ รวมถึงการค้นคว้าหาข้อมูลในการจัดทำสารนิพนธ์ของผู้วิจัยครั้งนี้สำเร็จลุล่วงไปด้วยดี ผู้วิจัยรู้สึกซาบซึ้งเป็นอย่างยิ่ง จึงขอขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ท้ายนี้ผู้วิจัยขอขอบพระคุณ ผู้บริหาร อาจารย์ ผู้เชี่ยวชาญ เจ้าหน้าที่ และลูกจ้างที่ปฏิบัติงานจากหน่วยงานต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล ที่กรุณาสละเวลาให้ความร่วมมือในการตอบแบบสอบถามครั้งนี้ และขอขอบพระคุณสมาชิกในครอบครัว ญาติพี่น้อง หัวหน้างาน และเพื่อนสนิทที่คอยให้กำลังใจและให้ความช่วยเหลือตลอดมาจนทำให้สารนิพนธ์สำเร็จสมบูรณ์ทุกประการ ข้าพเจ้าหวังว่างานสารนิพนธ์ชิ้นนี้จะเป็นประโยชน์ต่อผู้ที่ต้องการนำข้อมูลไปทำการศึกษาหรือนำไปใช้ประโยชน์ และหากมีข้อบกพร่องประการใด ผู้วิจัยขอน้อมรับไว้แต่เพียงผู้เดียว

ศิวกร รัตติโชติ

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญตาราง (ต่อ)

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในโลกปัจจุบัน เทคโนโลยีสารสนเทศดิจิทัลเข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กร ทั้งในส่วนของการบริหารจัดการ การตรวจสอบ การจัดเก็บ และการประมวลผลข้อมูลของระบบงานสำคัญต่าง ๆ เป็นต้น รวมถึงหน่วยงานของรัฐเกือบทั้งหมดได้ถูกกำหนดให้ดำเนินการตามนโยบาย e – Government ตั้งแต่แผนแม่บทเทคโนโลยีสารสนเทศและสื่อสาร (ฉบับที่ 2) พ.ศ. 2552 – 2556 และพัฒนาอย่างต่อเนื่อง จนรัฐบาลตระหนักถึงความสำคัญของการปรับเปลี่ยนกระบวนการทำงานของหน่วยงานทั้งภาครัฐ และภาคเอกชน โดยการนำระบบเทคโนโลยีสารสนเทศเข้ามาเพิ่มประสิทธิภาพ ลดต้นทุน และการแข่งขันทางธุรกิจ เช่น การจัดทำตรวจสอบ และติดตามการใช้จ่ายงบประมาณ การบริหารงานพัสดุ การบริหารทรัพยากรบุคคล การบริหารลูกค้าและการตลาด และการบริหารการเงินและบัญชี เป็นต้น สู่ระบบการประมวลผลข้อมูลขนาดใหญ่ (Big Data) ผ่านระบบคอมพิวเตอร์และระบบคราวน์ เป็นต้น เพื่อสนับสนุนการทำธุรกรรม ตั้งแต่การบันทึกรายการธุรกรรมต่าง ๆ ที่เกิดขึ้นประจำวัน การให้บริการลูกค้า และการวิเคราะห์ข้อมูลเพื่อประกอบการตัดสินใจ และให้ระบบสารสนเทศที่จะเป็นเครื่องมือที่จะช่วยให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ (สำนักงานพัฒนารัฐบาลดิจิทัล, 2563) ในขณะเดียวกันการนำเทคโนโลยีสารสนเทศดิจิทัลมาใช้ก็มีความเสี่ยงหลายประการ ถ้าหากองค์กรไม่มีการบริหารจัดการที่ดีและการรักษาความปลอดภัยของข้อมูลที่รัดกุมเพียงพอ รวมถึงการคุ้มครองข้อมูลส่วนบุคคล ก็อาจจะส่งผลกระทบระบบงานหรือความเสียหายกับองค์กรและลูกค้าได้ ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศดิจิทัลที่เกี่ยวข้องกับการปฏิบัติงานสามารถแบ่งออกเป็น 4 ประเภท ได้แก่ Access Risk, Integrity Risk, Availabily Risk แลInfrastructure Risk เป็นต้น

ด้านการพัฒนาระบบงาน ก็มีผลการวิจัยเกี่ยวกับสาเหตุที่หน่วยงานล้มเหลวในการพัฒนาระบบงานคอมพิวเตอร์ ได้แก่ ผู้บริหารระดับสูงไม่สนับสนุนหรือไม่มีส่วนร่วมในการพัฒนา หรือไม่มีคณะกรรมการระดับสูง (Steering Committee) ในการพัฒนาระบบงาน การเปลี่ยนความต้องการหรือวัตถุประสงค์ของระบบงานบ่อย การเลือกเทคโนโลยีที่ก้าวหน้าล้ำสมัยเกินกว่าที่พนักงานจะทำความเข้าใจ การขาดคู่มือหรือวิธีการพัฒนาระบบงานให้เป็นขั้นตอนอย่างเป็นมาตรฐาน และบุคลากรที่เกี่ยวข้องกับการพัฒนาระบบมีไม่เพียงพอและได้รับการฝึกอบรมที่ไม่เพียงพอ สอดคล้องกับผลการตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศของรัฐจำนวน 11 หน่วยงาน โดยคัดเลือกหน่วยงานที่มีการใช้งานระบบสารสนเทศที่ให้บริการโครงสร้างพื้นฐานที่สำคัญของประเทศ และสนับสนุนโครงการของรัฐบาลหรือมีประชาชนใช้บริการเป็นจำนวนมาก ในปีงบประมาณ พ.ศ. 2562 – 2563 ดำเนินการตรวจสอบ 2 ด้าน ได้แก่ การควบคุมทั่วไป (IT General Controls) และการควบคุมเฉพาะระบบปฏิบัติการ (IT Application Controls) ปีงบประมาณ พ.ศ. 2564 ด้วยวิธีการวิเคราะห์ข้อมูลการตรวจสอบ (Audit Data Analytics: ADAs) โดยอ้างอิงมาตรฐานการตรวจเงินแผ่นดินขององค์การสถาบันการตรวจสอบสูงสุดระหว่างประเทศ (ISSAIs) มาตรฐาน COBIT, GTAG และ

หลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินภาพรวม พบว่า ไม่มีหน่วยงานใดที่มีผลการประเมินประสิทธิภาพการควบคุมเป็นไปตามมาตรฐานการตรวจสอบที่กำหนด (สำนักงานการตรวจเงินแผ่นดิน, 2565) ดังนั้น ทุกวันนี้หลายองค์กรในประเทศไทยและทั่วโลก ได้พิจารณาถึง “Best Practices” หรือมาตรฐานที่ควรนำมาเป็นแนวทางในการเตรียมระบบสารสนเทศขององค์กรให้พร้อมเข้าสู่ยุค IT Governance โดยที่ “Best Practices” ที่นิยมใช้กันได้แก่ มาตรฐาน ISO/IEC27001: 2013 มาตรฐาน COBIT และมาตรฐาน COSO เป็นต้น เพื่อป้องกันความเสี่ยงตามมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งหน่วยงานจะต้องนำมาประยุกต์ใช้ในการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (ภาพร ภิยโยดิลกชัย, 2553; สุวันต์นา เสมอเนตร, 2562)

คณะแพทยศาสตร์ศิริราชพยาบาล เป็นหน่วยงานที่มีการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศที่ดี ซึ่งได้กำหนดขอบเขตเพื่อดำเนินการตามมาตรฐานที่กำหนด ครอบคลุมโครงสร้างพื้นฐานระบบสารสนเทศที่อยู่ภายในศูนย์ข้อมูลสารสนเทศ (Data Center) และกระบวนการทำงานควบคุม ตรวจสอบความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ให้มีกระบวนการและมาตรการในการรักษาความลับ ความถูกต้องครบถ้วน สอดคล้องตามข้อกำหนดของกฎหมายด้านธุรกรรมอิเล็กทรอนิกส์ จนผ่านการรับรองมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 รอบ Re – Certification Audit ประจำปี 2563 จากผลงานโครงการต่าง ๆ ได้แก่ 1) การกำหนดมาตรฐานความปลอดภัยทางไซเบอร์ (Cyber Security) 2) การพัฒนาและปรับปรุงระบบโครงสร้างสารสนเทศ (IT Infrastructure) 3) ต่อยอดพัฒนาโครงการจัดทำศูนย์สารสนเทศสำรองฉุกเฉินในการให้ความต่อเนื่องของการให้บริการผู้ป่วย 4) การสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ 5) การพัฒนาขยายต่อยอดการสื่อสารภายในองค์กรผ่านระบบ SivWork ซึ่งเป็นศูนย์กลางเชื่อมโยงระบบงานแอปพลิเคชันต่าง ๆ 6) การพัฒนาระบบ Work from Home เป็นต้น และได้รับรางวัลนวัตกรรมโครงการ เช่น การพัฒนาระบบ Siriraj Connect Application เป็นระบบดิจิทัลแพลตฟอร์มที่เชื่อมโยงข้อมูลการให้บริการสุขภาพในรูปแบบออนไลน์ผ่านโทรศัพท์มือถือ และการพัฒนาจัดทำและจัดเก็บใบเสร็จรับเงินรูปแบบอิเล็กทรอนิกส์ (e-Receipt) ด้านการรับชำระเงินรัฐบาล รางวัลเลิศรัฐ ประจำปี 2563 (คณะแพทยศาสตร์ศิริราชพยาบาล, 2563)

จากเหตุผลดังกล่าวข้างต้น และผลการศึกษาวิจัยที่ผ่านมาเกี่ยวกับการบริหารความเสี่ยง และความมั่นคงปลอดภัยด้านสารสนเทศ และองค์ประกอบการบริหารงานความมั่นคงปลอดภัยด้านสารสนเทศยังมีอยู่น้อย ดังนั้น ผู้วิจัยจึงมีความสนใจที่จะศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล เพื่อใช้เป็นแนวทางในการบริหารงานติดตาม ควบคุม และตรวจสอบระบบสารสนเทศให้เป็นไปตามมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ และสร้างการตระหนักรู้ความเข้าใจให้กับบุคลากรในหน่วยงาน รวมถึงยังป้องกันความเสี่ยงอันเกิดจากการปฏิบัติงานที่ใช้เทคโนโลยีสารสนเทศ และยังสามารถเป็นแบบอย่างที่ดีในการบริหารงานและการปฏิบัติงานของหน่วยงานภาครัฐให้มีความโปร่งใส ถูกต้อง รวดเร็ว และตรวจสอบได้ตามหลักการควบคุมภายใน อีกอย่างหนึ่งผลการศึกษานี้จะช่วยให้การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลมีประสิทธิภาพ ตลอดจนใช้เป็นแนวทางในการพัฒนาบุคลากรให้เข้าใจถึงความสำคัญของการบริหารจัดการ

ความมั่นคงปลอดภัยสารสนเทศ อีกทั้งยังเป็นประโยชน์ต่อหน่วยงานต่าง ๆ ทั้งภายในและภายนอกมหาวิทยาลัย และโรงพยาบาลศิริราช เพื่อช่วยสร้างคุณค่าให้แก่องค์กรนำไปสู่การเจริญเติบโตอย่างยั่งยืนต่อไปอีกด้วย

1.2 วัตถุประสงค์ของการศึกษา

เพื่อศึกษาถึงองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัย ด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 คณะแพทยศาสตร์ศิริราชพยาบาลได้มีแนวทาง และองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศสำหรับวางแผน กำกับ ติดตาม และควบคุมภายในของผลการปฏิบัติงานด้วยระบบข้อมูลสารสนเทศต่าง ๆ ให้สามารถดำเนินงานสอดคล้องกับกฎระเบียบ มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีประสิทธิภาพ

1.3.2 ผู้บริหารและหัวหน้าฝ่ายต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาลสามารถนำ องค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสนเทศ ไปปรับใช้ โดยการกำหนดนโยบายบริหารความมั่นคงปลอดภัยสารสนเทศ ของคณะแพทยศาสตร์ศิริราชพยาบาล และถ่ายทอดให้ผู้ปฏิบัติถือปฏิบัติได้

1.3.3 ผู้ปฏิบัติงานด้านต่าง ๆ สามารถนำองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลไปปรับใช้กับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามนโยบายที่กำหนด และปรับเปลี่ยนพฤติกรรมการทำงานให้ดียิ่งขึ้น

1.3.4 บุคลากรและหน่วยงานอื่นภายนอกคณะแพทยศาสตร์ศิริราชพยาบาล สามารถนำความรู้ที่ได้จากดำเนินงานการบริหารความมั่นคงปลอดภัยสารสนเทศของคณะแพทย์ศาสตร์ศิริราชพยาบาลไปประยุกต์ใช้ รวมถึงการแลกเปลี่ยนเรียนรู้ และสามารถนำข้อมูลสารสนเทศที่มีการเผยแพร่ไปใช้ประโยชน์เหมาะสมกับบริบทหน่วยงาน

1.4 ขอบเขตของงานวิจัย

1.4.1 ขอบเขตด้านเนื้อหา

ศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลในด้านกระบวนงานการกำกับดูแล และบริหารจัดการเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

1.4.2 ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

การศึกษาวิจัยนี้ กลุ่มประชากรที่ใช้ในการศึกษา เป็นเจ้าหน้าที่ผู้ปฏิบัติงานของคณะแพทยศาสตร์ศิริราชพยาบาล จำนวน 16,720 คน (ข้อมูล ณ วันที่ 31 มกราคม 2565) และผู้วิจัยได้คำนวณหากลุ่มตัวอย่างโดยใช้สูตรการคำนวณของ Taro Yamane (Yamane, 1973) มีค่าความเชื่อมั่น

ที่ 95% ดังนั้น จำนวนกลุ่มตัวอย่างที่คำนวณ จำนวน 320 คน และเพื่อให้ข้อมูลเกิดความน่าเชื่อถือ ผู้วิจัยจึงได้เก็บจำนวนกลุ่มตัวอย่าง จำนวน 400 คน

1.4.3 ตัวแปรที่ศึกษา

ตัวแปรที่ใช้ในการศึกษาจากการสังเคราะห์องค์ประกอบ โดยการศึกษา ทฤษฎี เอกสารและงานวิจัยที่เกี่ยวข้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศระดับสากล ได้แก่ ISO/IEC 27001: 20013 ISO/IEC 27001: 2005 และ COBIT 5 และเสนอให้กับผู้เชี่ยวชาญพิจารณา ตรวจสอบความสอดคล้อง และความเป็นไปได้ จำนวน 4 องค์ประกอบ 15 ตัวชี้วัด ดังนี้

องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย ตัวชี้วัดที่ 1 การกำกับดูแล (Governance) ตัวชี้วัดที่ 2 โครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ ตัวชี้วัดที่ 3 การบริหารจัดการทรัพย์สิน ตัวชี้วัดที่ 4 การติดตาม วัดผลและการประเมินผล ตัวชี้วัดที่ 5 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย และตัวชี้วัดที่ 6 ความสอดคล้องที่เกี่ยวข้องกับกฎหมายและการป้องกันในขั้นตอนต่าง ๆ

องค์ประกอบที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย ตัวชี้วัดที่ 1 การควบคุมการเข้าถึง ตัวชี้วัดที่ 2 ความมั่นคงปลอดภัยทางด้านกายภาพ สภาพแวดล้อม การดำเนินงาน และการสื่อสารข้อมูล ตัวชี้วัดที่ 3 การจัดหา การพัฒนา และการบำรุงรักษาระบบ ตัวชี้วัดที่ 4 ความสัมพันธ์กับผู้ให้บริการภายนอก และตัวชี้วัดที่ 5 การเข้ารหัสข้อมูล

องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย ตัวชี้วัดที่ 1 ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ และตัวชี้วัดที่ 2 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ ประกอบด้วย ตัวชี้วัดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ และตัวชี้วัดที่ 2 การบริหารจัดการกลยุทธ์ความมั่นคงปลอดภัยสารสนเทศ

1.5 คำนิยามศัพท์

ความมั่นคงปลอดภัยสารสนเทศ หมายถึง การดำเนินการที่เกี่ยวข้องกับข้อมูล ระบบ หรือการกระทำทั้งหมด เพื่อทำให้ข้อมูลหรือองค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลสารสนเทศในทุกรูปแบบเช่น การเข้าถึง การใช้งาน การเปิดเผย การทำลาย การดัดแปลง การขัดจังหวะ หรือการเผยแพร่สารสนเทศโดยไม่ได้รับอนุญาต ตลอดจนการตอบสนองภัยคุกคาม เพื่อให้เกิดความมั่นคงของสารสนเทศ ได้แก่ 1) ความลับ (Confidentiality) 2) บูรณภาพ (Integrity) 3) ความพร้อม (Availability) ทั้งนี้ได้มีการแบ่งกลุ่มและสิ่งที่เกี่ยวข้องกับความมั่นคงของสารสนเทศตามวัตถุประสงค์ของการใช้งานสารสนเทศ เช่น ความมั่นคงของสารสนเทศ ความมั่นคงของคอมพิวเตอร์ ความมั่นคงของเครือข่าย ความมั่นคงของแอปพลิเคชัน และความมั่นคงของไซเบอร์ เป็นต้น

การบริหารความมั่นคงปลอดภัยสารสนเทศ หมายถึง การดำเนินการด้านสารสนเทศ หรือ ระบบ Information Security Management System: ISMS ซึ่งรายละเอียดมุ่งเน้นกระบวนการที่สามารถใช้เป็นเกณฑ์สำหรับการนำไปใช้งานได้จริง และสามารถขอการรับรองได้ และเมื่อทำการเปรียบเทียบ ISMS ตามกระบวนการ PDCA มาพัฒนาเป็น 1) การวางแผน (Planning) 2) การดำเนินการ (Operation) 3) การประเมินประสิทธิภาพ (Performance Evaluation) และ 4) การปรับปรุง (Improvement)

องค์ประกอบของการบริหารจัดการความมั่นคงปลอดภัย ด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล หมายถึง การสังเคราะห์องค์ประกอบจากการศึกษา ทฤษฎี เอกสารและงานวิจัยที่เกี่ยวข้องกับมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศระดับสากล ได้แก่ ISO/IEC 27001:20013 ISO/IEC 27001: 2005 และ COBIT 5 และเสนอให้กับผู้เชี่ยวชาญช่วยตรวจสอบความสอดคล้อง และวิเคราะห์ข้อมูลทางสถิติที่สร้างองค์ประกอบจากตัวแปรหลาย ๆ ตัวแปรที่เกี่ยวข้องสัมพันธ์กันเป็นองค์ประกอบเดียวกัน ซึ่งเป็นเทคนิคทางสถิติสำหรับลดปริมาณข้อมูลให้ลดน้อยลง และเข้าใจง่ายและนำองค์ประกอบที่ได้มาปรับใช้กับการดำเนินงานเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศกับหน่วยงานที่สอดคล้องกับบริบทของประเทศไทย

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่องศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัย ด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลจะเป็นการสะท้อนมุมมองช่วยให้องค์กรมีความสามารถในการบริหารจัดการสารสนเทศขององค์กรให้มีความมั่นคงปลอดภัย โดยเริ่มตั้งแต่การวางแผน การกำกับดูแล การจัดหาหรือสร้างระบบสารสนเทศ การส่งมอบ การตรวจสอบ และดูแลทางด้านเทคโนโลยีของผู้ปฏิบัติงาน รวมทั้งเป็นคุ้มครองความลับ ความสมบูรณ์ และความพร้อมในการใช้งานระบบเทคโนโลยีดิจิทัล โดยการประยุกต์ใช้กระบวนการบริหารจัดการความเสี่ยง และการสร้างความเชื่อมั่นต่อลูกค้าและผู้มีส่วนเกี่ยวข้องว่ามีการบริหารจัดการความเสี่ยงอย่างเหมาะสม โดยผู้วิจัยได้ทำการค้นคว้าแนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง ดังนี้

2.1 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.1 ความหมายของความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.2 ศาสตร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.3 หลักการความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.4 การควบคุมภายในการตรวจสอบระบบงานข้อมูลสารสนเทศ และกฎหมายระเบียบด้านเทคโนโลยีสารสนเทศดิจิทัล

2.1.5 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.6 องค์ประกอบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ

2.2 การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

2.3 ทฤษฎีการวิเคราะห์องค์ประกอบ

2.4 กรอบแนวคิดงานวิจัย (Conceptual Framework)

2.1 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.1 ความหมายของความมั่นคงปลอดภัยด้านสารสนเทศ

คำว่า “สารสนเทศ” ปรากฏในเกือบทุกศาสตร์ แต่ความหมายของสารสนเทศอาจจะถูกนิยามไว้แตกต่างกัน ตัวอย่าง เช่น พจนานุกรรมภาษาอังกฤษออนไลน์ของมหาวิทยาลัยออกฟอร์ด ให้ความหมายของสารสนเทศ (Information) ว่า คือ การกำหนด การเรียนรู้ข้อเท็จจริงเกี่ยวกับบางสิ่งหรือบางคน และด้านการจัดการเทคโนโลยีสารสนเทศ หมายถึง ผลจากข้อมูลที่เป็นรายละเอียดมาประมวลผลให้ได้ข้อสรุปที่ทำให้เห็นภาพของเหตุการณ์ที่เกิดขึ้นได้อย่างชัดเจน (ประสิทธิ์ ทีฆพุฒิ และ ครรชิต มาลัยวงศ์, 2549) ในขณะเดียวกัน ความมั่นคง (Security) เป็นคุณภาพที่ถูกรับรู้และถูกนิยามไว้แตกต่างกัน ตัวอย่างเช่น พจนานุกรมภาษาอังกฤษออนไลน์ของ มหาวิทยาลัยออกฟอร์ด ได้นิยามความหมายของคำว่าความมั่นคงหรือความมั่นคงในลักษณะความรู้สึกว่าเป็นสถานะที่ปลอดจากอันตรายหรือภัยคุกคาม (The state of being free from danger or

threat) ในขณะที่สถาบันฝึกอบรมและให้ความรู้เกี่ยวกับระบบการบริหาร เครือข่าย และความมั่นคงปลอดภัย หรือ SANS (System Administration, Networking, and Security Institute) ได้นิยามความมั่นคงของสารสนเทศ ไว้ คือกระบวนการหรือวิธีการที่ถูกออกแบบและประยุกต์ใช้เพื่อป้องกันข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรืออ่อนไหวต่อความรู้สึกในรูปแบบต่าง ๆ เช่น เอกสาร หรืออิเล็กทรอนิกส์ จากการเข้าถึงใน การใช้งาน การเปิดเผย การทำลาย การดัดแปลง การขัดจังหวะ และไม่ได้รับอนุญาต

ดังนั้น ความมั่นคงปลอดภัยด้านสารสนเทศ จึงเป็นวิธีการ กระบวนการของการประเมินที่ต้องใช้ความรอบคอบเพื่อปกป้องระบบข้อมูลสารสนเทศจากภัยคุกคาม เช่น การเข้าถึง การใช้งานการเปิดเผย การทำลาย การดัดแปลง การขัดจังหวะ หรือการเผยแพร่สารสนเทศโดยไม่ได้รับอนุญาต ตลอดจนการตอบสนองภัยคุกคาม เพื่อให้สารสนเทศอยู่ในสถานะที่ปลอดจากสิ่งที่ส่งผลกับความรู้สึก มั่นคงของผู้มีส่วนเกี่ยวข้องกับสารสนเทศนั้น ในตำรานี้ คำว่าความมั่นคงจะถูกใช้แทนความหมายของคำว่า Security ในขณะที่ความปลอดภัยจะใช้แทนความหมายของคำว่า Safety เพื่อไม่ให้เกิดความสับสน ทั้งนี้ได้มีการแบ่งกลุ่มและสิ่งที่เกี่ยวข้องกับความมั่นคงของสารสนเทศไว้หลากหลาย จึงสามารถถูกจำแนกตามขอบเขต สภาพแวดล้อม และวัตถุประสงค์ของการใช้งาน เช่น ความมั่นคงด้านข้อมูลสารสนเทศ ความมั่นคงของระบบคอมพิวเตอร์และเครือข่าย ความมั่นคงของแอปพลิเคชัน และความมั่นคงของไซเบอร์

2.1.2 ศาสตร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อมูลและสารสนเทศอาจถูกจำแนกไว้แตกต่างกัน โดย “ข้อมูล” หมายถึง ข้อเท็จจริงที่เป็นตัวเลข ข้อความ ภาพ เสียง ที่ถูกจัดเก็บรวบรวมอย่างต่อเนื่อง ในขณะที่ “สารสนเทศ” หมายถึง การประมวลผลข้อมูล และสามารถนำไปใช้เป็นแนวทางในการตัดสินใจและการดำเนินชีวิต ซึ่งข้อมูลและสารสนเทศยังสามารถถูกจำแนกในรูปแบบของการจัดเก็บและประมวลผล เช่น ออฟไลน์ (Offline) หรือ ออนไลน์ (Online) เป็นต้น เนื่องจากข้อมูลและสารสนเทศในโลกดิจิทัลได้ถูกประมวลผลโดยระบบสารสนเทศและส่งผ่านระบบเครือข่ายและจัดเก็บในโหนดต่าง ๆ เช่น ระบบคอมพิวเตอร์ อุปกรณ์เคลื่อนที่ เครื่องแม่ข่าย เป็นต้น มีรายละเอียด (An dress, 2014; Stallings & Brown, 2018) ดังนี้

1. ความมั่นคงของข้อมูลสารสนเทศดิจิทัล (Digital Data & Information Security) เกี่ยวข้องกับมาตรการที่ใช้เพื่อปกป้อง ข้อมูลสารสนเทศขององค์กรในภาพรวมสำหรับการเข้าถึงโดยไม่ได้รับอนุญาตที่อาจส่งผลกระทบต่อข้อมูลความลับ (Confidentiality) บูรณภาพ (Integrity) และความพร้อมสำหรับการใช้งานสารสนเทศ (Availability) ซึ่งความต้องการทั้ง 3 นี้ถูกเรียกในภาพรวมว่า CIA และเป็นองค์ประกอบที่สำคัญและจำเป็นสำหรับองค์กรสำหรับการ รักษาความมั่นคงในด้านอื่น ๆ เช่น ความมั่นคงของไซเบอร์ ความมั่นคงของเครือข่ายคอมพิวเตอร์ และความมั่นคงของแอปพลิเคชัน เป็นต้น

2. ความมั่นคงของคอมพิวเตอร์ (Computer Security) เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยอุปกรณ์ที่ใช้และประมวลผลสารสนเทศ เช่น เครื่องคอมพิวเตอร์และแม่ข่าย ระบบปฏิบัติการเสมือนและอุปกรณ์เคลื่อนที่ โดยความมั่นคงของคอมพิวเตอร์จะมุ่งเน้นที่การป้องกันซอฟต์แวร์ อันตรายรวมถึงการจัดการช่องโหว่ที่อาจเปิดโอกาสให้กับภัยคุกคามที่ส่งผลต่อ CIA ของข้อมูลสารสนเทศในคอมพิวเตอร์

3. ความมั่นคงของเครือข่าย (Network Security) เกี่ยวข้องกับมาตรการที่องค์กรใช้ในการรักษาความมั่นคงของเครือข่ายคอมพิวเตอร์โดยใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ โดยมีจุดมุ่งหมายเพื่อรักษา CIA ของข้อมูลสารสนเทศในระบบเครือข่าย นอกเหนือจากนี้ ความมั่นคงของเครือข่ายยัง ครอบคลุมถึงความต้องการในด้านอื่น ๆ เช่น การควบคุมการเข้าถึง การพิสูจน์สิทธิ์ เป็นต้น ในปัจจุบันองค์กรเกือบทุกแห่งที่บริหารจัดการข้อมูลจำนวนมากจะมีมาตรการในการต่อต้านภัยคุกคามต่อความมั่นคงของเครือข่ายที่แตกต่างกัน ดังนั้น ความมั่นคงของเครือข่ายเป็นการป้องกันสื่อและเทคโนโลยีสำหรับการติดต่อสื่อสารที่เกี่ยวข้องกับองค์ประกอบการเชื่อมต่อ และข้อมูลของแม่ข่ายคอมพิวเตอร์ ซึ่งภัยคุกคามทางไซเบอร์หลายประเภทสามารถถูกจัดอยู่ในความมั่นคงของเครือข่าย เนื่องจากขอบเขตการทำงานที่มีความสัมพันธ์กัน

4. ความมั่นคงของแอปพลิเคชัน (Application Security) เกี่ยวข้องกับมาตรการความมั่นคงของแอปพลิเคชันที่มีจุดมุ่งหมายเพื่อป้องกันไม่ให้ข้อมูลหรือรหัสโค้ดภายในแอปพลิเคชันถูกขโมยหรือถูกแย่งชิงไป รวมถึงการป้องกันการโจมตีในรูปแบบต่าง ๆ เช่น การใช้ซอฟต์แวร์อันตราย การใช้ประโยชน์จากช่องโหว่หรือข้อบกพร่องของซอฟต์แวร์การโจมตีรหัสผ่านเพื่อเข้าใช้ซอฟต์แวร์เป็นต้น ดังนั้น ความมั่นคงของแอปพลิเคชันยังเกี่ยวข้องกับกระบวนการในการพัฒนาการเพิ่ม และการทดสอบคุณลักษณะของความมั่นคงภายในแอปพลิเคชันเพื่อป้องกันช่องโหว่ด้านความปลอดภัยจากภัยคุกคาม เช่น การควบคุมสำหรับการเข้าถึง (Access Control) การตรวจสอบพิสูจน์สิทธิ์ (Authentication) การอนุญาต (Authorization) ความรับผิดชอบ (Accountability) เป็นต้น ดังนั้น ความมั่นคงของแอปพลิเคชันจึงครอบคลุมตั้งแต่อุปกรณ์ปลายทางและอุปกรณ์ที่บริหารจัดการเครือข่าย

5. ความมั่นคงของไซเบอร์ (Cyber Security) เกี่ยวข้องกับมาตรการการป้องกันภัยคุกคามบนโลกอินเทอร์เน็ตที่ปัจจุบันกลายเป็นช่องทางการสื่อสารและให้บริการผ่านเว็บเซอร์วิสในรูปแบบต่าง ๆ เช่น รัฐบาลดิจิทัล ธุรกิจดิจิทัล สื่อสังคมออนไลน์ ซึ่งภัยคุกคามทางไซเบอร์ครอบคลุมตั้งแต่ไวรัส คอมพิวเตอร์การละเมิดข้อมูล การโจมตีแบบปฏิเสธบริการ (DoS) และการโจมตีรูปแบบอื่นที่เป็น อันตรายที่พยายามสร้างความเสียหายให้กับข้อมูล ขโมยข้อมูล หรือขัดขวางชีวิตดิจิทัลโดยทั่วไป ซึ่งมีจุดมุ่งหมายเพื่อการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต การทำลาย/สร้างความเสียหาย ขัดขวาง หรือขโมยสินทรัพย์ดิจิทัลบนเครือข่ายอินเทอร์เน็ต เช่น ทรัพย์สินทาง ปัญญา ข้อมูลทางการเงิน ข้อมูลส่วนบุคคล หรือข้อมูลที่อ่อนไหวต่อความรู้สึก

นอกเหนือจากศาสตร์ของความมั่นคงปลอดภัยสารสนเทศอาจสามารถถูกจำแนกตามอุปกรณ์สื่อสารหรือชื่ออื่นที่มีความหมายใกล้เคียงกัน เช่น ความมั่นคงของอุปกรณ์เคลื่อนที่ (Mobile Security) ความมั่นคงของซอฟต์แวร์ (Software Security) เป็นต้น ดังนั้น ศาสตร์ของความมั่นคงปลอดภัยสารสนเทศ จะนิยามคำศัพท์ข้างต้น โดยทั่วไปที่เกี่ยวข้องกับข้อมูล ระบบ หรือการกระทำเพื่อทำให้ข้อมูลสารสนเทศปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลสารสนเทศในทุกรูปแบบ ตลอดจนอาชญากรรมและถูกโจมตีในรูปแบบต่าง ๆ และปัจจุบันการรักษาระบบข้อมูลสารสนเทศทางอินเทอร์เน็ตหรือระบบออนไลน์ให้ปลอดภัย เพื่อสร้างภูมิคุ้มกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ สำหรับการทำธุรกรรมในรูปแบบอิเล็กทรอนิกส์ รวมถึงการรักษาความมั่นคงปลอดภัยทางโลกดิจิทัล ซึ่งมีความเกี่ยวข้องกับการรักษาความลับของข้อมูล

และควบคุมการทำรายการผ่านระบบออนไลน์ การป้องกัน การละเมิดข้อมูล รวมถึงมาตรฐาน วิธีการ รักษาความปลอดภัย สร้างความเชื่อมั่นของผู้ใช้ด้วยข้อมูลที่ที่มากขึ้นผ่านช่องทางดิจิทัลที่มีความปลอดภัย และการคุ้มครองความเป็นส่วนตัวอำนวยความสะดวกในการเข้าถึงระบบของผู้ใช้งานแต่ละบุคคลด้วย ทั้งนี้การมุ่งเน้นรักษาความมั่นคงปลอดภัยในระดับชาติ อาจทำให้เกิดการลุกล้ำความเป็นส่วนตัวของบุคคล ซึ่งเป็นสิ่งจำเป็นที่จะต้องรักษาสมดุลระหว่างความมั่นคงปลอดภัยด้านสารสนเทศ การคุ้มครองความเป็นส่วนตัว และการเข้าถึงระบบให้เหมาะสม โดยจะเห็นได้ว่าไม่ได้มุ่งเฉพาะความมั่นคงของความปลอดภัยในระบบสารสนเทศและเครือข่าย ที่ส่งผลต่อความมั่นคงทางเศรษฐกิจ ทางการเมือง และการทหาร เป็นต้น

2.1.3 หลักการความมั่นคงปลอดภัยด้านสารสนเทศ

หลักการ แนวคิดความมั่นคงปลอดภัยด้านสารสนเทศ เป็นคำที่ใช้โดยทั่วไปในการคุ้มครองความลับ ความสมบูรณ์ และความพร้อมใช้งานต่อการเข้าถึงบางสิ่งบางอย่างที่ได้รับการควบคุมการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ทรัพย์สินจะได้รับความปลอดภัยเมื่อมีความคุ้มครองจากการบุกรุกจากผู้ที่ไม่พึงประสงค์ไม่ว่าจะใช้ระบบทางกายภาพ หรือกลไกทางอิเล็กทรอนิกส์บางอย่างที่ห้ามผู้ที่ไม่มีกุญแจหรือไม่ได้รับอนุญาตให้เข้าได้ ซึ่งนักวิชาการและนักปฏิบัติได้สร้างโมเดลความต้องการความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้ในการวิเคราะห์ และประเมินผล เช่น CIA, PAIN, 3A, Parkerian Hexad และ CIAAN เป็นต้น แต่ที่เป้าหมายสำคัญ และเป็นที่ต้องการในการดำเนินกิจกรรมต่าง ๆ โดยใช้หลักการ และความต้องการด้านความมั่นคงของสารสนเทศเป็นโมเดลตามแผน และทิศทางที่กำหนด รวมถึงการกำกับ ติดตาม และประเมินผล แต่จากสถานการณ์ในโลกปัจจุบันที่เทคโนโลยีดิจิทัล และข้อมูลสารสนเทศมีการจัดทำ รวบรวมและจัดเก็บข้อมูลในรูปแบบดิจิทัลที่เพิ่มขึ้น รวมถึงมีความก้าวหน้าและซับซ้อนมากขึ้น และศาสตร์ที่เกี่ยวข้องกับความมั่นคงของสารสนเทศจึงสามารถถูกจำแนกตามขอบเขต สภาพแวดล้อม และวัตถุประสงค์ของการใช้งานด้านสารสนเทศ เช่น ความมั่นคงของไซเบอร์ ข้อมูลสารสนเทศ เครือข่าย เป็นต้น ซึ่งมาตรการรักษาความมั่นคงของสารสนเทศส่วนมากจะใช้หลักการความต้องการของโมเดล CIA ได้แก่ 1) ความลับ (Confidentiality) 2) บูรณภาพ (Integrity) และ 3) ความพร้อม (Availability) ของข้อมูลสารสนเทศ นอกเหนือจากนี้ ยังมีโมเดลความต้องการด้านความมั่นคงของสารสนเทศอื่น ๆ ที่มีความเหมาะสมกับสถานการณ์ เช่น PAIN ที่เพิ่มความต้องการความเป็นส่วนตัว (Privacy) การตรวจสอบพิสูจน์สิทธิ์ (Authentication) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) เพิ่มเติมจากหลักการของ CIA ซึ่งมีความสำคัญในการทำธุรกรรมอิเล็กทรอนิกส์ที่ผู้ขายและผู้ซื้อต้องมีการพิสูจน์สิทธิ์ โดยผู้ขายห้ามปฏิเสธในการส่งสินค้าให้กับผู้ซื้อ และผู้ซื้อห้ามปฏิเสธการสั่งซื้อสินค้าจากผู้ซื้อ และถูกสร้างการยอมรับในวงการวิชาการถูกเข้าใจในชื่อย่อว่า CIA ซึ่งมีหลักการสำคัญ 3 ประการ รายละเอียดดังนี้ (Ghosh, 1998; Stamp, 2006; Stein, 1998)

1. เพื่อรักษาความลับ (Confidentiality) โดยการทำให้เจ้าของหรือผู้ใช้งานระบบคอมพิวเตอร์เกิดความมั่นใจได้ว่า ระบบจะถูกเก็บเป็นความลับ และจะมีเพียงบุคคลที่ได้รับอนุญาตจากผู้แลความมั่นคงปลอดภัยที่จะสามารถเข้าถึง (Access) เพื่อกระทำการใด ๆ กับระบบคอมพิวเตอร์และเครือข่าย บางครั้งเรียกว่า การรักษาความเป็นส่วนตัว (Privacy) บ่อยครั้งที่พบข้อความประกาศว่า บุคคลหรือระบบที่ได้รับอนุญาตจึงจะสามารถเข้าถึงข้อมูลที่ถูกป้องกันไว้ได้ (Authorized) ดังนั้น การรักษาความลับเป็นหลักการและ

สิ่งสำคัญในการความเชื่อถือให้กับเจ้าของข้อมูล และการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์และเครือข่ายที่สามารถเข้าใจได้ง่ายกว่าหลักการด้านอื่น ๆ เช่น ตัวอย่างรหัสผ่าน (PIN) ที่ให้ผู้อื่นเพื่อเข้าถึงบัญชีหรือเข้าใช้งานข้อมูลของหน่วยงานกับผู้ที่ไม่ประสงค์ดีส่งผลอย่างมากต่อองค์กรที่มีความเสี่ยงการสูญเสียข้อมูลที่เป็นความลับที่ส่วนบุคคล

ดังนั้น การรักษาความลับ คือ การคุ้มครองข้อมูลที่มีความอ่อนไหวทุกประเภท ข้อมูลที่เกี่ยวข้องกับแหล่งกำเนิด จริยธรรม เชื้อชาติ การเมือง ศาสนาหรือปรัชญา สุขภาพ หรือวิถีชีวิตทางเพศถือว่าสมควรได้รับการพิจารณาเป็นความลับ ในทางธุรกิจการรักษาความลับหมายถึงการเก็บข้อมูลลูกค้าอย่างมิดชิดและไม่เปิดเผยต่อผู้อื่น รวมถึงเพื่อนร่วมงาน เพื่อน ครอบครัว ของลูกค้า เว้นแต่จะได้รับอนุญาตจากลูกค้า ตัวอย่างการรักษาความลับ ได้แก่ การใช้วิทยาการรหัสลับเพื่อเข้ารหัสข้อมูล การไม่เปิดเผยต่อผู้อื่นว่ามีข้อมูลใดอยู่ในไฟล์ของลูกค้าเว้นแต่พวกเขาจะได้รับอนุญาตจากลูกค้า การไม่ถูกบอกข้อมูลลูกค้ากับบุคคลที่ลูกค้าไม่อนุญาตถือว่าเป็นการคุกคามต่อความต้องการด้านความลับ

2. เพื่อรักษาความครบถ้วนสมบูรณ์หรือความเป็นบูรณภาพ (Integrity) โดยการทำให้เจ้าของหรือผู้ใช้ระบบงานคอมพิวเตอร์เกิดความมั่นใจว่าจะไม่ถูกกระทำการใด ๆ เกิดการแก้ไขปรับปรุง การลบ การสร้างใหม่ เปลี่ยนแปลง (Modify) โดยบุคคลหรือวิธีการใด ๆ ที่ไม่ได้รับอนุญาตจากผู้ดูแลความมั่นคงปลอดภัย การทำให้ความครบถ้วนสมบูรณ์ของระบบคงอยู่ อาจหมายถึง ความแม่นยำ (Precise) ความถูกต้อง (Accurate) ความสอดคล้อง (Consistent) ไม่เปลี่ยนแปลง (Unmodified) เปลี่ยนแปลงโดยวิธีที่ยอมรับได้ เปลี่ยนแปลงโดยบุคคลที่ได้รับอนุญาต หรือเปลี่ยนแปลงโดยกระบวนการที่ได้รับอนุญาต

ดังนั้น ความเป็นบูรณภาพของแหล่งที่มา (Source Integrity) คือ การรับรองว่าสถานะของผู้ส่งข้อมูลจะไม่มีการเปลี่ยนแปลง สร้างความเชื่อมั่นให้กับผู้ที่เกี่ยวข้องกับข้อมูลนั้น และการรักษาความเป็นบูรณภาพของข้อมูลหมายถึงการปกป้องข้อมูลจากการถูกแก้ไขโดยบุคคลที่ไม่ได้รับอนุญาต เช่น ข้อมูลส่วนบุคคล ผลการศึกษา เอกสารทางราชการข้อมูลทางการเงิน ฯลฯ ในทางธุรกิจการขาดความเป็นบูรณภาพของข้อมูล เช่น การที่ข้อมูลถูกดัดแปลงแก้ไขอาจส่งผลต่อธุรกิจ และความเชื่อมั่นของลูกค้า อาทิเช่น หากข้อมูลการชำระเงินหรือประวัติของลูกค้าถูกเปลี่ยนแปลงและไม่ได้รับอนุญาต ซึ่งการปลอมแปลงแหล่งที่มาของข้อมูลถือว่าเป็นภัยคุกคามต่อบูรณภาพของแหล่งที่มาของข้อมูล ซึ่งวิทยาการรหัสลับเป็นสิ่งสำคัญสำคัญที่ต้องสร้างความน่าเชื่อถือด้านความเป็นบูรณภาพของข้อมูล การแฮชข้อมูลหรือการสร้างข้อมูลย่อยจากข้อความต้นฉบับคือวิธีการที่ใช้กันทั่วไปเพื่อปกป้องความถูกต้องของข้อมูล โดยข้อความเดียวกันเมื่อถูกย่อยหรือบีบอัดต้องให้ข้อมูลย่อยที่เหมือนเดิมทุกครั้ง

3. เพื่อรักษาสภาพพร้อมใช้งาน (Availability) โดยการเข้าถึงสารสนเทศเมื่อมีความพร้อมตามที่เจ้าของหรือผู้ใช้ที่มีสิทธิ์เข้าถึงข้อมูล ซึ่งหมายความว่าระบบสารสนเทศต้องมีความพร้อมในการให้บริการทำการร้องขอ เพื่อทำให้ผู้ใช้ระบบรู้สึกมั่นคงว่าข้อมูลสารสนเทศสามารถพร้อมตอบสนองความต้องการของผู้ใช้ระบบเมื่อเวลาใดก็ตาม ความไม่พร้อมของระบบสารสนเทศสามารถสร้างความรู้สึกที่ไม่ดีต่าง ๆ ที่เป็นผลพวงจากความรู้สึกไม่มั่นคงของผู้ใช้ระบบ และอาจทำให้ผู้ใช้ระบบเลี่ยงไปใช้บริการจากระบบสารสนเทศที่เป็นคู่แข่งขัน ซึ่งทุกวันนี้การปฏิเสธการเข้าถึงข้อมูลกลายเป็นภัยคุกคามที่พบเป็นประจำ เว็บไซต์ที่มีชื่อเสียงกลายเป็นเป้าหมายหลักของการโจมตีที่มุ่งหวังไม่ให้เว็บไซต์เหล่านั้นให้บริการต่อไปได้ ซึ่งการหยุดทำงานของเว็บไซต์ที่มีการซื้อขายจำนวนมากอาจ

ทำให้ธุรกิจของเว็บไซต์นั้นขาดรายได้จำนวนมหาศาล และอาจรวมถึงอุบัติเหตุหรือภัยธรรมชาติ เช่น ไฟดับ ไฟไหม้ น้ำท่วม แผ่นดินไหว ฯลฯ ตัวอย่างการรักษาความพร้อมของข้อมูล อาทิ การสำรองข้อมูลที่ถือว่าเป็นวิธีการสำคัญที่สนับสนุนให้ข้อมูลนั้นมีความพร้อมใช้หากข้อมูลปัจจุบันได้รับผลกระทบ การสำรองข้อมูลนอกสถานที่เป็นประจำสามารถลดความเสียหายต่อความพร้อมของข้อมูลที่เกิดจากความเสียหายจากภัยธรรมชาติ ดังภาพที่ 2.1

ภาพที่ 2.1 ความต้องการด้านความมั่นคงของสารสนเทศตามหลัก CIA Triad

ที่มา: พิทา จารุพูนพล (2564)

2.1.4 การควบคุมภายใน การตรวจสอบระบบงานข้อมูลสารสนเทศ กฎหมายระเบียบด้านเทคโนโลยีสารสนเทศดิจิทัล

2.1.4.1 การควบคุมภายใน ด้านเทคโนโลยีสารสนเทศ

การควบคุมภายใน หมายถึง กระบวนการ วิธีการที่กำหนดให้มีขึ้นเพื่อให้เกิดความมั่นใจในการดำเนินงานตามวัตถุประสงค์ ได้แก่ 1) การปฏิบัติตามกฎหมาย และระเบียบข้อบังคับโดยเฉพาะการควบคุมภายในด้านเทคโนโลยีสารสนเทศ 2) ความเชื่อถือได้ของการรายงานทางการเงิน และ 3) ประสิทธิผล และประสิทธิภาพของการดำเนินงาน ทั้งนี้ การควบคุมภายในด้านเทคโนโลยีสารสนเทศก็ยังเป็นวิธีการ และเครื่องมือโดยคณะกรรมการ ฝ่ายบริหาร และผู้ที่อยู่ภายใต้การควบคุมของฝ่ายบริหาร เพื่อจัดทำให้มั่นใจว่า บรรลุวัตถุประสงค์ในด้านต่าง ๆ ได้แก่ 1) การคุ้มครองป้องกันสินทรัพย์ ประกอบด้วย ป้องกัน ตรวจพบจากการใช้โดยผู้ไม่มีหน้าที่ได้อย่างทันท่วงที 2) การรักษาไว้ซึ่งรายการที่บันทึกสินทรัพย์ให้มีรายละเอียดอย่างเพียงพอ 3) การจัดเตรียมสารสนเทศที่ถูกต้องแม่นยำและเชื่อถือได้ 4) การจัดทำรายงานทางการเงินตามหลักการบัญชีที่รับรองทั่วไป 5) การส่งเสริมและพัฒนากระบวนงานรายได้และค่าใช้จ่ายมีผู้มีอำนาจเป็นผู้สั่งการ อย่างมีประสิทธิภาพและ 6) กระตุ้นให้เกิดการยึดมั่นในการกำหนดนโยบายการบริหาร ซึ่งการควบคุมภายในของระบบสารสนเทศ แบ่งออกเป็น 2 ประเภท (ครรชิต มาลัยวงศ์, 2554) ดังนี้

(1) การควบคุมทั่วไป (General Control) การควบคุมการบริหาร อุปกรณ์เทคโนโลยีสารสนเทศ และการจัดการความปลอดภัย

(2) การควบคุมระบบงาน (Application Control) เป็นการป้องกัน ตรวจพบ และแก้ไขความผิดพลาดของรายการค้าและการทุจริตของข้อมูลในระบบ ตั้งแต่การบันทึกเข้า การวิเคราะห์/ประมวลผล การรวบรวม/จัดเก็บ การส่งต่อเชื่อมโยงไประบบอื่น และการรายงานผลการควบคุมภายในดังกล่าว มีกรอบงานการควบคุมที่สำคัญ 3 กรอบงาน ดังนี้

(2.1) กรอบงาน COBIT (Control Objectives for Information and related Technology) ได้รับการพัฒนาจาก สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ ซึ่งเป็นกรอบงานความปลอดภัยของข้อมูลในระบบสารสนเทศและแนวปฏิบัติทางด้านเทคโนโลยีสารสนเทศ ซึ่งกรอบนี้จะช่วยสนับสนุนฝ่ายบริหารในการควบคุมความเสี่ยงและสารสนเทศ เพื่อสร้างความมั่นใจให้กับผู้ใช้งานด้านการรักษาความปลอดภัย

(2.2) กรอบงานการควบคุมภายในของ COSO มีองค์ประกอบที่ต้องพิจารณา 5 หัวข้อ คือ สภาพแวดล้อมการควบคุม (Control Environment) การประเมินผลความเสี่ยง (Risk Assessment) กิจกรรมการควบคุม (Control Activities) การสื่อสารและข้อมูลสารสนเทศ (Information and communication) และการติดตามและประเมินผล (Monitoring & Assessment)

(2.3) กรอบงานการบริหารความเสี่ยงทั่วทั้งองค์กร (Risk Management)

2.1.4.2 การตรวจสอบระบบงานสารสนเทศ

การตรวจสอบ หมายถึง กระบวนการให้ความเชื่อมั่นและการให้คำปรึกษา (Assurance & Consulting) เพื่อความเที่ยงธรรมและเป็นอิสระ เพิ่มคุณค่า และปรับปรุงการปฏิบัติงานของหน่วยงานให้ดีขึ้น บรรลุถึงเป้าหมายที่กำหนด โดยการประเมินและปรับปรุงกระบวนการบริหารความเสี่ยง การควบคุมและการกำกับดูแลอย่างเป็นระบบ มีวัตถุประสงค์ เพื่อช่วยผู้ปฏิบัติงานในองค์กรสามารถทำงานได้ตามหน้าที่ ภารกิจความรับผิดชอบอย่างมีประสิทธิภาพและเกิดประสิทธิผลภายใต้ค่าใช้จ่ายที่เหมาะสม โดยเฉพาะการควบคุมตรวจสอบของระบบงานด้านเทคโนโลยีสารสนเทศ รวมถึงมีนักวิชาการได้ให้ความหมายคำว่าการตรวจสอบ คือ กิจกรรมที่หน่วยงานต้องการควบคุมภายในสารสนเทศ (Audit IT) สำหรับการดำเนินงานให้เป็นไปตามวัตถุประสงค์กำหนดไว้หรือไม่ และวัตถุประสงค์ของการควบคุมของผู้บริหารหรือผู้ออกแบบระบบสามารถตรวจสอบเพื่อให้มั่นใจว่าระบบที่ออกแบบไว้นั้นยังคงเพียงพอ เหมาะสมและได้ผลตามวัตถุประสงค์ที่กำหนดไว้อย่างไรหรือไม่ รวมถึงเป็นกระบวนการรวบรวม และการประเมินหลักฐานสำหรับการพิจารณาถึงการนำคอมพิวเตอร์มาใช้เพื่อช่วยดูแลรักษาสินทรัพย์และความถูกต้องของข้อมูลซึ่งช่วยให้บรรลุเป้าหมายอย่างมีประสิทธิผล และใช้ทรัพยากรอย่างคุ้มค่าและมีประสิทธิภาพ ซึ่งขอบเขตการตรวจสอบมีดังต่อไปนี้ (อุษณา ภัทรมนตรี, 2547; อุทัยวรรณ จรุงวิภู, 2550; ครรชิต มาลัยวงศ์, 2554)

(1) การควบคุมเบื้องต้น คือ การตรวจสอบว่าผู้บริหารของหน่วยงานมีความสนใจในเรื่องการวางแผน การกำหนดกลยุทธ์และทิศทาง งบประมาณ นโยบายด้านการซื้อ License หรือการใช้

Software และการควบคุม เป็นต้น โดยการตรวจสอบจากนโยบายเกี่ยวกับการใช้เทคโนโลยีดิจิทัล และการวัดผลการประเมินความเสี่ยง ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตามกฎระเบียบ

(2) การปฏิบัติงานของศูนย์ไอที คือ การพิจารณาเงื่อนไขทางด้านกายภาพและสิ่งแวดล้อม เช่น มีการวางแผนสมรรถนะและความพร้อมให้บริการ ระบบพลังงาน ภัยคุกคามจากมนุษย์ ความมั่นคงทางกายภาพและธรรมชาติ มีขั้นตอนการกู้ระบบและการให้บริการยามฉุกเฉิน การสำรองข้อมูลทั้งใน และนอกสถานที่ตั้ง และมีการวางแผนการกู้ระบบ และการวางแผนปฏิบัติงานอย่างต่อเนื่อง

(3) โครงสร้างเครือข่ายและอุปกรณ์ คือ การพิจารณา ตรวจสอบอุปกรณ์ต่าง ๆ เช่น การประเมินโครงสร้างระบบ (configuration) และการกู้ระบบ ตรวจสอบเรื่องความมั่นคง และการกำกับดูแลความมั่นคงทางกายภาพ มีการวิเคราะห์ระบบการตรวจจับ รวมถึง Router, Switch, Firewall และอุปกรณ์อื่น ๆ พร้อมงานประยุกต์ เป็นต้น

(4) บริหารอุปกรณ์พกพาและระบบไร้สายและ (Mobile) คือ การตรวจสอบระบบการกำหนดนโยบาย สถานภาพ และสอบทานวิธีการเข้ารหัสลับสำหรับงานอุปกรณ์พกพา เครือข่ายสนับสนุนงานอุปกรณ์พกพาและความมั่นคงด้านสารสนเทศ มีการประเมินจุดให้บริการ และความพอเพียงของสัญญาณ

(5) ระบบปฏิบัติการ คือ การบริหารระบบปฏิบัติการตามนโยบายบริหารความมั่นคงปลอดภัยสารสนเทศ การซ่อมแซมโปรแกรม มีการปิดกั้นการให้บริการและไม่ยอมให้งานบริการไม่จำเป็น มีการบันทึกการใช้งานและการประเมินการใช้งาน เช่น มีนโยบายกลุ่ม การบริหารรหัสผ่าน การบริหารการแบ่งกันใช้ข้อมูล เป็นต้น

(6) ระบบสารสนเทศและฐานข้อมูล คือ การประเมินงานประยุกต์ ได้แก่ การใช้งานและการปรับให้เป็นปัจจุบัน (Update) การตรวจสอบสิทธิ์ในการใช้ (License) และมีการวิเคราะห์เครื่องบริการฐานข้อมูล (Database server) เช่น การตรวจสอบความมั่นคงและการใช้งาน การบันทึกการใช้งานและความมั่นคง การตรวจสอบเว็บและการประยุกต์อิงอินเทอร์เน็ต และการตรวจสอบการฝึกอบรมผู้ใช้ทางด้านการใช้อินเทอร์เน็ต และอีเมล เป็นต้น

(7) การดำเนินงานโครงการ คือ การตรวจสอบกระบวนการ และข้อกำหนดความต้องการของระบบใหม่ การจัดการความเปลี่ยนแปลง และการตรวจสอบเอกสารของระบบ มีการประเมินการทดสอบโครงการ และตรวจสอบการวางแผนความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณารายละเอียดแผนงาน โครงการ ระยะเวลา งบประมาณ กับรายงานในโครงการว่าสอดคล้องน่าเชื่อถือหรือไม่

กล่าวโดยสรุปว่า การตรวจสอบระบบสารสนเทศ เป็นวิธีการสนับสนุนวัตถุประสงค์การตรวจแบบเดิม (Traditional Auditing) ซึ่งจะเน้นการบริการ การดูแลรักษาสินทรัพย์ให้ปลอดภัย และความครบถ้วน ถูกต้องของข้อมูลให้มีประสิทธิภาพและประสิทธิผล รวมถึงให้ความเชื่อมั่นว่าองค์กร ได้ปฏิบัติตามนโยบาย แผนงาน หรือเงื่อนไขของกฎหมาย ระเบียบและข้อบังคับ

2.1.4.3 กฎหมายและระเบียบด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

(1) พระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

กฎหมายมีวัตถุประสงค์เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ได้อย่างถูกต้องปลอดภัยของสารสนเทศในด้านต่าง ๆ อยู่บนพื้นฐานของหลัก CIA ประกอบด้วย การรักษาความลับของข้อมูล (Confidentiality) เพื่อให้ข้อมูลสารสนเทศเปิดเผยเฉพาะส่วนบุคคลและได้รับอนุญาตเท่านั้น ความสมบูรณ์ถูกต้องของข้อมูล (Integrity) เพื่อเป็นการยืนยันว่าข้อมูลสารสนเทศไม่ถูกเปลี่ยนแปลงไปจากเดิมโดยผู้ที่ไม่มีสิทธิ์ และความพร้อมใช้ของข้อมูล (Availability) เพื่อให้ระบบสารสนเทศมความพร้อมให้บริการอยู่เสมอ และไม่ทำให้การดำเนินงานหยุดชะงักลดความเสียหาย เป็นต้น และส่งเสริมการบริหารจัดการความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ เพื่อช่วยลดความสูญเสียหรือความเสียหายที่คาดว่าจะเกิดขึ้นจากเหตุการณ์ที่ไม่ได้คาดการณ์ไว้ การเพิ่มความปลอดภัยและความมั่นคงของระบบ และการยกระดับความมั่นคงปลอดภัยด้านสารสนเทศให้เกิดประโยชน์ และสร้างความน่าเชื่อถือ อีกทั้งในมาตราที่ 25 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 บัญญัติไว้ว่าให้ธุรกรรมใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดไว้ในกฎหมายนี้ ให้ถือว่าเป็นวิธีการที่น่าเชื่อถือได้ เนื่องจากปัจจุบันการใช้เทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทสำคัญต่อการดำเนินการของภาครัฐและเอกชน ดังนั้นทุกหน่วยงานต้องส่งเสริมให้มีการบริหารจัดการและรักษาความมั่นคงปลอดภัยของสินทรัพย์สารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์

(2) แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 และที่ประกาศเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2556

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้หน่วยงานภาครัฐมีแนวปฏิบัติในการทำงานด้วยวิธีการทางอิเล็กทรอนิกส์ เกิดความมั่นคงปลอดภัยและความน่าเชื่อถือสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ในระดับสากล และผลักดัน และส่งเสริมให้ประเทศเพิ่มความสามารถทางการแข่งขันกับประเทศอื่น ๆ ได้ จึงได้กำหนดนโยบายและแนวปฏิบัตินี้ขึ้นมา ตามมาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) ต้องกำหนดหน้าที่ และความรับผิดชอบในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดที่ชัดเจนสาเหตุจากความบกพร่องฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ดังนั้น หน่วยภาครัฐต้องกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศและจัดทำ ทบทวน ปรับปรุงนโยบายและข้อปฏิบัติที่สอดคล้องกับนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรให้เป็นปัจจุบัน และประกาศนโยบายและข้อปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องทั้งหมดรับทราบ เป็นลายลักษณ์อักษร เพื่อให้เข้าถึง เข้าใจและปฏิบัติตามนโยบายและข้อปฏิบัติ และจัดทำโครงสร้าง กำหนดผู้รับผิดชอบให้ชัดเจน มีการจัดการการเข้าถึงหรือการควบคุมการใช้สารสนเทศมีการจัดให้มีระบบสารสนเทศ และระบบสำรองระบบสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อให้การปฏิบัติงานได้อย่างต่อเนื่อง และการตรวจสอบ และประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

2.1.4.4 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักงานคณะกรรมการพัฒนาระบบราชการ หรือ สำนักงาน ก.พ.ร. (2552) ได้ระบุว่า ส่วนราชการต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศและระบบฐานข้อมูล ได้แก่ 1) มีการจัดทำแผนแก้ไขปัญหาจาก

สถานการณ์ความไม่แน่นอนและความเสียหายที่เกิดขึ้นกับระบบสารสนเทศ 2) มีระบบรักษาความมั่นคงฐานข้อมูลที่ปลอดภัย 3) มีการกำหนดสิทธิ์ของผู้ใช้ในแต่ละระดับ 4) มีการประเมินความเสี่ยง โดยพิจารณาจากโอกาสความบ่อยครั้งที่จะเกิดความเสี่ยง (Likelihood 5) วิเคราะห์พิจารณาถึงระดับความเสี่ยงที่เกิดผลกระทบรุนแรง (Impact) 6) วิธีการจัดลำดับความเสี่ยง/ความสำคัญ โดยพิจารณาจากคะแนนระหว่างโอกาสที่จะเกิดความเสียหาย/ผลกระทบและใช้ในการตัดสินใจสำหรับแก้ไข 7) นำเสนอผลของความเสี่ยงเพื่อให้ผู้บริหารและหน่วยงานได้เห็นภาพรวมของความเสี่ยง และ 8) จัดทำข้อเสนอในการจัดการความเสี่ยง เช่น การจำกัด ป้องกัน หรือลดความเสี่ยงเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟู กู้คืนและสำรองข้อมูลจากความเสียหาย และการถ่ายโอนผลความเสี่ยง เป็นต้น

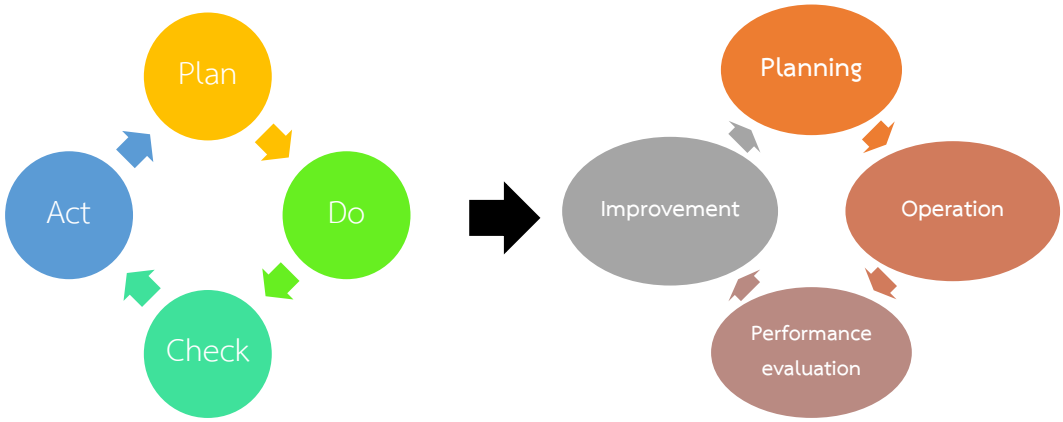
สำหรับกรณีระดับความเสี่ยงที่รุนแรงไม่มากหน่วยงานจะต้องดำเนินการควบคุมและเฝ้าระวังติดตามความเสี่ยงอย่างใกล้ชิด นอกจากนี้ หน่วยงานควรมีการบริหารรรความเสี่ยง โดยการจัดทำแผนความต่อเนื่องทางธุรกิจ ซึ่งแต่ละหน่วยงานจะต้องมีการจัดทำแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศดิจิทัล (Business Continuity Plan for IT) โดยมีวัตถุประสงค์เพื่อ 1) กำหนดแผนที่ชัดเจนและเป็นลายลักษณ์อักษรสำหรับการดำเนินการในกรณีเกิดอุบัติการณ์ 2) เพื่อกำหนดโครงสร้างในการดำเนินแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศดิจิทัล ที่สอดคล้องกับแผนความต่อเนื่องทางธุรกิจหลัก 3) เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินธุรกิจหรือการให้บริการ 4) เพื่อบรรเทาความเสียหายให้อยู่ระดับที่ยอมรับได้ ทั้งนี้ได้มีการวัดผลความสำเร็จของการดำเนินการตามแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ สามารถทำได้โดยการเปรียบเทียบระหว่างค่าของระยะเวลาสูงสุดที่จะกู้ข้อมูลได้หลังจากเกิดสถานการณ์ฉุกเฉิน (Recovery Time Objectives: RTO) ที่กำหนด และค่า RTO ที่ใช้จริงในการกู้คืน และนำมาประเมินผล ในกรณีที่ค่าการกู้คืน RTO มีค่ามากกว่า RTO ที่กำหนด ควรมีการพิจารณาปรับกลยุทธ์ความต่อเนื่องทางธุรกิจเพื่อให้สามารถกู้คืนได้ตามที่กำหนด และไม่กระทบแผนความต่อเนื่องของหน่วยงาน

การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ด้านเทคโนโลยีสารสนเทศดิจิทัล เป็นกระบวนการขั้นตอนหนึ่งในระบบการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management System, BCMS) ซึ่ง BIA เป็นกระบวนการในการวิเคราะห์กิจกรรมต่าง ๆ และผลกระทบต่อกิจกรรมดังกล่าว หากภารกิจของหน่วยงานหรือองค์กรเกิดการหยุดชะงักขึ้น เนื่องจากการได้รับผลกระทบและปัจจัยความเสี่ยงซึ่งการวิเคราะห์ผลกระทบทางธุรกิจด้านเทคโนโลยีสารสนเทศนี้ เป็นกระบวนการวิเคราะห์โดยการพิจารณาแต่ละกิจกรรม หรือกระบวนการที่สำคัญ ตามขอบเขตที่กำหนด เช่น ระบบงานที่มีความสำคัญหรือการให้บริการสารสนเทศที่สำคัญ เพื่อศึกษาถึงผลกระทบที่เกิดขึ้นจากการหยุดชะงัก รวมถึงวิเคราะห์ความต้องการของผู้ใช้งานและผู้เกี่ยวข้องที่ได้รับผลกระทบจากการหยุดชะงักของระบบงาน หรือกระบวนงานที่สำคัญนั้น เพื่อหาเกณฑ์การยอมรับได้ในการหยุดชะงักของภารกิจจากองค์กร ลูกค้าหรือผู้มีส่วนเกี่ยวข้องที่ หลังจากนั้นองค์กรนำผลที่ได้ไปกำหนดกลยุทธ์ (Strategy) ในการรับมือกับสภาวะวิกฤตขององค์กรเมื่อได้รับผลกระทบ จัดทำแนวทางหรือรูปแบบการลดหรือบรรเทาความเสี่ยง (Risk Treatment) และรวบรวมข้อมูลที่ได้ไปจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ด้านเทคโนโลยีสารสนเทศ เพื่อใช้รับมือกับสภาวะวิกฤตที่หน่วยงานเป็นผู้ได้รับผลกระทบต่อไป

2.1.5 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

การบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศ (Information Security Management System: ISMS) ซึ่งเป็นระบบการจัดการที่ช่วยให้หน่วยงานมีความสามารถในการบริหารความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นระบบ เพื่อรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมในการใช้งาน โดยการประยุกต์ใช้กระบวนการบริหารจัดการความเสี่ยง และการสร้างความเชื่อมั่นต่อผู้รับบริการและผู้เกี่ยวข้อง

การบริหารความมั่นคงปลอดภัยด้านสารสนเทศ หรือ ระบบ ISMS ซึ่งรายละเอียดมุ่งเน้นกระบวนการบริหารคุณภาพ PDCA ซึ่งสามารถใช้เป็นเกณฑ์สำหรับการนำไปใช้งานได้จริง และสามารถขอการรับรองได้ และเมื่อทำการเปรียบเทียบ ISMS ตามกระบวนการ PDCA มาพัฒนาเป็น 1) การวางแผน (Planning) 2) การดำเนินการ (Operation) 3) การประเมินประสิทธิภาพ (Performance Evaluation) และ 4) การปรับปรุง (Improvement) ดังภาพที่ 2.2



ภาพที่ 2.2 การเปรียบเทียบ ISMS ตามกระบวนการ PDCA มาพัฒนาเป็น Planning Operation Performance evaluation Improvement

ที่มา: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (2550)

การบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยด้านสารสนเทศ เป็นสิ่งที่ควรให้ความสำคัญ เพื่อป้องกันการดำเนินงานที่จะเกิดความเสียหายและขาดความเชื่อมั่น และควรมีการกำหนดเป็นนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีดิจิทัลที่เป็นมาตรฐาน และเป็นข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยอย่างมีระบบ เพียงพอ และเหมาะสมต่อการดำเนินงานตามขั้นตอนกระบวนการบริหารคุณภาพ PDCA รวมถึงใช้แนวทางประกอบการพิจารณาผลการประเมินความเสี่ยง ซึ่งเป็นวิธีการที่จะ ช่วยลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบ และเป็นการรักษาความมั่นคงปลอดภัยสารสนเทศ (ณัฐวุฒิ วิศยทักษิณ, 2554; ธีรพล แสงอุทัย, 2555; ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2550)

ดังนั้น สรุปได้ว่าการศึกษาความมั่นคงปลอดภัยด้านสารสนเทศ และการบริหารจัดการ ซึ่งเป็นแนวทางหรือวิธีการในการจัดการความเสี่ยงของระบบสารสนเทศที่เกิดขึ้นนั้น มีสาเหตุจากหลายปัจจัยแต่สิ่งที่เป็นสาเหตุหลักคือ ยังขาดการวางนโยบายจากผู้บริหาร และกำหนดให้ถือปฏิบัติ แม้กระทั่งในส่วนขององค์กรที่ให้บริการทางด้านระบบเทคโนโลยีสารสนเทศดิจิทัล ก็ได้ประสบปัญหา ดังนั้นจึงจำเป็นต้องที่จะต้องเร่งดำเนินการแก้ไข เพื่อเรียกความเชื่อมั่นในการให้บริการกลับคืนมา (ณัฐวุฒิ วิศยทักษิณ, 2554; โชติทัต กมลคนธ์, 2555) สอดคล้องกับผลการตรวจสอบระบบสารสนเทศของหน่วยงานของรัฐ 11 หน่วย โดยคัดเลือกหน่วยงานรัฐที่มีการใช้งานระบบสารสนเทศที่ให้บริการโครงสร้างพื้นฐานที่สำคัญของประเทศ และสนับสนุนโครงการของรัฐบาลหรือมีประชาชนใช้บริการเป็นจำนวนมาก ในปีงบประมาณ พ.ศ. 2562 – 2563 พบว่า ไม่มีหน่วยงานใดที่มีผลการประเมินประสิทธิภาพ การควบคุมเป็นไปตามมาตรฐานการตรวจสอบอย่างมีประสิทธิภาพครบทุกด้าน และได้ให้ข้อเสนอแนะกับหน่วยงาน ได้แก่ 1) ควรให้ความสำคัญกับการดำเนินการการตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยการเพิ่มการควบคุม กำกับดูแลด้านเทคโนโลยีสารสนเทศอย่างเคร่งครัด 2) เพิ่มขั้นตอน วิธีปฏิบัติ ตามประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 สำหรับการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์และไม่คาดคิด 3) ควรมีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยให้เป็นปัจจุบันอย่างน้อยปีละหนึ่งครั้ง และ 4) เพิ่มการควบคุมการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ มติคณะรัฐมนตรีหรือแบบแผนราชการที่เกี่ยวข้องให้ครอบคลุมกับเทคโนโลยีดิจิทัลที่เปลี่ยนแปลง (สำนักงานการตรวจเงินแผ่นดิน, 2565)

ดังนั้น ผู้บริหารที่ต้องการแก้ไขปัญหาดังกล่าวข้างต้น โดยเฉพาะความปลอดภัยของข้อมูลสารสนเทศ ซึ่งองค์กรจำเป็นต้องนำระบบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ (ISMS) ไปใช้ในการบริหารจัดการ การบริหารความมั่นคงปลอดภัยสารสนเทศ และกำหนดเป็นระบบการจัดการสำหรับการจัดตั้ง และการรักษาสภาพแวดล้อมข้อมูลให้ปลอดภัย รวมถึงการดำเนินการตามกลยุทธ์เพื่อตอบสนองความต้องการ ด้านการวัดผล และการปรับปรุงทั้งกลยุทธ์การป้องกัน รวมถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และข้อมูลสารสนเทศครอบคลุมตามมาตรฐาน กระบวนการ และองค์ประกอบการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศตรงเหมาะสมกับบริบทองค์กร

2.1.6 องค์ประกอบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ

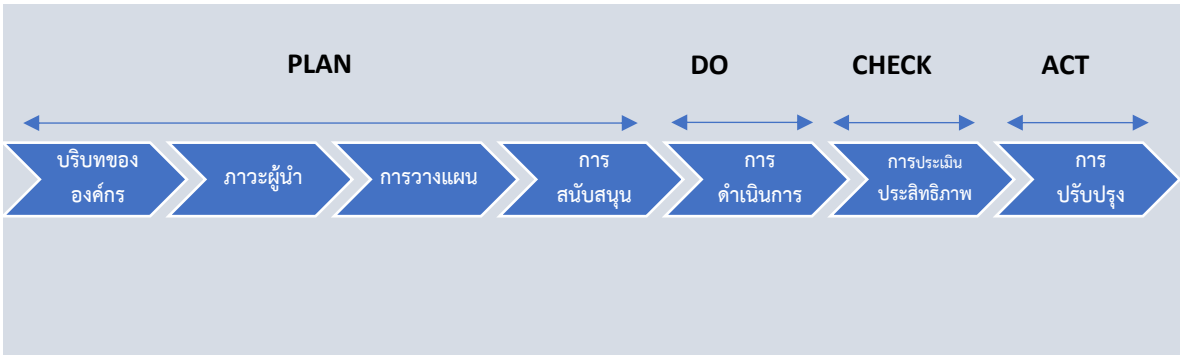
การบริหารความมั่นคงปลอดภัยด้านสารสนเทศ เป็นแนวทาง วิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เกิดประสิทธิภาพ และมีมาตรฐานในระดับเดียวกัน โดยแนวทางต่าง ๆ สามารถป้องกันความเสี่ยงด้านความมั่งคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้ ตลอดจนอยู่ในมาตรฐานที่ยอมรับได้สำหรับการควบคุมการปฏิบัติงาน และการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กรอย่างมีประสิทธิภาพ ซึ่งจากวิเคราะห์และทบทวนเอกสาร พบว่า มีระบบมาตรฐานการจัดการความมั่นคงปลอดภัยอยู่หลากหลายมาตรฐาน แต่ที่เป็นนิยมและมีความเป็นมาตรฐานสากล เพื่อการควบคุมภายใน และการตรวจสอบระบบงานด้านสารสนเทศ สอดคล้องกับระเบียบและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศดิจิทัล ได้แก่ 1) ความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน

ไอเอสโอ/ไออีซี ISO/IEC 27001: 2013 2) ความมั่นคงปลอดภัยสารสนเทศตามกรอบแนวทางของ COBIT 5 และ 3) การศึกษางานวิจัยที่เกี่ยวข้องและมาตรฐานความมั่นคงปลอดภัยสารสนเทศอื่น ๆ รายละเอียดดังนี้

2.1.6.1 มาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2013 ซึ่งเป็นส่วนหนึ่งของมาตรฐานของไอเอสโอ/ไออีซี (ISO/IEC) 27000 ซึ่งเป็นฉบับล่าสุดที่ได้รับการเผยแพร่ในปี 2013 โดยเน้นรายละเอียดเชิงเทคนิคที่เป็นมาตรฐานสำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ หรือ ระบบ ISMS โดยมาตรฐานไอเอสโอ/ไออีซี 27001: 2005 จะมีรายละเอียดมุ่งเน้นกระบวนการตามหลักการ PDCA ซึ่งสามารถใช้เป็นเกณฑ์สำหรับการนำไปใช้งานได้จริง และสามารถขอการรับรองได้ ส่วนมาตรฐานไอเอสโอ/ไออีซี 27001: 2013 ไม่ได้มีการระบุการมุ่งเน้นกระบวนการตามหลักการ PDCA แต่จะเป็นแบบมุ่งเน้นกระบวนการพัฒนาอย่างต่อเนื่องตามที่องค์กรมีอยู่ หรือจะใช้ตามหลักการ PDCA ก็ได้ ที่นำกระบวนการ PDCA มาพัฒนาเป็น 1) การวางแผน (Planning) 2) การดำเนินการ (Operation) 3) การประเมินประสิทธิภาพ (Performance evaluation) และ 4) การปรับปรุง (Improvement) ของมาตรฐานไอเอสโอ/ไออีซี 27001: 2013 (สุชาดา สิทธิ์จงสถาพร, 2563)

ข้อกำหนดหลักที่ต้องปฏิบัติตามมาตรฐานไอเอสโอ/ไออีซี 27001: 2013 มีการปรับปรุงตามแนวทางของคณะกรรมการการกำหนดมาตรฐาน และได้พัฒนาในส่วนของข้อกำหนด (Clause) ของตัวควบคุม ด้านความปลอดภัยในเอกสารแนบ A (Annex A) เพื่อให้แน่ใจว่ามาตรฐานจะสามารถใช้ได้กับภาวะความเสี่ยงล่าสุด เช่น การโจรกรรมข้อมูลส่วนบุคคล (Identify Theft) และภัยคุกคามบนอุปกรณ์โทรศัพท์ และช่องโหว่ของเทคโนโลยีออนไลน์ต่าง ๆ เป็นต้นจุดประสงค์โดยทั่ว ๆ ไปของมาตรฐานไอเอสโอ/ไออีซี 27001: 2013 โดยจะการระบุถึงความเสี่ยงของความปลอดภัยของข้อมูล และการดำเนินงานทางธุรกิจมากขึ้น โดยมุ่งเน้นที่ความจำเป็น และเหมาะสมกับสภาพแวดล้อมและบริบทขององค์กรทั้งภายในและภายนอกมากขึ้น อย่างไรก็ตาม มีมาตรฐานบางส่วนที่มีการเปลี่ยนโครงสร้างใหม่ เพื่อให้ตรงตามข้อกำหนด มาตรฐาน และระบบบริหารจัดการยุคใหม่ นอกจากนี้มาตรฐานไอเอสโอ/ไออีซี 27001: 2013 จะสอดคล้องกับข้อปฏิบัติและคำจำกัดความเกี่ยวกับความเสี่ยง (Risk Terminology) ของมาตรฐานการบริหารจัดการความเสี่ยง ISO 31000

เหตุผลสำคัญ (Clause) มีทั้งหมด 10 ข้อ ได้แก่ 1) ขอบเขต 2) การอ้างอิง เชิงบรรทัดฐาน 3) ข้อกำหนดและคำจำกัดความ 4) บริบทขององค์กร 5) ภาวะผู้นำ 6) การวางแผน 7) การสนับสนุน 8) การดำเนินการ 9) การวัดและประเมินประสิทธิภาพและประสิทธิผล และ 10) การปรับปรุง โดยข้อกำหนดที่ 1 ถึง 3 จะเหมือนกันทั้งมาตรฐานไอเอสโอ/ไออีซี 27001: 2005 และไอเอสโอ/ไออีซี 27001: 2013 ส่วนข้อกำหนดที่ 4 ถึง 10 เป็นข้อกำหนดหลักสำหรับการใช้งาน และการรับรองไอเอสโอ/ไออีซี 27001: 2013 โดยเริ่มต้นจะมีการกล่าวถึงบทนำ (Introduction) โดยมีรายละเอียดสรุปดังภาพที่ 2.3 ดังนี้



ภาพที่ 2.3 โครงสร้างข้อกำหนดหลักที่ต้องปฏิบัติตามมาตรฐานไอเอสโอ/ไออีซี 27001: 2013

ที่มา: สุชาดา สิทธิ์จงสถาพร (2563)

1. ขอบเขต (Scope) จะระบุถึงการใช้มาตรฐานภายในบริบทขององค์กร
2. การอ้างอิงเชิงบรรทัดฐาน (Normative references) จะระบุถึงภาพรวม (Overview) และคำศัพท์ที่กำหนดใช้ (Vocabulary) เป็นการให้รายละเอียดเกี่ยวกับมาตรฐานอ้างอิงหรือสิ่งตีพิมพ์ที่เกี่ยวข้องกับมาตรฐานดังกล่าว
3. ข้อกำหนดและคำจำกัดความ (Terms and definition) จะระบุถึงอภิธานศัพท์ (glossary) ที่เป็นทางการสั้น ๆ รวมทั้งคำศัพท์และคำจำกัดความที่ใช้ทั่วไป โดยรายละเอียดของข้อกำหนดและคำจำกัดความที่ใช้กับมาตรฐานเฉพาะนอกเหนือจากข้อกำหนดและคำจำกัดความที่เกี่ยวข้องอย่างเป็นทางการ
4. บริบทของหน่วยงาน (Context of the organization) สาระสำคัญ คือ การที่องค์กรจะต้องเข้าใจลักษณะขององค์กรธุรกิจ องค์ประกอบรอบด้านที่มีผลกระทบและได้รับผลกระทบจากองค์กรให้เข้าใจก่อนที่จะกำหนดขอบเขต เพื่อให้ระบบ ISMS ที่ได้จัดทำขึ้นสามารถที่สร้างคุณค่าได้อย่างแท้จริง เช่น ใครคือกลุ่มเป้าหมายที่องค์กรจำเป็นที่จะต้องตระหนักและให้ความสำคัญ แล้วกลุ่มคนเหล่านี้ สนใจประเด็นบ้างแล้ว จึงกลับมาพิจารณาขอบเขตของระบบ ISMS เพื่อให้มั่นใจว่าระบบที่กำลังจะดำเนินการสามารถสร้างคุณค่า และตอบสนองกลุ่มเป้าหมายได้อย่างถูกต้อง การกล่าวถึงความสัมพันธ์ที่เกี่ยวข้องกับองค์กร เพื่อให้ข้อกำหนดที่จะนำมาปฏิบัติใช้ครอบคลุมทุก ๆ ฝ่ายที่เกี่ยวข้องกัน มีรายละเอียดดังนี้

4.1 การทำความเข้าใจบริบทขององค์กร กำหนดประเด็นภายในและภายนอกขององค์กรที่ส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ต้องการของระบบ ISMS โดยได้มีการกำหนดประเด็นตามการกำหนดบริบทภายในและภายนอกองค์กรที่มีการพิจารณาในมาตรฐาน ISO 31000: 2009 ซึ่งเป็นตามมาตรฐาน และแนวทางในการบริหารความเสี่ยงขององค์กร ซึ่งสามารถนำไปประยุกต์ใช้ได้กับองค์กรตามประเภท ขนาด และทุกกิจกรรมขององค์กรทั้งภาครัฐและเอกชน

4.2 การวิเคราะห์ความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง องค์กรต้องกำหนดรายละเอียด ความต้องการของผู้ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ โดยมีการกำหนดรวมถึงความต้องการด้านกฎหมายและระเบียบข้อบังคับและข้อกำหนดในสัญญาจ้าง

4.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ องค์กรต้องกำหนดกรอบและการประยุกต์ระบบ ISMS เพื่อระบุขอบเขตการดำเนินการ ในการระบุขอบเขตต้องพิจารณารายละเอียด ได้แก่ 1) ความต้องการขององค์กร 2) ประเด็นสภาพภายใน และภายนอกองค์กร 3) การเชื่อมโยงและการสร้างความสัมพันธ์กันของกิจกรรมซึ่งกันและกันโดยองค์กรเองหรือโดยองค์กรอื่น ๆ และสามารถเข้าถึงได้ในรูปแบบลายลักษณ์อักษร

4.4 ระบบบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ มีการกำหนด ลงมือปฏิบัติ บำรุงรักษาและปรับปรุงอย่างต่อเนื่องกับระบบ ISMS สอดคล้องกับข้อกำหนดในเอกสารหลักฐานตามมาตรฐาน

5. ภาวะผู้นำ (Leadership) มีสาระสำคัญ คือ การที่ผู้นำระดับสูงขององค์กรมีส่วนร่วมในการกำกับดูแลและควบคุม นโยบายการจัดการความมั่นคงปลอดภัยสารสนเทศภายในองค์กรให้มีประสิทธิภาพ

5.1 ภาวะผู้นำและการให้ความสำคัญ ได้แก่ 1) ต้องกำหนดนโยบายการบริหารความมั่นคงปลอดภัยด้านสารสนเทศให้มีความสอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กร 2) ต้องประเมินความต้องการของระบบ ISMS กับกระบวนการขององค์กร 3) ต้องกำหนดทรัพยากรให้เหมาะสมกับการดำเนินงานของระบบ ISMS 4) ต้องชี้แจง สื่อสารความสำคัญของระบบ ISMS และผลสัมฤทธิ์ที่เกิด รวมถึงการดำเนินการตามความต้องการของระบบ ISMS ที่กำหนดไว้ 5) ต้องทำให้ระบบ ISMS บรรลุผลลัพธ์ตามเป้าหมาย 6) ต้องสั่งการ ส่งเสริม และสนับสนุนบุคลากร ให้นำผลสัมฤทธิ์ของระบบ ISMS ไปใช้ 7) ต้องส่งเสริม สนับสนุน ปรับปรุงการดำเนินงานอย่างต่อเนื่อง และ 8) ต้องระบุบทบาท หน้าที่ และการบริหารอื่น ๆ ภายใต้ขอบเขตความรับผิดชอบของของตนเองให้ชัดเจน

5.2 การกำหนดนโยบาย ได้แก่ 1) ระบุจุดประสงค์ขององค์กรที่ความเหมาะสม 2) กำหนดวัตถุประสงค์ หรือกำหนดกรอบการปฏิบัติ 3) การให้ความสำคัญของผู้บริหารสอดคล้องกับความต้องการ 4) การปรับปรุงระบบ ISMS อย่างต่อเนื่อง 5) สามารถเข้าถึงได้ และมีหลักฐานเป็นลายลักษณ์อักษร 6) นโยบายมีการสื่อสารให้ทราบกันภายในองค์กร และ 7) ผู้เกี่ยวข้องสามารถเข้าถึงนโยบายความมั่นคงปลอดภัยสารสนเทศได้ตามความเหมาะสม

5.3 บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ ได้แก่ 1) ผู้บริหารต้องปฏิบัติตามบทบาทหน้าที่ และความความรับผิดชอบ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ มีการมอบหมายและสื่อสารให้ได้รับทราบกันสอดคล้องกับข้อกำหนดของเอกสารมาตรฐานฉบับนี้ และ 2) มีการรายงานประสิทธิภาพและประสิทธิผลของระบบ ISMS ต่อผู้บริหารระดับสูง

6. การวางแผน (Planning) เป็นการวางแผนสำหรับระบบ ISMS โดยพิจารณาให้ครอบคลุมในทุก ๆ ประเด็น โดยมีสาระสำคัญในหัวข้อนี้ประกอบด้วย 2 ส่วน รายละเอียดดังนี้

6.1 การดำเนินการกับความเสี่ยงและโอกาส หัวข้อนี้ มีรายละเอียดที่เกี่ยวข้องกับภาพรวมการประเมินความเสี่ยงและการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ มีดังนี้

6.1.1 ภาพรวม เมื่อวางแผนสำหรับระบบ ISMS องค์กรต้องพิจารณาประเด็นภายในและภายนอกองค์กร รวมถึงกำหนดความเสี่ยงและโอกาสที่สอดคล้องกับวัตถุประสงค์ ได้แก่ 1) เพื่อให้ บรรลุผลลัพธ์ตามกำหนด 2) เพื่อให้ระบบป้องกัน หรือลดผลที่ไม่ต้องการ 3) เพื่อให้มีการทบทวน/ปรับปรุงอย่างต่อเนื่อง 4) เพื่อให้องค์กรวางแผนจัดการความเสี่ยงและโอกาส และ 5) เพื่อให้องค์กรต้องวางแผนวิธีการกระบวนการ การประเมินความสัมฤทธิ์ผล และนำสู่การปฏิบัติ

6.1.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องกำหนดและประยุกต์การประเมินความเสี่ยง ได้แก่ 1) กำหนดและปรับปรุงเกณฑ์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เช่น 1.1) เกณฑ์การยอมรับความเสี่ยง 1.2) เกณฑ์สำหรับการประเมินความเสี่ยง 2) การประเมินความเสี่ยงมีผลการประเมินที่ถูกต้อง สอดคล้อง และเปรียบเทียบกันได้ 3) การระบุความเสี่ยง เช่น 3.1) ประยุกต์กระบวนการประเมินความเสี่ยง และระบุความเสี่ยงที่เกี่ยวข้องกับ ความลับ ความถูกต้อง และสภาพความพร้อมใช้ของระบบ ISMS 3.2) ระบุผู้เป็นเจ้าของความเสี่ยง 4) การวิเคราะห์ความเสี่ยง เช่น 4.1) ประเมินผลคาดการณ์ถ้าความเสี่ยงที่ระบุไว้เกิดขึ้นจริง 4.2) ประเมินโอกาสหากเกิดขึ้นจริง 4.3) กำหนดระดับของความเสี่ยง 5) การประเมินความเสี่ยง เช่น 5.1) เปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ที่กำหนดไว้ 5.2) จัดลำดับความเสี่ยงที่วิเคราะห์ และจัดเก็บสารสนเทศที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร

6.1.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรประยุกต์กระบวนการจัดการความเสี่ยง ได้แก่ 1) กำหนดทางเลือกที่เหมาะสมโดยต้องนำผลการประเมินความเสี่ยงมาพิจารณาด้วย 2) กำหนดมาตรฐานการทั้งหมดเพื่อดำเนินการตามทางเลือกที่กำหนดไว้ และ 3) เปรียบเทียบมาตรการที่ปฏิบัติกับมาตรการที่กำหนด และตรวจสอบความครบถ้วนสมบูรณ์ 4) จัดทำเอกสารตามมาตรการ SoA (Statement of Applicability) ซึ่งประกอบด้วยมาตรการต่าง ๆ และคำอธิบายเหตุผลของการใช้มาตรการทั้งได้รับการปฏิบัติแล้วหรือไม่ก็ตามที่กำหนด 5) จัดทำแผนการจัดการความเสี่ยง และ 6) ขอการรับรองและการยอมรับจากแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่ยังเหลืออยู่ และจัดเก็บสารสนเทศที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร

6.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ โดยแบ่งเป็น 2 ส่วน ได้แก่

6.2.1 กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ดังต่อไปนี้ ได้แก่ 1) ความสอดคล้อง 2) สามารถวัดได้ปฏิบัติได้) 3) พิจารณาความต้องการ ผลการประเมิน และการจัดการความเสี่ยง 4) มีการสื่อสารให้รับทราบ 5) มีการปรับปรุงตามความเหมาะสม และจัดเก็บสารสนเทศไว้เป็นลายลักษณ์อักษร

6.2.2 กำหนดรายละเอียด วางแผนที่จะบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ได้แก่ 1) สิ่งที่ต้องดำเนินการ 2) ทรัพยากร 3) ผู้รับผิดชอบในการดำเนินการ 4) ระยะเวลา 5) วิธีประเมินผลการปฏิบัติการ สำหรับเรื่องการบริหารความเสี่ยง (Risk Management) มาตรฐานไอเอสโอ/ไออีซี 27001: 2013 (ISO/IEC 27001/2013 ได้แนะนำมาตรฐานการบริหารความเสี่ยง (Risk Management – Principles and guidelines) หรือมาตรฐาน ISO 31000 มาประกอบเพื่อประยุกต์ใช้ในทางปฏิบัติรายละเอียดทางเทคนิคสำหรับกาประเมินความเสี่ยงบางอย่างไป เพื่อให้เกิดความครอบคลุมในการนำมา

ประยุกต์ใช้งาน นอกจากนี้เมื่อมีการประเมินความเสี่ยงแล้ว องค์กรยังจำเป็นที่จะต้องวิเคราะห์และวางแผนการดำเนินงานอื่นที่จำเป็นอีก ตามวัตถุประสงค์ (Information Security Objectives) ได้

7. การสนับสนุน (Supporting) ที่เกี่ยวข้องต่าง ๆ เพื่อให้ระบบ ISMS มีประสิทธิภาพ ซึ่งในประเด็นนี้ประกอบด้วยข้อกำหนดย่อยจำนวน 5 หัวข้อ ได้แก่

7.1 ทรัพยากร องค์กรระบุทรัพยากร สำหรับการลงมือปฏิบัติ การบำรุงรักษา และการปรับปรุงต่อเนื่องต่อระบบ ISMS

7.2 สมรรถนะ องค์กรต้องระบุสมรรถนะที่จำเป็น ได้แก่ 1) กำหนดสมรรถนะของบุคลากรที่ส่งผลต่อประสิทธิภาพในการปฏิบัติงานด้านความมั่งคงปลอดภัยสารสนเทศ 2) กำหนดให้บุคลากรมีการพัฒนาตนเองตามความสามารถโดยการให้ความรู้ การฝึกอบรม การเป็นพี่เลี้ยง หรือจากประสบการณ์การทำงาน เป็นต้น 3) ดำเนินการตามสมรรถนะที่จำเป็นและประเมินความสัมฤทธิ์ผล และ 4) จัดเก็บสารสนเทศ หลักฐานแสดงสมรรถนะอย่างเป็นลายลักษณ์อักษร

7.3 การสร้างความตระหนัก ได้แก่ 1) นโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร 2) การมีส่วนในความสำเร็จของระบบ ISMS ซึ่งรวมถึงข้อดีของการปรับปรุงประสิทธิภาพในการปฏิบัติงาน และ 3) การรับผิดชอบกับการไม่ปฏิบัติตามความต้องการของระบบ ISMS

7.4 การสื่อสาร องค์กรต้องสื่อสารให้ทราบทั่งภายในและภายนอกที่เกี่ยวข้องกับระบบ ISMS ได้แก่ 1) เมื่อไรที่ต้องสื่อสารให้ทราบ 2) ใครบ้างที่ต้องสื่อสารให้ทราบ 3) กระบวนการที่เกี่ยวข้องกับการสื่อสาร 4) ใครเป็นผู้สื่อสารออกไป และ 5) มีอะไรบ้างที่ต้องสื่อสารให้ทราบ

7.5 สารสนเทศหลักฐานที่เป็นลายลักษณ์อักษร จะเป็นการกำหนดที่จำเป็นต้องมีสำหรับระบบ ISMS โดยมีหัวข้อที่เกี่ยวข้อง ได้แก่ 1) สารสนเทศที่กำหนดตามมาตรฐานและข้อกำหนดขององค์กร และ 2) สารสนเทศที่เป็นลายลักษณ์อักษรซึ่งกำหนดโดยองค์กรเองและจำเป็นสำหรับความสัมฤทธิ์ผลของระบบ ISMS เช่น ปริมาณของสารสนเทศ เช่น ขนาดขององค์กร ประเภทของกิจกรรม กระบวนการ ผลิตภัณฑ์และบริการ ความซับซ้อน และการเชื่อมโยงระหว่างกระบวนการ และความสามารถของบุคลากร 2) การสร้างและปรับปรุงลายลักษณ์อักษร เช่น ชื่อและรายละเอียด รูปแบบภาษาเวอร์ชัน กราฟิก และสื่อบันทึก และการทบทวน และการอนุมัติ 3) การควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร เช่น ความสามารถเข้าถึงได้สารสนเทศ เหมาะสมสำหรับการใช้งาน สถานที่ และวันเวลาในการใช้งาน และให้สารสนเทศได้รับการป้องกันอย่างเพียงพอ การสูญเสียความลับการใช้งานที่ไม่เหมาะสม ถูกต้องสมบูรณ์ เป็นต้น ดังนั้น สำหรับการควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร องค์กรต้องระบุกิจกรรมตามความเหมาะสม ได้แก่ (1) การแจกจ่าย การเข้าถึง การนำขึ้นมาใช้ (2) การจัดเก็บและการรักษาไว้ (3) การควบคุมการเปลี่ยนแปลงจากแหล่งภายในและภายนอกที่องค์กรกำหนดว่าจำเป็นสำหรับการวางแผนและดำเนินการระบบ ISMS หรือการอนุญาตและการให้อำนาจในการดูและเปลี่ยนแปลงสารสนเทศได้ด้วย หรืออื่น ๆ

8. การดำเนินการ (Operation) เป็นการนำแผนการลดความเสี่ยงดำเนินการทบทวนและปรับปรุงรายการความเสี่ยงและแผนการลดความเสี่ยง ได้แก่ 1) การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม ให้สอดคล้องกับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และลงมือปฏิบัติตามที่กำหนดเพื่อให้บรรลุ

วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ มีการดำเนินการตามแผนองค์กรต้องควบคุมการเปลี่ยนแปลงที่มีการวางแผนล่วงหน้าและทบทวนผลของการเปลี่ยนแปลงที่เกิดขึ้น 2) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องดำเนินการตามรอบระยะเวลาที่กำหนดไว้ โดยนำเกณฑ์ความเสี่ยงที่กำหนดไว้ข้างต้นมาพิจารณาด้วย และจัดเก็บผลของการประเมินความเสี่ยงเป็นลายลักษณ์อักษร และ 3) การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ลงมือปฏิบัติตามแผนการจัดการความเสี่ยง และจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร

9. การประเมินประสิทธิภาพ (Performance Evaluation) กล่าวถึง การตรวจสอบ (Check) ประกอบด้วย 3 ขั้นตอน โดยผลลัพธ์จากในข้อกำหนดนี้หากดำเนินการอย่างถูกต้อง จะเป็นกลไกที่ช่วยผลักดันไปสู่ระบบ ISMS ให้มีประสิทธิผลเกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีรายละเอียด ดังนี้

9.1 การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน องค์กรประเมินประสิทธิภาพและประสิทธิผลของระบบ องค์กรต้องกำหนดรายละเอียดที่เกี่ยวข้อง ได้แก่ 1) อะไรที่จำเป็นต้องเฝ้าระวังและวัดผล ซึ่งรวมถึงกระบวนการและมาตรการของระบบ 2) วิธีการที่เลือกใช้ควรให้ผลการประเมินที่สามารถเปรียบเทียบ ทำซ้ำกันได้ และได้ผลที่ถูกต้อง 3) เมื่อไรที่ต้องดำเนินการ 4) ใครเป็นผู้ดำเนินการ 5) เมื่อไรที่ผลต้องได้รับการวิเคราะห์และประเมิน และ 6) ใครเป็นผู้วิเคราะห์และประเมินผล องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐาน

9.2 การตรวจประเมินภายใน องค์กรดำเนินการตามรอบระยะเวลาที่กำหนด โดยมีวัตถุประสงค์ได้แก่ 1) ระบบ ISMS จะต้องสอดคล้องกับหลักการ คือ 1.1) ความต้องการขององค์สำหรับระบบ ISMS 1.2) ข้อกำหนดตามมาตรฐาน 2) มีการปฏิบัติและบำรุงรักษาไว้ 3) องค์กรต้องวางแผน กำหนด ลงมือปฏิบัติ และบำรุงรักษาโปรแกรมการตรวจประเมิน ซึ่งรวมถึงความถี่ วิธีการที่ใช้ หน้าที่ความรับผิดชอบและผลการตรวจประเมินครั้งก่อนมาพิจารณาร่วมด้วย 4) องค์กรต้องกำหนด เกณฑ์การตรวจประเมิน และขอบเขตของแต่ละครั้ง 5) องค์กรต้องเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินซึ่งเป็นไปตามข้อเท็จจริงและหลักฐานโดยมีความเป็นกลาง 6) มีการรายงานผลไปยังผู้บริหารที่เกี่ยวข้อง และ 7) จัดเก็บสารสนเทศที่โปรแกรมการตรวจประเมินและผลการตรวจประเมินเป็นหลักฐาน

9.3 การทบทวนโดยผู้บริหาร การทบทวนของผู้บริหารต้องรวมการพิจารณาในเรื่องต่าง ๆ ได้แก่ 1) สถานะของการดำเนินการจากผลครั้งก่อน 2) ผลการปลี่ยนแปลงในประเด็นภายในและภายนอกของระบบ ISMS 3) ผลตอบกลับที่แสดงประสิทธิภาพและประสิทธิผล เช่น ความไม่สอดคล้องและการดำเนินการแก้ไข ผลการเฝ้าระวังและวัดผล ผลการตรวจประเมิน และความสำเร็จตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ 4) ผลตอบกลับจากผู้ที่เกี่ยวข้อง 5) ผลการประเมินความเสี่ยงและสถานะของแผนการจัดการความเสี่ยง และ 6) โอกาสสำหรับการปรับปรุงอย่างต่อเนื่อง ซึ่งผลการทบทวนของผู้บริหารต้องรวมการตัดสินใจเกี่ยวกับโอกาสในการปรับปรุงอย่างต่อเนื่องและความจำเป็นสำหรับการเปลี่ยนแปลงต่อระบบ ISMS โดยองค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดงผลการทบทวนของผู้บริหาร

10. การปรับปรุงแก้ไข (Improvement) กล่าวถึงการปรับปรุงโดยแบ่งเป็น 2 ส่วน ได้แก่ 1) ความไม่สอดคล้องและการปรับปรุงแก้ไข โดยเนื้อหาของหัวข้อนี้จะมีการปรับปรุงให้กระชับขึ้น จึงเป็น

การรวมใจความของการดำเนินการแก้ไข (Corrective Action) และการดำเนินการป้องกัน (Preventive Action) เข้าด้วยกัน และ 2) การปรับปรุงและพัฒนาอย่างต่อเนื่อง

10.1 ความไม่สอดคล้องและการปรับปรุงแก้ไข องค์กรต้องจะต้องมีการดำเนินการ ได้แก่ 1) ตอบกลับต่อความไม่สอดคล้อง และดำเนินการเพื่อควบคุมแก้ไขผลที่เกิดขึ้น 2) ประเมินสำหรับการดำเนินการเพื่อขจัดไม่ให้เกิดเหตุการณ์ขึ้นซ้ำ เช่น การทบทวน การระบุสาเหตุ และการระบุว่าความไม่สอดคล้องที่คล้ายกันมีหรือไม่ 3) ดำเนินการแก้ไขที่จำเป็น 4) ทบทวนผลของการดำเนินการแก้ไขไปแล้ว และ 5) ทำการปรับเปลี่ยนแก้ไขต่อผลของความไม่สอดคล้องที่ตามหลักฐานที่แสดงถึงสภาพของความไม่สอดคล้อง และผลของการดำเนินแก้ไข

10.2 การปรับปรุงและพัฒนาอย่างต่อเนื่อง (Continual Improvement) องค์กรต้องปรับปรุง ความเพียงพอ ความเหมาะสม และความสัมฤทธิ์ผลของระบบอย่างต่อเนื่อง

11 มาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2013

การบริหารจัดการสารสนเทศให้มีความมั่นคงปลอดภัยจำตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2013 ได้แบ่งเนื้อหาออกเป็น 14 ประเด็น (Domain) ประกอบด้วย 35 วัตถุประสงค์ (Control objectives) และภายใต้ วัตถุประสงค์ แต่ละข้อประกอบด้วยมาตรการในการควบคุม 114 ข้อ (Controls) โดยมีประเด็นที่เพิ่มขึ้นจากมาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2005 จำนวน 3 ประเด็น เนื่องจากมีการใช้อุปกรณ์เทคโนโลยีสารสนเทศในระดับบุคคลและระดับองค์กรมากขึ้น รวมทั้งบทบาทของเทคโนโลยีเสมือนจริง (Virtual) และระบบประมวลผลกลาง (Cloud) ที่มีการนำมาใช้งานแพร่หลายเป็นอย่างมาก

ดังนั้น มาตรการควบคุมที่ใช้ในการจัดการความมั่นคงปลอดภัยสารสนเทศจะเริ่มต้นที่ A5 เนื่องจากเกี่ยวข้องกับมาตรฐานไอเอสโอ 27001 เริ่มต้นมาจากการเป็นมาตรฐาน BS (British standard) โดยข้อกำหนดที่ 1 ถึง 4 จะเกี่ยวข้องกับเรื่องทั่วไปที่เกี่ยวกับขอบเขตการจัดการที่เกี่ยวข้องกับองค์กร และตั้งแต่ข้อกำหนดที่ 5 เป็นต้น ซึ่งมีรายละเอียดดังตารางที่ 2.1 (สุชาดา สิทธิ์จงสถาพร, 2563)

ตารางที่ 2.1 การเปรียบเทียบรายละเอียดมาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2005 และ 27001: 2013

ประเด็น	ไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2005	ประเด็น	ไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2013
A5	นโยบายความมั่นคงปลอดภัย (Security Policy)	A5	นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)
A6	โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security)	A6	โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security)
A8	ความมั่นคงปลอดภัยสำหรับบุคลากร (Human resource security)	A7	ความมั่นคงปลอดภัยสำหรับบุคลากร (Human resource security)
A7	การบริหารจัดการทรัพย์สิน (Asset management)	A8	การบริหารจัดการทรัพย์สิน (Asset management)
A11	การควบคุมการเข้าถึง (Access control)	A9	การควบคุมการเข้าถึง (Access control)
		A10	การเข้ารหัสข้อมูล (Cryptography)
A9	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)	A11	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)
A10	การบริหารจัดการสื่อสารและการดำเนินการ (Communications and Operations security)	A12	ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations security)
A10	การบริหารจัดการสื่อสารและการดำเนินการ (Communications and Operations security)	A13	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
A12	การจัดหาสารสนเทศ การพัฒนาและการบำรุงรักษาระบบ (Information Systems Acquisition, Development and Main – tennance)	A14	การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)
		A15	ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)

ตารางที่ 2.1 (ต่อ)

ประเด็น	ไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2005	ประเด็น	ไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2013
A13	การจัดการเหตุการณ์ความปลอดภัยของข้อมูล (Information Security Incident Management)	A16	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)
A14	การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)	A17	ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)
A15	ความสอดคล้อง (Compliance)	A18	ความสอดคล้อง (Compliance)

รายละเอียดดังตารางที่ 2.1 กำหนดรายละเอียดตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2005 เปรียบเทียบกับ มาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2013 พบว่า ในรายละเอียดของมาตรฐานไอเอสโอ/ไออีซี 27001 มีการจัดกลุ่มใหม่ โดยเปลี่ยนจากมาตรฐานไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2005 จาก 11 ประเด็น เพิ่มเติมใหม่เป็น 14 ประเด็น ดังนี้

1. จากประเด็น A12.3 การควบคุมการเข้ารหัสลับ (Cryptographic controls) ในมาตรฐาน (ISO/IEC) 27001: 2005 มาตั้งเป็นประเด็นใหม่ A10 การเข้ารหัสลับ (Cryptography) ในมาตรฐาน (ISO/IEC) 27001: 2013

2. จากประเด็น A10 การบริหารจัดการ และการดำเนินการสื่อสาร (Communications and operations management) ในมาตรฐาน (ISO/IEC) 27001: 2005 แบ่งออกเป็น 2 ประเด็นย่อย ได้แก่ A12 การดำเนินการความมั่นคงปลอดภัย (Operations Security) และ A13 การสื่อสารความมั่นคงปลอดภัย (Communications Security) ในมาตรฐาน (ISO/IEC) 27001: 2013

3. ผู้ให้บริการ (Supplier) ได้แก่ ข้อย่อย A6.2 บุคคลภายนอก (External parties) และ A10.2 การบริหารจัดการการจัดส่งบริการของบุคคลที่สาม (Third Party Service delivery management) ในมาตรฐาน (ISO/IEC) 27001: 2005 และตั้งเป็นประเด็นใหม่ A15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) ดังนั้นมาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2013 มีความครอบคลุม ซึ่งเป็นมาตรฐานที่มีความทันสมัย ทำให้การควบคุมและจัดการระบบให้มีประสิทธิภาพ รายละเอียดดังตารางที่ 2.2 (สุชาดา สิทธิ์จงสถาพร, 2563)

ตารางที่ 2.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศไอเอสโอ/ไออีซี (ISO/IEC) 27001: 2013

ลำดับ	หัวข้อ
A5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policies)	
5.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัย (Management direction for information security)	
1	5.1.1 นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)
2	5.1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for information security)
A6 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security)	
6.1 โครงสร้างภายในองค์กร (Internal organization)	
3	6.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)
4	6.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)
5	6.1.3 การติดต่อกับผู้มีอำนาจ (Contact with authorities)
6	6.1.4 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups)
7	6.1.5 การบริหารจัดการโครงการให้มีความมั่นคงปลอดภัยสารสนเทศ (Information security in project management)
6.2 อุปกรณ์คอมพิวเตอร์แบบพกพา และการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)	
8	6.2.1 นโยบายสำหรับอุปกรณ์แบบพกพา (Mobile device policy)
9	6.2.2 การปฏิบัติงานทางไกล (Teleworking)
A7 ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human resource security)	
7.1 ก่อนการจ้างงาน (Prior to employment)	
10	7.1.1 การคัดเลือก (Screening)
11	7.1.2 ข้อตกลง และเงื่อนไขในการจ้างงาน (Terms and conditions of employment)

ตารางที่ 2.2 (ต่อ)

ลำดับ	หัวข้อ
7.2 ระหว่างการจ้างงาน (During employment)	
12	7.2.1 หน้าที่ความรับผิดชอบ (Management responsibilities)
13	7.2.2 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมความปลอดภัยสารสนเทศ (Information security awareness, education and training)
14	7.2.3 กระบวนการทางวินัย (Disciplinary process)
7.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)	
15	7.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)
A8 การบริหารจัดการทรัพย์สิน (Asset management)	
8.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)	
16	8.1.1 บัญชีทรัพย์สิน (Inventory of asset)
17	8.1.2 ผู้ถือครองทรัพย์สิน (Ownership of assets)
18	8.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)
19	8.1.4 การคืนทรัพย์สิน (Return of assets)
8.2 การจัดชั้นความลับของสารสนเทศ (Information classification)	
20	8.2.1 ชั้นความลับของสารสนเทศ (Classification of information)
21	8.2.2 การบ่งชี้สารสนเทศ (Labeling of information)
22	8.2.3 การจัดการทรัพย์สิน (Handling of assets)
8.3 การจัดการสื่อบันทึกข้อมูล (Media handling)	
23	8.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media)
24	8.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of media)
25	8.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer)
A9 การควบคุมการเข้าถึง (Access control)	
9.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirement of access control)	
26	9.1.1 นโยบายควบคุมการเข้าถึง (Access control policy)
27	9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย (Access to networks and network services)

ตารางที่ 2.2 (ต่อ)

ลำดับ	หัวข้อ
28	9.2.1 การลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน (User registration and deregistration)
29	9.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)
30	9.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)
31	9.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตน (Management of secret authentication information of users)
32	9.2.5 การทบทวนสิทธิการเข้าถึง (Review of user access rights)
33	9.2.6 การถอดหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)
9.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	
34	9.3.1 การใช้ข้อมูลลับเพื่อการพิสูจน์ตัวตน (User of secret authentication information)
9.4 การควบคุมการเข้าถึงระบบ (System and application access control)	
35	9.4.1 การจำกัดการเข้าถึง (Information access restriction)
36	9.4.2 ขั้นตอนการล็อกอินเข้าระบบที่มีความปลอดภัย (Secure log-on procedures)
37	9.4.3 การจัดการรหัสผ่าน (Password management system)
38	9.4.4 การใช้โปรแกรมอรรถประโยน์ (Use of privileged utility programs)
39	9.4.5 การควบคุมการเข้าถึงซอร์สโค้ด (Access control to program source code)
A10 การเข้ารหัสข้อมูล (Cryptography)	
10.1 มาตรการเข้ารหัสข้อมูล (**Cryptographic controls)**	
40	10.1.1 นโยบายการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)
41	10.1.2 การบริหารจัดการกุญแจ (Key management)
A11 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)	
11.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)	
42	11.1.1 ขอบเขตโดยรอบทางกายภาพ (Physical security perimeter)
43	11.1.2 ควบคุมการเข้าออกทางกายภาพ (Physical entry controls)
44	11.1.3 รักษาความมั่นคงปลอดภัยสำหรับห้องสำนักงานและอุปกรณ์ (Securing office, room and facilities)

ตารางที่ 2.2 (ต่อ)

ลำดับ	หัวข้อ
45	11.1.4 การป้องกันต่อภัยคุกคามและสภาพแวดล้อมจากภายนอก (Protecting against external end environmental thetas)
46	11.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working in secure areas)
47	11.1.6 พื้นที่สำหรับรับส่ง (Delivery and loading areas)
11.2 อุปกรณ์ (Equipment)	
48	11.2.1 การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)
49	11.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)
50	11.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)
51	11.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)
52	11.2.5 การนำทรัพย์สินขององค์กรออกจากสำนักงาน (Removal of assets)
53	11.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off-premises)
54	11.2.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)
55	11.2.8 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment)
56	11.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)
A12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)	
12.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational procedures and responsibilities)	
57	12.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)
58	12.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change management)
59	12.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)
60	12.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา ทดสอบและการให้บริการ (Separation of development, testing and operational environments)
12.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from malware)	
61	12.2.1 การป้องกันโปรแกรมไม่ประสงค์ดี (Control against malware)
12.3 การสำรองข้อมูล (Backup)	

ตารางที่ 2.2 (ต่อ)

ลำดับ	หัวข้อ
62	12.3.1 การสำรองข้อมูล (Information backup)
12.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and monitoring)	
63	12.4.1 การบันทึกข้อมูลแสดงเหตุการณ์ (Event logging)
64	12.4.2 การป้องกันข้อมูล (Protection of log information)
65	12.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ (Administrator and operator logs)
66	12.4.4 การตั้งนาฬิกา (Clock synchronization)
12.5 การควบคุมการติดตั้งซอฟต์แวร์ (Control of operational software)	
67	12.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)
12.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical vulnerability management)	
68	12.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)
69	12.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)
12.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (**Information systems audit considerations)**	
70	12.7.1 มาตรการการตรวจประเมินระบบ (Information system audit controls)
A13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)	
13.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network security management)	
71	13.1.1 มาตรการเครือข่าย (Network controls)
72	13.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)
73	13.1.3 การแบ่งแยกเครือข่าย (Segregation in networks)
13.2 การถ่ายโอนสารสนเทศ (Information transfer)	
74	13.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอน (Information transfer policies and procedures)
75	13.2.2 ข้อตกลงสำหรับการถ่ายโอน (Agreements on information transfer)
76	13.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)
77	13.2.4 ข้อตกลงการรักษาความลับ (Confidentiality or non - disclosure agreements)

ตารางที่ 2.2 (ต่อ)

ลำดับ	หัวข้อ
A14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)	
14.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)	
78	14.1.1 การวิเคราะห์และกำหนดความต้องการ (Information security requirements analysis and specification)
79	14.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่าย (Securing application services on public networks)
80	14.1.3 การป้องกันธุรกรรมของบริการ (Protecting application services transactions)
14.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)	
81	14.2.1 นโยบายการพัฒนาระบบให้ปลอดภัย (Secure development policy)
82	14.2.2 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลง (System change control procedures)
83	14.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐาน (Technical review of applications after operating platform changes)
84	14.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์ (Restrictions on changes to software packages)
85	14.2.5 หลักการวิศวกรรมระบบความมั่นคงปลอดภัย (Secure system engineering principles)
86	14.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)
87	14.2.7 การจ้างหน่วยงานภายนอก (Outsourced development)
88	14.2.8 การทดสอบความมั่นคงปลอดภัย (System security testing)
89	14.2.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing)
14.3 ข้อมูลสำหรับการทดสอบ (Test data)	
90	14.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)

ตารางที่ 2.2 (ต่อ)

ลำดับ	หัวข้อ
A15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)	
15.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)	
91	15.1.1 นโยบายด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)
92	15.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Addressing security within supplier agreements)
93	15.1.3 ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)
15.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)	
94	15.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier services)
95	15.2.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services)
A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident Management)	
16.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)	
96	16.1.1 หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติ (Responsibilities and procedures)
97	16.1.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events)
98	16.1.3 การรายงานจุดอ่อน (Reporting information security weaknesses)
99	16.1.4 การประเมินและตัดสินใจต่อสถานการณ์ (Assessment of and decision on information security events)
100	16.1.5 การตอบสนองต่อเหตุกาณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)
101	16.1.6 การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning form information security incidents)

ตารางที่ 2.2 (ต่อ)

ลำดับ	หัวข้อ
102	16.1.7 การเก็บรวบรวมหลักฐาน (Collection of evidence)
A17 ประเด็นความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)	
17.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)	
103	17.1.1 การวางแผนความต่อเนื่อง (Planning information security continuity)
104	17.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่อง (Implementing information security continuity)
105	17.1.3 การตรวจสอบ การทบทวนและการประเมินความต่อเนื่อง (Verify, review and evaluate information security continuity)
17.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)	
106	17.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)
A18 ความสอดคล้อง (Compliance)	
18.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)	
107	18.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้าง (Identification of applicable legislation and contractual requirements)
108	18.1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)
109	18.1.3 การป้องกันข้อมูล (Protection of records)
110	18.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)
111	18.1.5 ระเบียบข้อบังคับการเข้ารหัสข้อมูล (Regulation of cryptographic controls)
18.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)	
112	18.2.1 การทบทวนอย่างอิสระ (Independent review of information security)
113	18.2.2 ความสอดคล้องกับนโยบายและมาตรฐาน (Compliance with security policies and standards)
114	18.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

2.1.6.2 มาตรฐานความมั่นคงปลอดภัยสารสนเทศตามกรอบแนวทางของ COBIT 5 (Control Objectives for Information and Related Technology)

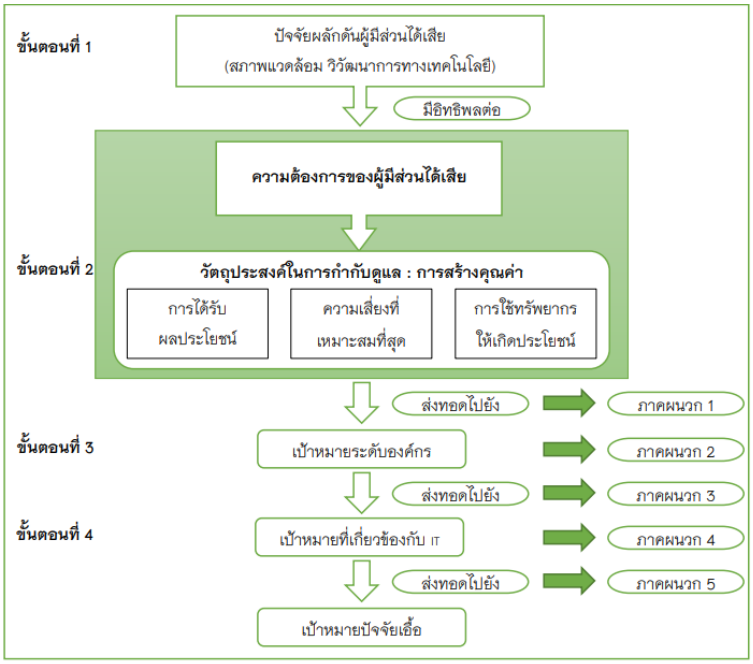
มาตรฐานความมั่นคงปลอดภัยสารสนเทศตามกรอบแนวทางของ COBIT 5 เป็นกรอบแนวทางการบริหารจัดการระบบเทคโนโลยีสารสนเทศที่เป็นมาตรฐาน พร้อมทั้งแนวทางการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่าง ๆ ที่เป็นกรอบแนวทางสำหรับการบริหารจัดการโครงการและการกำกับดูแลองค์กรที่ดี ปัจจุบันได้พัฒนามาถึงเวอร์ชั่น 5 ซึ่งมีการนำมาตรฐาน (Standard) และ แนวปฏิบัติที่ดี (Best Practice) มาใช้อ้างอิงมากกว่า 60 แหล่ง เช่น ITIL V3, ISO 27000 Series, ISO 20000, ISO 38500: 2008, TOGAF V9 และ ISO 9000: 2008 เป็นต้น (Musa et al., 2014; Spremic, 2015) การนำกรอบปฏิบัติ COBIT ไปใช้พัฒนากลยุทธ์ทางธุรกิจทางด้านเทคโนโลยีสารสนเทศ เพื่อให้องค์กรบรรลุวัตถุประสงค์การกำกับดูแล และการบริหารจัดการระบบเทคโนโลยีสารสนเทศขององค์กร ครอบคลุมหน้าที่ตามความรับผิดชอบโดยพิจารณาถึงผลประโยชน์ที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศของผู้มีส่วนได้เสียทั้งภายในและภายนอก จำนวน 5 ประการ (Khther & Othman, 2013; Maria et al., 2012; Musa et al., 2014) ดังภาพที่ 2.4 ต่อไปนี้

ภาพที่ 2.4 หลักการของกรอบปฏิบัติ COBIT 5.0

ที่มา: ISACA (2012)

หลักการสำคัญตามกรอบแนวทางของ COBIT 5 มีรายละเอียดดังนี้

หลักการที่ 1 การตอบสนองต่อความต้องการของผู้ที่เกี่ยวข้อง (Meeting Stakeholder Needs) การรักษาความสมดุลระหว่างผลประโยชน์ ความเสี่ยง และการใช้ทรัพยากร โดยมีขั้นตอนการถ่ายโอนค่าเป้าหมาย ซึ่งช่วยให้มีการระบุเป้าหมายที่เฉพาะเจาะจง เพื่อสนับสนุนเป้าหมาย และความต้องการในภาพรวมและสอดคล้องกันระหว่างความต้องการขององค์กรกับกระบวนการการแก้ไขปัญหาและการให้บริการ โดยมีขั้นตอนรายละเอียดดังภาพที่ 2.5



ภาพที่ 2.5 ขั้นตอนการถ่ายโอนค่าเป้าหมายของ COBIT 5

ที่มา : ISACA (2012)

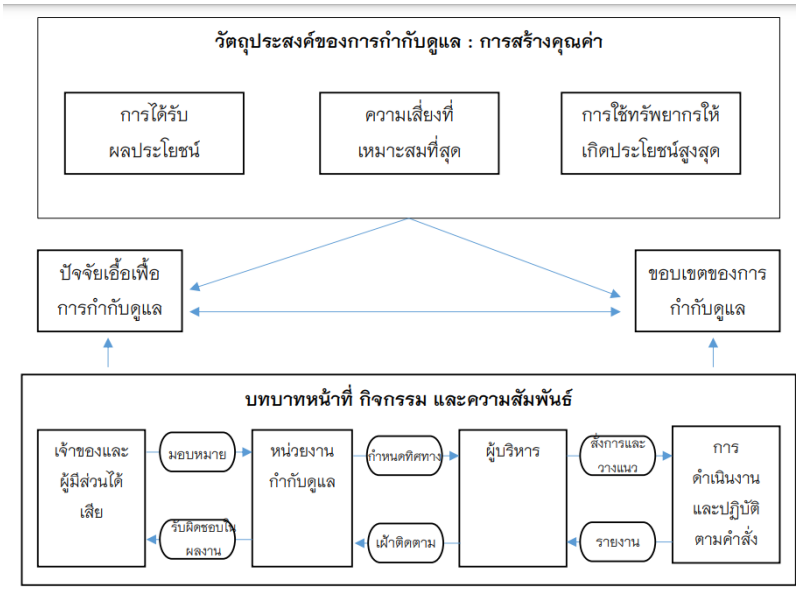
หลักการที่ 2 การครอบคลุมทั่วทั้งองค์กร (Covering the Enterprise End-to-End) เป็นการครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร โดยการบูรณาการเทคโนโลยีสารสนเทศ เข้าไปในการกำกับดูแลองค์กรและกระบวนการภายในองค์กร โดยมีแนวคิดการกำกับดูแลและการบริหารจัดการ COBIT 5

2.1 ปัจจัยเอื้อเพื่อการกำกับดูแลของกรอบแนวคิดของ COBIT 5 อธิบายถึงปัจจัยเอื้อไว้ 7 ประเภท ได้แก่ 1) นโยบาย หลักการและกรอบการดำเนินงาน เป็นสิ่งที่นำไปสู่พฤติกรรมที่คาดหวังให้เป็นแนวทางปฏิบัติ 2) กระบวนการ เป็นกลุ่มของแนวปฏิบัติและกิจกรรมที่ใช้ดำเนินการเพื่อให้ได้ผลลัพธ์ตามวัตถุประสงค์โดยภาพรวม 3) โครงสร้างการจัดองค์กร ระบุถึงองค์กรที่เป็นหลักในการตัดสินในในองค์กร 4) วัฒนธรรม จริยธรรม และพฤติกรรม ทั้งในส่วนบุคคลและขององค์กร 5) สารสนเทศทั้งที่เกิดจากและที่ใช้โดยองค์กร เพื่อใช้ในการดำเนินกิจกรรมและเพื่อการกำกับ ดูแล แต่สำหรับในระดับปฏิบัติการเท่านั้น 6)

บริการ โครงสร้างพื้นฐาน และระบบงาน รวมถึงโครงสร้างพื้นฐาน เทคโนโลยี และระบบงานที่ ใช้สำหรับการประมวลผลและบริการอื่น ๆ ด้านเทคโนโลยีแก่องค์กร และ 7) บุคลากร ทักษะ และศักยภาพเชื่อมโยงกับตัวบุคคลและสิ่งจำเป็นที่จะช่วยให้กิจกรรมทั้งหมด สำเร็จลุล่วง และช่วยให้ตัดสินใจได้อย่างถูกต้องพร้อมทั้งดำเนินการแก้ไข

2.2 ขอบเขตของการกำกับดูแล ได้แก่ การกำกับดูแลสามารถประยุกต์ใช้กับทั่วทั้งองค์กรกับหน่วยงานใดหน่วยงานหนึ่งกับสินทรัพย์และอื่น ๆ กล่าวคือ สามารถกำหนดการนำการกำกับดูแลไปประยุกต์ใช้ในมุมมองที่แตกต่างกันไปของแต่ละองค์กร

2.3 บทบาทกิจกรรมและความสัมพันธ์ ได้แก่ ระบุว่าใครมีส่วนร่วมในการกำกับดูแลอย่างไร และบุคคลเหล่านั้นทำอะไร และจะมีปฏิสัมพันธ์ระหว่างกันอย่างไร ภายใต้ขอบเขตของระบบการกำกับดูแลใน COBIT 5 จะแบ่งแยกกิจกรรม การกำกับดูแลออกจากกิจกรรมการบริหารจัดการอย่างชัดเจน รายละเอียดดังภาพที่ 2.6



ภาพที่ 2.6 แนวคิดการกำกับดูแล และการบริหารจัดการ COBIT 5

ที่มา : ISACA (2012)

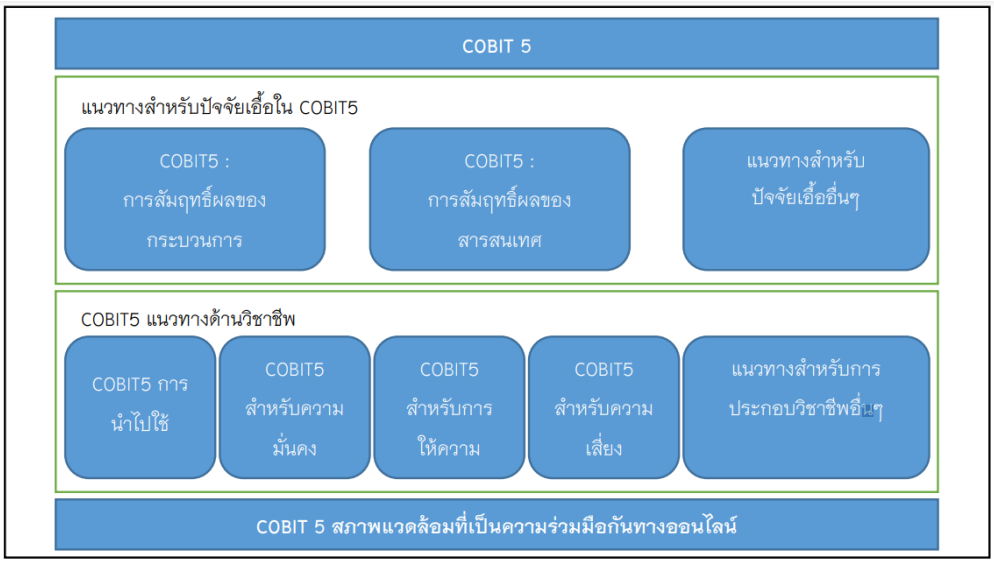
หลักการที่ 3 การรวมมาตรฐานต่างๆ ให้อยู่ภายใต้กรอบเดียวกัน (Applying a Single Integrated Framework) เป็นการประยุกต์ใช้กรอบวิธีปฏิบัติ COBIT 5 กับการบูรณาการให้สอดคล้องกันในภาพรวม จึงสามารถใช้เป็นกรอบการดำเนินงานที่ครอบอยู่เหนือกรอบการดำเนินงานอื่น ๆ ดังนี้

3.1 สอดคล้องกับมาตรฐานและกรอบการดำเนินงานอื่น ๆ ที่เกี่ยวข้อง ซึ่งช่วยให้องค์กรสามารถใช้ COBIT5 เสมือนกรอบการดำเนินงานที่ครอบอยู่เหนือการบูรณาการกำกับดูแลและการบริหารจัดการ

3.2 ครอบคุลมทั่วทั้งองค์กรอย่างสมบูรณ์ ซึ่งให้หลักในการบูรณาการใช้กรอบการดำเนินการ มาตรฐาน และแนวปฏิบัติอื่น ๆ อย่างมีประสิทธิผล ทำให้การนำแนวทางจากแหล่งต่าง ๆ มาใช้สอดคล้องและบูรณาการเข้าด้วยกัน โดยไม่ภาษาเชิงเทคนิคหรือภาษาด้านเทคโนโลยี

3.3 สถาปัตยกรรมโครงสร้างของระบบที่เรียบง่าย สำหรับจัดโครงสร้างของเอกสารประกอบแนวทางและการจัดทำชุดผลิตภัณฑ์ที่สอดคล้องกัน

3.4 บูรณาการองค์ความรู้ต่าง ๆ ที่กระจัดกระจายอยู่ตามกรอบการดำเนินงานของ ISACA ได้วิจัยประเด็นสำคัญๆ เกี่ยวกับการกำกับดูแลระดับองค์กรมาหลายปี และจัดทำกรอบการดำเนินงานออกมาใช้มากมาย ไม่ว่าจะเป็น COBIT, Val IT, Risk IT, BMIS เอกสารที่ชื่อว่าบทสรุปการกำกับดูแลระบบเทคโนโลยีสารสนเทศของกรรมการบริหาร และให้แนวทางและการสนับสนุนแก่องค์กร COBIT 5 ได้บูรณาการองค์ความรู้ทั้งหมดนี้เข้าไว้ด้วยกันเป็นชุดผลิตภัณฑ์ของ COBIT 5 ดังภาพที่ 2.7



ภาพที่ 2.7 ตัวอย่างการบูรณาการองค์ความรู้ ตามชุดผลิตภัณฑ์ของ COBIT 5

ที่มา: ISACA (2012)

หลักการที่ 4 การใช้ปัจจัยก่อเกิดร่วมกันทั้งหมดในการปฏิบัติ (Enabling a Holistic Approach) เป็นการใช้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผลกรอบวิธีปฏิบัติ COBIT 5 ระบุถึงกลุ่มของปัจจัยสนับสนุนการกำกับดูแล และการจัดการด้านระบบเทคโนโลยีสารสนเทศระดับองค์กร โดยปัจจัยที่เอื้อต่อความต้องการข้อมูลจากปัจจัยอื่น ๆ เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ เช่น กระบวนการต้องการสารสนเทศ โครงสร้างขององค์กรต้องการทักษะและพฤติกรรม เป็นต้น การส่งมอบผลลัพธ์ที่เป็นประโยชน์แก่ปัจจัยเอื้ออื่น ๆ ยกตัวอย่างเช่น กระบวนการส่งมอบสารสนเทศ ทักษะและพฤติกรรมช่วยให้กระบวนการมีประสิทธิผล เป็นต้น โดยปัจจัยที่เอื้อขององค์กรใน COBIT 5 แบ่งออกได้เป็น 7 ประเภท รายละเอียดดังนี้

4.1 นโยบาย หลักการ และกรอบการดำเนินงาน สำหรับการตัดสินใจของผู้บริหารด้านการกำกับดูแล และการจัดการเทคโนโลยีสารสนเทศภายในองค์กร ซึ่งในการกำหนด นโยบาย หลักการที่ดีนั้น ผู้บริหารควรนึกถึงประสิทธิภาพให้สอดคล้องกับสภาพการทำงาน และสามารถบรรลุวัตถุประสงค์ที่องค์กรได้กำหนดไว้ และการเข้าถึงหลักการ และนโยบายของผู้มีส่วนเกี่ยวข้อง

4.2 กระบวนการ เป็นแนวปฏิบัติงานของเจ้าหน้าที่ เพื่อให้บรรลุวัตถุประสงค์ ในการควบคุมภายในด้านเทคโนโลยีสารสนเทศภายใต้หน้าที่และความรับผิดชอบที่ได้รับมอบหมายตามนโยบายที่ผู้บริหารกำหนด

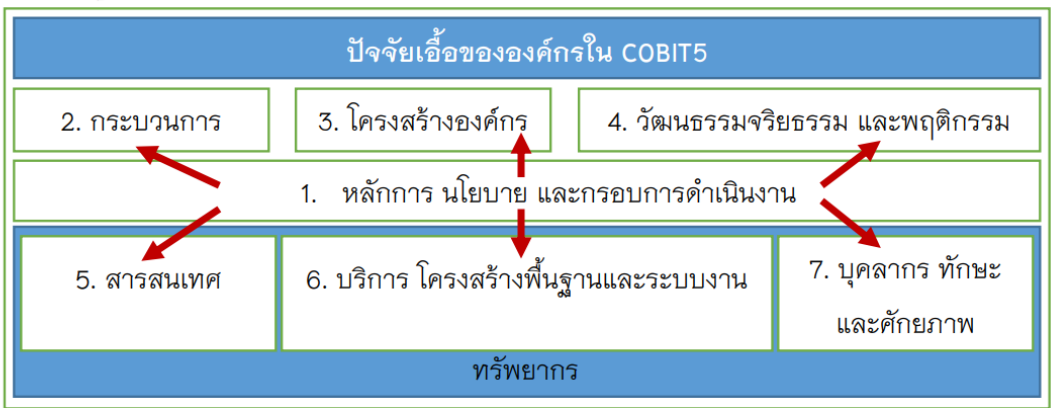
4.3 โครงสร้างองค์กร และหน้าที่ความรับผิดชอบของทุกส่วนงานในองค์กร รวมทั้งการบริหารจัดการบุคลากรในองค์กรให้บรรลุผลการดำเนินงาน

4.4 วัฒนธรรม จริยธรรม และพฤติกรรมเป็นลักษณะการงานของบุคลากร ซึ่งเป็นปัจจัยสนับสนุนหลักในด้านการควบคุมภายใน โดยสอดคล้องกับการจัดโครงสร้างองค์กร และสภาพแวดล้อมการทำงานที่ดี

4.5 สารสนเทศเป็นการนำมาใช้ในการควบคุมภายในของกระบวนการทำงานด้านเทคโนโลยีสารสนเทศของคนในองค์กรให้มีคุณภาพตามที่กำหนด

4.6 บริการโครงสร้างพื้นฐาน ระบบงาน และเทคโนโลยีที่ใช้ในการประมวลผลข้อมูลกาทำงานของผู้ใช้งานระบบภายในองค์กร รวมทั้งทรัพยากรและกระบวนการทำงานให้บรรลุเป้าหมายตามวัตถุประสงค์ที่กำหนด

4.7 ทักษะและศักยภาพของบุคลากร หมายถึง ความรู้ความสามารถของผู้ใช้งานระบบขึ้นอยู่กับกิจกรรมการดำเนินงานภายในองค์กร ดังภาพที่ 2.8



ภาพที่ 2.8 การกำกับดูแล และการบริหารจัดการอย่างเป็นระบบด้วยปัจจัยเอื้อที่เชื่อมต่อถึงกันใน COBIT 5

ที่มา: ISACA (2012)

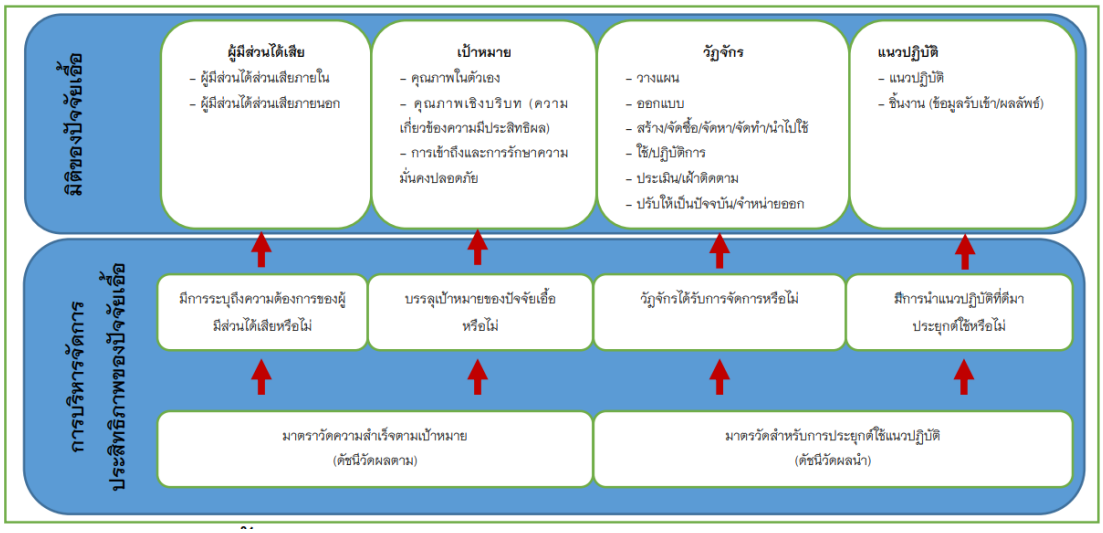
ดังนั้น เมื่อต้องการกำกับดูแลและการบริหารจัดการระบบเทคโนโลยีสารสนเทศอย่างเป็นระบบ และต้องรับมือกับความต้องการผู้มีส่วนได้ส่วนเสีย ปัจจัยเอื้อต่าง ๆ ที่มีความสัมพันธ์กัน และเชื่อมโยงถึงกัน และได้รับการจัดการเมื่อเกิดปัญหา ผู้บริหารระดับสูงจะต้องผลักดันแนวคิดดังกล่าว ตามองค์ประกอบปัจจัยเอื้อด้านการบริการ โครงสร้างพื้นฐาน และระบบงาน ดังนี้

1. ผู้มีส่วนได้ส่วนเสีย สามารถแบ่งกลุ่มผู้มีส่วนได้ส่วนเสียเป็น 2 ประเภท ได้แก่ 1.1) ผู้มีส่วนได้ส่วนเสียภายใน คือ บุคคลภายในองค์กรที่มีทำให้เกิดกระบวนการทำงาน และ 1.2) ผู้มีส่วนได้ส่วนเสียภายนอก คือ บุคคลภายนอกที่ได้รับผลกระทบจากการดำเนินงานตามกระบวนการขององค์กร

2. เป้าหมาย คือ ผลลัพธ์ที่องค์กรคาดหวังจากการปฏิบัติงานตามกระบวนการที่ผู้บริหารได้กำหนดไว้ โดยเป้าหมายของกระบวนการแบ่งออกเป็น 3 ประเภท ได้แก่ 2.1) เป้าหมายในตนเอง (Intrinsic goal) คือ กระบวนการมีความสอดคล้องกับแนวทางปฏิบัติตามนโยบาย และกฎระเบียบที่องค์กรกำหนดไว้ 2.2) เป้าหมายเชิงบริบท (Contextual goal) คือ กระบวนการขององค์กรมีการปรับเปลี่ยนตามสถานการณ์ที่เกิดโดยเฉพาะขององค์กร และ 2.3) เป้าหมายการเข้าถึงและการรักษาความปลอดภัยกระบวนการทำงานขององค์กรควรเป็นความลับเท่านั้น

3. วัฏจักร ได้แก่ 3.1) การวางแผน 3.2) การออกแบบ 3.3) การจัดซื้อ 3.4) การปฏิบัติงาน 3.5) การประเมินติดตาม และ 3.6) ปรับปรุงแก้ไขให้เป็นปัจจุบัน โดยจะต้องมีกระบวนการดำเนินงานให้มีความเหมาะสมกับสภาพการทำงาน

4. แนวปฏิบัติที่ดี ได้แก่ 4.1) แนวปฏิบัติภาพรวม เช่น ควรมีคำแถลงการณ์การปฏิบัติการ (Statement of Actions) เพื่อใช้ในการควบคุมระดับความเสี่ยง 4.2) ผู้บริหารระดับสูงขององค์กรจะต้องทำการตัดสินใจ เช่น สามารถเลือกและตัดสินใจในการนำกระบวนการมาประยุกต์ใช้งาน เป็นต้น ดังภาพที่ 2.9



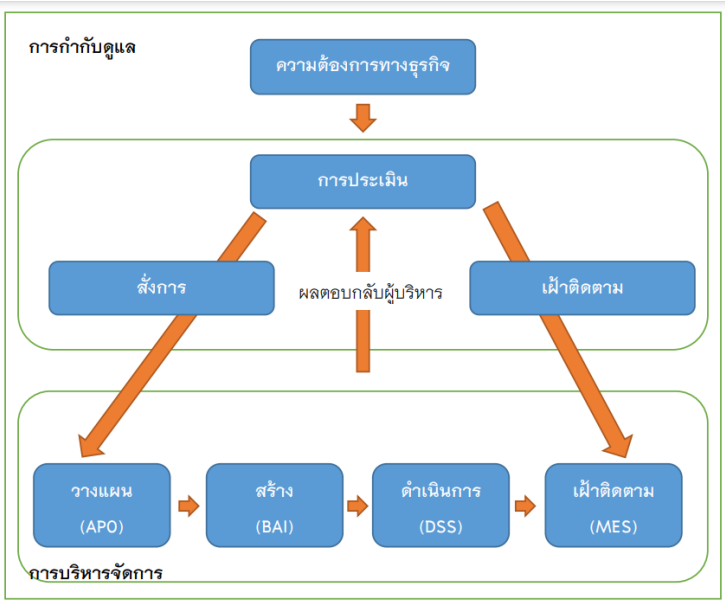
ภาพที่ 2.9 แผนผังองค์ประกอบปัจจัยเอื้อด้านการบริการโครงสร้างพื้นฐานและระบบงาน

ที่มา: ISACA (2012)

หลักการที่ 5 การแยกเรื่องของการกำกับดูแลกับการบริหารจัดการ (Separating Governance From Management) เป็นการแบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ เนื่องจากมีกิจกรรมที่ต่างกัน และโครงสร้างการจัดองค์กรที่แตกต่างกัน ซึ่งได้ให้มุมมองและจุดประสงค์ที่แตกต่างกัน คือ

5.1 การกำกับดูแล (Governance) มีจุดประสงค์เพื่อให้มั่นใจ เช่น ความต้องการเงื่อนไข และทางเลือกของผู้เกี่ยวข้องที่ได้รับการประเมิน เพื่อกำหนดวัตถุประสงค์ที่องค์กรต้องการให้เห็นชอบร่วมกัน และการกำหนดทิศทางผ่านการตัดสินใจ และการจัดลำดับ รวมถึงการเฝ้าติดตามผลการดำเนินงานและการปฏิบัติตามวัตถุประสงค์ที่ตกลงร่วมกัน

5.2 การบริหารจัดการ (Management) มีจุดประสงค์การวางแผน การดำเนินงาน และเฝ้าติดตามกิจกรรมต่างๆ ให้สอดคล้องกับทิศทางที่กำหนด ดังภาพที่ 2.10



ภาพที่ 2.10 แผนผังความสัมพันธ์ระหว่างการกำกับดูแลและการบริหารจัดการ

ที่มา : ISACA (2012)

ดังนั้น จากภาพที่ 2.10 องค์ประกอบการกำกับดูแลและการบริหารจัดการของกรอบปฏิบัติ COBIT 5 ได้มีการกำหนดกระบวนการต่าง ๆ ในด้านการกำกับดูแล และการบริหารจัดการ ซึ่งกระบวนการทำงานมาจากหลักการของ COBIT 4.1 มาใช้ในการกำหนดกระบวนการควบคุม ซึ่งบางกระบวนการที่มีการแบ่งแยก เพื่อกำหนดแนวทางกิจกรรมการบริหารจัดการเทคโนโลยีสารสนเทศเฉพาะเจาะจงมากขึ้น และมีการปรับปรุงกระบวนการให้เหมาะสมจาก 4 กระบวนการเปลี่ยนเป็น 5 กระบวนการ และมีการเพิ่มกระบวนการด้านกำกับดูแลองค์กรมาเป็นส่วนหนึ่งของกระบวนการควบคุมกำกับดูแลเทคโนโลยีสารสนเทศ ปรับจาก 34 กระบวนการ มาเป็น 37 กระบวนการ จากทั้งหมด 5 ประเด็น โดยมีการกำหนดรหัสกระบวนการจาก 2 ตัว เป็น 3 ตัว ได้แก่ 1) EDM (Evaluation, Direct and Monitor) 2) APO (Align, Plan and Organize) 3) BAI (Build, Acquire and Implement) 4) DSS (Deliver, Service and Support) และ5) MEA (Monitor,

Evaluation and Access) (Ibrahim & Nurpulaela, 2017; Maria et al., 2012; Musa et al., 2014) ดังภาพที่ 2.11 รายละเอียดดังนี้

กระบวนการต่างๆ สำหรับการควบคุมกำกับดูแลไอทีระดับองค์กร ประเมิน สั่งการ และเฝ้าติดตาม							
จัดวางแนว จัดทำแผน และจัดระบบ							เฝ้าติดตาม วัดผล และประเมิน
APO01 บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที	APO02 บริหารจัดการกลยุทธ์	APO03 บริหารจัดการสถาปัตยกรรมองค์กร	APO04 บริหารจัดการนวัตกรรม	APO05 บริหารจัดการกลุ่มของชุดโครงการ	APO06 บริหารจัดการงบประมาณและต้นทุน	APO07 บริหารจัดการทรัพยากรบุคคล	
APO08 บริหารจัดการความสัมพันธ์	APO09 บริหารจัดการข้อตกลงการให้บริการ	APO10 บริหารจัดการผู้ขายหรือผู้ให้บริการ	APO11 บริหารจัดการคุณภาพ	APO12 บริหารจัดการความเสี่ยง	APO13 บริหารจัดการความมั่นคงปลอดภัย		MEA01 เฝ้าติดตาม วัดผล และประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน
จัดสร้าง จัดหา และนำไปใช้							
BAI01 บริหารจัดการโครงการและชุดโครงการ	BAI02 บริหารจัดการข้อกำหนดความต้องการ	BAI03 บริหารจัดการการระบุและจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ	BAI04 บริหารจัดการความพร้อมใช้งานและขีดความสามารถ	BAI05 บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล	BAI06 บริหารจัดการการเปลี่ยนแปลง	BAI07 บริหารจัดการการยอมรับการเปลี่ยนและการปรับเปลี่ยน	MES02 เฝ้าติดตามวัดผลและประเมินระบบการควบคุมภายใน
BAI08 บริหารจัดความรู้	BAI09 บริหารจัดการสินทรัพย์	BAI10 บริหารจัดการองค์ประกอบของระบบ					
ส่งมอบ ให้บริการ และสนับสนุน							MEA03 เฝ้าติดตามวัดผลและประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก
DSS01 บริหารจัดการปฏิบัติการ	BSS02 บริหารจัดการคำร้องขอ บริการและเหตุการณ์ที่เกิดขึ้น	DSS03 บริหารจัดการปัญหา	DSS04 บริหารจัดการความต่อเนื่อง	DSS05 บริหารจัดการบริการด้านความมั่นคงปลอดภัย	DSS06 บริหารจัดการการควบคุมกระบวนการทางธุรกิจ		
กระบวนการสำหรับการบริหารจัดการไอทีระดับองค์กร							

ภาพที่ 2.11 โครงสร้างกระบวนการสำหรับการกำกับดูแล และการบริหารจัดการเทคโนโลยีสารสนเทศ ระดับองค์กรตามกระบวนการใน COBIT 5

ที่มา : ISACA (2012)

โดยสรุปเกี่ยวกับมาตรการ และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร มีวัตถุประสงค์เพื่อให้การดำเนินงาน เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และเป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติจากทุกหน่วยอย่างต่อเนื่อง มีการตรวจสอบและปรับปรุง

อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไป ดังนั้น นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จะเป็นเครื่องมือให้กับผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กรได้

2.1.6.3 การศึกษางานวิจัยที่เกี่ยวข้องและมาตรฐานความมั่นคงปลอดภัยสารสนเทศอื่น ๆ

เนื่องจากงานวิจัยเป็นการศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัย ด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ผู้วิจัยได้มีการศึกษางานวิจัยเพิ่มเติมเพื่อให้การทบทวนวรรณกรรมมีความแน่ชัดจากการศึกษางานวิจัย โดยสามารถแบ่งเป็น 3 ประเด็น ได้แก่ 1) การประยุกต์หลักการควบคุมทั่วไปของระบบสารสนเทศทางการบัญชีตามสภาพแวดล้อมของธุรกิจ 2) ความสัมพันธ์หลักการควบคุมภายในกับการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และ 3) หลักการควบคุมภายในเชิงเทคโนโลยีสารสนเทศ (IT Governance) สามารถสรุปประเด็นได้ดังต่อไปนี้

(1) การประยุกต์หลักการควบคุมทั่วไปของระบบสารสนเทศทางการบัญชีตามสภาพแวดล้อมของธุรกิจแต่ละประเภท โดยงานวิจัยของนันทิดา โยธานวล และศักดิ์ชาย จันทร์เรือง (2558) ได้ทำการวิจัยเรื่องการควบคุมภายในทั่วไปของระบบสารสนเทศทางการบัญชี จากกรณีศึกษา บริษัท อี.เทค จำกัด จากการสัมภาษณ์ และสังเกตการณ์พนักงานตามหลักการควบคุมทั่วไปของระบบสารสนเทศทางการบัญชี พบว่า การควบคุมภายในด้านสารสนเทศของบริษัทอยู่ในระดับดี เนื่องจาก บริษัทมีการปฏิบัติงานตามแนวทางด้านการควบคุมทั่วไปของระบบสารสนเทศ จึงส่งผลให้มีระบบการทำงานทางสารสนเทศมีประสิทธิภาพ ข้อมูลมีความครบถ้วน ถูกต้อง โปร่งใส และสามารถตรวจสอบได้ สอดคล้องกับงานวิจัยของภิรมย์พร เยาคำ และคณะ (2559) ได้ทำการศึกษาการควบคุมภายในและการนำระบบสารสนเทศมาช่วยในการทำงานด้านการเงินและบัญชี ที่ส่งผลกต่อระบบด้านการเงินและบัญชีของหน่วยงานภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS) ของหน่วยงานในจังหวัดระนอง พบว่า ระบบ GFMIS มีประสิทธิภาพโดยรวมอยู่ในระดับที่ดี ทั้งด้านความโปร่งใส และความถูกต้องของข้อมูลในระบบ ซึ่งระบบ GFMIS เป็นระบบที่ช่วยเพิ่มประสิทธิภาพในการทำงานด้านการเงินการคลังของหน่วยงานภาครัฐ และ Hou et al. (2020) ได้ทำการศึกษาที่เกี่ยวกับ network security and privacy security in ubiquitous electricity Internet of Things พบว่า ในช่วงปีที่ผ่านมาที่เกิดเหตุการณ์ไฟฟ้าดับจากการโจมตีทางไซเบอร์ส่งผลกระทบต่อความปลอดภัยของข้อมูล โดยเฉพาะเครือข่ายในด้านพลังงานที่เกี่ยวข้องกับแหล่งจ่ายไฟโดยตรง โดยงานวิจัยส่วนใหญ่จะมุ่งเน้นไปที่การวิเคราะห์ความปลอดภัยของเครือข่ายและความปลอดภัยความเป็นข้อมูลส่วนตัว ภายใต้สภาพแวดล้อมของระบบ Internet of thing ซึ่งอธิบายถึงแนวคิดและสถาปัตยกรรมของการรักษาความปลอดภัยเครือข่ายในสภาพแวดล้อม Internet of Things ที่ใช้ไฟฟ้าแพร่หลาย จากการวิเคราะห์แนวโน้มการพัฒนาเครือข่ายด้านข้อกำหนด และการดำเนินการทางด้านเทคนิค การศึกษานี้นำเสนอถึงระบบอัจฉริยะและการจัดซื้อที่เหมาะสมสำหรับระบบการรับข้อมูลและการตรวจสอบอุปกรณ์การสื่อสารแบบสองทาง โดยมีการกำหนดรหัสโปรโตคอลที่ใช้หมายเลขสุ่มเพื่อตรวจสอบตัวตนของทั้งสองฝ่ายในการสื่อสารจากคีย์ความปลอดภัยที่ฝังอยู่ในอุปกรณ์ เพื่อระบุความถูกต้องตามกฎหมายของข้อมูลส่วนบุคคลของอุปกรณ์ที่ใช้เข้าถึง หลีกเลี่ยงการใช้บริการของบุคคลที่สาม เพื่อป้องกันการโจมตีจากคนกลางอย่างมีประสิทธิภาพและการกระทำซ้ำ ๆ จากการโจมตีทำให้มั่นใจได้ถึงความน่าเชื่อถือ

โดยจากการทดลองใช้งานปัจจุบันแสดงให้เห็นว่า เวลาในการเข้ารหัสและถอดรหัสข้อมูลของอัลกอริทึมทั่วไปกับการดำเนินการพัฒนาอัลกอริทึมด้วยวิธีการใหม่จะมีประสิทธิภาพดีกว่าที่ช่วยในการป้องกันการเข้าถึง ซึ่งสอดคล้องกับระบบควบคุมอุตสาหกรรมที่ต้องการการสื่อสารที่ทันท่วงที รวมถึง Bertino (2017) ได้เสนอภาพร่างความเสี่ยงด้านความมั่นคงปลอดภัยและความเป็นส่วนใน IoT และความมั่นคงปลอดภัยด้านแอพพลิเคชันโดเมน รวมทั้งเสนอแผนงานด้านความมั่นคงปลอดภัยใน 3 ด้าน ได้แก่ 1) การควบคุมการเข้าถึง เป็นการรักษาความมั่นคงปอลดภัยขั้นพื้นฐาน เมื่อต้องมีการแบ่งปันข้อมูลที่มีความสำคัญกับอุปกรณ์และเครือข่ายอื่น 2) ความมั่นคงปลอดภัยของซอฟต์แวร์และเฟริมแวร์ ซอฟต์แวร์เป็นองค์ประกอบสำคัญของ IoT มีการโจมตีหลายครั้งที่ทำให้ซอฟต์แวร์ทำงานผิดพลาด และยังมีการโจมตีโดยอาศัยช่วงการอัพเดทของเฟริมแวร์ด้วย และ 3) ระบบตรวจจับการบุกรุก ที่เหมาะสมกับ IoT จะต้องได้รับการออกแบบมาเพื่อรองรับการกำหนดค่าที่ยืดหยุ่นในระบบ IoT และที่สำคัญคือต้องการตรวจจับการบุกรุกได้โดยที่ไม่ต้องติดตั้งซอฟต์แวร์เพิ่มเติมในอุปกรณ์ IoT

ดังนั้น การนำระบบข้อมูลสารสนเทศทางมาประยุกต์ใช้กับงานต่าง ๆ ของหน่วยงาน เช่น งานบริการ งานการเงินและบัญชี งานการตลาด งานบริหารทั่วไป เป็นต้น ของธุรกิจขนาดกลางและขนาดย่อม และมีปัจจัยต่าง ๆ ที่ส่งผลต่อการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธุรกิจ ซึ่งการวิจัยของ Dung and Tuan (2015) ได้ทำการสอบถามความคิดเห็นของเจ้าหน้าที่ที่ทำบัญชีในธุรกิจขนาดกลางและขนาดย่อม ในเรื่องปัจจัยที่ส่งผลกระทบในเรื่องการนำระบบสารสนเทศทางการบัญชีมาใช้ในกิจการได้แก่ อุปกรณ์คอมพิวเตอร์ โปรแกรมซอฟต์แวร์ และข้อมูลรายงานทางการเงินของระบบสารสนเทศทางการบัญชี โดยเฉพาะปัจจัยด้านข้อมูลรายงานทางการเงินเป็นสิ่งสำคัญมากที่สุดที่ใช้ในการตัดสินใจ รองลงมาเป็นส่วนประกอบของโปรแกรมซอฟต์แวร์ และอุปกรณ์คอมพิวเตอร์ สอดคล้องกับ Eigeles (2006) ได้ทำการวิจัยเรื่อง การควบคุมภายในของระบบสารสนเทศทางการบัญชีในสภาพแวดล้อมของระบบเครือข่าย โดยใช้โครงสร้างการทำงาน ระหว่างระบบการควบคุมภายในกับระบบบัญชีให้สอดคล้องกับหลักการยืนยันตัวตนและระบุตัวตน ซึ่งผลการวิจัยชี้ให้เห็นว่า ประสิทธิภาพของการตรวจสอบสิทธิ กำหนดสิทธิเข้าใช้และการบริหารจัดการแบบอัจฉริยะที่มีความยืดหยุ่นและครอบคลุมสำหรับปัญหา นำแนวทางปฏิบัติที่เป็นไปได้ของการสื่อสารที่มีความปลอดภัยมาใช้ในระบบรักษาความปลอดภัย และหลักการ I3A สามารถจัดหาโครงสร้างแบบเปิดซึ่งมีการให้อำนาจในด้านการสื่อสารที่มีความปลอดภัย และการบริหารจัดการของการใช้งานซอฟต์แวร์ระบบ Firmware สำหรับอุปกรณ์แบบพกพา อย่างเช่น แท็บเล็ต โทรศัพท์มือถือ และอุปกรณ์คอมพิวเตอร์ เป็นต้น ซึ่งทุกคนสามารถได้รับประโยชน์ โดยไม่จำเป็นต้องมีความรู้ทักษะพิเศษหรือความพยายามในการลงทุนภายนอก รวมถึง Cox. (2012) ทำการศึกษาเรื่อง Information Systems User Security: A Structured model of the knowing-doing gap เพื่อศึกษาความปลอดภัยของผู้ใช้ระบบสารสนเทศ โดยใช้แบบจำลองโครงสร้างของช่องว่างทางความรู้ พบว่า ผู้ใช้ระบบข้อมูลขององค์กรมักจะมีส่วนร่วมในพฤติกรรมเสี่ยงที่สามารถคุกคามความปลอดภัยและความสมบูรณ์ขององค์กร โดยการเปิดเผยข้อมูลที่ละเอียดอ่อนหรือทำให้การรักษาความปลอดภัยขอบเขตเทคโนโลยีที่มีอยู่อ่อนแอลง พฤติกรรมของผู้ใช้ที่มีความเสี่ยงนี้อาจเกิดขึ้นโดยตั้งใจ หรือไม่ตั้งใจ แต่ในกรณีใดกรณีหนึ่งอาจสร้างความเสียหายร้านแรงต่อชื่อเสียงขององค์กร รวมทั้งอาจขยายไปสู่อันตรายต่อลูกค้า และลูกค้าขององค์กรด้วย ผู้ใช้ระบบสารสนเทศที่

ไม่ปฏิบัติตามนโยบายความปลอดภัยขององค์กร แม้ว่าพวกเขาจะทราบนโยบายดังกล่าวแล้วก็ตาม เรียกว่าเป็นพฤติกรรมที่ละเลยของผู้ใช้งาน งานวิจัยนี้ตรวจสอบความเข้าใจด้านการรับประกันข้อมูลและความตระหนักด้านความปลอดภัยในระดับผู้ใช้โดยการพัฒนารูปแบบโครงสร้างของช่องว่างในการรับรู้ การกระทำของผู้ใช้ตัวแบบตรวจสอบบทบาทของการหลงตัวเองในองค์กร และผลกระทบต่อทัศนคติของผู้ใช้ต่อการปฏิบัติตามนโยบายและขั้นตอนการรักษาความปลอดภัยของข้อมูลองค์กร นอกจากนี้ยังรวมถึงการรับรู้ว่าภัยคุกคามเป็นปัจจัยที่ส่งผลต่อทัศนคติของผู้ใช้ต่อการปฏิบัติตามกฎความปลอดภัยของข้อมูล เช่นเดียวกับบรรทัดฐานส่วนตัวและการควบคุมพฤติกรรมการรับรู้ที่สอดคล้องกับทฤษฎี พฤติกรรมที่วางแผนไว้ แบบจำลองที่มีโครงสร้างนี้ให้กรอบงานและคำอธิบายเกี่ยวกับพฤติกรรมความปลอดภัยของข้อมูลผู้ใช้และช่องว่างในการทำความเข้าใจ และ Ismail and Zainab (2011) ได้ทำการศึกษา Information systems security in special and public libraries: An assessment of status เพื่อประเมินการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศของการใช้ห้องสมุด โดยชุดเครื่องมือการประเมินชื่อว่า Library Information System Security Assessment Model (LISSAM) เพื่อประเมินสภาพการดำเนินงานจำนวน 155 แห่งสำหรับห้องสมุดสาธารณะ และห้องสมุดวัตถุประสงค์พิเศษของประเทศมาเลเซีย ซึ่งการศึกษานี้มีวัตถุประสงค์เพื่อกำหนดสถานการณ์ดำเนินการขององค์ประกอบทางเทคโนโลยีและองค์กรตามแบบจำลอง LISSAM มีการนำเสนอดัชนีการใช้งานและเครื่องมือให้คะแนนเพื่อประเมินมาตรการป้องกันความปลอดภัยทางด้านสารสนเทศ (Information Security) ของห้องสมุด ซึ่งข้อมูลที่ใช้มาจากแบบสอบถามที่รวบรวมจากบุคคลทั้งหมด 50 คนที่รับผิดชอบระบบสารสนเทศ Information systems และ Information Technology ในห้องสมุดวัตถุประสงค์พิเศษและห้องสมุดสาธารณะในมาเลเซีย ผลการวิจัยพบว่า ห้องสมุดมากกว่าร้อยละ 95 มีการใช้งานเทคโนโลยีในระดับสูง แต่ร้อยละ 54 มีมาตรการองค์กรที่แยกพอสมควร โดยเฉพาะอย่างยิ่งการขาดกระบวนการรักษาความปลอดภัย เครื่องมือการบริหาร และกิจกรรมสร้างความตระหนักรู้

(2) ความสัมพันธ์หลักการควบคุมภายในกับการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พบว่า การควบคุมภายในของระบบสารสนเทศทางการบัญชีในสภาพของระบบเครือข่ายโครงสร้างการทำงานของระบบบัญชีกับหลักการควบคุมภายในแบบกรอบการทำงาน COSO ซึ่งหลักการควบคุมภายในขององค์กร ทั้งภาครัฐและภาคเอกชนจะประสบผลสำเร็จได้ขึ้นอยู่กับวัตถุประสงค์ในการดำเนินงานด้านการเงินการบัญชี สภาพแวดล้อมขององค์กร ความพร้อมของอุปกรณ์ในการงานระบบสารสนเทศทางการบัญชี รวมทั้งโครงสร้างองค์กรที่เป็นไปตามมาตรฐานที่กำหนด และการพัฒนาบุคคลให้มีความรู้ ความสามารถพื้นฐานในการใช้งานระบบสารสนเทศทางการบัญชี และพัฒนาระบบควบคุมภายในระบบสารสนเทศทางบัญชีภายในองค์กรมีประสิทธิภาพมากขึ้น และลดความเสี่ยงที่อาจจะเกิดขึ้นทันท่วงที (ธารินี เณรวงศ์, 2558) ซึ่งสอดคล้องกับงานวิจัยของ Rubino et al. (2017) ได้ทำการศึกษาเรื่องความสัมพันธ์ระหว่างการควบคุมเชิงเทคโนโลยีสารสนเทศ กับสภาพแวดล้อมในการควบคุมโดยใช้หลักการวิเคราะห์การควบคุมภายในบนพื้นฐาน 3 อย่าง ได้แก่ 1) การควบคุมภายในองค์กร (Organization Controls) 2) กระบวนการควบคุมภายใน (Process Controls) และ 3) การควบคุมตัวแปรที่สนับสนุน (Soft Variables Controls) หลักการควบคุมภายในจะประสบความสำเร็จได้ขึ้นอยู่กับการบริหารจัดการและพนักงานภายในองค์กร รวมถึงการวิเคราะห์โครงสร้างการควบคุมสภาพแวดล้อม และการควบคุมเฉพาะระบบปฏิบัติการ และผู้สอบบัญชีสามารถศึกษาความรู้ในเรื่องการควบคุม

ความมั่นคงปลอดภัยสารสนเทศ และเข้าใจกระบวนการทำงานขององค์กร รวมทั้งสามารถระบุความเสี่ยงที่เกิดขึ้นได้ในระบบการควบคุมภายใน และได้ทำการศึกษาผลกระทบของกรอบการดำเนินงานด้านธรรมาภิบาลเทคโนโลยีสารสนเทศ (IT Governance) ที่ส่งผลต่อสภาพแวดล้อมของการควบคุมภายในองค์กร โดยอ้างอิงโครงสร้างและกระบวนการทำงานของกรอบการดำเนินงานการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (COBIT) ตามหลักการ 5 ประการ ได้แก่ การประเมิน (Evaluate) การสั่งการและกำกับติดตาม (Direct and Monitor) (EDM); Align , plan and organize (APO); Build, acquire and implement (BAI); Deliver, Service and Support (DSS); และ Monitor, Evaluate and Assess (MEA) รวมถึง Sharbaf (2014) ได้ทำการศึกษาเรื่อง A New Perspective to Information Security: Total Quality Information Security Management นำเสนอแนวคิดใหม่ในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยการออกแบบการพัฒนาและการสร้างแบบจำลอง TQISM เพื่อการรักษาความมั่นคงสารสนเทศและสินทรัพย์ขององค์กร และการบริหารจัดการของผู้บริหาร พนักงาน และผู้มีส่วนเกี่ยวข้องมีส่วนร่วมในการพัฒนาอย่างต่อเนื่อง

ทั้งนี้ Smet and Mayer (2016) ได้ทำการศึกษาการบูรณาการจัดการความเสี่ยง และการกำกับดูแลองค์กรที่ดีด้านระบบสารสนเทศ ด้วยวิธีการระบบประกอบด้วย 3 องค์ประกอบ GRC ซึ่งเป็นตัวย่อที่ครอบคลุมหลักสามด้านของการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ โดยมีวัตถุประสงค์เพื่อศึกษาการดำเนินการเชื่อมโยง บูรณาการเกี่ยวกับ 3 องค์ประกอบ GRC ว่ามีการนำไปบูรณาการในระดับใด พบว่า การกำกับดูแลแบบบูรณาการความเสี่ยงที่เป็นการปฏิบัติตามกฎ ระเบียบภายในองค์กรสอดคล้องกับความต้องการทางด้านนโยบายภายใน ซึ่งเป็นความรับผิดชอบของผู้เกี่ยวข้อง และมีความสัมพันธ์กับการบริหารการจัดการความเสี่ยงในองค์กร เพื่อให้เกิดแนวคิดที่มีประสิทธิภาพของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศขององค์กร และชาญชัย ประมูลเฉโก และ วศิณ ชูประยูร (2564) ได้ทำการวิจัยเพื่อพัฒนาแผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร โดยมีวัตถุประสงค์เพื่อศึกษาความคิดเห็นของกำลังพลกรมการสื่อสารทหาร กองบัญชาการกองทัพไทยเกี่ยวกับกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ 2) พัฒนาและพิจารณา (ร่าง) แผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร พบว่า กำลังพลส่วนใหญ่มีความต้องการมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในระดับมาก และการทดสอบสมมติฐาน พบว่า ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีอิทธิผลต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศที่ขนาดอิทธิพล (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) แผนดังกล่าว ได้ผ่านการพิจารณาเห็นชอบจากคุณวุฒิของกรมการสื่อสารทหาร จำนวน 11

คน ซึ่งสามารถนำไปปรับปรุงกระบวนการทำงานด้านสภาพแวดล้อมการควบคุมภายในภาพรวม รวมทั้งช่วยให้ผู้บริหารและผู้สอบบัญชีสามารถบริหารความเสี่ยงภายในด้านระบบเทคโนโลยีสารสนเทศทางการบัญชีได้

(3) หลักการกำกับดูแลที่ดีเชิงเทคโนโลยีสารสนเทศ (IT Governance) โดยการกำกับดูแลที่ดีเชิงเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งในหลักการกำกับดูแลกิจการที่ดี (Good Governance) ซึ่งจากงานวิจัยได้มีการศึกษาเรื่องการสืบสวนอุปสรรคของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานจากกรณีศึกษาธนาคารของประเทศจอร์แดน พบว่า อุปสรรคที่ทำให้การรักษาความมั่นคงปลอดภัยสารสนเทศที่มีปัญหา 3 อันดับแรก ได้แก่ 1) พนักงานป้อนข้อมูลที่ไม่เหมาะสมด้วยความประมาทเลินเล่อ 2) พนักงานลบข้อมูลโดยไม่ได้ตั้งใจ และ 3) พนักงานจงใจป้อนข้อมูลที่ไม่เหมาะสม และส่วนใหญ่จะเป็นปัญหาที่เกิดจากการประมาทเลินเล่อ (Hayale & Khadra, 2008) รวมถึงยังมีกรอบการควบคุมภายในเชิงเทคโนโลยีสารสนเทศอื่น ๆ ที่ช่วยให้การดำเนินงานด้านเทคโนโลยีได้อย่างรัดกุม ซึ่งงานวิจัยของ Hessou and Lai (2017) ได้ทำการศึกษาเรื่องความน่าจะเป็นเรื่องการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในรูปแบบของกรอบการดำเนินงานของ Basel III ซึ่งเป็นกรอบการควบคุมภายในของธนาคารทั่วโลกที่นิยมใช้กัน โดยทำการวิเคราะห์ข้อมูล ความเสี่ยงเหตุการณ์ต่าง ๆ ของสหกรณ์ออมทรัพย์ของประเทศแคนนาดา พบว่า การนำกรอบการดำเนินงาน Basel III มาพัฒนาด้านการควบคุมภายในเชิงเทคโนโลยีสารสนเทศของสหกรณ์ช่วยให้หน่วยงานมีคุณภาพ

ทั้งนี้ กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับหน่วยงาน ตามวัตถุประสงค์การควบคุมภายในด้านสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง (Control Objectives for Information and related Technology: COBIT) เพื่อให้หลักการควบคุมภายในเทคโนโลยีสารสนเทศขององค์กรมีความสอดคล้องกับสภาพแวดล้อมและนโยบายด้านการควบคุมภายในเป็นที่นิยมของหน่วยงาน รวมถึงมีการพัฒนา ปรับปรุง และทบทวนกรอบงานการกำกับดูแลเทคโนโลยีสารสนเทศอย่างต่อเนื่องมาจนถึงปัจจุบัน ซึ่งสอดคล้องกับงานวิจัยของ วรัญญาภรณ์ สิริพิพัฒนพร และสมชาย นำประเสริฐชัย (2558) ได้ทำการศึกษาประเด็นความเสี่ยงด้านการปฏิบัติงานด้านเทคโนโลยีสาสนเทศของหน่วยงานภาครัฐ โดยใช้หลักการ COBIT ที่ใช้ในกระบวนการธุรกิจความเสี่ยงทาง ICT ของหน่วยงานภาครัฐ พบว่า การขาดแคลนบุคลากรที่มีความรู้ ทักษะ ความสามารถด้านเทคโนโลยีสารสนเทศ คอมพิวเตอร์ขั้นสูง และด้านการเงินการคลัง เนื่องจากเงินงบประมาณที่ได้รับมาไม่เพียงพอต่อการพัฒนาระบบและความต้องการด้านเทคโนโลยีสารสนเทศของคนในหน่วยงาน และ Ohki et al. (2009) ได้ทำการศึกษาเรื่อง Information Security Governance Framework ผลจากการศึกษาทำให้ได้ Information Security Governance model ซึ่งเป็นโมเดลสำหรับการบริหารจัดการความมั่นคงปลอดภัยในองค์กร ประกอบไปด้วยกระบวนการ Direct, Montor, Evaluate, Oversee และ Report โดยกระบวนการทั้ง 5 กระบวนการนี้ ครอบคลุมฟังก์ชันที่ขาดหายไปของการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

หลักการและมาตรฐานการควบคุมและกำกับดูแลการใช้เทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพ ในการทำงานภายในองค์กรปัจจุบัน สามารถนำมาประยุกต์ด้วยกันได้ อย่างเช่น การนำกรอบงาน COBIT และหลักการ ISO 27001 มาใช้งานร่วมกันในด้านการควบคุมความปลอดภัยของเทคโนโลยีสารสนเทศ ซึ่งงานวิจัยของ ธัญญรัตน์ ปิยวัฒน์กานนท์ และ ชุติมา เบี้ยวไขมุข (2560) ได้นำหลักการทั้งสองมาช่วยในการเพิ่มเต็มช่องว่างในการทำงานด้านการบริหารความมั่นคงปลอดภัยสารสนเทศ และจากการศึกษามาตรฐานการจัดการความมั่นคงปลอดภัย ได้แก่

มาตรฐาน ISO/IEC 27001:20013 ISO/IEC 27001:2005 COBIT ITIL และ ISO17799 เป็นต้น ซึ่งมาตรฐานดังกล่าวมีความสอดคล้องกันและและมีกระบวนการองค์ประกอบที่เกี่ยวข้องกัน รวมถึง Yazdanmehr and Wang (2016). ได้ทำการศึกษาโดยการสำรวจบทบาท อำนาจหน้าที่ บรรทัดฐานในการปฏิบัติงานตามนโยบายความปลอดภัยข้อมูลขององค์กร (ISP) ของพนักงาน จากทฤษฎีบรรทัดฐานทางสังคม และวรรณกรรมที่เกี่ยวข้องเชิงจริยธรรม และเสนอรูปแบบจำลองเพื่อตรวจสอบบรรทัดฐานส่วนบุคคลที่เกี่ยวข้องกับการปฏิบัติงานตามนโยบายความปลอดภัยข้อมูลของพนักงานว่ามีการดำเนินการอย่างไร และรวบรวบข้อมูลเพื่อวิเคราะห์ตามสมมติฐานที่ตั้งขึ้น พบว่า บรรทัดฐานส่วนบุคคลที่เกี่ยวข้องกับนโยบายความปลอดภัยข้อมูลองค์กร (ISP) นำไปสู่พฤติกรรมการปฏิบัติตามข้อกำหนดของนโยบายความปลอดภัยข้อมูลองค์กร (ISP) ส่งผลให้การดำเนินการมีความเข้มแข็งขึ้น โดยเกิดจากความรับผิดชอบส่วนบุคคลและบรรทัดฐานทางสังคมที่มาจากบรรยากาศทางจริยธรรมขององค์กร สอดคล้องกับงานวิจัย สุวันต์นา เสมอเนตร (2562) การพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC) พบว่า การพัฒนาอย่างรวดเร็วของเทคโนโลยีที่ใช้ง่าย และมีราคาถูกทำให้ประชากรสามารถเข้าถึงสารสนเทศได้อย่างไร้ขีดจำกัด ประเทศใช้เทคโนโลยีขับเคลื่อนระบบเศรษฐกิจและสังคม เพิ่มรายได้และลดความเหลื่อมล้ำของประชาชนอย่างไรก็ตาม ภัยคุกคามไซเบอร์ก็ทวีความรุนแรงไปพร้อมกับการเติบโตระบบเศรษฐกิจและสังคมดิจิทัล ผู้วิจัยจึงได้ศึกษาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อประโยชน์ในการป้องกันสินทรัพย์สารสนเทศที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศ ของศูนย์ปฏิบัติการ MOPH IDC (Ministry of Public Health Internet Data Center) จากภัยคุกคามภายในและภายนอกในการดำเนินงานด้านเทคโนโลยีสารสนเทศโดยนำมาตรฐาน ISO/IEC 27001: 2013 มาประยุกต์ใช้ซึ่งมีการดำเนินการแบ่งออกเป็น (1) ศึกษามาตรฐาน (2) วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (3) พัฒนาระบบและแนวทางปฏิบัติในการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ตามมาตรฐานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001: 2013 และ (4) จัดทำข้อเสนอแนะเพื่อสร้างแนวทางปฏิบัติจากผลความพึงพอใจของผู้รับบริการระบบบริหารความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO/IEC 27001: 2013 พบว่า กลุ่มที่ 1 ผู้ใช้บริการ VM (Virtual Machine) และ web hosting มีความพึงพอใจในภาพรวมทุกด้านในระดับมาก คะแนนเฉลี่ย 4.17 และกลุ่มที่ 3 ผู้รับบริการทั่วไป มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก คะแนนเฉลี่ย 3.98 เช่นกัน การนำมาตรฐาน ISO/IEC 27001: 2013 เข้ามาใช้เพื่อเพิ่มความมั่นคงปลอดภัยขององค์กรให้เป็นไปตามมาตรฐานสากล ผลการดำเนินงานประสบผลสำเร็จเป็นอย่างดี

ดังนั้น ในเบื้องต้นผู้วิจัยจึงได้ทำการวิเคราะห์หาองค์ประกอบที่สำคัญสำหรับเป็นแนวทางในการบริหารความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นการสังเคราะห์องค์ประกอบจากการศึกษา และทบทวนมาตรฐานความมั่นคงปลอดภัยสารสนเทศของมาตรฐาน ISO/IEC 27001:20013 ISO/IEC 27001:2005 และ COBIT 5 และเสนอให้กับผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศช่วยตรวจสอบความสอดคล้องและความเป็นไปได้ ได้แบ่งออกเป็นจำนวน 4 องค์ประกอบ 15 ตัวชี้วัด ดังตารางที่ 2.3 โดยมีรายละเอียดและข้อกำหนดที่สำคัญของแต่ละองค์ประกอบ ดังนี้

ตารางที่ 2.3 การวิเคราะห์องค์ประกอบที่สำคัญ มาตรฐานความมั่นคงปลอดภัยสารสนเทศของมาตรฐาน ISO/IEC 27001: 20013 ISO/IEC 27001: 2005 และ COBIT 5

องค์ประกอบ	ISO/IEC 27001:20013	ISO/IEC 27001:2005	COBIT 5
องค์ประกอบที่ 1 การกำกับดูแล การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ			
1. การกำกับดูแล (Governance) ได้แก่			√
- ดำเนินงานการกำกับดูแลและการบำรุงรักษา			
- การส่งมอบผลประโยชน์			
- ความเสี่ยงที่เหมาะสม			
- การใช้ทรัพยากรให้เกิดประโยชน์สูงสุด			
- ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย			
2. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ	√	√	√
3. การบริหารจัดการทรัพย์สิน	√	√	√
4. การติดตาม วัดผล และประเมินผล ได้แก่			√
- เฝ้าติดตาม วัดผลและประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน			
- เฝ้าติดตาม วัดผลและประเมินระบบการควบคุมภายใน			
- เฝ้าติดตาม วัดผลและประเมินการปฏิบัติตามข้อกำหนดของหน่วยงานภายนอก			
5. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	√	√	√
6. ความสอดคล้องที่เกี่ยวข้องกับกฎหมายและการป้องกันในขั้นตอนต่าง ๆ	√	√	√
องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ			
7. การควบคุมการเข้าถึง	√	√	
8. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม การดำเนินงานและการสื่อสารข้อมูล	√	√	√
9. การจัดหา การพัฒนา และการบำรุงรักษาระบบ	√	√	
10. ความสัมพันธ์กับผู้ให้บริการภายนอก	√		√

ตารางที่ 2.3 (ต่อ)

องค์ประกอบ	ISO/IEC 27001:20013	ISO/IEC 27001:2005	COBIT
11. การเข้ารหัสข้อมูล (Cryptography)	√	√	
องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัย ด้านสารสนเทศ			
12. ด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ	√	√	√
13. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	√	√	√
องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์			
14. นโยบายความมั่นคงปลอดภัยสารสนเทศ	√	√	√
15. การบริหารจัดการกลยุทธ์ความมั่นคงปลอดภัยสารสนเทศ			√

องค์ประกอบที่ 1 การกำกับดูแล การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ แบ่งออกเป็น 6 ตัวชี้วัด ดังนี้

ตัวชี้วัดที่ 1 การกำกับดูแล (Governance)

1.1 มั่นใจในการกำหนดกรอบการดำเนินงานการกำกับดูแล และการบำรุงรักษาหน่วยงานที่รับผิดชอบจัดทำระบบจะต้องกำหนดกรอบการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศที่มีความเชื่อมั่นตามขอบเขตที่ได้มีการกำหนดไว้ รวมทั้งการบำรุงรักษาระบบ เครื่องมือ และอุปกรณ์การเข้าใช้งานระบบสารสนเทศของหน่วยงาน ให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง ให้ครอบคลุมกับการทำงานของหน่วยงานตามความต้องการของผู้ใช้งานระบบอย่างแท้จริง

1.2 มั่นใจในการส่งมอบผลประโยชน์ หน่วยงานต้องให้ความเชื่อมั่นในการจัดทำระบบสารสนเทศ เพื่อช่วยให้การดำเนินงานมีความรวดเร็ว ทันเวลา และข้อมูลสารสนเทศความครบถ้วน ถูกต้อง และเป็นปัจจุบัน รวมถึงผู้รับบริการที่ใช้งานระบบจะได้ทราบถึงข้อดีของระบบ เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้

1.3 มั่นใจในความเสี่ยงที่เหมาะสม หน่วยงานจัดทำระบบสารสนเทศของ และมีการวิเคราะห์ความเสี่ยง รวมถึงแนวโน้มในการนำระบบสารสนเทศมาใช้ในหน่วยงานในอนาคต เพื่อกำหนดแนวทางและหลักการในการใช้งานระบบสารสนเทศ ให้มีความรอบคอบ ปลอดภัย และตามหลักการควบคุมภายในที่ดี ซึ่งหน่วยงานจะต้องรับรู้ปัญหาในการใช้งานระบบ และสามารถนำปัญหาไปปรับปรุงได้

1.4 มั่นใจต่อการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด หน่วยงานมีการตรวจสอบและประเมินผลการใช้ทรัพยากรของระบบสารสนเทศให้มีความคุ้มค่า เช่น ด้านบุคลากร ควรมีความรู้ความสามารถและทักษะที่ดี ด้านกระบวนการทำงานในระบบสารสนเทศให้มีความรอบคอบตามหลักการควบคุมภายในและความต้องการใช้งานของหน่วยงานภาครัฐ และด้านการใช้งานเทคโนโลยีสารสนเทศจัดทำให้ระบบสารสนเทศมีความคุ้มค่า และช่วยให้สามารถดำเนินงานได้ตามแผนที่กำหนดไว้

1.5 มั่นใจในความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย หน่วยงานตรวจสอบสมรรถนะด้านเทคโนโลยีสารสนเทศ ให้มีความสอดคล้องกับการใช้งานระบบสารสนเทศ และมีเป้าหมายในการดำเนินงานตามภารกิจหน่วยงาน ซึ่งสามารถตรวจสอบการทำงานทุกขั้นตอน และใช้งานระบบอย่างมีประสิทธิภาพ รวมถึงด้านความโปร่งใสของการดำเนินงาน

ตัวชี้วัดที่ 2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ โดยมีการควบคุมการดำเนินงาน ดังนี้

2.1 โครงสร้างภายในองค์กร การกำหนดโครงสร้างภายในองค์กรจะต้องมีการดำเนินการโดยเริ่มต้นและควบคุม การปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร ดังนี้

2.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบตามส่วนงานที่รับผิดชอบที่มีการเปลี่ยนแปลงทรัพย์สินขององค์กรหรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม ต้องมีการแยกหน้าที่ดังกล่าวออกจากกันเพื่อลดโอกาสการเกิดขึ้นนั้น

2.1.3 การติดต่อกับหน่วยงานผู้มีอำนาจซึ่งมีการรักษา เพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.1.4 การติดต่อกับกลุ่มที่มีความสนใจเดียวกันโดยเฉพาะ หรือกลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมอาชีพต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.1.5 การบริหารจัดการโครงการสอดคล้องกับความมั่นคงปลอดภัยสารสนเทศ โดยมีการระบุความมั่นคงปลอดภัยสารสนเทศในโครงการนั้น

2.2 อุปกรณ์คอมพิวเตอร์แบบพกพา และการทำงานระยะไกล การกำหนดนโยบายและการปฏิบัติงานที่เกี่ยวข้องกับการใช้งาน การใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาโดยมีการควบคุมการดำเนินงาน ได้แก่ 1) นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพาตามนโยบาย และมาตรการสนับสนุนเพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว และ 2) การทำงานระยะไกล เป็นนโยบายและมาตรการที่สนับสนุนการทำงานจากสถานที่หนึ่งไปอีกสถานที่หนึ่งในระยะไกล เพื่อป้องกันการเข้าถึงของข้อมูล การประมวลผล หรือการจัดเก็บข้อมูลจากสถานที่ดังกล่าว

ตัวชี้วัดที่ 3 การบริหารจัดการทรัพย์สิน จะเกี่ยวข้องกับการจัดการทรัพย์สินให้มีประสิทธิภาพ โดยมีการดำเนินการควบคุมดังนี้

3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน เพื่อให้มีการระบุทรัพย์สินขององค์กร และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สิน ได้แก่ (1) บัญชีทรัพย์สินที่เกี่ยวกับสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ โดยจะต้องมีการระบุทะเบียนทรัพย์สิน และปรับปรุงให้ทันสมัย (2) ผู้ถือครองทรัพย์สินต้องมีผู้ถือครองทรัพย์สิน (3) การใช้ทรัพย์สินอย่างเหมาะสม เป็นกฎเกณฑ์การใช้อย่างเหมาะสมสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้อง และจะต้องมีการระบุ จัดทำเป็นลายลักษณ์อักษร และ (4) การคืนสินทรัพย์โดยหน่วยงานภายนอกทั้งหมดต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง

3.2 การจัดชั้นความลับของสารสนเทศ มีวัตถุประสงค์เพื่อให้สารสนเทศได้รับระดับการป้องกัน โดยมีการควบคุมการดำเนินงาน ได้แก่ 1) ชั้นความลับของสารสนเทศตามข้อกฎหมาย ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยโดยไม่ได้รับอนุญาต 2) การบ่งชี้สารสนเทศ ขั้นตอนปฏิบัติสำหรับการบงชี้สารสนเทศต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่หน่วยงานกำหนด และ 3) การจัดการทรัพย์สิน ต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

3.3 การจัดการสื่อบันทึกข้อมูล เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาตให้เปลี่ยนแปลงขนย้าย การทำลายหรือการลบข้อมูลสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล ได้แก่ 1) การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ 2) การทำลายสื่อบันทึกข้อมูล และ 3) การขนย้ายสื่อบันทึกข้อมูล

ตัวชี้วัดที่ 4 การติดตาม วัดผล และการประเมินผล ซึ่งแบ่งออกเป็น 3 ประเด็นย่อย

4.1 เฝ้าติดตาม วัดผลและประเมินประสิทธิภาพ และความสอดคล้องในการดำเนินงาน หน่วยงานมีการจัดเก็บข้อมูล ตรวจสอบและประเมินผลการดำเนินงานของระบบสารสนเทศของหน่วยงาน รวมทั้งการตรวจสอบให้สามารถทำงานได้อย่างมีประสิทธิภาพ และใช้งานระบบตรงตามระเบียบที่หน่วยงานกำหนด

4.2 เฝ้าติดตาม วัดผลและประเมินระบบการควบคุมภายใน หน่วยงานตรวจสอบติดตาม และประเมินผลการควบคุมภายในระบบสารสนเทศ เพื่อระบุข้อบกพร่องในการใช้งานระบบ และปรับปรุงระบบกระบวนการดำเนินงานที่ให้มีประสิทธิภาพ และข้อมูลมีความครบถ้วน ถูกต้อง และเป็นปัจจุบัน

4.3 เฝ้าติดตาม วัดผลและประเมินการปฏิบัติตามข้อกำหนดของหน่วยงานภายนอก หน่วยงานมีการสนับสนุนการดำเนินงานของหน่วยงานภายนอก ด้านเทคโนโลยีสารสนเทศให้ดำเนินการตามข้อปฏิบัติการรักษาความปลอดภัย ตามกฎระเบียบ และแผนการดำเนินงานด้านความปลอดภัยที่หน่วยงานที่กำกับ ดูแลระบบความมั่นคงปลอดภัยของสารสนเทศจากภายนอกกำหนด โดยหน่วยงานที่เป็นเจ้าของระบบสารสนเทศควรให้ความสนใจและหมั่นคอยตรวจสอบระบบไม่ให้ถูกโจรกรรมข้อมูลสารสนเทศของหน่วยงาน

ตัวชี้วัดที่ 5 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ หน่วยงานมีการดำเนินงานให้สอดคล้องกันกับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ โดยมีการดำเนินการควบคุม ได้แก่ 1) หน้าที่ ความรับผิดชอบ และขั้นตอนปฏิบัติ เพื่อให้มีการตอบสนองอย่างรวดเร็ว และตามลำดับต่อเหตุการณ์ที่

เกิด 2) การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ 3) การรายงานจุดอ่อน 4) การประเมินและตัดสินใจต่อสถานการณ์ 5) การตอบสนองต่อเหตุการณ์ 6) การเรียนรู้จากเหตุการณ์ และ 7) การเก็บรวบรวมหลักฐาน

ตัวชี้วัดที่ 6 ความสอดคล้อง ที่เกี่ยวข้องกับกฎหมาย การป้องกันและการทบทวนขั้นตอนต่าง ๆ โดยมีการดำเนินการควบคุม ดังนี้

6.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง โดยมีการดำเนินการควบคุม ได้แก่ 1) การระบุกฎหมายและความต้องการในสัญญาจ้าง 2) สิทธิในทรัพย์สินทางปัญหา และการใช้ผลิตภัณฑ์ซอฟต์แวร์ 3) การป้องกันข้อมูล จากการสูญหาย ทำลาย และการปลอมแปลง 4) ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล และ 5) ระเบียบข้อบังคับสำหรับการเข้ารหัสข้อมูล

6.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ มีวัตถุประสงค์เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศสอดคล้องกับนโยบายและมีการดำเนินการควบคุม ได้แก่ 1) มีการทบทวนตามรอบระยะเวลาที่กำหนดไว้อย่างอิสระ 2) ความสอดคล้องกับนโยบายและมาตรฐาน โดยต้องทบทวนความสอดคล้องอย่างสม่ำเสมอ และ 3) การทบทวนความสอดคล้องทางเทคนิคกับนโยบายและมาตรฐานที่กำหนด

องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ แบ่งออกเป็น 5 ตัวชี้วัด ดังนี้

ตัวชี้วัดที่ 7 การควบคุมการเข้าถึง จะเกี่ยวข้องและสัมพันธ์กับการเข้าถึงสารสนเทศเพื่อนำไปใช้งาน โดยมีการควบคุมการดำเนินงาน ดังนี้

7.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง โดยจะดำเนินการควบคุม ได้แก่ 1) การกำหนด และจัดทำนโยบายควบคุมการเข้าถึงเป็นลายลักษณ์อักษร 2) การเข้าถึงเครือข่ายและบริการเครือข่ายต้องได้รับสิทธิการเข้าถึงเฉพาะที่ได้รับอนุมัติ

7.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน โดยมีการควบคุมการดำเนินงาน ได้แก่ 1) การลงทะเบียน และการถอดถอนสิทธิผู้ใช้งาน 2) การจัดการสิทธิการเข้าถึง 3) การบริหารจัดการสิทธิการเข้าถึง 4) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตน 5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และ 6) การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง

7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน โดยการใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ซึ่งผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูลการพิสูจน์ตัวตน ซึ่งเป็นข้อมูลลับ

7.4 การควบคุมการเข้าถึงระบบ โดยมีการควบคุมการดำเนินงาน ได้แก่ 1) การจำกัดการเข้าถึงสารสนเทศ 2) ขั้นตอนปฏิบัติสำหรับการล็อคอินเข้าระบบที่มีความมั่นคง 3) ระบบบริหารจัดการรหัสผ่าน 4) การใช้โปรแกรมอรรถประโยชน์ และ 5) การควบคุมการเข้าถึง Source Code ของโปรแกรม

ตัวชี้วัดที่ 8 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม การดำเนินงาน และการสื่อสารข้อมูล การป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ โดยมีการควบคุมการดำเนินงาน ดังนี้

8.1 พื้นที่ต้องการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตที่มีต่อสารสนเทศและอุปกรณ์ประมวลสารสนเทศ ได้แก่ 1) ขอบเขตหรือบริเวณโดยรอบทางกายภาพที่ต้องการรักษาความมั่นคงปลอดภัย 2) การควบคุมการเข้าโดยกำหนดให้เฉพาะผู้ที่ได้รับอนุญาต 3) การรักษาความปลอดภัยสำหรับห้องทำงาน สำนักงาน และอุปกรณ์ต่าง ๆ ต้องมีการให้ปลอดภัย 4) การป้องกันต่อภัยคุกคามจากภายนอก 5) การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย และ 6) พื้นที่สำหรับส่งสิ่งของ เป็นการกำหนดจุดและควรมีการแยกออกมาจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศ

8.2 อุปกรณ์ เพื่อป้องกันการสูญหาย การเสียหาย โดยมีการควบคุมการดำเนินงาน ได้แก่ 1) การจัดตั้งป้องกันอุปกรณ์ 2) อุปกรณ์สนับสนุนการทำงาน 3) การเดินสายสัญญาณและสายสื่อสารที่ปลอดภัย 4) การบำรุงรักษาอุปกรณ์ 5) การนำทรัพย์สินออกนอกสำนักงาน 6) ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอก 7) ความมั่นคงปลอดภัยสำหรับการกำจัดอุปกรณ์และไปใช้อย่างอื่น 8) อุปกรณ์ของผู้ใช้งานไม่มีเจ้าของ และ 9) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์

8.3 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ เพื่อให้การปฏิบัติงานกับอุปกรณ์สารสนเทศเป็นไปอย่างถูกต้องและมีความปลอดภัย โดยมีการดำเนินการควบคุม ได้แก่ 1) ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร 2) การบริหารจัดการกระบวนการทำงาน อุปกรณ์ประมวลผลสารสนเทศ และระบบที่มีการเปลี่ยนแปลง 3) การบริหารจัดการขีดความสามารถของระบบ และมีการติดตาม ปรับปรุง เพิ่มเติมในอนาคตให้มีประสิทธิภาพ และ 4) การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบและการให้บริการ โดยต้องออกจากกันเพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลง

8.4 การป้องกันโปรแกรมไม่ประสงค์ดี การป้องกันจากโปรแกรมที่เข้ามาไม่ดี โดยการตรวจหา การป้องกัน และการกู้คืนจากโปรแกรมไม่ประสงค์ดี และสร้างความตระหนักให้กับบุคลากร

8.5 การสำรองข้อมูล มีเพื่อป้องกันการสูญหายของข้อมูล โดยการสำรองข้อมูล จะเป็นข้อมูลสำรองสำหรับสารสนเทศ และซอฟต์แวร์ของระบบ

8.6 การบันทึกข้อมูล log การเฝ้าระวัง เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน ได้แก่ (1) การบันทึก log แสดงเหตุการณ์ (2) การป้องกันข้อมูล log (3) ข้อมูล log กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการโดยจะต้องมีการบันทึกอย่างสม่ำเสมอ และ (4) การตั้งเวลาของระบบให้ถูกต้อง ซึ่งเป็นการตั้งเวลาของระบบที่เกี่ยวข้องภายในหน่วยงาน ให้ตรงและเทียบกับแหล่งอ้างอิง

8.7 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ เพื่อให้ระบบมีการทำงานที่ถูกต้อง โดยการติดตั้งซอฟต์แวร์บนระบบ สำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องสอดคล้องกัน

8.8 การบริหารจัดการช่องโหว่ทางเทคนิค เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค ได้แก่ (1) การจัดการข้อมูลช่องโหว่ต้องมีการติดตามอย่างทันที เพื่อจัดการกับความเสี่ยง และ (2) การติดตั้งซอฟต์แวร์ โดยผู้ใช้งานต้องดำเนินงานตามข้อกำหนด

8.9 การพิจารณาการตรวจประเมินระบบ เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ โดยมีมาตรการตรวจสอบประเมินระบบและกิจกรรมการตรวจประเมินระบบให้บริการ และมีการวางแผน และทำข้อตกลงร่วมกันอย่างระมัดระวัง

8.10 การบริหารจัดการความมั่งคงปลอดภัยของเครือข่าย โดยมีการดำเนินการควบคุม ได้แก่ 1) การกำหนดมาตรการเครือข่ายเพื่อป้องกันสารสนเทศในระบบ 2) ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย ต้องมีการระบุ และรวบรวมไว้ในข้อตกลงการให้บริการเครือข่าย และ 3) การแบ่งแยกเครือข่ายเป็นการแบ่งกลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด

8.11 การถ่ายโอนสารสนเทศ เพื่อให้มีสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก โดยจะต้องมีการดำเนินการควบคุม ได้แก่ 1) มีนโยบาย และขั้นตอนสำหรับการถ่ายโอนสารสนเทศตามมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการ 2) ข้อตกลงสำหรับการถ่ายโอนสารสนเทศระหว่างองค์กรกับหน่วยงานภายอื่น ๆ 3) การส่งข้อความทางอิเล็กทรอนิกส์ การส่งข้อความทางอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม และ 4) ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยข้อมูลส่วนบุคคล และข้อมูลที่เป็นความลับ ต้องมีการระบุ ทบทวนอย่างสม่ำเสมอ และบันทึกไว้อย่างเป็นลายลักษณ์อักษร

ตัวชี้วัดที่ 9 การจัดหา การพัฒนา และการบำรุงรักษาระบบ โดยมีการดำเนินการควบคุม ดังนี้

9.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบหนึ่งของการพัฒนาระบบ ซึ่งรวมถึงการให้บริการผ่านระบบเครือข่าย โดยมีการดำเนินการควบคุม ได้แก่ 1) การวิเคราะห์และกำหนดความต้องการรวมเข้ากับความต้องการสำหรับระบบใหม่หรือการปรับปรุงระบบ 2) บริการสารสนเทศบนเครือข่ายสาธารณะต้องได้รับการป้องกัน การฉ้อโกง การโต้เถียง และการเปิดเผยที่ไม่ได้รับอนุญาต และ 3) การป้องกันธุรกรรมของบริการสารสนเทศ เป็นการกำหนดให้สารสนเทศที่เกี่ยวกับธุรกรรมการบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ ข้อมูลผิดพลาดผิดเส้นทาง การเปลี่ยนแปลงข้อความและเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

9.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน เพื่อดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ ได้แก่ 1) นโยบายการพัฒนาระบบให้มีความปลอดภัย 2) การควบคุมการเปลี่ยนแปลงระบบ 3) การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐาน 4) การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป 5) ยึดหลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย 6) สภาพแวดล้อมของการพัฒนาระบบ 7) การจ้างหน่วยงานภายนอกพัฒนาระบบ โดยการเฝ้าระวังและติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอก (8) การทดสอบด้านความมั่นคงปลอดภัยของระบบ และ (9) การทดสอบเพื่อรับรองระบบ เป็นแผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบเมื่อมีการดำเนินการระบบใหม่ หรือปรับปรุงเวอร์ชั่นใหม่

9.3 ข้อมูลสำหรับการทดสอบ เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ โดยการป้องกันข้อมูลสำหรับการทดสอบ และต้องมีการคัดเลือกอย่างระมัดระวัง มีการป้องกัน และควบคุมการนำมาใช้งาน

ตัวชี้วัดที่ 10 ความสัมพันธ์กับผู้ให้บริการภายนอก มีการดำเนินการควบคุม ดังนี้

10.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก โดยมีการดำเนินการควบคุม ได้แก่ 1) การกำหนดนโยบายกับผู้ให้บริการภายนอกและต้องมีข้อกำหนดเป็นลายลักษณ์อักษร 2) การระบุข้อตกลงการให้บริการภายนอก เช่น การเข้าถึง การจัดเก็บ การประมวลผล การสื่อสารและการให้บริการ เป็นต้น และ 3) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศโดยผู้ให้บริการภายนอกซึ่งกำหนดข้อตกลงร่วมกัน

10.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก มีการดำเนินการควบคุม ได้แก่ (1) การติดตาม และทบทวนบริการของผู้ให้บริการภายนอก และ (2) การบริหารจัดการของผู้ให้บริการภายนอก โดยการกำหนดระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องและต้องทบทวนการประเมินความเสี่ยงใหม่

ตัวชี้วัดที่ 11 การเข้ารหัสข้อมูล (Cryptography) มีรายละเอียดดังนี้

การเข้ารหัสข้อมูล (Cryptography) เพื่อให้มีการกำหนดนโยบายการเข้ารหัสข้อมูลอย่างเหมาะสม ป้องกันความลับ และการปลอมแปลง โดยมีการควบคุมการดำเนินงาน ได้แก่ 1) นโยบายการใช้มาตรการเข้ารหัสข้อมูล 2) การบริหารจัดการกุญแจ (Access Key) เป็นต้น

องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัย

ด้านสารสนเทศ แบ่งออกเป็น 2 ตัวชี้วัด ดังนี้

ตัวชี้วัดที่ 12 ด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ เพื่อให้เกิดการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการดำเนินการควบคุม ดังนี้

12.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ ได้มีการดำเนินการควบคุม ได้แก่ 1) การวางแผนความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น 2) การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องทางธุรกิจ และ 3) การตรวจสอบ การทบทวน และการประเมินความต่อเนื่อง

12.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง เพื่อจัดเตรียมสภาพความพร้อมการใช้ของอุปกรณ์ โดยอุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอสามารถใช้งานตลอด

ตัวที่วัดที่ 13 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร จะเกี่ยวข้องกับการจ้างงานบุคลากร โดยควบคุมตั้งแต่ก่อนการจ้างงาน ในระหว่างทำงาน และหลังจากเลิกจ้างงาน ดังนี้

13.1 ก่อนการจ้างงาน เพื่อให้พนักงานและผู้ที่จ้างเข้าใจในหน้าที่ความรับผิดชอบตามบทบาทของตนเอง โดยมีการควบคุมการดำเนินงาน ได้แก่ 1) การคัดเลือก จากการตรวจสอบภูมิหลังของผู้สมัครงานตามระเบียบ ข้อบังคับ กฎหมาย และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสม

กับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง และ 2) ข้อตกลงและเงื่อนไขการจ้างงานกับพนักงาน และผู้ที่ทำสัญญาจ้างต้องกล่าวถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของพนักงาน

13.2 ระหว่างการจ้างงาน ขั้นตอนที่เกี่ยวข้องระหว่างการจ้างงาน เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง โดยมีการควบคุมการดำเนินงาน ได้แก่ 1) หน้าที่ความรับผิดชอบของผู้บริหาร โดยผู้บริหารต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาจ้างทั้งหมด โดยปฏิบัติให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติที่กำหนดไว้ 2) การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมพนักงานขององค์กร และทบทวนเพิ่มเติมเรื่องขั้นตอนปฏิบัติขององค์กรที่เกี่ยวข้องกับงานที่ตนเองปฏิบัติ และ 3) กระบวนการทางวินัย มีการกำหนดอย่างเป็นทางการและมีการสื่อสารให้พนักงานได้รับทราบ เพื่อดำเนินการต่อพนักงานที่ละเมิดระเบียบขององค์กร

13.3 การสิ้นสุด หรือการเปลี่ยนการจ้างงาน ขั้นตอนที่เกี่ยวข้องกับการออกจ้างงานหรือสิ้นสุดงาน เพื่อป้องกันผลประโยชน์ขององค์กร โดยมีการดำเนินการควบคุมให้ปฏิบัติตามอย่างสอดคล้องกันนโยบายที่หน่วยงานกำหนด และสื่อสารให้ได้รับทราบ

องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ แบ่งออกเป็น 2 ตัวชี้วัด ดังนี้

ตัวชี้วัดที่ 14 นโยบายความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศ ได้แก่ 1) นโยบายสำหรับความมั่นคงปลอดภัยที่ต้องมีการจัดทำอนุมัติโดยผู้บริหาร และสื่อสารให้พนักงานและหน่วยงานภายนอกได้รับทราบ และ 2) การทบทวนนโยบายตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญด้วยความเหมาะสม เพียงพอ

ตัวชี้วัดที่ 15 การบริหารจัดการกลยุทธ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นการดำเนินงานของหน่วยงานที่กำหนดทิศทางในการสร้างและพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ โดยมีการประเมินสภาพแวดล้อม และความสามารถของบุคลากรในหน่วยงาน เกี่ยวกับการกำหนดกลยุทธ์การบริหารงาน โดยนำเทคโนโลยีตามที่ต้องการเพื่อขับเคลื่อนแผนการดำเนินงานสร้างระบบความมั่นคงปลอดภัยของสารสนเทศของหน่วยงาน ให้มีความสอดคล้องกับนโยบายของหน่วยงานในปัจจุบัน

ดังนั้น การสังเคราะห์องค์ประกอบจากการศึกษา และทบทวนมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศของมาตรฐาน ISO/IEC 27001:20013 ISO/IEC 27001:2005 และ COBIT 5 และเสนอให้กับผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศช่วยตรวจสอบความสอดคล้องและความเป็นไปได้ โดยแบ่งออกเป็นจำนวน 4 องค์ประกอบ รายละเอียดดังกล่าวข้างต้น เพื่อใช้สำหรับการวิเคราะห์หาองค์ประกอบที่สำคัญ และกำหนดแนวทางในการบริหารความมั่นคงปลอดภัยด้านสารสนเทศจากคณะแพทยศาสตร์ศิริราชพยาบาลที่มีวิธีการและแนวปฏิบัติของการบริหารจัดการด้านความมั่นคงปลอดภัยด้านสารสนเทศที่ดี และเพื่อค้นหา วิเคราะห์ และนำองค์ประกอบที่ได้มาปรับใช้กับการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศกับหน่วยงานอื่น ๆ ที่มีบริบท สอดคล้อง ตรงกับความต้องการของหน่วยงาน กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้องในบริบทของประเทศไทย

2.2 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล เป็นหน่วยงานที่ได้รับการรับรองมาตรฐาน ISO/IEC 27001/2013 (Information Security Management System : ISMS) เมื่อปี พ.ศ. 2560 และคณะแพทยศาสตร์ศิริราชพยาบาลเป็นองค์กรหนึ่งที่ขับเคลื่อนพันธกิจขององค์กรโดยใช้เทคโนโลยีสารสนเทศเป็นโครงสร้างพื้นฐานที่สำคัญ ไม่ว่าจะเป็นในด้านการบริการผู้ป่วย ด้านวิชาการ ด้านการศึกษา และด้านการวิจัยต่างก็ใช้เทคโนโลยีสารสนเทศทั้งสิ้น โดยกิจกรรมที่สำคัญของมาตรฐาน ISO/IEC 27001:2013 ที่หน่วยงานดำเนินการ คือ การจัดการความเสี่ยง และโอกาสเกิดขึ้นซึ่งมุ่งเน้นการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศควบคู่ไปกับการประเมินความเสี่ยงจากการปฏิบัติงานทั่วไป ซึ่งการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นการระบุความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของข้อมูล เช่น ความลับของข้อมูล ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูล เป็นต้น

ด้วยเหตุนี้ การประเมินความเสี่ยงและการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จึงเป็นหัวใจสำคัญขององค์กร โดยฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลที่ได้รับมอบหมายให้บริหารจัดการ และควบคุมดูแลในเรื่องของเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล จึงให้ความสำคัญในเรื่องดังกล่าว ตั้งแต่ปี พ.ศ. 2561 เป็นต้นมา และได้มีการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ลงวันที่ 7 เมษายน 2564 ตามระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ลงวันที่ 1 เมษายน 2564 ให้กับบุคลากรในองค์กรได้ยึดถือและปฏิบัติ และตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือ โดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล จึงได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ปฏิบัติได้ดำเนินการ สรุปได้ดังต่อไปนี้

1. การเข้าถึงและควบคุมการใช้งานสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ได้แก่ 1) ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึงและช่องทางการเข้าถึง 2) ต้องควบคุมให้มีการกำหนดสิทธิการใช้งานของผู้ใช้งานตามหน้าที่ความรับผิดชอบ รวมถึงการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการลักลอบทำสำเนาข้อมูลสารสนเทศ 3) ต้องดำเนินการฝึกอบรมการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ 4) ต้องควบคุมการเข้าถึงเครือข่าย ระบบปฏิบัติ และโปรแกรมประยุกต์หรือแอพพลิเคชั่นเพื่อป้องกันการเข้าบริการโดยไม่ได้รับอนุญาต

2. การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินของคณะแพทยศาสตร์ศิริราชพยาบาล โดยคัดเลือกระบบที่สำคัญ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินด้วยวิธีการทาง

อิเล็กทรอนิกส์ เพื่อให้ใช้งานได้อย่างต่อเนื่องปกติ และมีการปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบ รวมถึงระบบสำรอง และให้มีการทดสอบสภาพพร้อมใช้งานของระบบดังกล่าวอย่างสม่ำเสมอ

3. การตรวจสอบและประเมินความเสี่ยงของคณะแพทยศาสตร์ศิริราชพยาบาล ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor)

4. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ที่สอดคล้องกับนโยบายให้ผู้เกี่ยวข้องทั้งหมดทราบและปฏิบัติตามนโยบายและแนวปฏิบัติได้ รวมถึงกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย อันเนื่องจากความบกพร่อง ละเลย หรือ ฝ่าฝืนการปฏิบัติตามนโยบาย โดยได้มีการกำหนดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 11 ข้อ ได้แก่ 1) การบริหารจัดการ 2) การจัดโครงสร้างด้านในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศทั้งภายในและภายนอกหน่วยงาน 3) ด้านบุคลากร 4) การบริหารจัดการสินทรัพย์สารสนเทศ 5) ด้านกายภาพและสภาพแวดล้อม 6) การสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบสารสนเทศ 7) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ ระบบข้อมูลสารสนเทศ 8) การจัดหา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานข้อมูลสารสนเทศ 9) การบริหารจัดการสถานการณ์ที่ไม่พึงประสงค์ 10) การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง 11) การตรวจสอบและการประเมินผลปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ รวมทั้งข้อกำหนดอย่างสม่ำเสมอ

5. ให้มีการทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ และแนวปฏิบัติของคณะแพทยศาสตร์ศิริราชพยาบาล เพื่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง

ผู้วิจัยจึงได้นำแนวคิดการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชการพยาบาลที่มีวิธีการและแนวปฏิบัติที่ดี ตามการสังเคราะห์ และทบทวนมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศจากมาตรฐาน ISO/IEC 27001:20013 ISO/IEC 27001:2005 และ COBIT 5 และเสนอให้กับผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศช่วยตรวจสอบความสอดคล้องและความเป็นไปได้จำนวน 4 องค์ประกอบ และ 15 ตัวชี้วัด และผู้วิจัยจึงได้นำวิธีการทางสถิติมาช่วยในการสร้างองค์ประกอบจากตัวแปรหลาย ๆ ตัวแปร โดยรวมกลุ่มตัวแปรที่เกี่ยวข้องสัมพันธ์กันเป็นองค์ประกอบเดียวกัน ตัวแปรที่อยู่ในองค์ประกอบเดียวกันจะมีความสัมพันธ์กัน โดยองค์ประกอบหนึ่ง ๆ จะแทนตัวแปรแฝง อันเป็นคุณลักษณะที่ผู้วิจัยต้องการศึกษาเพื่อนำองค์ประกอบที่ได้มาปรับใช้กับการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศกับหน่วยงานอื่น ๆ ที่มีบริบท สอดคล้อง ตรงกับความต้องการของหน่วยงาน กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้องในบริบทของประเทศไทย

2.3 ทฤษฎีการวิเคราะห์องค์ประกอบ

2.3.1 ความหมายของการวิเคราะห์องค์ประกอบ

การวิเคราะห์องค์ประกอบมีความหมาย และวัตถุประสงค์เพื่อศึกษาคุณลักษณะภายในตัวบุคคลที่เป็นตัวแปรแฝง ซึ่งไม่สามารถสังเกตได้โดยตรง และต้องศึกษาคุณลักษณะดังกล่าวนั้น โดยการวัดหรือการสังเกตพฤติกรรมที่ต้องการศึกษา ในทางปฏิบัติผู้วิจัยจะเก็บรวบรวมข้อมูลได้เป็นตัวแปรสังเกตได้หลายตัว และใช้วิเคราะห์องค์ประกอบมาวิเคราะห์ข้อมูลเพื่อให้ได้องค์ประกอบอันเป็นคุณลักษณะของบุคคลที่ผู้วิจัยต้องการศึกษา โดยการวิเคราะห์ข้อมูลทางสถิติที่ช่วยสร้างองค์ประกอบจากตัวแปรหลาย ๆ ตัวแปร โดยรวมกลุ่มตัวแปรที่เกี่ยวข้องสัมพันธ์กันเป็นองค์ประกอบ ดังนั้น การวิเคราะห์องค์ประกอบเป็นเทคนิคทางสถิติที่ใช้ในการลดปริมาณข้อมูลให้ลดน้อยลง (Data Reduction) เพื่อให้ง่ายต่อความเข้าใจ และทำให้ทราบถึงโครงสร้างและแบบแผน (Structure and pattern of Data) (นงลักษณ์ วิรัชชัย, 2537; สุชาติ ประสิทธิ์รัฐสินธุ์ และ ลัดดาวัลย์ รอดมณี, 2527; สุภมาส อังศุโชติ และคณะ, 2551) ดังนั้น ตัวแปรที่มีความคล้ายคลึงกันจะถูกอธิบายด้วยองค์ประกอบ (Factor) เดียวกัน หลังการวิเคราะห์องค์ประกอบแล้ว ความแปรปรวนของตัวแปรเดิมจะถูกอธิบายด้วยองค์ประกอบที่มีจำนวนน้อยกว่าตัวแปรเดิม และเทคนิคการวิเคราะห์ปัจจัย (Factor Analysis) เป็นเทคนิคที่แบ่งกลุ่มตัวแปรออกเป็นกลุ่ม ๆ หรือรวมตัวแปรที่มีความสัมพันธ์กันไว้ในกลุ่มเดียวกัน และความสัมพันธ์อาจจะอยู่ในทิศทางเดียวกัน (ค่าสัมประสิทธิ์สหสัมพันธ์เป็นบวก) หรืออยู่ในทิศทางตรงกันข้าม (ค่าสัมประสิทธิ์สหสัมพันธ์เป็นลบ) แต่ตัวแปรที่อยู่ต่าง Factor กันจะไม่มีความสัมพันธ์กัน หรือมีความสัมพันธ์กันน้อย ในเทคนิคนี้จะใช้ค่าสัมประสิทธิ์สหสัมพันธ์ (Correlation) วัดความสัมพันธ์ระหว่างตัวแปร รวมถึง ตัวแปรที่ใช้เทคนิค Factor Analysis ได้ควรเป็นตัวแปรเชิงปริมาณ (Interval หรือ Ratio Scale) (กัลยา วานิชย์บัญชา, 2546; ดุษฎี โยเหลา, 2541)

2.3.2 วัตถุประสงค์สำคัญของการวิเคราะห์องค์ประกอบ

วัตถุประสงค์ของการวิเคราะห์องค์ประกอบมีหลักการ 2 ประการ ได้แก่ 1) เพื่อสำรวจและระบุองค์ประกอบร่วม และอธิบายความสัมพันธ์ระหว่างตัวแปร และผลการวิเคราะห์องค์ประกอบช่วยให้ลดจำนวนตัวแปรลง ซึ่งทำให้เข้าใจลักษณะของข้อมูลได้ง่าย และสะดวกในการแปลความหมายรวมทั้งได้ทราบแบบแผน (Patten) และโครงสร้าง (Structure) ความสัมพันธ์ของข้อมูลด้วย และ 2) เพื่อทดสอบสมมุติฐานเกี่ยวกับแผนและโครงสร้างความสัมพันธ์ของข้อมูล หรือจะเรียกอีกอย่างหนึ่งว่าการยืนยันในทฤษฎี จากข้อมูลเชิงประจักษ์มีความสอดคล้องกับสมมติฐานเพียงใด โดยผู้วิจัยต้องกำหนดสมมติฐานก่อนว่าคุณลักษณะที่ศึกษามีกี่องค์ประกอบ (กัลยา วานิชย์บัญชา, 2546; นงลักษณ์ วิรัชชัย, 2537)

2.3.3 ประโยชน์ของการวิเคราะห์องค์ประกอบ ซึ่งประโยชน์ของการวิเคราะห์องค์ประกอบตามเทคนิค Factor Analysis มีรายละเอียดดังนี้

2.3.3.1 สามารถที่จะลดจำนวนตัวแปร โดยการรวมตัวแปรหลาย ๆ ตัว และปัจจัยใหม่ที่สร้างขึ้นสามารถหาค่าของปัจจัยที่สร้างขึ้นได้ เรียกว่า Factor Score และนำปัจจัยดังกล่าวไปเป็นตัวแปรสำหรับการวิเคราะห์ทางสถิติต่อไป

2.3.3.2 ใช้ในการแก้ปัญหาการที่ตัวแปรอิสระของเทคนิคการวิเคราะห์ความถดถอยมีความสัมพันธ์กัน (Multicollinearity) วิธีการอย่างหนึ่งในการแก้ปัญหา Multicollinearity ซึ่งการรวมตัวแปรอิสระที่มีความสัมพันธ์กันไว้ด้วยกัน หรือเรียกว่าปัจจัยโดยใช้เทคนิค Factor Analysis แล้วนำปัจจัยดังกล่าวไปเป็นตัวแปรอิสระในการวิเคราะห์ความถดถอยต่อไป

2.3.3.3 ใช้เป็นเครื่องมือตรวจสอบโครงสร้างความสัมพันธ์ของตัวแปรที่ศึกษา เนื่องจากเทคนิค Factor Analysis จะหาค่าสัมประสิทธิ์สหสัมพันธ์ (Correlation) ของตัวแปรที่ละคู่แล้วรวมตัวแปรที่สัมพันธ์กันมากไว้ในปัจจัยเดียวกัน

2.3.3.4 สามารถอธิบายความหมายของแต่ละปัจจัยได้ตามความหมายของตัวแปรต่าง ๆ สามารถนำไปใช้ในด้านการวางแผนได้ ช่วยลดความซ้ำซ้อน อธิบายตัวแปรกลุ่มหรือชั้นของข้อมูลที่มีลักษณะร่วมกัน

2.3.3.5 ใช้ในการวัด (Scaling) เพื่อวัดลักษณะของบุคคลหรือของปรากฏการณ์ โดยการแบ่งลักษณะออกเป็นกลุ่ม ๆ แยกออกจากกันตัวประกอบแต่ละตัวคือ กลุ่มของลักษณะแต่ละกลุ่ม เมื่อได้ตัวประกอบแล้วก็ให้น้ำหนักในแต่ละลักษณะ เพื่อนำมารวมกันภายในตัวประกอบแต่ละตัว ซึ่งน้ำหนักเหล่านี้ได้มาจากความแปรเปลี่ยนตามลักษณะของแต่ละองค์ประกอบ และน้ำหนักที่รวมกันให้ก็จะได้สเกลหรือมาตราที่ต้องการ

2.3.3.6 การตรวจสอบสมมติฐาน ซึ่งเกี่ยวข้องกับมิติของทัศนคติ พฤติกรรม บุคลิกภาพของกลุ่มในสังคม ส่งผลให้การวิเคราะห์องค์ประกอบสามารถช่วยตอบคำถามว่ามิติเหล่านี้มีจริงหรือไม่สัมพันธ์กันอย่างไร และผลการตรวจสอบมีนัยสำคัญหรือไม่

2.3.3.7 การเปลี่ยนแปลงข้อมูล เป็นการวิเคราะห์ และเปลี่ยนข้อมูลให้อยู่ในรูปที่ต้องการ หรือองค์ประกอบที่สนใจตามข้อตกลงทางสถิติ เช่น การวิเคราะห์ความถดถอย มีข้อตกลงว่า ตัวทำนายจะต้องเป็นอิสระเชิงสถิติกัน ถ้ากรณีมีความสัมพันธ์กันการวิเคราะห์องค์ประกอบจะช่วยลดตัวทำนาย และเหลือเฉพาะตัวที่เป็นอิสระกัน

2.3.3.8 การสำรวจและตรวจค้น การวิเคราะห์องค์ประกอบจะช่วยการสำรวจตัวแปรที่ยังไม่เคยทราบ สามารถลดความซับซ้อนของปรากฏการณ์และจัดกระทำให้อยู่ในรูปเชิงเส้นตรง โดยวิธีการวิเคราะห์องค์ประกอบได้

2.3.3.9 เป็นแผนที่ การวิเคราะห์ตัวประกอบทำเสมือนแผนที่ให้ผู้วิจัยมองภาพปรากฏการณ์หรือการสร้างมโนทัศน์ และความแปรปรวนให้เป็นระบบมากขึ้น เพื่อเป็นข้อมูลสำหรับการวิจัยต่อ ๆ ไปได้

2.3.3.10 ทฤษฎี การวิเคราะห์องค์ประกอบเกิดจากทฤษฎีโครงสร้างทางคณิตศาสตร์ในสาขาพีชคณิตเชิงเส้นตรงที่นำมาช่วยลดเรื่องต่าง ๆ ลงได้ การวิเคราะห์ตัวประกอบสามารถนำมาประยุกต์ใช้ในด้านต่าง ๆ ของทฤษฎี การสร้างทฤษฎีได้หรือทดสอบสมมติฐาน (อุทุมพร ทองอุไทย, 2524; กัลยา วานิชย์บัญชา, 2546; สุภมาส อังศุโชติ และคณะ, 2551)

2.3.4 ข้อตกลงเบื้องต้นสำหรับการทดสอบ

ข้อตกลงเบื้องต้นที่สำคัญ คือ ตัวแปรต้องมีความสัมพันธ์กัน เนื่องจากวัตถุประสงค์หลักของการวิเคราะห์องค์ประกอบเพื่อรวมกลุ่มของตัวแปรที่สัมพันธ์กัน และเป็นการตรวจสอบข้อมูลเบื้องต้นสำหรับชุดข้อมูล

สามารถนำมาวิเคราะห์องค์ประกอบได้หรือไม่ โดยการพิจารณาเมทริกซ์สหสัมพันธ์ของตัวแปรชุดนั้น โดยต้องมีความสัมพันธ์กันไม่น้อยกว่า .30 นอกจากนี้ ยังมีนักวิชาการได้มีการกำหนดเกณฑ์เพิ่มเติม ทั้งนี้ สามารถตรวจสอบได้โดยการคำนวณค่าสหสัมพันธ์บางส่วน (Partial Correlation) คือ การหาความสัมพันธ์ของตัวแปรเมื่อควบคุมตัวแปรอื่นซึ่งควรจะมีค่าต่ำ คือ ค่า KMO and Bartlett's Test เมื่อเลือกสถิติทดสอบตัวนี้จะได้ค่าสถิติทดสอบ 2 ค่า ตัวแรก คือ ค่า Kaiser- Meyer -Olkin Measure of Sampling Adequacy (MSA) ดัชนีตัวนี้ มีค่าระหว่าง 0 ถึง 1 ค่าจะเท่ากับ 1 เมื่อตัวแปรแต่ละตัวสามารถทำนายได้ด้วยตัวแปรอื่น โดยปราศจากความคลาดเคลื่อน ส่วนค่าในช่วงอื่น ๆ แปลความหมายการวิเคราะห์องค์ประกอบโดยการวิเคราะห์ด้วยโปรแกรม SPSS ดังนี้ (สุภมาส อังศุโชติ และคณะ, 2551; Hair et al., 2006)

.80 ขึ้นไป	เหมาะสมระดับดีมาก
.70 - .79	เหมาะสมระดับดี
.60 - .69	เหมาะสมระดับปานกลาง
.50 - .59	เหมาะสมระดับน้อย
น้อยกว่า .50	ไม่เหมาะสมที่จะนำมาวิเคราะห์

สถิติตัวที่สอง คือ Bartlett's Test of Sphericity ใช้ทดสอบว่าตัวแปรต่าง ๆ มีความสัมพันธ์กันหรือไม่ โดยมีสมมติฐานของการทดลองดังนี้

H_0: Correlation matrix เป็น Identity matrix หรือตัวแปรต่าง ๆ ไม่สัมพันธ์กัน พิจารณาจากค่าเมทริกซ์ที่มีค่าในแนวทแยงเป็น 1 ค่านอกแนวทแยงเป็น 0

H_1: Correlation matrix ไม่เป็น Identity matrix หรือตัวแปรต่าง ๆ มีความสัมพันธ์กัน

ดังนั้น กรณีที่ค่า Bartlett's test of Sphericity มีนัยสำคัญทางสถิติ ตัวแปรต่าง ๆ เหล่านั้นมีความสัมพันธ์กัน จึงสามารถนำไปวิเคราะห์องค์ประกอบต่อไปได้

2.3.5 โมเดลการวิเคราะห์องค์ประกอบ

โมเดลการวิเคราะห์องค์ประกอบ (Factor Analysis Model) แบ่งออกเป็น 2 รูปแบบ ได้แก่ 1) การวิเคราะห์องค์ประกอบเชิงสำรวจ และ 2) การวิเคราะห์องค์ประกอบเชิงยืนยัน สำหรับการวิจัยในครั้งนี้ ผู้วิจัยได้ทำการวิจัยเพื่อศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยวิธีการวิเคราะห์องค์ประกอบที่ใช้จะเกี่ยวกับการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis : EFA) ดังนั้นในการนำเสนอเฉพาะ โมเดลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis : EFA) เท่านั้น รายละเอียดดังนี้

การวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis : EFA) คือ การวิเคราะห์ข้อมูลเพื่อสำรวจ กำหนดองค์ประกอบร่วมที่มีความสัมพันธ์และสามารถอธิบายตัวแปรสังเกตได้ โดยการสร้างเป็นตัวแปรใหม่ ลดจำนวนตัวแปรสังเกต และสร้างตัวแปรในองค์ประกอบร่วม โดยมีแนวคิดของการวิเคราะห์องค์ประกอบ ข้อตกลงเบื้องต้น ขั้นตอนการวิเคราะห์องค์ประกอบ ดังนี้ (สุภมาส อังศุโชติ และคณะ, 2551; นงลักษณ์ วิรัชชัย, 2537; ฉัตรศิริ ปิยิพิมลสิทธิ์. 2551)

1. แนวคิด

ผลความแปรปรวนในตัวแปรสังเกตได้มาจากองค์ประกอบร่วม (Common Factor: F) และองค์ประกอบเฉพาะ (Unique Factor: U) ซึ่งองค์ประกอบเฉพาะ (Unique Factor: U) ยังประกอบด้วยความแปรปรวน เนื่องจากลักษณะเฉพาะของตัวแปร (P) และความคลาดเคลื่อนในการวัด (e) (U = p+e) ค่าตัวแปรสังเกตได้มีความสัมพันธ์กัน เนื่องจากมีองค์ประกอบร่วมเป็นตัวเดียวกัน

ดังนั้น เมื่อพิจารณาค่าของตัวแปรสังเกตได้แต่ละตัว ในรูปแบบคะแนนมาตรฐาน (Standard Score) จะได้ตัวแบบสำหรับการวิเคราะห์องค์ประกอบในรูปสมการดังนี้

$Z = a_1F_1 + a_2F_2 + a_3F_3 + U = \sum aF + U$

เมื่อ z คือ ผลบวกเชิงเส้นขององค์ประกอบร่วม F_1, F_2, และ F_3 และ องค์ประกอบเฉพาะ (U) โดยที่

a_1, a_2, a_3 เป็นค่าน้ำหนักขององค์ประกอบของ หรือ Factor Loading ซึ่งเป็นความสัมพันธ์ระหว่างตัวแปรสังเกตได้กับองค์ประกอบกำลังสองของน้ำหนักองค์ประกอบ ซึ่งสามารถอธิบายเป็นค่าร้อยละความแปรปรวนที่ตัวแปรนั้นอธิบายองค์ประกอบหนึ่งได้

ทั้งนี้ ผลบวกของกำลังสองของน้ำหนักองค์ประกอบของตัวแปรสังเกตได้ตัวหนึ่ง ได้แก่ ค่า Communality – h^2 หรือความร่วมกัน หรือค่าผลบวกของความแปรปรวนที่ตัวแปรสังเกตแบ่งปันให้กับองค์ประกอบอื่น ๆ หรือค่าความแปรปรวนของตัวแปรนั้น สามารถอธิบายได้ด้วยองค์ประกอบร่วมนั่นเอง

สำหรับค่าไอแกน (Eigen values) หรือผลร่วมของกำลังสองของน้ำหนักองค์ประกอบหนึ่งของตัวแปรสังเกตได้ทุกตัว ซึ่งเป็นค่าความแปรปรวนขององค์ประกอบที่สามารถอธิบายได้ด้วยตัวแปรสังเกตได้ทุกตัว

2. ข้อตกลงเบื้องต้น

การดำเนินการเพื่อพิจารณา ตรวจสอบก่อนการวิเคราะห์ข้อมูล คือ 1) องค์ประกอบร่วมทุกตัวเป็นต้องเป็นอิสระต่อกัน หรือมีความสัมพันธ์กัน 2) ตัวแปรสังเกตได้ทุกตัวได้รับอิทธิพลทางตรงจากทุกองค์ประกอบ (F) 3) ตัวแปรสังเกตได้ทุกตัวได้รับอิทธิพลจากองค์ประกอบเฉพาะ หรือความคลาดเคลื่อนเพียงตัวเดียว (e) และ 4) ความคลาดเคลื่อนทุกตัวเป็นอิสระต่อกันและเป็นอิสระจากองค์ประกอบทุกตัว

3. ขั้นตอนการวิเคราะห์ ได้มีการกำหนด ไว้ดังนี้

3.1 การสกัดองค์ประกอบขั้นต้น (Factor Extraction) มี 2 วิธีดังนี้

วิธีที่ 1 วิธี Component Analysis ซึ่งเรียกกันทั่วไปว่า Principal Component Analysis เหมาะสำหรับการวิเคราะห์ที่ต้องการองค์ประกอบจำนวนน้อย ๆ ที่จะอธิบายความแปรปรวนของตัวแปรสังเกตได้มากที่สุด และค่าความแปรปรวนเฉพาะ (u = p + e) มีค่าน้อย เปรียบเทียบกับความแปรปรวนทั้งหมด ในขั้นแรกระบุให้ค่าความแปรปรวนร่วมกัน เท่ากับ 1

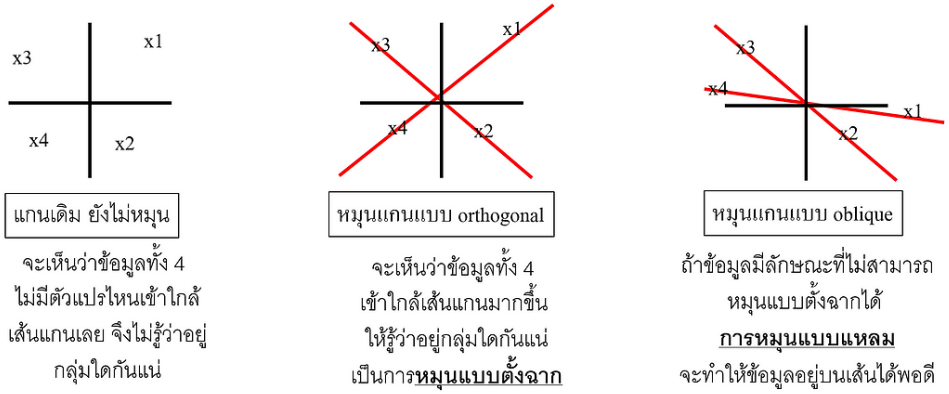
วิธีที่ 2 วิธี Common Factor เพื่อวิเคราะห์และระบุมิติแฝง (Latent Dimension) หรือโครงสร้างที่เป็นตัวแทนของชุดข้อมูลตัวแปรสังเกตได้ กรณีที่มีความรู้ เกี่ยวกับแปรปรวนเฉพาะน้อยมาก หรือไม่มีทฤษฎี และประสงค์ต้องการขจัดความแปรปรวนออกไป แต่วิธีนี้มีความยุ่งยากมากกว่า Component Analysis จึงได้รับความนิยมน้อยกว่า

ดังนั้น เกณฑ์การกำหนดจำนวนองค์ประกอบ พิจารณาได้จาก ค่าไอเกน (Eigen values) มากกว่า 1 จากการกำหนดจำนวนตัวองค์ประกอบล่วงหน้า มีค่าร้อยละของความแปรปรวนสะสม 60% ขึ้นไป และพิจารณาจากเส้นกราฟ Scree Plot จากเส้นตรงที่เริ่มขนานกับแกนนอน ถือว่าเป็นจำนวนองค์ประกอบสูงสุด

3.2 การหมุนแกนองค์ประกอบ (Factor Rotation) เพื่อให้ได้องค์ประกอบร่วมดำเนินการได้ 2 วิธี ดังนี้

วิธีที่ 1 Orthogonal เป็นการหมุนแกนที่ให้แกนองค์ประกอบตั้งฉาก โดยที่องค์ประกอบที่ได้เป็นอิสระต่อกัน ซึ่งวิธี Varimax เป็นวิธีที่นิยมใช้กัน

วิธีที่ 2 Oblique เป็นการหมุนแกนที่องค์ประกอบไม่ต้องตั้งฉากกัน องค์ประกอบที่สกัดได้จะมีความสัมพันธ์กัน ดังแสดงในภาพที่ 2.12



ภาพที่ 2.12 การหมุนแกนแบบมุมฉาก Orthogonal และการหมุนแกนแบบมุมแหลม Oblique

ที่มา: ประยุกต์จากสุภมาส อังศุโชติ และคณะ (2551)

3.3 การสร้างคะแนนองค์ประกอบ (Factor Score) เพื่อสร้างตัวแปรแฝงจากตัวแปรสังเกตได้

3.4 การตั้งชื่อองค์ประกอบ สื่อ และแสดงความหมายถึงตัวแปรทั้งหมดในองค์ประกอบ โดยวิธีการแต่ละขั้นตอนมีรายละเอียดดังนี้

ขั้นตอนที่ 1 การเตรียมเมทริกซ์สหสัมพันธ์ เมทริกซ์สหสัมพันธ์ที่จะใช้เป็นข้อมูลในการวิเคราะห์องค์ประกอบเชิงสำรวจ มี 2 แบบ ได้แก่ 1) เมทริกซ์สหสัมพันธ์แบบอาร์ (R- type) เมทริกซ์ของสหสัมพันธ์ระหว่างตัวแปรแต่ละคู่ และคะแนนที่นำมาหาค่าสหสัมพันธ์แต่ละคู่ที่เป็นจำนวนหน่วยตัวอย่าง และ 2) เมทริกซ์ของสหสัมพันธ์แบบคิว (Q- type) เมทริกซ์ของสัมประสิทธิ์สหสัมพันธ์ระหว่างหน่วยตัวอย่างแต่ละคู่ และคะแนนที่นำมาหาค่าสหสัมพันธ์แต่ละคู่เป็นจำนวนตัวแปรหรือคุณลักษณะของหน่วยตัวอย่างละคน ทั้งนี้ การวิเคราะห์องค์ประกอบที่นิยมใช้ข้อมูลจะเป็นแบบเมทริกซ์สหสัมพันธ์อาร์ เพื่อศึกษาตัวแปรที่แสดงออกเป็นตัวแปรสังเกตได้ แต่ก็ควรใช้เมทริกซ์สหสัมพันธ์แบบคิวด้วย

เมทริกซ์สหสัมพันธ์ที่เตรียมไว้เพื่อวิเคราะห์องค์ประกอบนั้น ควรมีค่าสหสัมพันธ์แตกต่างจากศูนย์ จึงจัดให้มีการทดสอบสมมติฐานว่าเมทริกซ์สหสัมพันธ์นั้นไปวิเคราะห์เป็นเมทริกซ์เอกลักษณ์ (Identity Matrix) หรือไม่โดยใช้ Bartlett's Test of Sphericity ซึ่งเป็นการทดสอบไค- สแควร์ของ Determinant นอกจากนี้ ยังมีการทดสอบโดยการคำนวณค่าสถิติเรียกว่า Kaiser-Meyer-Olkin Measure of Sampling Adequacy ซึ่งเป็นดัชนีบอกความแตกต่างระหว่างแมทริกซ์สหสัมพันธ์ของตัวแปรสังเกตได้กับเมทริกซ์สหสัมพันธ์ Anti – Image Correlation Matrix ซึ่งเป็นเมทริกซ์ของสหสัมพันธ์ระหว่างตัวแปรแต่ละคู่สำหรับขจัดความแปรปรวนของตัวแปรอื่น ๆ ออกไป ทั้งนี้ ควรจะมีค่าเข้าใกล้หนึ่ง ดังนั้น ถ้าค่าความสัมพันธ์ระหว่างตัวแปรน้อย จึงไม่เหมาะสมที่จะวิเคราะห์องค์ประกอบ

ขั้นตอนที่ 2 การสกัดองค์ประกอบขั้นต้น (Extraction of the Initial Factor) การสกัดองค์ประกอบเชิงสำรวจ เป็นการสกัดให้มีจำนวนองค์ประกอบร่วมน้อยที่สุด และสามารถนำค่าน้ำหนักองค์ประกอบไปคำนวณค่าเมทริกซ์สหสัมพันธ์ได้ค่าใกล้เคียงกับเมทริกซ์สหสัมพันธ์ของตัวแปรสังเกตของข้อมูลเชิงประจักษ์ที่รวบรวมมาวิเคราะห์ โดยกระบวนการสกัดจะมีการคำนวณวนซ้ำหลายรอบ พิจารณาเริ่มต้นจากสมมติฐานว่ามีองค์ประกอบเพียงองค์ประกอบเดียว หลังจากนั้นนำค่า Factor ไปคำนวณหาเมทริกซ์สหสัมพันธ์เปรียบเทียบกับข้อมูลเชิงประจักษ์ ทั้งนี้ หากมีความแตกต่างกัน จะพิจารณาตั้งสมมติฐานว่ามีสององค์ประกอบแล้วดำเนินการวิเคราะห์ใหม่อีกครั้ง จนกว่าจะได้เมทริกซ์สหสัมพันธ์ที่คำนวณได้นั้นมีค่าใกล้เคียงกับข้อมูลเชิงประจักษ์

วิธีการสกัดองค์ประกอบสามารถแยกได้เป็น 6 กลุ่ม คือ 1) การวิเคราะห์ส่วนประกอบมุขสำคัญ 2) การหาองค์ประกอบแกนมุขสำคัญ 3) วิธีกำลังสองน้อยที่สุด 4) วิธีไลด์ลิฮู้คสูงสุด 5) วิเคราะห์ภาพ และ 6) การหาองค์ประกอบแบบแอลฟา แต่ละกลุ่มมีหลักการคล้ายคลึงกัน แต่มีวิธีการแตกต่างกัน โดยวิธีการที่ 2 – 6 จะมีความแตกต่างจากวิธีที่ 1 เนื่องจากเป็นวิธีการวิเคราะห์องค์ประกอบร่วม (Common Factor Analysis) ทั้งนี้ถึงแม้ว่าวิธีการวิเคราะห์ส่วนประกอบมุขสำคัญ จะแตกต่างจากการวิเคราะห์องค์ประกอบร่วมวิธีอื่น ๆ แต่มีหลักการแบบเดียวกัน ดังนั้น สำหรับการวิจัยครั้งนี้ ผู้วิจัยเลือกใช้วิธี Principal Component Analysis โดยโปรแกรม SPSS ซึ่งผลลัพธ์ของการวิเคราะห์องค์ประกอบ คือ "eigen value > 1" และเพื่อสร้างตัวแปรชุดใหม่ให้มีจำนวนน้อย ไม่จำเป็นต้องมีทฤษฎีพื้นฐาน แต่การวิเคราะห์องค์ประกอบร่วม จำเป็นต้องมีทฤษฎี มีสมมติฐานเป็นแนวทางในการวิเคราะห์ ซึ่งมีรายละเอียด ดังนี้

วิธีการวิเคราะห์ส่วนประกอบมุขสำคัญ (Principal Component Analysis) ตามหลักการวิเคราะห์ส่วนประกอบมุขสำคัญ ตัวแปรสังเกตได้จะถูกเปลี่ยนรูปผลบวกเชิงเส้นของตัวแปรสังเกตได้ทั้งหมด โดยที่ตัวแปรในองค์ประกอบตัวแรกอธิบายความแปรปรวนของตัวแปรสังเกตได้มากที่สุด และดำเนินการสร้างตัวแปรในองค์ประกอบตัวถัดไปที่ไม่สัมพันธ์กับตัวแรก และอธิบายความแปรปรวนของตัวแปรสังเกตได้ที่เหลืออยู่ให้มากที่สุดเรื่อย ๆ ไป และผลจากการวิเคราะห์จะได้ตัวแปรในองค์ประกอบชุดหนึ่งที่ไม่สัมพันธ์กันเลยจากข้อมูลตัวแปรสังเกตได้ซึ่งมีความสัมพันธ์กัน ดังนั้นถ้าตัวแปรไม่มีความสัมพันธ์กันการวิเคราะห์ส่วนประกอบมุขสำคัญจะทำไม่ได้ ทั้งนี้ วิธีการวิเคราะห์ส่วนประกอบมุขสำคัญ จะแตกต่างจากวิธีการวิเคราะห์องค์ประกอบร่วมวิธีอื่น ๆ ข้างต้น ซึ่งการวิเคราะห์ส่วนประกอบมุขสำคัญตัวแปรสังเกตได้ คือ ผลบวกเชิงเส้นของส่วนประกอบมุขสำคัญ (องค์ประกอบ)

นั่นคือ ตัวแปรส่วนประกอบอธิบายความแปรปรวนในตัวแปรสังเกตได้ทั้งหมด แต่โมเดลการวิเคราะห์องค์ประกอบร่วม คือ ผลบวกเชิงเส้นขององค์ประกอบร่วมหลายองค์ประกอบ และองค์ประกอบเฉพาะ นั้นคือ องค์ประกอบร่วมอธิบายความแปรปรวนในตัวแปรสังเกตได้เฉพาะส่วนที่มีความแปรผันร่วมกันกับองค์ประกอบ

ขั้นตอนที่ 3 วิธีการหมุนแกน (Method of Rotation) เพื่อให้ได้องค์ประกอบที่มีโครงสร้างง่าย (Simple Structure) ไม่ซับซ้อน จัดกลุ่มตัวแปรได้องค์ประกอบมีโครงสร้างง่ายดังกล่าวทำได้ 3 วิธี ได้แก่ 1) การหมุนแกนโดยใช้กราฟ 2) การหมุนแกนโดยใช้วิธีการวิเคราะห์ให้ได้ผลตามเกณฑ์ที่กำหนด และ 3) วิธีการหมุนแกนให้เมทริกซ์องค์ประกอบมีลักษณะตามเมทริกซ์เป้าหมายที่กำหนด โดยผู้วิจัยได้เลือกใช้วิธีการหมุนแกนโดยใช้การวิเคราะห์ (Analytical Rotation) รายละเอียดดังนี้

การหมุนแกนโดยใช้การวิเคราะห์ (Analytical Rotation) การนำหลักการของ Thurstone มาสร้างเกณฑ์เพื่อปรับค่าสัมประสิทธิ์ในเมทริกซ์องค์ประกอบ โดยมีหลักการข้อหนึ่งของ Thurstone องค์ประกอบจะมีโครงสร้างง่ายเมื่อพิกัดของตัวแปรอยู่บนแกนอ้างอิงแกนเดียว นั่นคือ สมาชิกในแต่ละแถวของเมทริกซ์องค์ประกอบควรจะมีค่าสูงเฉพาะองค์ประกอบใดองค์ประกอบหนึ่งเท่านั้น และควรมีค่าต่ำสำหรับทุกองค์ประกอบที่เหลือ ถ้ากำลังสองของน้ำหนักองค์ประกอบเฉพาะองค์ประกอบหนึ่งมีค่าเท่ากับค่าการร่วมของตัวแปรนั้น หมายความว่าตัวแปรนั้นวัดองค์ประกอบเดียว ซึ่งจะตีความหมายของตัวแปรนั้นได้ง่าย และอีกหลักการข้อที่สอง คือ การหมุนแกนเชิงวิเคราะห์โดยให้กำลังสองของน้ำหนักองค์ประกอบแต่ละสดมภ์ (Column) ของแมทริกซ์องค์ประกอบที่มีค่าสูงสุด ทำให้ได้องค์ประกอบเฉพาะ (Specific Factor) ซึ่งตีความหมายองค์ประกอบแต่ละองค์ประกอบแต่ได้ง่ายตามแบบของ Thurstone จากหลักเกณฑ์สองประการนี้นำไปสู่การหมุนแกนเชิงวิเคราะห์แบบต่าง ๆ ซึ่งจัดแยกได้เป็น 2 กลุ่ม ได้แก่ 1) การหมุนแกนแบบตั้งฉาก (Orthogonal Rotation) แบบตั้งฉากและ 2) การหมุนแกนแบบมุมแหลม (Oblique Rotation) ซึ่งจากการวิจัยครั้งนี้ ผู้วิจัยเลือกใช้วิธีการ การหมุนแกนโดยใช้วิธีการวิเคราะห์ให้ได้ผลตามเกณฑ์ที่กำหนด ในรูปแบบการหมุนแกนแบบตั้งฉาก (Orthogonal Rotation) โดยการหมุนแกนแบบแวร์ริแมกซ์ (Varimax Rotation) มีรายละเอียดดังต่อไปนี้ ดังนี้

การหมุนแกนแบบตั้งฉาก (Orthogonal Rotation) แบ่งออกเป็นวิธีย่อยตามเกณฑ์ที่ใช้

1. การหมุนแกนแบบควอร์ติแมกซ์ (Quarimax Rotation) เป็นวิธีการการหมุนแกนโดยให้กำลังสองของน้ำหนักองค์ประกอบแต่ละแถวในเมทริกซ์องค์ประกอบมีค่าสูงสุด แต่ในสูตรการคำนวฯต้องใช้ค่าน้ำหนักองค์ประกอบยกกำลังสี่ ผู้พัฒนาสูตรนี้จึงตั้งชื่อนี้ว่า วิธีควอร์ติแมกซ์ คือ การทำค่าผลรวมของกำลังสี่ของน้ำหนักองค์ประกอบในแต่ละแถวให้มีค่าสูงสุด ผลจากวิธีนี้จะได้องค์ประกอบที่มีน้ำหนักองค์ประกอบมีค่าสูงบางตัวแปรและมีน้ำหนักองค์ประกอบปานกลางและค่าบนตัวแปรที่เหลือ เป็นผลให้ได้องค์ประกอบทั่วไป

2. การหมุนแกนแบบแวร์ริแมกซ์ (Varimax Rotation) เป็นวิธีการหมุนแกนโดยให้กำลังสองของน้ำหนักองค์ประกอบแต่ละสดมภ์ (Column) ในเมทริกซ์องค์ประกอบจะมีค่าสูงสุด วิธีนี้ได้องค์ประกอบที่มีโครงสร้างง่ายตามแบบของ Thurstone และได้องค์ประกอบเฉพาะ (Specific Factor) ซึ่งทำให้การแปลความหมายองค์ประกอบสะดวกขึ้น ซึ่งเป็นวิธีที่ผู้วิจัยใช้ในการศึกษาครั้งนี้

3. การหมุนแกนแบบอีควอแมกซ์ (Equamax Rotation) เป็นวิธีที่ผสมผสานวิธีคอวร์ติแมกซ์และวิธีแวร์ริแมกซ์ องค์ประกอบที่ได้จะมีลักษณะกลาง ๆ ระหว่างสองวิธีนี้ นอกจากที่กล่าวมาแล้ว 3 วิธี ยังมีวิธีทรานส์วาร์ริแมกซ์ (Thansvarimax) เพิ่มเติมอีก

ขั้นตอนที่ 4 การสร้างตัวแปรหรือองค์ประกอบ การวิเคราะห์องค์ประกอบหลังจากมีการหมุนแกน ผู้วิจัยจะต้องมีการสร้างตัวประกอบ (Composition Variable) หรือสเกลองค์ประกอบ (Factor Scale) ในที่นี้ผู้วิจัยต้องพิจารณาก่อนว่าจะสร้างหรือใช้องค์ประกอบ จำนวนมากน้อยเท่าไร วิธีการตัดสินใจเกี่ยวกับจำนวนองค์ประกอบรวม 5 วิธี ได้แก่ 1) การทดสอบนัยสำคัญ (Significance Test) เมื่อมีการวิเคราะห์องค์ประกอบโดยใช้วิธีสกัดองค์ประกอบแบบไลค์ลิฮูดสูงสุด โดยต้องมีการทดสอบความกลมกลืนสอดคล้องระหว่างเมทริกซ์สหสัมพันธ์ที่คำนวณได้จากองค์ประกอบกับเมทริกซ์ที่เป็นข้อมูลเชิงประจักษ์ ถ้าผลการทดสอบสอบมีความกลมกลืน (ค่าไค-สแควร์ต่ำมากและไม่ปฏิเสธสมมติฐานหลัก) ให้ใช้จำนวนองค์ประกอบที่ได้นั้น 2) การกำหนดค่าไอเกน (Eigenvalue Specification) โดยทั่วไปนิยมกำหนดค่าไอเกนที่เกินหนึ่งเป็นเกณฑ์ในการเลือกองค์ประกอบไปใช้ วิธีการนี้ใช้กรณีที่ใส่เมทริกซ์สหสัมพันธ์เข้าไปวิเคราะห์องค์ประกอบโดยยังไม่มีการปรับค่าสมาชิกของเมทริกซ์ในแนวทแยงและการณีที่มีการปรับแก้ด้วยค่าประมาณค่าการร่วม 3) ความสำคัญเชิงทฤษฎี (Substantive Importance) วิธีนี้ผู้วิจัยต้องมีทฤษฎีพื้นฐานในการวิเคราะห์องค์ประกอบ และทราบความสำคัญของแต่ละองค์ประกอบนำมากำหนดเป็นเกณฑ์ในการเลือกองค์ประกอบ 4) การทดสอบสกรี (Scree – Test) เมื่อนำค่าไอเกนและหมายเลขอันดับขององค์ประกอบมาลงกราฟจะได้กราฟสกรี แสดงความแตกต่างของค่าไอเกน เส้นกราฟจะมีความชัน และค่อย ๆ ลาดลงในตอนองค์ประกอบอันดับหลัง วิธีการตัดสินใจเลือกองค์ประกอบให้เลือกองค์ประกอบอันดับต้น ๆ ที่เส้นกราฟมีความชัน และ 5) เกณฑ์การไม่แปรค่า (Invariance Criteria) วิธีนี้เป็นวิธีผสมผสานจากเกณฑ์ที่ใช้ทุกวิธีข้างต้นประกอบกับเหตุผลของผู้วิจัย โดยเลือกองค์ประกอบที่เกณฑ์ทุกข้อให้ผลสอดคล้องกันและมีเหตุผลเพียงพอต่อที่นักวิจัยต้องการ ทั้งนี้ เนื่องจากวิธีการวิเคราะห์ส่วนประกอบมุขสำคัญ แตกต่างจากวิธีการวิเคราะห์องค์ประกอบแบบอื่น ๆ ได้แก่ 1) ค่าการร่วมแต่ละตัวแปรมีค่าเป็นหนึ่งหรือตัวแปรสังเกตในรูปผลบวกเชิงเส้นของตัวแปร แต่ในการวิเคราะห์องค์ประกอบค่าการร่วมของตัวแปรมีค่าน้อยกว่าหนึ่ง ตัวแปรสังเกตได้เป็นผลบวกเชิงเส้นของตัวแปรองค์ประกอบร่วม องค์ประกอบเฉพาะและค่าความคาดเคลื่อน ดังนั้นการสร้างตัวแปรองค์ประกอบและการสร้างสเกลองค์ประกอบจึงใช้วิธีการแตกต่างรายละเอียด ดังนี้

4.1 การสร้างตัวประกอบ (Component Variables)

ตัวแปรในองค์ประกอบเป็นผลบวกเชิงเส้นของตัวแปรสังเกตได้ และในการสกัดองค์ประกอบโดยวิธีการวิเคราะห์ส่วนประกอบมุขสำคัญนั่น ไม่มีทฤษฎีเป็นพื้นฐานของการรวมกลุ่มตัวแปรเข้าเป็นตัวแปรประกอบ ดังนั้นการสร้างตัวประกอบจึงสร้างจากผลบวกเชิงเส้นของตัวแปรสังเกตได้ ดังสมการในการสร้างตัวแปรประกอบ F ตัวใดตัวหนึ่งดังนี้

$$F = (w1)(Z1) + (w2)(Z2) + \ldots + (wn)(Zn)$$

โดย n คือ จำนวนตัวแปรสังเกตได้ และ w1, w2, ... Wn คือ สัมประสิทธิ์คะแนนตัวแปรประกอบ (Component Score Coefficients) แต่สำหรับโปรแกรม SPSS จะให้สัมประสิทธิ์คะแนน เมทริกซ์สัมประสิทธิ์คะแนนองค์ประกอบ (Factor Score Coefficient Matrix)

4.2 การสร้างสเกลองค์ประกอบ (Factor Scales)

เนื่องจากองค์ประกอบร่วมมีส่วนที่กำหนดไม่ได้ และในการวิจัยมีความคลาดเคลื่อนจากการสุ่มตัวอย่าง และสเกลองค์ประกอบที่สร้างขึ้น ดังนั้นการสร้างองค์ประกอบต้องมีเกณฑ์การสร้างให้สเกลองค์ประกอบใกล้เคียงกับองค์ประกอบร่วมที่ควรจะเป็นมากที่สุด วิธีการสร้างและเกณฑ์ที่ใช้แต่ละวิธี ได้แก่ 1) วิธีการสร้างสเกลองค์ประกอบตามหลักการถดถอย วิธีนี้เป็นการสร้างสเกลองค์ประกอบ โดยให้ความสัมพันธ์ระหว่างสเกลองค์ประกอบที่สร้างขึ้นกับองค์ประกอบร่วมตามทฤษฎีมีค่าสูงสุด หรือให้ค่าผลรวมกำลังสองของความแตกต่างระหว่างสเกล 2) วิธีการสร้างสเกลองค์ประกอบตามหลักกำลังสองน้อยที่สุด วิธีนี้เป็นการสร้างสเกลองค์ประกอบโดยให้ผลรวมของกำลังสองของผลต่างระหว่างตัวแปรสังเกตได้และส่วนที่เป็นองค์ประกอบร่วมคำนวณจากสเกลองค์ประกอบที่มีค่าน้อยที่สุด 3) วิธีสร้างสเกลองค์ประกอบตามหลักเกณฑ์ของ Bartlett วิธีนี้ได้นำความคลาดเคลื่อนจากการสุ่มตัวอย่างมาพิจารณาด้วย ในการสร้างสเกลองค์ประกอบ ตัวแปรที่มีความคลาดเคลื่อนมากจะถูกถ่วงน้ำหนักด้วยค่าน้อยกว่าน้ำหนักของตัวแปรที่มีความคลาดเคลื่อนน้อย และ 4) วิธีสร้างสเกลองค์ประกอบตามวิธีของ Anderson และ Rubin ผลจากการสร้างองค์ประกอบทั้งสามวิธีที่กล่าวมาส่วนใหญ่จะได้สเกลองค์ประกอบที่สัมพันธ์กัน แม้ว่าจะมีการหมุนแกนแบบมุมฉาก

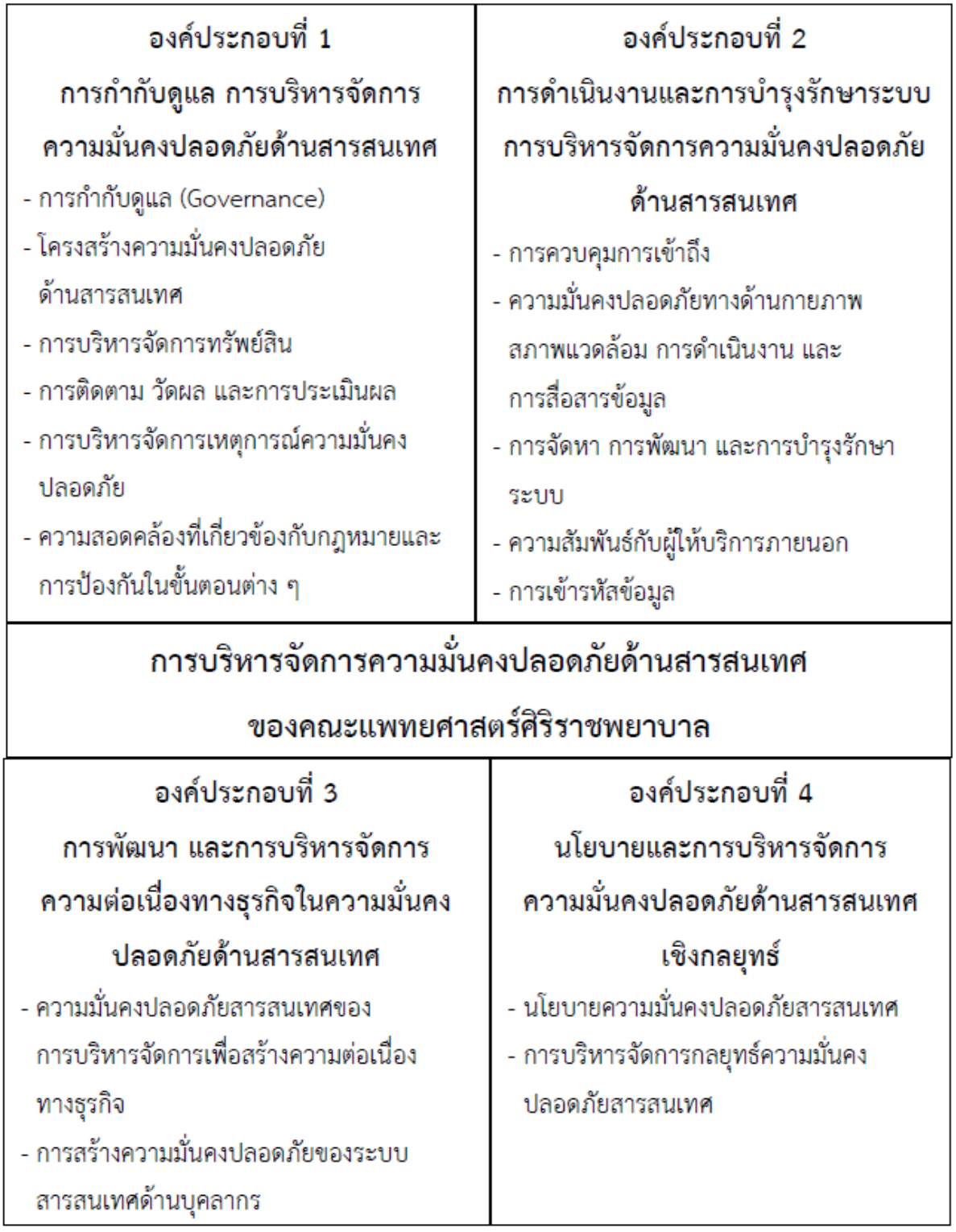
4.3 การสร้างสเกลโดยใช้องค์ประกอบพื้นฐาน (Factor – based Scales) ผู้วิจัยและนักวิชาการ พบว่า การวิจัยมีความคลาดเคลื่อนจากการสุ่มตัวอย่าง จึงทำให้ การสร้างสเกลองค์ประกอบจากสัมประสิทธิ์คะแนนองค์ประกอบทุกตัวแปรนั้นไม่จำเป็น แต่ควรเลือกมาเฉพาะบางตัวแปร เสนอว่า ตามกฎที่ได้มาจากประสบการณ์ (Rule of Thumb) ควรจะแยกเฉพาะตัวแปรที่มีค่าน้ำหนักองค์ประกอบเกิน 0.30 ดังนั้น การเลือกค่า Loading เพื่อจะได้ทราบว่าตัวแปรใดบรรจุอยู่ในองค์ประกอบใด อาจจะมีการพิจารณาที่ค่า Loading โดยปกติในงานวิจัยส่วนใหญ่จะใช้เกณฑ์ที่ 0.3 – 0.4 เพราะในงานวิจัยนั้นมักจะใช้กลุ่มตัวอย่างมีจำนวนมาก ของตารางแสดงความสัมพันธ์ระหว่างค่า Loading ที่มีนัยสำคัญทางสถิติที่ระดับ .05 ต่อจำนวนกลุ่มตัวอย่าง (Hair et al., 2006) ดังตารางที่ 2.4

ตารางที่ 2.4 ค่า Loading ที่มีนัยสำคัญทางสถิติที่ระดับ .05 ต่อจำนวนกลุ่มตัวอย่าง

Factor loading	0.30	0.35	0.40	0.45	0.50	0.55	0.60	0.65	0.70	0.75
จำนวนกลุ่มตัวอย่าง	350	250	200	150	120	100	85	70	60	50

2.4 กรอบแนวคิดงานวิจัย

กรอบแนวคิดในการวิจัย การวิเคราะห์องค์ประกอบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล เกิดจากการสังเคราะห์องค์ประกอบตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศที่เป็นมาตรฐานสากล ได้แก่ ISO/IEC 27001:20013 ISO/IEC 27001:2005 และ COBIT 5 และงานวิจัยที่เกี่ยวข้อง รวมถึงเสนอให้กับผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศช่วยตรวจสอบความสอดคล้องและความเป็นไปได้ ซึ่งแบ่งออกเป็นจำนวน 4 องค์ประกอบ 15 ตัวชี้วัด ได้แก่ องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ องค์ประกอบที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ ดังภาพที่ 2.13



ภาพที่ 2.13 กรอบแนวคิดงานวิจัย

บทที่ 3
ระเบียบวิธีวิจัย

งานวิจัยเรื่อง ศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลเป็นการวิจัยเชิงปริมาณ (Quantitative Research) ซึ่งวัตถุประสงค์ในการทำวิจัยนี้เพื่อศึกษาถึงองค์ประกอบของการบริหารความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ซึ่งผู้วิจัยได้ดำเนินการตามขั้นตอนดังนี้

3.1 ประชากรและกลุ่มตัวอย่าง

3.2 เครื่องมือที่ใช้ในงานวิจัย

3.3 การตรวจสอบคุณภาพของเครื่องมือวิจัย

3.4 การเก็บรวบรวมข้อมูล

3.5 วิธีวิเคราะห์ข้อมูล

3.1 ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัย

ประชากรที่ใช้ในการวิจัยครั้งนี้ได้แก่ บุคลากรผู้ใช้งานระบบสารสนเทศในแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล จำนวน 16,720 คน (ข้อมูล ณ วันที่ 31 มกราคม 2565)

กลุ่มตัวอย่างที่ใช้ในการวิจัย

กลุ่มตัวอย่างที่ใช้ในการวิจัย คือ ผู้วิจัยได้ทำการเลือกกลุ่มตัวอย่างที่ใช้ในการวิจัย คือ การเลือกแบบความน่าจะเป็นโดยเลือกใช้วิธีการสุ่มอย่างง่าย (Simple random sampling) จากการคัดเลือกจากสัดส่วนบุคลากรของแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล ซึ่งได้กำหนดขนาดตัวอย่างโดยใช้สูตรของยามาเน่ (Yamane, 1973) ด้วยการกำหนดความคาดเคลื่อนของการสุ่มตัวอย่างร้อยละ 5 หรือ 0.05 และแทนค่าจากสูตร ดังนี้

$$n = N / 1+N (e^2)$$

โดย n คือ จำนวนตัวอย่างหรือขนาดของกลุ่มตัวอย่าง

N คือ ขนาดของประชากรทั้งหมด

e คือ ความคาดเคลื่อนของการสุ่มตัวอย่าง ซึ่งในรายงานการวิจัยกำหนดให้มีความคลาดเคลื่อนได้ร้อยละ 5 หรือ 0.05

แทนค่า $n = 16,720 / 1+16,720 (0.05)^2$

$n = 16,720/42.8$

$n = 390.65$

ดังนั้น ผลจากการคำนวณ ได้กลุ่มตัวอย่างในการวิจัยครั้งนี้เท่ากับ 391 คน และสำรองไว้ เพื่อป้องกันความผิดพลาดจากแบบสอบถามที่ไม่สมบูรณ์ ผู้วิจัยจึงรวมขนาดกลุ่มตัวอย่างทั้งหมด 400 คน

3.2 เครื่องมือที่ใช้ในงานวิจัย

ในการวิจัยครั้งนี้ ใช้แบบสอบถาม (Questionnaire) ที่ผู้วิจัยสร้างขึ้นเป็นเครื่องมือในการเก็บรวบรวมข้อมูล โดยมีขั้นตอนการดำเนินการดังนี้

3.2.1 ศึกษาแนวคิด ทฤษฎี ผลงานวิจัยที่เกี่ยวข้องและเอกสารต่าง ๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ

3.2.2 กำหนดโครงสร้าง เนื้อหา รูปแบบของคำถามให้สอดคล้องกับเนื้อหาที่ผู้วิจัยทำการสังเคราะห์หาองค์ประกอบจากแนวคิด ทฤษฎี ผลงานวิจัยร่วมกับผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ จำนวน องค์ประกอบทั้ง 4 องค์ประกอบ พร้อมกำหนดนิยามเชิงปฏิบัติการ และกำหนดตัวบ่งชี้แต่ละองค์ประกอบ เพื่อสร้างเป็นข้อคำถามในแบบสอบถาม และพิจารณาคำถามแต่ละข้อกับอาจารย์ที่ปรึกษา โดยตรวจสอบความเหมาะสมของเนื้อหา ความถูกต้องของภาษา และความสอดคล้องตามนิยามเชิงปฏิบัติการและตัวบ่งชี้ แล้วนำมาปรับปรุงแก้ให้เหมาะสมตามคำแนะนำ

3.2.3 ร่างแบบสอบถาม ในการวัดระดับความคิดเห็นของกระบวนงานด้านการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยแบบสอบถามแบ่งออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม ได้แก่ เพศ อายุ ระดับการศึกษา ตำแหน่งหน่วยงานที่ปฏิบัติงาน ประสบการณ์การทำงานในหน่วยงานปัจจุบัน และระบบสารสนเทศที่ใช้ในการปฏิบัติงาน โดยแบบสอบถามจะกำหนดให้ผู้ตอบแบบสอบถามเป็นประเภทแบบตรวจสอบ (Check list)

ตอนที่ 2 สอบถามความคิดเห็นเกี่ยวกับกระบวนงานการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทย์ศาสตร์ศิริราชพยาบาล ในมุมมองของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศของหน่วยงานแบ่งออกเป็น 4 องค์ประกอบ 15 ตัวชี้วัด โดยแบบสอบถามจะกำหนดให้ผู้ตอบแบบสอบถามการศึกษาองค์ประกอบด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล สำหรับตอนที่ 1 จะเป็นประเภทแบบตรวจสอบ (Checklist) และตอนที่ 2 จะเป็นแบบมาตรวัดระดับชั้น (Rating Scale) และเกณฑ์ในการกำหนดค่าน้ำหนักการประเมินตามวิธีลิเคิร์ท (Likert Scale) เป็น 5 ระดับ ดังนี้

ระดับ 5	หมายถึง	มีความสำคัญมากที่สุด
ระดับ 4	หมายถึง	มีความสำคัญมาก
ระดับ 3	หมายถึง	มีความสำคัญปานกลาง
ระดับ 2	หมายถึง	มีความสำคัญน้อย
ระดับ 1	หมายถึง	มีความสำคัญน้อยที่สุด

ส่วนการแปลผล เพื่อจัดระดับคะแนนเฉลี่ยในการวิเคราะห์ข้อมูล ผู้วิจัยใช้เกณฑ์ ค่าเฉลี่ย ซึ่งคำนวณโดยใช้สูตรการหาความกว้างของอัตรภาคชั้น ดังนี้ (พิมพา หิรัญกิตติ และคณะ, 2552)

คำนวณได้จากสูตรช่วงของอันตรภาคชั้น

$$\frac{\text{Maximum} - \text{Minimum}}{\text{Interval}} = \frac{\text{คะแนนสูงสุด - คะแนนต่ำสุด}}{\text{จำนวนชั้น}}$$

$$= \frac{5 - 1}{5}$$

$$= 0.80$$

ดังนั้น การแปลผลของคะแนนที่ได้จากความคิดเห็น สามารถแยกระดับเกณฑ์คะแนน ที่จะใช้ประเมิน องค์ประกอบการบริหารจัดการเทคโนโลยีความมั่นคงสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ดังต่อไปนี้

ค่าฉลี่ย 4.21 – 5.00 หมายถึง ความสำคัญมากที่สุด

ค่าฉลี่ย 3.41 – 4.20 หมายถึง ความสำคัญสำคัญมาก

ค่าฉลี่ย 2.61 – 3.40 หมายถึง ความสำคัญปานกลาง

ค่าฉลี่ย 1.81 – 2.60 หมายถึง ความสำคัญน้อย

ค่าฉลี่ย 1.00 – 1.80 หมายถึง ความสำคัญน้อยที่สุด

ตอนที่ 3 ข้อเสนอแนะหรือความคิดเห็นเกี่ยวกับองค์ประกอบการบริหารจัดการเทคโนโลยีความมั่นคงสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลในปัจจุบันและอนาคต โดยแบบสอบถามจะกำหนดให้ผู้ตอบแบบสอบถามเป็นประเภทการเขียนตอบรรยาย

3.3 การตรวจสอบคุณภาพของเครื่องมือวิจัย

นำแบบสอบถามให้ผู้เชี่ยวชาญเฉพาะเรื่องด้านระบบสารสนเทศ ด้านการวัดและประเมินผล และการควบคุมภายใน เป็นต้น เพื่อตรวจสอบความเที่ยงตรง (Validity) เนื้อหาการวิจัย ซึ่งคำถามการวิจัยจะต้องมีค่าดัชนีความสอดคล้องระหว่างข้อคำถามและวัตถุประสงค์ (Item – Objective Congruence Index: IOC) พร้อมทั้งพิจารณาความถูกต้องชัดเจนของภาษาที่ใช้ แล้วนำมาปรับปรุงแก้ไขตามคำแนะนำของผู้เชี่ยวชาญ โดยผู้วิจัยจะนำข้อคำถามที่มีค่า IOC มากกว่า หรือเท่ากับ 0.5 มาใช้เป็นข้อคำถามในแบบสอบถาม ซึ่งมีทั้งหมด 35 ข้อ มีค่า IOC ผลรวมเฉลี่ยเท่ากับ 0.9619 นำแบบสอบถามที่ได้รับการปรับปรุงให้มีความสมบูรณ์นำไปหาความเชื่อมั่นของเครื่องมือ (Reliability) ของเนื้อหาโดยนำแบบสอบถามไปทดสอบขั้นต้น (Try out) กับกลุ่มที่ไม่ใช่กลุ่มตัวอย่างที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่างจำนวน 30 คน แล้วนำผลที่ได้ไปวิเคราะห์หาความเชื่อมั่นของแบบสอบถาม โดยวิธีการหาค่าสัมประสิทธิ์แอลฟาของครอนบัค (Cronbach alpha coefficient) ค่าแอลฟาที่ได้จะแสดงถึงระดับความคงที่ของแบบสอบถามโดยจะมีค่าระหว่าง $0 < \alpha < 1$ ค่าที่ใกล้เคียงกับ 1 มาก แสดงว่ามีความเชื่อมั่นสูง โดยกำหนดเกณฑ์ค่าความเชื่อมั่นของแบบสอบถามที่ยอมรับได้

ควรมีค่ามากกว่า 0.70 ซึ่งจากการทดสอบพบว่าค่า Cronbach alpha ของแบบสอบถามที่ใช้ในการทำวิจัยครั้งนี้เท่ากับ 0.986

3.4 การเก็บรวบรวมข้อมูล

หลังจากที่ผู้วิจัยได้รวบรวมแนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง เพื่อนำมาเป็นแนวทางในการสร้างเครื่องมือที่ใช้ในการศึกษาตามกรอบแนวคิดในการวิจัย โดยผู้วิจัยได้ดำเนินการรวบรวมข้อมูลในการวิจัยครั้งนี้อย่างเป็นขั้นเป็นตอน

3.4.1 นำหนังสือขออนุญาตจากมหาวิทยาลัยธุรกิจบัณฑิต เพื่อขอความอนุเคราะห์ในการใช้สถานที่เก็บรวบรวมข้อมูลและสนับสนุนงานวิจัย

3.4.2 ผู้วิจัยทาการแจกแบบสอบถาม ให้กับกลุ่มประชากรตัวอย่าง และเก็บรวบรวมข้อมูลแบบสอบถามที่สมบูรณ์ จำนวน 400 คน

3.4.3 ตรวจสอบความถูกต้องของข้อมูล จัดหมวดหมู่ของข้อมูลในแบบสอบถาม กำหนดรหัสและลงบันทึกข้อมูล

3.4.4 นำข้อมูลไปวิเคราะห์ทางสถิติ

3.5 วิธีวิเคราะห์ข้อมูล

เมื่อได้รับแบบสอบถามกลับคืนมา จำนวน 400 ชุด ผู้วิจัยนำแบบสอบถามที่รวบรวมได้ มาทำการตรวจสอบข้อมูลพร้อมลงรหัส (Coding) นำมาวิเคราะห์และประมวลผลด้วยโปรแกรม คอมพิวเตอร์สำเร็จรูป โดยตัวแปรต่าง ๆ จะถูกนำมาลงรหัสเพื่อเปลี่ยนสภาพข้อมูลให้อยู่ในรูป ตัวเลขแล้วนำ มาวิเคราะห์เพื่อหาความสัมพันธ์ระหว่างปัจจัยตามสมมติฐานที่ตั้งไว้โดยใช้เครื่องมือทางสถิติมาวิเคราะห์ข้อมูลต่อไปนี้

3.5.1 สถิติเชิงพรรณนา (Descriptive statistics) เพื่อใช้อธิบายรายละเอียดเกี่ยวกับลักษณะข้อมูล ส่วนบุคคลในตอนที่ 1 ข้อมูลทั่วไปของประชากรศาสตร์ ประกอบด้วย การแจกแจงค่าความถี่ (Frequency) แสดงผลเป็นค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และส่วนค่าเบี่ยงเบนมาตรฐาน (Standard Deviation: SD) ในการอธิบายและสรุปลักษณะทั่วไปของตัวแปรต่าง ๆ โดยแสดงเป็นตารางพร้อมคำอธิบาย

3.5.2 สถิติเชิงอนุมาน (Inferential statistics) การวิเคราะห์องค์ประกอบการบริหารจัดการเทคโนโลยีความมั่นคงสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ในมุมมองของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน ผู้วิจัยได้ทำการวิเคราะห์โดย Factor Analysis แบบสกัดปัจจัยโดยใช้โปรแกรมสำเร็จรูปทางสถิติ มาช่วยในการวิเคราะห์องค์ประกอบแต่ละตัวและค่า Factor Loading ขององค์ประกอบกระบวนการด้านการบริหารจัดการเทคโนโลยีความมั่นคงสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลในปัจจุบัน ข้อมูลที่ได้จากการวิเคราะห์แสดงถึงความสำคัญขององค์ประกอบของกระบวนงานด้านการบริหารจัดการเทคโนโลยีความมั่นคงสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลที่ผู้ตอบแบบสอบถามให้ความสำคัญมากในการใช้งานระบบสารสนเทศเพื่อการบริหารจัดการเทคโนโลยีความมั่นคงสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

บทที่ 4
ผลการวิเคราะห์ข้อมูล

งานวิจัยเรื่อง ศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลเป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยมีวัตถุประสงค์เพื่อศึกษาถึงองค์ประกอบของการบริหารความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ซึ่งผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลโดยการแจกแบบสอบถามให้กับบุคลากรของแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล ด้วยวิธีการในรูปแบบออนไลน์ และได้รับแบบสอบถามกลับคืนมาครั้งที่ 1 จำนวน 255 ชุด คิดเป็นร้อยละ 63.75 และครั้งที่ 2 จำนวน 145 ชุด คิดเป็นร้อยละ 36.25 ทั้งนี้ ผู้วิจัยก็ได้ทำการตรวจสอบความถูกต้องและครบถ้วนของแบบสอบถาม พบว่า แบบสอบถามมีความถูกต้องสมบูรณ์ครบถ้วนทั้งหมด รวมจำนวนทั้งสิ้น 400 ชุด คิดเป็นร้อยละ 100 จากจำนวนแบบสอบถามทั้งหมดที่แจกไป มาใช้ในการวิเคราะห์ผลและนำเสนอผลการศึกษา ดังนี้

4.1 ผลการวิเคราะห์ข้อมูลสถิติเชิงพรรณนา

4.2 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA)

4.1 ผลการวิเคราะห์ข้อมูลสถิติเชิงพรรณนา

4.1.1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถามที่เป็นบุคลากรผู้ใช้งานระบบสารสนเทศในแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล จำนวน 400 คน ซึ่งข้อมูลที่ใช้ในการวิเคราะห์ ได้แก่ เพศ อายุ ระดับการศึกษา ตำแหน่ง หน่วยงานที่ปฏิบัติงาน ประสบการณ์ทำงานในหน่วยงานปัจจุบัน และระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ปัจจุบัน ในรูปแบบค่าความถี่ (Frequency) และค่าร้อยละ (Percentage) ได้ดังนี้

ตารางที่ 4.1 จำนวน ร้อยละของกลุ่มตัวอย่างบุคลากรผู้ใช้งานระบบสารสนเทศในแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล

สถานภาพส่วนบุคคล	จำนวน	ร้อยละ
1. เพศ		
ชาย	103	25.80
หญิง	297	74.20
รวม	**400**	**100**

ตารางที่ 4.1 (ต่อ)

สถานภาพส่วนบุคคล	จำนวน	ร้อยละ
2. อายุ		
น้อยกว่า 20 ปี	12	3.00
21 – 30 ปี	82	20.50
31 – 40 ปี	154	38.50
41 – 50 ปี	152	38.00
มากกว่า 50 ปี	0	0
รวม	**400**	**100**
3. ระดับการศึกษา		
ต่ำกว่าปริญญาตรี	30	7.50
ปริญญาตรี	209	52.20
ปริญญาโท	147	36.80
ปริญญาเอก	14	3.50
รวม	**400**	**100**
4. ตำแหน่ง		
เจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป	171	42.80
เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT	75	18.80
นักศึกษา	17	4.20
แพทย์/พยาบาล/เภสัชกร/นักสาธารสุข	26	6.50
หัวหน้างาน/ผู้บริหาร	86	21.50
อาจารย์/นักวิชาการ/นักวิจัย	25	6.20
รวม	**400**	**100**
5. หน่วยงานที่ปฏิบัติงาน		
ฝ่ายการคลัง	102	25.50
ฝ่ายสารสนเทศ	80	20.00
หน่วยตรวจสอบภายใน	41	10.20
ฝ่ายทรัพยากรบุคคล	32	8.00
ฝ่ายนโยบายและแผน	19	4.80
ฝ่ายทรัพย์สินและพัสดุ	19	4.80

ตารางที่ 4.1 (ต่อ)

สถานภาพส่วนบุคคล	จำนวน	ร้อยละ
ฝ่ายวิศวกรรมบริการและอาคารสถานที่	13	3.20
ฝ่ายวิจัย	34	8.50
ฝ่ายการพยาบาล	22	5.50
ฝ่ายเภสัชกรรม	2	0.50
ฝ่ายโภชนาการ	2	0.50
ฝ่ายการศึกษา	34	8.50
รวม	**400**	**100**
6. ประสบการณ์ทำงาน (ถ้าเกิน 6 เดือนให้นับเป็น 1 ปี)		
น้อยกว่า 1 ปี	47	11.80
1 – 5 ปี	128	32.00
6 – 10 ปี	88	22.00
11 – 15 ปี	62	15.50
16 – 20 ปี	22	5.50
มากกว่า 20 ปี	53	13.20
รวม	**400**	**100**
7. ระบบเทคโนโลยีสารสนเทศที่ใช้ในปัจจุบัน (ตอบได้มากกว่า 1 ข้อ)		
ระบบสำนักงานอัตโนมัติ	5	1.05
ระบบประมวลผลรายการ	71	14.98
ระบบงานสร้างความรู้	91	19.20
ระบบสารสนเทศเพื่อการจัดการ	201	42.41
ระบบสนับสนุนการตัดสินใจ	60	12.66
ระบบสารสนเทศสำหรับผู้บริหารระดับสูง	38	8.01
ระบบอื่น ๆ เช่น งานสารบัญ งานการเงิน	8	1.69
รวม	**474**	**100**

จากตารางที่ 4.1 พบว่าข้อมูลทั่วไปของผู้ตอบแบบสอบถามของบุคลากรผู้ใช้งานระบบสารสนเทศในแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล จำนวน 400 คน จำแนกได้ดังนี้

เพศ พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง จำนวน 297 คน คิดเป็นร้อยละ 74.20 และเป็นเพศชาย จำนวน 103 คิดเป็นร้อยละ 25.80

อายุ พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่อยู่ระหว่างอายุ 31 – 40 ปี จำนวน 154 คน คิดเป็นร้อยละ 38.50 รองลงมาอยู่ระหว่างอายุ 41 – 50 ปี จำนวน 152 คน คิดเป็นร้อยละ 38.00 และ อยู่ระหว่างอายุ 21 – 30 ปี จำนวน 82 คน คิดเป็นร้อยละ 20.50 ตามลำดับ

ระดับการศึกษา พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่มีระดับการศึกษา ระดับปริญญาตรี จำนวน 209 คน คิดเป็นร้อยละ 52.20 รองลงมาระดับการศึกษา ระดับปริญญาโท จำนวน 147 คน คิดเป็นร้อยละ 36.80 และระดับการศึกษา ระดับต่ำกว่าปริญญาตรี จำนวน 30 คน คิดเป็นร้อยละ 7.50 ตามลำดับ

ตำแหน่ง พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่มีตำแหน่ง เจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป จำนวน 171 คน คิดเป็นร้อยละ 42.80 รองลงมาตำแหน่ง หัวหน้างาน/ผู้บริหาร จำนวน 86 คน คิดเป็นร้อยละ 21.50 และตำแหน่ง เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT จำนวน 75 คน คิดเป็นร้อยละ 18.80 ตามลำดับ

หน่วยงานที่ปฏิบัติงาน พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่ปฏิบัติงานที่ ฝ่ายการคลัง จำนวน 102 คน คิดเป็นร้อยละ 25.50 รองลงมาปฏิบัติงานที่ ฝ่ายสารสนเทศ จำนวน 80 คน คิดเป็นร้อยละ 20.00 และปฏิบัติงานที่ หน่วยตรวจสอบภายใน จำนวน 41 คน คิดเป็นร้อยละ 10.20 ตามลำดับ

ประสบการณ์ทำงาน (ถ้าเกิน 6 เดือนให้นับเป็น 1 ปี) พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่ ประสบการณ์ทำงานอยู่ระหว่าง 1 – 5 ปี จำนวน 128 คน คิดเป็นร้อยละ 32.00 รองลงมาประสบการณ์ ทำงานอยู่ระหว่าง 6 – 10 ปี จำนวน 88 คน คิดเป็นร้อยละ 22.00 และประสบการณ์ทำงานอยู่ระหว่าง11 – 15 ปี จำนวน 62 คน คิดเป็นร้อยละ 15.50 ตามลำดับ

ระบบเทคโนโลยีสารสนเทศที่ใช้ปัจจุบัน (ตอบได้มากกว่า 1 ข้อ) พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่ใช้ ระบบเทคโนโลยีสารสนเทศประเภท ระบบสารสนเทศเพื่อการจัดการ จำนวน 201 คน คิดเป็นร้อยละ 42.41 รองลงมา ใช้ระบบเทคโนโลยีสารสนเทศประเภทอยู่ระหว่าง ระบบงานสร้างความรู้จำนวน 91 คน คิดเป็นร้อยละ 19.20 และใช้ ระบบเทคโนโลยีสารสนเทศประเภท ระบบประมวลผลรายการ จำนวน 71 คน คิดเป็นร้อยละ 14.98 ตามลำดับ

4.1.2 ข้อมูลความคิดเห็นเกี่ยวกับองค์ประกอบกระบวนการบริหารจัดการความมั่งคงปลอดภัยด้าน สารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ผลการวิเคราะห์ข้อมูลเกี่ยวกับความคิดเห็นองค์ประกอบกระบวนการบริหารจัดการความมั่นคง ปลอดภัยด้านสารสนเทศ ของบุคลากรของแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาลจากแนวคิด ทฤษฎี ผลงานวิจัยที่เกี่ยวข้องและเอกสารต่าง ๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ ร่วมกับ ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศแบ่งออกเป็น 4 องค์ประกอบ ได้แก่ 1) การกำกับดูแล การบริหารจัดการความ มั่นคงปลอดภัยด้านสารสนเทศ 2) การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคง ปลอดภัยด้านสารสนเทศ 3) การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัย ด้านสารสนเทศ และ 4) นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ ดังนี้

ตารางที่ 4.2 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ระดับความคิดเห็นขององค์ประกอบกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลในภาพรวม

ข้อ	องค์ประกอบกระบวนการบริการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
1	การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	3.79	0.8030	มาก
2	การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	3.68	0.8390	มาก
3	การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ	3.73	0.9230	มาก
4	นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์	3.65	0.8625	มาก
	รวม	**3.71**	**0.7720**	**มาก**

จากตารางที่ 4.2 ระดับความคิดเห็นเฉลี่ยของผู้ตอบแบบสอบถามโดยภาพรวมขององค์ประกอบกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลอยู่ในระดับมาก ($\bar{X}$ = 3.71, S.D. = 0.7720) และผลการพิจารณารายข้อ พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมากทุกข้อ ($\bar{X}$ = 3.65-3.79, S.D. = 0.8030 – 0.9230) โดยความคิดเห็นเฉลี่ยค่าสูงที่สุด คือ ด้านการกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับมาก ($\bar{X}$ = 3.79, S.D. = 0.8030) รองลงมา คือ ด้านการพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับมาก ($\bar{X}$ = 3.73, S.D. = 0.9230) และด้านการดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับมาก ($\bar{X}$ = 3.68, S.D. = 0.8390) ตามลำดับ

เมื่อพิจารณารายข้อตามองค์ประกอบของกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลแบ่งออกเป็น 4 องค์ประกอบ ได้แก่ 1) การกำกับดูแล การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ 2) การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ 3) การพัฒนาและการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ และ 4) นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ ดังนี้

องค์ประกอบที่ 1 การกำกับดูแล การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

ผลการวิเคราะห์ข้อมูลเกี่ยวกับค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความคิดเห็นองค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ของบุคลากรแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล สามารถอธิบายได้ ดังนี้

ตารางที่ 4.3 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ระดับความคิดเห็นขององค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

ประเด็น	องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
1	มีการกำหนดกรอบการดำเนินงานด้านการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เช่น การบำรุงรักษาระบบ เครื่องมือเทคโนโลยีสารสนเทศ อุปกรณ์การเข้าใช้งานระบบสารสนเทศ เป็นต้น ให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง	3.93	0.9408	มาก
2	มีการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานให้มีความรวดเร็ว ข้อมูลมีความถูกต้องครบถ้วน และเป็นปัจจุบัน เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้	4.10	0.8757	มาก
3	มีการมอบหมายภารกิจด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้กับผู้ปฏิบัติงานได้อย่างชัดเจน	3.73	0.8590	มาก
4	มีการจัดทำข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่อนุญาตให้บุคคลหรือหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน	3.59	0.9769	มาก
5	มีมาตรการด้านความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์พกพา เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว	3.75	0.9649	มาก

ตารางที่ 4.3 (ต่อ)

ประเด็น	องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
6	มีการกำหนดข้อปฏิบัติในการใช้คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ เช่น เครื่องคอมพิวเตอร์แบบพกพา สมาร์ทโฟน เป็นต้น เพื่อให้มีความมั่นคงปลอดภัย และเกิดประสิทธิภาพต่อการใช้งาน	3.79	0.9623	มาก
7	มีการเก็บบันทึก และจำแนกประเภทของบัญชีทรัพย์สิน ข้อมูลสารสนเทศ เพื่อกำหนดระดับของการป้องกันทรัพย์สินด้าสารสนเทศ	3.86	0.9980	มาก
8	มีการจัดทำทะเบียน รับ – คืนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ	3.81	0.9624	มาก
9	มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ	3.86	0.8912	มาก
10	มีการจัดทำบันทึกข้อตกลงให้ผู้ปฏิบัติงานต้องรักษาทรัพย์สินให้ปลอดภัย และข้อมูลที่เป็นความลับ	3.83	0.9713	มาก
11	มีการรวบรวมข้อมูล ตรวจสอบ และประเมินผลการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศตามแนวทางการควบคุมภายในด้านการใช้งานระบบสารสนเทศของหน่วยงาน เพื่อระบุข้อบกพร่องในการใช้งานระบบ และนำมาปรับปรุงให้สามารถทำงานได้อย่างมีประสิทธิภาพ	3.76	0.9564	มาก
12	มีขั้นตอน หรือแผนรองรับในการบริหารจัดการเหตุการณ์ผิดปกติ และปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ พร้อมทั้งช่องทางการรายงานเหตุการณ์ปัญหาที่พบผิดปกติที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศ อย่างเหมาะสมและทันท่วงที	3.67	0.9381	มาก
13	มีมาตรการป้องกันภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น เพื่อป้องกันไม่ให้ทรัพย์สินสารสนเทศเสียหาย	3.71	0.9376	มาก

ตารางที่ 4.3 (ต่อ)

ประเด็น	องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
14	มีการป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ และเป้าหมายของงานที่รับผิดชอบ	3.75	0.9753	มาก
	รวม	**3.79**	**0.8030**	**มาก**

จากตารางที่ 4.3 ระดับความคิดเห็นเฉลี่ยของผู้ตอบแบบสอบถามขององค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.79, S.D. = 0.8030) โดยผลการพิจารณารายประเด็น พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นค่าเฉลี่ยทุกข้ออยู่ในระดับมาก ($\bar{X}$ = 3.59 – 4.10, S.D. = 0.8590 – 0.9980) โดยความคิดเห็นเฉลี่ยค่าสูงที่สุด คือ มีการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานให้มีความรวดเร็ว ข้อมูลมีความถูกต้องครบถ้วน และเป็นปัจจุบัน เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้อยู่ในระดับมาก ($\bar{X}$ = 4.10, S.D. = 0.8757) รองลงมา คือ มีการกำหนดกรอบการดำเนินงานด้านการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เช่น การบำรุงรักษาระบบ เครื่องมือเทคโนโลยีสารสนเทศ อุปกรณ์การเข้าใช้งานระบบสารสนเทศ เป็นต้น ให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง อยู่ในระดับมาก ($\bar{X}$ = 3.93, S.D. = 0.9408) และมีการเก็บบันทึก และจำแนกประเภทของบัญชีทรัพย์สิน ข้อมูลสารสนเทศ เพื่อกำหนดระดับของการป้องกันทรัพย์สินด้านสารสนเทศ ($\bar{X}$ = 3.86, S.D. = 0.9980) และ มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ ($\bar{X}$ = 3.86, S.D. = 0.8912) เท่ากัน ตามลำดับ

องค์ประกอบที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

ผลการวิเคราะห์ข้อมูลเกี่ยวกับค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความคิดเห็นองค์ประกอบที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ของบุคลากรแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล สามารถอธิบายได้ ดังนี้

ตารางที่ 4.4 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ระดับความคิดเห็นขององค์ประกอบที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

ประเด็น	องค์ประกอบที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
1	มีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก	3.78	0.9333	มาก
2	มีการกำหนดขั้นตอน ควบคุมการตรวจสอบ ป้องกันและกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์	3.69	0.9230	มาก
3	มีการรักษาความมั่งคงของแม่ข่าย (Server) และอุปกรณ์ที่ใช้งานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรม ไม่พึงประสงค์ดี (Malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหล ของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต	3.74	0.9175	มาก
4	มีการจัดทำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไว้ในเงื่อนไขการจ้างพัฒนาหรือปรับปรุงระบบ เช่น เอกสารรายละเอียดคุณสมบัติทางเทคนิคในการจัดซื้อจัดจ้างโดยครอบคลุมถึงเรื่องรักษาความมั่นคงปลอดภัย	3.69	0.9235	มาก
5	มีการดูแล ควบคุม ติดตามตรวจสอบการพัฒนาระบบสารสนเทศ โดยหน่วยงานภายนอก รวมถึงการจ้างช่วงพัฒนาระบบ	3.65	0.9953	มาก
6	มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงาน ต้องปฏิบัติตามสัญญาหรือข้อตกลงในการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ	3.77	0.9464	มาก

ตารางที่ 4.4 (ต่อ)

ประเด็น	องค์ประกอบที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
7	มีการจ้างผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจในการร่วมพัฒนา มีการคำนึงถึงความต่อเนื่องในการดำเนินธุรกิจ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และการยกเลิกหรือสิ้นสุดสัญญา (Exit Strategy)	3.49	0.9472	มาก
8	มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ หรือธุรกรรมออนไลน์กับบุคคลหรือหน่วยงานภายนอก (เช่น การสั่งซื้อ/ขายสินค้าหรือบริการผ่านระบบอิเล็กทรอนิกส์ การชำระเงินผ่านระบบอิเล็กทรอนิกส์) เป็นต้น	3.55	0.9975	มาก
9	มีการกำหนดให้มีการเข้าใช้งานระบบสารสนเทศตามมาตรการเข้ารหัสข้อมูล (Cryptography) และการบริหารจัดการกุญแจ (Access Key) เป็นต้น	3.71	0.9764	มาก
10	มีการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงาน สอดคล้องกับชั้นความลับของสารสนเทศ	3.72	0.9773	มาก
	รวม	**3.68**	**0.8390**	**มาก**

จากตารางที่ 4.4 ระดับความคิดเห็นเฉลี่ยของผู้ตอบแบบสอบถามขององค์ประกอบที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.68, S.D. = 0.8390) ผลการพิจารณารายประเด็น พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นค่าเฉลี่ยทุกข้ออยู่ในระดับมาก ($\bar{X}$ = 3.49 – 3.78, S.D. = 0.8590 – 0.9975) โดยความคิดเห็นเฉลี่ยค่าสูงที่สุด คือ มีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก อยู่ในระดับมาก ($\bar{X}$ = 3.78, S.D. = 0.9333) รองลงมา คือ มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงาน

ต้องปฏิบัติตามสัญญาหรือข้อตกลงในการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ อยู่ในระดับมาก ($\bar{X}$ = 3.77, S.D. = 0.9464) และ มีการรักษาความมั่งคงของแม่ข่าย (Server) และอุปกรณ์ที่ใช้งานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่พึงประสงค์ดี (Malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหล ของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาตอยู่ในระดับมาก ($\bar{X}$ = 3.74, S.D. = 0.9175) ตามลำดับ

องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ

ผลการวิเคราะห์ข้อมูลเกี่ยวกับค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความคิดเห็นองค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศของบุคลากรแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล สามารถอธิบายได้ ดังนี้

ตารางที่ 4.5 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ระดับความคิดเห็นขององค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ

ประเด็น	องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
1	มีการบำรุงรักษาและดูแลอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน	3.84	0.9696	มาก
2	มีการจัดทำ และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบต่าง ๆ เพื่อให้ผู้ปฏิบัติงานสามารถนำไปปฏิบัติได้อย่างถูกต้องและปลอดภัย	3.73	0.9815	มาก
3	มีการกำหนดให้ผู้ปฏิบัติงานหรือบุคคลภายนอกที่หน่วยงานว่าจ้างจะต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย และบทลงโทษ ในกรณีที่ผู้ปฏิบัติงานฝ่าฝืนนโยบายหรือระเบียบที่หน่วยงานประกาศใช้อย่างชัดเจน	3.70	0.9871	มาก
4	มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้เป็นปัจจุบันโดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน	3.76	0.9866	มาก

ตารางที่ 4.5 (ต่อ)

ประเด็น	องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
5	มีการกำหนดให้เจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงาน เมื่อสิ้นสุดการจ้างงาน	3.67	0.9841	มาก
6	มีการพัฒนา อบรม เพิ่มพูน ทักษะและความสามารถของผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	3.67	0.9841	มาก
	รวม	**3.73**	**0.9230**	**มาก**

จากตารางที่ 4.5 ระดับความคิดเห็นเฉลี่ยของผู้ตอบแบบสอบถามขององค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.73, S.D. =0.9230) และผลการพิจารณารายประเด็น พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นค่าเฉลี่ยทุกข้ออยู่ในระดับมาก ($\bar{X}$ = 3.67 – 3.84, S.D. = 0.9696 – 0.9871) โดยความคิดเห็นเฉลี่ยค่าสูงที่สุด คือมีการบำรุงรักษาและดูแลอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน อยู่ในระดับมาก ($\bar{X}$ = 3.84, S.D. = 0.9696) รองลงมา คือ มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน อยู่ในระดับมาก ($\bar{X}$ = 3.76, S.D. = 0.9866) และมีการจัดทำ และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบต่าง ๆ เพื่อให้ผู้ปฏิบัติงานสามารถนำไปปฏิบัติได้อย่างถูกต้องและปลอดภัย อยู่ในระดับมาก ($\bar{X}$ = 3.73, S.D. = 0.9815) ตามลำดับ

องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์

ผลการวิเคราะห์ข้อมูลเกี่ยวกับค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความคิดเห็นองค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ ของบุคลากรแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล สามารถอธิบายได้ ดังนี้ดังนี้

ตารางที่ 4.6 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ระดับความคิดเห็นขององค์ประกอบที่ 4 นโยบาย และการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์

ประเด็น	องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน	ระดับความคิดเห็น
1	มีการกำหนดกลยุทธ์เพื่อการบริหารงานของหน่วยงานโดยการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินงานสอดคล้องกับนโยบาย บทบาท ภารกิจของหน่วยงาน และระบบความมั่นคงปลอดภัยด้านสารสนเทศ	3.77	0.9986	มาก
2	มีการกำหนดนโยบายและแนวทางสำหรับความมั่นคงปลอดภัยด้านสารสนเทศเพื่อควบคุม และป้องกันความเสี่ยงด้านสารสนเทศเป็นลายลักษณ์อักษร และประกาศหรือแจ้งนโยบายดังกล่าวให้ผู้ปฏิบัติงานรับทราบทั่วกัน	3.69	0.9952	มาก
3	มีการวิเคราะห์ความเสี่ยง (Risk analysis) และประเมินค่าความเสี่ยง (Risk Evaluation) เพื่อประเมินระดับผลกระทบและโอกาสเกิดเหตุการณ์ และจัดลำดับความเสี่ยงในการจัดการด้านสารสนเทศของหน่วยงาน	3.57	0.9754	มาก
4	มีการจัดการความเสี่ยง (Risk Treatment) กำหนดแนวทางติดตาม ทบทวน และประเมินความเสี่ยงที่เกิดขึ้นด้านสารสนเทศ เช่น ด้านข้อมูล ด้านอุปกรณ์เทคโนโลยีสารสนเทศ ด้านซอฟแวร์คอมพิวเตอร์ เป็นต้น อย่างสม่ำเสมอ	3.66	0.9556	มาก
5	มีการรายงานผลการบริหารความเสี่ยงด้านสารสนเทศ และแนวโน้มของความเสี่ยงที่อาจจะเกิดขึ้นตามนโยบายที่กำหนดให้ท่านทราบ อยู่ในระดับใดอิเล็กทรอนิกส์การชำระเงินผ่านระบบอิเล็กทรอนิกส์) เป็นต้น	3.56	0.8506	มาก
	รวม	**3.65**	**0.8625**	**มาก**

จากตารางที่ 4.6 ระดับความคิดเห็นเฉลี่ยของผู้ตอบแบบสอบถามขององค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ โดยรวมอยู่ในระดับมาก ($\bar{X}$ = 3.65, S.D. = 0.8625) และผลการพิจารณารายประเด็น พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นค่าเฉลี่ยทุกข้ออยู่ใน

ระดับมาก ($\bar{X}$ = 3.56 – 3.77, S.D. = 0.8506 – 0.9986) โดยความคิดเห็นเฉลี่ยค่าสูงที่สุด คือ มีการกำหนดกลยุทธ์เพื่อการบริหารงานของหน่วยงาน โดยการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินงานสอดคล้องกับนโยบาย บทบาท ภารกิจของหน่วยงาน และระบบความมั่นคงปลอดภัยด้านสารสนเทศอยู่ในระดับมาก ($\bar{X}$ = 3.77, S.D. = 0.9986) รองลงมา คือ มีการกำหนดนโยบายและแนวทางสำหรับความมั่นคงปลอดภัยด้านสารสนเทศเพื่อควบคุมและป้องกันความเสี่ยงด้านสารสนเทศเป็นลายลักษณ์อักษร และประกาศหรือแจ้งนโยบายดังกล่าวให้ผู้ปฏิบัติงานรับทราบทั่วกันอยู่ในระดับมาก ($\bar{X}$ = 3.69, S.D. = 0.9952) และมีการจัดการความเสี่ยง (Risk Treatment) กำหนดแนวทาง ติดตาม ทบทวน และประเมินความเสี่ยงที่เกิดขึ้นด้านสารสนเทศ เช่น ด้านข้อมูล ด้านอุปกรณ์เทคโนโลยีสารสนเทศ ด้านซอฟแวร์คอมพิวเตอร์ เป็นต้น อย่างสม่ำเสมออยู่ในระดับมาก ($\bar{X}$ = 3.66, S.D. = 0.9556) ตามลำดับ

4.2 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA)

ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ซึ่งเป็นการวิเคราะห์ข้อมูลข้อ 4.2 นี้เป็นการตอบวัตถุประสงค์เพื่อค้นหาองค์ประกอบของการบริหารความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยการวิเคราะห์องค์ประกอบในขั้นตอนนี้เป็นเทคนิคการวิเคราะห์ทางสถิติที่ใช้ในการจัดกลุ่มจำนวนตัวแปรที่มีอยู่จำนวนมาก และอาจมีคุณสมบัติในการอธิบายลักษณะของข้อมูลเหมือนกันได้ให้อยู่ในกลุ่มเดียวกัน เรียกว่า “องค์ประกอบ” (Factor) เหตุผลในการวิเคราะห์องค์ประกอบนี้เพื่อให้ได้จำนวนองค์ประกอบที่สามารถอธิบายความผันแปรของข้อมูล และเป็นการศึกษาลักษณะการรวมตัวของกลุ่มตัวแปรในลักษณะเส้นตรง (Linear Combination) ผลการวิเคราะห์องค์ประกอบเชิงสำรวจในการวิจัยนี้ ดังนี้

4.2.1 ผลการวิเคราะห์ข้อตกลงเบื้องต้นและการทดสอบ

ข้อตกลงเบื้องต้นที่สำคัญของการวิเคราะห์องค์ประกอบ คือ ตัวแปรต้องมีความสัมพันธ์กัน เนื่องจากวัตถุประสงค์หลักของการวิเคราะห์องค์ประกอบเพื่อรวมกลุ่มของตัวแปรที่สัมพันธ์กัน ซึ่งการตรวจสอบสอบเบื้องต้นว่าข้อมูลชุดนั้น จะนำมาวิเคราะห์องค์ประกอบได้หรือไม่คือ การพิจารณาเมทริกซ์สหสัมพันธ์ของตัวแปรชุดนั้น ตัวแปรที่จะนำมาวิเคราะห์องค์ประกอบจะต้องมีความสัมพันธ์กันไม่น้อยกว่า .30 นอกจากนี้ ยังมีนักวิชาการได้มีการกำหนดเกณฑ์การตรวจสอบว่าตัวแปรมีความสัมพันธ์กันหรือไม่ สามารถตรวจสอบได้โดยการคำนวณค่าสหสัมพันธ์บางส่วน (Partial Correlation) คือการหาความสัมพันธ์ของตัวแปรเมื่อควบคุมตัวแปรอื่น ซึ่งควรจะมีค่าต่ำ สำหรับการวิเคราะห์องค์ประกอบด้วยโปรแกรม SPSS ค่าสถิติทดสอบเพื่อพิจารณาว่าข้อมูลชุดนี้เหมาะสมที่จะนำมาวิเคราะห์องค์ประกอบหรือไม่ คือ ค่า KMO and Bartlett’s Test เมื่อเลือกสถิติทดสอบตัวนี้จะได้ค่าสถิติทดสอบ 2 ค่า สถิติทดสอบตัวแรก คือ ค่า Kaiser- Meyer -Olkin Measure of Sampling Adequacy (MSA) ดัชนีตัวนี้ มีค่าระหว่าง 0 ถึง 1 ค่าจะเท่ากับ 1 เมื่อตัวแปรแต่ละตัวสามารถทำนายได้ด้วยตัวแปรอื่น โดยปราศจากความคลาดเคลื่อน ส่วนค่าในช่วงอื่น ๆ แปลความหมายดังนี้ (สุภมาส อังศุโชติ และคณะ, 2551; Hair et al., 2006)

.80 ขึ้นไป	เหมาะสมที่จะวิเคราะห์องค์ประกอบดีมาก
.70 - .79	เหมาะสมที่จะวิเคราะห์องค์ประกอบดี
.60 - .69	เหมาะสมที่จะวิเคราะห์องค์ประกอบปานกลาง
.50 - .59	เหมาะสมที่จะวิเคราะห์องค์ประกอบน้อย
น้อยกว่า .50	ไม่เหมาะสมที่จะนำข้อมูลชุดนั้นมาวิเคราะห์องค์ประกอบ

สถิติทดสอบตัวที่สอง คือ Bartlett's Test of Sphericity ใช้ทดสอบว่าตัวแปรต่าง ๆ มีความสัมพันธ์กันหรือไม่ โดยมีสมมติฐานของการทดลองดังนี้

H_0 : Correlation matrix เป็น Identity matrix (เมทริกซ์ที่มีค่าในแนวทแยงเป็น 1 ค่านอกแนวทแยงเป็น 0) หรือตัวแปรต่าง ๆ ไม่สัมพันธ์กัน

H_1 : Correlation matrix ไม่เป็น Identity matrix หรือตัวแปรต่าง ๆ มีความสัมพันธ์กัน

ถ้าค่า Bartlett's test of Sphericity มีนัยสำคัญ แสดงว่า ตัวแปรต่าง ๆ มีความสัมพันธ์กัน สามารถนำไปวิเคราะห์องค์ประกอบได้ รายละเอียดดังตารางที่ 4.7

ตารางที่ 4.7 แสดงค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตได้ในการวิเคราะห์องค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

Item	1	2	3	4	5	6	7	8	9	10	11	12	13
1	.982												
2	.733**	.977											
3	.567**	.622**	.923										
4	.643**	.681**	.888**	.942									
5	.729**	.703**	.641**	.733**	.986								
6	.715**	.680**	.637**	.735**	.775**	.986							
7	.689**	.681**	.629**	.708**	.734**	.692**	.976						
8	.672**	.707**	.599**	.687**	.677**	.635**	.776**	.970					
9	.646**	.619**	.579**	.644**	.707**	.736**	.592**	.664**	.982				
10	.692**	.683**	.651**	.753**	.703**	.736**	.713**	.783**	.719**	.980			
11	.678**	.645**	.715**	.788**	.733**	.720**	.693**	.656**	.651**	.755**	.978		
12	.653**	.639**	.710**	.804**	.754**	.708**	.690**	.673**	.659**	.735**	.832**	.976	
13	.711**	.622**	.609**	.706**	.727**	.744**	.701**	.705**	.688**	.787**	.757**	.792**	.988
14	.700**	.684**	.688**	.785**	.726**	.740**	.649**	.683**	.656**	.746**	.744**	.822**	.780**
15	.646**	.618**	.638**	.706**	.688**	.705**	.697**	.663**	.665**	.709**	.703**	.699**	.710**
16	.570**	.640**	.621**	.700**	.674**	.728**	.647**	.604**	.634**	.751**	.738**	.707**	.728**
17	.644**	.619**	.619**	.706**	.686**	.705**	.683**	.650**	.674**	.703**	.707**	.709**	.708**
18	.567**	.637**	.617**	.701**	.670**	.727**	.644**	.601**	.634**	.750**	.737**	.708**	.727**
19	.547**	.526**	.599**	.676**	.614**	.669**	.607**	.571**	.627**	.687**	.622**	.644**	.676**
20	.596**	.585**	.586**	.680**	.627**	.658**	.555**	.593**	.638**	.731**	.716**	.686**	.703**
21	.527**	.505**	.483**	.574**	.559**	.584**	.493**	.469**	.541**	.587**	.643**	.584**	.549**
22	.550**	.531**	.514**	.600**	598**	.612**	.532**	.501**	.568**	.609**	.675**	.613**	.582**
23	.560**	.538**	.478**	.579**	.600**	.699**	.530**	.520**	.655**	.741**	.690**	.698**	.709**
24	.565**	.540**	.483**	585**	.605**	.705**	.533**	.524**	.662**	.747**	.694**	.700**	.711**
25	.702**	.666**	.612**	.680**	.724**	.733**	.663**	.678**	.765**	.697**	.703**	.694**	.708**
26	.618**	.609**	.521**	628**	.659**	.663**	.607**	.615**	.696**	.625**	.639**	.635**	.647**
27	.631**	.656**	.625**	.738**	.687**	.693**	.659**	.656**	.677**	.680**	.748**	.761**	.697**
28	.682**	.686**	.685**	.765**	.721**	.733**	.687**	.689**	.711**	.714**	.792**	.799**	.729**
29	.615**	.637**	.601**	.722**	.675**	.679**	.650**	.640**	.658**	.662**	.725**	.746**	.680**
30	.623**	.646**	.626**	.721**	.676**	.683**	.655**	.648**	.666**	.670**	.743**	.747**	.682**
31	.477**	.414**	.505**	.592**	.604**	.628**	.423**	.378**	.582**	.543**	.492**	.558**	.738**
32	.444**	.403**	.484**	.566**	.571**	.593**	.399**	.365**	.564**	.516**	.454**	.523**	.553**
33	.608**	.584**	.574**	.686**	.701**	.709**	.571**	.544**	.614**	.638**	.662**	.680**	.662**
34	.417**	.386**	.467**	.546**	.552**	.673**	.371**	.337**	.525**	.487**	.441**	.511**	.533**
35	.617**	.571**	.551**	.668**	.694**	.713**	.572**	.512**	.591**	.628**	.667**	.684**	.664**
$\bar{x}$	3.93	4.10	3.73	3.59	3.75	3.79	3.86	3.81	3.86	3.83	3.76	3.67	3.71
SD	0.9408	0.8757	0.8590	0.9769	0.9649	0.9623	0.9980	0.9624	0.8912	0.9713	0.9564	0.9381	0.9376

** มีนัยสำคัญทางสถิติที่ระดับ .01 ; * มีนัยสำคัญทางสถิติที่ระดับ .05 ,ค่าแนวทแยง คือ ค่า MSA

ตารางที่ 4.7 (ต่อ)

Item	14	15	16	17	18	19	20	21	22	23	24	25
14	.980											
15	.670**	.936										
16	.664**	.815**	.928									
17	.684**	.969**	.808**	.937								
18	.666**	.811**	.999**	.806**	.929							
19	.616**	.749**	.794**	.734**	.792**	.968						
20	.688**	.712**	.795**	.714**	.793**	.801**	.982					
21	.574**	.650**	.695**	.655**	.696**	.722**	.718**	.912				
22	.594**	.682**	.721**	.685**	.719**	.751**	.736**	.973**	.916			
23	.649**	.663**	.745**	.675**	.749**	.676**	.732**	.678**	.687**	.889		
24	.651**	.670**	.747**	.677**	.751**	.678**	.736**	.681**	.689**	.996**	.889	
25	.711**	.653**	.634**	.658**	.633**	.576**	.625**	.561**	.592**	.646**	.649**	.866
26	.644**	.569**	.585**	.606**	.587**	.516**	.572**	.530**	.532**	.604**	.593**	.920**
27	.735**	.652**	.668**	.680**	.670**	.599**	.659**	.625**	.626**	.660**	.656**	.770**
28	.771**	.704**	.700**	.714**	.699**	.634**	.692**	.640**	.665**	.680**	.684**	.808**
29	.720**	.635**	.653**	.661**	.655**	.585**	.641**	.613**	.607**	.649**	.643**	.754**
30	.719**	.646**	.656**	.668**	.655**	.588**	.648**	.619**	.617**	.643**	.640**	.760**
31	.593**	.424**	.567**	.443**	.574**	.464**	.488**	.425**	.435**	.591**	.597**	.522**
32	.563**	.395**	.539**	.421**	.546**	.434**	.434**	.414**	.411**	.561**	.560**	.495**
33	.675**	.530**	.596**	.572**	.600**	.590**	.590**	.562**	.561**	.600**	.598**	.652**
34	.554**	.363**	.508**	.401**	.515**	.407**	.407**	.390**	.389**	.551**	.547**	.479**
35	.657**	.527**	.583**	.549**	.585**	.588**	.588**	.585**	.568**	.594**	.591**	.647**
$\bar{x}$	3.75	3.78	3.69	3.74	3.69	3.65	3.77	3.49	3.55	3.71	3.72	3.84
SD	0.9753	0.9333	0.9230	0.9175	0.9235	0.9953	0.9464	0.9472	0.9975	0.9764	0.9773	0.9696

** มีนัยสำคัญทางสถิติที่ระดับ .01 ; * มีนัยสำคัญทางสถิติที่ระดับ .05 ,ค่าแนวทแยง คือ ค่า MSA

ตารางที่ 4.7 (ต่อ)

Item	26	27	28	29	30	31	32	33	34	35
26	.850									
27	.800**	.894								
28	.734**	.955**	.883							
29	.793**	.982**	.936**	.906						
30	.782**	.975**	.946**	.991**	.905					
31	.485**	.502**	.521**	.497**	.483**	.910				
32	.524**	.524**	.490**	.523**	.502**	.956**	.925			
33	.696**	.714**	.674**	.695**	.682**	.622**	.674**	.953		
34	.513**	.507**	.476**	.502**	.486**	.931**	.940**	.677**	.962	
35	.674**	.710**	.675**	.705**	.702**	.641**	.650**	.883**	.641**	.941
$\bar{x}$	3.73	3.70	3.76	3.67	3.67	3.77	3.69	3.57	3.66	3.56
SD	0.9815	0.9871	0.9866	0.9841	0.9841	0.9986	0.9952	0.9754	0.9556	0.8506
Bartlett's test: χ^2 = 25997.821, p<.05, KMO=.938										

** มีนัยสำคัญทางสถิติที่ระดับ .01 ; * มีนัยสำคัญทางสถิติที่ระดับ .05 ,ค่าแนวทแยง คือ ค่า MSA

จากตารางที่ 4.7 พบว่า ผลการวิเคราะห์ความสัมพันธ์ของตัวแปรที่ใช้ในการวิเคราะห์องค์ประกอบ พบว่าความสัมพันธ์ระหว่างตัวแปรสังเกตได้ทั้ง 35 ตัวแปร จำนวน 70 คู่ มีความสัมพันธ์ทางบวกทุกคู่ (r_{xy} = .337 ถึง .999) อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 โดยคู่ที่มีความสัมพันธ์กันสูงสุดคือ Item 16 กับ Item 18 (r_{xy} = .999) ส่วนคู่ที่มีความสัมพันธ์กันต่ำสุดคือ Item 8 กับ Item 34 (r_{xy} = .337) พบว่าตัวแปรมีความสัมพันธ์กันไม่น้อยกว่า .30 ดังนั้นตัวแปรจึงมีความเหมาะสมที่จะนำมาวิเคราะห์องค์ประกอบ

เมื่อตรวจสอบความเหมาะสมของข้อมูลพบว่าเมทริกซ์สหสัมพันธ์ระหว่างข้อคำถามแตกต่างจากเมทริกซ์เอกลักษณ์อย่างมีนัยสำคัญ (Bartlett's test: χ^2 = 25997.821, p<.05, KMO=0.938) โดยพบว่าค่าสถิติ Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) เท่ากับ 0.938 แสดงว่า ค่าความสัมพันธ์ของตัวแปรมีความเหมาะสมในการวิเคราะห์องค์ประกอบดี (Hair et al., 1998) ค่า Bartlett's Test of Sphericity เท่ากับ χ^2 = 25997.821 และค่าพิสัยของค่าความเพียงพอของการเลือกตัวอย่าง (MSA) มีค่าระหว่าง 0.850 ถึง 0.988 ซึ่งมากกว่า .50 ทุกค่า แสดงว่าข้อมูลชุดนี้มีความสัมพันธ์เพียงพอ และมีนัยสำคัญทางสถิติที่ระดับ .05 แสดงว่า ยอมรับสมมติฐาน H_1 นั้นคือ ตัวแปรต่าง ๆ มีความสัมพันธ์กัน และสามารถนำมาใช้วิเคราะห์องค์ประกอบได้

นอกจากนี้ได้มีการตรวจสอบความเหมาะสมของข้อมูลค่าความร่วมกัน (Communalities) ซึ่งเป็นค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรหนึ่งกับตัวแปรอื่น ๆ ที่เหลือทั้งหมดคำนวณจากผลบวกกำลังสองของน้ำหนักองค์ประองประกอบของตัวแปรตัวหนึ่ง ๆ ในทุกองค์ประกอบ มีค่าอยู่ระหว่าง 0 ถึง 1 ถ้าค่าความร่วมกันเป็น 0 แสดงว่าองค์ประกอบร่วม (Common Factor) ไม่สามารถอธิบายความผันแปรของตัวแปรได้ (ยุทธ ไกยวรรณ์, 2555) รายละเอียดดังตารางที่ 4.8

ตารางที่ 4.8 ค่าความร่วมมือกัน (Communalities)

Item	Initial	Extraction
Item1	1.000	.680
Item2	1.000	.685
Item3	1.000	.660
Item4	1.000	.793
Item5	1.000	.763
Item6	1.000	.763
Item7	1.000	.753
Item8	1.000	.761
Item9	1.000	.659
Item10	1.000	.781
Item11	1.000	.763
Item12	1.000	.766
Item13	1.000	.757
Item14	1.000	.756
Item15	1.000	.827
Item16	1.000	.859
Item17	1.000	.801
Item18	1.000	.858
Item19	1.000	.774
Item20	1.000	.778
Item21	1.000	.805
Item22	1.000	.814
Item23	1.000	.796
Item24	1.000	.798
Item25	1.000	.778
Item26	1.000	.776
Item27	1.000	.943
Item28	1.000	.910
Item29	1.000	.935

ตารางที่ 4.8 (ต่อ)

Item	Initial	Extraction
Item30	1.000	.934
Item31	1.000	.941
Item32	1.000	.935
Item33	1.000	.750
Item34	1.000	.928
Item35	1.000	.732

Extraction Method: Principal Component Analysis

จากตารางที่ 4.8 ผลการวิเคราะห์ค่าความร่วมกันโดยการวิเคราะห์ค่าความร่วมกันด้วยโปรแกรมสำเร็จรูปซึ่งใช้วิธีองค์ประกอบหลัก (Principal Component Analysis) พบว่า ค่า Initial Communalities ทุกตัวมีค่าเป็น1 และคำนวณค่าความร่วมกันหลังสกัดปัจจัย Extraction Communalities โดยมีค่าระหว่าง .660 ถึง .943 สำหรับการวิจัยทางสังคมศาสตร์ยอมรับค่าความร่วมกันที่มีค่ามากกว่า 0.4 ขึ้นไป (Preuss, 2014) แสดงว่าองค์ประกอบสามารถอธิบายความผันแปรของตัวแปรในการศึกษา

4.2.2 ผลการวิเคราะห์องค์ประกอบ

สำหรับผลการวิเคราะห์องค์กอบโดยพิจารณาจากค่า Total Variance Explained ซึ่งเป็นค่าสถิติของแต่ละองค์ประกอบทั้งก่อนและหลังการสกัดปัจจัย ด้วยวิธีการวิเคราะห์องค์ประกอบหลัก ประกอบด้วย 1) จำนวนองค์ประกอบ (Component) 2) ค่าไอเก้น (Eigenvalue) ซึ่งเป็นค่าความผันแปรในองค์ประกอบหนึ่งที่อธิบายได้ด้วยค่าตัวแปรทุกตัวในองค์ประกอบเดียวกัน คำนวณจากผลบวกกำลังสองของค่าน้ำหนักองค์ประกอบ 3) ค่าร้อยละของความแปรปรวน (Percentage of Variance) และ 4) ค่าร้อยละสะสมของความแปรปรวน (Accumulative Percentage of Variance) ดังตารางที่ 4.9

ตารางที่ 4.9 แสดงค่า Total Variance Explained

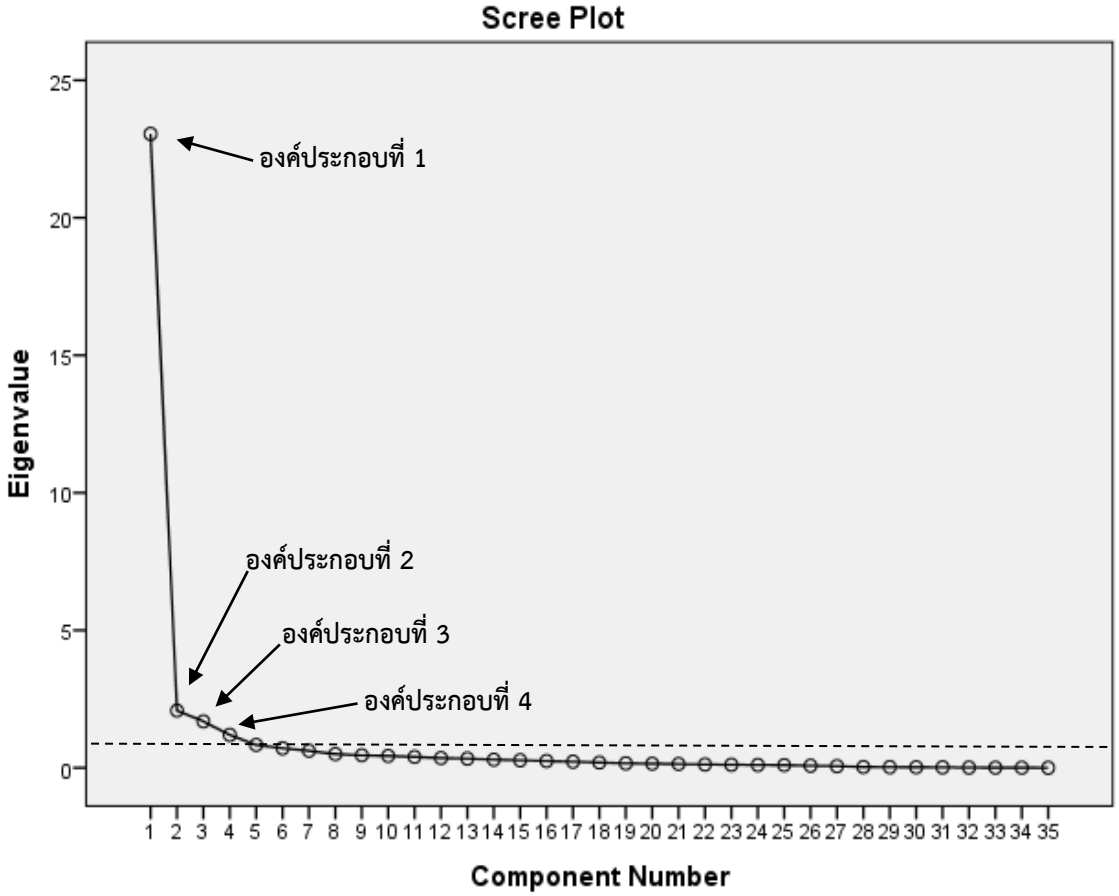
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	23.048	65.851	65.851	23.048	65.851	65.851	8.998	25.708	25.708
2	2.079	5.940	71.791	2.079	5.940	71.791	7.881	22.517	48.225
3	1.688	4.824	76.614	1.688	4.824	76.614	6.076	17.361	65.586
4	1.197	3.419	80.033	1.197	3.419	80.033	5.056	14.447	80.033
5	.831								
6	.710								
7	.617								
8	.498								
9	.454								
10	.434								
11	.397								
12	.354								
13	.332								
14	.298								
15	.274								
16	.248								
17	.223								
18	.192								
19	.162								
20	.150								
:	:	:	:	:	:	:	:	:	:
35	.001	.003	100						

Extraction Method: Principal Component Analysis

*ค่า Eigen (Root) ที่ 21-34 มีค่าสถิติต่าง ๆ น้อยลงตามลำดับ ในที่นี้ย่อส่วนไว้ เนื่องจากเป็นองค์ประกอบที่ไม่สำคัญต่อการพิจารณา

จากตารางที่ 4.9 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ สกัดตัวแปรออกเป็น 4 องค์ประกอบ มีค่าความแปรปรวนของตัวแปร (Initial Eigenvalues) มากกว่า 1 ทุกองค์ประกอบ ค่าร้อยละของความแปรปรวนองค์ประกอบที่ 1 เท่ากับร้อยละ 65.85 องค์ประกอบที่ 2 เท่ากับร้อยละ 5.94 องค์ประกอบที่ 3 เท่ากับร้อยละ 4.82 และองค์ประกอบที่ 4 เท่ากับร้อยละ 3.42 โดยมีค่าร้อยละสะสมของความแปรปรวน (Cumulative of Variance) เท่ากับร้อยละ 80.03 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ นำเสนอใน

รูปแบบกราฟ Scree plot แสดงความสัมพันธ์ระหว่างค่าความแปรปรวนขององค์ประกอบและจำนวนองค์ประกอบที่สกัดได้ โดยแกนแนวตั้งแสดงค่าความแปรปรวนขององค์ประกอบและแกนแนวนอนแสดงจำนวนองค์ประกอบ ดังภาพที่ 4.1



ภาพที่ 4.1 กราฟแสดงค่า Eigenvalues ขององค์ประกอบ (Scree plot)

ภาพที่ 4.1 แสดงความสัมพันธ์ระหว่างค่าความแปรปรวนขององค์ประกอบและจำนวนองค์ประกอบที่สกัดโดยเรียงจากมากไปหาน้อย พิจารณาจำนวนองค์ประกอบจากกราฟที่เริ่มขนานกับแกนนอน พบว่า เริ่มจากองค์ประกอบที่ 1 ดังนั้น จำนวนองค์ประกอบสูงสุด คือ 4 องค์ประกอบที่มีค่าไอเก้นมากกว่า 1 โดยค่าสูงสุดคือ 23.048 และค่าต่ำสุดคือ 1.197

ดังนั้น ผลการวิเคราะห์องค์ประกอบของค่าน้ำหนักองค์ประกอบ (Factor Loading) ซึ่งเป็นค่าความสัมพันธ์ระหว่างตัวแปรสังเกตได้กับองค์ประกอบ โดยผลการวิเคราะห์ค่าน้ำหนักองค์ประกอบในการวิจัยครั้งนี้ นำเสนอดังตารางที่ 4.10

ตารางที่ 4.10 ค่าน้ำหนักองค์ประกอบและชื่อองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ตัวแปรสังเกตได้	น้ำหนักองค์ประกอบ	ชื่อองค์ประกอบ
Item8: มีการจัดทำทะเบียน รับ – คืนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ	.770	การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Supervision and Management of Information Security)
Item7: มีการเก็บบันทึก และจำแนกประเภทของบัญชีทรัพย์สิน ข้อมูลสารสนเทศ เพื่อกำหนดระดับของการป้องกันทรัพย์สินด้านสารสนเทศ	.756	
Item2: มีการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานให้มีความรวดเร็ว ข้อมูลมีความถูกต้องครบถ้วนและเป็นปัจจุบัน เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้	.690	
Item4: มีการจัดทำข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่อนุญาตให้บุคคลหรือหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน	.682	
Item3: มีการมอบหมายภารกิจด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้กับผู้ปฏิบัติงานได้อย่างชัดเจน	.680	
Item1: มีการกำหนดกรอบการดำเนินงานด้านการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เช่น การบำรุงรักษาระบบเครื่องมือเทคโนโลยีสารสนเทศ อุปกรณ์การเข้าใช้งานระบบสารสนเทศ เป็นต้น ให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง	.672	
Item5: มีมาตรการด้านความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์พกพา เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว	.650	
Item10: มีการจัดทำบันทึกข้อตกลงให้ผู้ปฏิบัติงานต้องรักษาทรัพย์สินให้ปลอดภัย และข้อมูลที่เป็นความลับ	.643	
Item14: มีการป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ และเป้าหมายของงานที่รับผิดชอบ	.609	
Item13: มีมาตรการป้องกันภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิดการก่อจลาจล เป็นต้น เพื่อป้องกันไม่ให้ทรัพย์สินสารสนเทศเสียหาย	.608	

ตารางที่ 4.10 (ต่อ)

ตัวแปรสังเกตได้	น้ำหนักองค์ประกอบ	ชื่อองค์ประกอบ
Item12: มีขั้นตอน หรือแผนรองรับในการบริหารจัดการเหตุการณ์ผิดปกติ และปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ พร้อมทั่งช่องทางการรายงานเหตุการณ์ปัญหาที่พบผิดปกติที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที	.591	การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Supervision and Management of Information Security)
Item11: มีการรวบรวมข้อมูล ตรวจสอบ และประเมินผลการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศ ตามแนวทางการควบคุมภายในด้านการใช้งานระบบสารสนเทศของหน่วยงาน เพื่อระบุข้อบกพร่องในการใช้งานระบบ และนำมาปรับปรุงให้สามารถทำงานได้อย่างมีประสิทธิภาพ	.575	
Item6: มีการกำหนดข้อปฏิบัติในการใช้คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ เช่น เครื่องคอมพิวเตอร์แบบพกพา สมาร์ทโฟน เป็นต้น เพื่อให้มีความมั่นคงปลอดภัย และ เกิดประสิทธิภาพต่อการใช้งาน	.573	
Item9: มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ	.514	
ค่า Eigen	**23.048**	
ค่าร้อยละของความแปรปรวน	**65.851**	

ตารางที่ 4.10 (ต่อ)

ตัวแปรสังเกตได้	น้ำหนักองค์ประกอบ	ชื่อองค์ประกอบ
Item22: มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ หรือธุรกรรมออนไลน์กับบุคคลหรือหน่วยงานภายนอก (เช่น การสั่งซื้อ/ขายสินค้าหรือบริการผ่านระบบอิเล็กทรอนิกส์ การชำระเงินผ่านระบบอิเล็กทรอนิกส์) เป็นต้น	.795	การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Operation and Maintenance of Information Security Management)
Item21: มีการจ้างผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจในการร่วมพัฒนา มีการคำนึงถึงความต่อเนื่องในการดำเนินธุรกิจ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และการยกเลิกหรือสิ้นสุดสัญญา (Exit Strategy)	.789	
Item19: มีการดูแล ควบคุม ติดตามตรวจสอบการพัฒนาระบบสารสนเทศ โดยหน่วยงานภายนอก รวมถึงการจ้างช่วงพัฒนาระบบ	.733	
Item18: มีการจัดทำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไว้ในเงื่อนไขการจ้างพัฒนาหรือปรับปรุงระบบ เช่น เอกสารรายละเอียดคุณสมบัติทางเทคนิค ในการจัดซื้อจัดจ้างโดยครอบคลุมถึงเรื่องรักษาความมั่นคงปลอดภัย	.731	

ตารางที่ 4.10 (ต่อ)

ตัวแปรสังเกตได้	น้ำหนักองค์ประกอบ	ชื่อองค์ประกอบ
Item16: มีการกำหนดขั้นตอน ควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์	.730	การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Operation and Maintenance of Information Security Management Systems)
Item20: มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงาน ต้องปฏิบัติตามสัญญาหรือข้อตกลงในการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการและระดับการให้บริการ	.714	
Item24: มีการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงาน สอดคล้องกับชั้นความลับของสารสนเทศ	.709	
Item23: มีการกำหนดให้มีการเข้าใช้งานระบบสารสนเทศตามมาตรการเข้ารหัสข้อมูล (Cryptography) และการบริหารจัดการกุญแจ (Access Key) เป็นต้น	.705	
Item15: มีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก	.641	
Item17: มีการรักษาความมั่งคงของแม่ข่าย (Server) และอุปกรณ์ที่ใช้งานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่พึงประสงค์ดี (Malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหล ของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต	.632	
ค่า Eigen	**2.079**	
ค่าร้อยละของความแปรปรวน	**5.940**	

ตารางที่ 4.10 (ต่อ)

ตัวแปรสังเกตได้	น้ำหนักองค์ประกอบ	ชื่อองค์ประกอบ
Item29: มีการกำหนดให้เจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงาน เมื่อสิ้นสุดการจ้างงาน	.799	การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ (Development and Business Continuity Management of Information Security)
Item30: มีการพัฒนา อบรม เพิ่มพูน ทักษะและความสามารถของผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	.793	
Item27: มีการกำหนดให้ผู้ปฏิบัติงานหรือบุคคลภายนอกที่หน่วยงานว่าจ้างจะต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย และบทลงโทษ ในกรณีที่ผู้ปฏิบัติงานฝ่าฝืนนโยบายหรือระเบียบที่หน่วยงานประกาศใช้อย่างชัดเจน	.786	
Item28: มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน	.701	
Item26: มีการจัดทำ และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบต่าง ๆ เพื่อให้ผู้ปฏิบัติงานสามารถนำไปปฏิบัติได้อย่างถูกต้องและปลอดภัย	.698	
Item25: มีการบำรุงรักษาและดูแลอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน	.600	
ค่า Eigen	**1.688**	
ค่าร้อยละของความแปรปรวน	**4.824**	

ตารางที่ 4.10 (ต่อ)

ตัวแปรสังเกตได้	น้ำหนักองค์ประกอบ	ชื่อองค์ประกอบ
Item34: มีการจัดการความเสี่ยง (Risk Treatment) กำหนดแนวทาง ติดตาม ทบทวน และประเมินความเสี่ยงที่เกิดขึ้นด้านสารสนเทศ เช่น ด้านข้อมูล ด้านอุปกรณ์เทคโนโลยีสารสนเทศ ด้านซอฟแวร์คอมพิวเตอร์ เป็นต้น อย่างสม่ำเสมอ	.909	นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ (Strategic Policy and Management of Information Security)
Item32: มีการกำหนดนโยบายและแนวทางสำหรับความมั่นคงปลอดภัยด้านสารสนเทศเพื่อควบคุม และป้องกันความเสี่ยงด้านสารสนเทศเป็นลายลักษณ์อักษร และประกาศหรือแจ้งนโยบายดังกล่าวให้ผู้ปฏิบัติงานรับทราบทั่วกัน	.903	
Item31: มีการกำหนดกลยุทธ์เพื่อการบริหารงานของหน่วยงาน โดยการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินงานสอดคล้องกับนโยบาย บทบาท ภารกิจของหน่วยงาน และระบบความมั่นคงปลอดภัยด้านสารสนเทศ	.895	
Item33: มีการวิเคราะห์ความเสี่ยง (Risk analysis) และประเมินค่าความเสี่ยง (Risk Evaluation) เพื่อประเมินระดับผลกระทบและโอกาสเกิดเหตุการณ์ และจัดลำดับความเสี่ยงในการจัดการด้านสารสนเทศของหน่วยงาน	.558	
Item35: มีการรายงานผลการบริหารความเสี่ยงด้านสารสนเทศ และแนวโน้มของความเสี่ยงที่อาจจะเกิดขึ้นตามนโยบายที่กำหนดให้ท่านทราบ อยู่ในระดับใดอิเล็กทรอนิกส์ การชำระเงินผ่านระบบอิเล็กทรอนิกส์)	.529	
ค่า Eigen	**1.197**	
ค่าร้อยละของความแปรปรวน	**3.419**	

Extraction Method: Principal Component Analysis

Rotation Method: Varimax with Kaiser Normalization.[a]a. Rotation converged in 7 iterations

จากตารางที่ 4.10 ผลการศึกษาและตั้งชื่อองค์ประกอบของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ผลการสกัดปัจจัยร่วมด้วยวิธีวิเคราะห์แกนหลัก (Principal Component Analysis) และการหมุนแกนทำมุมฉากด้วยวิธี Varimax เพื่อสืบค้นเมื่อหาความหมายโครงสร้างแฝงเร้นของชุดตัวแปร (หรือข้อความ) ตัวบ่งชี้ของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลที่อยู่เบื้องหลังทั้ง 4 องค์ประกอบ ในการพิจารณาว่าตัวแปรใดควรอยู่ในองค์ประกอบใดนั้นจะพิจารณาจากค่าน้ำหนักขององค์ประกอบ (Factor loading) ถ้าค่าน้ำหนักขององค์ประกอบใดมีค่ามากจะจัดตัวแปรให้อยู่ในองค์ประกอบนั้น การวิเคราะห์ข้อมูลครั้งนี้พิจารณาค่าน้ำหนักขององค์ประกอบที่มีค่า 0.3 ขึ้นไปทุกตัวแปรสังเกต และจำนวนกลุ่มตัวอย่างในการวิจัยครั้งนี้มีจำนวน 400 คน ซึ่งมากกว่า 350 คน และจำนวนตัวแปรที่ร่วมกันชี้วัดค่าความแปรปรวนของแต่ละองค์ประกอบตั้งแต่ 3 ตัวขึ้นไป (Hair et al., 2006) ดังนั้น แสดงว่าตัวแปรสังเกตได้ทุกตัวในการวิจัยครั้งนี้ สามารถนำไปวิเคราะห์องค์ประกอบ อย่างไรก็ตามถ้าข้อความบ่งชี้องค์ประกอบไม่เด่นชัด เนื่องจากถ่วงน้ำหนักมากกว่าหนึ่งองค์ประกอบ (cross-loading or secondary loading) ผู้วิจัยพิจารณาตัดทิ้ง สำหรับการกำหนดชื่อองค์ประกอบจากกลุ่มตัวแปรในแต่ละองค์ประกอบ ซึ่งผู้วิจัยได้พิจารณาตั้งชื่อองค์ประกอบให้ครอบคลุมตัวแปรต่าง ๆ ที่อยู่ในองค์ประกอบเดียวกัน และสรุปผลการวิเคราะห์องค์ประกอบเชิงสำรวจ จากจำนวนองค์ประกอบ 4 องค์ประกอบ มีดังนี้

องค์ประกอบที่ 1 สามารถอธิบายด้วยตัวแปรสังเกตได้ จำนวน 6 ตัวแปรหลัก จากข้อคำถาม 14 ข้อ ได้แก่ Item8, Item7, Item2, Item4, Item3, Item1, Item5, Item10, Item14, Item13, Item12, Item11, Item6 และ Item9 ซึ่งมีพิสัยของค่าน้ำหนักองค์ประกอบระหว่าง 0.514 ถึง 0.770 มีค่า Eigen เท่ากับ 23.048 และมีค่าค่าร้อยละของความแปรปรวน เท่ากับ 65.851 โดยข้อความเกี่ยวข้องกับ การกำกับดูแล (Governance) โครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ การบริหารจัดการทรัพย์สิน การติดตามวัดผลและการประเมินผล การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย และความสอดคล้องที่เกี่ยวข้องกับกฎหมายและการป้องกันในขั้นตอนต่าง ๆ จึงตั้งชื่อองค์ประกอบนี้ว่า การกำกับดูแล การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Supervision and Management of Information Security)

องค์ประกอบที่ 2 สามารถอธิบายด้วยตัวแปรสังเกตได้ จำนวน 5 ตัวแปรหลัก จากข้อคำถามจำนวน 10 ข้อ ได้แก่ Item22, Item21, Item19, Item18, Item16, Item20, Item24, Item23, Item15 และItem17 ซึ่งมีพิสัยของค่าน้ำหนักองค์ประกอบระหว่าง 0.632 ถึง 0.795 มีค่า Eigen เท่ากับ 2.369 และมีค่าค่าร้อยละของความแปรปรวน เท่ากับ 5.924 โดยข้อความเกี่ยวข้องกับการควบคุมการเข้าถึง ความมั่นคงปลอดภัยทางด้านกายภาพ สภาพแวดล้อม การดำเนินงาน และการสื่อสารข้อมูล การจัดหา การพัฒนา และการบำรุงรักษาระบบความสัมพันธ์กับผู้ให้บริการภายนอก และการเข้ารหัสข้อมูลจึงตั้งชื่อองค์ประกอบนี้ว่า การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Operation and Maintenance of Information Security Management)

องค์ประกอบที่ 3 สามารถอธิบายด้วยตัวแปรสังเกตได้ จำนวน 2 ตัวแปรหลัก จากข้อคำถามจำนวน 6 ข้อ ได้แก่ Item29, Item30, Item27, Item28, Item26 และItem25 ซึ่งมีพิสัยของค่าน้ำหนัก

องค์ประกอบระหว่าง 0.533 ถึง 0.698 มีค่า Eigen เท่ากับ 1.688 และมีค่าค่าร้อยละของความแปรปรวนเท่ากับ 4.824 โดยข้อความเกี่ยวข้องกับ ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ และการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร จึงตั้งชื่อองค์ประกอบนี้ว่า การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ (Development and Business Continuity Management of Information Security)

องค์ประกอบที่ 4 สามารถอธิบายด้วยตัวแปรสังเกตได้ จำนวน 2 ตัวแปรหลัก จากข้อคำถาม 5 ข้อ ได้แก่ Item34, Item32, Item31, Item33 และ Item35 ซึ่งมีพิสัยของค่าน้ำหนักองค์ประกอบระหว่าง 0.529 ถึง 0.909 มีค่า Eigen เท่ากับ 1.197 และมีค่าค่าร้อยละของความแปรปรวน เท่ากับ 3.419 โดยข้อความเกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และการบริหารจัดการกลยุทธ์ความมั่นคงปลอดภัยสารสนเทศ จึงตั้งชื่อองค์ประกอบนี้ว่า นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ (Strategic Policy and Management of Information Security)

เมื่อพิจารณาถึงมีความสัมพันธ์ระหว่างองค์ประกอบของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล พบว่า ทุกองค์ประกอบมีความสัมพันธ์กันอยู่ในทางบวกและมีระดับสัมพันธ์สูง โดยค่าสหสัมพันธ์ระหว่างองค์ประกอบที่ 1 กับองค์ประกอบที่ 3 อยู่ในระดับสูง (r=.853) รองลงมาระหว่างองค์ประกอบที่ 1 กับองค์ประกอบที่ 2 (r=.846) และระหว่างองค์ประกอบที่ 2 กับองค์ประกอบที่ 3 (r=.764) รายละเอียดดังตาราง 4.11

ตารางที่ 4.11 ความสัมพันธ์ระหว่างองค์ประกอบของการบริหารจัดการความมั่นคงปลอดภัย ด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

องค์ประกอบที่	1	2	3	4
1	1.000			
2	.846	1.000		
3	.853	.764	1.000	
4	.719	.647	.674	1.000

นอกจากนี้ผู้วิจัยได้ดำเนินการจัดกลุ่มตัวแปรสังเกตได้ (Grouping) ในแต่ละองค์ประกอบได้ผลการจัดกลุ่มตัวแปรดังนี้

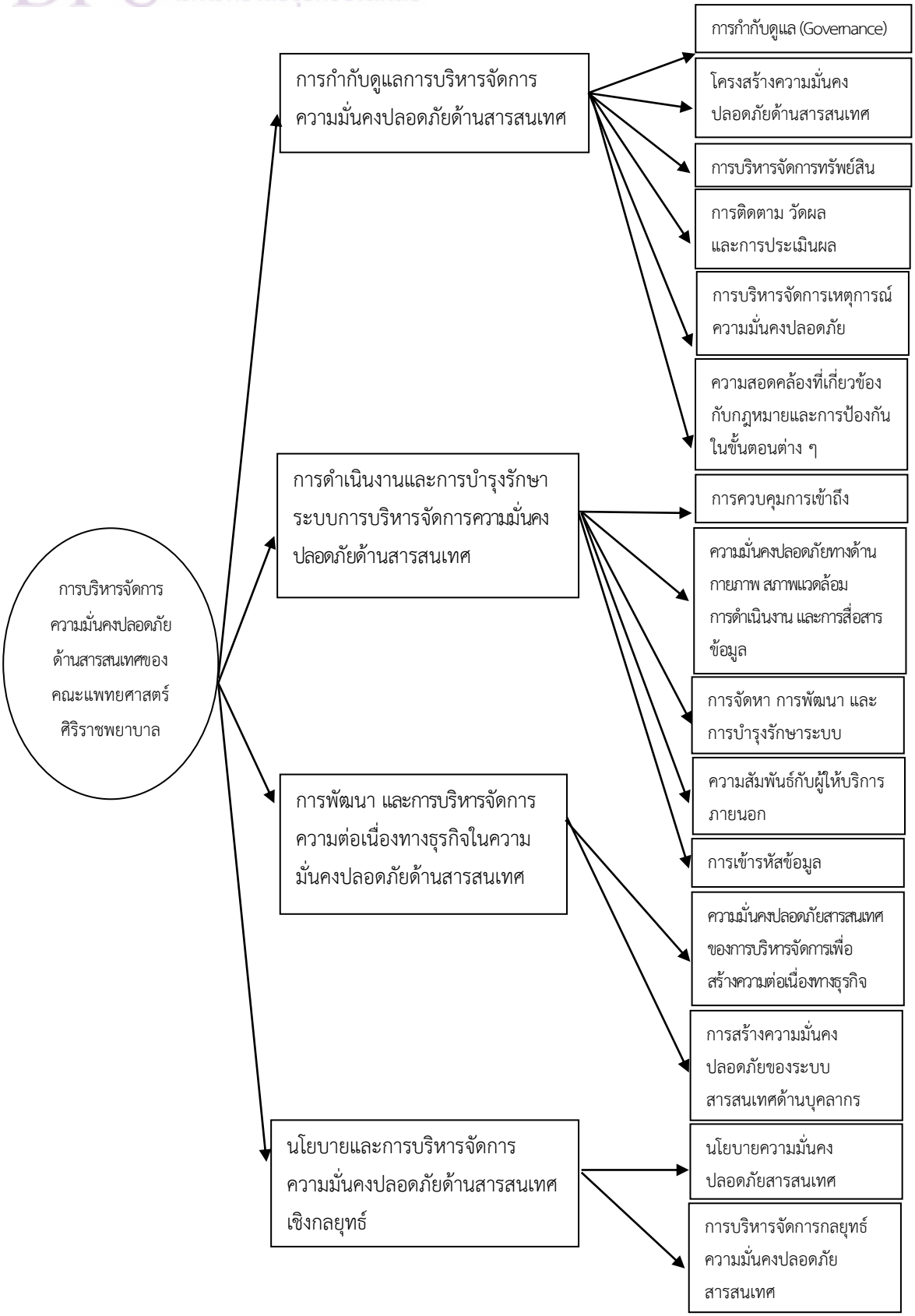
องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วยชุดตัวแปรสังเกตได้ที่บ่งชี้ถึง การกำกับดูแล (Governance) (Item1, 2) โครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Item3, 4, 5) การบริหารจัดการทรัพย์สิน (Item6, 7, 8, 9, 10) การติดตาม วัดผล และการประเมินผล (Item11) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Item12, 13) และความสอดคล้องที่เกี่ยวข้องกับกฎหมาย การป้องกัน และการทบทวนขั้นตอนต่าง ๆ (Item14)

องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วยชุดตัวแปรสังเกตได้ที่บ่งชี้ถึง การควบคุมการเข้าถึง (Item15) ความมั่นคงปลอดภัยทางด้านกายภาพสภาพแวดล้อม การดำเนินงาน และการสื่อสารข้อมูล (Item16, 17) การจัดหาการพัฒนา และการบำรุงรักษาระบบ (item18) ความสัมพันธ์กับผู้ให้บริการภายนอก (Item19, 20, 21, 22) การเข้ารหัสข้อมูล (Item23, 24)

องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วยชุดตัวแปรสังเกตได้ที่บ่งชี้ถึง ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Item25, 26) และการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Item27, 28, 29, 30)

องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ ประกอบด้วยชุดตัวแปรสังเกตได้ที่บ่งชี้ถึง การบริหารจัดการกลยุทธ์ความมั่นคงปลอดภัยสารสนเทศ (Item31) นโยบายความมั่นคงปลอดภัยสารสนเทศ (Item32, 33, 34, 35)

จากการสืบค้นหาองค์ประกอบจากเอกสารงานวิจัยที่เกี่ยวข้อง แล้วดำเนินการวิเคราะห์องค์ประกอบ ซึ่งผู้วิจัยสามารถเขียนเป็นโมเดลการวัดการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ได้ดังภาพที่ 4.2



ภาพที่ 4.2 โมเดลการวัดการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ของคณะแพทยศาสตร์ศิริราชพยาบาล

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

ผลจากการวิจัยเรื่อง ศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยมีวัตถุประสงค์ในการทำวิจัยนี้ เพื่อศึกษาถึงองค์ประกอบของการบริหารความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ซึ่งผู้วิจัยสามารถสรุปผลการศึกษา และข้อเสนอแนะได้ดังนี้

5.1 สรุปผลการวิจัย

งานวิจัยนี้ผู้วิจัยได้ทำการรวบรวมข้อมูลโดยการแจกแบบสอบถามให้กับบุคลากรของแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล ซึ่งผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลกับบุคลากร ของแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาล โดยทำการศึกษาด้านภาพรวมของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล และองค์ประกอบด้านการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศจากแนวคิด ทฤษฎี ผลงานวิจัยและเอกสารต่าง ๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ ร่วมกับผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ เพื่อวิเคราะห์ข้อมูลเกี่ยวกับความคิดเห็นขององค์ประกอบกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของบุคลากรของแผนกต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาลแบ่งออกเป็น 4 องค์ประกอบ ได้แก่ ด้านที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ด้านที่ 2 การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ด้านที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ และด้านที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ ซึ่งเป็นการศึกษาองค์ประกอบที่มีความสำคัญต่อการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในหน่วยงาน

ผู้วิจัยได้ทำการเก็บข้อมูล โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บข้อมูล แบ่งออกเป็น 3 ส่วน คือ ส่วนที่ 1 ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม ส่วนที่ 2 กระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล และส่วนที่ 3 ข้อเสนอแนะ จำนวน 400 ชุด ด้วยวิธีการในรูปแบบออนไลน์ และได้รับแบบสอบถามกลับคืนมาครั้งที่ 1 จำนวน 255 ชุด คิดเป็นร้อยละ 63.75 ของจำนวนแบบสอบถามทั้งหมด และครั้งที่ 2 จำนวน 145 ชุด คิดเป็นร้อยละ 36.25 ของจำนวนแบบสอบถามทั้งหมด จากนั้นผู้วิจัยได้ทำการวิเคราะห์ข้อมูล และประมวลผลโดยใช้โปรแกรม Microsoft Excel และโปรแกรมสำเร็จรูปทางสถิติ (SPSS) ซึ่งการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถามทางสถิติเชิงพรรณนา โดยข้อมูลทั่วไปที่ใช้ในการวิเคราะห์ คือ เพศ อายุ ระดับการศึกษา ตำแหน่ง หน่วยงานที่ปฏิบัติงาน ประสบการณ์ทำงาน และระบบเทคโนโลยีสารสนเทศที่ใช้ปัจจุบัน และการวิเคราะห์องค์ประกอบโดยใช้วิธี Factor Analysis แบบ

การสกัดปัจจัยวิธีองค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) สามารถสรุปผลการวิเคราะห์ข้อมูลดังนี้

5.1.1 ผลการศึกษาข้อมูลทั่วไป และความคิดเห็นเกี่ยวกับองค์ประกอบกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลของผู้ตอบแบบสอบถามจากสถิติเชิงพรรณนา

ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง คิดเป็นร้อยละ 74.20 อายุอยู่ระหว่าง 31 – 40 ปี คิดเป็นร้อยละ 38.50 ระดับการศึกษาระดับปริญญาตรี คิดเป็นร้อยละ 38.50 ตำแหน่งเจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป คิดเป็นร้อยละ 42.80 ประสบการณ์ทำงานอยู่ระหว่าง 1 – 5 ปี คิดเป็นร้อยละ 32.00 และใช้ระบบเทคโนโลยีสารสนเทศประเภทระบบสารสนเทศเพื่อการจัดการ คิดเป็นร้อยละ 42.41

ความคิดเห็นเฉลี่ยของผู้ตอบแบบสอบถามโดยภาพรวมขององค์ประกอบกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลอยู่ในระดับมาก และผลการพิจารณารายข้อ พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมากทุกข้อ โดยความคิดเห็นเฉลี่ยค่าสูงที่สุด คือ ด้านการกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับมาก

5.1.2 สรุปผลการศึกษาองค์ประกอบกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ผลจากการศึกษาองค์ประกอบกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยการวิเคราะห์แบบ Factor Analysis และวิธีหมุนแกนสกัดปัจจัยแบบ Varimax เพื่อหาค่า Factor Loading ของตัวแปรแต่ละตัว ผู้วิจัยสามารถสรุปองค์ประกอบที่มีความสำคัญมากที่สุดไปยังความสำคัญน้อยที่สุด และแต่ละองค์ประกอบการศึกษานี้ มีตัวแปรในการศึกษา ดังนี้

องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย ชุดตัวแปรสังเกตได้ (Observed Variables) ดังนี้

1.1 การกำกับดูแล (Governance) (Item1, 2)

1.2 โครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Item3, 4, 5)

1.3 การบริหารจัดการทรัพย์สิน (Item6, 7, 8, 9, 10)

1.4 การติดตาม วัดผล และการประเมินผล (Item11)

1.5 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Item12, 13)

1.6 ความสอดคล้องที่เกี่ยวข้องกับกฎหมาย การป้องกัน และการทบทวนขั้นตอนต่าง ๆ (Item14)

องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วยชุดตัวแปรสังเกตได้ (Observed Variables) ดังนี้

2.1 การควบคุมการเข้าถึง (Item15)

2.2 ความมั่นคงปลอดภัยทางด้านกายภาพสภาพแวดล้อม การดำเนินงาน และการสื่อสารข้อมูล (Item16, 17)

2.3 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (item18)

2.4 ความสัมพันธ์กับผู้ให้บริการภายนอก (Item19, 20, 21, 22) การเข้ารหัสข้อมูล (Item23, 24)

องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วยชุดตัวแปรสังเกตได้ (Observed Variables) ดังนี้

3.1 ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Item25, 26)

3.2 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Item27, 28, 29, 30)

องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ ประกอบด้วยชุดตัวแปรสังเกตได้ (Observed Variables) ดังนี้

4.1 การบริหารจัดการกลยุทธ์ความมั่นคงปลอดภัยสารสนเทศ (Item31)

4.2 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Item32, 33, 34, 35)

5.2 อภิปรายผล

การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ใช้การวิเคราะห์แบบ Factor Analysis แบบการสกัดปัจจัยวิธีองค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ในโปรแกรมสำเร็จรูปทางสถิติ (SPSS) เป็นเครื่องมือในการวิเคราะห์ ซึ่งใช้วิธีการสกัดปัจจัยองค์ประกอบเบื้องต้น (Principal Component Analysis: PCA) และการหมุนแกนสกัดปัจจัยดังกล่าวแบบวิธี Varimax จำนวน 7 รอบเพื่อให้ได้ค่า Factor Loading ของตัวแปรแต่ละตัว ซึ่งแสดงผลการศึกษาองค์ประกอบทั้ง 4 องค์ประกอบ ดังนี้

5.2.1 องค์ประกอบของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลโดยภาพรวม

องค์ประกอบของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลโดยภาพรวม พบว่า ผู้ตอบแบบสอบถามให้ความสำคัญระดับมากมีคะแนนเฉลี่ยเท่ากับ 3.71 และผลการพิจารณารายข้อ พบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นอยู่ในระดับมากทุกข้อ โดยความคิดเห็นเฉลี่ยค่าสูงที่สุด คือ ด้านการกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับมาก ซึ่งสอดคล้องกับงานวิจัย สุวันต์นา เสมอเนตร (2562) ที่ทำการศึกษาเพื่อการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001: 2013 ของศูนย์ปฏิบัติการข้อมูลกลางของกระทรวงศึกษาธิการ (DATA MOPH Center) พบว่า ผู้ใช้บริการ VM (Virtual Machine) และ Web hosting มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก คะแนนเฉลี่ย 3.99 กลุ่มที่ 2 ผู้ให้บริการ (vendor) มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก คะแนนเฉลี่ย 4.17 และกลุ่มที่ 3 ผู้รับบริการทั่วไป มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก คะแนนเฉลี่ย 3.98 เช่นกัน ซึ่งการนำมาตรฐาน ISO/IEC 27001:2013 เข้ามาใช้เพื่อเพิ่มความ

มั่นคงปลอดภัยขององค์กรให้เป็นไปตามมาตรฐานสากล ผลการดำเนินงานประสบผลสำเร็จเป็นอย่างดี และงานวิจัยของชาญชัย ประมูลเฉโก และวศิณ ชูประยูร (2564) ได้ทำการศึกษาความคิดเห็นของกำลังพลกรมการสื่อสารทหาร กองบัญชาการกองทัพไทยเกี่ยวกับกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อพัฒนาแผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร โดยกำลังพลส่วนใหญ่มีความต้องการมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในระดับมากตามกรอบมาตรฐาน ISO/IEC 27001: 2013 เช่นเดียวกับสมมติฐานเกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีความสัมพันธ์ต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศโดยมีขนาดความสัมพันธ์อยู่ระหว่าง 0.491-0.933 และมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศในบริบทปัจจุบัน มีอิทธิพลต่อความต้องการแผนความเสี่ยงเทคโนโลยีสารสนเทศที่ขนาดความสัมพันธ์อยู่ระหว่าง 0.195 – 0.933

เนื่องจาก คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ถูกได้รับการรับรองตามมาตรฐาน ISO/IEC 27001/2013 (Information Security Management System : ISMS) เมื่อปี พ.ศ. 2560 จากผลการดำเนินการเพื่อจัดการความเสี่ยงและโอกาสเกิดขึ้น และมุ่งเน้นการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศควบคู่ไปกับการปฏิบัติงานทั่วไป ซึ่งเป็นการระบุความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของข้อมูล เช่น ความถูกต้อง ความลับ และความพร้อมใช้งานของข้อมูล เป็นต้น และได้มีการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ลงวันที่ 7 เมษายน 2564 ตามระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ลงวันที่ 1 เมษายน 2564 ให้กับบุคลากรในองค์กรได้ยึดถือและปฏิบัติ และตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิสก์กับหน่วยงานของรัฐ หรือ โดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ได้แก่ 1) การเข้าถึงและควบคุมการใช้งานสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล 2) การจัดทำระบบสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินของคณะแพทยศาสตร์ศิริราชพยาบาล 3) การตรวจสอบ และประเมินความเสี่ยงของคณะแพทยศาสตร์ศิริราชพยาบาล 4) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล และให้มีการทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ และแนวปฏิบัติของคณะแพทยศาสตร์ศิริราชพยาบาล

5.2.2 องค์ประกอบของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล จำนวน 4 องค์ประกอบ ดังนี้

การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยการใช้การวิเคราะห์แบบ Factor Analysis ซึ่งใช้วิธีการสกัดปัจจัยองค์ประกอบเบื้องต้น (Principal Component Analysis: PCA) และการหมุนแกนสกัดปัจจัยดังกล่าวแบบวิธี Varimax จำนวน 7 รอบ เพื่อให้ได้ค่า Factor Loading ของตัวแปรแต่ละตัว ซึ่งแสดงผลการศึกษาองค์ประกอบทั้ง 4 องค์ประกอบ ได้แก่ 1) การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ 2) การดำเนินงาน และการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้าน

สารสนเทศ 3) การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ และ 4) นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ โดยตัวแปรที่ผู้ตอบแบบสอบถามให้ความสำคัญมากที่สุดคือ การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งเป็นประเด็นหลักสำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งสอดคล้องกับงานวิจัยของนักวิชาการต่างประเทศ ที่ได้ทำการศึกษา Information Security Governance Framework ผลจากการศึกษาทำให้ได้ Information Security Governance Model ใหม่ซึ่งเป็นโมเดลสำหรับการบริหารจัดการความมั่นคงปลอดภัยภายในองค์กร ประกอบไปด้วยกระบวนการ Direct, Monitor, Evaluate, Oversee และ Report และผลการศึกษาเรื่อง A New Perspective to Information Security: Total Quality Information Security Management งานวิจัยนี้ได้นำเสนอแนวคิดใหม่ในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยการออกแบบการพัฒนาและการสร้างแบบจำลอง TQISM เพื่อการรักษาความมั่นคงสารสนเทศ และสินทรัพย์ขององค์กร TQISM เป็นการรวมของการรักษาความมั่นคงปลอดภัยสารสนเทศ และการบริหารจัดการโดยที่ผู้บริหารและพนักงานมีส่วนร่วมในการพัฒนาอย่างต่อเนื่อง (Sharbaf, 2014; Ohki et al., 2009) และสอดคล้องกับการงานวิจัยของชาญชัย ประมูลเฉโก และวศิณ ชูประยูร (2564) ได้มีการพัฒนาแผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย ประกอบด้วย 14 แผนย่อย ตามมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ โดยในแต่ละแผนยังได้กำหนดตัวชี้วัดในการดำเนินการ ได้แก่ 1) แผนปฏิบัติการด้านนโยบายความมั่นคงปลอดภัยสารสนเทศ 2) แผนปฏิบัติการด้านโครงสร้างความมั่นคงปลอดภัยสารสนเทศ 3) แผนปฏิบัติการด้านความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล 4) แผนปฏิบัติการด้านการบริหารจัดการทรัพย์สิน 5) แผนปฏิบัติการด้านการควบคุมการเข้าถึง 6) แผนปฏิบัติการด้านการเข้ารหัสข้อมูล 7) แผนปฏิบัติการด้านความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม 8) แผนปฏิบัติการด้านความมั่นคงปลอดภัยสำหรับการดำเนินการ 9) แผนปฏิบัติการด้านความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล 10) แผนปฏิบัติการด้านการจัดหา การพัฒนาและการบำรุงรักษาระบบ 11) แผนปฏิบัติการด้านความสัมพันธ์กับผู้ให้บริการภายนอก 12) แผนปฏิบัติการด้านการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ 13) แผนปฏิบัติการประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ และ 14) แผนปฏิบัติการด้านความสอดคล้อง โดยมีรายละเอียด ดังนี้

องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ จากผลการศึกษา พบว่า ผู้ตอบแบบสอบถามให้ความสำคัญอยู่ในระดับมาก ซึ่งตัวแปรที่ผู้ตอบแบบสอบถามให้ความสำคัญสูงที่สุด คือ มีการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานให้มีความรวดเร็ว ข้อมูลมีความถูกต้องครบถ้วน และเป็นปัจจุบัน เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้อยู่ในระดับมาก โดยเป็นตัวชี้วัดของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ด้านการกำกับดูแล (Governance) ซึ่งสอดคล้องกับผลการศึกษาในอดีตที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศ พบว่า องค์การจะมีการยอมรับในสิ่งใดสิ่งหนึ่งอย่างยั่งยืน โดยเฉพาะการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานนั้น ทัศนคติ นับเป็นสิ่งสำคัญที่จะทำให้เกิดการยอมรับหรือปฏิเสธได้ ดังนั้น หากต้องการให้

องค์การเกิดการริเริ่มที่ทำสิ่งใหม่ ๆ จึงควรสนใจในส่วนของการสร้างทัศคติที่ดีแก่พนักงาน และงานวิจัยหลายงานในอดีตได้มีการระบุว่าการที่บุคคลรับรู้ถึงประโยชน์ที่ได้จะส่งผลโดยตรงต่อทัศนคติ และการที่จะทำให้บุคคลรับรู้ถึงประโยชน์ที่จะได้จากการกำกับดูแลเทคโนโลยีสารสนเทศนั้น การสื่อสารภายในองค์การก็นับเป็นสิ่งที่ช่วยสร้างความเข้าใจในนโยบายของผู้บริหาร และเป็นสิ่งที่เชื่อมความสัมพันธ์ระหว่างบุคคลในองค์การ และเพื่อให้เกิดประสิทธิภาพและประสิทธิผลต่อองค์การในทางบวก เพราะนโยบายการบริหารงานการจัดการขององค์การเป็นส่วนสำคัญ และเพื่อให้การดำเนินงานบรรลุเป้าหมายที่วางไว้ การสื่อสารภายในองค์การ จึงเป็นสิ่งจำเป็นยิ่งสำหรับกิจกรรมและการดำเนินงานต่าง ๆ ที่จะเกิดขึ้นในองค์การ อย่างไรก็ดีประสบการณ์ในอดีตก็นับเป็นอีกหนึ่งสิ่งที่เป็นตัวกระตุ้นให้บุคคลนั้น ๆ เกิดการรับรู้ประโยชน์ (Lee et al., 2008; Pereira et al., 2013; Ngwube, 2013)

ทั้งนี้ งานวิจัยของ Tanner et al. (2015) วิจัยเรื่อง Gaining an Edge in Cyberspace with Advances Situation Awareness พบว่า องค์กรภาคธุรกิจมีการพึ่งพาระบบคอมพิวเตอร์ที่มีนำมาใช้วางระบบต้องเผชิญกับวิกฤตการคุมคามทางไซเบอร์ องค์กรต่าง ๆ มีภารกิจสำคัญในการพัฒนาระบบรักษาความปลอดภัยในโลกไซเบอร์โดยให้แนวคิดการตระหนักรู้ในสถานการณ์ (Situation Awareness: SA) ประยุกต์ใช้ทำให้ต้องมีการวิเคราะห์สถานการณ์ มีการจำลองสถานการณ์ขั้นสูงโดยสร้างเป็นระบบ OODA ได้แก่ 1) สังเกต (Observe) 2) ปรับทิศทาง (Orient) 3) ตัดสินใจ (Decide) และ 4) การลงมือทำ (Act) เพื่อสร้างทำแผนรองรับสถานการณ์ ทำความรู้ความเข้าใจในแบบเรียลไทม์ใกล้เคียงกับสภาพแวดล้อมขององค์กรและภัยคุกคามทางไซเบอร์จะส่งผลกระทบทางธุรกิจ และงานวิจัยของ Thomas (2010) ได้ทำการศึกษาการกำกับดูแลเทคโนโลยีสารสนเทศในธุรกิจขนาดเล็ก และขนาดกลาง โดยพบว่า ธุรกิจจะเลือกที่จะนำการกำกับดูแลเทคโนโลยีสารสนเทศมาใช้นั้น ไม่ใช่เพียงเพราะต้องการทำตามกฎระเบียบที่เกิดขึ้น หากแต่การนำการกำกับดูแลเทคโนโลยีสารสนเทศมาใช้นั้นทำให้องค์การรู้สึกมั่นคงปลอดภัย และความรู้สึกต้องทำให้ถูกต้องต่อสังคมแวดล้อมที่เกี่ยวข้อง ซึ่งงานวิจัยของ Nan et al. (2008) ก็ได้พบว่า การรักษาภาพลักษณ์ขององค์การก็ส่งผลให้องค์การรับรู้ถึงประโยชน์ของการนำเทคโนโลยีสารสนเทศมาใช้ และงานวิจัยของ Jongsureyapart (2006) ที่พบว่าเหตุการณ์วิกฤติทางการเงินในปี 1997 ทำให้หลายองค์การเริ่มยอมรับให้มีการกำกับดูแลกิจการในองค์การของพวกเขา เนื่องจากอยากให้องค์การมีการกำกับดูแลที่ดี เพื่อที่จะไม่ส่งผลให้เกิดเหตุการณ์ซ้ำกับในอดีต เพราะแต่ละเหตุการณ์ไม่ดีที่เกิดขึ้นกับองค์การนั้นย่อมทำให้ภาพลักษณ์และชื่อเสียงขององค์การเสียไปด้วย

องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ จากผลการศึกษา พบว่า ผู้ตอบแบบสอบถามให้ความสำคัญอยู่ในระดับมาก ซึ่งตัวแปรที่ผู้ตอบแบบสอบถามให้ความสำคัญสูงที่สุด คือ มีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอกอยู่ในระดับมาก โดยเป็นตัวชี้วัดของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ด้านการควบคุมการเข้าถึง คณะแพทยศาสตร์ศิริราชพยาบาลมีการป้องกันการเข้าถึงระบบปฏิบัติการ ได้แก่ 1) ต้อง

ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง 2) ต้องควบคุมให้มีการกำหนดสิทธิการใช้งานของผู้ใช้งานตามหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย รวมถึงการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ 3) ต้องดำเนินการฝึกอบรมการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากร 4) ต้องควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าบริการทางเครือข่ายโดยไม่ได้รับอนุญาต 5) ต้องควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และ 6) ต้องควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศโดยไม่ได้รับอนุญาตซึ่งเป็นไปตามรับรองมาตรฐาน ISO/IEC 27001/2013 (Information Security Management System : ISMS) ซึ่งสอดคล้องกับผลการศึกษาของแววตา เตชาทวีวรรณ (2563) ที่พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐมีการกำหนดการเข้าถึงและการควบคุมการใช้งานสารสนเทศ การบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน และการควบคุมการเข้าถึงเครือข่าย โดยการกำหนดสิทธิและระดับของบุคคลทั้งทางกายภาพและทางอิเล็กทรอนิกส์ เนื่องจากระบบสารสนเทศประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล เครือข่าย และบุคคล และการดำเนินธุรกรรมต่าง ผ่านระบบเครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล เครื่องแม่ข่ายระบบเครือข่าย เครื่องแม่ข่ายเว็บไซต์ อุปกรณ์ระบบเครือข่าย เป็นต้น จึงต้องมีการป้องกันการเข้าถึงอุปกรณ์ต่าง ๆ ทางกายภาพโดยอนุญาตเฉพาะผู้ที่เกี่ยวข้องเข้าถึงอุปกรณ์ต่าง ๆ ได้ โดยกำหนดกฎระเบียบ และใช้อุปกรณ์ป้องกันบุคคลอื่นเข้าถึงโดยไม่ได้รับอนุญาต

นอกจากนี้จากการคุกคามทางระบบไซเบอร์ สามารถกระทำได้โดยแฮคเกอร์ (Hacker) ซึ่งกระทำได้หลายรูปแบบ ได้แก่ การขโมยข้อมูล ทำให้ข้อมูลเสียหาย หรือกระบวนการทำงาน โดยใช้ซอฟต์แวร์ เช่น ไวรัสคอมพิวเตอร์ มัลแวร์ (Malware) รันซัมแวร์ (Ransomware) สนิฟเฟอร์ (Sniffer) เป็นต้น ผู้ปฏิบัติงานต้องระมัดระวังเรื่องการใช้ซอฟต์แวร์ คอมพิวเตอร์ และอินเทอร์เน็ต เพื่อเลี่ยงความเสี่ยงที่จะเกิดขึ้น คณะแพทยศาสตร์ศิริราชพยาบาลจึงจำเป็นต้องมีมาตรการป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ชอบดังกล่าว ซึ่งประเด็นที่มีความเสี่ยงสูงต่อการรักษาความปลอดภัยสารสนเทศของหน่วยงาน ได้แก่ การเข้าใช้งานอินเทอร์เน็ต และการใช้ระบบเครือข่ายไร้สายที่ไม่เกี่ยวกับการปฏิบัติงานของพนักงาน การเปลี่ยนหน้าเว็บโดยไม่ได้รับอนุญาต และการเจาะระบบโดยผู้ไม่ประสงค์ดี ซึ่งจากงานวิจัยของ Hou et al. (2020) ที่พบว่าการโจมตีทางเครือข่ายโดยเฉพาะปัจจุบันที่เป็นสังคม IoT: Internet of Things ก่อให้เกิดความเสียหายทั้งการใช้งานเครือข่ายและข้อมูลขององค์กร และ Bertino (2017) ได้เสนอภาพร่างความเสี่ยงด้านความมั่นคงปลอดภัยและความเป็นส่วนใน IoT และความมั่นคงปลอดภัยด้านแอพพลิเคชันโดเมน รวมทั้งเสนอแผนงานด้านความมั่นคงปลอดภัยใน 3 ด้าน ได้แก่ 1) การควบคุมการเข้าถึง เป็นการรักษาความมั่นคงปลอดภัยขั้นพื้นฐาน เมื่อต้องมีการแบ่งปันข้อมูลที่มีความสำคัญกับอุปกรณ์และเครือข่ายอื่น 2) ความมั่นคงปลอดภัยของซอฟต์แวร์และ

เฟริมแวร์ ซอฟต์แวร์เป็นองค์ประกอบสำคัญของ IoT มีการโจมตีหลายครั้งที่ทำให้ซอฟต์แวร์ทำงานผิดพลาด และยังมีการโจมตีโดยอาศัยช่วงการอัพเดทของเฟริมแวร์ด้วย และ 3) ระบบตรวจจับการบุกรุก ที่เหมาะสมกับ IoT จะต้องได้รับการออกแบบมาเพื่อรองรับการกำหนดค่าที่ยืดหยุ่นในระบบ IoT และที่สำคัญคือต้องการตรวจจับการบุกรุกได้โดยที่ไม่ต้องติดตั้งซอฟต์แวร์เพิ่มเติมในอุปกรณ์ IoT และงานวิจัยของ Cox (2012) ที่พบว่า พฤติกรรมไม่ใส่ใจในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้ใช้เป็นสาเหตุหลักของการเกิดความเสี่ยงต่อความปลอดภัยของระบบสารสนเทศ

องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ จากผลการศึกษา พบว่า ผู้ตอบแบบสอบถามให้ความสำคัญอยู่ในระดับมาก ซึ่งตัวแปรที่ผู้ตอบแบบสอบถามให้ความสำคัญสูงที่สุด คือ มีการบำรุงรักษาและดูแลอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน โดยเป็นตัวชี้วัดของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ คณะแพทยศาสตร์ศิริราชพยาบาลมีการจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินของ โดยคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้ใช้งานได้อย่างต่อเนื่องปกติ โดยต้องมีการปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบสารสนเทศ ระบบสำรอง และให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ ตามมาตรฐาน ISO/IEC 27001:2013 และฝ่ายสารสนเทศจึงให้ความสำคัญในเรื่องดังกล่าว โดยการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ตั้งแต่ปี พ.ศ. 2561 เป็นต้นมา และได้มีการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ลงวันที่ 7 เมษายน 2564 ตามระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ลงวันที่ 1 เมษายน 2564 ให้กับบุคลากรในองค์กรได้ยึดถือและปฏิบัติ ซึ่งสอดคล้องกับผลการศึกษาของแววตา เตชาทวีวรรณ (2563) ที่พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐมีการสำรองข้อมูลของระบบสารสนเทศต่าง ๆ มากกว่าหนึ่งวิธี ซึ่งนอกเหนือจากการปฏิบัติตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ ข้อ 2 (2) แล้ว ห้องสมุดจำเป็นต้องสร้างความมั่นคงและปลอดภัยแก่ข้อมูลในระบบสารสนเทศที่เป็นสินทรัพย์ในงานบริการที่สำคัญของห้องสมุด การสำรองข้อมูลในระบบสารสนเทศของทุกห้องสมุดทั้งระบบมือหรือระบบอัตโนมัติมีการกระทำมากกว่า 1 วิธี เพื่อสร้างความมั่นใจและประกันความเสียหาย รวมทั้งมีการทำซ้ำ (Redundancy) ในกรณีที่ระบบใดระบบหนึ่งเกิดความเสียหายก็สามารถใช้อีกระบบแทนได้ นอกจากนี้ห้องสมุดมีการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ ซึ่งเป็นการปฏิบัติตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ข้อ 2 (3) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน...") และเป็นการปฏิบัติตามหลักการ

ประกันคุณภาพของห้องสมุดสถาบันอุดมศึกษา รวมทั้งเป็นหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานที่เกี่ยวข้อง โดยเฉพาะฝ่ายเทคโนโลยีห้องสมุด ซึ่งเป็นมาตรฐานสากลที่ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และสอดคล้องกับงานวิจัยของ Ismail and Zainab (2011) พบว่า การปฏิบัติงานระบบสารสนเทศของหน่วยงานส่วนใหญ่มีความเสี่ยงเรื่องข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์แม่ข่ายสูญหาย ระบบไม่สามารถให้บริการได้ต่อเนื่องนานกว่า 1 ชั่วโมง และโปรแกรมระบบปฏิบัติการไม่สามารถทำงานได้ตามปกติ ดังนั้นหน่วยงานจึงต้องกำหนดการบำรุงรักษาอุปกรณ์ต่าง ๆ ให้อยู่ในสภาพสมบูรณ์ เป็นมาตรการหนึ่งในการเพิ่มประสิทธิภาพการรักษาความมั่นคองปลอดภัยระบบสารสนเทศ ซึ่งห้องสมุดส่วนใหญ่ร้อยละ 95 มีการดำเนินงานรักษาความปลอดภัยของระบบสารสนเทศในด้านเทคนิคอยู่ในระดับดี

องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์

องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์ จากผลการศึกษา พบว่า ผู้ตอบแบบสอบถามให้ความสำคัญอยู่ในระดับมาก ตัวแปรที่ผู้ตอบแบบสอบถามให้ความสำคัญสูงที่สุด การกำหนดกลยุทธ์เพื่อการบริหารงานของหน่วยงาน โดยการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินงาน และสอดคล้องกับนโยบาย บทบาท ภารกิจของหน่วยงาน และระบบความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงมีการกำหนดตัวชี้วัดของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อการขับเคลื่อนการบริหารจัดการกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยขับเคลื่อนการบริหารขององค์กร และการวางแผนออกแบบการปฏิบัติงานโดยนำเทคโนโลยีสารสนเทศเป็นโครงสร้างพื้นฐานที่สำคัญ เพื่อสนับสนุนการทำงานในด้านต่าง ๆ ได้แก่ ด้านการศึกษา ด้านวิชาการ ด้านการวิจัย และด้านการบริการผู้ป่วยต่างก็ใช้เทคโนโลยีสารสนเทศทั้งสิ้น ด้วยเหตุนี้การประเมินความเสี่ยงและการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ดังนั้น การประเมินความเสี่ยงและการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจึงเป็นหัวใจสำคัญของหน่วยงาน ซึ่งรับผิดชอบโดยตรงจากฝ่ายสารสนเทศ ด้วยเหตุนี้ฝ่ายสารสนเทศจึงให้ความสำคัญในเรื่องดังกล่าว และนำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ตั้งแต่ปี พ.ศ. 2561 เป็นต้นมา และได้มีการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ลงวันที่ 7 เมษายน 2564 ตามระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ลงวันที่ 1 เมษายน 2564 ให้กับบุคลากรในองค์กรได้ยึดถือและปฏิบัติ และตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิสก์กับหน่วยงานของรัฐ หรือ โดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ซึ่งสอดคล้องกับผลการศึกษาของ แววตา เตชาทวีวรรณ (2563) พบว่า นโยบายรักษาความมั่นคงระบบสารสนเทศถูกกำหนดอย่างเป็นลายลักษณ์อักษรโดยห้องสมุดหรือสำนักคอมพิวเตอร์ของมหาวิทยาลัยเพื่อให้บุคลากรทุกคนปฏิบัติตาม ซึ่งนโยบายที่เป็นลายลักษณ์อักษรดังกล่าวมีเพียงบางห้องสมุดเท่านั้น เนื่องจากการกำหนดนโยบายดังกล่าวต้องดำเนินการโดยคณะกรรมการของมหาวิทยาลัยและมีอธิการบดีเป็นประธาน

เมื่อร่างนโยบายเสร็จต้องนำเสนอต่อสำนักงาคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อพิจารณา ซึ่งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จัดทำประกาศรายชื่อหน่วยงานที่ผ่านการความเห็นชอบการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐผ่านเว็บไซต์ ซึ่งแสดงว่า รัฐบาลเข้มงวดและให้ความสำคัญต่อนโยบายดังกล่าว รวมทั้งการปฏิบัติต้องเป็นไปอย่างเคร่งครัด ซึ่งมีมหาวิทยาลัยที่ผ่านีความเห็นชอบจำนวนน้อยมาก ดังนั้น ห้องสมุดทุกแห่งจึงต้องมีการกำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของห้องสมุดขึ้นมาเอง โดยนำนโยบาย กฎหมาย และพระราชบัญญัติต่าง ๆ ที่เกี่ยวข้องมากำหนดเป็นประกาศและข้อปฏิบัติสำหรับบุคลากรและผู้ใช้ห้องสมุดเพื่อป้องกันความเสียหายที่อาจเกิดขึ้น และงานวิจัยของ Smet and Mayer (2016) ที่ศึกษาการกำกับดูแลแบบบูรณาการความเสี่ยงที่เป็นการปฏิบัติตามกฎ ระเบียบภายในองค์กร การปฏิบัติดังกล่าว องค์กรต้องมีจริยธรรมและสอดคล้องกับความต้องการทางด้านนโยบายภายใน ซึ่งเป็นความรับผิดชอบของผู้เกี่ยวข้อง เพราะมีความสัมพันธ์กับการบริหารการจัดการความเสี่ยงในองค์กร การสร้างกฎเกณฑ์ต่าง ๆ เป็นมาตรการจัดการความเสี่ยงด้านโครงสร้างเทคโนโลยีสารสนเทศ เพื่อให้เกิดแนวคิดที่มีประสิทธิภาพของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศขององค์กร รวมถึงงานวิจัย Yazdanmehr and Wang (2016) ที่ให้ความสำคัญต่อการนำโยบายความมั่นคงปลอดภัยสารสนเทศไปใช้ในองค์กร เพื่อให้เกิดผลในทางปฏิบัติโดยเกิดจากความรับผิดชอบส่วนบุคคลและบรรทัดฐานทางสังคมที่มาจากบรรยากาศทางจริยธรรมขององค์กร

5.3 ข้อเสนอสำหรับงานวิจัย

5.3.1 ข้อเสนอแนะที่ได้จากการศึกษางานวิจัย

5.3.1.1 คณะแพทย์ศาสตร์ศิริราชพยาบาล และหน่วยงานอื่น ๆ ควรมีการทบทวนนโยบายและปรับปรุงนโยบายให้มีความทันสมัยกับสถานการณ์ที่เปลี่ยนแปลงของระบบสารสนเทศ เพื่อไม่ให้เกิดช่องโหว่ เหมาะสมกับสภาวะปัจจุบัน และรองรับการเติบโตในอนาคตขององค์กร โดยให้มีการดำเนินการประเมินความเสี่ยงและการควบคุมภายในหน่วยงาน ได้แก่ 1) ด้านการบริหารจัดการ 2) ด้านเทคโนโลยีสารสนเทศ และ 3) ด้านข้อมูลสารสนเทศที่สำคัญของหน่วยงาน เพราะจะทำให้ได้ทราบถึงสภาพ ปัญหา และความเสี่ยงต่าง ๆ ที่อาจจะเกิดขึ้นกับทรัพย์สินของหน่วยงาน และการนำผลการประเมินความเสี่ยงนั้น ไปกำหนดแนวทางนโยบายในการบริหารความเสี่ยงที่เกิดขึ้นได้อย่างถูกต้อง ตลอดจนการควบคุมภายในหน่วยงาน และควรดำเนินการขยายผลไปยังหน่วยงานอื่น ๆ เพื่อเป็นต้นแบบในการปฏิบัติงานที่ดี

5.3.1.2 คณะแพทย์ศาสตร์ศิริราชพยาบาล และหน่วยงานอื่น ๆ ควรมีการวางแผนการพัฒนาระบบเทคโนโลยีสารสนเทศ และการเชื่อมโยงข้อมูลสารสนเทศหลักของหน่วยงาน เช่น ระบบแลกเปลี่ยนประวัติสุขภาพผู้ป่วยอิเล็กทรอนิกส์ (Health Information Exchange) ซึ่งเป็นข้อมูลหลักด้านสุขภาพ และระบบสารสนเทศกลางที่สนับสนุนการดำเนินงาน เช่น ด้านการบริการ ด้านบุคลากร ด้านการบัญชีและการเงิน และด้านการคลังสุขภาพควบคู่กับการพัฒนากลไกกระบวนการ เครื่องมือ เพื่อการสนับสนุน Digital Transformation การป้องกันและควบคุม รักษาความปลอดภัย และความลับส่วนบุคคลของข้อมูลสุขภาพ โดย

พิจารณาประโยชน์ทั้งการป้องกันข้อมูลส่วนบุคคลและการเปิดเผยข้อมูลที่จำเป็น โดยมีมาตรการป้องกันที่เหมาะสมในกรณีที่ต้องละเมิดความเป็นส่วนตัวของบุคคล โดยกฎหมายและระเบียบที่ปรับปรุงให้เอื้อต่อการพัฒนาระบบเทคโนโลยีสารสนเทศ

5.3.1.3 คณะแพทย์ศาสตร์ศิริราชพยาบาล และหน่วยงานอื่น ๆ ควรมีการออกแบบความมั่นคงปลอดภัย โดยการเชื่อมโยงข้อมูลผ่านวิธีการ Application Program Interface: API เพื่อให้สามารถรับส่งข้อมูลระหว่างระบบ Cloud และควรมีการยืนยันตัวตนเองด้วยกระบวนการ Private Key ที่ใช้ในการเข้ารหัสเพื่อยืนยันตัวตน เช่น การตรวจสอบลายมือ (Fingerprinting) การระบุพิกัด (Geolocation) เป็นต้น ตลอดจนการนำระบบโปรแกรมด้านปัญญาประดิษฐ์ (Artificial Intelligent: AI) เข้ามาช่วยในการดำเนินการตรวจสอบควบคุม ป้องกันความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ รวมถึงเป็นการลดการใช้ทรัพยากรบุคคล และการจัดทำแหล่งสำรองข้อมูล (Disaster Recovery Site: DR site) เป็นการสำรองข้อมูลในกรณีที่ระบบหลักเกิดความเสียหายจากภัยพิบัติตามธรรมชาติหรือจากการใช้งานของผู้ปฏิบัติงาน และจากการโจรกรรมข้อมูล ก็สามารถใช้ข้อมูลที่สำรองไว้มาทำงานต่อได้ทันที ปัจจุบันการสำรองข้อมูลเฉพาะบางระบบงานสำคัญเท่านั้น

5.3.1.4 คณะแพทย์ศาสตร์ศิริราชพยาบาล และหน่วยงานอื่น ๆ ควรมีการสื่อสารกับเจ้าหน้าที่ทุกระดับอย่างต่อเนื่อง เนื่องจากบุคลากรมีการโยกย้าย เปลี่ยนแปลงบ่อย และยังมีบางรายไม่ทราบและเข้าใจเกี่ยวกับการปฏิบัติตามมาตรการความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน หน่วยงานควรดำเนินการบริหารความเสี่ยงและการควบคุมภายในโดยกำหนดกิจกรรมต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ เช่น การจัดบอร์ดประชาสัมพันธ์ การฝึกอบรม และพัฒนาทักษะให้กับเจ้าหน้าที่เพื่อให้ตระหนักถึงความสำคัญของงานที่รับผิดชอบ และเพิ่มเติมทักษะที่สำคัญในการทำงานตามมาตรฐาน เกณฑ์ สอดคล้องกับการปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

5.3.2 ข้อเสนอแนะในการวิจัยครั้งต่อไป

5.3.2.1 ผู้วิจัยสามารถทำการศึกษา ติดตาม และประเมินผลการปฏิบัติงานตามองค์ประกอบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยนำองค์ประกอบดังกล่าวไปเป็นตัวแปรสำหรับการวัดและประเมินผล เพื่อใช้ในการแก้ปัญหา ปรับปรุงแผนการดำเนินงานการควบคุมภายใน และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ และหน่วยงานเอกชนที่มีบริบท หรือรูปแบบการปฏิบัติงานที่คล้ายกันให้เป็นไปตามความต้องการของผู้ใช้งานระบบต่าง ๆ ได้อย่างปลอดภัย

5.3.2.2 ผู้วิจัยสามารถศึกษาความสำคัญขององค์ประกอบการบริหารจัดการความมั่นคงปลอดภัย ด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยการวิเคราะห์จำแนกกลุ่ม (Discriminant Analysis) เพื่อจำแนกปัจจัย ว่ามีปัจจัยใดบ้าง ที่มีอิทธิผลต่อมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ หรือการนำตัวแปรที่วิเคราะห์ไปยืนยันองค์ประกอบโดยวิธีทางสถิติ (Confirmatory Factor Analysis) หรือการประเมินอิงผู้เชี่ยวชาญ (Connoisseurship)

5.3.2.3 ผู้วิจัยสามารถขยายขอบเขตการศึกษาของกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ครอบคลุมทุกหน่วยงาน และมาตรฐานของมาตรการการป้องกัน ควบคุมความมั่นคงด้าน

สารสนเทศ ตลอดจนระเบียบ และวิธีการปฏิบัติงานใหม่ ๆ เช่น พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้นเพื่อนำผลของการศึกษาสภาพการทำงานที่เกิดขึ้นมาปรับปรุงกระบวนการทำงาน แนวทางการบริหารจัดการด้านการควบคุมภายใน และการบริหารความมั่นคงปลอดภัยสารสนเทศ รวมถึงการจัดทำคู่มือการปฏิบัติงาน และประกาศมาตรการการป้องกันความมั่นคงปลอดภัยด้านสารสนเทศ เป็นต้น ต่อไป

5.4 ข้อจำกัดงานวิจัย

การรวบรวมข้อมูลงานวิจัยครั้งนี้ใช้วิธีการแจกแบบสอบถามในรูปแบบสำรวจออนไลน์ (Online Survey) แต่มีผู้ตอบสอบถามตอบแบบสอบถามมาในครั้งแรกในปริมาณที่น้อยกว่าเป้าหมายที่กำหนดไว้ เนื่องจากผู้ตอบแบบสอบถามมีความหลากหลาย และอยู่กันแตกต่างกันในแต่ละแผนกของคณะแพทยศาสตร์ศิริราชพยาบาล และเจ้าหน้าที่บางคนไม่สะดวกในการตอบแบบสอบถาม และคิดว่าการตอบแบบสอบถามในรูปแบบออนไลน์มีความยุ่งยากและซับซ้อน จึงไม่ค่อยยอมทำแบบสอบถามทางออนไลน์

บรรณานุกรม

บรรณานุกรม

กัลยา วานิชย์บัญชา. (2546). *การวิเคราะห์สถิติขั้นสูงด้วย (เอสพีเอสเอส ฟอร์วินโดวส์) SPSS for Windows* (พิมพ์ครั้งที่ 3). ธรรมสาร.

คณะแพทยศาสตร์ศิริราชพยาบาล. (2560). *Statistical report 2018*. เวชทะเบียนสารสนเทศ.

คณะแพทยศาสตร์ศิริราชพยาบาล. (2563). *รายงานประจำปี 2563.* ผู้แต่ง.

ครรชิต มาลัยวงศ์. (2554). *รายงานสำรวจสถานภาพและความพร้อมในการใช้งานคอมพิวเตอร์และระบบอินเทอร์เน็ตของโรงเรียนมัธยมศึกษาทั่วประเทศ.* สถาบันเทคโนโลยีเพื่อการศึกษาแห่งชาติ.

ฉัตรศิริ ปิยิพิมลสิทธิ์. (2551). *ความเที่ยงตรง* [เอกสารอัดสำเนา]. มหาวิทยาลัยศรีนครินทรวิโรฒ.

ชาญชัย ประมูลเฉโก และ วศิณ ชูประยูร. (2564). *การพัฒนาแผนปฏิบัติการกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย* [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยรังสิต]. มหาวิทยาลัยรังสิต.

โชติทัต กมลคนธ์. (2555). *การสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ ภายใต้มาตรฐาน ISO 27001 กรณีศึกษาบริษัท เอ็น.ซี.ซี แมนเนจเม้นแอนดีวีลอบเม้น จำกัด* [สารนิพนธ์ปริญญาโทมหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีมหานคร]. มหาวิทยาลัยเทคโนโลยีมหานคร.

ณัฐนันท์ เสริฐสุวรรณกุล. (2562). *การศึกษาองค์ประกอบการบริหารจัดการเทคโนโลยีสารสนเทศตามกรอบงาน COBIT5* [สารนิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิตย์]. ศูนย์เรียนรู้และหอสมุดมหาวิทยาลัยธุรกิจบัณฑิตย์. https://libdoc.dpu.ac.th/thesis/Nutthanun.Ser.pdf

ณัฐวุฒิ วิศยทักษิณ. (2554). *การพัฒนานโยบายด้านความปลอดภัยภายใต้มาตรฐาน ISO 27001 และการบริหารความเสี่ยง มหาวิทยาลัยกรุงเทพ* [สารนิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีมหานคร]. มหาวิทยาลัยเทคโนโลยีมหานคร.

ดุษฎี โยเหลา. (2541). *วิชา วป 712 สถิติเพื่อการวิเคราะห์ข้อมูลทางพฤติกรรมศาสตร์ IV. (เอกสารประกอบคำสอน)* [เอกสารอัดสำเนา]. สถาบันวิจัยพฤติกรรมการศาสตร์ มหาวิทยาลัยศรีนครินทร์วิโรฒ.

ธัญญรัตน์ ปิยวัฒน์กานนท์ และชุติมา เบี้ยวไข่มุก. (2560). การวิเคราะห์ช่องว่างการดำเนินการด้านไอทีของบริษัทด้านการเงินที่ผ่านการรับรองมาตรฐานสากลด้านความมั่งคงปลอดภัยตามกรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร. ใน *รายงานการประชุมวิชาการระดับชาติ มหาวิทยาลัยรังสิต ประจำปี 2560.* (น. 200-210). https://rsucon.rsu.ac.th/files/proceedings/nation2017/G2-12.pdf

ธารินี เณรวงศ์. (2558). ปัจจัยที่มีผลต่อระดับการควบคุมภายในระบบสารสนเทศทางการบัญชี ภายใต้การบริหารการเงินการคลังภาครัฐของหน่วยงานสนับสนุนภารกิจฝ่ายการเมือง. *วารสารวิชาการบริหารธุรกิจ สมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทย (สสอท.), 4*(1), 76-91. https://so02.tci-thaijo.org/index.php/apheitvu/article/view/95124/74321

บรรณานุกรม (ต่อ)

ธีรพล แสงอุทัย. (2555). *การพัฒนาความมั่นคงปลอดภัยของระบบเครือข่ายตามมาตรฐาน ISO 27001/17799 สำหรับบริษัท เน็ตมาร์ค (ประเทศไทย) จำกัด* [สารนิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีมหานคร]. มหาวิทยาลัยเทคโนโลยีมหานคร.

นงลักษณ์ วิรัชัย. (2537). *ความสัมพันธ์โครงสร้างเชิงเส้น (ลิสเรล) LISREL: สถิติวิเคราะห์สำหรับการวิจัยทางสังคมและพฤติกรรมศาสตร์.* โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

นภสินธุ์ บุญมาก และ เลอพงศ์ แก้วอินทร์. (2564). การตรวจประเมินภายในตามข้อกำหนดมาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ. *วารสาร Mahidol R2R e –Journal, 8*(2), 53-67. https://he01.tci-thaijo.org/index.php/mur2r/article/view/251349/169798

นันทิดา โยธานวล และ ศักดิ์ชาย จันทร์เรือง. (2558). *การควบคุมทั่วไปของระบบสารสนเทศทางการบัญชี.* อี.เทค.

ประสิทธิ์ ทีฆพุฒิ และ ครรชิต มาลัยวงศ์. (2549). *การจัดการเทคโนโลยีสารสนเทศ.* ดอกหญ้ากรุ๊ป.

พิทา จารุพูนพล. (2564). *ความมั่นคงของสารสนเทศ.* คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏภูเก็ต.

พิมพา หิรัญกิตติ, ปณิศา มีจินดา, สมชาย หิรัญกิตติ, สุวิมล แม้นจริง, และ อุดม สายะพันธุ์. (2552). *การศึกษาพฤติกรรมการท่องเที่ยวเชิงบริการทางการแพทย์ของนักท่องเที่ยวชาวต่างชาติ* [รายงานผลการวิจัย, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี]. มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

ภาพร ภิยโยดิลกชัย. (2553). *การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT* [งานค้นคว้าอิสระปริญญามหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิตย์]. ศูนย์เรียนรู้และหอสมุด มหาวิทยาลัยธุรกิจบัณฑิตย์. https://libdoc.dpu.ac.th/thesis/141275.pdf

ภิรมย์พร เยาดำ, ธนสุวิทย์ ทับหิรัญรักษ์, และ สุคนธ์ เครือน้ำคำ. (2559). ประสิทธิภาพของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS) ในเขตพื้นที่จังหวัดระนอง. ใน *รายงานการประชุมวิชาการและนำเสนอผลงานวิจัยระดับชาติและนานาชาติ ครั้งที่ 7* (น. 1365-1376).

ภุมวุฒิ วิทวัสสำราญกุล. (2563). *แนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ* [สารนิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิตย์]. ศูนย์เรียนรู้และหอสมุด มหาวิทยาลัยธุรกิจบัณฑิตย์. https://libdoc.dpu.ac.th/thesis/Poomwoot.Vit.pdf

ยุทธ ไกยวรรณ์. (2555). *หลักสถิติวิจัยและการใช้โปรแกรม SPSS.* จุฬาลงกรณ์มหาวิทยาลัย.

วรัญญาภรณ์ สิริพิพัฒนพร และ สมชาย นำประเสริฐชัย. (2558*). การวิเคราะห์และแนวทางจัดการความเสี่ยงด้านไอทีของหน่วยงานภาครัฐ.* วิศวกรรมสาร มก.

บรรณานุกรม (ต่อ)

แววตา เตชาทวีวรรณ. (2563). สภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาของรัฐ. *วารสารวิจัย สมาคมห้องสมุดแห่งประเทศไทยฯ, 13*(2), 96-115. https://so06.tci-thaijo.org/index.php/tla_research/article/view/246908/167673

ศิวลีย์ สิริโรจน์บริรักษ์. (2558). การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber security) ของกระทรวงมหาดไทย. *วารสารสถาบันวิชาการป้องกันประเทศ, 6*(3), 19-29. https://so04.tci-thaijo.org/index.php/ndsijournal/article/view/39369/32571

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. (2550). *มาตรฐานการรักษาความมั่นคง ปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5).* ผู้แต่ง.

ศูนย์วิจัยกฎหมายและการพัฒนา. (2563). *Thailand data protection guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.* โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

สำนักงานการตรวจเงินแผ่นดิน. (2565). *เจาะลึกผลการตรวจสอบระบบสารสนเทศของหน่วยงานของรัฐ 11 แห่ง* สำนักประชาสัมพันธ์และสื่อสารองค์กร สำนักงานการตรวจเงินแผ่นดิน.

สำนักงานคณะกรรมการพัฒนาระบบราชการ. (2552). เทคนิคการปรับปรุงและพัฒนาองค์การ. อมรินทร์พริ้นติ้ง แอนด์ พับบลิชชิ่ง.

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2563). *แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย.* ผู้แต่ง.

สุชาดา สิทธิ์จงสถาพร. (2563) *เอกสารการสอนชุดวิชาความมั่นคงปลอดภัยไซเบอร์ หน่วยที่ 1 – 5.* สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช.

สุชาติ ประสิทธิ์รัฐสินธุ์ และ ลัดดาวัลย์ รอดมณี. (2527). *เทคนิคการวิเคราะห์ตัวแปรหลายตัวสำหรับการวิจัยทางสังคมศาสตร์.* ภาพพิมพ์.

สุภมาส อังศุโชติ, สมถวิล วิจิตรวรรณา, และ รัชนีกูล ภิญโญภานุวัฒน์. (2551)**.** *สถิติวิเคราะห์สำหรับการวิจัยทางสังคมศาสตร์และพฤติกรรมศาสตร์: เทคนิคการใช้โปรแกรม (ลิสเรล) LISREL*. มิสชั่น มีเดีย.

สุวันต์นา เสมอเนตร. (2562). การพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายใต้มาตรฐาน SO/IEC 27001: 2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center. *วารสารวิชาการสาธารณสุข, 28*(1), 117-132. https://thaidj.org/index.php/JHS/article/view/5914/5747

อุทัยวรรณ จรุงวิภู. (2550). แนวคิดเกี่ยวกับระบบสารสนเทศทางการบัญชี. ใน *ระบบสารสนเทศทางการบัญชี หน่วยที่ 1* (พิมพ์ครั้งที่ 9). มหาวิทยาลัยสุโขทัยธรรมธิราช.

อุทุมพร ทองอุไทย. (2524). *วิธีวิเคราะห์ตัวประกอบ.* ภาควิชาวิจัยการศึกษา คณะครุศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

อุษณา ภัทรมนตรี. (2547). *การตรวจสอบภายในสมัยใหม่.* เท็กซ์ แอนด์ เจอร์นัลพับลิเคชั่น.

An dress, J. (2014). *The basics of information security* (2nd ed.)*.* Syngress.

บรรณานุกรม (ต่อ)

Bertino, E. (2017). *Security and privacy in the IoT*. In X. Chen, D. Lin, & M. Yung (eds), *Information security and cryptology. Inscrypt 2017*. Lecture Notes in Computer Science, 10726. Springer, Cham. https://doi.org/10.1007/978-3-319-75160-3_1

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior, 28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

Eigeles, D. (2006). Intelligent authentication, authorization, and administration (I3A). *Information Management & Computer Security, 14*(1), 5-23. http://www.emeraldinsight.com/doi/pdfplus/10.1108/09685220610648346.

Ghosh, A. K. (1998). *E-Commerce security, weak links, best defences.* John Wiley and Sons.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariante data analysis* (5th ed.). Prentice Hall.

Hair J. F., Black, W. C, Babin, B. J., Andreson, R. E., & Tatham, R. L. (2006). *Multivariate data statistical*. Prenitce-Hall.

Hayale, T. A., & Khadra, H. A. (2008)**.** Investigating perceived security threats of computerized accounting information systems: An empirical research applied on Jordanian banking sector. *Journal of Economic and Administrative Sciences, 24*(1).

Hessou, H., & Lai, V. S. (2017). Basel III capital buffer requirement and credit union prudential regulation: Canadian evidence. *Journal of Financial Stability, 30*, 92-110. https://doi.org/10.1016/j.jfs.2017.05.002.

Hou, R., Ren, G., Zhou, C., Yue, H., Liu, H., & Liu, J. (2020). Analysis and research on network security and privacy security in ubiquitous electricity Internet of Thing. *Computer Communication, 158,* 64-72. https://doi.org/10.1016/j.comcom.2020.04.019.

Ibrahim, & Nurpulaela, L. (2017). Evaluation of IT governance to support IT operation excellent based on COBIT 4.1 at the PT Timah Tbk. *Proceedings. 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (*pp. 336-339). Semarang, Indonesia. https://doi.prg/10.1109/ICITACEE.2016.7892467

บรรณานุกรม (ต่อ)

ISACA. (2012). *Cobit 5 enable processes*. Author. https://thegioibantin.com/wp-content/uploads/2016/07/COBIT5-EnablingProcess.pdf

Ismail, R., & Zainab, A. N. (2011). Information systems security in special and public libraries: An assessment of status. *Malaysian Journal of Library & Information Science*, *16*(2), 45-62. https://mjlis.um.edu.my/index.php/MJLIS/article/view/6697/4379

Jongsureyapart, C. (2006). *Factors that determine corporate governance in Thailand* [Doctoral dissertation, Victoria University]. Victoria University CRICOS. https://vuir.vu.edu.au/1504/1/Jongsureyapart.pdf

Khther, R. A., & Othman, M. (2013). Cobit framework as a guideline of effective it governance in higher education: A review. *International Journal of Information Technology Convergence and Services, 3*(1), 21–29. https://www.airccse.org/journal/ijitcs/papers/3113ijitcs02.pdf

Lee, J., Lee, C., & Jeong, K.-Y. (2008). Governance inhibitors in IT strategy and management: An empirical study of Korean Enterprises. *Global Economic Review, 37*(1), 1-22. https://doi.org/10.1080/12265080801911899

Lenders, V., Tanner, A., & Blarer, A. (2015). Gaining an edge in cyberspace with advance situation awareness. *IEEE Security & Privacy, 13*(2), 65-74. https://doi.org/10.1109/MSP.2015.30

Maria, E., Fibriani, C., & Sinatra, L. (2012). The measurement of information technology performance in Indonesian Higher Education Institutions in The Context of Achieving Institution Business Goals using COBIT framework version 4.1. *International Refereed Research Journal, 3*(3), 9-19.

Musa, N., Abang Ibrahim, D. H., Bolhassan, N. A., Abdullah, J., Kulathuramaiyer, N., & Khairuddin, M. N. (2014). An IT governance framework for achieving the development of academic programme in higher institutions: A case of Universiti Malaysia Sarawak (UNIMAS). In *2014 the 5th International Conference on Information and Communication Technology for the Muslim World.*

Nan, Z., Guo, X., & Chen, G. (2008). IDT-TAM Integrated mode for IT adoption. *Journal of Tsinghua University (Science and Technology), 13*(3), 306-311. https://doi.org/10.1016/S1007-0214(08)70049-X

บรรณานุกรม (ต่อ)

Ngwube, A. (2013). Determinant factors for success of corporate governance in an organization. *Singaporean Journal of Business Economics and Management Studies*, *1*(11), 18-24. https://www.singaporeanjbem.com/pdfs/SG_VOL_1_(11)/4.pdf

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., Kagaya, T. (2009). *Information security governance framework*. In WISG '09: Proceedings of the first ACM workshop on Information security governance (pp. 1–6). https://doi.org/10.1145/1655168.1655170

Pereira, G. V., Luciano, E. M., Macadar, M. A., & Daniel, V. M. (2013). Information technology governance practices adoption through and institutional perspective: The perception of Brazilian and American CIOs. In *2013 46th Hawaii International Conference on System Sciences*, Wailea, HI, USA (pp. 4446-4455). https://doi.org/10.1109/HICSS.2013.276

Dung, P. D., & Tuan, P. A. (2015). Accounting Information System affecting efficiency of Vietnam's small and medium enterprises in the ASEAN Economic Community (AEC). *Phat Trien & Hoi Nhap, 20*(30), 87-96. https://user-cdn.uef.edu.vn/newsimg/tap-chi-uef/2015-01-02-20/13.pdf

Preuss, C. (2014). *Retail marketing and sales performance: A definitive guide to optimizing service quality and sales effecitvenss*. Springer Gabler.

Rubino, M., Vitolla, F., & Garzoni, A. (2017). How IT controls improve the control environment. *Management Research Review, 40*(2), 218-234. https://doi.org/10.1108/MRR-04-2016-0093

Sharbaf, M. S. (2014). A new perspective to information security: Total quality information security management. In *Proceedings of the 7th International Conference on Security of Information and Networks* (pp. 56–60). https://doi.org/10.1145/2659651.2659666

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

Spremic, M. (2015). Corporate governance of enterprise IT: Research study on IT governance maturity. *International Journal of Economics and Management Engineering, 9*(9), 3071-3075. https://doi.org/10.5281/zenodo.1108661

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice***.** Pearson.

บรรณานุกรม (ต่อ)

Stamp, M. (2006). *Information security.* Wiley.

Stein, L. D. (1998). *Web security.* Addison-Wesley.

Thomas, C. A. (2010). *IT governance in small and medium enterprises post Sarbanes Oxley* [Doctoral dissertation, Louisiana State University]. LSU Digital Commons. https://doi.org/10.31390/gradschool_dissertations.1207

Yamane, T. (1973). *Statistics: An introductory analysis* (2nd ed.). Harper and Row.

Yazdanmehr, A., & Wang. J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92,* 36-46. https://doi.org/10.1016/j.dss.2016.09.009

ภาคผนวก

ภาคผนวก ก

แบบสอบถามเพื่อประเมินดัชนีความสอดคล้อง (IOC)

ร่างแบบสอบถามเพื่อการวิจัย (IOC)

เรื่อง การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

ของคณะแพทยศาสตร์ศิริราชพยาบาล

คำชี้แจง:

1. แบบสอบถามฉบับนี้ มีวัตถุประสงค์หลักเพื่อศึกษาถึงองค์ประกอบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

2. แบบสอบถามฉบับนี้มุ่งตรวจสอบ เพื่อหาค่าความเที่ยงตรง (Validity) โดยการวิเคราะห์ดัชนีความสอดคล้อง (Index of item objective Congruence: IOC) ของแบบสอบถามและข้อเสนอแนะของผู้เชี่ยวชาญ เพื่อนำไปปรับปรุงแบบสอบถามให้สมบูรณ์ยิ่งขึ้น

3. แบบสอบถามฉบับนี้มีทั้งหมด 3 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

ส่วนที่ 2 กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ส่วนที่ 3 ข้อเสนอแนะ

4. ขอความกรุณาผู้ทรงคุณวุฒิหรือท่านผู้เชี่ยวชาญ ช่วยพิจารณาร่างแบบสอบถามว่ามีความสอดคล้องกับตัวแปรของการวิจัยเรื่องนี้หรือไม่ ด้วยการให้คะแนนในแต่ละข้อคำถามในระบบ IOC โดยการทำเครื่องหมาย ☑ ลงในช่องว่าง เกณฑ์การให้คะแนนในระบบ IOC

1. ให้ 1 คะแนน **เมื่อแน่ใจ**ว่าข้อนั้นมีเนื้อหาที่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา
2. ให้ 0 คะแนน **เมื่อไม่แน่ใจ**ว่าข้อนั้นมีเนื้อหาที่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา
3. ให้ -1 คะแนน **เมื่อแน่ใจ**ว่าข้อนั้นมีเนื้อหาไม่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

5. ผู้วิจัยขอความกรุณาท่านผู้ทรงคุณวุฒิและผู้เชี่ยวชาญ ให้ข้อเสนอแนะหรือความคิดเห็นเพิ่มเติมในประเด็นที่ยังไม่สมบูรณ์ โดยการเขียนข้อเสนอแนะไว้ท้ายข้อความนั้น ๆ

ผู้วิจัยขอขอบคุณในความกรุณาของท่านมา ณ โอกาสนี้

นายศิวกร รัตติโชติ
นักศึกษาปริญญาโท สาขาวิชาการบัญชี
วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิต

ส่วนที่ 1 ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย ☑ ลงในตาราง หน้าข้อความที่ตรงตามความเป็นจริง

คำชี้แจงสำหรับผู้เชี่ยวชาญ: โปรดพิจารณาว่าข้อความเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1	**เพศ**				
	☐ 1. ชาย				
	☐ 2. หญิง				
2	**อายุ**				
	☐ 1. น้อยกว่า 20 ปี				
	☐ 2. 21 – 30 ปี				
	☐ 3. 31 - 40 ปี				
	☐ 4. 41 – 50 ปี				
	☐ 5. มากกว่า 50 ปี				
3	**ระดับการศึกษา**				
	☐ 1. ต่ำกว่าปริญญาตรี				
	☐ 2. ปริญญาตรี				
	☐ 3. ปริญญาโท				
	☐ 4. ปริญญาเอก				
4	**ตำแหน่ง**				
	☐ 1. เจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป				
	☐ 2. เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT				
	☐ 3. นักศึกษา				
	☐ 4. แพทย์/พยาบาล/เภสัชกร/นักสาธารสุข				
	☐ 5. หัวหน้างาน/ผู้บริหาร				
	☐ 6. อาจารย์/นักวิชาการ/นักวิจัย				
	☐ 7. อื่น ๆ (โปรดระบุ).....				
5	**หน่วยงานที่ปฏิบัติงาน**				
	☐ 1. ฝ่ายการคลัง				
	☐ 2. ฝ่ายสารสนเทศ				
	☐ 3. หน่วยตรวจสอบภายใน				
	☐ 4. ฝ่ายทรัพยากรบุคคล				

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1	**เพศ**				
	☐ 1. ชาย				
	☐ 5. ฝ่ายนโยบายและแผน				
	☐ 6. ฝ่ายทรัพย์สินและพัสดุ				
	☐ 7. ฝ่ายวิศวกรรมบริการและอาคาร				
	☐ 8. ฝ่ายวิจัย				
	☐ 9. ฝ่ายการพยาบาล				
	☐ 10. ฝ่ายเภสัชกรรม				
	☐ 11. ฝ่ายโภชนาการ				
	☐ 12. ภาควิชา (โปรดระบุ).....				
	☐ 13. อื่น ๆ (โปรดระบุ).....				
6	**ประสบการณ์ทำงานในหน่วยงานปัจจุบัน (ถ้าเกิน 6 เดือนให้นับเป็น 1 ปี)**				
	☐ 1. น้อยกว่า 1 ปี				
	☐ 2. 1 – 5 ปี				
	☐ 3. 6 - 10 ปี				
	☐ 4. 11 – 15 ปี				
	☐ 5. 16 - 20 ปี				
	☐ 6. มากกว่า 20 ปี				
7	**ระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ปัจจุบัน (สามารถตอบได้มากกว่า 1 ข้อ)**				
	☐ 1. ระบบสำนักงานอัตโนมัติ				
	☐ 2. ระบบประมวลผลรายการ				
	☐ 3. ระบบงานสร้างความรู้				
	☐ 4. ระบบสารสนเทศเพื่อการจัดการ				
	☐ 5. ระบบสนับสนุนการตัดสินใจ				
	☐ 6. ระบบสารสนเทศสำหรับผู้บริหารระดับสูง				
	☐ 7. อื่น ๆ (โปรดระบุ).....				

ส่วนที่ 2 กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับความคิดเห็นองค์ประกอบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยการสังเคราะห์เอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้องเกี่ยวกับการการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ จำนวน 5 ด้าน โปรดอ่านและพิจารณาตอบคำถาม โดยทำเครื่องหมาย ☑ ลงในช่องว่าง ระดับความคิดเห็นที่ตรงกับความคิดเห็นกับท่านมากที่สุดเพียง 1 ข้อ

คำชี้แจงสำหรับผู้เชี่ยวชาญ: โปรดพิจารณาว่าข้อความเกี่ยวกับความคิดเห็นต่อกระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล สอดคล้องกับตัวแปรและวัตถุประสงค์ที่จะวัดหรือไม่

คำชี้แจง โปรดทำเครื่องหมาย ☑ ลงในตาราง หน้าข้อความที่ตรงตามความเป็นจริง

ลำดับ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ					
1	มีการกำหนดกรอบการดำเนินงานด้านการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เช่น การบำรุงรักษาระบบ เครื่องมือเทคโนโลยีสารสนเทศ อุปกรณ์การเข้าใช้งานระบบสารสนเทศ เป็นต้น ให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง อยู่ในระดับใด				
2	มีการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานให้มีความรวดเร็ว ข้อมูลมีความถูกต้องครบถ้วน และเป็นปัจจุบัน เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้ อยู่ในระดับใด				
3	มีการมอบหมายภารกิจด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้กับผู้ปฏิบัติงานได้อย่างชัดเจน อยู่ในระดับใด				
4	มีการจัดทำข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่อนุญาตให้บุคคลหรือหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน อยู่ในระดับใด				
5	มีมาตรการด้านความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์พกพา เพื่อ				

ลำดับ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
	บริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว อยู่ในระดับใด				
6	มีการกำหนดข้อปฏิบัติในการใช้คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ เช่น เครื่องคอมพิวเตอร์แบบพกพาสมาร์ทโฟน เป็นต้น เพื่อให้มีความมั่นคงปลอดภัย และเกิดประสิทธิภาพต่อการใช้งาน อยู่ในระดับใด				
7	มีการเก็บบันทึก และจำแนกประเภทของบัญชีทรัพย์สิน ข้อมูลสารสนเทศ เพื่อกำหนดระดับของการป้องกันทรัพย์สินด้านสารสนเทศ อยู่ในระดับใด				
8	มีการจัดทำทะเบียน รับ – คืนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ อยู่ในระดับใด				
9	มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ อยู่ในระดับใด				
10	มีการจัดทำบันทึกข้อตกลงให้ผู้ปฏิบัติงานต้องรักษาทรัพย์สินให้ปลอดภัย และข้อมูลที่เป็นความลับ อยู่ในระดับใด				
11	มีการรวบรวมข้อมูล ตรวจสอบ และประเมินผลการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศตามแนวทางการควบคุมภายในด้านการใช้งานระบบสารสนเทศของหน่วยงาน เพื่อระบุข้อบกพร่องในการใช้งานระบบ และนำมาปรับปรุงให้สามารถทำงานได้อย่างมีประสิทธิภาพ อยู่ในระดับใด				
12	มีขั้นตอน หรือแผนรองรับในการบริหารจัดการเหตุการณ์ผิดปกติ และปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ พร้อมทั้งช่องทางการรายงานเหตุการณ์ปัญหาที่พบผิดปกติที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศ อย่างเหมาะสมและทันท่วงที อยู่ในระดับใด				

ลำดับ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
13	มีมาตรการป้องกันภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น เพื่อป้องกันไม่ให้ทรัพย์สินสารสนเทศเสียหาย อยู่ในระดับใด				
14	มีการป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ และเป้าหมายของงานที่รับผิดชอบ อยู่ในระดับใด				
องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ					
15	มีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก อยู่ในระดับใด				
16	มีการกำหนดขั้นตอน ควบคุมการตรวจสอบ ป้องกันและกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ อยู่ในระดับใด				
17	มีการรักษาความมั่งคงของแม่ข่าย (Server) และอุปกรณ์ที่ใช้งานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่พึงประสงค์ดี (Malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหล ของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต อยู่ในระดับใด				
18	มีการจัดทำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไว้ในเงื่อนไขการจ้างพัฒนาหรือปรับปรุงระบบ เช่น เอกสารรายละเอียดคุณสมบัติทางเทคนิคในการจัดซื้อจัดจ้างโดยครอบคลุมถึงเรื่องรักษาความมั่นคงปลอดภัย อยู่ในระดับใด				
19	มีการดูแล ควบคุม ติดตามตรวจสอบการพัฒนาระบบสารสนเทศ โดยหน่วยงานภายนอก รวมถึงการจ้างช่วงพัฒนาระบบ อยู่ในระดับใด				

ลำดับ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
20	มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงาน ต้องปฏิบัติตามสัญญาหรือข้อตกลงในการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ อยู่ในระดับใด				
21	มีการจ้างผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจในการร่วมพัฒนา มีการคำนึงถึงความต่อเนื่องในการดำเนินธุรกิจ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และการยกเลิกหรือสิ้นสุดสัญญา (Exit Strategy) อยู่ในระดับใด				
22	มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ หรือธุรกรรมออนไลน์กับบุคคลหรือหน่วยงานภายนอก (เช่น การสั่งซื้อ/ขายสินค้าหรือบริการผ่านระบบอิเล็กทรอนิกส์ การชำระเงินผ่านระบบอิเล็กทรอนิกส์) เป็นต้น อยู่ในระดับใด				
23	มีการกำหนดให้มีการเข้าใช้งานระบบสารสนเทศตามมาตรการเข้ารหัสข้อมูล (Cryptography) และการบริหารจัดการกุญแจ (Access Key) เป็นต้น อยู่ในระดับใด				
24	มีการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงาน สอดคล้องกับชั้นความลับของสารสนเทศ อยู่ในระดับใด				
องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ					
25	มีการบำรุงรักษาและดูแลอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน อยู่ในระดับใด				

ลำดับ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
26	มีการจัดทำ และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบต่าง ๆ เพื่อให้ผู้ปฏิบัติงานสามารถนำไปปฏิบัติได้อย่างถูกต้องและปลอดภัย อยู่ในระดับใด				
27	มีการกำหนดให้ผู้ปฏิบัติงานหรือบุคคลภายนอกที่หน่วยงานว่าจ้างจะต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย และบทลงโทษ ในกรณีที่ผู้ปฏิบัติงานฝ่าฝืนนโยบายหรือระเบียบที่หน่วยงานประกาศใช้อย่างชัดเจน อยู่ในระดับใด				
28	มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน อยู่ในระดับใด				
29	มีการกำหนดให้เจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงาน เมื่อสิ้นสุดการจ้างงาน อยู่ในระดับใด				
30	มีการพัฒนา อบรม เพิ่มพูน ทักษะและความสามารถของผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับใด				
องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์					
31	มีการกำหนดกลยุทธ์เพื่อการบริหารงานของหน่วยงาน โดยการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินงานสอดคล้องกับนโยบาย บทบาท ภารกิจของหน่วยงาน และระบบความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับใด				
32	มีการกำหนดนโยบายและแนวทางสำหรับความมั่นคงปลอดภัยด้านสารสนเทศเพื่อควบคุม และป้องกันความเสี่ยงด้านสารสนเทศเป็นลายลักษณ์อักษร และประกาศหรือแจ้งนโยบายดังกล่าวให้ผู้ปฏิบัติงานรับทราบทั่วกัน อยู่ในระดับใด				

ลำดับ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
33	มีการวิเคราะห์ความเสี่ยง (Risk analysis) และประเมินค่าความเสี่ยง (Risk Evaluation) เพื่อประเมินระดับผลกระทบและโอกาสเกิดเหตุการณ์ และจัดลำดับความเสี่ยงในการจัดการด้านสารสนเทศของหน่วยงาน อยู่ในระดับใด				
34	มีการจัดการความเสี่ยง (Risk Treatment) กำหนดแนวทาง ติดตาม ทบทวน และประเมินความเสี่ยงที่เกิดขึ้นด้านสารสนเทศ เช่น ด้านข้อมูล ด้านอุปกรณ์เทคโนโลยีสารสนเทศ ด้านซอฟแวร์คอมพิวเตอร์ เป็นต้น อย่างสม่ำเสมอ อยู่ในระดับใด				
35	มีการรายงานผลการบริหารความเสี่ยงด้านสารสนเทศและแนวโน้มของความเสี่ยงที่อาจจะเกิดขึ้นตามนโยบายที่กำหนดให้ท่านทราบ อยู่ในระดับใด				

ตอนที่ 3 ข้อเสนอแนะ

คำชี้แจงของผู้ตอบแบบสอบถาม : กรุณาแสดงความคิดเห็นที่ตรงกับความคิดเห็นของท่านมากที่สุด

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาความเหมาะสมของข้อคำถาม

ลำดับ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	- 1	
1	ท่านมีข้อเสนอแนะที่ต้องการได้รับการสนับสนุนจากหน่วยงาน				
2	ท่านมีข้อเสนอแนะเพื่อเป็นการพัฒนาการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน				
3	ข้อเสนอแนะอื่น ๆ				

ข้อเสนอแนะของผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ

.....

.....

.....

ลงชื่อ .....

(.....)

ผู้ทรงคุณวุฒิ

ภาคผนวก ข

ผลการประเมินดัชนีความสอดคล้อง (Index of Item Congruence : IOC)

DPU
DHURAKIJ PUNDIT UNIVERSITY
มหาวิทยาลัยธุรกิจบัณฑิตย์

ที่ บช.0403(1)/0929

วันที่ 23 พฤศจิกายน 2565

เรื่อง ขอเรียนเชิญเป็นผู้ทรงคุณวุฒิตรวจสอบเครื่องมือวิจัย

เรียน ผู้ช่วยศาสตราจารย์ ดร.รัฐพล พรหมสะอาด

สิ่งที่ส่งมาด้วย 1. โครงการวิจัยและเครื่องมือวิจัย จำนวน 1 ชุด

ด้วย นายศิวกร รัตติโชติ นักศึกษาบัญชีมหาบัณฑิต วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์ ได้จัดทำวิจัยเรื่อง การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ในการนี้ หลักสูตรบัญชีมหาบัณฑิต วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์ จึงใคร่ขอเรียนเชิญ ผู้ช่วยศาสตราจารย์ ดร.รัฐพล พรหมสะอาด คณะครุศาสตร์ มหาวิทยาลัยราชภัฏภูเก็ต เป็นผู้ทรงคุณวุฒิตรวจสอบเครื่องมือวิจัยดังกล่าว ตามรายละเอียดโครงการวิจัยและเครื่องมือวิจัยที่แนบมาพร้อมนี้ โดยจะขอรับเครื่องมือกลับคืนภายใน วันที่ 30 พฤศจิกายน 2565

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จะเป็นพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศิริเดช คำสุพรหม)
คณบดีวิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี

ผู้ประสานงาน นายศิวกร รัตติโชติ
โทร. 080 534 9480

มหาวิทยาลัยธุรกิจบัณฑิตย์ 110/1-4 ถนนประชาชื่น เขตหลักสี่ กรุงเทพฯ 10210
Dhurakij Pundit University 110/1-4 Prachachuen Road, Laksi, Bangkok 10210, Thailand
Tel. (66) 2954-7300 www.dpu.ac.th

DPU
DHURAKIJ PUNDIT UNIVERSITY
มหาวิทยาลัยธุรกิจบัณฑิตย์

ที่ บช.0403(1)/0927

วันที่ 23 พฤศจิกายน 2565

เรื่อง ขอเรียนเชิญเป็นผู้ทรงคุณวุฒิตรวจสอบเครื่องมือวิจัย
เรียน ดร. จุฬาลักษณ์ ทรัพย์สุทธิ
สิ่งที่ส่งมาด้วย 1. โครงการวิจัยและเครื่องมือวิจัย จำนวน 1 ชุด

ด้วย นายศิวกร รัตติโชติ นักศึกษาบัญชีมหาบัณฑิต วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์ ได้จัดทำวิจัยเรื่อง การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ในการนี้ หลักสูตรบัญชีมหาบัณฑิต วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์ จึงใคร่ขอเรียนเชิญ ดร. จุฬาลักษณ์ ทรัพย์สุทธิ ผู้อำนวยการกลุ่มภารกิจวิจัยและพัฒนาระบบบริหาร กลุ่มพัฒนาระบบบริหาร สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เป็นผู้ทรงคุณวุฒิตรวจสอบเครื่องมือวิจัยดังกล่าว ตามรายละเอียดโครงการวิจัยและเครื่องมือวิจัยที่แนบมาพร้อมนี้ โดยจะขอรับเครื่องมือกลับคืนภายใน วันที่ 30 พฤศจิกายน 2565

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จะเป็นพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศิริเดช คำสุพรหม)
คณบดีวิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี

มหาวิทยาลัยธุรกิจบัณฑิตย์ 110/1-4 ถนนประชาชื่น เขตหลักสี่ กรุงเทพฯ 10210
Dhurakij Pundit University 110/1-4 Prachachuen Road, Laksi, Bangkok 10210, Thailand
Tel. (66) 2954-7300 www.dpu.ac.th

DPU
DHURAKIJ PUNDIT UNIVERSITY
มหาวิทยาลัยธุรกิจบัณฑิตย์

ที่ บช.0403(1)/0928

วันที่ 23 พฤศจิกายน 2565

เรื่อง ขอเรียนเชิญเป็นผู้ทรงคุณวุฒิตรวจสอบเครื่องมือวิจัย
เรียน เลขาธิการสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม
สิ่งที่ส่งมาด้วย 1. โครงการวิจัยและเครื่องมือวิจัย จำนวน 1 ชุด

ด้วย นายศิวกร รัตติโชติ นักศึกษาบัญชีมหาบัณฑิต วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์ ได้จัดทำวิจัยเรื่อง การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ในการนี้ หลักสูตรบัญชีมหาบัณฑิต วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์ จึงใคร่ขอเรียนเชิญ ดร. ภาสินี อภิศักดิ์มนตรี นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม บุคลากรในหน่วยงานของท่าน เป็นผู้ทรงคุณวุฒิตรวจสอบเครื่องมือวิจัยดังกล่าวตามรายละเอียดโครงการวิจัยและเครื่องมือวิจัยที่แนบมาพร้อมนี้ โดยจะขอรับเครื่องมือกลับคืนภายใน วันที่ 30 เดือน พฤศจิกายน 2565

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จะเป็นพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศิริเดช คำสุพรหม)
คณบดีวิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี

มหาวิทยาลัยธุรกิจบัณฑิตย์ 110/1-4 ถนนประชาชื่น เขตหลักสี่ กรุงเทพฯ 10210
Dhurakij Pundit University 110/1-4 Prachachuen Road, Laksi, Bangkok 10210, Thailand
Tel. (66) 2954-7300 www.dpu.ac.th

แบบตรวจสอบคุณภาพของเครื่องมือของผู้เชี่ยวชาญ
การหาค่าดัชนีความสอดคล้องของวัตถุประสงค์ (Index of Item Congruence: IOC)
เรื่อง การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ
ของคณะแพทยศาสตร์ศิริราชพยาบาล

คำชี้แจง:

1. แบบสอบถามฉบับนี้ มีวัตถุประสงค์หลักเพื่อศึกษาถึงองค์ประกอบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

2. แบบสอบถามฉบับนี้มุ่งตรวจสอบ เพื่อหาค่าความเที่ยงตรง (Validity) โดยการวิเคราะห์ดัชนีความสอดคล้อง (Index of item objective Congruence: IOC) ของแบบสอบถามและข้อเสนอแนะของผู้เชี่ยวชาญ เพื่อนำไปปรับปรุงแบบสอบถามให้สมบูรณ์ยิ่งขึ้น

3. แบบสอบถามฉบับนี้มีทั้งหมด 3 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

ส่วนที่ 2 กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ส่วนที่ 3 ข้อเสนอแนะ

4. ขอความกรุณาผู้ทรงคุณวุฒิหรือท่านผู้เชี่ยวชาญ ช่วยพิจารณาร่างแบบสอบถามว่ามีความสอดคล้องกับตัวแปรของการวิจัยเรื่องนี้หรือไม่ ด้วยการให้คะแนนในแต่ละข้อคำถามในระบบ IOC โดยการทำเครื่องหมาย ☑ ลงในช่องว่าง เกณฑ์การให้คะแนนในระบบ IOC

1. ให้ 1 คะแนน **เมื่อแน่ใจ**ว่าข้อนั้นมีเนื้อหาที่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา
2. ให้ 0 คะแนน **เมื่อไม่แน่ใจ**ว่าข้อนั้นมีเนื้อหาที่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา
3. ให้ -1 คะแนน **เมื่อแน่ใจ**ว่าข้อนั้นมีเนื้อหาไม่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

5. ผู้วิจัยขอความกรุณาท่านผู้ทรงคุณวุฒิและผู้เชี่ยวชาญ ให้ข้อเสนอแนะหรือความคิดเห็นเพิ่มเติมในประเด็นที่ยังไม่สมบูรณ์ โดยการเขียนข้อเสนอแนะไว้ท้ายข้อความนั้น ๆ

ผู้วิจัยขอขอบคุณในความกรุณาของท่านมา ณ โอกาสนี้

นายศิวกร รัตติโชติ
นักศึกษาปริญญาโท สาขาวิชาการบัญชี
วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิ

ส่วนที่ 1 ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย ☑ ลงในตาราง หน้าข้อความที่ตรงตามความเป็นจริง

คำชี้แจงสำหรับผู้เชี่ยวชาญ: โปรดพิจารณาว่าข้อความเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

ข้อ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
1	**เพศ** ☐ 1. ชาย ☐ 2. หญิง	1	1	1	1	ใช้ได้
2	**อายุ** ☐ 1. น้อยกว่า 20 ปี ☐ 2. 21 – 30 ปี ☐ 3. 31 - 40 ปี ☐ 4. 41 – 50 ปี ☐ 5. มากกว่า 50 ปี	1	1	1	1	ใช้ได้
3	**ระดับการศึกษา** ☐ 1. ต่ำกว่าปริญญาตรี ☐ 2. ปริญญาตรี ☐ 3. ปริญญาโท ☐ 4. ปริญญาเอก	1	1	1	1	ใช้ได้
4	**ตำแหน่ง** ☐ 1. เจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป ☐ 2. เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT ☐ 3. นักศึกษา ☐ 4. แพทย์/พยาบาล/เภสัชกร/นักสาธารสุข ☐ 5. หัวหน้างาน/ผู้บริหาร ☐ 6. อาจารย์/นักวิชาการ/นักวิจัย ☐ 7. อื่น ๆ (โปรดระบุ).....	1	1	1	1	ใช้ได้
5	**หน่วยงานที่ปฏิบัติงาน** ☐ 1. ฝ่ายการคลัง ☐ 2. ฝ่ายสารสนเทศ ☐ 3. หน่วยตรวจสอบภายใน ☐ 4. ฝ่ายทรัพยากรบุคคล ☐ 5. ฝ่ายนโยบายและแผน ☐ 6. ฝ่ายทรัพย์สินและพัสดุ	1	1	1	1	ใช้ได้

ข้อ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
	☐ 7. ฝ่ายวิศวกรรมบริการและอาคารสถานที่ ☐ 8. ฝ่ายวิจัย ☐ 9. ฝ่ายการพยาบาล ☐ 10. ฝ่ายเภสัชกรรม ☐ 11. ฝ่ายโภชนาการ ☐ 12. ภาควิชา (โปรดระบุ)..... ☐ 13. อื่น ๆ (โปรดระบุ).....					
6	**ประสบการณ์ทำงานในหน่วยงานปัจจุบัน (ถ้าเกิน 6 เดือนให้นับเป็น 1 ปี)** ☐ 1. น้อยกว่า 1 ปี ☐ 2. 1 – 5 ปี ☐ 3. 6 - 10 ปี ☐ 4. 11 – 15 ปี ☐ 5. 16 - 20 ปี ☐ 6. มากกว่า 20 ปี	1	1	1	1	ใช้ได้
7	**ระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ปัจจุบัน (สามารถตอบได้มากกว่า 1 ข้อ)** ☐ 1. ระบบสำนักงานอัตโนมัติ ☐ 2. ระบบประมวลผลรายการ ☐ 3. ระบบงานสร้างความรู้ ☐ 4. ระบบสารสนเทศเพื่อการจัดการ ☐ 5. ระบบสนับสนุนการตัดสินใจ ☐ 6. ระบบสารสนเทศสำหรับผู้บริหารระดับสูง ☐ 7. อื่น ๆ (โปรดระบุ).....	1	1	1	1	ใช้ได้
	รวม	**1**	**1**	**1**	**1**	**ใช้ได้**

ส่วนที่ 2 กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

คำชี้แจงของผู้ตอบแบบสอบถาม : โปรดทำเครื่องหมาย ☑ ลงในตารางข้อที่ตรงกับความคิดเห็นของหน่วยงานท่าน

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาข้อความเกี่ยวกับความคิดเห็น ว่าเหมาะสมหรือไม่ อย่างไร

ลำดับ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ						
1	มีการกำหนดกรอบการดำเนินงานด้านการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เช่น การบำรุงรักษาระบบ เครื่องมือเทคโนโลยีสารสนเทศ อุปกรณ์การเข้าใช้งานระบบสารสนเทศ เป็นต้น ให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง อยู่ในระดับใด	1	1	1	1	ใช้ได้
2	มีการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานให้มีความรวดเร็ว ข้อมูลมีความถูกต้องครบถ้วน และเป็นปัจจุบัน เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้ อยู่ในระดับใด	1	1	1	1	ใช้ได้
3	มีการมอบหมายภารกิจด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้กับผู้ปฏิบัติงานได้อย่างชัดเจน อยู่ในระดับใด	1	1	1	1	ใช้ได้
4	มีการจัดทำข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่อนุญาตให้บุคคลหรือหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน อยู่ในระดับใด	1	1	1	1	ใช้ได้
5	มีมาตรการด้านความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์พกพา เพื่อบริหารจัดการความเสี่ยงที่มีต่อ	1	1	1	1	ใช้ได้

ลำดับ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
	อุปกรณ์ดังกล่าว อยู่ในระดับใด					
6	มีการกำหนดข้อปฏิบัติในการใช้คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ เช่น เครื่องคอมพิวเตอร์แบบพกพาสมาร์ทโฟน เป็นต้น เพื่อให้มีความมั่นคงปลอดภัย และเกิดประสิทธิภาพต่อการใช้งาน อยู่ในระดับใด	1	1	1	1	ใช้ได้
7	มีการเก็บบันทึก และจำแนกประเภทของบัญชีทรัพย์สิน ข้อมูลสารสนเทศ เพื่อกำหนดระดับของการป้องกันทรัพย์สินด้านสารสนเทศ อยู่ในระดับใด	1	1	1	1	ใช้ได้
8	มีการจัดทำทะเบียน รับ – คืน รายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ อยู่ในระดับใด	1	1	1	1	ใช้ได้
9	มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ อยู่ในระดับใด	1	1	1	1	ใช้ได้
10	มีการจัดทำบันทึกข้อตกลงให้ผู้ปฏิบัติงานต้องรักษาทรัพย์สินให้ปลอดภัย และข้อมูลที่เป็นความลับ อยู่ในระดับใด	1	1	1	1	ใช้ได้
11	มีการรวบรวมข้อมูล ตรวจสอบ และประเมินผลการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศ ตามแนวทางการควบคุมภายในด้านการใช้งานระบบสารสนเทศของหน่วยงาน เพื่อระบุข้อบกพร่องในการใช้งานระบบ และนำมาปรับปรุงให้สามารถทำงานได้อย่างมีประสิทธิภาพ อยู่ในระดับใด	1	1	0	0.6667	ใช้ได้
12	มีขั้นตอน หรือแผนรองรับในการบริหารจัดการเหตุการณ์ผิดปกติ และปัญหาที่เกิดจากการใช้	1	1	1	1	ใช้ได้

ลำดับ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
	เทคโนโลยีสารสนเทศ พร้อมทั้งช่องทางการรายงานเหตุการณ์ปัญหาที่พบผิดปกติที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศ อย่างเหมาะสมและทันท่วงที อยู่ในระดับใด					
13	มีมาตรการป้องกันภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น เพื่อป้องกันไม่ให้ทรัพย์สินสารสนเทศเสียหาย อยู่ในระดับใด	1	1	1	1	ใช้ได้
14.	มีการป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ และเป้าหมายของงานที่รับผิดชอบ อยู่ในระดับใด	1	1	1	1	ใช้ได้
องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ						
15	มีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก อยู่ในระดับใด	1	1	1	1	ใช้ได้
16	มีการกำหนดขั้นตอน ควบคุมการตรวจสอบป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ อยู่ในระดับใด	1	1	1	1	ใช้ได้
17	มีการรักษาความมั่งคงของแม่ข่าย (Server) และอุปกรณ์ที่ใช้งานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่พึงประสงค์ดี (Malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหล ของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต อยู่ในระดับใด	1	0	1	0.6667	ใช้ได้
18	มีการจัดทำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไว้ในเงื่อนไขการจ้างพัฒนา	1	1	1	1	ใช้ได้

ลำดับ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
	หรือปรับปรุงระบบ เช่น เอกสารรายละเอียดคุณสมบัติทางเทคนิค ในการจัดซื้อจัดจ้างโดยครอบคลุมถึงเรื่องรักษาความมั่นคงปลอดภัย อยู่ในระดับใด					
19	มีการดูแล ควบคุม ติดตามตรวจสอบการพัฒนาระบบสารสนเทศ โดยหน่วยงานภายนอก รวมถึงการจ้างช่วงพัฒนาระบบ อยู่ในระดับใด	1	1	1	1	ใช้ได้
20	มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงาน ต้องปฏิบัติตามสัญญาหรือข้อตกลงในการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ อยู่ในระดับใด	1	1	1	1	ใช้ได้
21	มีการจ้างผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจในการร่วมพัฒนา มีการคำนึงถึงความต่อเนื่องในการดำเนินธุรกิจ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และการยกเลิกหรือสิ้นสุดสัญญา (Exit Strategy) อยู่ในระดับใด	1	1	1	1	ใช้ได้
22	มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์หรือธุรกรรมออนไลน์กับบุคคลหรือหน่วยงานภายนอก (เช่น การสั่งซื้อ/ขายสินค้าหรือบริการผ่านระบบอิเล็กทรอนิกส์ การชำระเงินผ่านระบบอิเล็กทรอนิกส์) เป็นต้น อยู่ในระดับใด	1	1	1	1	ใช้ได้
23	มีการกำหนดให้มีการเข้าใช้งานระบบสารสนเทศตามมาตรการเข้ารหัสข้อมูล	1	1	1	1	ใช้ได้

ลำดับ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
	(Cryptography) และการบริหารจัดการกุญแจ (Access Key) เป็นต้น อยู่ในระดับใด					
24	มีการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงาน สอดคล้องกับชั้นความลับของสารสนเทศ อยู่ในระดับใด	1	1	1	1	ใช้ได้
องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ						
25	มีการบำรุงรักษาและดูแลอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน อยู่ในระดับใด	1	1	1	1	ใช้ได้
26	มีการจัดทำ และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบต่าง ๆ เพื่อให้ผู้ปฏิบัติงานสามารถนำไปปฏิบัติได้อย่างถูกต้องและปลอดภัย อยู่ในระดับใด	1	0	1	0.6667	ใช้ได้
27	มีการกำหนดให้ผู้ปฏิบัติงานหรือบุคคลภายนอกที่หน่วยงานว่าจ้างจะต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย และบทลงโทษ ในกรณีที่ผู้ปฏิบัติงานฝ่าฝืนนโยบายหรือระเบียบที่หน่วยงานประกาศใช้อย่างชัดเจน อยู่ในระดับใด	1	1	1	1	ใช้ได้
28	มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้เป็นปัจจุบันโดยเฉพาะเมื่อมีการเปลี่ยนแปลง	1	1	1	1	ใช้ได้

ลำดับ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
	ตำแหน่งงานหรือสิ้นสุดการจ้างงาน อยู่ในระดับใด					
29	มีการกำหนดให้เจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงาน เมื่อสิ้นสุดการจ้างงาน อยู่ในระดับใด	1	1	1	1	ใช้ได้
30	มีการพัฒนา อบรม เพิ่มพูน ทักษะและความสามารถของผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับใด	1	1	1	1	ใช้ได้
องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์						
31	มีการกำหนดกลยุทธ์เพื่อการบริหารงานของหน่วยงาน โดยการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินงานสอดคล้องกับนโยบาย บทบาท ภารกิจของหน่วยงาน และระบบความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับใด	1	1	1	1	ใช้ได้
32	มีการกำหนดนโยบายและแนวทางสำหรับความมั่นคงปลอดภัยด้านสารสนเทศเพื่อควบคุม และป้องกันความเสี่ยงด้านสารสนเทศเป็นลายลักษณ์อักษร และประกาศหรือแจ้งนโยบายดังกล่าวให้ผู้ปฏิบัติงานรับทราบทั่วกัน อยู่ในระดับใด	1	1	1	1	ใช้ได้
33	มีการวิเคราะห์ความเสี่ยง (Risk analysis) และประเมินค่าความเสี่ยง (Risk Evaluation) เพื่อประเมินระดับผลกระทบและโอกาสเกิดเหตุการณ์ และจัดลำดับความเสี่ยงในการจัดการด้านสารสนเทศของหน่วยงาน อยู่ในระดับใด	1	0	1	0.6667	ใช้ได้
34	มีการจัดการความเสี่ยง (Risk Treatment) กำหนดแนวทาง ติดตาม ทบทวน และ	1	1	1	1	ใช้ได้

ลำดับ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
	ประเมินความเสี่ยงที่เกิดขึ้นด้านสารสนเทศ เช่น ด้านข้อมูล ด้านอุปกรณ์เทคโนโลยีสารสนเทศ ด้านซอฟแวร์คอมพิวเตอร์ เป็นต้น อย่างสม่ำเสมอ อยู่ในระดับใด					
35	มีการรายงานผลการบริหารความเสี่ยงด้านสารสนเทศ และแนวโน้มของความเสี่ยงที่อาจจะเกิดขึ้นตามนโยบายที่กำหนดให้ท่านทราบ อยู่ในระดับใด	1	1	1	1	ใช้ได้
	รวม		**0.9143**	**0.9714**	**0.9619**	**ใช้ได้**

ตอนที่ 3 ข้อเสนอแนะ

คำชี้แจงของผู้ตอบแบบสอบถาม : กรุณาแสดงความคิดเห็นที่ตรงกับความคิดเห็นของท่านมากที่สุด

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาความเหมาะสมของข้อคำถาม

ลำดับ	ข้อคำถาม	ประมาณค่าความคิดเห็นผู้เชี่ยวชาญ			ค่า IOC	แปลผล
		1	2	3		
1	ท่านมีข้อเสนอแนะที่ต้องการได้รับการสนับสนุนจากหน่วยงาน	1	1	1	1	ใช้ได้
2	ท่านมีข้อเสนอแนะเพื่อเป็นการพัฒนาการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	1	1	1	1	ใช้ได้
3	ข้อเสนอแนะอื่น ๆ	1	1	1	1	ใช้ได้
	รวม	**1**	**1**	**1**	**1**	**ใช้ได้**

ภาคผนวก ค

ผลการทดสอบความเชื่อมั่น (Reliability) ด้วย

Cronbach’s Alpha Method

ผลการทดสอบความเชื่อมั่น (Reliability) ด้วย Cronbach’s Alpha Method

ข้อคำถาม	Cronbach's Alpha if Item Deleted
องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	
ข้อ 1	0.986
ข้อ 2	0.986
ข้อ 3	0.986
ข้อ 4	0.986
ข้อ 5	0.987
ข้อ 6	0.986
ข้อ 7	0.986
ข้อ 8	0.986
ข้อ 9	0.987
ข้อ 10	0.985
ข้อ 11	0.985
ข้อ 12	0.986
ข้อ 13	0.986
ข้อ 14	0.986
องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	
ข้อ 15	0.986
ข้อ 16	0.985
ข้อ 17	0.985
ข้อ 18	0.985
ข้อ 19	0.985
ข้อ 20	0.986
ข้อ 21	0.986
ข้อ 22	0.985
ข้อ 23	0.985

ข้อคำถาม	Cronbach's Alpha if Item Deleted
ข้อ 24	0.985
องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ	
ข้อ 25	0.985
ข้อ 26	0.985
ข้อ 27	0.986
ข้อ 28	0.985
ข้อ 29	0.985
ข้อ 30	0.987
องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์	
ข้อ 31	0.986
ข้อ 32	0.985
ข้อ 33	0.986
ข้อ 34	0.986
ข้อ 35	0.985
รวม	**0.986**

ภาคผนวก ง

แบบสอบถามเพื่อการวิจัย

เอกสารหมายเลข.....

แบบสอบถามเพื่อการวิจัย

เรื่อง การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

ของคณะแพทยศาสตร์ศิริราชพยาบาล

คำชี้แจง: แบบสอบถามชุดนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรบัญชีมหาบัณฑิต สาขาวิชาการบัญชี วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิต โดยมีวัตถุประสงค์หลักเพื่อศึกษาถึงองค์ประกอบการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล โดยข้อมูลที่ได้จะเก็บเป็นความลับ และจะไม่นำข้อมูลที่ท่านให้ไปก่อให้เกิดความเสียหายใด ๆ ทั้งทางตรงและทางอ้อม

จึงขอความกรุณาผู้ได้รับแบบสอบถามตอบแบบสอบถามตามความเป็นจริง และโอกาสนี้ผู้วิจัยขอขอบพระคุณผู้ตอบแบบสอบถามทุกท่านเป็นอย่างสูง ที่ให้ความร่วมมือในการตอบแบบสอบถามในครั้งนี้

แบบสอบถามแบ่งออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

ส่วนที่ 2 กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

ส่วนที่ 3 ข้อเสนอแนะ

ส่วนที่ 1 ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย ☑ ลงในตาราง หน้าข้อความที่ตรงตามความเป็นจริง

1. เพศ

☐ 1. ชาย ☐ 2. หญิง

2. อายุ

☐ 1. น้อยกว่า 20 ปี ☐ 2. 21 – 30 ปี ☐ 3. 31 - 40 ปี

☐ 4. 41 – 50 ปี ☐ 5. มากกว่า 50 ปี

3. ระดับการศึกษา

☐ 1. ต่ำกว่าปริญญาตรี ☐ 2. ปริญญาตรี ☐ 3. ปริญญาโท

☐ 4. ปริญญาเอก

4. ตำแหน่ง

☐ 1. เจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป ☐ 2. เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT

☐ 3. นักศึกษา ☐ 4. แพทย์/พยาบาล/เภสัชกร/นักสาธารสุข

☐ 5. หัวหน้างาน/ผู้บริหาร ☐ 6. อาจารย์/นักวิชาการ/นักวิจัย

☐ 7. อื่น ๆ (โปรดระบุ).....

5. หน่วยงานที่ปฏิบัติงาน

☐ 1. ฝ่ายการคลัง ☐ 2. ฝ่ายสารสนเทศ ☐ 3. หน่วยตรวจสอบภายใน
☐ 4. ฝ่ายทรัพยากรบุคคล ☐ 5. ฝ่ายนโยบายและแผน ☐ 6. ฝ่ายทรัพย์สินและพัสดุ
☐ 7. ฝ่ายวิศวกรรมบริการและอาคารสถานที่ ☐ 8. ฝ่ายวิจัย ☐ 9. ฝ่ายการพยาบาล
☐ 10. ฝ่ายเภสัชกรรม ☐ 11. ฝ่ายโภชนาการ
☐ 12. ภาควิชา (โปรดระบุ).....
☐ 13. อื่น ๆ (โปรดระบุ).....

6. ประสบการณ์ทำงานในหน่วยงานปัจจุบัน (ถ้าเกิน 6 เดือนให้นับเป็น 1 ปี)

☐ 1. น้อยกว่า 1 ปี ☐ 2. 1 – 5 ปี ☐ 3. 6 - 10 ปี
☐ 4. 11 – 15 ปี ☐ 5. 16 - 20 ปี ☐ 6. มากกว่า 20 ปี

7. ระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ปัจจุบัน (สามารถตอบได้มากกว่า 1 ข้อ)

☐ 1. ระบบสำนักงานอัตโนมัติ ☐ 2. ระบบประมวลผลรายการ
☐ 3. ระบบงานสร้างความรู้
☐ 4. ระบบสารสนเทศเพื่อการจัดการ ☐ 5. ระบบสนับสนุนการตัดสินใจ
☐ 6. ระบบสารสนเทศสำหรับผู้บริหารระดับสูง
☐ 7. อื่น ๆ (โปรดระบุ).....

ส่วนที่ 2 กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล

คำชี้แจง โปรดทำเครื่องหมาย ☑ ลงในตารางข้อที่ตรงกับความคิดเห็นของหน่วยงานท่าน

ลำดับ	กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศ	ระดับความคิดเห็น				
		5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
องค์ประกอบที่ 1 การกำกับดูแลการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ						
1	มีการกำหนดกรอบการดำเนินงานด้านการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เช่น การบำรุงรักษาระบบ เครื่องมือเทคโนโลยีสารสนเทศ อุปกรณ์การเข้าใช้งานระบบสารสนเทศ เป็นต้น ให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง อยู่ในระดับใด					
2	มีการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานให้มีความรวดเร็ว ข้อมูลมีความถูกต้อง					

ลำดับ	กระบวนการบริหารจัดการความมั่งคงปลอดภัย ด้านสารสนเทศ	ระดับความคิดเห็น				
		5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
	ครบถ้วน และเป็นปัจจุบัน เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้ อยู่ในระดับใด					
3	มีการมอบหมายภารกิจด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้กับผู้ปฏิบัติงานได้อย่างชัดเจน อยู่ในระดับใด					
4	มีการจัดทำข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่อนุญาตให้บุคคลหรือหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน อยู่ในระดับใด					
5	มีมาตรการด้านความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์พกพา เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว อยู่ในระดับใด					
6	มีการกำหนดข้อปฏิบัติในการใช้คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ เช่น เครื่องคอมพิวเตอร์แบบพกพา สมาร์ทโฟน เป็นต้น เพื่อให้มีความมั่นคงปลอดภัยและเกิดประสิทธิภาพต่อการใช้งาน อยู่ในระดับใด					
7	มีการเก็บบันทึก และจำแนกประเภทของบัญชีทรัพย์สินข้อมูลสารสนเทศ เพื่อกำหนดระดับของการป้องกันทรัพย์สินด้านสารสนเทศ อยู่ในระดับใด					
8	มีการจัดทำทะเบียน รับ – คืนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ อยู่ในระดับใด					
9	มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ อยู่ในระดับใด					
10	มีการจัดทำบันทึกข้อตกลงให้ผู้ปฏิบัติงานต้องรักษาทรัพย์สินให้ปลอดภัย และข้อมูลที่เป็นความลับ อยู่ในระดับใด					
11	มีการรวบรวมข้อมูล ตรวจสอบ และประเมินผลการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศตามแนวทางการควบคุมภายในด้านการใช้งานระบบ					

ลำดับ	กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศ	ระดับความคิดเห็น				
		5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
	สารสนเทศของหน่วยงาน เพื่อระบุข้อบกพร่องในการใช้งานระบบ และนำมาปรับปรุงให้สามารถทำงานได้อย่างมีประสิทธิภาพ อยู่ในระดับใด					
12	มีขั้นตอน หรือแผนรองรับในการบริหารจัดการเหตุการณ์ผิดปกติ และปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ พร้อมทั่งช่องทางการรายงานเหตุการณ์ปัญหาที่พบผิดปกติที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศ อย่างเหมาะสมและทันท่วงที อยู่ในระดับใด					
13	มีมาตรการป้องกันภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น เพื่อป้องกันไม่ให้ทรัพย์สินสารสนเทศเสียหาย อยู่ในระดับใด					
14	มีการป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์และเป้าหมายของงานที่รับผิดชอบ อยู่ในระดับใด					
องค์ประกอบที่ 2 การดำเนินงานและการบำรุงรักษาระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ						
15	มีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก อยู่ในระดับใด					
16	มีการกำหนดขั้นตอน ควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ อยู่ในระดับใด					
17	มีการรักษาความมั่งคงของแม่ข่าย (Server) และอุปกรณ์ที่ใช้งานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่พึงประสงค์ดี (Malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหล ของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต อยู่ในระดับใด					
18	มีการจัดทำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไว้ในเงื่อนไขการจ้างพัฒนาหรือปรับปรุงระบบ เช่น					

ลำดับ	กระบวนการบริหารจัดการความมั่งคงปลอดภัย ด้านสารสนเทศ	ระดับความคิดเห็น				
		5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
	เอกสารรายละเอียดคุณสมบัติทางเทคนิค ในการจัดซื้อจัดจ้างโดยครอบคลุมถึงเรื่องรักษาความมั่นคงปลอดภัย อยู่ในระดับใด					
19	มีการดูแล ควบคุม ติดตามตรวจสอบการพัฒนาระบบสารสนเทศ โดยหน่วยงานภายนอก รวมถึงการจ้างช่วงพัฒนาระบบ อยู่ในระดับใด					
20	มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงาน ต้องปฏิบัติตามสัญญาหรือข้อตกลงในการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ อยู่ในระดับใด					
21	มีการจ้างผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจในการร่วมพัฒนา มีการคำนึงถึงความต่อเนื่องในการดำเนินธุรกิจ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และการยกเลิกหรือสิ้นสุดสัญญา (Exit Strategy) อยู่ในระดับใด					
22	มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ หรือธุรกรรมออนไลน์กับบุคคลหรือหน่วยงานภายนอก (เช่น การสั่งซื้อ/ขายสินค้าหรือบริการผ่านระบบอิเล็กทรอนิกส์ การชำระเงินผ่านระบบอิเล็กทรอนิกส์) เป็นต้น อยู่ในระดับใด					
23	มีการกำหนดให้มีการเข้าใช้งานระบบสารสนเทศตามมาตรการเข้ารหัสข้อมูล (Cryptography) และการบริหารจัดการกุญแจ (Access Key) เป็นต้น อยู่ในระดับใด					
24	มีการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงานสอดคล้องกับชั้นความลับของสารสนเทศ อยู่ในระดับใด					

ลำดับ	กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศ	ระดับความคิดเห็น				
		5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
องค์ประกอบที่ 3 การพัฒนา และการบริหารจัดการความต่อเนื่องทางธุรกิจในความมั่นคงปลอดภัยด้านสารสนเทศ						
25	มีการบำรุงรักษาและดูแลอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน อยู่ในระดับใด					
26	มีการจัดทำ และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบต่าง ๆ เพื่อให้ผู้ปฏิบัติงานสามารถนำไปปฏิบัติได้อย่างถูกต้องและปลอดภัย อยู่ในระดับใด					
27	มีการกำหนดให้ผู้ปฏิบัติงานหรือบุคคลภายนอกที่หน่วยงานว่าจ้างจะต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย และบทลงโทษ ในกรณีที่ผู้ปฏิบัติงานฝ่าฝืนนโยบายหรือระเบียบที่หน่วยงานประกาศใช้อย่างชัดเจน อยู่ในระดับใด					
28	มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน อยู่ในระดับใด					
29	มีการกำหนดให้เจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อสิ้นสุดการจ้างงาน อยู่ในระดับใด					
30	มีการพัฒนา อบรม เพิ่มพูน ทักษะและความสามารถของผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับใด					
องค์ประกอบที่ 4 นโยบายและการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเชิงกลยุทธ์						
31	มีการกำหนดกลยุทธ์เพื่อการบริหารงานของหน่วยงานโดยการนำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินงานสอดคล้องกับนโยบาย บทบาท ภารกิจของหน่วยงาน และระบบความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับใด					

ลำดับ	กระบวนการบริหารจัดการความมั่งคงปลอดภัยด้านสารสนเทศ	ระดับความคิดเห็น				
		5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
32	มีการกำหนดนโยบายและแนวทางสำหรับความมั่นคงปลอดภัยด้านสารสนเทศเพื่อควบคุม และป้องกันความเสี่ยงด้านสารสนเทศเป็นลายลักษณ์อักษร และประกาศหรือแจ้งนโยบายดังกล่าวให้ผู้ปฏิบัติงานรับทราบทั่วกัน อยู่ในระดับใด					
33	มีการวิเคราะห์ความเสี่ยง (Risk analysis) และประเมินค่าความเสี่ยง (Risk Evaluation) เพื่อประเมินระดับผลกระทบและโอกาสเกิดเหตุการณ์ และจัดลำดับความเสี่ยงในการจัดการด้านสารสนเทศของหน่วยงานอยู่ในระดับใด					
34.	มีการจัดการความเสี่ยง (Risk Treatment) กำหนดแนวทาง ติดตาม ทบทวน และประเมินความเสี่ยงที่เกิดขึ้นด้านสารสนเทศ เช่น ด้านข้อมูล ด้านอุปกรณ์เทคโนโลยีสารสนเทศ ด้านซอฟแวร์คอมพิวเตอร์ เป็นต้น อย่างสม่ำเสมอ อยู่ในระดับใด					
35	มีการรายงานผลการบริหารความเสี่ยงด้านสารสนเทศและแนวโน้มของความเสี่ยงที่อาจจะเกิดขึ้นตามนโยบายที่กำหนดให้ท่านทราบ อยู่ในระดับใด					

ส่วนที่ 3 ข้อเสนอแนะ

1. ท่านมีข้อเสนอแนะที่ต้องการได้รับการสนับสนุนจากหน่วยงาน

.....

.....

2. ท่านมีข้อเสนอแนะเพื่อเป็นการพัฒนาการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

.....

.....

3. ข้อเสนอแนะอื่น ๆ

.....

.....

ขอบคุณครับ

ภาคผนวก จ

จริยธรรมการวิจัยในมนุษย์

DPU DHURAKIJ PUNDIT UNIVERSITY มหาวิทยาลัยธุรกิจบัณฑิตย์

บันทึก

Memorandum

ที่ DPUHREC 1101/2565 วันที่ 23 ธันวาคม 2565

จาก สำนักงานคณะกรรมการจริยธรรมการวิจัยในมนุษย์ มหาวิทยาลัยธุรกิจบัณฑิตย์

เรียน คุณศิวกร รัตติโชติ

เรื่อง แจ้งผลการประเมินตนเองเกี่ยวกับจริยธรรมการวิจัยในมนุษย์

ตามที่ นายศิวกร รัตติโชติ นักศึกษาระดับมหาบัณฑิต สาขาการบัญชี วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์ ได้ขอความอนุเคราะห์ให้ทางสำนักงานคณะกรรมการจริยธรรมการวิจัยในมนุษย์ฯ พิจารณาผลการประเมินตนเองเกี่ยวกับจริยธรรมการวิจัยในมนุษย์ ของโครงการวิจัยเรื่อง การศึกษาองค์ประกอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล จากการตรวจสอบเบื้องต้นโดยพิจารณาจาก แบบตรวจสอบ IRB Checklist DPUHREC โครงร่างการวิจัย และแบบสอบถามที่ใช้เก็บข้อมูลของโครงการวิจัย ทางคณะกรรมการจริยธรรมการวิจัยในมนุษย์ฯ ได้พิจารณาแล้วเห็นว่า การดำเนินงานวิจัยข้างต้น เข้าข่ายการได้รับยกเว้นการประเมินจริยธรรมการวิจัยในมนุษย์ (exemption review)

ทั้งนี้ผลการพิจารณาเอกสารดังกล่าวข้างต้น ไม่ถือเป็นการรับรองจริยธรรมการวิจัยในมนุษย์ เนื่องจากคณะกรรมการฯ จะไม่ให้การรับรองโครงการย้อนหลัง กรณีที่โครงการได้ดำเนินการไปแล้ว

จึงเรียนมาเพื่อโปรดทราบ

(รองศาสตราจารย์ ดร.พยงค์ วณิเกียรติ)

ประธานคณะกรรมการจริยธรรมการวิจัยในมนุษย์

โทร. 128, 632

สำนักงานคณะกรรมการจริยธรรมการวิจัยในมนุษย์ มหาวิทยาลัยธุรกิจบัณฑิตย์ (DPUHREC)

ประวัติผู้เขียน

ชื่อ – นามสกุล ศิวกร รัตติโชติ

ประวัติการศึกษา

พ.ศ. 2554 - ปริญญาตรี ศิลปศาสตรบัณฑิต (รัฐศาสตร์)
มหาวิทยาลัยรามคำแหง

พ.ศ. 2551 - ปริญญาตรี บริหารธุรกิจบัณฑิต เกียรตินิยมอันดับ 2 (ธุรกิจระหว่างประเทศ)
มหาวิทยาลัยเกษตรศาสตร์

ตำแหน่งและสถานที่ทำงาน

นักวิชาการศึกษาชำนาญการพิเศษ
สำนักทดสอบทางการศึกษา
สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน