การจัดทำแนวทางการตรวจสอบภายในตามมาตรฐาน ISO 27001 : 2013 กรณีศึกษาการทางพิเศษแห่งประเทศไทย

PREPARATION OF ISO 27001 : 2013 INTERNAL AUDIT GUIDELINES CASE STUDY OF EXPRESSWAY AUTHORITY OF THAILAND

ภัทราพร โชติมหา

PATARAPORN CHOTIMAHA

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
พ.ศ. 2561

การจัดทำแนวทางการตรวจสอบภายในตามมาตรฐาน ISO 27001 : 2013 กรณีศึกษาการทางพิเศษแห่งประเทศไทย

ภัทราพร โชติมหา

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
พ.ศ. 2561

PREPARATION OF ISO 27001 : 2013 INTERNAL AUDIT GUIDELINES CASE STUDY EXPRESSWAY AUTHORITY OF THAILAND

PATARAPORN CHOTIMAHA

A THEMATIC SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF MASTER

OF SCIENCE IN INFORMATION TECHNOLOGY

SCHOOL OF INFORMATION TECHNOLOGY

SRIPATUM UNIVERSITY

2018

สารนิพนธ์เรื่อง การจัดทำแนวทางการตรวจสอบภายในตามมาตรฐาน ISO 27001 : 2013 กรณีศึกษาการทางพิเศษแห่งประเทศไทย

คำสำคัญ แนวทางการตรวจสอบ/มาตรฐาน ISO 27001

นักศึกษา ภัทราพร โชติมหา

อาจารย์ที่ปรึกษาสารนิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย

หลักสูตร วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะ เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

พ.ศ. 2561

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อทำการศึกษามาตรฐาน ISO 27001 เพื่อจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศสำหรับผู้ตรวจสอบภายในให้สอดคล้องกับแนวทางตามมาตรฐาน ISO 27001 และสอดคล้องกับการดำเนินงานของการทางพิเศษแห่งประเทศไทย ทำให้ผู้ตรวจสอบภายในมีแนวทางการตรวจสอบที่เป็นมาตรฐานสากล และเป็นไปในแนวทางเดียวกัน ส่งผลให้เกิดประสิทธิภาพในการตรวจสอบเทคโนโลยีสารสนเทศมากยิ่งขึ้น และทำให้มั่นใจได้ยิ่งขึ้นว่าการดำเนินงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศขององค์กรมีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศตามมาตรฐานสากล โดยการประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศจากผู้ตรวจสอบภายใน มีผลความพึงพอใจโดยรวมด้านรูปแบบ เนื้อหา และการนำไปประยุกต์ใช้งาน เท่ากับ 4.22 ส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.33 ซึ่งอยู่ในระดับมาก

THEMATIC TITLE	PREPARATION OF ISO 27001 : 2013 INTERNAL AUDIT GUIDELINES CASE STUDY OF EXPRESSWAY AUTHORITY OF THAILAND
KEYWORDS	AUDIT GUIDELINES/ISO 27001 STANDARD
STUDENT	PATRAPORN CHOTMAHA
ADVISOR	ASS.PROF.DR. NIVET CHIRAWICHITCHAI
LEVEL OF STUDY	MASTER OF SCIENCE INFORMATION TECHNOLOGY
FACULTY	SCHOOL OF INFORMATION TECHNOLOGY SRIPATUM UNIVERSITY
YEAR	2018

ABSTRACT

The purpose of this research was to study ISO 27001 as the guideline to prepare information technology audit program for internal auditor based on ISO 27001 and consistent with the operation of Expressway Authority of Thailand. The internal auditor have standard guideline audit program and same guideline, which add efficiency information technology and add assurance to information technology operation about information security on base international standard. The evaluating satisfaction of information technology audit program from internal auditor. Found that the evaluation of the overall satisfaction in format, content and audit program can be applied to use was 4.22, standard deviation was 0.33, which was at a high level.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี เนื่องด้วยผู้วิจัยได้รับความกรุณาเป็นอย่างยิ่งจากผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย อาจารย์ที่ปรึกษาสารนิพนธ์ที่ได้ให้ความกรุณาสละเวลาอันมีค่าให้คำแนะนำความรู้อันเป็นประโยชน์อย่างอเนกประการ รวมถึงให้คำปรึกษาเพื่อนำไปสู่การแก้ไขปัญหาและข้อบกพร่องต่าง ๆ ที่เกิดขึ้นในการทำวิจัยตั้งแต่เริ่มต้นจนกระทั่งจัดทำสารนิพนธ์สำเร็จเป็นรูปเล่ม ผู้วิจัยรู้สึกซาบซึ้งและขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ผู้วิจัยขอกราบขอบพระคุณคณาจารย์ทุกท่านที่ประสิทธิ์ประสาทวิชาความรู้จนสามารถสำเร็จการศึกษาในระดับมหาบัณฑิตและขอขอบคุณผู้ที่เกี่ยวข้องกับงานวิจัยนี้ที่ให้ความช่วยเหลือและอนุเคราะห์ในการตอบแบบสอบถามในครั้งนี้เป็นอย่างดี เพื่อให้ได้ข้อมูลที่เป็นประโยชน์ต่อการศึกษาและผู้ที่ผู้วิจัยได้กล่าวอ้างอิงในสารนิพนธ์ฉบับนี้ทุกท่าน

สุดท้ายนี้ผู้วิจัยขอมอบความสำเร็จครั้งนี้แด่คุณพ่อ คุณแม่ สามี และบุตรชายที่สนับสนุนในทุก ๆ ด้าน และให้กำลังใจมาโดยตลอด ซึ่งทำให้ผู้วิจัยสามารถทุ่มเทเวลาในการศึกษาและจัดทำสารนิพนธ์ฉบับนี้ได้อย่างลุล่วง และหวังเป็นอย่างยิ่งว่า สารนิพนธ์ฉบับนี้จะเป็นจะเป็นประโยชน์แด่ผู้ที่ต้องการศึกษาด้านการตรวจสอบระบบเทคโนโลยีสารสนเทศ และหากมีข้อผิดพลาดประการใดในสารนิพนธ์ฉบับนี้ ผู้วิจัยต้องกราบขออภัยเป็นอย่างสูงมา ณ ที่นี้ด้วย

ภัทราพร โชติมหา

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

ISO 27001 เป็นมาตรฐานการบริหารจัดการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ได้รับการยอมรับระดับสากล มุ่งเน้นการรักษาความปลอดภัยของข้อมูลสารสนเทศตามระดับความเสี่ยงด้านการรักษาความลับ การรักษาความถูกต้องสมบูรณ์ และความพร้อมใช้งาน โดยมีแนวทางบริหารจัดการให้ข้อมูลสารสนเทศขององค์กรสามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ ข้อมูลสารสนเทศมีความถูกต้อง ครบถ้วน สมบูรณ์ไม่ถูกเปลี่ยนแปลงหรือแก้ไขจากผู้ที่ไม่ได้รับอนุญาต และข้อมูลสารสนเทศมีความพร้อมที่จะให้ผู้มีสิทธิเข้าใช้งานอยู่เสมอ หากองค์กรต่าง ๆ นำมาตรฐาน ISO 27001 มาประยุกต์ใช้ในการดำเนินงานจะสามารถทำให้ผู้มีส่วนได้ส่วนเสียเกิดความมั่นใจในความมั่นคงปลอดภัยของข้อมูลสารสนเทศมากยิ่งขึ้น เนื่องจากการดำเนินงานตามมาตรฐาน ISO 27001 จะช่วยปกป้องข้อมูลสารสนเทศขององค์กรจากความเสี่ยงของภัยคุกคามต่าง ๆ ไม่ว่าจะเป็นไวรัสคอมพิวเตอร์ที่ทำให้ข้อมูลสารสนเทศเสียหาย การบุกรุกระบบเพื่อขโมย ข้อมูลสารสนเทศ การบุกรุกระบบเพื่อเปลี่ยนแปลงข้อมูลสารสนเทศ หรือความเสียหายที่เกิดจากความไม่ตั้งใจของผู้ใช้งานในระบบ ฯลฯ ซึ่งส่งผลกระทบต่อการดำเนินงานขององค์กร สร้างความเสียหายด้านรายได้ เวลา ภาพลักษณ์ และความน่าเชื่อถือขององค์กร

ปัจจุบันการทางพิเศษแห่งประเทศไทยมีการใช้งานเทคโนโลยีสารสนเทศจำนวนมากเพื่อใช้ในการดำเนินงานและให้บริการผู้ใช้บริการทางพิเศษ ประกอบกับเทคโนโลยีมีความก้าวหน้าอย่างรวดเร็ว ซึ่งก่อให้เกิดภัยคุกคามด้านความมั่นคงปลอดภัยขึ้นอย่างรวดเร็วเช่นกัน การทางพิเศษแห่งประเทศไทยเป็นองค์กรที่ถูกจัดให้เป็นโครงสร้างที่สำคัญของประเทศ ดังนั้น เพื่อให้มั่นใจว่าองค์กรมีการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่เหมาะสม การตรวจสอบภายในเป็นเครื่องมือหรือผู้ช่วยที่สำคัญในการสร้างความเชื่อมั่นให้กับผู้บริหาร โดยการตรวจสอบประเมินประสิทธิภาพและประสิทธิผลการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ผู้วิจัยซึ่งปฏิบัติงานอยู่ในสายงานตรวจสอบภายในขององค์กรจึงมีแนวคิดที่จะจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ โดยอิงตามมาตรฐาน ISO 27001 เพื่อให้ผู้ตรวจสอบภายในที่ส่วนใหญ่ไม่มีพื้นฐานทางด้านเทคโนโลยีสารสนเทศมีแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศที่เป็นมาตรฐานสากลและเหมาะสมกับองค์กร รวมทั้ง การที่ผู้ตรวจสอบภายในปฏิบัติงานตรวจสอบระบบเทคโนโลยีสารสนเทศ โดยใช้แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศที่สอดคล้องตามมาตรฐาน ISO 27001 จะส่งผลให้ข้อมูลสารสนเทศ

ขององค์กรมีความมั่นคงปลอดภัยยิ่งขึ้น เนื่องจากผู้บริหาร พนักงานทั่วไป และพนักงานด้านเทคโนโลยีสารสนเทศมีความตระหนักรู้ และธำรงรักษาการปฏิบัติงานให้สอดคล้องเป็นไปตามมาตรฐาน ISO 27001

1.2 วัตถุประสงค์ของการวิจัย

1. ศึกษามาตรฐาน ISO 27001 : 2013 เพื่อจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศสำหรับผู้ตรวจสอบภายใน การทางพิเศษแห่งประเทศไทย
2. ได้แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศที่สอดคล้องกับมาตรฐาน ISO 27001 : 2013 ไปใช้ในการปฏิบัติงานตรวจสอบ สำหรับการทางพิเศษแห่งประเทศไทย

1.3 ขอบเขตของการวิจัย

งานวิจัยนี้เป็นการศึกษามาตรฐาน ISO 27001 : 2013 เพื่อจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามข้อกำหนดในมาตรฐาน โดยแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ ประกอบด้วยหัวข้อการตรวจสอบ วัตถุประสงค์การตรวจสอบ และวิธีการตรวจสอบ

1.4 ประโยชน์ที่คาดว่าจะได้รับ

การที่หน่วยตรวจสอบภายในมีแนวทางการตรวจสอบภายในที่สอดคล้องกับมาตรฐาน ISO 27001 : 2013 ไปใช้ในการปฏิบัติงานตรวจสอบ ผู้วิจัยคาดว่าจะองค์กรจะได้รับประโยชน์ ดังนี้

1. องค์กรมีการดำเนินงานด้านเทคโนโลยีสารสนเทศสอดคล้องกับมาตรฐาน ISO 27001 : 2013
2. ช่วยลดความสูญเสียหรือความเสียหายจากภัยคุกคามด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นกับข้อมูลสารสนเทศขององค์กร
3. ข้อมูลสารสนเทศขององค์กรได้รับการปกป้องให้มีความถูกต้อง สมบูรณ์ และมีความพร้อมใช้งาน
4. ระบบสารสนเทศขององค์กรมีความพร้อมในการให้บริการอยู่เสมอ
5. ช่วยยกระดับความมั่นคงปลอดภัย และความน่าเชื่อถือด้านข้อมูลสารสนเทศให้กับองค์กร

บทที่ 2
แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่องการศึกษามาตรฐาน ISO 27001 เพื่อจัดทำแนวทางการตรวจสอบเทคโนโลยีสารสนเทศของผู้ตรวจสอบภายใน ในบทนี้จะกล่าวถึงแนวคิด ทฤษฎีและงานวิจัยที่ที่จะนำมาใช้เป็นพื้นฐานและแนวทางในการศึกษาค้นคว้าอิสระ ผลการศึกษาจำแนกหัวข้อตามลำดับ ดังนี้

2.1 เป้าหมายการรักษาความมั่นคงปลอดภัยสารสนเทศ

2.2 มาตรฐาน ISO 27001

2.3 การตรวจสอบระบบงานสารสนเทศ

2.3.1 ความหมายของการตรวจสอบระบบงานสารสนเทศ

2.3.2 วัตถุประสงค์การควบคุมและตรวจสอบระบบสารสนเทศ

2.3.3 แนวทางการตรวจสอบ (Audit Program)

2.4 งานวิจัยที่เกี่ยวข้อง

2.1 เป้าหมายการรักษาความมั่นคงปลอดภัยสารสนเทศ

เป้าหมายการรักษาความมั่นคงปลอดภัยสารสนเทศ คือ การปกป้องดูแลข้อมูลสารสนเทศให้มีคุณสมบัติ 3 ประการ ดังนี้

1. ความลับ (Confidentiality)

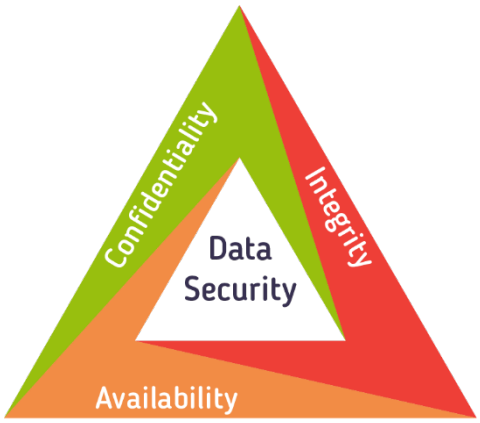
การรักษาความลับเป็นคุณสมบัติที่สำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ เป้าหมายของการรักษาความลับ คือ การปกป้องข้อมูลสารสนเทศจากการเข้าถึงจากผู้ไม่มีสิทธิ ดังนั้น ผู้มีสิทธิหรือผู้ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลสารสนเทศได้ โดยมีการจัดประเภทข้อมูลที่สามารถเข้าถึงได้ตามบทบาทและอำนาจหน้าที่

2. ความถูกต้องสมบูรณ์ (Integrity)

การรักษาความถูกต้องสมบูรณเป็นสิ่งสำคัญส่งผลถึงความน่าเชื่อถือของสารสนเทศ เป้าหมายของการรักษาความถูกต้องสมบูรณ์ คือ การปกป้องข้อมูลไม่ให้ถูกเปลี่ยนแปลง แก้ไขหรือเกิดความเสียหายจากผู้ไม่มีสิทธิหรือผู้ไม่ได้รับอนุญาตไม่ว่าจะโดยเจตนาหรือความไม่ตั้งใจ

3. ความพร้อมใช้งาน (Availability)

ความพร้อมใช้งานเป็นการสร้างความเชื่อมั่นว่าระบบสารสนเทศสามารถตอบสนองเมื่อผู้มีสิทธิหรือผู้ที่ได้รับอนุญาตต้องการใช้งาน โดยการบริหารจัดการให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่อง (อรนุช คงศรี, 2558; Sarah Vonnegut, 2016)



ภาพประกอบที่ 2.1 เป้าหมายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Sarah Vonnegut, 2016)

2.2 มาตรฐาน ISO 27001

มาตรฐาน ISO 27001 เป็นมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศที่พัฒนาโดยองค์กรสากล ISO (International Organization for Standardization) ซึ่งได้รับการยอมรับในระดับนานาชาติ เป็นมาตรฐานที่ใช้อ้างอิงกฎหมายด้านไอซีทีของประเทศ ที่มีผลบังคับใช้กับหน่วยงานต่าง ๆ อาทิ พระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 พระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 โดยเวอร์ชั่นล่าสุด คือ ISO 27001 : 2013 ประกาศใช้เมื่อวันที่ 1 ตุลาคม 2556 เป็นมาตรฐานสากลที่ได้กำหนดแนวทางดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของหน่วยงาน โดยมีกระบวนการบริหารจัดการสารสนเทศที่มีความสำคัญขององค์กรให้มีความมั่นคงปลอดภัยตามหลัก C I A (Confidentiality , Integrity , Availability) ซึ่งมีแนวทางการปฏิบัติตามขั้นตอนของกระบวนการดังนี้ เริ่มตั้งแต่ทำการวิเคราะห์และประเมินความเสี่ยง เพื่อทำให้ทราบว่าสารสนเทศใดที่มีความสำคัญต่อการดำเนินธุรกิจขององค์กร โอกาสที่จะเกิดความเสี่ยงและความเสียหายอันส่งผลกระทบต่อการดำเนินธุรกิจขององค์กรจากภัยคุกคามทั้งภายในภายนอกกับสารสนเทศนั้นมากน้อยแค่ไหน มีวิธีการบริหารจัดการในการป้องกันความเสี่ยงดังกล่าวอย่างไร โดยจำเป็นต้องจัดลำดับความสำคัญของความเสี่ยงทั้งหมดที่พบ และพิจารณาว่าสิ่งใดจำเป็นต้องรีบบริหารจัดการก่อนและหลัง จากนั้นจึงดำเนินการตามวงจร P (Plan หรือการวางแผน) D (Do หรือการประยุกต์ใช้หรือการดำเนินการ) C (Check หรือการตรวจสอบ) A (Action หรือการบำรุงรักษาหรือการปรับปรุง) โดยเริ่มจากทำการออกแบบระบบบริหารจัดการ ซึ่งในที่นี้หมายถึงกระบวนการที่เปรียบเสมือนเป็นเครื่องมือในการรักษาความมั่นคงปลอดภัย แต่ไม่ได้หมายรวมเพียงแค่การนำระบบเทคโนโลยีสารสนเทศมาสนับสนุน

เท่านั้น ยังหมายรวมถึงการพัฒนาขั้นตอนปฏิบัติหรือการนำขั้นตอนปฏิบัติที่มีอยู่เดิมมาปรับปรุงเพื่อให้เกิดกระบวนการป้องกันและรักษาความมั่นคงปลอดภัยของสารสนเทศที่ใช้ในการดำเนินธุรกิจขององค์กรอย่างเหมาะสม โดยหลังจากที่ได้ระบบที่ต้องการแล้วทำการดำเนินการตามระบบที่ได้วางแผนไว้ จากนั้นทำการตรวจสอบการดำเนินงานว่ามีการดำเนินงานครบถ้วนตามวัตถุประสงค์และแผนที่วางไว้หรือไม่และยังมีจุดอ่อนอยู่ที่จุดใด อย่างไร เมื่อได้ข้อมูลครบถ้วนแล้วก็นำมาพิจารณาทำการบำรุงรักษากระบวนการเดิมที่มีประสิทธิภาพเหมาะสมเพียงพอ และทำการปรับปรุงกระบวนการที่ยังมีจุดอ่อนให้ดีขึ้น เพื่อทำให้ระบบบริหารจัดการที่ประยุกต์ใช้ในองค์กรนั้นมีคุณภาพ ทันสมัย และเหมาะสมอยู่เสมอ

โครงสร้าง ISO 27001 : 2013 แบ่งเนื้อหาออกเป็น 14 หัวข้อใหญ่ (Domain) ซึ่งแต่ละหัวข้อประกอบด้วยวัตถุประสงค์จำนวนแตกต่างกัน รวมแล้วจำนวน 35 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความมั่นคงปลอดภัยแตกต่างกัน รวมแล้ว 114 ข้อ (Controls) (สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2560; บริษัท ที-เน็ต จำกัด, 2556; ภูมิพัฒน์ สุขศรีใส, 2559)

ภาพประกอบที่ 2.2 โครงสร้าง ISO 27001 : 2013 (Ahmed Riad, 2015)

ตารางที่ 2.1 โครงสร้าง ISO 27001 : 2013

ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย 14 ข้อ			วัตถุประสงค์การควบคุม รวม 35 วัตถุประสงค์	การควบคุม 114 ข้อ
1	A.5	นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)	1	2
2	A.6	โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security)	2	7
3	A.7	ความมั่นคงปลอดภัยสำหรับบุคลากร (Human resource security)	3	6
4	A.8	การบริหารจัดการทรัพย์สิน (Asset management)	3	10
5	A.9	การควบคุมการเข้าถึง (Access control)	4	14
6	A.10	การเข้ารหัสข้อมูล (Cryptography)	1	2
7	A.11	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)	2	15
8	A.12	ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations security)	7	14
9	A.13	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)	2	7
10	A.14	การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)	3	13
11	A.15	ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)	2	5
12	A.16	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)	1	7
13	A.17	ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)	2	4
14	A.18	ความสอดคล้อง (Compliance)	2	8

ตารางที่ 2.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยและมาตรการควบคุม

ลำดับ	หัวข้อ
A.5 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)
A.6 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 การติดต่อกับหน่วยงานผู้มีอานาจ (Contact with authorities)
6.	6.1.4 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)
7.	6.1.5 ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)
6.2 อุปกรณ์คอมพิวเตอร์แบบพกพา และการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)	
8.	6.2.1 นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)
9.	6.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)
A.7 ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human resource security)	
7.1 ก่อนการจ้างงาน (Prior to employment)	
10.	7.1.1 การคัดเลือก (Screening)
11.	7.1.2 ข้อตกลงและเงื่อนไขในการจ้างงาน (Terms and conditions of employment)

ลำดับ	หัวข้อ
7.2 ระหว่างการจ้างงาน (During employment)	
12.	7.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)
13.	7.2.2 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (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)
A.8 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)
A.9 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)

ลำดับ	หัวข้อ
9.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)	
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 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)
32.	9.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)
33.	9.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)
9.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	
34.	9.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of secret authentication information)
9.4 การควบคุมการเข้าถึงระบบ (System and application access control)	
35.	9.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)
36.	9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)
37.	9.4.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)
38.	9.4.4 การใช้โปรแกรมอรรถประโยน์ (Use of privileged utility programs)
39.	9.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)
A.10 การเข้ารหัสข้อมูล (Cryptography)	
10.1 มาตรการเข้ารหัสข้อมูล (Cryptographic controls)	
40.	10.1.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)
41.	10.1.2 การบริหารจัดการกุญแจ (Key management)

ลำดับ	หัวข้อ
A.11 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)	
11.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)	
42.	11.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)
43.	11.1.2 การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)
44.	11.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงานห้องทำงาน และอุปกรณ์ (Securing office, room and facilities)
45.	11.1.4 การป้องกันต่อภัยคุกคามจากภายนอก และสภาพแวดล้อม (Protecting against external end environmental thetas)
46.	11.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)
47.	11.1.6 พื้นที่สำหรับรับส่งสิ่งของ (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)

ลำดับ	หัวข้อ
A.12 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 การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)
12.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from malware)	
61.	12.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control against malware)
12.3 การสำรองข้อมูล (Backup)	
62.	12.3.1 การสำรองข้อมูล (Information backup)
12.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and monitoring)	
63.	12.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)
64.	12.4.2 การป้องกันข้อมูลล็อก (Protection of log information)
65.	12.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)
66.	12.4.4 การตั้งนาฬิกาให้ถูกต้อง (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)

ลำดับ	หัวข้อ
A.13 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 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)
75.	13.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)
76.	13.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)
77.	13.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)
A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)	
14.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)	
78.	14.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification)
79.	14.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสารธารณะ (Securing application services on public networks)
80.	14.1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)
14.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)	
81.	14.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)
82.	14.2.2 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

ลำดับ	หัวข้อ
83.	14.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)
84.	14.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)
85.	14.2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)
86.	14.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)
87.	14.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)
88.	14.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (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)
A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)	
15.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)	
91.	15.1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)
92.	15.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (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)

ลำดับ	หัวข้อ
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 การรายงานจุดอ่อนทางความมั่นคงสารสนเทศ (Reporting information security weaknesses)
99.	16.1.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (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)
102.	16.1.7 การเก็บรวบรวมหลักฐาน (Collection of evidence)
A.17 ประเด็นความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)	
17.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)	
103.	17.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)
104.	17.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity)
105.	17.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

ลำดับ	หัวข้อ
17.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)	
106.	17.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)
A.18 ความสอดคล้อง (Compliance)	
18.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)	
107.	18.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (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 ระเบียบข้อบังคับสาหรับมาตรการเข้ารหัสข้อมูล (Regulation of cryptographic controls)
18.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)	
112.	18.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)
113.	18.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)
114.	18.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

2.3 การตรวจสอบระบบงานสารสนเทศ

2.3.1 ความหมายของการตรวจสอบระบบงานสารสนเทศ

การตรวจสอบระบบงานสารสนเทศ หมายถึง การตรวจสอบเพื่อแสดงความเห็นต่อระบบการควบคุมสารสนเทศที่องค์กรใช้ ว่าเหมาะสมและเป็นไปตามวัตถุประสงค์ของการควบคุมที่กำหนดไว้หรือไม่ ทั้งนี้วัตถุประสงค์ของการควบคุมอาจกำหนดโดยผู้บริหารหรือผู้ออกแบบระบบ แต่ผู้ตรวจสอบจะตรวจสอบเพื่อให้มั่นใจว่าระบบที่ออกแบบไว้นั้นยังคงเพียงพอ เหมาะสม มีการปฏิบัติตาม และได้ผลตามวัตถุประสงค์ที่กำหนดไว้อย่างไรหรือไม่ (อุษณา ภัทรมนตรี, 2547, น. 1-8)

การตรวจสอบระบบงานสารสนเทศ หมายถึง กระบวนการของการรวบรวมและการประเมินหลักฐานเพื่อพิจารณาถึงการนำคอมพิวเตอร์มาใช้เพื่อช่วยดูแลรักษาสินทรัพย์ รักษาความครบถ้วนและถูกต้องของข้อมูล ซึ่งช่วยให้บรรลุเป้าหมายขององค์กรอย่างมีประสิทธิผล และใช้ทรัพยากรอย่างมีประสิทธิภาพ (รองศาสตราจารย์อุทัยวรรณ จรุงวิภู และคณะ, 2558, น. 4-11)

2.3.2 วัตถุประสงค์การควบคุมและตรวจสอบระบบสารสนเทศ

การควบคุมระบบสารสนเทศ หมายถึง กระบวนการหรือวิธีการต่าง ๆ ที่ผู้บริหารกำหนดขึ้นเพื่อใช้ป้องกัน ค้นพบ และแก้ไขเหตุการณ์ที่ไม่ต้องการหรือลดโอกาสความเสี่ยงไม่ให้เกิดขึ้น เช่น ความเสี่ยงที่สารสนเทศในระบบไม่ถูกต้องเชื่อถือได้ ความเสี่ยงจากการลักลอบเข้าระบบโดยผู้ที่ไม่ได้รับอนุญาต ความเสี่ยงในการเปลี่ยนแปลงทำลายข้อมูล และความรั่วไหล วัตถุประสงค์ในการควบคุมสารสนเทศ อาจแบ่งได้หลายประการ ดังนี้

1. ความครบถ้วนและถูกต้องหรือบูรณาการของข้อมูล (Integrity of Data) ข้อมูลที่บันทึกและประมวลผลในระบบ ต้องเป็นข้อมูลที่ได้รับการอนุมัติ (Authorization) มีความถูกต้องแม่นยำ (Accuracy) ครบถ้วน (Completeness) และสามารถพิสูจน์หาร่องรอยหรือหลักฐานยืนยันได้ (Validity) รวมทั้งเป็นข้อมูลสาระสำคัญที่เกี่ยวข้องกับเรื่องที่จะตัดสินใจ (Relevance)

2. การรักษาความลับ (Confidentiality) ข้อมูลที่อยู่ในระบบสารสนเทศต้องควบคุมให้ใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ไม่ให้เกิดการรั่วไหล ไม่เปิดเผยหรือเกิดกรณีลักลอบใช้ข้อมูลอย่างไม่ได้รับอนุญาต

3. ความหาได้เมื่อต้องการใช้ (Availability, Accessibility) วัตถุประสงค์ข้อนี้อาจดูตรงข้ามกับวัตถุประสงค์ในการเก็บรักษาความลับ แต่กิจการต้องพิจารณาว่าสารสนเทศที่จำเป็นในการใช้งานของผู้ใด ต้องให้ผู้นั้นได้รับทราบ และไม่ให้เกิดปัญหาการหวงข้อมูลระหว่างหน่วยงาน แต่ต้องสามารถใช้ประโยชน์จากข้อมูลร่วมกัน

ดังนั้น วัตถุประสงค์ทั้งสามประการจึงเป็นวัตถุประสงค์พื้นฐานที่สำคัญในการควบคุมข้อมูลและสารสนเทศ ข้อมูลสารสนเทศที่ถูกต้องเป็นทรัพย์สินที่มีค่าในการปฏิบัติงาน จึงต้องมีการเก็บรักษาความลับข้อมูลไม่ให้รั่วไหล แต่ไม่ใช่เป็นความลับจนกระทั่งข้อมูลหาไม่ได้เมื่อต้องการใช้ ทั้งนี้ข้อมูลที่ไม่ถูกต้องย่อมไม่มีคุณค่าเป็นข้อมูลขยะ ซึ่งควรควบคุมไม่ให้เกิดขึ้นในระบบสารสนเทศของกิจการ

นอกจากนั้น วัตถุประสงค์การควบคุมสารสนเทศยังรวมถึง

4. การดูแลรักษาทรัพย์สินให้ปลอดภัย (Asset Safeguarding) ทรัพย์สินในระบบสารสนเทศ ได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์อื่น ฐานข้อมูล และแฟ้มข้อมูล ฯลฯ ที่ต้องดูแลรักษาให้ปลอดภัย ตัวอย่างเช่น

การเก็บรักษาทรัพย์สินในสถานที่ที่ปลอดภัย รวมทั้งการควบคุมด้านสภาพแวดล้อม การเก็บรักษาดูแลตัวเครื่องและระบบงานในศูนย์คอมพิวเตอร์ไม่ให้เสียหาย ควบคุมให้เฉพาะผู้มีสิทธิเท่านั้นที่จะเข้าถึงหรือใช้งานได้

การควบคุมการพัฒนาและการปรับปรุงแก้ไขโปรแกรมระบบงาน โดยต้องได้รับการอนุมัติ ทดสอบ อย่างเหมาะสมก่อนนำมาใช้ปฏิบัติงานจริง

การป้องกันการหยุดชะงักในการปฏิบัติงาน เช่น การกำหนดแผนป้องกันอุบัติเหตุ อุบัติภัย การมีระบบสำรอง การจัดทำแฟ้มสำเนา เป็นต้น

5. การควบคุมด้านประสิทธิภาพและประสิทธิผลของระบบงาน การประเมินประสิทธิภาพจะพิจารณาเกี่ยวข้องกับการประเมินเปรียบเทียบกับ ระยะเวลา ทรัพยากร ต้นทุน และคุณภาพที่ได้ เช่น การวิเคราะห์เปรียบเทียบต้นทุนกับประโยชน์ที่เกิดขึ้นว่าคุ้มค่าต่อการลงทุนหรือไม่ เป็นต้น

ส่วนการประเมินประสิทธิผล โดยปกติอาจประเมินพร้อมกับการประเมินประสิทธิภาพ แต่จะเน้นการพิจารณาว่าระบบงานสามารถใช้งานตามวัตถุประสงค์ของโครงการที่กำหนดไว้หรือไม่ การประเมินความพึงพอใจของผู้ใช้งาน ประโยชน์ของสารสนเทศที่ได้รับความสามารถในการปรับปรุงต่อการเปลี่ยนแปลงในอนาคต โดยปกติการประเมินประสิทธิผลจะกระทำได้เมื่อกิจการได้ระบุความต้องการดังกล่าวไว้ชัดเจนล่วงหน้า และผ่านระยะเวลาการเรียนรู้ในการใช้งานระบบนั้นไประยะหนึ่งแล้ว

6. การปฏิบัติตามนโยบาย ข้อกำหนด และกฎระเบียบที่เกี่ยวข้อง (Compliance with Policies, Statutes and Regulations) ซึ่งอาจเป็นการปฏิบัติตามกฎหมายและกฎระเบียบจากสถาบันผู้กำกับดูแลภายนอก เช่น การใช้โปรแกรมบัญชีตามมาตรฐานที่กำหนดโดยกรมสรรพากร และการปฏิบัติตามนโยบาย ข้อกำหนดภายใน เช่น การเก็บรักษารหัสผ่าน การปฏิบัติงานตามระดับอนุมัติที่ได้รับ เป็นต้น (อุษณา ภัทรมนตรี, 2547, น. 1-9-1-10)

การควบคุมระบบงานสารสนเทศมีวัตถุประสงค์เพื่อสร้างกระบวนการหรือมาตรการที่จะใช้ลดโอกาสและความเสียหายที่ไม่ต้องการให้เกิดขึ้นในระบบงานสารสนเทศ ซึ่งประกอบด้วยวัตถุประสงค์ที่สำคัญ ดังนี้

1. การลดความเสี่ยงเนื่องจากกิจการนำคอมพิวเตอร์มาใช้ รวมทั้งโอกาสที่จะเกิดความผิดพลาดโดยรวม เช่น ความไม่ปลอดภัย ข้อผิดพลาด การใช้ระบบงานที่ไม่ชอบ การหยุดชะงักของธุรกิจ การทุจริต โดยมีระบบการเตือนภัย มาตรการวิธีการป้องกัน ค้นพบ แจ้งปัญหาและการแก้ไขข้อผิดพลาดที่เกิดขึ้นอย่างทันเวลา

2. การควบคุมข้อมูล วัตถุประสงค์ที่สำคัญของการควบคุมข้อมูลสารสนเทศ คือ การหากระบวนการและวิธีการทำงานที่สร้างความมั่นใจต่อผู้บริหารอย่างสมเหตุสมผลว่า

- การรักษาความลับ (Confidentiality) สำหรับข้อมูลที่อยู่ในระบบงานสารสนเทศ โดยควบคุมให้ใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ไม่ให้เกิดการรั่วไหล ไม่เปิดเผย หรือเกิดกรณีลักลอบใช้ข้อมูลโดยไม่ได้รับอนุญาต

- ความครบถ้วนและถูกต้องของข้อมูล (Integrity of Data) ข้อมูลในระบบเป็นข้อมูลที่ได้รับการอนุมัติ (Authorization) ถูกต้อง (Accuracy) ครบถ้วน (Completeness) การพิสูจน์หาร่องรอยหรือหลักฐานยืนยันได้ (Validity)

- ความพร้อมเมื่อต้องการใช้ (Availability) รวมทั้งเป็นข้อมูลที่มีสาระสำคัญและเกี่ยวข้องกับเรื่องที่จะตัดสินใจ (Relevance) วัตถุประสงค์ข้อนี้อาจดูตรงข้ามกับวัตถุประสงค์ในการเก็บรักษาความลับ แต่กิจการต้องพิจารณาว่า สารสนเทศที่จำเป็นในการใช้งานของผู้ใดต้องให้ผู้นั้นได้รับทราบ และทำให้ไม่เกิดการถือสิทธิ์ความเป็นเจ้าของในข้อมูล

3. การดูแลรักษาสินทรัพย์ให้ปลอดภัย สินทรัพย์ในระบบงานสารสนเทศ ได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์รอบข้าง ฐานข้อมูล และแฟ้มข้อมูลที่ต้องดูแลรักษาให้ปลอดภัย ตัวอย่างเช่น

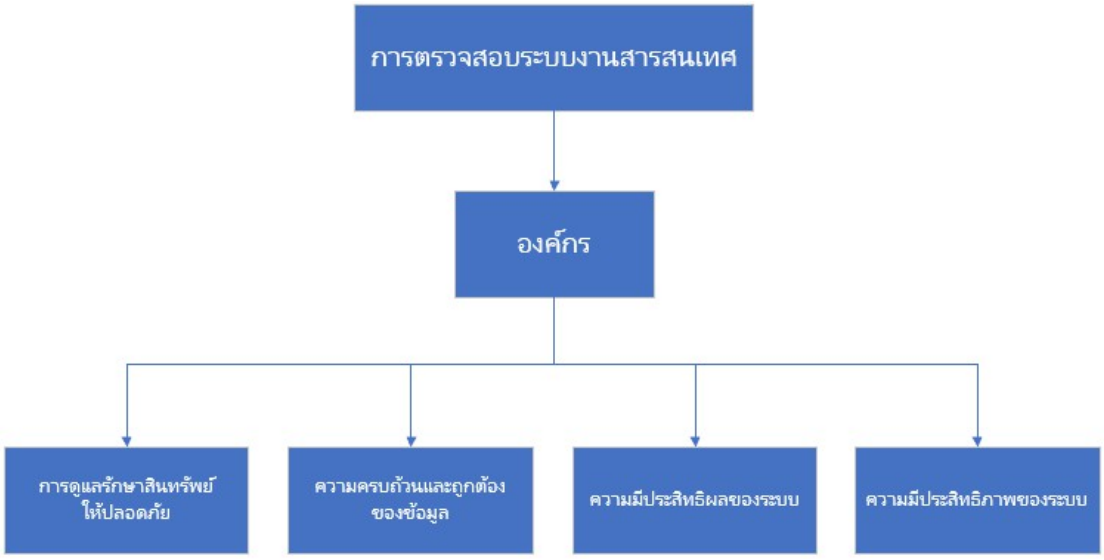
- การเก็บรักษาสินทรัพย์ดังกล่าวในสถานที่ที่ปลอดภัย รวมทั้งการควบคุมด้านสภาพแวดล้อม การเก็บรักษาดูแลตัวเครื่อง และระบบงานในศูนย์คอมพิวเตอร์ไม่ให้เสียหาย ควบคุมให้เฉพาะผู้มีสิทธิเท่านั้นที่จะเข้าถึงหรือใช้ได้

- การควบคุมการพัฒนาโปรแกรมระบบงาน และการปรับปรุงแก้ไขในภายหลังต้องได้รับการอนุมัติ ทดสอบอย่างเหมาะสม ก่อนนำมาใช้ปฏิบัติงานจริง

- การดูแลรักษาสินทรัพย์ไม่ให้เกิดการปฏิบัติงานต้องหยุดชะงัก หรือมีแผนป้องกันอุบัติเหตและอุบัติภัย

4. การเพิ่มประสิทธิภาพและประสิทธิผลของระบบงาน การประเมินประสิทธิภาพจะพิจารณาโดยเปรียบเทียบต้นทุนของการลงทุนในระบบงานกับประโยชน์ที่เกิดขึ้นว่าคุ้มค่าต่อการลงทุนหรือไม่ ซึ่งอาจทำได้ยาก เพราะประโยชน์บางประการจากระบบงานไม่อาจตีค่าเป็นจำนวนเงิน เช่น ความพึงพอใจของลูกค้าหรือผู้รับบริการ เป็นต้น อย่างไรก็ตาม อาจต้องพิจารณาประเมินประสิทธิภาพถ้าหากพบว่ามีการใช้งานไม่เต็มกำลัง หรือระบบใช้เวลาในการประมวลผลช้ากว่าที่ควรหรือเป็นระบบที่ทำให้ผู้ใช้ต้องรอคอยคำตอบ หรือไม่สะดวกในการใช้งานเท่าที่คาดไว้ในแผนงาน หรืออาจพิจารณาจากอุปกรณ์หรือโปรแกรมบางอย่างที่ซื้อมาโดยไม่มีการใช้งาน หรือใช้งานน้อยมาก ส่วนการประเมินประสิทธิผลจะเป็นการพิจารณาว่า ระบบงานสามารถใช้งานตามวัตถุประสงค์ของผู้ใช้หรือไม่ โดยปกติผู้ตรวจสอบภายในจะประเมินประสิทธิผลได้เมื่อทราบความต้องการใช้งานที่แท้จริง และระบบนั้นมีการใช้งานผ่านไประยะเวลาหนึ่งแล้ว

การตรวจสอบระบบงานสารสนเทศช่วยสนับสนุนวัตถุประสงค์การตรวจแบบเดิม (Traditional Auditing) เช่น วัตถุประสงค์ทางการพิสูจน์ซึ่งจะเน้นการดูแลรักษาสินทรัพย์ให้ปลอดภัยและความครบถ้วนถูกต้องของข้อมูล และวัตถุประสงด้านการบริหาร ซึ่งนอกจากจะรวมวัตถุประสงค์ทางการพิสูจน์แล้ว ยังรวมวัตถุประสงค์ทางประสิทธิภาพและประสิทธิผลอีกด้วย บางครั้งการตรวจสอบระบบงานสารสนเทศยังมีวัตถุประสงค์อื่นอีก กล่าวคือ ให้ความเชื่อมั่นว่าองค์กรได้ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ นโยบาย แผนงาน หรือเงื่อนไข ตัวอย่างเช่น ธนาคารจะต้องปฏิบัติตามกฎหมายของรัฐเกี่ยวกับจำนวนเงินให้กู้ยืม วัตถุประสงค์การตรวจสอบระบบงานสารสนเทศ



ภาพประกอบที่ 2.3 วัตถุประสงค์ของการตรวจสอบระบบงานสารสนเทศต่อองค์กร

ตามภาพประกอบที่ 2-3 แสดงให้เห็นว่าการตรวจสอบระบบงานสารสนเทศมีผลทำให้องค์กรสามารถบรรลุวัตถุประสงค์หลัก 4 อย่าง ได้แก่

1. การดูแลรักษาสินทรัพย์ให้ปลอดภัย

ระบบสารสนเทศที่เป็นสินทรัพย์ขององค์กร ซึ่งรวมฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์ประกอบอื่น แฟ้มข้อมูล ระบบเอกสารประกอบ และเครื่องใช้สำนักงาน ควรได้รับการปกป้องดูแลภายในระบบการควบคุมภายในเช่นเดียวกับสินทรัพย์อื่น ๆ เนื่องจากฮาร์ดแวร์สามารถถูกทำลายได้ สิทธิการเป็นเจ้าของซอฟต์แวร์และข้อมูลที่อยู่ในแฟ้มข้อมูลสามารถถูกขโมยหรือถูกทำลายได้ ดังนั้น การดูแลรักษาสินทรัพย์ให้ปลอดภัย จึงเป็นวัตถุประสงค์หลักที่องค์กรต่าง ๆ จะต้องให้ความสำคัญ

2. ความครบถ้วนและถูกต้องของข้อมูล

ความครบถ้วนและถูกต้องของข้อมูลเป็นแนวคิดพื้นฐานในการตรวจสอบระบบงานสารสนเทศ ข้อมูลควรมีคุณสมบัติดังนี้ ความครบถ้วน สมบูรณ์ ถูกต้อง และเป็นจริง ถ้าความถูกต้องตรงกันของข้อมูลไม่ได้รับการดูแล องค์กรจะไม่มีข้อมูลที่แท้จริงขององค์กรหรือของเหตุการณ์ ซึ่งอาจจะมีผลกระทบต่อการตัดสินใจของผู้บริหารหรือผู้ใช้ข้อมูล ยิ่งไปกว่านั้น ถ้าความครบถ้วนและถูกต้องของข้อมูลขององค์กรอยู่ในระดับต่ำ องค์กรจะประสบปัญหาจากการสูญเสียข้อได้เปรียบในการแข่งขัน

3. ความมีประสิทธิภาพของระบบ

ระบบงานสารสนเทศที่มีประสิทธิภาพผลก็คือจะบรรลุวัตถุประสงค์ที่กำหนดไว้ ซึ่งการตรวจสอบในเรื่องการมีประสิทธิผลของระบบมักจะเกิดขึ้นหลังจากที่ระบบทำงานไปในระยะเหนึ่ง ผู้บริหารความให้มีการตรวจสอบหลังจากที่ระบบทำงานแล้ว เพื่อพิจารณาว่าระบบได้บรรลุถึงวัตถุประสงค์ การประเมินนี้จะช่วยให้ได้ข้อมูลเพื่อตัดสินใจว่าจะยกเลิกระบบ หรือจะยังคงใช้ระบบต่อไป หรือจะเปลี่ยนแปลงแก้ไขระบบไปในทางใดทางหนึ่ง

นอกจากนั้น ผู้บริหารอาจต้องการให้ผู้ตรวจสอบภายในทำการประเมินโดยอิสระว่าการออกแบบนั้นบรรลุตรงตามความต้องการของผู้ใช้หรือไม่ ผู้ใช้มักจะระบุสิ่งที่ตนเองต้องการได้ยาก ยิ่งไปกว่านั้น ปัญหาในการติดต่อสื่อสารมักจะเกิดขึ้นระหว่างผู้ออกแบบและผู้ใช้ระบบ และถ้าระบบงานที่มีความซับซ้อน ต้นทุนในการนำระบบงานไปใช้ก็จะสูง

4. ความมีประสิทธิภาพของระบบ

ระบบงานสารสนเทศที่มีประสิทธิภาพจะมุ่งเน้นถึงการใช้ทรัพยากรอย่างประหยัดเพื่อให้การปฏิบัติงานเป็นไปตามวัตถุประสงค์ที่ต้องการ ระบบงานสารสนเทศมีการใช้ทรัพยากรที่หลากหลาย เช่น เวลาในกรใช้เครื่อง ซอฟต์แวร์ระบบ และแรงงาน ซึ่งทรัพยากรเหล่านี้เป็นทรัพยากรที่หาได้ยาก และใช้โปรแกรมระบบงานที่แตกต่างกัน

ความมีประสิทธิภาพของระบบได้กลายเป็นส่วนหนึ่งที่มีความความสำคัญที่ผู้สอบบัญชีควรมุ่งเน้นเพื่อตอบสนองให้แก่ผู้บริหาร เช่น ผู้บริหารอาจต้องตัดสินใจในเรื่องที่จะพัฒนาถึงประสิทธิภาพของระบบ โดยต้องมีการซื้อทรัพยากรพิเศษเพิ่มเติม แต่เนื่องจากฮาร์ดแวร์และซอฟต์แวร์พิเศษนั้นต้องคำนึงถึงเรื่องต้นทุน ผู้บริหารจึงจำเป็นที่จะต้องทราบถึงขีดความสามารถของระบบที่ถูกใช้ไปจนหมดเป็นเพราะโปรแกรมระบบงานนั้นไม่มีประสิทธิภาพหรือเป็นเพราะการปันส่วนทรัพยากรที่มีอยู่ไม่เหมาะสม (รองศาสตราจารย์อุทัยวรรณ จรุงวิภู และคณะ, 2558, น. 4-11-4-13)

2.3.3 แนวทางการตรวจสอบ (Audit Program)

การตรวจสอบที่ดีผู้ตรวจสอบภายในทั้งหลายต้องมีการทำแผนการตรวจสอบ หรือก็คือ แผนการตรวจสอบ (Audit Plan) ที่ผู้ตรวจสอบภายในที่ต้องจัดทำล่วงหน้า เพื่อให้การปฏิบัติงานสำเร็จลุล่วงตามแผนการตรวจสอบและสำเร็จลุล่วงไปด้วยดี เพราะฉะนั้น เครื่องมือช่วยเหลือผู้ตรวจสอบภายในที่จะควบคุมให้ทำงานได้ตามแผนการตรวจสอบ คือ แนวการตรวจสอบภายใน (Audit Program) ที่ต้องจัดทำเป็นลายลักษณ์อักษร โดยต้องมีหัวข้อที่ตรวจสอบ วิธีการตรวจสอบและเทคนิคที่ใช้ในการตรวจสอบ (SeRia, 2558)

แนวทางการปฏิบัติงานตรวจสอบ (Audit Program) หมายความถึง การกำหนดรายละเอียดเกี่ยวกับวิธีการปฏิบัติงานตามที่ได้รับมอบหมาย ซึ่งผู้ตรวจสอบภายในต้องจัดทำเป็นลายลักษณ์อักษร ซึ่งจะเป็นส่วนหนึ่งของแผนการปฏิบัติงาน เพื่อให้ทีมงานใช้เป็นแนวทางในการปฏิบัติงานในแต่ละเรื่อง ว่าจะตรวจสอบด้วยวัตถุประสงค์อะไร ที่หน่วยรับตรวจใด ณ เวลาใด ใช้วิธีการและเทคนิคการตรวจสอบใด จึงจะช่วยให้การรวบรวมหลักฐานในรายละเอียดเป็นไปอย่างมีประสิทธิภาพ (กลุ่มตรวจสอบภายในระดับกระทรวง กระทรวงศึกษาธิการ, 2558)

แนวทางการปฏิบัติงานตรวจสอบจัดเป็นเครื่องมือที่สำคัญสำหรับผู้ตรวจสอบ ซึ่งจะช่วยให้ผู้ตรวจสอบทราบว่าในแต่ละเรื่องที่ตรวจสอบ จะทำการตรวจสอบในประเด็นใด วัตถุประสงค์การตรวจสอบในแต่ละประเด็น ขั้นตอนและวิธีการตรวจสอบ แหล่งข้อมูล และเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล การกำหนดแนวทางการปฏิบัติงานตรวจสอบเป็นการลดความเสี่ยงที่อาจทำให้การตรวจสอบไม่บรรลุวัตถุประสงค์ และจะทำให้งานของผู้ตรวจสอบมีประสิทธิภาพยิ่งขึ้น(สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน, 2549)

2.4 งานวิจัยที่เกี่ยวข้อง

มนสิชา ทองประศาสน์ (2558) ได้พัฒนานโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา บริษัท อีวาตาร์ อินเทอมีเดีย โดยมีมาตรฐาน ISO/IEC 27001 : 2013 เป็นเครื่องมือในการพัฒนาเพื่อให้องค์กรดำเนินงานอย่างมีประสิทธิภาพ โดยการระบุรายการของทรัพย์สินเฉพาะในส่วนของ Data Center ซึ่งมีระบบงานที่มีความสำคัญกับข้อมูลสารสนเทศขององค์กรในอันดับต้นของบริษัทและมีการประเมินความเสี่ยง (ก่อน-หลัง) และนำ Control ของ ISO 27001 : 2013 มาปรับใช้กับแผนการจัดการความเสี่ยงทำให้องค์กรมีการบริหารความเสี่ยงที่ดีขึ้น และมีความเสี่ยงลดลง

ณัทรัฏฐ์ มณีรัสยากร (2559) ได้พัฒนานโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา บริษัท เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น จำกัดโดยมีมาตรฐาน ISO/IEC 27001 : 2013 เป็นเครื่องมือในการพัฒนาเพื่อเป็นบรรทัดฐานและแนวทางปฏิบัติให้กับการทำงานของผู้ดูแลระบบและผู้ที่เกี่ยวข้อง โดยการวิเคราะห์และประเมินความเสี่ยง

สารสนเทศในแง่ของโอกาสที่เกิดเหตุการณ์ความเสี่ยง และระดับความรุนแรงของผลกระทบที่ตามมาและบริหารจัดการความเสี่ยงหลังการประเมิน พบว่า เมื่อแก้ไขความเสี่ยงตามมาตรฐาน ISO 27001 ส่งผลให้องค์กรมีการบริหารจัดการสารสนเทศที่ดีขึ้นและมีความเสี่ยงลดลง

อภินัทธ์ แช่มลำเจียก (2557) ได้ศึกษามาตรฐาน ISO/IEC 27001 : 2013 เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศโดยปรับปรุงและพัฒนานโยบายด้านความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา บริษัท เว็ลธ์ แมเนจเม้นท์ ซิสเท็ม จำกัด" ผลการศึกษาทำให้องค์กรได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยทางสารสนเทศ ได้รับรู้ถึงความเสี่ยงและจุดอ่อนด้านเทคโนโลยีสารสนเทศที่ทางองค์กรเผชิญอยู่ และได้จัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อหามาตรการป้องกันและหลีกเลี่ยงความเสี่ยงได้อย่างมีประสิทธิภาพ

ธิดา ลิ่มทองวิรัตน์ (2553) ได้ศึกษาแนวทางเพื่อประเมินประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศ เพื่อวิเคราะห์ปัญหาอุปสรรคและจุดอ่อนในระบบการควบคุมภายในสารสนเทศรวมถึงเสนอแนะแนวทางการควบคุมที่มีประสิทธิภาพ รวมถึงเพื่อประเมินการปฏิบัติงานของพนักงานให้เป็นไปตามขั้นตอนมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO 27001 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ผลที่ได้จากการศึกษา พบว่า ในภาพรวมบริษัทมีการควบคุมภายในด้านสารสนเทศในระดับเพียงพอแล้ว โดยมีระดับการควบคุมที่ดี โดยบริษัทยังคงต้องให้ความสนใจในเรื่องที่ยังไม่ได้มีการปฏิบัติตามมาตรฐานในระดับที่เพียงพอ 3 เรื่องคือ เรื่องการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอเพื่อให้อยู่ในสภาพสมบูรณ์ เรื่องการบันทึกเหตุการณ์ข้อผิดพลาด และเรื่องการตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน ข้อเสนอแนะเกี่ยวกับการบำรุงรักษาอุปกรณ์คือ ควรเพิ่มกระบวนการควบคุมและการเก็บรักษาอุปกรณ์ รวมถึงกระบวนการซ่อมแซมและการบำรุงรักษาอุปกรณ์ ในเรื่องการบันทึกเหตุการณ์ข้อผิดพลาด ควรเพิ่มรายงานเหตุการณ์ที่เกิดขึ้น เพื่อจัดทำรายงานประจำสัปดาห์เสนอต่อผู้บริหารทราบ และเรื่องการตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน ผู้ดูแลระบบต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

น้ำหนึ่ง กล้าหาญ (2555) ได้พัฒนาโปรแกรมประยุกต์สำหรับการประเมินความมั่นคงปลอดภัยสารสนเทศในองค์กรปกครองส่วนท้องถิ่นในจังหวัดสุพรรณบุรี โดยอิงมาตรฐาน ISO/IEC 27001 พบว่า มีความพร้อมอยู่ในระดับปานกลางทุกด้าน ทั้งนี้เป็นเพราะมีแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Security Policy) ที่ยังไม่ชัดเจน ซึ่งเป็นสิ่งแรกที่สำคัญ และจำเป็นสำหรับองค์กรที่ต้องมีเพื่อเป็นแนวทาง และสนับสนุนการรักษาความมั่นคงปลอดภัยสารสนเทศในหน่วยงานหรือองค์กร ดังนั้นการกำหนดบทบาทขององค์กรและบุคลากรในภาพรวมตามลำดับ คือ ผู้นำ/ผู้บริหาร หัวหน้าหน่วย/งาน และบุคลากรผู้ปฏิบัติงาน ดังนี้

1. ผู้บริหาร แสดงเจตจำนงต่อการสร้างความมั่นคงปลอดภัยสารสนเทศให้เกิดภายในองค์กรสนับสนุนการประกาศนโยบายความมั่นคงปลอดภัยสารสนเทศ เป็นต้นแบบและเสริมสร้างวัฒนธรรมแห่งความมั่นคงปลอดภัยระบบสารสนเทศ การร่วมจัดทำกลยุทธ์กับบุคลากรระดับอื่นและสื่อสารชัดเจนสู่ทุกหน่วยงาน

2. หัวหน้าหน่วยงาน ช่วยสื่อสารให้ความรู้แก่ผู้ปฏิบัติ ติดตามการปฏิบัติตามนโยบายมีการรายงานผลการดำเนินงาน สร้างบรรยากาศในการเรียนรู้

3. ผู้ปฏิบัติ ยอมรับและปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและร่วมสร้างบรรยากาศความมั่นคงปลอดภัยให้ยั่งยืน

ภาพร ภิยโยดิลกชัย (2533) ได้ศึกษาเกี่ยวกับการตรวจสอบระบบสารสนเทศ โดยการนำมาตรฐานของ COBIT Framework มาประยุกต์ในการจัดทาแนวการตรวจสอบระบบสารสนเทศ (Audit Program) ผลการศึกษาพบว่า แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถนำมาใช้เป็นเครื่องมือในการปฏิบัติงานตรวจสอบ และหัวหน้าหน่วยงานตรวจสอบสามารถใช้เป็นเครื่องมือในการสอบทานและควบคุมงาน ซึ่งทาให้การตรวจสอบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างครอบคลุมตามระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร และบรรลุวัตถุประสงค์ของการตรวจสอบ อย่างไรก็ตาม รายละเอียดของการนำไปปฏิบัติในกระบวนการต่าง ๆ ในมาตรฐาน COBIT ผู้ตรวจสอบจะต้องพิจารณาข้อมูลเพิ่มเติมจาก FRAMEWORK อื่น ๆ เช่น มาตรฐาน ISO/IEC 27001 ,ISO/IEC 17799 ที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร, ITIL (IT Infrastructure Library) ซึ่งเป็นแนวทางปฏิบัติว่าด้วยเรื่องเกี่ยวกับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เป็นต้น

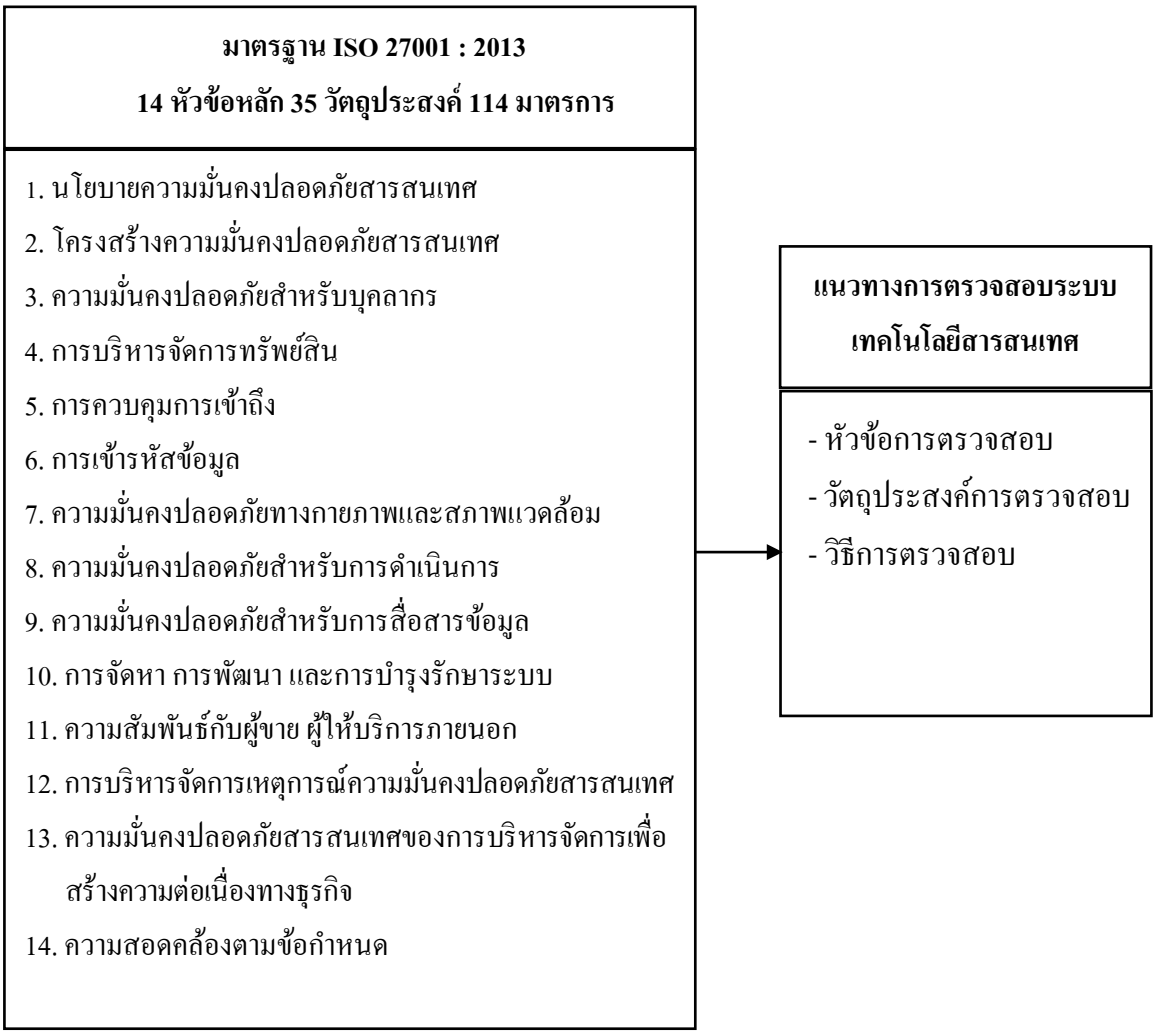
JOŽE ŠREKL และ ANDREJKA PODBREGAR (2014) ได้ศึกษาถึงการเสริมสร้างความมั่นคงปลอดภัยให้กับข้อมูลในองค์กร โดยการใช้มาตรฐาน ISO/IEC 27000 โดยให้ความเห็นว่าทุกองค์กรควรจะให้ความสำคัญกับการรักษาความปลอดภัยของข้อมูลที่มีอยู่ในองค์กร หากองค์กรต้องการความต่อเนื่องและเพิ่มประสิทธิภาพในการดำเนินการทางธุรกิจ นอกเหนือจากการรักษาความมั่นคงปลอดภัยของข้อมูลแล้ว องค์กรต้องตระหนักถึงภัยคุกคามจากการถูกบุกรุกและการถูกละเมิดจากผู้ไม่ประสงค์ดี รวมถึงภัยคุกคามจากภายในองค์กรเอง อันเกิดจากความรู้เท่าไม่ถึงการณ์ หรือขาดความตระหนักของบุคลากรหรือการใช้เทคโนโลยีที่ไม่เหมาะสมในองค์กร ซึ่งองค์กรเองต้องพิจารณาและประเมินหาช่องโหว่นั้น เพื่อเป็นการสร้างความมั่นใจในความปลอดภัยของข้อมูล อาจจะต้องมีการลงทุนในเรื่องของการรักษาความมั่นคงปลอดภัยสารสนเทศมากขึ้น เนื่องจากข้อมูลที่อยู่ในองค์กร ล้วนแล้วแต่สามารถที่จะเพิ่มมูลค่าให้กับองค์กรได้ และเป็นการลดช่องโหว่และความเสี่ยงต่อระบบสารสนเทศในองค์กรจากการถูกโจมตีทั้งจากภายในและภายนอกองค์กรได้

Pavol Sojčík (2012) ได้ทำการศึกษาเรื่อง Tools for information security management ซึ่งทำให้ทราบว่าปัจจุบันการรักษาความมั่นคงปลอดภัยสารสนเทศนั้นเป็นสิ่งที่องค์กรควรให้ความสำคัญ ในแต่ละองค์กรจะมีการเลือกใช้มาตรการควบคุมที่แตกต่างกันขึ้นอยู่กับการให้ความสำคัญของข้อมูลที่สำคัญขององค์กรบนพื้นฐานของการรักษาความมั่นคงปลอดภัยของสารสนเทศนั้นจะต้องเริ่มในระดับบุคคล โดยบุคลากรในองค์กรจะต้องเกิดความตระหนักว่าตนเองอาจจะเป็นช่องโหว่ ทำให้เกิดภัยคุกคามในระดับองค์กรได้ อีกทั้งหลายๆ องค์กรเองไม่ได้มีระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศที่ดีและมีประสิทธิภาพ จึงเป็นเหตุผลที่สนับสนุนว่าองค์กรควรมีระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดยอ้างอิงจากมาตรฐาน ISO/IEC 27001 ซึ่งสามารถขอรับรองมาตรฐานได้ สำหรับแนวทางในการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศนั้น สามารถดูได้จากเอกสาร ISO/IEC 27002 ซึ่งจะระบุแนวปฏิบัติทั้งหมด โดยสามารถเลือกเฉพาะกระบวนที่เหมาะสมกับองค์กร ให้สอดคล้องกับช่องโหว่ขององค์กร ในการศึกษานี้ได้กล่าวถึงประโยชน์และกระบวนการทั้งหมดของการเข้ารับการรับรองมาตรฐาน ISO/IEC 27001 โดยการรับการรับรองมาตรฐาน ISO/IEC 27001 นั้น เป็นสิ่งที่องค์กรควรกำหนดเป็นเป้าประสงค์ร่วมกันทั้งองค์กร เพื่อให้เกิดความร่วมมือกันในองค์กรในการปฏิบัติเพื่อให้บรรลุวัตถุประสงค์ของมาตรการควบคุมที่เลือกมาใช้งานในองค์กร ประโยชน์ที่จะได้รับจากการเข้ารับการรับรองมาตรฐาน เช่น องค์กรมีการบูรณาการการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการระดับองค์กร เป็นต้น การเข้ารับการรับรองมาตรฐานเป็นการสร้างความน่าเชื่อถือให้กับองค์กร ซึ่งจะส่งผลถึงความได้เปรียบเชิงธุรกิจ ทั้งยังส่งเสริมให้พนักงานมีความรับผิดชอบในการรักษาความปลอดภัยของข้อมูลทั้งข้อมูลส่วนตัวและข้อมูลขององค์กร ทำให้มีการปรับปรุงและพัฒนาระบบบริหารจัดการอยู่อย่างต่อเนื่อง ทำให้เกิดความมั่นใจว่าทรัพยากรขององค์กรที่เกี่ยวกับการให้บริการด้านสารสนเทศจะสามารถดำเนินการให้บริการได้อย่างต่อเนื่อง ทำให้ทราบถึงเหตุการณ์ที่อาจจะทำให้เกิดการหยุดชะงักของการให้บริการด้านสารสนเทศในองค์กร อันจะส่งผลถึงการรักษาความสมบูรณ์และความพร้อมใช้ของสารสนเทศ และยังช่วยลดการรั่วไหลของข้อมูลในองค์กรอีกด้วย

บทที่ 3
ระเบียบวิธีวิจัย

งานวิจัยนี้เป็นการศึกษามาตรฐาน ISO 27001 : 2013 เพื่อจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามข้อกำหนดในมาตรฐาน ISO 27001 : 2013 สำหรับผู้ตรวจสอบภายใน การทางพิเศษแห่งประเทศไทย โดยมีแนวทางการวิจัยอย่างเป็นขั้นตอนต่อเนื่องไปตามลำดับ ดังนี้

3.1 กรอบแนวคิดการวิจัย



ภาพประกอบที่ 3.1 กรอบแนวคิดการวิจัย

3.2 ขั้นตอนการวิจัย

3.2.1 ศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง รวมทั้งศึกษารายละเอียดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยและมาตรการควบคุมตามมาตรฐาน ISO 27001 : 2013

3.2.2 จัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ ซึ่งประกอบด้วยหัวข้อการตรวจสอบ วัตถุประสงค์การตรวจสอบ และวิธีการตรวจสอบ ให้สอดคล้องตามข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยและมาตรการควบคุมตามมาตรฐาน ISO 27001 : 2013 รวมทั้งสอดคล้องกับการดำเนินงานของการทางพิเศษแห่งประเทศไทย

3.2.3 สร้างแบบสอบถามเพื่อประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศและนำไปเก็บข้อมูลจากกลุ่มตัวอย่าง จากนั้นวิเคราะห์ข้อมูลด้วยค่าทางสถิติเพื่อหาค่าความพึงพอใจในแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

3.3 เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย

3.3.1 แบบประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

3.3.2 ฮาร์ดแวร์ที่ใช้ในการวิจัยประกอบด้วย

3.3.2.1 เครื่องคอมพิวเตอร์โน้ตบุ๊ค

3.3.2.2 ซีพียู Intel Core i7-7500

3.3.2.3 หน่วยความจำ (RAM) 8 GB

3.3.2.4 ความจุของฮาร์ดดิสก์ 1 TB

3.2.3 ซอฟต์แวร์ที่ใช้ในการวิจัย

3.3.3.1 ระบบปฏิบัติการ Microsoft Windows 10

3.3.3.2 โปรแกรม Microsoft Office 2013

3.3.3.3 โปรแกรม SPSS 16.0

3.3.3.4 Internet Explorer Version 11

3.4 การสร้างแบบสอบถามเพื่อประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

แบบสอบถามเพื่อประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ ประกอบด้วย 2 ส่วน ได้แก่ ส่วนที่ 1 ประเมินความพึงพอใจด้านรูปแบบและเนื้อหาของแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ และส่วนที่ 2 ประเมินความพึงพอใจด้านการนำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศไปประยุกต์ในการใช้งาน

3.5 ประชากรและกลุ่มตัวอย่าง

ประชากรและกลุ่มตัวอย่างในการประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ เป็นผู้ตรวจสอบภายในในหน่วยงานการทางพิเศษแห่งประเทศไทย จำนวน 10 คน จากทั้งหมดจำนวน 24 คน

3.6 การวิเคราะห์ข้อมูล

3.6.1 สถิติที่ใช้ในการวิเคราะห์ระดับความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ ประกอบด้วยค่าเฉลี่ย (Arithmetic Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

3.6.2 มาตรวัดตามมาตราส่วนประมาณค่ากำหนดระดับค่าคะแนนในการตอบแบบประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ มี 5 ระดับ ดังนี้

5 หมายถึง มีความพึงพอใจมากที่สุด
4 หมายถึง มีความพึงพอใจมาก
3 หมายถึง มีความพึงพอใจปานกลาง
2 หมายถึง มีความพึงพอใจมากน้อย
1 หมายถึง มีความพึงพอใจน้อยที่สุด

3.6.3 การแปลความหมายระดับค่าคะแนนเฉลี่ย ข้อมูลวัดมาตราส่วนประมาณค่าพิจารณาตามเกณฑ์การวิเคราะห์ของเบสท์ (Best W. John., 1997: 190) แบ่งช่วงคะแนนสำหรับการแปลผลดังนี้

ระดับคะแนนเฉลี่ย	4.50 - 5.00	หมายถึง	มีความพึงพอใจมากที่สุด
ระดับคะแนนเฉลี่ย	3.50 - 4.49	หมายถึง	มีความพึงพอใจมาก
ระดับคะแนนเฉลี่ย	2.50 - 3.49	หมายถึง	มีความพึงพอใจปานกลาง
ระดับคะแนนเฉลี่ย	1.50 - 2.40	หมายถึง	มีความพึงพอใจน้อย
ระดับคะแนนเฉลี่ย	1.00 - 1.49	หมายถึง	มีความพึงพอใจน้อยที่สุด

3.6.4 ค่าเฉลี่ย (Arithmetic Mean) ($\bar{X}$) ใช้คำนวณค่าเฉลี่ยของตัวแปร เพื่อดูแนวโน้มของระดับความพึงพอใจของผู้ตอบแบบสอบถาม

ค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) (S.D.) ใช้คำนวณเพื่อวัดการกระจายระดับความคิดเห็นของข้อมูลความพึงพอใจของผู้ตอบแบบสอบถาม

3.7 ระยะเวลาดำเนินการวิจัย

ระยะเวลาดำเนินการวิจัย สรุปได้ดังตารางที่ 3.1

ตารางที่ 3.1 ระยะเวลาดำเนินการวิจัย

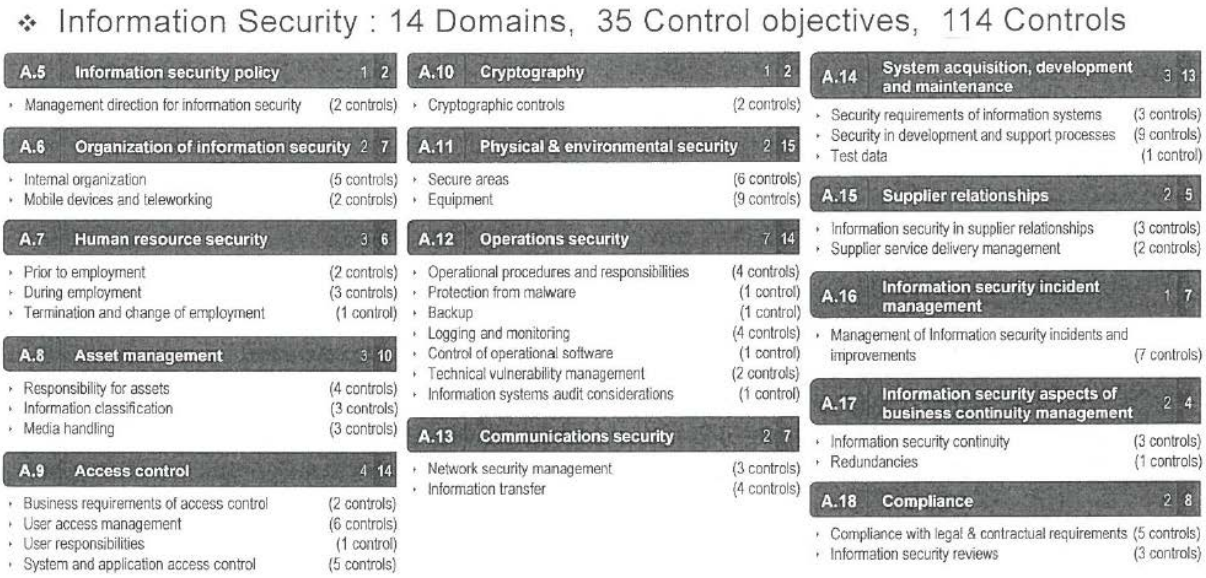
ขั้นตอนการวิจัย	ระยะเวลาดำเนินการ (เดือน)											
	1	2	3	4	5	6	7	8	9	10	11	12
1. ศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง	■	■										
2. จัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ			■	■	■	■	■	■	■			
3. สร้างแบบสอบถามและประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ และสรุปผล										■		
4. การนำเสนอและเผยแพร่ผลงานวิจัย											■	
5. จัดทำเอกสารงานวิจัย		■	■	■	■	■	■	■	■	■	■	■

บทที่ 4
ผลการวิจัย

งานวิจัยนี้เป็นการศึกษามาตรฐาน ISO 27001 : 2013 เพื่อจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามมาตรฐาน และสอดคล้องกับการดำเนินงานของการทางพิเศษแห่งประเทศไทย โดยแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ สำหรับผู้ตรวจสอบภายใน การทางพิเศษแห่งประเทศ มีผลการวิจัยเป็นไปลำดับตามขั้นตอนการวิจัย ดังนี้

4.1 การศึกษารายละเอียดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยและมาตรการควบคุมตามมาตรฐาน ISO 27001 : 2013

มาตรฐาน ISO 27001 เป็นมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีกระบวนการบริหารจัดการสารสนเทศที่มีความสำคัญขององค์กรให้มีความมั่นคงปลอดภัยตามหลักของ C I A (Confidentiality , Integrity , Availability) โดย ISO 27001 : 2013 แบ่งเนื้อหาออกเป็น 14 หัวข้อใหญ่ (Domain) ซึ่งแต่ละหัวข้อประกอบด้วยวัตถุประสงค์จำนวนแตกต่างกัน รวมแล้วจำนวน 35 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความมั่นคงปลอดภัยแตกต่างกัน รวมแล้ว 114 ข้อ (Controls) ดังภาพประกอบที่ 4.1



ภาพประกอบที่ 4.1 ISO 27001 : 2013 (บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด, 2560, น. 63)

4.2 การจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ สำหรับผู้ตรวจสอบภายในการทางพิเศษแห่งประเทศไทยที่จัดทำตามข้อกำหนดของมาตรฐาน ISO 27001 : 2013 ประกอบด้วย เรื่องที่ตรวจสอบ วัตถุประสงค์การตรวจสอบ และวิธีการตรวจสอบ จำนวน 14 หัวข้อใหญ่ 114 ข้อย่อย ดังตารางที่ 4.1

ตารางที่ 4.1 แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.5 นโยบายความมั่นคงปลอดภัยสารสนเทศ		
A.5.1	**ทิศทางการบริหารจัดการความมั่นคงปลอดภัย**	
A.5.1.1	**นโยบายความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรและได้รับอนุมัติจากผู้บริหาร รวมทั้งมีการสื่อสารให้พนักงาน และหน่วยงานภายนอกที่เกี่ยวข้องรับทราบ	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การจัดทำและเผยแพร่นโยบายความมั่นคงปลอดภัยฯ 2. สอบทานความมีอยู่จริงและการอนุมัติเอกสารนโยบายความมั่นคงปลอดภัยฯ 3. สอบทานวิธีการ/ช่องทางการเผยแพร่นโยบายความมั่นคงปลอดภัยฯ ให้พนักงานและหน่วยงานที่เกี่ยวข้อง เช่น ผู้ให้บริการภายนอก ผู้รับจ้างพัฒนาระบบ/บำรุงรักษาระบบ เป็นต้น
A.5.1.2	**การทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า นโยบายความมั่นคงปลอดภัยสารสนเทศ มีความเหมาะสม เพียงพอ และมีประสิทธิผล โดยได้รับการทบทวนตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การทบทวนนโยบายความมั่นคงปลอดภัยฯ 2. สอบทานการกำหนดรอบการทบทวนนโยบายความมั่นคงปลอดภัยฯ 3. สอบทานการทบทวนนโยบายความมั่นคงปลอดภัยฯ ตามรอบระยะเวลาที่กำหนด

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.6 โครงสร้างความมั่นคงปลอดภัยสารสนเทศขององค์กร		
A.6.1	**โครงสร้างภายในองค์กร**	
A.6.1.1	**บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่ามีการกำหนดขอบเขต กำหนดนิยาม และมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน และเป็นลายลักษณ์อักษร ทั้งพนักงานภายในองค์กรและคู่สัญญาผู้ให้บริการภายนอก	1. สอบทานความมีอยู่จริงของคำสั่งแต่งตั้งคณะกรรมการหรือคณะทำงานที่มีขอบเขต หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร 2. สอบทานสัญญาจ้างว่ามีการกำหนดหน้าที่ความรับผิดชอบของคู่สัญญาด้านความมั่นคงปลอดภัยสารสนเทศ
A.6.1.2	**การแบ่งแยกหน้าที่ความรับผิดชอบ**	
	เพื่อให้มั่นใจว่า มีแบ่งแยกหน้าที่และกำหนดความรับผิดชอบหน่วยงานเทคโนโลยีสารสนเทศเพื่อควบคุมเข้าถึงข้อมูลและทรัพย์สินสารสนเทศอย่างชัดเจน และเหมาะสม	สอบทานการแบ่งแยกหน้าที่หน่วยงานเทคโนโลยีสารสนเทศจากโครงสร้างการแบ่งส่วนงานว่ามีความชัดเจน เหมาะสม และกำหนดหน้าที่ความรับผิดชอบการดำเนินงานที่ไม่สามารถข้ามสิทธิกันได้
A.6.1.3	**การติดต่อกับหน่วยงานที่มีอำนาจด้านความมั่นคงปลอดภัย**	
	เพื่อให้มั่นใจว่ามีข้อมูลที่เป็นปัจจุบันสำหรับติดต่อกับผู้มีอำนาจตัดสินใจภายในองค์กร และหน่วยงานภายนอกองค์กร หากเกิดเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ	สอบทานความมีอยู่จริงและความเป็นปัจจุบันของรายชื่อและเบอร์ติดต่อที่สำคัญของหน่วยงานภายใน เช่น ผู้บริหารระดับสูงที่มีอำนาจตัดสินใจหากเกิดเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศเป็นต้น และหน่วยงานภายนอกองค์กร เช่น สถานีดับเพลิง สถานีตำรวจ โรงพยาบาล ผู้ให้บริการภายนอกที่ให้ความช่วยเหลือได้ในกรณีเกิดเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศได้ เป็นต้น

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.6.1.4	**การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน**	
	เพื่อให้มั่นใจว่า มีข้อมูลที่เป็นปัจจุบัน สำหรับติดต่อหน่วยงานที่มีความรอบรู้ความชำนาญด้านความมั่นคงปลอดภัยเพื่อใช้ในการแลกเปลี่ยน เรียนรู้เทคโนโลยีสารสนเทศ ภัยคุกคาม หรือจุดอ่อนใหม่	สอบทานความมีอยู่จริงและความเป็นปัจจุบันของรายชื่อและเบอร์ติดต่อที่สำคัญของหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัย เช่น ข้อมูลผู้ผลิตทางด้านฮาร์ดแวร์และซอฟต์แวร์ที่องค์กรใช้งาน เป็นต้น เพื่อใช้ในการศึกษาและติดตามแนวโน้มทางด้านเทคโนโลยีสารสนเทศ
A.6.1.5	**การรักษาความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ**	
	เพื่อให้มั่นใจว่า การบริหารโครงการมีการระบุประเด็นเรื่องการรักษาความมั่นคงปลอดภัยขององค์กร	สอบทานการระบุข้อตกลงในการรักษาความลับข้อมูลสารสนเทศขององค์กรจากเอกสารสัญญาจ้าง เอกสาร TOR โครงการด้านเทคโนโลยีสารสนเทศ
A.6.2	**การควบคุมอุปกรณ์พกพาและการปฏิบัติงานจากระยะไกล**	
A.6.2.1	**นโยบายสำหรับอุปกรณ์สื่อสารแบบพกพา**	
	เพื่อให้มั่นใจว่า มีแนวทางการใช้งานอุปกรณ์สื่อสารแบบพกพา และมีการดำเนินงานตามนโยบายหรือแนวทางที่กำหนดรวมทั้งมีการสื่อสารให้พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องรับทราบ	1. สอบทานความมีอยู่จริงของแนวทางปฏิบัติงานสำหรับอุปกรณ์สื่อสารแบบพกพาและวิธีการ/ช่องทางการเผยแพร่ให้ผู้เกี่ยวข้องรับทราบ 2. สุ่มสัมภาษณ์ความเข้าใจในแนวทางฯ กับพนักงานที่เกี่ยวข้อง และสังเกตการณ์การดำเนินงานตามที่แนวทางกำหนด
A.6.2.2	**การปฏิบัติงานจากระยะไกลภายนอกองค์กร**	
	เพื่อให้มั่นใจว่า มี แนวทางการปฏิบัติงานจากระยะไกล เพื่อควบคุมการเข้าถึง การประมวลผล และจัดเก็บข้อมูลการใช้งาน รวมทั้งมีการสื่อสารให้พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องรับทราบ	1. สอบทานความมีอยู่จริงของแนวทางปฏิบัติงานจากระยะไกล และวิธีการ/ช่องทางการเผยแพร่แนวทางให้ผู้เกี่ยวข้องรับทราบ 2. สุ่มสัมภาษณ์ความเข้าใจในแนวทางฯ กับพนักงานที่เกี่ยวข้องและสังเกตการณ์การดำเนินงานตามที่แนวทางกำหนด

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.7 ความมั่นคงปลอดภัยด้านบุคลากร		
A.7.1	**ความมั่นคงปลอดภัยก่อนการจ้างงาน**	
A.7.1.1	**การคัดเลือกบุคลากร**	
	เพื่อให้มั่นใจว่า หน่วยงานบริหารทรัพยากรบุคคลมีการตรวจสอบประวัติการทำงานย้อนหลังของผู้สมัครตามกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง	สัมภาษณ์พนักงานและสอบทานเอกสารที่เกี่ยวข้องกับกระบวนการตรวจสอบคุณสมบัติของผู้สมัครก่อนการจ้างว่ามีความเหมาะสม สอดคล้องกับกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง เช่น เอกสารการตรวจสอบประวัติการศึกษา ประวัติคดีอาญา เป็นต้น
A.7.1.2	**ข้อตกลงและเงื่อนไขการจ้างงาน**	
	เพื่อให้มั่นใจว่า ข้อตกลงในการจ้างมีการระบุให้ผู้รับจ้างปฏิบัติตามกฎระเบียบ และระบุความรับผิดชอบด้านความมั่นคงปลอดภัยขององค์กร	สัมภาษณ์พนักงานและสอบทานเอกสารที่เกี่ยวข้องกับการจัดทำบันทึกตกลงสภาพการจ้างว่ามีการระบุให้ผู้รับจ้างปฏิบัติตามกฎ ระเบียบ และระบุความรับผิดชอบด้านความมั่นคงปลอดภัย
A.7.2	**ความมั่นคงปลอดภัยระหว่างการจ้างงาน**	
A.7.2.1	**หน้าที่ความรับผิดชอบของผู้บริหาร**	
	เพื่อให้มั่นใจว่า ผู้บริหารมีการกำกับดูแลให้พนักงานปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ	สอบทานระเบียบ ข้อบังคับว่ามีการกำหนดให้พนักงานปฏิบัติตามนโนบายด้านความมั่นคงปลอดภัย และมีการกำหนดให้มีกำกับดูแลตามสายบังคับบัญชา
A.7.2.2	**การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัย**	
	เพื่อให้มั่นใจว่า มีการสร้างความตระหนัก สร้างความรู้และฝึกอบรมเรื่องนโยบายความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ	สัมภาษณ์พนักงานและสอบทานเอกสารที่เกี่ยวข้องกับการฝึกอบรมเพื่อสร้างความตระหนักด้านนโยบายความมั่นคงปลอดภัยฯ และกระบวนการปฏิบัติขององค์กร เช่น เอกสารการจัดอบรม รายชื่อผู้เข้าร่วมอบรม เป็นต้น

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.7.2.3	**กระบวนการวินัยเพื่อลงโทษ**	
	เพื่อให้มั่นใจว่า มีการกำหนดกระบวนการทางวินัย เพื่อลงโทษหากมีการละเมิดความมั่นคงปลอดภัย	สอบทานระเบียบ ข้อบังคับ หรือนโยบายความมั่นคงปลอดภัยว่ามีการกำหนดกระบวนการทางวินัยและบทลงโทษ หากมีการละเมิดความมั่นคงปลอดภัย
A.7.3	**การสิ้นสุดการจ้างงานหรือการเปลี่ยนการจ้างงาน**	
A.7.3.1	**การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบ**	
	เพื่อให้มั่นใจว่า หน่วยงานบริหารทรัพยากรบุคคลมีการกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของพนักงานที่พ้นสภาพหรือเปลี่ยนแปลงตำแหน่งงาน	สัมภาษณ์พนักงานและสอบทานเอกสารที่เกี่ยวข้องกับขั้นตอนการปฏิบัติเมื่อพนักงานสิ้นสุดการจ้างหรือเปลี่ยนแปลงตำแหน่งงาน
A.8 การบริหารจัดการทรัพย์สิน		
A.8.1	**หน้าที่ความรับผิดชอบต่อทรัพย์สิน**	
A.8.1.1	**บัญชีทรัพย์สิน**	
	เพื่อให้มั่นใจว่า มีการจัดทำบัญชีทรัพย์สิน โดยมีรายการทรัพย์สินที่เกี่ยวข้องกับสารสนเทศหรือการประมวลผลสารสนเทศครบถ้วนและเป็นปัจจุบัน	1. สัมภาษณ์พนักงานที่เกี่ยวข้อง เรื่องกระบวนการจัดทำบัญชีทรัพย์สินสารสนเทศ 2. สอบทานความมีอยู่จริงของบัญชีทรัพย์สินและสอบทานความครบถ้วน ความเป็นปัจจุบันของรายการทรัพย์สินในบัญชีทรัพย์สิน
A.8.1.2	**ผู้ถือครองทรัพย์สิน**	
	เพื่อให้มั่นใจว่า บัญชีทรัพย์สินสารสนเทศ มีผู้รับผิดชอบทุกรายการ	สอบทานบัญชีทรัพย์สินสารสนเทศว่ารายการทรัพย์สินทุกรายการมีการระบุสถานที่จัดเก็บ และผู้รับผิดชอบ
A.8.1.3	**การใช้งานทรัพย์สินอย่างเหมาะสม**	
	เพื่อให้มั่นใจว่า มีข้อกำหนดหรือแนวทางการใช้ทรัพย์สินสารสนเทศอย่างเหมาะสม	สอบทานนโยบายความมั่นคงปลอดภัยว่ามีการระบุข้อกำหนดและข้อปฏิบัติในการใช้งานทรัพย์สินสารสนเทศ

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.8.1.4	**การคืนทรัพย์สิน**	
	เพื่อให้มั่นใจว่า หน่วยงานบริหารทรัพยากรบุคคลมีการกำหนดให้พนักงานคืนทรัพย์สินทั้งหมดที่ถือครองเมื่อสิ้นสุดการจ้างงาน	สัมภาษณ์พนักงานและสอบทานเอกสารที่เกี่ยวข้องเกี่ยวกับขั้นตอนคืนทรัพย์สินเมื่อพนักงานสิ้นสุดการจ้างหรือเปลี่ยนแปลงตำแหน่งงาน
A .8.2	**การจัดชั้นความลับของสารสนเทศ**	
A.8.2.1	**การจัดแบ่งประเภทของสารสนเทศ**	
	เพื่อให้มั่นใจว่า สารสนเทศมีการแบ่งชั้นความลับเป็นไปตามข้อกำหนดทางกฎหมาย ระดับความสำคัญ และระดับผลกระทบต่อองค์กร	1. สอบทานความมีอยู่จริงของข้อปฏิบัติในการจัดชั้นความลับของข้อมูลและขั้นตอนการปฏิบัติงานการจัดระดับชั้นความลับของข้อมูลในนโยบาย 2. สุ่มสัมภาษณ์พนักงานที่เกี่ยวข้องและสอบทานเอกสารการจัดแบ่งชั้นความลับสารสนเทศว่ามีการดำเนินงานตามนโยบาย
A.8.2.2	**การบ่งชี้สารสนเทศ**	
	เพื่อให้มั่นใจว่า มีขั้นตอนปฏิบัติการบ่งชี้สารสนเทศเหมาะสมสอดคล้องกับประเภทของสารสนเทศ	1. สอบทานความมีอยู่จริงของขั้นตอนปฏิบัติการบ่งชี้สารสนเทศว่าเหมาะสมสอดคล้องกับประเภทของสารสนเทศในนโยบาย 2. สุ่มสัมภาษณ์พนักงานที่เกี่ยวข้องและสุ่มสอบทานเอกสารที่มีการจัดแบ่งชั้นความลับว่ามีการบ่งชี้สารสนเทศตามนโยบาย
A.8.2.3	**การจัดการสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีขั้นตอนปฏิบัติการจัดการ/จัดเก็บสารสนเทศเหมาะสม สอดคล้องกับประเภทของสารสนเทศ	1. สอบทานความมีอยู่จริงของขั้นตอนปฏิบัติการจัดการ/จัดเก็บสารสนเทศว่าเหมาะสม สอดคล้องกับประเภทของสารสนเทศในนโยบาย 2. สุ่มสัมภาษณ์พนักงานที่เกี่ยวข้องและสุ่มสอบทานการจัดการ/การจัดเก็บสารสนเทศตามนโยบาย

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.8.3	**การจัดการสื่อบันทึกข้อมูล**	
A.8.3.1	**การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้**	
	เพื่อให้มั่นใจว่า มีการกำหนดแนวทางการบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้เหมาะสม สอดคล้องกับประเภทของสารสนเทศ	สอบทานความมีอยู่จริงของขั้นตอนปฏิบัติการจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ว่ามีความเหมาะสม สอดคล้องกับประเภทของสารสนเทศในนโยบาย
A.8.3.2	**การทำลายสื่อบันทึกข้อมูล**	
	เพื่อให้มั่นใจว่า มีขั้นตอนปฏิบัติการทำลายข้อมูลบนสื่อบันทึกข้อมูลเหมาะสม สอดคล้องกับประเภทของสารสนเทศ	1. สอบทานความมีอยู่จริงของขั้นตอนปฏิบัติการทำลายข้อมูลบนสื่อบันทึกข้อมูล และสอบทานว่าขั้นตอนมีความเหมาะสม สอดคล้องกับประเภทของสารสนเทศในนโยบาย 2. สุ่มสอบทานหลักฐานการทำลายสื่อบันทึกข้อมูลว่าเป็นไปตามนโยบาย
A.8.3.3	**การขนย้ายสื่อบันทึกข้อมูล**	
	เพื่อให้มั่นใจว่า มีขั้นตอนปฏิบัติการขนย้ายสื่อบันทึกข้อมูลเหมาะสม สอดคล้องกับประเภทของสารสนเทศ	1. สอบทานความมีอยู่จริงของขั้นตอนปฏิบัติการขนย้ายสื่อบันทึกข้อมูล และสอบทานว่าขั้นตอนมีความเหมาะสม สอดคล้องกับประเภทของสารสนเทศในนโยบาย 2. สุ่มสังเกตการณ์การขนย้ายสื่อบันทึกข้อมูลว่ามีการขนย้ายเป็นไปตามนโยบาย
A.9 การควบคุมการเข้าถึง		
A.9.1	**ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึง**	
A.9.1.1	**นโยบายการควบคุมการเข้าถึง**	
	เพื่อให้มั่นใจว่า มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเหมาะสม และมีการทบทวนอย่างสม่ำเสมอ	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การจัดทำนโยบายการควบคุมการเข้าถึง และการกำหนดระยะเวลาทบทวน 2. สอบทานเนื้อหานโยบายการควบคุมการเข้าถึงว่ามีเนื้อหาเหมาะสม เช่น การบริหารจัดการรหัสผ่าน การพิสูจน์ตัวตน และการเข้าถึงศูนย์คอมพิวเตอร์ เป็นต้น

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.9.1.2	**การเข้าถึงเครือข่ายและบริการเครือข่าย**	
	เพื่อให้มั่นใจว่า ผู้ใช้งานสามารถเข้าถึงเครือข่ายและบริการเครือข่ายเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง แนวทาง/นโยบายการจัดการความมั่นคงปลอดภัยสำหรับเครือข่าย 2. สอบทานเนื้อหาแนวทาง/นโยบายการจัดการความมั่นคงปลอดภัยสำหรับเครือข่ายว่ามีเนื้อหาเหมาะสม เช่น การลงทะเบียน/ขอสิทธิการเข้าถึงเครือข่าย แนวทางการจัดแบ่งเครือข่าย เป็นต้น
A.9.1	**การบริหารจัดการการเข้าถึงของผู้ใช้งาน**	
A.9.2.1	**การลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน**	
	เพื่อให้มั่นใจว่า มีขั้นตอนปฏิบัติการลงทะเบียนผู้ใช้งานใหม่และขั้นตอนปฏิบัติการถอดถอนสิทธิการใช้งานเมื่อออกจากองค์กร	สอบทานความมีอยู่จริงของขั้นตอนการลงทะเบียนและขั้นตอนการถอดถอนสิทธิการใช้งานในนโยบาย
A.9.2.2	**การจัดการสิทธิการเข้าถึงของผู้ใช้งาน**	
	เพื่อให้มั่นใจว่าการกำหนดระดับสิทธิการเข้าถึงระบบงาน ระบบปฏิบัติการ ระบบฐานข้อมูล หรือระบบงานอื่นๆ เหมาะสมต่อความจำเป็นในการใช้งานของผู้ใช้งานแต่ละตำแหน่ง	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การจัดทำตารางกำหนดสิทธิ 2. สอบทานความมีอยู่จริงของตารางกำหนดสิทธิการเข้าถึงระบบงาน ระบบปฏิบัติการ ระบบฐานข้อมูลของแต่ละตำแหน่งงาน
A.9.2.3	**การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ**	
	เพื่อให้มั่นใจว่า มีการจำกัด การควบคุม และการจัดสรรสิทธิระดับสูงอย่างเหมาะสม	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การบริหารจัดการสิทธิระดับสูง 2. สอบทานการจัดการสิทธิการเข้าถึงระดับสูง เช่น Root เป็นต้น ว่ามีการระบุตัวตนผู้ใช้สิทธิ มีการควบคุม และการจัดเก็บที่เหมาะสม

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.9.2.4	**การบริหารจัดการข้อมูลความลับสำหรับพิสูจน์ตัวตนผู้ใช้งาน**	
	เพื่อให้มั่นใจว่า มีการแนวทางการกำหนดรหัสผ่านที่ปลอดภัยและมีขั้นตอนการจัดสรรรหัสผ่าน	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง แนวทางการกำหนดรหัสผ่านและการจัดสรรรหัสผ่านในนโยบาย 2. สุ่มสอบทานหลักฐานการขอรหัสผ่านและรหัสผ่านที่กำหนดให้ว่าดำเนินการตามแนวทางที่กำหนด
A.9.2.5	**การทบทวนสิทธิของผู้ใช้งาน**	
	เพื่อให้มั่นใจว่า มีขั้นตอนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานและมีการปฏิบัติตาม	1. สอบทานความมีอยู่จริงของขั้นตอนการทบทวนสิทธิการเข้าถึงในนโยบาย 2. สุ่มสอบทานหลักฐานการทบทวนสิทธิและสุ่มสอบทานสิทธิที่ได้รับในระบบงานเปรียบเทียบกับหลักฐานการทบทวนสิทธิ
A.9.2.6	**การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง**	
	เพื่อให้มั่นใจว่า มีขั้นตอนถอดถอนสิทธิหรือปรับปรุงสิทธิการเข้าถึงของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน	1. สอบทานความมีอยู่จริงของขั้นตอนถอดถอนหรือปรับปรุงสิทธิการเข้าถึงของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน 2. สุ่มสอบทานผู้ใช้งานที่โอนย้ายตำแหน่งว่ามีการถอดถอนสิทธิตำแหน่งเดิม และมีการกำหนดสิทธิตำแหน่งใหม่ตามตารางกำหนดสิทธิ
A.9.3	**หน้าที่ความรับผิดชอบของผู้ใช้งาน**	
A.9.3.1	**การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ**	
	เพื่อให้มั่นใจว่า ผู้ใช้งานมีการใช้งานรหัสผ่านเป็นไปตามที่นโยบายกำหนด	1. สอบทานการกำหนดรหัสผ่านของผู้ใช้งานใน Password Policy บน Domain Controller ว่าเป็นไปตามแนวทางที่กำหนดในนโยบาย 2. สุ่มสังเกตการณ์การจัดเก็บรหัสผ่านของผู้ใช้งาน

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.9.4	**การควบคุมการเข้าถึงระบบ**	
A.9.4.1	**การจำกัดการเข้าถึงสารสนเทศ**	
	เพื่อให้มั่นใจว่า การเข้าถึงสารสนเทศหรือฟังก์ชันต่าง ๆ ในระบบงานมีการควบคุมให้สอดคล้องกับหน้าที่ความรับผิดชอบ	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การบริหารจัดการการเข้าถึงสารสนเทศของพนักงานแต่ละตำแหน่ง 2. สอบทานความเหมาะสมในการกำหนดสิทธิของผู้ใช้งานแต่ละตำแหน่งงานจากตารางกำหนดสิทธิ เช่น โปรแกรมเมอร์ไม่ควรได้รับสิทธิเข้าเพื่อแก้ไขหรือปรับปรุงระบบงานในระหว่างปฏิบัติงานจริงควรได้สิทธิแก้ไขจากระบบงานทดสอบไม่ใช่ระบบงานที่อยู่ระหว่างปฏิบัติงาน เป็นต้น
A.9.4.2	**ความมั่นคงปลอดภัยในการเข้าถึงระบบ**	
	เพื่อให้มั่นใจว่า ระบบงานได้รับการควบคุม โดยขั้นตอนการ Log on ที่มั่นคงปลอดภัย	สุ่มสอบทานการกำหนดระยะเวลาสิ้นสุดการใช้งานของระบบงานเมื่อไม่มีกิจกรรมหรือการกำหนดระยะเวลาในการเชื่อมต่อระบบงาน (Session timeout)
A.9.4.3	**ระบบบริหารจัดการรหัสผ่าน**	
	เพื่อให้มั่นใจว่า มีการบริหารจัดการรหัสผ่านเป็นไปตามนโยบายและมีลักษณะการทำงานแบบตอบสนองผู้ใช้งาน (Interactive)	สุ่มสอบทานการเข้าถึงระบบงานว่าระบบงานมีการโต้ตอบ/แจ้งเตือนผู้ใช้งานเมื่อผู้ใช้งานเข้ารหัสไม่ถูกต้องหรือกำหนดรหัสผ่านใหม่ไม่ตรงตามนโยบาย
A.9.4.4	**การใช้โปรแกรมอรรถประโยชน์**	
	เพื่อให้มั่นใจว่า มีการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์	1. สอบทานความมีอยู่จริงของแนวทางการลงโปรแกรมอรรถประโยชน์ในนโยบาย 2. สุ่มสอบทานเครื่องคอมพิวเตอร์ที่ใช้งานว่าไม่มีการติดตั้งโปรแกรมอรรถประโยชน์ที่อยู่นอกเหนือจากที่องค์กรกำหนด และสุ่มทดสอบลงโปรแกรมโดยสิทธิของผู้ใช้งาน

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.9.4.5	**การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม**	
	เพื่อให้มั่นใจว่า มีการจำกัดและควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้องเรื่อง การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม 2. สุ่มทดสอบการเข้าถึงซอร์สโค้ดโปรแกรมที่สำคัญ
A.10 การเข้ารหัสข้อมูล		
A .10.1	**นโยบายการควบคุมการเข้ารหัสข้อมูล**	
A.10.1.1	**นโยบายการใช้มาตรการเข้ารหัสข้อมูล**	
	เพื่อให้มั่นใจว่า มีนโยบายการเข้ารหัสข้อมูลและมีการปฏิบัติตาม	สอบทานความมีอยู่จริงของนโยบายการควบคุมการเข้ารหัสข้อมูล และสุ่มสอบทานการเข้ารหัสข้อมูลว่าเป็นไปตามที่กำหนด
A.10.1.2	**การบริหารจัดการกุญแจเข้ารหัสข้อมูล**	
	เพื่อให้มั่นใจว่า มีนโยบายการใช้งาน การป้องกัน และการบริหารจัดการกุญแจเข้ารหัสข้อมูล	สอบทานความมีอยู่จริงของนโยบายการบริหารจัดการกุญแจเข้ารหัสข้อมูล และสุ่มสอบทานการจัดเก็บและระยะเวลาการจัดเก็บกุญแจเข้ารหัสข้อมูล
A.11 ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม		
A.11.1	**บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย**	
A.11.1.1	**ขอบเขตหรือบริเวณโดยรอบทางกายภาพ**	
	เพื่อให้มั่นใจว่า มีการกำหนดขอบเขตหรือบริเวณโดยรอบทางกายภาพที่ต้องมีการรักษาความมั่นคงปลอดภัย	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การกำหนดขอบเขตหรือบริเวณโดยรอบของศูนย์คอมพิวเตอร์ 2. สำรวจศูนย์คอมพิวเตอร์ว่าได้รับการแบ่งแยกพื้นที่เหมาะสมเป็นไปตามที่กำหนด
A.11.1.2	**การควบคุมการเข้าออกทางกายภาพ**	
	เพื่อให้มั่นใจว่า ศูนย์คอมพิวเตอร์มีการควบคุมการเข้าออกของพื้นที่เฉพาะผู้ที่มีสิทธิหรือผู้ที่ได้รับอนุญาต	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้องเรื่อง การจัดทำขั้นตอนปฏิบัติสำหรับเข้าออกศูนย์คอมพิวเตอร์ และวิธีการสื่อสารถึงผู้ที่เกี่ยวข้อง 2. สอบทานความมีอยู่จริงของเอกสารขั้นตอนสำหรับเข้าออกศูนย์คอมพิวเตอร์

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
		3. สอบทานวิธีการ/ช่องทางการสื่อสารขั้นตอนสำหรับเข้าออกศูนย์คอมพิวเตอร์ให้พนักงานที่เกี่ยวข้องรับทราบและปฏิบัติตาม 4. สุ่มสอบทานเอกสารการขออนุญาตเข้าออกศูนย์คอมพิวเตอร์ว่าได้รับอนุมัติจากผู้มีอำนาจ 5. สุ่มสอบทานเอกสารแบบบันทึกข้อมูลการเข้าออกศูนย์คอมพิวเตอร์ 6. สุ่มตรวจสอบการปฏิบัติตามขั้นตอนและความถูกต้องของการบันทึกข้อมูลการเข้าออกศูนย์คอมพิวเตอร์จากกล้องวงจรปิด
A.11.1.3	**การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและสิ่งอำนวยความสะดวก**	
	เพื่อให้มั่นใจว่า มีการออกแบบการรักษาความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงานและสิ่งอำนวยความสะดวกมีการออกแบบ และใช้งานอย่างเหมาะสม	สำรวจพื้นที่ห้องทำงานของหน่วยงานสารสนเทศ และศูนย์คอมพิวเตอร์ว่ามีโครงสร้างทางกายภาพ และมีการติดตั้งสิ่งอำนวยความสะดวกที่เหมาะสม เช่น มี Access Control หรือกล้องวงจรปิด เป็นต้น
A.11.1.4	**การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม**	
	เพื่อให้มั่นใจว่า ศูนย์คอมพิวเตอร์มีการป้องกันภัยทางธรรมชาติ การโจมตีหรือการบุกรุกจากภายนอก หรืออุบัติเหตุ	สำรวจพื้นที่ศูนย์คอมพิวเตอร์ว่ามีการป้องกันทางกายภาพที่เหมาะสม เช่น มีการติดตั้ง Fire Alarm, Air Condition, Smoke Detector, เครื่องตรวจความชื้น , ถังดับเพลิง เป็นต้น
A.11.1.5	**การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีขั้นตอนสำหรับการปฏิบัติงานในศูนย์คอมพิวเตอร์และมีการปฏิบัติตาม	1. สอบทานความมีอยู่จริงของขั้นตอนการปฏิบัติงานในศูนย์คอมพิวเตอร์ในนโยบาย 2. สุ่มตรวจสอบการเข้าปฏิบัติงานในศูนย์คอมพิวเตอร์จากกล้อง CCTV ว่ามีการปฏิบัติตามขั้นตอนที่กำหนด

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.11.1.6	**การกำหนดพื้นที่รับส่งสิ่งของ**	
	เพื่อให้มั่นใจว่า มีการแยกพื้นที่สำหรับส่งมอบทรัพย์สิน	สำรวจพื้นที่สำหรับการส่งมอบทรัพย์สินบริเวณศูนย์คอมพิวเตอร์ ว่ามีการแบ่งแยกพื้นที่ออกจากศูนย์คอมพิวเตอร์
A.11.2	**อุปกรณ์**	
A.11.2.1	**การจัดวางและป้องกันอุปกรณ์**	
	เพื่อให้มั่นใจว่า อุปกรณ์มีการจัดวางอย่างปลอดภัย เหมาะสม และผู้มีสิทธิเท่านั้นที่เข้าถึงอุปกรณ์ได้	สำรวจศูนย์คอมพิวเตอร์ว่าอุปกรณ์จัดวางอย่างที่ปลอดภัยและมีการควบคุม เช่น ติดตั้งอุปกรณ์ในตู้ Rack และมีผู้รับผิดชอบกุญแจตู้ Rack เป็นต้น
A.11.2.2	**ระบบและอุปกรณ์สนับสนุนการทำงาน**	
	เพื่อให้มั่นใจว่า อุปกรณ์ต่าง ๆ ได้รับการป้องกันจากการที่ไม่สามารถใช้งานได้	สำรวจศูนย์คอมพิวเตอร์ว่ามีการป้องกันการหยุดชะงักของอุปกรณ์ เช่น มีการติดตั้ง UPS สำรองไฟ ระบบควบคุมอุณหภูมิ และเครื่องกำเนิดไฟฟ้า เป็นต้น
A.11.2.3	**ความมั่นคงปลอดภัยของการจัดวางสายไฟฟ้าและสายสื่อสาร**	
	เพื่อให้มั่นใจว่า การเดินสายไฟฟ้าและสายสื่อสารมีการป้องกันและไม่ขัดขวางการทำงานหรือการแทรกแซงสัญญาณหรือการทำให้เสียหาย	สำรวจศูนย์คอมพิวเตอร์ว่ามีการจัดทำ Label และจัดระเบียบสายไฟ สายสื่อสาร และสายเคเบิ้ล
A.11.2.4	**การบำรุงรักษาอุปกรณ์**	
	เพื่อให้มั่นใจว่า มีการบำรุงรักษาอุปกรณ์ให้มีความพร้อมใช้งาน	สุ่มสอบทานสัญญาจ้างบำรุงรักษาอุปกรณ์เปรียบเทียบกับผลการบำรุงรักษาในรายงานการบำรุงรักษาอุปกรณ์ว่ามีการปฏิบัติเป็นไปตามสัญญาจ้าง

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.11.2.5	**การนำทรัพย์สินเข้าออกศูนย์คอมพิวเตอร์**	
	เพื่อให้มั่นใจว่า มีขั้นตอนการนำทรัพย์สินเข้าออกศูนย์คอมพิวเตอร์และมีการปฏิบัติตาม	1. สอบทานความมีอยู่จริงของขั้นตอนการนำทรัพย์สินเข้าออกศูนย์คอมพิวเตอร์ในโยบาย 2. สุ่มสังเกตการณ์การนำทรัพย์สินเข้าออกศูนย์คอมพิวเตอร์จากกล้องวงจรปิดว่ามีการปฏิบัติตามขั้นตอนที่กำหนด
A.11.2.6	**ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานนอกองค์กร**	
	เพื่อให้มั่นใจว่า มีการรักษาความปลอดภัยทรัพย์สินที่นำไปใช้งานนอกองค์กร	1. สอบทานความมีอยู่จริงของขั้นตอนการนำอุปกรณ์ไปใช้งานนอกสถานที่ในนโยบาย 2. สุ่มสังเกตการณ์การนำอุปกรณ์ไปใช้งานนอกสถานที่ว่ามีการปฏิบัติตามขั้นตอนที่กำหนด
A.11.2.7	**ความมั่นคงปลอดภัยของการกำจัดหรือการนำอุปกรณ์มาใช้งานใหม่**	
	เพื่อให้มั่นใจว่า อุปกรณ์สื่อบันทึกข้อมูลมีการตรวจสอบข้อมูลหรือซอฟต์แวร์สำคัญก่อนที่จะกำจัดหรือนำกลับมาใช้ใหม่	1. สอบทานความมีอยู่จริงของขั้นตอนการจัดการสื่อบันทึกข้อมูลในนโยบาย 2. สุ่มสอบทานสื่อบันทึกข้อมูลที่กลับมาใช้ใหม่ว่าไม่มีข้อมูลหรือซอฟต์แวร์ที่สำคัญ
A.11.2.8	**การรักษาความปลอดภัยอุปกรณ์ที่ไม่มีผู้ดูแล**	
	เพื่อให้มั่นใจว่า มีการกำหนดมาตรการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ดูแล	สุ่มสอบทานเครื่องคอมพิวเตอร์ว่ามีการป้องกันให้มีความปลอดภัยขณะที่ไม่มีการใช้งาน เช่น มีการปิดหน้าจอและกำหนดการเข้ารหัสในการใช้งาน เป็นต้น
A.11.2.9	**นโยบายการปลอดเอกสารสำคัญบนโต๊ะทำงานและหน้าจอคอมพิวเตอร์**	
	เพื่อให้มั่นใจว่า มีการเก็บเอกสารสำคัญไว้ในที่ปลอดภัย และมีการป้องกันหน้าจอคอมพิวเตอร์	1. สุ่มสังเกตการณ์การจัดเก็บเอกสารบนโต๊ะทำงานว่าไม่วางเอกสารประเภทลับลับมาก ลับที่สุดบนโต๊ะทำงาน 2. สุ่มสอบทานเครื่องคอมพิวเตอร์ว่ามีการป้องกันให้มีความปลอดภัยขณะที่ไม่มีการใช้งาน เช่น มีตั้งค่า Session time out หรือ Screen sever เป็นต้น

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.12 การรักษาความมั่นคงปลอดภัยด้านการดำเนินการ		
A.12.1	**ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ**	
A.12.1.1	**ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร**	
	เพื่อให้มั่นใจว่า มีขั้นตอนปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร และเป็นปัจจุบัน โดยเอกสารทั้งหมดได้รับการอนุมัติ และสื่อสารไปยังผู้ที่เกี่ยวข้อง	1. สุ่มสอบทานความมีอยู่จริง ความเป็นปัจจุบัน และการอนุมัติเอกสารขั้นตอนปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เช่น ขั้นตอนการปฏิบัติงานในศูนย์คอมพิวเตอร์ การสำรองข้อมูล การนำข้อมูลเข้าระบบงาน การกู้คืนระบบ เป็นต้น 2. สอบทานวิธีการ/ช่องทางการเผยแพร่ขั้นตอนการปฏิบัติให้ผู้ที่เกี่ยวข้องรับทราบ
A.12.1.2	**การบริหารจัดการการเปลี่ยนแปลง**	
	เพื่อให้มั่นใจว่า มีขั้นตอนปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลงแก้ไขที่มีผลกระทบต่อความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบัน โดยเอกสารทั้งหมดได้รับการอนุมัติ และสื่อสารไปยังผู้ที่เกี่ยวข้อง	1. สุ่มสอบทานความมีอยู่จริง ความเป็นปัจจุบัน และการอนุมัติเอกสารขั้นตอนปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบเทคโนโลยีสารสนทศ 2. สอบทานวิธีการ/ช่องทางการเผยแพร่ขั้นตอนปฏิบัติงานให้ผู้ที่เกี่ยวข้องรับทราบ
A.12.1.3	**การบริหารจัดการขีดความสามารถของระบบ**	
	เพื่อให้มั่นใจว่า มีการขั้นตอน/แผนการบริหารจัดการทรัพยากรระบบสารสนเทศอย่างเหมาะสม	สุ่มสอบทานความมีอยู่จริงของขั้นตอน/แผนการบริหารจัดการทรัพยากร เช่น ขั้นตอนการติดตั้งอุปกรณ์เพื่อติดตามเฝ้าระวังและตรวจสอบ Capacity ของ CPU และมีการวิเคราะห์ผล เพื่อตรวจสอบความเพียงพอต่อการใช้งาน เป็นต้น
A.12.1.4	**การแยกสภาพแวดล้อมสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน**	
	เพื่อให้มั่นใจว่า มีการการแยกสภาพแวดล้อมสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน	สุ่มสอบทานเครื่องที่ใช้ในการพัฒนาหรือทดสอบระบบงานว่ามีการการแยกระบบออกจากเครื่องที่ให้บริการระบบจริง

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.12.2	**การป้องกันโปรแกรมไม่ประสงค์ดี**	
A.12.2.1	**มาตรการป้องกันโปรแกรมไม่ประสงค์ดี**	
	เพื่อให้มั่นใจว่า มีมาตรการในการป้องกันโปรแกรมไม่ประสงค์ดี และมีการสร้างความตระหนักในการจัดการโปรแกรมไม่ประสงค์ดี	1. สุ่มสอบทานเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ตั้งโต๊ะว่ามีการติดตั้ง Anti-virus และตั้ง Auto Update ทุกวัน 2. สอบทานวิธีการ/ช่องทางการเผยแพร่การสร้างความตระหนักในการจัดการโปรแกรมไม่ประสงค์ดี และสุ่มสอบถามผู้ใช้งานเรื่องการจัดการโปรแกรมไม่ประสงค์ดี
A.12.3	**การสำรองข้อมูล**	
A.12.3.1	**การสำรองข้อมูล**	
	เพื่อให้มั่นใจว่า มีขั้นตอนการสำรองข้อมูลและทดสอบข้อมูลที่สำรองอย่างสม่ำเสมอ	1. สอบทานความมีอยู่จริงของขั้นตอนปฏิบัติการสำรองข้อมูลและทดสอบข้อมูลที่สำรองในนโยบาย 2. สุ่มสอบทานข้อมูลที่สำรองและรายงานผลการทดสอบข้อมูลที่สำรอง
A.12.4	**การบันทึกข้อมูลล็อกและการเฝ้าระวัง**	
A.12.4.1	**การบันทึกข้อมูลล็อกแสดงเหตุการณ์**	
	เพื่อให้มั่นใจว่า มีขั้นตอนการเฝ้าระวัง ตรวจสอบ และบันทึกข้อมูลล็อกอย่างเหมาะสม และเป็นไปตามกฎหมายที่เกี่ยวข้อง	1. สอบทานความมีอยู่จริงของขั้นตอนจัดเก็บข้อมูลล็อกและระยะเวลาการจัดเก็บให้เป็นไปตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในนโยบาย 2. สุ่มสอบทานข้อมูลล็อกและระยะเวลาที่จัดเก็บข้อมูลล็อก
A.12.4.2	**การป้องกันข้อมูลล็อก**	
	เพื่อให้มั่นใจว่า อุปกรณ์บันทึกล็อกมีการป้องกันให้เฉพาะผู้มีสิทธิเข้าถึงได้	สอบทานเอกสารการกำหนดสิทธิการเข้าถึงอุปกรณ์บันทึกล็อกว่ามีความเหมาะสมและมีการทบทวนให้เป็นปัจจุบัน

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.12.4.3	**ข้อมูลล็อกและกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ**	
	เพื่อให้มั่นใจว่า มีการจัดเก็บข้อมูลล็อกของผู้ดูแลระบบ	สอบทานความมีอยู่จริงของการจัดเก็บข้อมูลล็อกเมื่อมีการดำเนินงานของผู้ดูแลระบบ
A.12.4.4	**การตั้งเวลาเครื่องคอมพิวเตอร์**	
	เพื่อให้มั่นใจว่า ระบบที่สำคัญทั้งหมดมีการตั้งเวลาให้ถูกต้องเทียบกับแหล่งอ้างอิงเวลา	1. สัมภาษณ์พนักงานที่เกี่ยวข้องเกี่ยวกับการตั้งเวลาของระบบประมวลผลสารสนเทศขององค์กร 2. สอบทานเวลาของระบบประมวลผลว่าถูกต้อง ตรงกันกับอุปกรณ์ที่ให้บริการเทียบเวลา NTP Server
A.12.5	**การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ**	
A.12.5.1	**การติดตั้งซอฟต์แวร์บนระบบให้บริการ**	
	เพื่อให้มั่นใจว่า มีขั้นตอนปฏิบัติการติดตั้งซอฟต์แวร์บนระบบให้บริการ และมีการอนุมัติการติดตั้งจากผู้มีอำนาจ	1. สอบทานความมีอยู่จริงขั้นตอนปฏิบัติการติดตั้งซอฟต์แวร์บนระบบให้บริการในนโยบาย 2. สุ่มสอบทานการติดตั้งซอฟต์แวร์บนระบบให้บริการว่ามีการปฏิบัติตามขั้นตอนและได้รับอนุมัติจากผู้มีอำนาจ
A.12.6	**การบริหารจัดการช่องโหว่ทางเทคนิค**	
A.12.6.1	**การบริหารจัดการช่องโหว่ทางเทคนิค**	
	เพื่อให้มั่นใจว่า มีการบริหารจัดการช่องโหว่อย่างเหมาะสม ทันเวลา	สัมภาษณ์พนักงานและสอบทานเอกสารที่เกี่ยวข้องเกี่ยวกับการติดตาม เฝ้าระวัง และประเมินความเสี่ยงช่องโหว่ที่เกิดขึ้น และมาตรการจัดการช่องโหว่ที่เกิดขึ้น
A.12.6.2	**การจำกัดการติดตั้งซอฟต์แวร์**	
	เพื่อให้มั่นใจว่า มีการควบคุมการติดตั้งซอฟต์แวร์	สัมภาษณ์พนักงานที่เกี่ยวข้องเกี่ยวกับสิทธิการติดตั้งซอฟต์แวร์ว่ามีความเหมาะสมและเป็นปัจจุบัน และสอบทานเอกสารกำหนดสิทธิการติดตั้งซอฟต์แวร์

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.12.7	**สิ่งที่ต้องพิจารณาในการตรวจประเมิน**	
A.12.7.1	**มาตรการการตรวจประเมินระบบ**	
	เพื่อให้มั่นใจว่า มีการวางแผนการตรวจสอบอย่างเหมาะสมและคำนึงถึงความมั่นคงปลอดภัย ความต่อเนื่องของระบบ	สัมภาษณ์พนักงานและสอบทานเอกสารที่เกี่ยวข้องกับการตรวจสอบจากหน่วยงานภายในองค์กร
A.13 ความมั่นคงปลอดภัยด้านการสื่อสารข้อมูล		
A.13.1	**การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย**	
A.13.1.1	**มาตรการเครือข่าย**	
	เพื่อให้มั่นใจว่า มีการบริหารจัดการและควบคุมการเครือข่ายอย่างเหมาะสม	สัมภาษณ์พนักงานและสอบทานเอกสารที่เกี่ยวข้องเกี่ยวกับการแบ่งแยกโซนเครือข่าย การแบ่งแยก VLAN กลุ่มผู้ใช้งาน
A.13.1.2	**ความมั่นคงปลอดภัยสำหรับการบริการเครือข่าย**	
	เพื่อให้มั่นใจว่า มีการกำหนดข้อตกลงระดับการให้บริการเครือข่ายไว้อย่างเหมาะสม สำหรับการให้บริการภายในองค์กรและสำหรับผู้ให้บริการภายนอก	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่องการกำหนดข้อตกลงระดับการให้บริการเครือข่ายภายในองค์กรและผู้ให้บริการเครือข่ายภายนอก 2. สอบทานความมีอยู่จริงของเอกสารการกำหนดข้อตกลงระดับการให้บริการเครือข่ายภายในและภายนอกองค์กร 3. สุ่มสอบทานสัญญาจ้างผู้ให้บริการเครือข่ายว่ามีการกำหนดข้อตกลงระดับการให้บริการ
A.13.1.3	**การแบ่งแยกเครือข่าย**	
	เพื่อให้มั่นใจว่า มีการแบ่งแยกเครือข่ายระหว่างผู้ใช้งาน ผู้ดูแลระบบและผู้ให้บริการสนับสนุนเครือข่าย	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การแบ่งแยกเครือข่ายสำหรับระบบทั่วไปกับระบบที่มีความสำคัญ 2. สอบทานความมีอยู่จริง และความเป็นปัจจุบันของเอกสารการแบ่งแยกเครือข่าย

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.13.2	**การแลกเปลี่ยนสารสนเทศ**	
A.13.2.1	**นโยบายและขั้นตอนการแลกเปลี่ยนสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการกำหนดนโยบายและขั้นตอนการแลกเปลี่ยนสารสนเทศอย่างเหมาะสม	สอบทานความมีอยู่จริงของขั้นตอนการแลกเปลี่ยนสารสนเทศในนโยบาย
A.13.2.2	**ข้อตกลงการแลกเปลี่ยนสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการกำหนดข้อตกลงการแลกเปลี่ยนสารสนเทศระหว่างองค์กรกับหน่วยงานภายนอก	สุ่มสอบทานสัญญาจ้างหน่วยงานภายนอกที่เกี่ยวข้องกับการให้บริการเครือข่ายว่ามีการกำหนดข้อตกลงการการแลกเปลี่ยนสารสนเทศขององค์กรกับหน่วยงานภายนอก
A.13.2.3	**การส่งข้อความทางอิเล็กทรอนิกส์**	
	เพื่อให้มั่นใจว่า มีการกำหนดแนวทางการส่งข้อความทางอิเล็กทรอนิกส์อย่างมั่นคงปลอดภัย	1. สอบทานความมีอยู่จริงของแนวทางการส่งข้อความทางอิเล็กทรอนิกส์ในนโยบาย 2. สุ่มสอบทานการส่งข้อความทางอีเมล์ว่ามีการปฏิบัติตามแนวทางที่กำหนด
A.13.2.4	**ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ**	
	เพื่อให้มั่นใจว่า มีการกำหนดข้อตกลงการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูลสารสนเทศขององค์กรกับหน่วยงานภายนอก	สุ่มสอบทานสัญญาจ้างหน่วยงานภายนอกที่เกี่ยวข้องกับการให้บริการเครือข่ายว่ามีการกำหนดให้รักษาความลับหรือการไม่เปิดเผยสารสนเทศขององค์กร
A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ		
A.14.1	**ความต้องการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ**	
A.14.1.1	**การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการกำหนดข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศในกระบวนการจัดหา พัฒนาและปรับปรุงระบบสารสนเทศ	สุ่มสอบทานสัญญาจ้างจัดหา/พัฒนาระบบใหม่/ปรับปรุงระบบสารสนเทศเดิมว่ามีการกำหนดให้ปฏิบัติตามนโยบายความมั่นคงปลอดภัยขององค์กรในส่วนการปฏิบัติงานของหน่วยงานภายนอก

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.14.1.2	**ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ**	
	เพื่อให้มั่นใจว่า มีกระบวนการจัดการ/ป้องกันข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายสาธารณะจากการถูกเปิดเผยหรือเปลี่ยนแปลงแก้ไขจากผู้ที่ไม่มีสิทธิ	1. สอบทานความมีอยู่จริงของแนวทางการรักษาความมั่นคงปลอดภัยการให้บริการโปรแกรมบนเครือข่ายสาธารณะในนโยบาย 2. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การวิเคราะห์ช่องโหว่หรือการทดสอบเจาะระบบที่มีการส่งข้อมูลผ่านเครือข่ายสาธารณะ รวมทั้งสอบทานความมีอยู่จริงของเอกสารการวิเคราะห์ช่องโหว่หรือเอกสารรายงานการทดสอบเจาะระบบ
A.14.1.3	**การป้องกันธุรกรรมของบริการสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีกระบวนการจัดการป้องกันข้อมูลสารสนเทศบนธุรกรรมออนไลน์จากการรับส่งข้อมูลสารสนเทศไม่สมบูรณ์ ผิดเส้นทาง หรือมีการเปลี่ยนแปลงแก้ไขจากผู้ที่ไม่มีสิทธิ	1. สอบทานความมีอยู่จริงของแนวทางการรักษาความมั่นคงปลอดภัยการทำธุรกรรมออนไลน์ในนโยบาย 2. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การวิเคราะห์ช่องโหว่หรือการทดสอบเจาะระบบที่เกี่ยวข้องกับธุรกรรมออนไลน์ รวมทั้งสอบทานความมีอยู่จริงของเอกสารการวิเคราะห์ช่องโหว่หรือเอกสารรายงานการทดสอบเจาะระบบ
A.14.2	**ความมั่นคงปลอดภัยในกระบวนการพัฒนาและสนับสนุน**	
A.14.2.1	**นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย**	
	เพื่อให้มั่นใจว่า มีการกำหนดข้อตกลงในการพัฒนาระบบให้มีความมั่นคงปลอดภัย และมีการตรวจสอบว่ามีการปฏิบัติตามข้อตกลง	1. สอบทานความมีอยู่จริงของแนวทางการพัฒนาระบบของหน่วยงานภายนอกในนโยบายและสุ่มสอบทานสัญญาจ้างพัฒนาระบบว่ามีการกำหนดให้หน่วยงานภายนอกปฏิบัติตามนโยบายขององค์กร 2. สุ่มสอบทานเอกสารการรายงานความก้าวหน้าของการพัฒนาระบบงานว่ามีการติดตาม/ตรวจสอบการปฏิบัติตามข้อตกลง

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.14.2.2	**ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ**	
	เพื่อให้มั่นใจว่า มีการกำหนดแนวทางการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ รวมถึงการทดสอบหลังการเปลี่ยนแปลง โดยได้รับการอนุมัติ การประเมินผลกระทบจากผู้มีอำนาจ และมีการรายงานผลการดำเนินการทุกครั้ง	1. สอบทานความมีอยู่จริงของแนวทางการจัดการเปลี่ยนแปลงในนโยบาย และสอบทานว่ามีการกำหนดอย่างเหมาะสม เช่น กำหนดแบบฟอร์ม กำหนดการประเมินผลกระทบการดำเนินการ กำหนดผู้อนุมัติ กำหนดการทดสอบการเปลี่ยนแปลง เป็นต้น 2. สุ่มสอบทานเอกสารการเปลี่ยนแปลงหรือแก้ไขระบบที่สำคัญจากข้อมูล Log ว่ามีการปฏิบัติตามแนวทางที่กำหนด
A.14.2.3	**การทบทวนค่าทางเทคนิคของแอพพลิเคชั่นภายหลังการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ**	
	เพื่อให้มั่นใจว่า การดำเนินการเปลี่ยนแปลงโครงสร้างพื้นฐานระบบที่สำคัญมีการทบทวนและทดสอบว่าไม่มีผลกระทบต่อการปฏิบัติงานและไม่มีผลกระทบด้านความมั่นคงปลอดภัย	สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้องและสอบทานเอกสารเกี่ยวกับการทบทวนและทดสอบภายหลังการดำเนินการเปลี่ยนแปลงโครงสร้างพื้นฐานระบบที่สำคัญ เพื่อให้มั่นใจว่าไม่มีผลกระทบต่อการปฏิบัติงานและระบบมีความมั่นคงปลอดภัย
A.14.2.4	**การจำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป**	
	เพื่อให้มั่นใจว่า มีการจำกัดและกำหนดผู้รับผิดชอบ ผู้อนุมัติในการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป	1. สอบทานความมีอยู่จริงของแนวทางการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูปในนโยบาย 2. สุ่มสอบทานหลักฐานการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูปว่าเป็นไปตามแนวทางที่กำหนด
A.14.2.5	**หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย**	
	เพื่อให้มั่นใจว่า มีการกำหนดหลักการวิศวกรรมระบบให้มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและเป็นปัจจุบัน	สอบทานเอกสาร Network Diagram ว่ามีการจัดทำอย่างมั่นคงปลอดภัย เป็นปัจจุบัน และมีการจัดเก็บอย่างเหมาะสมโดยให้มีการเข้าถึงได้เฉพาะผู้ที่เกี่ยวข้อง

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.14.2.6	**สภาพแวดล้อมการพัฒนาระบบที่มีความมั่นคงปลอดภัย**	
	เพื่อให้มั่นใจว่า มีการกำหนดและป้องกันสภาพแวดล้อมเพื่อใช้ในการพัฒนาระบบอย่างเหมาะสม และมีความมั่นคงปลอดภัย	สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การพัฒนาระบบว่ามีการแบ่งแยกสภาพแวดล้อมสำหรับการทดสอบระบบออกจากระบบที่ใช้งานจริง และมีการกำหนดสิทธิและตรวจสอบการเข้าถึงระบบ
A.14.2.7	**การพัฒนาระบบโดยหน่วยงานภายนอก**	
	เพื่อให้มั่นใจว่า มีการควบคุมดูแลการพัฒนาระบบที่จัดจ้างหน่วยงานภายนอกให้มีการดำเนินการพัฒนาอย่างเหมาะสม และมีความมั่นคงปลอดภัย	1. สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การควบคุมดูแลการพัฒนาระบบที่จัดจ้างหน่วยงานภายนอก 2. สุ่มสอบทานสัญญาจ้างหน่วยงานภายนอกว่ามีการกำหนดประเด็นสำคัญด้านความมั่นคงปลอดภัยในการพัฒนาระบบ เช่น ลิขสิทธิ์ทรัพย์สินทางปัญญา ข้อกำหนดหรือสัญญาการออกแบบด้านความมั่นคงปลอดภัยในการออกแบบ พัฒนา และการทดสอบระบบ เกณฑ์การยอมรับการส่งมอบที่มีคุณภาพ เป็นต้น
A.14.2.8	**การทดสอบการตรวจรับระบบ**	
	เพื่อให้มั่นใจว่า มีการแผนการทดสอบเพื่อรองรับระบบที่พัฒนาหรือระบบที่ได้รับการปรับปรุง และตรวจรับการทดสอบตามแผนการทดสอบ	สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การทดสอบการตรวจรับระบบ และสุ่มสอบทานรายงานการทดสอบและตรวจรับระบบ
A.14.3	**ข้อมูลสำหรับการทดสอบ**	
A.14.3.1	**การป้องกันข้อมูลสำหรับการทดสอบ**	
	เพื่อให้มั่นใจว่า มีการควบคุมดูแลการนำข้อมูลที่นำมาใช้ในการทดสอบอย่างเหมาะสมและรัดกุม	สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง แนวทางการเลือกข้อมูลที่ใช้สำหรับทดสอบว่ามีการควบคุมดูแลอย่างเหมาะสม เช่น การกำหนดสิทธิเมื่อมีการคัดลอกข้อมูลการดำเนินงานไปยังสภาพแวดล้อมของการทดสอบหรือการลบข้อมูลทันทีภายหลังจากการทดสอบข้อมูลเสร็จสิ้น เป็นต้น

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก		
A.15.1	**ความต้องการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ**	
A.15.1.1	**นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก**	
	เพื่อให้มั่นใจว่า มีแนวทางการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศระหว่างองค์กรกับผู้ให้บริการภายนอก	สอบทานความมีอยู่จริงของแนวทางการดำเนินงานด้านความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอกในนโยบาย เช่น การกำหนดการสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก เป็นต้น
A.15.1.2	**การระบุข้อกำหนดความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก**	
	เพื่อให้มั่นใจว่า มีการกำหนดข้อตกลงระหว่างองค์กรกับผู้ให้บริการภายนอกเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ	สุ่มสอบทานสัญญาจ้างผู้ให้บริการภายนอกว่ามีการกำหนดข้อความด้านความมั่นคงปลอดภัยตามแนวทางที่กำหนด
A.15.1.3	**ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารจากผู้ให้บริการภายนอก**	
	เพื่อให้มั่นใจว่า ข้อตกลงระหว่างองค์กรกับผู้ให้บริการภายนอกจะต้องรวมถึงข้อกำหนดที่เกี่ยวข้องกับความเสี่ยงที่เกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก	สุ่มสอบทานสัญญาจ้างผู้ให้บริการภายนอกว่ามีข้อกำหนดการควบคุมการดำเนินงานของผู้ให้บริการภายนอกและผู้ที่เกี่ยวข้องปฏิบัติตามข้อกำหนดขององค์กร
A.15.2	**การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก**	
A.15.2.1	**การติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอก**	
	เพื่อให้มั่นใจว่า มีการติดตามทบทวนการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ	สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้องและสอบทานเอกสารการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอก เช่น รายงานผลการดำเนินงานและข้อผิดปกติ เอกสารการประเมินผลการบริการ เป็นต้น

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.15.2.2	**การบริหารจัดการการเปลี่ยนแปลงของผู้ให้บริการภายนอก**	
	เพื่อให้มั่นใจว่า มีการแนวทางการบริหารจัดการการเปลี่ยนแปลงการให้บริการจากผู้ให้บริการภายนอก	สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้องและสอบทานเอกสารเกี่ยวกับการบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก เช่น การประชุมกับผู้ให้บริการภายนอกเป็นระยะ และหารือถึงแนวทางพัฒนาการดำเนินงานให้ดียิ่งขึ้น การทบทวนรายละเอียดการเปลี่ยนแปลงรายละเอียดสัญญาจ้างงานทุกปีตามรอบระยะเวลาการจ้าง เป็นต้น
A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ		
A.16.1	**ความต้องการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ**	
A.16.1.1	**หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ**	
	เพื่อให้มั่นใจว่า มีการกำหนดหน้าที่ความรับผิดชอบและแนวทางการปฏิบัติงานเพื่อตอบสนองต่อเหตุขัดข้องได้อย่างทันท่วงทีและมีประสิทธิภาพ	สอบทานความมีอยู่จริงของการกำหนดหน้าที่ความรับผิดชอบการปฏิบัติงานจากขั้นตอนการจัดการเหตุขัดข้องในนโยบาย
A.16.1.2	**การรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการกำหนดขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม	สอบทานความมีอยู่จริงของขั้นตอนการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศในนโยบาย
A.16.1.3	**การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า พนักงาน คู่สัญญาและผู้ใช้งานจากภายนอกมีส่วนร่วมในการแจ้งและรายงานสิ่งที่สังเกตพบหรือสิ่งต้องสงสัยเกี่ยวกับความมั่นคงปลอดภัยที่พบในระบบหรือบริการ	สุ่มสอบทานเอกสารบันทึกการแจ้ง Incident ที่แจ้งผ่านทาง Helpdesk และรายงาน Service Report จาก Vendor

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.16.1.4	**การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการกำหนดเกณฑ์การประเมินสถานการณ์ความมั่นคงปลอดภัย	1. สอบทานความมีอยู่จริงของเกณฑ์สำหรับการประเมินเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศเพื่อบริหารจัดการและแก้ไขเหตุการณ์ไม่พึงประสงค์จากเอกสารวิธีปฏิบัติการแก้ไขเหตุขัดข้อง 2. สุ่มสอบทานรายการบันทึก Incident ที่เกิดขึ้นว่ามีการประเมินเหตุขัดข้องตามที่กำหนดไว้
A.16.1.5	**การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า สถานการณ์ความมั่นคงปลอดภัยได้รับการตอบสนองเพื่อจัดการปัญหาตามขั้นตอนที่กำหนดไว้	1. สอบทานความมีอยู่จริงของแนวทางการตอบสนองหรือการจัดการปัญหาจากขั้นตอนการจัดการเหตุขัดข้องในนโยบาย 2. สุ่มสอบทานรายการบันทึก Incident ที่เกิดขึ้นว่าได้รับการแก้ไขตามที่กำหนดไว้
A.16.1.6	**การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า ความรู้ ความเข้าใจจากการวิเคราะห์ และการแก้ไขเหตุการณ์ความมั่นคงความปลอดภัยสารสนเทศถูกนำมาใช้เพื่อลดโอกาส หรือผลกระทบของเหตุการณ์ที่อาจเกิดในอนาคต	สุ่มสอบทานเอกสารเกี่ยวกับการวิเคราะห์และการแก้ไข Incident ว่ามีการจัดทำสรุปจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อหาแนวทางในการแก้ไขระยะยาว
A.16.1.7	**การเก็บรวบรวมหลักฐาน**	
	เพื่อให้มั่นใจว่า มีการกำหนดแนวทางการระบุ รวบรวม จัดหาและจัดเก็บหลักฐานข้อมูลสารสนเทศ	สัมภาษณ์ผู้บริหารและพนักงานที่เกี่ยวข้อง เรื่อง การรวบรวมหลักฐานเมื่อเหตุการณ์ที่เกิดขึ้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย และสุ่มสอบทานการจัดเก็บข้อมูล Log ระบบงานที่สำคัญว่าเป็นไปตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ		
A.17.1	**ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ**	
A.17.1.1	**การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีข้อกำหนดสำหรับความมั่นคงปลอดภัยสารสนเทศและความต่อเนื่องสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในสถานการณ์ร้ายแรง	สอบทานความมีอยู่จริงของข้อกำหนดการวางแผนเตรียมการสภาพความพร้อมใช้ของระบบงานในนโยบาย ว่ามีการประเมินผลกระทบทางธุรกิจกรณีระบบงานหยุดชะงักและกำหนดระดับความสำคัญของระบบงาน มีการกำหนดค่า MTPD (Maximum Tolerable Period of Disruption) ค่า MTDL (Maximum Tolerable Data Loss) และค่า RTO (Recovery Time Objective)
A.17.1.2	**การดำเนินการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan : BCP) อย่างเป็นลายลักษณ์อักษร โดยได้รับอนุมัติจากผู้มีอำนาจและเผยแพร่อย่างทั่วถึง	สอบทานความมีอยู่จริง ความเป็นปัจจุบัน การอนุมัติจากผู้มีอำนาจ และการสื่อสาร BCP
A.17.1.3	**การตรวจสอบ ทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการทดสอบมาตรการต่าง ๆ ใน BCP ว่าสามารถใช้งานได้และมีประสิทธิภาพเมื่อเกิดเหตุเสียหายตามระยะเวลาที่กำหนด	สอบทานหลักฐานผลการทดสอบและผลการประเมินมาตรการตาม BCP ว่าเป็นไปตามขั้นตอนและระยะเวลาที่กำหนดใน BCP

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.17.2	**การเตรียมอุปกรณ์ประมวลผลสำรอง**	
A.17.2.1	**ความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการสำรองอุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอตรงตามความต้องการและมีความพร้อมใช้งาน	สุ่มสอบทานสัญญาจ้างบำรุงรักษาอุปกรณ์ประมวลผลสารสนเทศของผู้ให้บริการภายนอก และข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ว่าอุปกรณ์มีความพร้อมใช้งานได้รับการบำรุงรักษาอย่างเหมาะสม และมีสำรองกรณีชำรุดเสียหายไม่สามารถซ่อมได้
A.18 การปฏิบัติตามข้อกำหนด		
A.18.1	**การปฏิบัติตามข้อกำหนดทางกฎหมายและสัญญา**	
A.18.1.1	**การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมายและสัญญา**	
	เพื่อให้มั่นใจว่า มีข้อกำหนดซึ่งเป็นประเด็นที่สำคัญทางกฎหมายโดยมีผลบังคับใช้หรือมีผลทางสัญญาที่ตรงตามข้อกำหนดขององค์กรไว้เป็นลายลักษณ์อักษร เป็นปัจจุบัน และเผยแพร่อย่างทั่วถึง	สอบทานความมีอยู่จริง และความเป็นปัจจุบันของการจัดทำรายการข้อกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศที่องค์กรต้องปฏิบัติ
A.18.1.2	**การป้องกันสิทธิและทรัพย์สินทางปัญญา**	
	เพื่อให้มั่นใจว่า มีการจัดทำขั้นตอนการปฏิบัติงานการจัดการลิขสิทธิ์ซอฟต์แวร์ และมีการบริหารจัดการลิขสิทธิ์ซอฟต์แวร์ที่อย่างเหมาะสม	สอบทานความมีอยู่จริงของขั้นตอนการปฏิบัติงานการจัดการลิขสิทธิ์ซอฟต์แวร์ในนโยบาย
A.18.1.3	**การป้องกันข้อมูล**	
	เพื่อให้มั่นใจว่า ข้อมูลได้รับการปกป้องจากการเข้าถึงของผู้ที่ไม่ได้รับอนุญาต โดยสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และสัญญาจ้าง	สอบทานความมีอยู่จริงของขั้นตอนการปฏิบัติงานการจัดระดับชั้นความลับของข้อมูล การทำป้ายแสดงระดับชั้นความลับ และการจัดการสารสนเทศในนโยบาย

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.18.1.4	**ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล**	
	เพื่อให้มั่นใจว่า มีการปกป้องข้อมูลที่สามารถระบุตัวบุคคลเป็นไปตามที่กำหนดในกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง	สอบทานกฎหมาย ระเบียบ และข้อบังคับด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศขององค์กรว่ามีการกำหนดให้ปฏิบัติตามกฎหมายที่เกี่ยวกับการปกป้องข้อมูลส่วนบุคคลเช่น ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2533 เป็นต้น
A.18.1.5	**ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล**	
	เพื่อให้มั่นใจว่า มาตรการเข้ารหัสข้อมูลต้องมีการใช้ให้สอดคล้องกับข้อตกลง กฎหมาย และระเบียบทั้งหมดที่เกี่ยวข้อง	สอบทานมาตรการการเข้ารหัสข้อมูลว่าเป็นไปตาม พรบ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540 และ พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551
A.18.2	**การทบทวนความมั่งคงปลอดภัยสารสนเทศ**	
A.18.2.1	**การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ**	
	เพื่อให้มั่นใจว่า มีการทบทวนด้านความมั่นคงปลอดภัยสารสนเทศ สารสนเทศ โดยผู้ตรวจสอบภายใน	สอบทานหลักฐานการดำเนินการตรวจสอบภายในว่ามีการดำเนินการเป็นประจำตามระยะเวลาที่กำหนด และหลักฐานการตรวจสอบจากผู้ตรวจสอบภายนอกตามรอบระยะเวลาที่กำหนด (ถ้ามี)
A.18.2.2	**การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัยสารสนเทศ**	
	เพื่อให้มั่นใจว่า มีการทบทวนนโยบายความมั่นคงปลอดภัยให้สอดคล้องและเป็นไปตามมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้อง	สอบทานหลักฐานการทบทวนนโยบายความมั่นคงปลอดภัยว่ามีการทบทวนโดยการเปรียบเทียบกับมาตรฐาน ISO 27001 ฉบับปัจจุบัน

ข้อกำหนดที่	เรื่องที่ตรวจสอบ/ วัตถุประสงค์การตรวจสอบ	วิธีการตรวจสอบ
A.18.2.3	**การทบทวนการปฏิบัติตามข้อกำหนดทางด้านเทคนิค**	
	เพื่อให้มั่นใจว่า ระบบได้รับการทบทวนการปฏิบัติตามข้อกำหนดด้านเทคนิคให้สอดคล้องกับนโยบายความมั่นคงปลอดภัย	สอบทานหลักฐานการตรวจสอบช่องโหว่ในระบบที่สำคัญ และหลักฐานการตรวจประสิทธิภาพตัวควบคุมการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต/รายงานการทดสอบการบุกรุกและการประเมินความเสี่ยงระบบงานที่สำคัญ

4.3 การประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

4.3.1 แบบสอบถามเพื่อประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ ประกอบด้วย 2 ส่วน ได้แก่ ส่วนที่ 1 การประเมินความพึงพอใจด้านรูปแบบและเนื้อหา และส่วนที่ 2 การประเมินความพึงพอใจด้านการนำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศไปประยุกต์ในการใช้งาน

4.3.2 ผลการประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศจากกลุ่มตัวอย่างผู้ตรวจสอบภายใน การทางพิเศษแห่งประเทศไทย มีรายละเอียดดังตารางที่ 4.2

ตารางที่ 4.2 ผลการประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

รายการประเมินความพึงพอใจแนวทางการตรวจสอบ	ค่าเฉลี่ย ($\bar{X}$)	ค่าเบี่ยงเบนมาตรฐาน (S.D.)	การแปลผล
รูปแบบและเนื้อหา			
ครอบคลุมตามมาตรฐาน ISO 27001	4.20	0.57	มาก
มีความเหมาะสมกับองค์กร	4.10	0.52	มาก
มีความชัดเจน เข้าใจง่าย	4.40	0.79	มาก
การประยุกต์ใช้งาน			
สามารถประยุกต์ใช้ปฏิบัติงานตรวจสอบจริงได้	4.10	0.74	มาก
สามารถประยุกต์ใช้สอบทานงาน และควบคุมงานตรวจสอบจริงได้	4.30	0.48	มาก
ความพึงพอใจโดยรวม	**4.22**	**0.33**	**มาก**

จากตารางที่ 4.2 ผลการวิเคราะห์ความพึงพอใจของกลุ่มตัวอย่างผู้ตรวจสอบภายในการทางพิเศษแห่งประเทศไทยต่อแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ สรุปผลความพึงพอใจแต่ละส่วน และสรุปผลความพึงพอใจโดยรวม ดังนี้

ส่วนที่ 1 ความพึงพอใจด้านรูปแบบและเนื้อหาแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศอยู่ในระดับมาก โดยรูปแบบและเนื้อหามีความชัดเจน เข้าใจง่าย มีค่าเฉลี่ยสูงสุดเท่ากับ 4.40 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.79 ลำดับต่อมาคือ รูปแบบและเนื้อหาครอบคลุมตามมาตรฐาน ISO 27001 มีค่าเฉลี่ยเท่ากับ 4.20 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.57 และลำดับสุดท้ายรูปแบบและเนื้อหามีความเหมาะสมกับองค์กร มีค่าเฉลี่ยเท่ากับ 4.10 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.52

ส่วนที่ 2 ความพึงพอใจด้านการประยุกต์ใช้งานแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศอยู่ในระดับมาก โดยแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศสามารถประยุกต์ใช้สอบทานงานและควบคุมงานตรวจสอบจริงได้ มีค่าเฉลี่ยสูงสุดเท่ากับ 4.30 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.48 และแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศสามารถสามารถประยุกต์ใช้ปฏิบัติงานตรวจสอบจริงได้ มีค่าเฉลี่ยเท่ากับ 4.10 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.74

สรุปผลการความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศโดยรวมทั้งด้านรูปแบบ เนื้อหา และด้านการนำไปประยุกต์ใช้งานอยู่ในระดับมาก โดยมีค่าเฉลี่ยเท่ากับ 4.22 และค่าส่วนเบี่ยงเบนมาตรฐาน เท่ากับ 0.33

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การวิจัยเรื่องการจัดทำแนวทางการตรวจสอบภายในตามมาตรฐาน ISO 27001 : 2013 กรณีศึกษาการทางพิเศษแห่งประเทศไทย มีจุดมุ่งหมายเพื่อศึกษามาตรฐาน ISO 27001 : 2013 ที่เป็นมาตรฐานการบริหารจัดการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศระดับสากล และนำผลการศึกษามาจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศที่สอดคล้องกับมาตรฐาน ISO 27001 : 2013 เพื่อนำไปใช้ในการปฏิบัติงานตรวจสอบภายใน การทางพิเศษแห่งประเทศไทย ซึ่งเป็นองค์กรที่มีการใช้งานเทคโนโลยีสารสนเทศในการดำเนินงานและให้บริการผู้ใช้บริการทางพิเศษจำนวนมาก ขั้นตอนการดำเนินการวิจัยมีดังนี้ (1) ศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง และศึกษารายละเอียดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยและมาตรการควบคุมตามมาตรฐาน ISO 27001 : 2013 (2) จัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศให้ครอบคลุมตามข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยและมาตรการควบคุมตามมาตรฐานISO 27001 : 2013 และสอดคล้องกับการดำเนินงานของการทางพิเศษแห่งประเทศไทยโดยแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศประกอบด้วยเรื่องที่ตรวจสอบ วัตถุประสงค์การตรวจสอบ และวิธีการตรวจสอบ จำนวน 14 หัวข้อใหญ่ 114 ข้อย่อย (3) สร้างแบบสอบถามเพื่อประเมินความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศและนำไปเก็บข้อมูลจากกลุ่มตัวอย่างผู้ตรวจสอบภายใน การทางพิเศษแห่งประเทศไทย จำนวน 10 คน จากทั้งหมดจำนวน 24 คน และวิเคราะห์ข้อมูลด้วยค่าทางสถิติ ซึ่งผลความพึงพอใจในแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศในภาพรวมทั้งด้านรูปแบบและเนื้อหา และด้านการประยุกต์ใช้งานแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศมีค่าเฉลี่ยเท่ากับ 4.22 และค่าส่วนเบี่ยงเบนมาตรฐาน เท่ากับ 0.33 แปลผลความพึงพอใจในแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศอยู่ในระดับมาก

5.2 อภิปรายผล

จากผลการศึกษามาตรฐาน ISO 27001 เพื่อจัดทำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ สำหรับผู้ตรวจสอบภายใน การทางพิเศษแห่งประเทศไทย พบว่า ความพึงพอใจในแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศของผู้ตรวจสอบภายในภาพรวมอยู่ในระดับมาก โดยผู้ตรวจสอบภายใน เห็นว่า แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศที่มีกรอบการดำเนินงานตามมาตรฐาน ISO 27001 : 2013 สามารถนำมาใช้เป็นเครื่องมือ

ในการปฏิบัติงาน การสอบทานงาน และการควบคุมงานตรวจสอบได้ เนื่องจากแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศที่จัดทำมีเนื้อหา รูปแบบที่ชัดเจน เข้าใจง่าย ครอบคลุมตามมาตรฐาน ISO 27001 : 2013 และสอดคล้องกับการปฏิบัติงานตรวจสอบของการทางพิเศษแห่งประเทศไทย ซึ่งการที่หน่วยตรวจสอบภายในดำเนินงานตรวจสอบระบบเทคโนโลยีสารสนเทศ โดยใช้แนวทางการตรวจสอบอ้างอิงตามมาตรฐาน ISO 27001 : 2013 ทำให้ผู้ตรวจสอบภายในที่มีแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศที่เป็นมาตรฐานสากลและเหมาะสมกับองค์กร รวมทั้ง ทำให้ผู้บริหารมั่นใจยิ่งขึ้นได้ว่าการดำเนินงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศขององค์กรมีการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศตามมาตรฐานสากล

5.3 ข้อเสนอแนะ

5.1 นำระบบสารสนเทศมาช่วยในการจัดทำแนวทางการตรวจสอบ เพื่อให้ผู้ใช้งานสามารถจัดทำแนวทางการตรวจสอบ บันทึกผลการตรวจสอบ รวมทั้งสามารถจัดรายงานผลการตรวจสอบในระบบสารสนเทศ

5.2 ศึกษามาตรฐานด้านอื่น ๆ เพิ่มเติม เช่น มาตรฐาน COBIT ที่มีแนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีที่ดี หรือมาตรฐาน ITIL (IT Infrastructure Library) ซึ่งเป็นแนวทางปฏิบัติที่ดีด้านการบริหารจัดการด้าน IT Service เป็นต้น เพื่อเพิ่มพูนความรู้ของผู้ตรวจสอบเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศ และนำมาประยุกต์รวมกับแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

บรรณานุกรม

Ahmed Riad. (2015). **ISO/IEC 27001 : 2013.** 22/11/2017, website: https://www.linkedin.com/pulse/newest-integrated-model-isoiec-270012013-iso-223012012-

Best, John W. (1977). **Research in Education.** 3rd ed. Englewood Cliffs, NJ: Prentice-Hall.

Pavol Sojčí. (2012). **Tools for information security management.** website: http://is.muni.cz/th/359439/fi_b/Sojcik_-Tools_for_information_security_management.pdf-->Sojcik_-_Tools_for_information _security_management

JOŽE ŠREKL and ANDREJKA PODBREGAR. (2014). **ENHANCING SAFETY INFORMATION SYSTEMS WITH THE USE ISO/IEC 27000.** doi: 10.7562/SE2014.4.01.03

Sarah Vonnegut. (2016). **Confidentiality Integrity Availability.** 22/11/2017, website: https://www.checkmarx.com/2016/06/24/20160624the-importance-of-database- security-and-integrity

กลุ่มตรวจสอบภายในระดับกระทรวง กระทรวงศึกษาธิการ. (2558). **คู่มือการจัดทำแนวทางการตรวจสอบและกระดาษทำการ.** สืบค้นเมื่อ 23 พฤศจิกายน 2560, จากเว็บไซต์: http://audit.kpru.ac.th/images/pdf-manual/Guidelines-and-working-papers.pdf

ซีเรีย. (2558). Audit Program. สืบค้นเมื่อ 23 พฤศจิกายน 2560, จากเว็บไซต์: https://myseria.com/2014/09/จ-/ความรู้ทั่วไปเกี่ยวกับ-a/#more-12

ณัทรัฏฐ์ มณีรัสยากร. (2559). **การพัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001 ขององค์กรกรณีศึกษา บจก. เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น.** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

ธิดา ลิ่มทองวิรัตน์. (2553). **การประเมินประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO 27001 : กรณีศึกษาบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน).** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยหอการค้าไทย.

น้ำหนึ่ง กล้าหาญ. (2555). **โปรแกรมประยุกต์สำหรับการประเมินความมั่นคงปลอดภัยสารสนเทศในองค์กรปกครองส่วนท้องถิ่นในจังหวัดสุพรรณบุรี.** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม.

บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด. (2560). **ความรู้เนื้อหาของผู้ตรวจสอบภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001 : 2013. การทางพิเศษแห่งประเทศไทย.**

ภาพร ภิยโยดิลกชัย. (2553). **การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT.** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร บัณฑิตวิทยาลัยมหาวิทยาลัยธุรกิจบัณฑิตย์

ภูมิพัฒน์ สุขศรีใส. (2559). **ระบบบริหารความปลอดภัยของข้อมูล.** สืบค้นเมื่อ 22 พฤศจิกายน 2560, จากเว็บไซต์: http://tiwphumipat.blogspot.com/2016/07/5-iso-270001-iso-27001-270012005.html

มนสิชา ทองประศาสน์. (2558). **การพัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001 ขององค์กรกรณีศึกษา บจก. เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น.** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน. (2549). **คู่มือการปฏิบัติงานตรวจสอบภายใน 2549.** สืบค้นเมื่อ 23 พฤศจิกายน 2560, จากเว็บไซต์: http://www.au.nkp2.go.th/images/manual.pdf

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. (2560). **ความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 : 2013.** สืบค้นเมื่อ 22 พฤศจิกายน 2560, จากเว็บไซต์: https://www.nstdaacademy.com/webnsa/index.php/advancedtraining/practitioner/iso2017-1

อภินัทธ์ แช่มลำเจียก. (2557). **การสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศภายใต้มาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา บริษัท เวิลธ์ แมเนจเม้นท์ ซิสเท็ม จำกัด.** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาความมั่นคงทางระบบสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

อรนุช คงศรี. (2558). **ความมั่นคงปลอดภัยของสารสนเทศ.** สืบค้นเมื่อ 22 พฤศจิกายน 2560, จากเว็บไซต์: http://jjsao.blogspot.com/2015/05/blog-post.html

อุทัยวรรณ จรุงวิภู และคณะ. (2558). **การใช้เทคโนโลยีสารสนเทศทางการบัญชีและการสอบบัญชี.** (พิมพ์ครั้งที่ 2). กรุงเทพมหานคร: มหาวิทยาลัยสุโขทัยธรรมาธิราช.

อุษณา ภัทรมนตรี. (2547). **การตรวจสอบและควบคุมด้านคอมพิวเตอร์**. กรุงเทพมหานคร: เทกซ์ แอนด์เจอร์นัล พับลิเคชั่น.

ภาคผนวก

ภาคผนวก ก
แบบตอบรับการเป็นผู้เชี่ยวชาญ เพื่อตรวจสอบเครื่องมือที่ใช้ในการวิจัย

SPU
SRIPATUM UNIVERSITY

แบบตอบรับการเป็นผู้เชี่ยวชาญ เพื่อตรวจสอบเครื่องมือที่ใช้ในการวิจัย

ชื่อ (ยศ/นาย/นาง/นางสาว).....สมมารถ....พุ่มตาลพงษ์.....
ตำแหน่ง.....หัวหน้าแผนกตรวจสอบภายใน..... หน่วยงาน.....การทางพิเศษแห่งประเทศไทย.....
เบอร์โทรศัพท์.....025589800 ต่อ 2923..... e-mail.....Sommart_pum@exat.co.th.....

☑ มีความยินดีเป็นผู้เชี่ยวชาญ เพื่อตรวจสอบเครื่องมือที่ใช้ในการวิจัย
☐ ไม่สามารถเป็นผู้เชี่ยวชาญ เพื่อตรวจสอบเครื่องมือที่ใช้ในการวิจัย

ให้กับ (ยศ/นาย/นาง/นางสาว).....ภัทราพร.....โชติมหา.....
นักศึกษาระดับปริญญา.....โท..... แผน.....ข..สารนิพนธ์..... หลักสูตร.....ปริญญาโท..ภาคเสาร์-อาทิตย์.....
รหัสประจำตัว.....60501842..... สาขาวิชา.....เทคโนโลยีสารสนเทศ..... คณะ.....เทคโนโลยีสารสนเทศ.....

ลงชื่อ.....สมมารถ พุ่มตาลพงษ์.....
(นางสมมารถ พุ่มตาลพงษ์)
.....9...../....กรกฎาคม..../...2561.....

ภาคผนวก ข
แบบสอบถามการวิจัย เรื่อง การประเมินความพึงพอใจ แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

แบบสอบถามการวิจัย
เรื่อง การประเมินผลความพึงพอใจแนวทางการตรวจสอบ ระบบเทคโนโลยีสารสนเทศ

<u>คำชี้แจง</u>

แบบสอบถามชุดนี้ มีวัตถุประสงค์เพื่อประเมินระดับความพร้อมพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศจากผู้ตรวจสอบภายใน การทางพิเศษแห่งประเทศไทย ดังนั้นผู้วิจัยจึงขอความอนุเคราะห์ท่านได้โปรดพิจารณาตอบแบบสอบถามความพึงพอใจแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศแต่ละหัวข้อ เพื่อนำผลความพึงพอใจดังกล่าวมาแสดงผลการศึกษาและวิจัยเรื่อง การจัดทำแนวทางการตรวจสอบภายในตามมาตรฐาน ISO 21001 : 2013 เพื่อให้ทราบถึงความเหมาะสม ความสอดคล้องของแนวทางการตรวจสอบภายในที่จัดทำขึ้นตามแนวทางของมาตรฐาน ISO 27001 : 2013

<u>แบบสอบถามแบ่งออกเป็น 2 ส่วน คือ</u>

ส่วนที่ 1 เป็นแบบสอบถามหัวข้อการประเมินความพึงพอใจด้านรูปแบบและเนื้อหาของแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 2 เป็นแบบสอบถามหัวข้อด้านการนำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศไปประยุกต์ในการใช้งาน

<u>ความหมายของระดับค่าคะแนน</u>

การแปลค่าความหมาย แบ่งเป็น 5 ระดับ ดังต่อไปนี้

5	หมายถึง	มีความพึงพอใจมากที่สุด
4	หมายถึง	มีความพึงพอใจมาก
3	หมายถึง	มีความพึงพอใจปานกลาง
2	หมายถึง	มีความพึงพอใจน้อย
1	หมายถึง	มีความพึงพอใจน้อยที่สุด

ผู้วิจัยขอขอบพระคุณเป็นอย่างสูงในความร่วมมือด้วยดีของท่านมา ณ โอกาสนี้

โปรดทำเครื่องหมาย ✓ ในช่องที่ตรงกับระดับความพึงพอใจของท่านมากที่สุด

รายการประเมินความพึงพอใจแนวทางการตรวจสอบ	ระดับความพึงพอใจ					ข้อเสนอแนะ
	5	4	3	2	1	
ส่วนที่ 1 ด้านรูปแบบและเนื้อหา						
1.1 ครอบคลุมตามมาตรฐาน ISO 27001						
1.2 มีความเหมาะสมกับองค์กร						
1.3 มีความชัดเจน เข้าใจง่าย						
ส่วนที่ 2 ด้านประยุกต์การใช้งาน						
2.1 สามารถประยุกต์ใช้ปฏิบัติงานตรวจสอบจริงได้						
2.2 สามารถประยุกต์ใช้สอบทานงานและควบคุมงานตรวจสอบจริงได้						

ขอขอบพระคุณทุกท่านที่ให้ความอนุเคราะห์ในการตอบแบบสอบถามฉบับนี้อย่างครบถ้วน

ภาคผนวก ค

ใบตอบรับและเกียรติบัตรการนำเสนอผลงานการประชุมวิชาการ

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
SRIPATUM UNIVERSITY CHONBURI CAMPUS

ที่ มศป.ชบ 0522 / ว 1039

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
79 ถนนบางนา-ตราด ตำบลคลองตำหรุ
อำเภอเมือง จังหวัดชลบุรี 20000

30 เมษายน 2561

เรื่อง ตอบรับการนำเสนอผลงานทางวิชาการ

เรียน นางสาวภัทราพร โชติมหา

ตามที่ท่านส่งผลงานทางวิชาการเพื่อนำเสนอในการประชุมวิชาการระดับชาติ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี ประจำปี 2561 เรื่อง ผลงานวิจัยและนวัตกรรมเพื่อส่งเสริมความก้าวหน้าอุตสาหกรรม 4.0 กำหนดจัดขึ้นในวันพฤหัสบดีที่ 12 กรกฎาคม 2561 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี ความละเอียดทราบแล้วนั้น

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี จึงขอแจ้งให้ท่านทราบว่า ผลงานทางวิชาการของท่านผ่านการประเมินจากผู้ทรงคุณวุฒิและให้นำเสนอในการประชุมดังกล่าว วันพฤหัสบดีที่ 12 กรกฎาคม 2561 ขอให้ท่านตรวจสอบตารางวัน เวลา และสถานที่ การนำเสนอได้ที่ http://www.east.spu.ac.th/spuccon2018/ ตั้งแต่วันพุธที่ 2 พฤษภาคม 2561 เป็นต้นไป

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

กาญจนา มณีแสง

(รองศาสตราจารย์กาญจนา มณีแสง)
รองอธิการบดีฝ่ายวิจัยและแผน ปฏิบัติหน้าที่แทน
รองอธิการบดี วิทยาเขตชลบุรี

สำนักวิจัยและพัฒนานวัตกรรม
โทรศัพท์ 0-3814-6123 ต่อ 2506, 2507
โทรสาร 0-3814-6011 (ปิดทำการวันศุกร์-เสาร์)
e-mail : research@east.spu.ac.th

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

ขอมอบเกียรติบัตรนี้ไว้เพื่อแสดงว่า

ภัทราพร โชติมหา

ได้นำเสนอผลงานวิชาการภาคบรรยาย

เรื่อง การจัดทำแนวทางการตรวจสอบภายในตามมาตรฐาน ISO 27001: 2013

กรณีศึกษาการทางพิเศษแห่งประเทศไทย

ในการประชุมวิชาการระดับชาติและนานาชาติ ประจำปี 2561 (2018 SPUC National and International Conference)

เรื่อง ผลงานวิจัยและนวัตกรรมเพื่อส่งเสริมความก้าวหน้าอุตสาหกรรม 4.0

(Research and Innovation for Fostering Industries 4.0 Progressive)

วันพฤหัสบดีที่ 12 กรกฎาคม 2561

ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

(ดร.บุษบา ชัยจินดา)

รองอธิการบดี วิทยาเขตชลบุรี

ภาคผนวก ง

ผลการตรวจสอบการลอกเลียนวรรณกรรมทางวิชาการโดยอักขราวิสุทธิ์

Plagiarism Checking Report

Created on Aug 12, 2018 at 21:39 PM

Submission information

ID	SUBMISSION DATE	SUBMITTED BY	ORGANIZATION	FILENAME	STATUS	SIMILARITY INDEX
935527	Aug 12, 2018 at 21:39 PM	patraporn_cho@spulive.net	มหาวิทยาลัยศรีปทุม	บทที่ 1 ISO.docx	Completed	0.00 %

Match Overview

NO.	TITLE	AUTHOR(S)	SOURCE	SIMILARITY INDEX
No data available in table				

Plagiarism Checking Report

Created on Aug 12, 2018 at 21:46 PM

Submission Information

ID	SUBMISSION DATE	SUBMITTED BY	ORGANIZATION	FILENAME	STATUS	SIMILARITY INDEX
935531	Aug 12, 2018 at 21:46 PM	patraporn_cho@spulive.net	มหาวิทยาลัยศรีปทุม	บทที่ 2 ISO.docx	Completed	0.00 %

Match Overview

NO.	TITLE	AUTHOR(S)	SOURCE	SIMILARITY INDEX
No data available in table				

Plagiarism Checking Report

Created on Aug 12, 2018 at 21:48 PM

Submission Information

ID	SUBMISSION DATE	SUBMITTED BY	ORGANIZATION	FILENAME	STATUS	SIMILARITY INDEX
935533	Aug 12, 2018 at 21:48 PM	patraporn_cho@spulive.net	มหาวิทยาลัยศรีปทุม	บทที่ 3 ISO.docx	Completed	0.00 %

Match Overview

NO.	TITLE	AUTHOR(S)	SOURCE	SIMILARITY INDEX
No data available in table				

Plagiarism Checking Report

Created on Aug 12, 2018 at 21:49 PM

Submission Information

ID	SUBMISSION DATE	SUBMITTED BY	ORGANIZATION	FILENAME	STATUS	SIMILARITY INDEX
935535	Aug 12, 2018 at 21:49 PM	patraporn_cho@spulive.net	มหาวิทยาลัยศรีปทุม	บทที่ 4 ISO.docx	Completed	0.00 %

Match Overview

NO.	TITLE	AUTHOR(S)	SOURCE	SIMILARITY INDEX
No data available in table				

Plagiarism Checking Report

Created on Aug 12, 2018 at 21:51 PM

Submission Information

ID	SUBMISSION DATE	SUBMITTED BY	ORGANIZATION	FILENAME	STATUS	SIMILARITY INDEX
935536	Aug 12, 2018 at 21:51 PM	patraporn_cho@spulive.net	มหาวิทยาลัยศรีปทุม	บทที่ 5 ISO.docx	Completed	0.00 %

Match Overview

NO.	TITLE	AUTHOR(S)	SOURCE	SIMILARITY INDEX
No data available in table				

ประวัติผู้วิจัย

ชื่อ - สกุล	ภัทราพร โชติมหา
วัน เดือน ปีเกิด	13 มีนาคม 2527
สถานที่เกิด	จังหวัดกรุงเทพมหานคร
ประวัติการศึกษา	ปี พ.ศ. 2549
	ปริญญาตรี คณะบริหารธุรกิจ สาขาเทคโนโลยีสารสนเทศ
	มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกวิทยาเขตจักรพงษภูวนารถ
ประสบการณ์ทำงาน	ปี พ.ศ. 2550
	นักวิชาการคอมพิวเตอร์
	กรมอนามัย กระทรวงสาธารณาสุข
	ปี พ.ศ. 2551 – ปัจจุบัน
	พนักงานตรวจสอบภายใน
	การทางพิเศษแห่งประเทศไทย