ระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

นางสาววิไลวรรณ ทาน้อย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ.2560

Security Management System with ISO 27001
in Access Control to Information Systems
For Governor's Office, Office of the Permanent Secretary for Interior

Miss Wilaiwan Tanoi

A Thesis Submitted in Partial Fulfillment of the Requirements for

the Degree of Master of Science in Information and Communication Technology

School of Science and Technology

Sukhothai Thammathirat Open University

2017

หัวข้อวิทยานิพนธ์ ระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศสำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

ชื่อและนามสกุล นางสาววิไลวรรณ ทาน้อย

แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชา วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา 1. รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์

2. ผู้ช่วยศาสตราจารย์ (พิเศษ) ดร.สันติพัฒน์ อรุณธารี

วิทยานิพนธ์นี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 31 สิงหาคม 2561

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(อาจารย์ ดร.ดวงดาว วิชาดากุล)

..... กรรมการ

(รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ (พิเศษ) ดร.สันติพัฒน์ อรุณธารี)

..... ประธานกรรมการบัณฑิตศึกษา

(รองศาสตราจารย์ ดร.กฤษณา รุ่งโรจน์วณิชย์)

ชื่อวิทยานิพนธ์ ระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

ผู้วิจัย นางสาววิไลวรรณ ทาน้อย **รหัสนักศึกษา** 2549600340 **ปริญญา** วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร) **อาจารย์ที่ปรึกษา** (1) รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์ (2) ผู้ช่วยศาสตราจารย์ (พิเศษ) ดร.สันติพัฒน์ อรุณธารี **ปีการศึกษา** 2560

บทคัดย่อ

การพัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย มีวัตถุประสงค์เพื่อ 1) ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ตามมาตรฐาน ISO/IEC 27005 2) พัฒนากระบวนการบริหารจัดการความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC 27001 เพื่อควบคุมการเข้าถึง สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย 3) พัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

การดำเนินการวิจัย ได้แบ่งกระบวนการออกเป็น 1) ประเมินความเสี่ยง โดยอ้างอิงมาตรฐานสากล ISO/IEC 27005 2) ประเมินปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศตามมาตรฐาน ISO/IEC 27001 3) พัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

ผลการวิจัยพบว่า 1) หลังจากที่ทำการประเมินความเสี่ยงโดยระบบ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27005 พบว่าผลการประเมินอยู่ในระดับต่ำกว่าเกณฑ์ 2) จากการประเมินความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO 27001 ด้านการควบคุมการเข้าถึงระบบสารสนเทศ พบว่าผลการประเมินอยู่ที่ ร้อยละ 16 ซึ่งถือว่าอยู่ในเกณฑ์ที่ต่ำมาก 3) จากการพัฒนาระบบจัดการความมั่นคงปลอดภัยด้านตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย จะเห็นได้ว่าช่วยให้หน่วยงานมีแบบแผนในการดำเนินงานอย่างเป็นระบบ สามารถปฏิบัติตามนโยบายของรัฐบาลได้อย่างเป็นรูปธรรม และถือเป็นแนวทางปฏิบัติที่ดีในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ และหน่วยงานอื่นๆ สามารถนำกรอบวิธีปฏิบัตินี้ไปประยุกต์ใช้ได้

คำสำคัญ: การเข้าถึงสารสนเทศ ความมั่นคงปลอดภัยด้านสารสนเทศ เหตุการณ์ด้านความมั่นคงปลอดภัย สถานการณ์ด้านความมั่นคงปลอดภัย ระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001

Thesis title: Security Management System with ISO 27001 in Access Control to Information Systems For Governor's Office, Office of the Permanent Secretary for Interior

Researcher: Miss Wilaiwan Tanoi; **ID**: 2549600340; **Degree**: Master of Science in Information and Communication Technology**; Thesis advisors**: (1) Vipa Jaroenpuntaruk, Associate Professor; (2) Santipat Arunthari, Assistant Professor**; Academic year**: 2017

Abstract

The objectives of this study were 1) to assess information and communication technology risk of Provincial Governor's Office, Office of the Permanent Secretary for Interior according to ISO/ IEC 27005, 2) to develop the ISO / IEC 27001-based security management process to control the access to information system of Provincial Governor's Office, Office of the Permanent Secretary for Interior, and 3) to develop the ISO / IEC 27001-based in security management system to control the access to information system of Provincial Governor's Office, Office of the Permanent Secretary for Interior.

The research methodology was divided into the following steps: 1) risk assessment was conducted based on ISO / IEC 27005, 2) the problems of controlling the access to information system based on ISO / IEC 27001 were evaluated, and 3) the ISO 27001-based security management system was developed to control the access to information system of Provincial Governor's Office, Office of the Permanent Secretary for Interior.

The research results of this study indicated that 1) after assessing the risk by the system, controlling access to information system according to ISO/ IEC 27005 was lower than the set criteria, 2) in terms of assessing information security readiness according to ISO 27001, controlling access to information system was at very low with 16%, and 3) the development of the ISO / IEC 27001-based in security management system to control the access to information system of Provincial Governor's Office, Office of the Permanent Secretary for Interior could enable an organization to systematically formulate operational plan, to tangibly comply with government policies and leads to good practices in creating security for information technology systems. Besides, other agencies can practically apply this framework.

Keywords: Information access Information security Security incidents Security situations ISO 27001-based security management system

กิตติกรรมประกาศ

การจัดทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้เป็นอย่างดีด้วยความกรุณาจาก รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์ และ ผู้ช่วยศาสตราจารย์ (พิเศษ) ดร.สันติพัฒน์ อรุณธารี ที่ให้คำปรึกษา ชี้แนะ แนะนำแนวทางในการทำวิทยานิพนธ์ในครั้งนี้ พร้อมทั้งติดตามงานอย่างใกล้ชิด ส่งผลให้วิทยานิพนธ์ฉบับนี้เสร็จสมบูรณ์ด้วยดี ผู้วิจัยรู้สึกซาบซึ้งในความกรุณาของอาจารย์ทั้งสองท่านเป็นอย่างมาก

ขอขอบพระคุณ ดร.ดวงดาว วิชาดากุล ที่กรุณาได้เสียสละเวลา ให้คำแนะนำ และชี้แนะวิทยานิพนธ์ฉบับนี้ให้สมบูรณ์มากยิ่งขึ้น และขอขอบพระคุณหัวหน้าสำนักงานจังหวัดหนองคาย ผู้อำนวยการ ทุกกลุ่มงาน ตลอดจนข้าราชการ พนักงานราชการ และลูกจ้าง สำนักงานจังหวัดหนองคายทุกคน ที่ให้ความร่วมมือในการตอบแบบสอบถาม และสนับสนุนข้อมูลสำหรับการจัดทำวิทยานิพนธ์ฉบับนี้

สุดท้ายนี้ ขอขอบคุณ คณาจารย์ เจ้าหน้าที่ สาขาวิชา วิทยาศาสตร์และเทคโนโลยี แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยสุโขทัยธรรมาธิราช เพื่อนนักศึกษา ครอบครัว และผู้ที่มีส่วนเกี่ยวข้องทุกท่าน ที่ช่วยสนับสนุน และให้กำลังใจมาโดยตลอด

วิไลวรรณ ทาน้อย

สิงหาคม 2561

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1

บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

สืบเนื่องจากนโยบายของรัฐบาลที่มีความต้องการให้หน่วยงานของรัฐ ได้มีการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารมาช่วยในการปฏิบัติงานและบริหารงาน รวมทั้งการกระจายข้อมูลข่าวสารไปสู่ประชาชนเพื่อเพิ่มประสิทธิภาพการทำงานตามภารกิจ ให้เกิดการบูรณาการและเป็นเอกภาพในระบบข้อมูล ลดความซ้ำซ้อนในการปฏิบัติงาน เพื่อให้ประชาชนได้รับการบริการที่สะดวก รวดเร็ว มีความโปร่งใส ตรวจสอบได้อันจะนำมาสนับสนุนบรรยากาศที่เอื้อต่อการพัฒนาเศรษฐกิจโดยรวมของประเทศนั้น ปัจจุบันมีหลายหน่วยงานที่มีความพร้อมต่อการดำเนินการ จึงได้นำเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้ในการปฏิบัติงานและบริหารงานภายในหน่วยงานของตนเอง และเนื่องด้วยแต่ละหน่วยงานมีความแตกต่างด้านสภาพแวดล้อมและพื้นที่ที่แตกต่างกันไป และบุคลากรในบางหน่วยงานยังขาดความรู้ความเข้าใจในด้านเทคโนโลยีสารสนเทศ อันเป็นผลให้การพัฒนาเทคโนโลยีสารสนเทศเป็นไปอย่างไร้ทิศทาง ขาดกลยุทธ์ แนวทาง และเป้าหมายที่ชัดเจน ขาดความตระหนักในเรื่องการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร ส่งผลให้ปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศมีความรุนแรงเพิ่มขึ้น ทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์การ ภาครัฐ และภาคเอกชนที่มีการดำเนินงาน ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่น ๆ โดยการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย จึงเห็นความสำคัญโดยนำกฎหมายข้อบังคับต่างๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำ เพื่อช่วยให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ จึงได้กำหนดแนวนโยบายและแนวปฏิบัติในการรักษา

ความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ โดยได้ตราพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ขึ้น

ในการนี้ สำนักงานปลัดกระทรวงมหาดไทยก็ได้กำหนดนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย แต่ครอบคลุมเฉพาะศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นหน่วยงานที่อยู่ในส่วนกลาง ไม่ครอบคลุมถึงสำนักงานจังหวัด ซึ่งเป็นหน่วยงานส่วนภูมิภาคที่สังกัดสำนักงานปลัดกระทรวงมหาดไทยเช่นกัน

ดังนั้น เพื่อให้สอดคล้องกับนโยบายของสำนักงานปลัดกระทรวงมหาดไทย และนโยบายของภาครัฐในระดับประเทศ ผู้วิจัยจึงเกิดแนวคิดในการพัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย เพื่อเป็นเครื่องมือหนึ่งที่จะช่วยในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ให้เป็นไปตามมาตรฐานขั้นต่ำที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553 ประกาศ ณ วันที่ 31 พฤษภาคม พ.ศ.2553 ภายใต้แนวทางที่เป็นมาตรฐานขั้นต่ำตามที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด ซึ่งเพียงพอต่อการดำเนินงาน และไม่สร้างภาระให้หน่วยงานมากเกินความจำเป็น โดยการดำเนินงานดังกล่าว จะเป็นมาตรการหนึ่งที่ช่วยยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงานของรัฐ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงการดำเนินงานตามกรอบมาตรฐานสากล ISO/IEC 27001

2. วัตถุประสงค์การวิจัย

การวิจัยนี้มีวัตถุประสงค์เพื่อ

2.1 ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ตามมาตรฐาน ISO/IEC 27005

2.2 พัฒนากระบวนการบริหารจัดการความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC 27001 เพื่อควบคุมการเข้าถึง สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

2.3 พัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

3. กรอบแนวคิดการวิจัย

3.1 กำหนดและจัดประเภทของสินทรัพย์ที่จะต้องมีการประเมินความเสี่ยง

3.2 ระบุปัจจัยที่เกี่ยวข้องกับความเสี่ยงของสินทรัพย์ เช่น ภัยคุกคาม (Threat) และจุดอ่อน (Vulnerability) ของสินทรัพย์

3.3 ประเมินค่าที่เกี่ยวข้องกับความเสี่ยง เช่น ผลกระทบ (Impact) และความเป็นไปได้ (Probability) อย่างถูกต้อง

3.4 พัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

4. ขอบเขตของการวิจัย

การวิจัยดำเนินการตามลำดับดังต่อไปนี้

4.1 ประเมินความเสี่ยง (Risk Assessment Methodology) โดยอ้างอิงมาตรฐานสากล ISO/IEC 27005 ดังนี้

4.1.1 จัดทำทะเบียนสินทรัพย์และกำหนดค่าของสินทรัพย์ (Asset Identification and Valuation) ที่จะต้องมีการประเมินความเสี่ยง โดยประเภทของสินทรัพย์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ควรจะได้รับการประเมินความเสี่ยงและควบคุมดูแล ซึ่งมีองค์ประกอบหลัก ดังนี้

1. สินทรัพย์หลัก (Primary Assets) เป็นสินทรัพย์ที่มีความสำคัญกับหน่วยงาน ซึ่งแบ่งออกเป็น 2 ประเภท ได้แก่

1.1 กระบวนการทางธุรกิจ (Business Processes) หรือกระบวนการทำงาน หรือกิจกรรมที่มีความสำคัญกับ หน่วยงาน ซึ่งได้แก่

1.1.1 กระบวนการที่หากเกิดความเสียหาย (Loss) หรือ มีการเสื่อมสภาพ (Degradation) จะส่งผลให้ หน่วยงาน ไม่สามารถปฏิบัติหน้าที่ได้

1.1.2 กระบวนการที่เป็นความลับ (Secret) หรือกระบวนการที่ใช้เทคโนโลยีซึ่งเป็นกรรมสิทธิ์ (Propriety Technology) ของหน่วยงาน

1.1.3 กระบวนการที่หากถูกเปลี่ยนแปลงหรือแก้ไข (Modified) จะส่งผลให้ หน่วยงาน ไม่สามารถปฏิบัติภารกิจให้บรรลุเป้าหมายตามที่ได้กำหนดไว้

1.1.4 กระบวนการที่จะต้องปฏิบัติตามให้สอดคล้องกับสัญญา ระเบียบข้อบังคับ หรือกฎหมายที่เกี่ยวข้อง (Contractual, Legal, or Regulatory Requirements)

1.2 ข้อมูล (Information) ของหน่วยงาน ที่เก็บอยู่ในระบบสารสนเทศ และจำเป็นต้องได้รับการปกป้องและธำรงไว้ซึ่งความมั่นคงปลอดภัยซึ่งประกอบไปด้วย ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพความพร้อมใช้งาน (Availability) ซึ่งประกอบด้วยข้อมูลดังต่อไปนี้

1.2.1 ข้อมูลสำคัญ ที่จำเป็นต่อการปฏิบัติหน้าที่และภารกิจเพื่อให้บรรลุเป้าหมายของหน่วยงาน

1.2.2 ข้อมูลส่วนบุคคล ที่จะต้องได้รับการปกป้องและดูแลตามกฎหมาย

1.2.3 ข้อมูลทางกลยุทธ์ ที่จำเป็นสำหรับการทำงานเพื่อให้บรรลุวัตถุประสงค์ตามแผนกลยุทธ์ที่ได้กำหนดไว้

1.2.4 ข้อมูลมูลค่าสูง ที่มีการใช้เวลา และ/หรือ งบประมาณจำนวนมากในการรวบรวมจัดเก็บประมวลผล และการขนส่งข้อมูล

2. สินทรัพย์ประกอบ (Supporting Assets) คือสินทรัพย์ที่เกี่ยวข้องกับสินทรัพย์หลัก และอยู่ในขอบเขตของการประเมินความเสี่ยง ซึ่งสามารถแบ่งเป็นประเภทต่าง ๆ ได้แก่

2.1 ซอฟต์แวร์ (Software) ที่เกี่ยวข้องกับระบบสารสนเทศ ได้แก่ ระบบปฏิบัติการ (Operation System) โปรแกรมประยุกต์ (Application) โปรแกรมบริหารจัดการฐานข้อมูล (Database Management Software) และซอฟต์แวร์อื่น ๆ

2.2 ฮาร์ดแวร์ (Hardware) และอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศและการสื่อสาร ได้แก่ เครื่องบริการ (Server) คอมพิวเตอร์ส่วนบุคคล (Personal computer) อุปกรณ์สำรองข้อมูล (Media Storage) อุปกรณ์สำรองไฟฟ้า (UPS) ตัวเชื่อมต่อ (Connector) เครื่องพิมพ์ (Printer) รวมถึงอุปกรณ์ เครื่องมือ เครือข่ายโทรศัพท์สาธารณะ (Public Switching Telephone Network: PSTN) เครือข่ายคอมพิวเตอร์ (LAN) เครือข่ายไร้สาย (Wireless network) อุปกรณ์จัดเส้นทางแบบ (Router) ฮับ (Hub) สวิตซ์ (Switch) และสิ่งอำนวยความสะดวกอื่น ๆ

4.1.2 กำหนดภัยคุกคามต่อสินทรัพย์ (Threat Identification)

1. จัดทำรายงานภัยคุกคาม (Threat List)

2. ประเมินความเสียหายจากภัยคุกคามแต่ละรายการในทุกมิติของความมั่นคงปลอดภัยสารสนเทศ

4.1.3 กำหนดจุดอ่อนของสินทรัพย์ (Vulnerability Identification)

1. พิจารณารายการจุดอ่อนซึ่งเอื้อให้เกิดภัยคุกคามแต่ละรายการที่สร้างความเสียหายให้กับสินทรัพย์

4.1.4 วิเคราะห์มาตรการป้องกันที่มีอยู่ (Existing Control Analysis)

1. พิจารณามาตรการป้องกันที่มีอยู่ในปัจจุบัน

4.1.5 การประเมินระดับความเป็นไปได้ (Likelihood Determination)

1. ประเมินระดับความเป็นไปได้ (Likelihood) โดยประเมินต่อความเป็นไปได้ที่ภัยคุกคามอาจกระทำความเสียหายต่อสินทรัพย์

2. แนวโน้มการเกิดขึ้นของภัยคุกคาม

4.1.6 ประเมินผลกระทบและความเสียหาย (Impact Analysis)

1. ประเมินผลกระทบ (Impact) ซึ่งเกิดจากภัยคุกคามลงในรายการการประเมินความเสี่ยงสินทรัพย์ (Risk Assessment Report)

4.1.7 ประเมินระดับความเสี่ยง

1. ประเมินค่าระดับความเสี่ยงจากผลกระทบ (Impact) และ ความเป็นไปได้ (Likelihood)

4.2 ประเมินปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

4.3 พัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

5. นิยามศัพท์เฉพาะ

5.1 ผู้ใช้งาน หมายถึง ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

5.2 สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

5.3 สินทรัพย์ (Asset) หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

5.4 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

5.5 ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (Reliability)

5.6 เหตุการณ์ หรือ สถานการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

5.7 ภัยคุกคาม (Threat) หมายถึง ภาวะที่อาจเกิดต่อสินทรัพย์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล ไม่ว่าจะเป็นด้านความลับของข้อมูล (Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) หรือความพร้อมให้ใช้งานของข้อมูล (Availability) หรือเรียกโดยรวมว่าผลกระทบต่อ CIA

5.8 ค่าของสินทรัพย์ (CIA Value) หมายถึง ระดับความเสียหายเมื่อสินทรัพย์ได้รับผลกระทบด้าน CIA

5.8.1 C คือ Confidentiality การรักษาความลับของข้อมูล หมายถึง การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึงใช้หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

5.8.2 I คือ Integrity การรักษาความถูกต้องสมบูรณ์ครบถ้วนของข้อมูล หมายถึง การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ถูกต้องขณะที่มีการใช้งานประมวลผล โอนหรือเก็บรักษาเพื่อมิให้มีการเปลี่ยนแปลงแก้ไขทำให้สูญหายทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

5.8.3 A คือ Availability การรักษาความพร้อมให้ใช้งานของข้อมูล หมายถึง การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงานเข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

5.9 จุดอ่อน (Vulnerability) หมายถึง จุดต่าง ๆ ที่อาจอำนวยให้ภัยคุกคามสามารถเข้ากระทำความเสียหายต่อสินทรัพย์ได้ เช่น การไม่ได้ติดตั้งโปรแกรม Anti-virus บนเครื่องบริการ

5.10 ความเสี่ยง หมายถึง ความเป็นไปได้ (Probability) ที่ภัยคุกคาม (Threat) จะอาศัยจุดอ่อน (Vulnerability) เข้ากระทำความเสียหายและก่อให้เกิดผลกระทบ (Impact) ต่อสินทรัพย์

5.11 เครื่องมือควบคุม (Control) หมายถึง เครื่องมือหรือมาตรการต่าง ๆ ที่ถูกใช้เพื่อป้องกัน และ/หรือ ลดความเสี่ยงต่อสินทรัพย์

6. ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับจากการศึกษามีดังต่อไปนี้

6.1 ทราบถึงวิธีการตรวจประเมินความเสี่ยงและความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร ตามมาตรฐาน ISO/IEC 27005 ของ สำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ซึ่งใช้เป็นแนวทางปฏิบัติได้อย่างชัดเจนและเป็นรูปธรรม

6.2 สำนักงานจังหวัดมีเครื่องมือเพื่อช่วยประเมินความพร้อมของหน่วยงานด้านเทคโนโลยีสารสนเทศตามมาตรฐาน ISO 27001 ซึ่งเป็นมาตรฐานสากล

6.3 เป็นต้นแบบให้กับส่วนราชการอื่น ๆ

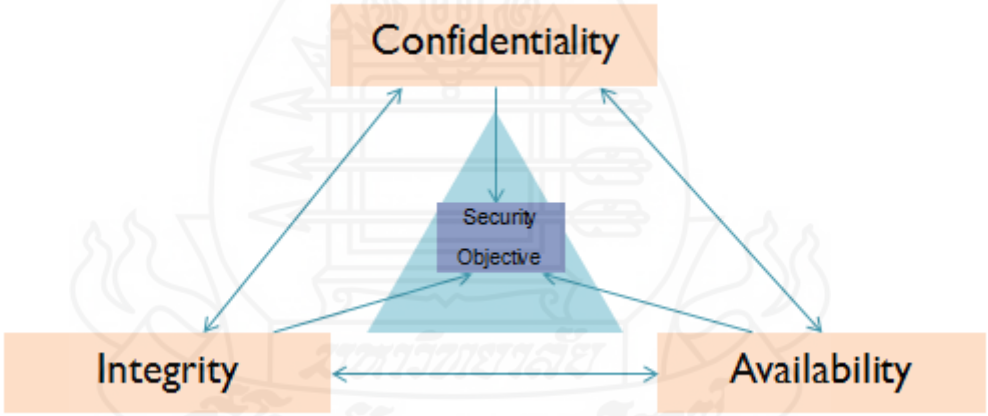
บทที่ 2

วรรณกรรมที่เกี่ยวข้อง

1. ทฤษฎีและแนวความคิด

1.1 ความมั่นคงปลอดภัยของสารสนเทศ (Information Security)

ความมั่นคงปลอดภัยของสารสนเทศนั้นมีองค์ประกอบด้วยกัน 3 ประการ คือ ความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ในการนี้ ทรัพย์สิน(Asset) ที่มีความมั่นคงปลอดภัยนั้นต้องประกอบด้วยองค์ประกอบทั้งสามอย่างครบถ้วน ไม่ว่าทรัพย์สินนั้นจะเป็นสิ่งที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย หรือทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูล เป็นต้น



ภาพที่ 2.1 องค์ประกอบความมั่นคงปลอดภัยของสารสนเทศ

ที่มา : http://jjsao.blogspot.com/2015/05/blog-post.html

(1) ความลับ (Confidentiality) คือ การรักษาความลับให้กับข้อมูลเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ หลักการสำคัญของการรักษาความลับคือ ผู้ที่มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ภาคธุรกิจให้

ความสำคัญกับการรักษาความลับทางธุรกิจ ประชาชนทั่วไปก็ต้องการปกป้องข้อมูลส่วนตัวตามสิทธิขั้นพื้นฐานเช่นเดียวกัน ยกตัวอย่างเช่น ข่าวการละเมิดมาตรการป้องกันของระบบคอมพิวเตอร์เข้าไปเจาะระบบทั้งในประเทศและต่างประเทศ แสดงให้เห็นว่ามาตรการที่มีอยู่ยังมีจุดอ่อนที่ ผู้ไม่ประสงค์ดีที่มีความรู้บุกรุกผ่านช่องโหว่ดังกล่าว แรงจูงใจของการกระทำการดังกล่าวมีหลายเหตุปัจจัย เช่น ทำเพื่อเงิน เพื่อสร้างชื่อเสียง การยอมรับในกลุ่ม และทำไปด้วยความคึกคะนอง ปฏิเสธไม่ได้ว่าแฮกเกอร์ที่สามารถเจาะทะลุระบบรักษาความปลอดภัยของหน่วยงานสำคัญระดับประเทศ จะกลายเป็นฮีโร่ในสายตาของแฮกเกอร์มือใหม่ทั่วโลก ดังนั้น ระบบรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีประสิทธิภาพ ต้องมีมาตรการตรวจสอบสิทธิก่อนเข้าถึง เพื่อยืนยันให้แน่ใจก่อนว่าผู้ที่ร้องขอนั้นมีสิทธิหรือได้รับอนุญาตให้เข้าถึงสารสนเทศ หรือระบบงานนั้นได้ กลไกพื้นฐานที่คุ้นเคยกันเป็นอย่างดี คือการใช้รหัสผ่าน(Password) ในการพิสูจน์ตัวตนและสิทธิที่ได้รับอนุญาต นอกจากมาตรการตรวจสอบสิทธิแล้วการกำหนดชั้นความลับเป็นระดับต่าง ๆ ตามความสำคัญช่วยให้บริหารจัดการมีประสิทธิภาพมากขึ้น ในบางหน่วยงานกำหนดชั้นความลับของสารสนเทศออกเป็น 4 ระดับ ประกอบด้วย ระดับชั้นความลับสุดยอด (Top Secret) ระดับชั้นความลับ (Secret) ระดับชั้นข้อมูลสำหรับใช้ภายในองค์กร(Internal Use) และระดับชั้นสารธารณะ (Public) ชั้นความลับนี้จะต้องมีเกณฑ์พิจารณาที่ชัดเจนว่าสารสนเทศลักษณะใดอยู่ในชั้นความลับที่กำหนด พร้อมทั้งกำหนดแนวทางการ การระบุชั้นความลับ การจัดเก็บ และการสื่อสารข้อมูลสารสนเทศในแต่ละชั้นความลับอย่างชัดเจน มาตรการทางเทคนิคที่ใช้ในการปกป้องความลับ เช่น การเข้ารหัส (Encryption) อาจถูกนำมาใช้เสริมความแข็งแกร่งให้กับมาตรการปกป้องสารสนเทศที่ต้องการมาตรการดูแลอย่างเข้มงวด

(2) ความถูกต้องสมบูรณ์ (Integrity) คือ การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ (Integrity) เป็นสิ่งสำคัญส่งผลถึงความน่าเชื่อถือของสารสนเทศนั้น ๆ ทำอย่างไรให้ข้อมูลมีความถูกต้องและน่าเชื่อถือเป็นสิ่งที่ผู้ดูแลระบบต้องหาคำตอบและดำเนินการให้เกิดขึ้น คำตอบในเชิงหลักการคือระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใด ๆ ต่อข้อมูลนั้น ยิ่งเทคโนโลยีสารสนเทศพัฒนาก้าวหน้าไปมากเท่าไร มนุษย์ก็ยิ่งจำเป็นต้องพึงพาเทคโนโลยีมากขึ้นตามไปด้วย บัตรประชาชนอัจฉริยะเป็นตัวอย่างใกล้ตัวเราที่ชี้ให้เห็นว่า ประชาชนทุกคนไม่ว่าจะยากดีมีจนอย่างไร ก็ต้องเกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเลี่ยงไม่ได้ อย่างน้อยข้อมูลส่วนตัวของเราก็ถูกจัดเก็บในฐานข้อมูลของรัฐบาล ลองนึกดูว่าจะเกิดอะไรขึ้นหากชื่อของนาย ก. ถูกลบออกจากบัญชีทะเบียนราษฎร์ นั่นหมายถึง นาย ก. ไม่มีตัวตนและไม่สามารถใช้สิทธิของประชาชนในการรับบริการรัฐได้ จะเห็นได้ว่าข้อมูลนี้มีความสำคัญมากเพราะเป็นหลักฐานในการพิสูจน์ตัวตนของเรา หากมองในแง่ความ

มั่นคงปลอดภัยของสารสนเทศแล้ว ข้อมูลนี้จำเป็นต้องได้รับการปกป้องดูแลความถูกต้องสมบูรณ์และความน่าเชื่อถือ หากข้อมูลถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดีย่อมส่งผลเสียต่อเจ้าของข้อมูลอย่างหลีกเลี่ยงไม่ได้

(3) ความพร้อมใช้งาน (Availability) คือ การทำให้ระบบตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ อุปสรรคที่บั่นทอนความพร้อมใช้งานของระบบคอมพิวเตอร์จำแนกได้ 2 แบบ คือ

- การที่ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service)
- ระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of data processing capability)

ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ อาจเกิดจากการกระทำของผู้ใช้ระบบ ผู้บุกรุกที่มีเจตนาร้าย หรือเกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหวทำให้ระบบคอมพิวเตอร์เสียหายก็เป็นได้ องค์กรที่ตระหนักถึงภัยคุกคามดังกล่าวอาจเตรียมแผนกู้คืนจากความเสียหาย (Disaster Recovery Plan) ไว้รองรับ หน่วยงานรัฐที่ให้บริการสาธารณะต่างใช้ระบบคอมพิวเตอร์ควบคุมการทำงาน เช่นไฟฟ้า ประปา โทรศัพท์ เป็นต้น หากคอมพิวเตอร์ที่ควบคุมระบบเหล่านี้เกิดความเสียหายไม่สามารถให้บริการได้ ทำให้บริการต่าง ๆ หยุดชะงักย่อมส่งผลเสียต่อประชาชนในวงกว้าง นอกจากนี้หากไฟฟ้าดับเป็นเวลานาน ระบบต่าง ๆ จะเกิดความเสียหายอย่างใหญ่หลวง ตัวอย่างจริงที่เคยเกิดขึ้นในต่างประเทศ เมื่อหลายปีก่อนระบบคอมพิวเตอร์ของศูนย์กระจายสินค้าเกิดความเสียหาย ไม่สามารถจ่ายกระแสไฟฟ้าไปยังคอนเทนเนอร์ที่ติดตั้งระบบทำความเย็นเป็นเวลาหลายวัน ส่งผลให้สินค้าในตู้คอนเทนเนอร์ดังกล่าวเสียหายทั้งหมด นอกจากนี้ยังทำให้ลูกค้าขอยกเลิกสัญญาเนื่องจากไม่ไว้วางใจในการบริการ เกิดความสูญเสียมูลค่ามหาศาล

ตารางที่ 2.1 เปรียบเทียบหลักการ CIA กับ พรบ.ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

หลักสำคัญ	ข้อกำหนดตามประกาศที่เกี่ยวข้อง
1. การธำรงไว้ซึ่งความลับ (Confidentiality)	ข้อ 8 ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) ข้อ 9 ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control)

ตารางที่ 2.1 (ต่อ)

หลักสำคัญ	ข้อกำหนดตามประกาศที่เกี่ยวข้อง
	ข้อ 10 ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control)
	ข้อ 11 ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)
2. ความถูกต้องครบถ้วน (Integrity)	ข้อ 5 ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)
	ข้อ 6 ให้มีข้อกำหนดการใช้งานตามภาคกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control)
	ข้อ 7 ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)
3. ความพร้อมใช้ หรือสภาพพร้อมใช้งาน (Availability)	ข้อ 12 หน่วยงานองรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง
	ข้อ 13 หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบการประเมินความเสี่ยงด้านสารสนเทศ

ที่มา: นโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย

ภัยคุกคาม และช่องโหว่ (Threat and Vulnerability)

(1) ภัยคุกคาม (Threat) อาจเป็นมนุษย์ ภัยธรรมชาติ หรือปัจจัยอื่น ๆ ที่มีแนวโน้มที่จะก่อให้เกิดความเสียหายได้ ทั้งที่เจตนาสร้างความเสียหายหรือไม่ก็ตาม การทำความเข้าใจและตระหนักถึงภัยคุกคามจะช่วยให้เข้าใจองค์ประกอบที่เกี่ยวข้องกันทั้งระบบได้เป็นอย่างดี หากจำแนกแหล่งกำเนิดของภัยคุกคาม อาจแบ่งได้ดังนี้

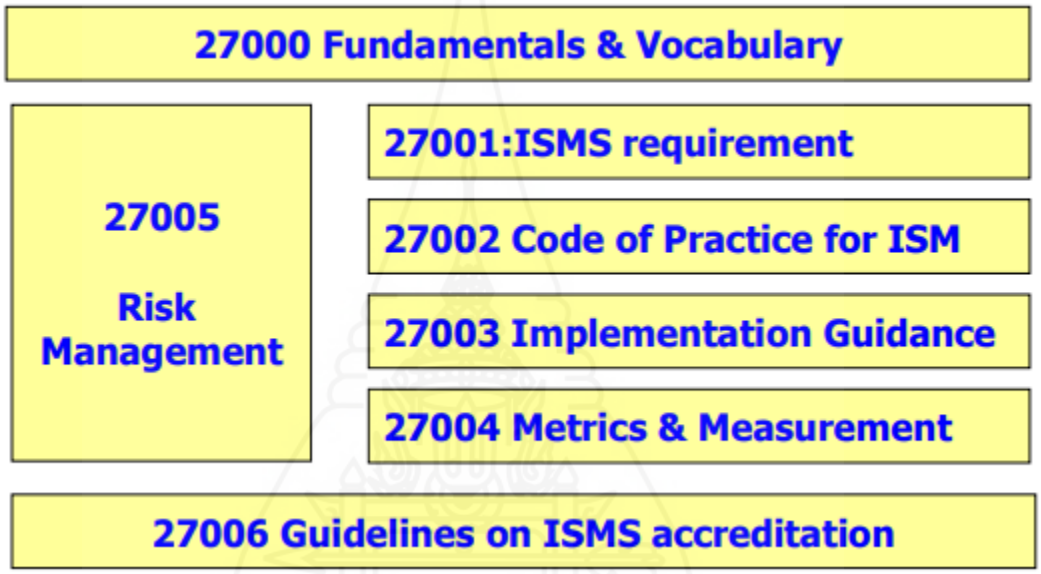
- มนุษย์ เช่น แฮกเกอร์ สายลับ ผู้ก่อการร้าย ผู้ไม่ประสงค์ดีที่โจมตีระบบสารสนเทศ ไวรัส โปรแกรมไม่ประสงค์ดีต่าง ๆ เป็นต้น
- ภัยธรรมชาติ เช่นน้ำท่วม ฟ้าผ่า พายุ แผ่นดินไหว เป็นต้น
- ข้อผิดพลาดทางเทคนิค เช่น อุปกรณ์ชำรุด เสื่อมสภาพ หรือทำงานผิดพลาดเป็นต้น

(2) ช่องโหว่ (Vulnerability) เป็นองค์ประกอบที่สำคัญของการศึกษาเรื่องความมั่นคงปลอดภัยของสารสนเทศ ภัยคุกคามที่กล่าวมาข้างต้นจะใช้ประโยชน์จากช่องโหว่นี้เพื่อสร้างความ

เสียหาย ดังนั้นหากช่องโหว่มีจำนวนมาก โอกาสที่ภัยคุกคามจะสร้างความเสียหายจากช่องโหว่ดังกล่าวก็มากตามไปด้วย กล่าวได้ว่าหากไม่มีช่องโหว่หรือจุดอ่อน ภัยคุกคามก็ไม่สามารถทำอันตรายแก่ระบบสารสนเทศได้

1.2 มาตรฐาน ISO

ISO 27000 Family ประกอบด้วย



ภาพที่ 2.2 ISO 27000 Family

ที่มา: https://www.iso.org

ISO 27000 มีวัตถุประสงค์เพื่อแสดง ศัพท์และนิยาม (Vocabulary and Definitions) ที่ใช้ในมาตรฐาน นั่นคือ ศัพท์บัญญัติ (Terminology) ทั้งหลายที่ใช้ในมาตรฐานการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Standards- ISMS)

ISO 27001 คือ มาตรฐานที่จำเป็นของ ISMS ได้แก่ คุณลักษณะเฉพาะ (Specification) ซึ่งองค์กรทั้งหลายจะต้องขอรับ "ใบรับรอง" (Certificate) จากหน่วยงานภายนอก ว่าได้มี "การปฏิบัติตามข้อกำหนด (Compliance)" เหล่านี้แล้ว อย่างเป็นทางการ

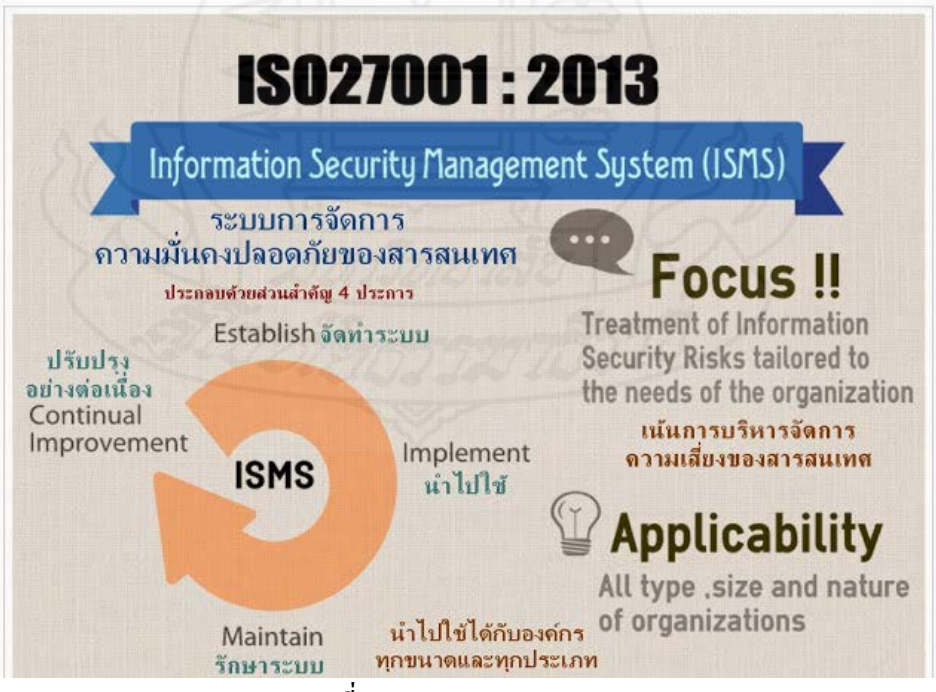
ISO 27002 เป็นชื่อเรียกใหม่ของ ISO 17799 ซึ่งเดิมเรียกว่า "BS 7799 Part 1" เป็นมาตรฐานแสดง หลักปฏิบัติสำหรับ ISM (Code of practice for Information Security Management) ที่อธิบายวัตถุประสงค์ของระเบียบวิธีการควบคุมด้าน IS ทั้งหลายอย่างละเอียด และแสดงรายการวิธีปฏิบัติที่ดีที่สุด ของการควบคุมความมั่นคงปลอดภัย (Best-practice security controls)

ISO 27003 เป็นแนวทางประยุกต์ใช้มาตรฐาน (Implementation guide)

ISO 27004 เป็นมาตรฐานการวัด ISM เพื่อที่จะช่วยวัดประสิทธิภาพหรือประเมินผลการนำ ISMS ไปใช้

ISO 27005 เป็นมาตรฐาน "การบริหารจัดการความเสี่ยงด้าน IS (Information Security Risk Management)" ซึ่งจะมาแทนที่มาตรฐานเดิม ได้แก่ "BS 7799 Part 3" ISO/IEC 27005 จึงเป็นมาตรฐานที่จัดเตรียมให้องค์กรมีวิธีการในการจัดเตรียมกรอบการดำเนินงานในการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ ISO/IEC 27005 เป็นเอกสารที่ให้สนับสนุนแนวคิดของมาตรฐาน ISO/IEC 27001 (ข้อกำหนดสำหรับการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล หรือ ISMS) มาตรฐานนี้ให้แนวทางของการบริหารจัดการความเสี่ยงในรายละเอียดเพื่อช่วยให้ตอบสนองข้อกำหนดที่เกี่ยวข้องตามมี่ระบุไว้ในมาตรฐาน ISO/IEC 27001 ทำให้สามารถนำไปใช้งาน รักษาไว้ซึ่งมาตรฐานและปรับปรุงระบบการจัดการด้านความปลอดภัยของข้อมูลอย่างต่อเนื่องซึ่งเหมาะกับบริบทขององค์กร

ISO 27006 เป็นแนวทางปฏิบัติสำหรับกระบวนการ ออกใบรับรอง (Certification process) หรือการลงทะเบียน (Registration process) .ให้กับหน่วยงานที่เกี่ยวข้อง (ISMS certification/registration bodies)

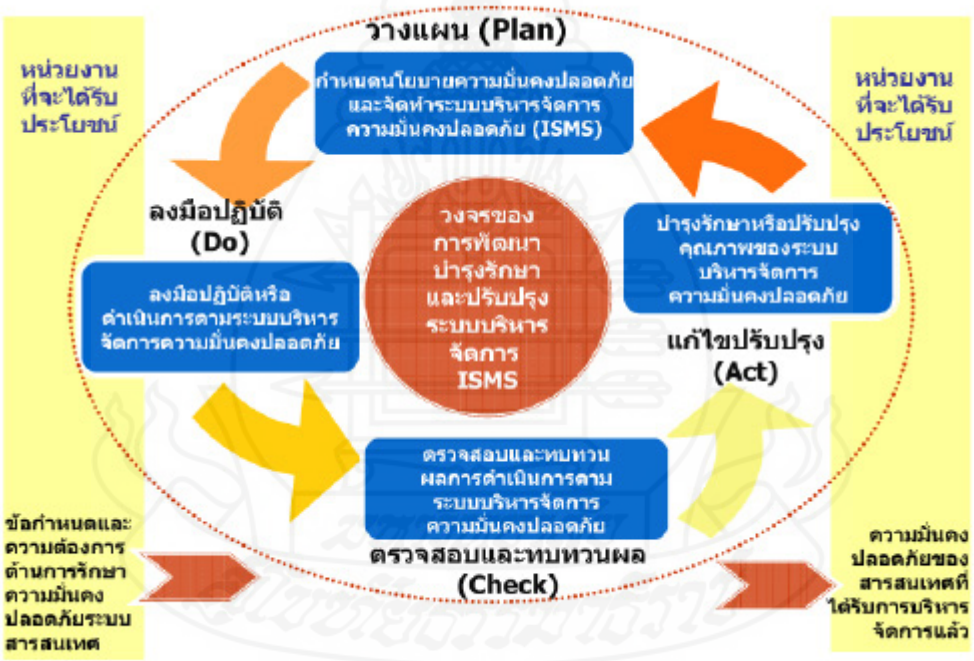


ภาพที่ 2.3 มาตรฐาน ISO 27001

ที่มา: http://www.club27001.com/2014/01/review-iso27001-2013-part1.html

Information Security Management System (ISMS) Standard หรือที่รู้จักกันในนาม ISO 27001 เป็นมาตรฐานที่เกี่ยวกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัย

องค์กร ISO - International Organization for Standardization เป็นหน่วยงานที่ให้กำเนิดมาตรฐาน ISO27001 โดยเวอร์ชั่นล่าสุดคือ ISO27001:2013 ประกาศเมื่อ 1 ต.ค. 2013 ส่วนเวอร์ชั่นแรกประกาศใช้ครั้งแรกเมื่อปี 2550 (ISO27001:2005) หลังจากประกาศใช้ก็ได้รับความสนใจจากองค์กรทั้งภาครัฐและเอกชนทั่วโลก นำมาใช้งานและขอการรับรอง (Certification) ประเทศไทยเองก็ไม่แพ้ชาติใดในโลก มีหน่วยงานรัฐและเอกชนเริ่มทำ ISO27001 และขอการรับรองได้สำเร็จ เช่น บริษัท ไทยออยล์ จำกัด (มหาชน) บริษัท ทรู อินเทอร์เน็ต ดาต้าเซ็นเตอร์ จำกัด (True IDC) และรัฐวิสาหกิจอีกหลายแห่ง โดยมาตรฐานนี้ออกแบบมาให้ใช้ได้ในประเภทธุรกิจ หน่วยราชการ สถานศึกษา และใช้ได้กับองค์กรทั้งขนาดเล็กและขนาดใหญ่



ภาพที่ 2.4 แผนภาพแสดงวงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act

ที่มา: http://prowcharinrat.blogspot.com/

จากภาพที่ 2.4 แสดงให้เห็นถึงแบบจำลองขั้นตอนการทำงานของระบบ ISMS ที่ตรงตามความต้องการของกลุ่มองค์กร รวมถึงระบบการปฏิบัติงานต่างๆ ที่เกิดขึ้นทำให้ระบบการรักษา

ความปลอดภัยข้อมูลตรงตามความต้องการและความคาดหมายได้ ซึ่งแต่ละขั้นตอนประกอบด้วยรายละเอียดโดยย่อดังต่อไปนี้ 1) Plan คือการวางแผน/กำหนดนโยบายความมั่นคงและจัดทำระบบ ISMS 2) Do คือการลงมือปฏิบัติหรือดำเนินการตามระบบ ISMS 3) Check คือการตรวจสอบและทบทวนผลการดำเนินการตามระบบ ISMS และ 4) Act คือ การแก้ไขปรับปรุง/บำรุงรักษาหรือปรับปรุงคุณภาพของระบบ ISMS

1. กำหนดและบริหารจัดการ ระบบบริหารจัดการความมั่นคงปลอดภัย ดังต่อไปนี้

1) กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan) โดยองค์กรควรกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยและกำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี นอกจากนี้ ยังต้องกำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร ระบบความเสี่ยง วิเคราะห์และประเมินความเสี่ยง ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ เลือกวัตถุประสงค์และมาตรการทางด้านความปลอดภัยเพื่อจัดการกับความเสี่ยง ขออนุมัติและความเห็นชอบสำหรับความเสี่ยงที่ยังหลงเหลืออยู่ในระบบบริหารจัดการความมั่นคงปลอดภัย ขอการอนุมัติเพื่อลงมือปฏิบัติและดำเนินการ และสุดท้ายคือ จัดทำเอกสาร SoA (Statement of Applicability) แสดงการใช้งานมาตรฐานตามที่แสดงไว้ในส่วนของมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์

2) ลงมือปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัย (Do) โดยองค์กรควรจัดทำแผนการจัดการความเสี่ยง ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงและตามมาตรฐานที่เลือกไว้ กำหนดวิธีการในการวัดความสัมฤทธิ์ผลของมาตรการที่เลือกมาใช้งาน จัดทำและลงมือปฏิบัติตามแผนการอบรมและสร้างความตระหนัก บริหารจัดการดำเนินงานและบริหารทรัพยากรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย รวมถึงจัดทำและลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่นๆ ซึ่งช่วยในการตรวจจับและรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย

3) เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check) โดยองค์กรควรลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่นๆ สำหรับการเฝ้าระวังและทบทวนดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ วัดความสัมฤทธิ์ผลของมาตรการทางด้านความมั่นคงปลอดภัย ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยงที่เหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ ดำเนินการตรวจสอบและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย ปรับปรุงแผนทางด้านความปลอดภัยโดยนำผลของการเฝ้าระวังและทบทวนกิจกรรมต่างๆ มาพิจารณาร่วมด้วย และ

บันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

4) บำรุงรักษาและปรับปรุงระบบบริหารจัดการด้านความมั่นคงปลอดภัย (Act) โดยองค์กรควรปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้ รวมถึงการใช้มาตรการเชิงแก้ไข ป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและองค์กรอื่น แจ้งการปรับปรุงและดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง และตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

2. ข้อกำหนดทางด้านการจัดทำเอกสาร

1) ความต้องการทั่วไป เอกสารที่จำเป็นต้องจัดทำจะรวมถึงบันทึกแสดงการตัดสินใจของผู้บริหาร ได้แก่ นโยบายความมั่นคงปลอดภัย ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย วิธีการประเมินความเสี่ยง เป็นต้น

2) การบริหารจัดการเอกสาร ซึ่งเอกสารตามข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยจะต้องได้รับการป้องกันและควบคุม ขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการจัดการเอกสาร ได้แก่ อนุมัติการใช้งานเอกสารก่อนที่จะเผยแพร่ ทบทวน ปรับปรุงและอนุมัติเอกสารตามความจำเป็น ระบุการเปลี่ยนแปลงและสถานภาพของเอกสารปัจจุบัน เป็นต้น

3) การบริหารจัดการบันทึกข้อมูลหรือฟอร์มต่างๆ องค์กรจะต้องมีการกำหนดจัดทำและบำรุงรักษาบันทึกข้อมูลหรือฟอร์มต่างๆ เพื่อใช้เป็นหลักฐานแสดงความสอดคล้องกับข้อกำหนดและการดำเนินการที่มีประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

การนำมาตรฐาน ISO/IEC 27001 มาใช้งาน มี 4 องค์ประกอบใหญ่ ดังนี้

ภาพที่ 2.5 บันได 4 ขั้น ตามมาตรฐาน ISO/IEC 27001

ที่มา: http://www.club27001.com

(1) บันไดขั้นที่ 1 การวางแผนจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Plan : Establish the ISMS) โดยเริ่มต้นด้วยการกำหนดขอบเขตของการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศให้ชัดเจน โดยแสดงถึงลักษณะของธุรกิจ องค์กร ทำเลที่ตั้ง ทรัพย์สิน และเทคโนโลยี หากไม่ครอบคลุมส่วนงานใด ต้องระบุรายละเอียดและเหตุผลดังกล่าว จากนั้นผู้บริหารระดับสูงกำหนดนโยบายการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System Policy : ISMS Policy) พร้อมทั้งอนุมัติและประกาศใช้นโยบายดังกล่าว เป็นกลไกให้มั่นใจว่าโครงการนี้ได้รับการสนับสนุนอย่างเป็นรูปธรรม และเป็นสัญญาณว่า ISMS ได้เริ่มอย่างเป็นทางการแล้ว ซึ่งการกำหนดคณะทำงานให้เหมาะสมและเพียงพอเป็นเรื่องสำคัญที่ต้องพิจารณา ตัวแทนหน่วยงานที่อยู่ในขอบเขตการจัดทำระบบควรเข้าร่วมเป็นคณะทำงานเพื่อให้มีส่วนร่วมในการจัดทำระบบที่สอดคล้องกับลักษณะการทำงาน เมื่อได้คณะทำงานเรียบร้อยแล้วก็เริ่มสำรวจภัยคุกคามและช่องโหว่ที่ก่อให้เกิดความเสี่ยงต่อสารสนเทศในขอบเขตการจัดทำระบบขององค์กร ตัวแทนหน่วยงานที่เป็นคณะทำงานก็รับผิดชอบสำรวจภัยคุกคามและช่องโหว่ในหน่วยงานของตนเอง ผลการประเมินความเสี่ยงจะบอกถึงระดับความเสี่ยงจากภัยคุกคามและช่องโหว่ในระบบสารสนเทศ คณะทำงานและผู้เกี่ยวข้องต้องกำหนดมาตรการจัดการกับความเสี่ยงนั้นให้ชัดเจนและมีประสิทธิภาพเพียงพอ

(2) บันไดขั้นที่ 2 การนำไปปฏิบัติ (Do : Implement and Operate the ISMS) ขั้นตอนการปฏิบัติ (Do) เป็นการนำผลลัพธ์ของขั้นตอนวางแผน (Plan) มาปฏิบัติให้เกิดผลตามวัตถุประสงค์ เช่น มาตรการป้องกันการบุกรุกระบบ มาตรการสำรองข้อมูล เป็นต้น ซึ่งก่อนจะปฏิบัติได้อย่างถูกต้องนั้น จำเป็นต้องมีการฝึกอบรม ถ่ายทอดความรู้แนวทางปฏิบัติที่ถูกต้องให้รับทราบทั่วกัน

(3) บันไดขั้นที่ 3 การเฝ้าระวังและทบทวน (Check : Monitoring and Review the ISMS) โดยหลังจากปฏิบัติตามมาตรการที่กำหนดแล้ว เราจะรู้ได้อย่างไรว่ามาตรการที่ปฏิบัตินั้นได้ผลตามเป้าหมายที่ต้องการ คำตอบคือต้องมีการวัดผลของมาตรการที่ใช้ควบคุมดูแล แนวทางการวัดผลและความถี่ในการเฝ้าระวังต้องสอดคล้องกับความเสี่ยง ดังนั้นกระบวนการระบบงาน หรือทรัพย์สินสารสนเทศที่มีความเสี่ยงสูงควรได้รับการเฝ้าระวังและวัดผลการปฏิบัติงานที่เข้มงวดกว่า เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบการตรวจวัดและเฝ้าระวังสามารถรายงานผลได้ทันเวลา

(4) บันไดขั้นที่ 4 การรักษามาตรฐานและปรับปรุงให้ดีขึ้น (Act : Maintain and Improve the ISMS) โดยหลังจากที่ตรวจพบปัญหาหรือสิ่งผิดปกติในขั้นตอนการตรวจสอบ(Check : Monitoring and Review the ISMS) ผู้ที่เกี่ยวข้องทุกระดับจำเป็นต้องร่วมกันแก้ไขปัญหาที่เกิดขึ้น

และป้องกันปัญหาที่อาจเกิดซ้ำในอนาคต รวมถึงหาแนวทางปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น กลไกสำคัญที่ช่วยให้ผลักดันให้การแก้ไขปัญหาและปรับปรุงดำเนินการได้อย่างเป็นรูปธรรม คือการมีส่วนร่วมของผู้บริหารระดับสูง บ่อยครั้งที่พบว่าปัญหาเกิดจากการขาดความชัดเจนในนโยบายการบริหารจัดการ ซึ่งผู้บริหารจะต้องให้ความกระจ่างและตัดสินใจแก้ไขปัญหาเชิงนโยบายให้เป็นรูปธรรม เพื่อให้คณะทำงานยึดถือเป็นแนวปฏิบัติต่อไป

1.3 โดเมนตามมาตรฐาน ISO/IEC 27001:2013

มาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็น Version ปัจจุบัน โดยแบ่งออกเป็น 14 โดเมน (บริษัท ที-เน็ต จำกัด, 2556) ประกอบด้วย ดังนี้

ภาพที่ 2.6 ข้อกำหนดหลักของมาตรฐาน ISO/IEC 27001

ที่มา: https://www.iso.org

A.5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy): ให้หน่วยงานกำหนดทิศทางในการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับภารกิจของหน่วยงาน

A.6 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security): ให้หน่วยงานจัดทำกรอบในการควบคุมให้เกิดการดำเนินงานด้านความมั่นคงปลอดภัย

A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security): ให้ผู้เกี่ยวข้องในหน่วยงานรู้หน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยของหน่วยงาน

A.8 การบริหารจัดการทรัพย์สิน (Asset Management): ให้หน่วยงานสามารถทรัพย์สินและกำหนดการดูแลรักษาทรัพย์สินของหน่วยงานได้

A.9 การควบคุมการเข้าถึง (Access Control): ให้หน่วยงานจำกัดการเข้าถึงเทคโนโลยีสารสนเทศของหน่วยงาน

A.10 การเข้ารหัสข้อมูล (Cryptography): ให้หน่วยงานมีการเข้ารหัสอย่างเหมาะสม เพื่อให้ข้อมูลมีความถูกต้องพร้อมใช้งาน

A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security): ให้หน่วยงานมีการป้องกันไม่ให้ผู้ไม่ได้รับอนุญาตเข้าถึงเทคโนโลยีสารสนเทศของหน่วยงานได้

A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security): ให้หน่วยงานปฏิบัติงานด้านความมั่นคงปลอดภัยอย่างถูกต้อง

A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security): ให้หน่วยงานมีการควบคุมการใช้งานระบบเครือข่ายอย่างเหมาะสมและปลอดภัย

A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance): ให้หน่วยงานมีการจัดหา พัฒนาระบบมีความมั่นคงปลอดภัย

A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships): ให้หน่วยงานมีการป้องกันการเข้าถึงทรัพย์สินจากบุคคลภายนอก

A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management): ให้หน่วยงานมีการบริหารจัดการด้านความมั่นคงปลอดภัยที่เหมาะสม

A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management): ให้หน่วยงานสามารถให้บริการประกอบการได้อย่างต่อเนื่อง

A.18 ความสอดคล้อง (Compliance): ให้หน่วยงานมีการจัดการรักษาความมั่นคงปลอดภัยที่เหมาะสม ไม่ขัดต่อระเบียบ ข้อกฎหมายที่เกี่ยวข้อง

1.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ตามมาตรฐาน ISO/IEC 27001:2013

ข้อกำหนดหลักที่ต้องปฏิบัติตามในการขอการรับรองตามมาตรฐาน ISO/IEC 27001:2013 มีจำนวน 7 ข้อ (บริษัท ที-เน็ต จำกัด, 2556) ดังนี้

ข้อที่ 1 บริบทขององค์กร (Context of the organization)

1.1 การทำความเข้าใจบริบทขององค์กร (Understanding the organization and its context) คือ องค์กรต้องกำหนดประเด็นภายในและภายนอกองค์กรที่เกี่ยวข้องกับจุดประสงค์ขององค์กรและที่ส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1.2 การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties) คือ องค์กรต้องกำหนด

(1) ผู้เกี่ยวข้อง ซึ่งเป็นผู้ที่เกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและ

(2) ความต้องการของผู้ที่เกี่ยวข้องเหล่านั้นซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

1.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system) องค์กรต้องกำหนดกรอบและการประยุกต์ระบบบริหารจัดการความมั่นคงลอดภัยสารสนเทศเพื่อระบุขอบเขตการดำเนินการ โดยในการระบุขอบเขต องค์กรต้องพิจารณา

(1) ประเด็นภายในและภายนอกองค์กร โดยอ้างอิงจากข้อ 1.1

(2) ความต้องการ โดยอ้างอิงจากข้อ 1.2 และ

(3) การเชื่อมโยงและการสัมพันธ์กันของกิจกรรมในลักษณะที่กิจกรรมขึ้นอยู่กับซึ่งกันและกันโดยมีกิจกรรมเหล่านี้อาจดำเนินการโดยองค์กรเองหรือโดยองค์กรอื่น ๆ

ขอบเขตต้องสามารถเข้าถึงได้โดยจัดทำเป็นลายลักษณ์อักษร

1.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) คือ องค์กรต้องกำหนด ลงมือปฏิบัติ บำรุงรักษา และปรับปรุงอย่างต่อเนื่องต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดยต้องมีความสอดคล้องกับข้อกำหนดในเอกสารมาตรฐานฉบับนี้

ข้อ 2 ภาวะผู้นำ (Leadership)

2.1 ภาวะผู้นำและการให้ความสำคัญ (Leadership and Commitment) คือ ผู้บริหารระดับสูงต้องแสดงให้เห็นถึงวาระผู้นำและการให้ความสำคัญต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดย

(1) ต้องทำให้นโยบายความมั่นคงปลอดภัยสารสนเทศและวัตถุประสงค์ปลอดภัยสารสนเทศมีการกำหนดขึ้นมาและมีความสอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กร

(2) ต้องทำให้มีการรวมความต้องการของระบบลริหารจัดการความมั่นคงปลอดภัยสารสนเทศเข้ากับกระบวนการขององค์กร

(3) ต้องทำให้มีทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการดำเนินการ

(4) ต้องสื่อสารความสำคัญของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สัมฤทธิ์ผลและของการดำเนินการตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่กำหนด

(5) ต้องทำให้ระบบบริหารจัดการความมั่นคงปลอดภัยารสนเทศบรรลุผลลัพธ์ตามที่ต้องการ

(6) ต้องสั่งการและสนับสนุบุคลากรเพื่อนำสู่ความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(7) ต้องส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง และ

(8) ต้องสนับสนุนบทบาทการบริหารอื่น ๆ ภายใต้ขอบเขตความรับผิดชอบของเพื่อแสดงภาวะผู้นำของตนเอง

2.2 นโยบาย (Policy) คือ ผู้บริหารระดับสูงต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศซึ่ง

(1) เหมาะสมต่อจุดประสงค์ขององค์กร

(2) รวมวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศไว้ด้วย (ดูข้อ 3.2) หรือกำหนดกรอบการปฏิบัติสำหรับการกำหนดวัตถุประสงค์ดังกล่าว

(3) รวมการให้ความสำคัญของผู้บริหารเพื่อให้สอดคล้องกับความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และ

(4) รวมการให้ความสำคัญของผู้บริหารในการปรับปรุงอย่างต่อเนื่องต่อระบบบริหารจัดการความมั่นคงลอดภัยสารสนเทศ

นโยบายความมั่นคงปลอดภัยสารสนเทศ :

(5) ต้องสามารถเข้าถึงได้โดยจัดทำเป็นลายลักษณ์อักษร

(6) ให้มีการรายงานประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง

2.3 บทบาท หน้าที่ ความรับผิดชอบ และอำนาจหน้าที่ (Organization role, responsibilities and authorities) คือ ผู้บริหารระดับสูงต้องทำให้หน้าที่ความรับผิดชอบและอำนาจหน้าที่ตามบทบาทที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศมีการมอบหมายและสื่อสารให้ได้รับทราบกัน

ผู้บริหารระดับสูงต้องมอบอำนาจหน้าที่ความรับผิดชอบและอำนาจหน้าที่เพื่อ

(1) ให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีความสอดคล้องกับข้อกำหนดของเอกสารมาตรฐานฉบับนี้ และ

(2) ให้มีรายงานประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง

ข้อ 3 การวางแผน (Planning)

3.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Action to address risk and opportunities) คือ

3.1.1 ภาพรวม (General) คือ เมื่อวางแผนสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องพิจารณาประเด็นภายในและภายนอกที่อ้างถึงในข้อ 1.1 และความต้องการที่อ้างถึงในข้อ 1.2 และต้องกำหนดความเสี่ยงและโอกาสที่จำเป็นต้องจัดทำเพื่อ

(1) ให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุผลลัพธ์ตามที่ต้องการ

(2) ป้องกัน หรือลดผลที่ไม่พึงปรารถนา และ

(3) ให้บรรลุการปรับปรุงอย่างต่อเนื่อง

องค์กรต้องวางแผน :

(4) การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส และ

(5) วิธีการที่จะ

(5.1) รวมการดำเนินการดังกล่าวเข้ากับกระบวนการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและนำสู่การปฏิบัติ คือ

(5.2) ประเมินความสัมฤทธิ์ผลของการดำเนินการดังกล่าว

3.1.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment) คือ องค์กรต้องกำหนดและประยุกต์กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศซึ่งต้อง

(1) กำหนดปรับปรุงเกณฑ์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งต้องรวมถึง

(1.1) เกณฑ์การยอมรับความเสี่ยง และ

(1.2) เกณฑ์สำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(2) ทำให้การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้ผลการประเมินที่สอดคล้องกัน ถูกต้อง และเปรียบเทียบกันได้

(3) ระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(3.1) ประยุกต์กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อระบุความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้ของสารสนเทศภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ

(3.2) ระบุผู้เป็นเจ้าของความเสี่ยง

(4) วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(4.1) ประเมินผลที่เป็นไปได้ที่จะเกิดขึ้นถ้าความเสี่ยงที่ระบุไว้ในข้อ 3.1.1 (3) เกิดขึ้นจริง

(4.2) ประเมินโอกาสการเกิดขึ้นสมจริงของความเสี่ยงที่ระบุไว้ในข้อ 3.1.2 (3) และ

(4.3) กำหนดระดับของความเสี่ยง

(5) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(5.1) เปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนดไว้ในข้อ 3.1.2 (1) และ

(5.2) จัดลำดับความเสี่ยงที่วิเคราะห์นั้นเพื่อการจัดการที่เหมาะสม

องค์กรต้องจัดเก็บสารสนเทศที่เกี่ยวข้องกับกระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อย่างเป็นลายลักษณ์อักษร

3.1.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment) คือ องค์กรต้องกำหนดและประยุกต์กระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศซึ่งต้อง

(1) กำหนดทางเลือกที่เหมาะสมในการจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศโดยต้องนำผลการประเมินความเสี่ยงมาพิจารณาด้วย

(2) กำหนดมาตรการทั้งหมดที่จำเป็นเพื่อดำเนินการตามทางเลือกที่กำหนดไว้

(3) เปรียบเทียบมาตรการที่กำหนดไว้ในข้อ 3.1.3 (2) กับมาตรการใน Annex A และตรวจสอบว่าไม่มาตรการข้อใดที่ละเลยไป

(4) จัดทำเอกสารแสดงการใช้มาตรการ SoA (Statement of Applicability) ซึ่งประกอบด้วยมาตรการที่จำเป็น (ดูข้อ 3.1.3 (2) และ (3)) และคำอธิบายเหตุผลของการใช้มาตรการไม่ว่ามาตรการเหล่านั้นจะได้รับการปฏิบัติแล้วหรือไม่ก็ตาม และคำอธิบายเหตุผลของการไม่ใช่มาตรการจาก Annex A

(5) จัดทำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และ

(6) ขอการรับรองจากผู้เป็นเจ้าของความเสี่ยงสำหรับแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และการยอมรับสำหรับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่ยังเหลืออยู่

องค์กรต้องจัดเก็บสารสนเทศที่เกี่ยวข้องกับกระบวนการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อย่างเป็นลายลักษณ์อักษร

3.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ (Information security objectives and plans to achieve them) องค์กรต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในฟังก์ชันงานและระดับที่เกี่ยวข้อง โดยวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศต้อง

(1) สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ

(2) สามารวัดได้ (ถ้าสามารถปฏิบัติได้)

(3) นำความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ผลการประเมินและการจัดการความเสี่ยงมาพิจารณาด้วย

(4) มีการสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ และ

(5) มีการปรับปรุงตามความเหมาะสม

องค์กรต้องจัดเก็บสารสนเทศสำหรับวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ไว้อย่างเป็นลายลักษณ์อักษร

เมื่อวางแผนวิธีการที่บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องกำหนด

(6) สิ่งที่ต้องดำเนินการ

(7) ทรัพยากรที่ต้องใช้

(8) ผู้รับผิดชอบในการดำเนินการ

(9) ระยะเวลาที่จะดำเนการให้เสร็จ และ

(10) วิธีประเมินผลการปฏิบัติการ

ข้อ 4 การสนับสนุน (Support)

4.1 ทรัพยากร (Resources) องค์กรต้องกำหนดและให้ทรัพยากรที่จำเป็นสำหรับการกำหนด การลงมือปฏิบัติ การบำรุงรักษา และการปรับปรุงอย่างต่อเนื่องต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4.2 สรรถนะ (Competence) องค์กรต้อง

(1) กำหนดสมรรถะของบุคลากรที่ทำงานภายใต้การควบคุมดูแลขององค์กร ซึ่งส่งผลต่อประสิทธิภาพในการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ

(2) ทำให้บุคลากรเหล่านี้มีความสามารถโดยการให้ความรู้ การฝึกอบรม หรือจากประสบการณ์การทำงานที่ได้รับ

(3) ดำเนินการตามความเหมาะสมเพื่อให้ได้มาซึ่งสมรรถนะที่จำเป็น และประเมินความสัมฤทธิ์ผลของการดำเนินการนั้น และ

(4) จัดเก็บสารสนเทศที่เหมาะสมอย่างเป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดงสมรรถนะ

4.3 การสร้างความตระหนัก (Awareness) บุคลากรที่ทำงานภายใต้การควบคุมดูแลขององค์กรต้องตระหนักถึง

(1) นโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

(2) การมีตนเองมีส่วนในความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงข้อดีของการปรับปรุงประสิทธิภาพในการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง และ

(3) สิ่งที่เกี่ยวข้องของการไม่ปฏิบัติตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4.4 การสื่อสารให้ทราบ (Communication) องค์กรต้องกำหนดความจำเป็นสำหรับการสื่อสารให้ทราบทั้งภายในและภายนอกที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึง

(1) อะไรบ้างที่ต้องสื่อสารให้ทราบ

(2) เมื่อไรที่ต้องสื่อสารให้ทราบ

(3) ใครบ้างที่ต้องสื่อสารให้ทราบ

(4) ใครเป็นผู้สื่อสารออกไป และ

(5) กระบวนการที่เกี่ยวข้องกับการสื่อสาร

4.5 สารสนเทศที่เป็นลายลักณ์อักษร (Documented information)

4.5.1 ภาพรวม (General) ระบบบริหารจัดการความมั่นคงปลอดภัยขององค์กรต้องรวม

(1) สารสนเทศที่เป็นลายลักณ์อักษรซึ่งกำหนดโดยมาตรฐานฉบับนี้ และ

(2) สารสนเทศที่เป็นลายลักษณ์อักษรซึ่งกำหนดโดยองค์กรเองและจำเป็นสำหรับความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4.5.2 การสร้างและปรับปรุง (Creating and updating) เมื่อมีการสร้างและปรังปรุงสารสนเทศที่เป็นลายลักณ์อักษร องค์กรต้องกำหนดประเด็นเหล่านี้ให้มีความเหมาะสม

(1) ชื่อและรายละเอียด (เช่น ชื่อเอกสาร วันที่ ผู้แต่ง หรือเลขที่อ้างอิง)

(2) รูปแบบ (เช่น ภาษา เวอร์ชั่น กราฟิก) และสื่อบันทึก (เช่น กระดาษ อิเล็กทรอนิกส์) และ

(3) การทบทวนและการอนุมัติเพื่อความเหมาะสมและเพียงพอ

4.5.3 การควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร (Control of documented information) สารสนเทศที่เป็นลายลักษณ์อักษรที่จำเป็นต้องมีสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและตามาตรฐานฉบับนี้ต้องมีการควบคุมเพื่อให้

(1) สารสนเทศสามารถเข้าถึงได้และเหมาะสมสำหรับการใช้งาน สถานที่และวันเวลาในการใช้งาน และ

(2) สารสนเทศที่ได้รับการป้องกันและเพียงพอ (เช่น จากการสูญเสียความลับ การใช้งานที่ไม่เหมาะสม หรือการสูญเสียความถูกต้องสมบูรณ์)

สำหรับการควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร องค์กรต้องระบุกิจกรรมดังต่อไปนี้ตามความเหมาะสม

(3) แจกจ่าย การเข้าถึง การนำขึ้นมาใช้ และการใช้งาน

(4) การจัดเก็บและการรักษาไว้ รวมถึงการรักษาไว้ให้สามารถอ่านใช้งานได้

(5) การควบคุมการเปลี่ยนแปลง (เช่น การควบคุมเวอร์ชั่น) และ

(6) การจัดเก็บ ระยะเวลาการจัดเก็บ และการทำลาย

สารสนเทศที่มาจากแหล่งภายนอกที่องค์กรกำหนดว่าจำเป็นสำหรับการวางแผนและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องมีการระบุตามความจำเป็น และต้องมีการควบคุม

ข้อ 5 การดำเนินการ (Operation)

5.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational planning and control) องค์กรต้องวางแผน ลงมือปฏิบัติ และควบคุมกระบวนการที่จำเป็นเพื่อให้สอดคล้องกับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และลงมือปฏิบัติตามที่กำหนดไว้ในข้อ 3.1 องค์กรยังต้องลงมือปฏิบัติตามแผนเพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ในข้อ 3.2

องค์กรต้องเก็บรักษาสารสนเทศที่เป็นลายลักษณ์อักษรในระดับที่จำเป็นเพื่อให้มีความมั่นใจว่ากระบวนการเหล่านั้นมีการดำเนินการตามแผน

องค์กรต้องควบคุมการเปลี่ยนแปลงที่มีการวางแผนล่วงหน้า และทบทวนผลของการเปลี่ยนแปลงที่เกิดขึ้นอย่างไม่ได้ตั้งใจ (เช่น การเปลี่ยนแปลงที่ไม่ได้วางแผนไว้และเกิดขึ้นแบบฉุกเฉิน) ดำเนินการเพื่อสดผลในทางลบตามความจำเป็น

องค์กรต้องทำให้มั่นใจว่ากระบวนการที่มีการจ้างหน่วยงานภายนอกดำเนินการมีการระบุและควบคุมการดำเนินการ

5.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment) องค์กรต้องดำเนินการมะเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามกรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มากเสนอขอ

ดำเนินการ หรือเมื่อมีการเปลี่ยนแปลงที่มากขึ้น โดยนำเกณฑ์ความเสี่ยงที่กำหนดไว้ในข้อ 3.1.2 (1) มาพิจารณาด้วย

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร ซึ่งเป็นผลของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

5.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment) องค์กรต้องลงมือปฏิบัติตามแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร ซึ่งเป็นผลของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ข้อ 6 การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)

6.1 การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน (Monitoring, measurement, analysis and evaluation) องค์กรต้องประเมินประสิทธิภาพและประสิทธิผลและความได้ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องกำหนด

(1) อะไรที่จำเป็นต้องเฝ้าระวังและวัดผล ซึ่งรวมถึงกระบวนการและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ

(2) วิธีการในการเฝ้าระวัง วัดผล วิเคราะห์ และประเมินตามที่เหมาะสมเพื่อให้ได้ผลการประเมินที่ถูกต้อง

6.2 การตรวจประเมินภายใน (Internal audit) องค์กรต้องดำเนินการตรวจประเมินภายในตามรอบระยะเวลาที่กำหนดไว้เพื่อให้มีสารสนเทศสำหรับการระบุว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(1) สอดคล้องกับ

1) ความต้องการขององค์กรเองสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ

2) ข้อกำหนดของมาตรฐานฉบับนี้

(2) มีการปฏิบัติและบำรุงรักษาไว้อย่างสัมฤทธิ์ผล องค์กรต้อง

(3) วางแผน กำหนด ลงมือปฏิบัติ และบำรุงรักษาโปรแกรมการตรวจประเมิน ซึ่งรวมถึงความถี่ วิธีการที่ใช้ หน้าที่ความรับผิดชอบ ความต้องการในการตรวจประเมินที่วางแผนไว้ และการรายงานผล โปรแกรมการตรวจประเมินต้องนำความสำคัญของกระบวนการที่เกี่ยวข้องและผลการตรวจประเมินครั้งก่อนมาพิจารณาร่วมด้วย

(4) กำหนดเกณฑ์การตรวจประเมินและขอบเขตของการตรวจประเมินแต่ละครั้ง

(5) เลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินซึ่งเป็นไปตามข้อเท็จจริงและหลักฐานและมีความเป็นกลางของกระบวนการตรวจประเมิน

(6) ทำให้ผลของการตรวจประเมินมีการรายงานไปยังผู้บริหารที่เกี่ยวข้อง และ

(7) จัดเก็บสารสนเทศที่เป็นลายบักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดงโปรแกรมการตรวจประเมินและผลการตรวจประเมิน

6.3 การทบทวนของผู้บริหาร (Management review) ผู้บริหารระดับสูงต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรตามรอบระยะเวลาที่กำหนดไว้เพื่อให้มีความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผล การทบทวนของผู้บริหารต้องรวมการพิจารณาในเรื่อง

(1) สถานะของการดำเนินการจากผลการทบทวนครั้งก่อน

(2) การเปลี่ยนแปลงในประเด็นภายในและภายนอกองค์กรที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(3) ผลตอบกลับของประสิทธิภาพและประสิทธิผลด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงแนวโน้มในเรื่อง

1) ความไม่สอดคล้องและการดำเนินการแก้ไข

2) ผลการเฝ้าระวังและวัดผล

3) ผลการตรวจประเมิน และ

4) ความสำเร็จตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

(4) ผลตอบกลับจากผู้ที่เกี่ยวข้อง

(5) ผลการประเมินความเสี่ยงและสถานะของแผนการจัดการความเสี่ยง และ

(6) โอกาสสำหรับการปรับปรุงอย่างต่อเนื่อง

ผลการทบทวนของผู้บริหารต้องรวมการตัดสินใจเกี่ยวกับโอกาสในการปรับปรุงอย่างต่อเนื่องและความจำเป็นสำหรับการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดงผลการทบทวนของผู้บริหาร

ข้อ 7 การปรับปรุง (Improvement)

7.1 ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and corrective action) เมื่อความไม่สอดคล้องหนึ่งเกิดขึ้น องค์กรต้อง

(1) ตอบกลับต่อความไม่สอดคล้องนั้นตามความเหมาะสม และ

1) ดำเนินการเพื่อควบคุมและแก้ไขความไม่สอดคล้อง และ

2) จัดการกับผลที่เกิดขึ้น

(2) ประเมินความจำเป็นสำหรับการดำเนินการเพื่อขจัดสาเหตุของความไม่สอดคล้องเพื่อให้ไม่เกิดขึ้นซ้ำหรือไม่เกิดขึ้นในที่อื่นโดย

1) การทบทวนความไม่สอดคล้อง

2) การระบุสาเหตุของความไม่สอดคล้อง และ

3) การระบุว่าความไม่สอดคล้องที่คล้ายกันมีหรือไม่ หรืออาจเป็นไปได้ที่จะเกิดขึ้น

(3) ดำเนินการแก้ไขที่จำเป็น

(4) ทบทวนความสัมฤทธิ์ผลของการดำเนินการแก้ไขที่ได้ดำเนินการไป และ

(5) ทำการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ถ้าจำเป็นการดำเนินการแก้ไขต้องเหมาะสมต่อผลของความไม่สอดคล้องที่พบ

องค์กรต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐานแสดง

(6) สภาพของความไม่สอดคล้องและการดำเนินการใด ๆ ที่ได้ดำเนินการไป และ

(7) ผลของการดำเนินการแก้ไข

7.2 การปรับปรุงอย่างต่อเนื่อง (Continual Improvement) องค์กรต้องปรับปรุงความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

1.5 สำนักงานจังหวัด (Governor's Office)

สำนักงานจังหวัดเป็นหน่วยงานบริหารราชการส่วนภูมิภาค ดำเนินการเป็นศูนย์กลาง ในการบริหารงานของผู้ว่าราชการจังหวัด เช่นเดียวกับสำนักงานปลัดกระทรวง

มหาดไทย ซึ่งเป็นศูนย์กลางของการบริหารราชการของกระทรวงมหาดไทยในส่วนกลางสำนักงานจังหวัด เป็นหน่วยงานที่ปรากฏชื่อเป็นครั้งแรกในพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. 2495 ซึ่งตามมาตรา 38 ของพระราชบัญญัติดังกล่าว กำหนดไว้ว่า “ให้แบ่งส่วนราชการของจังหวัดดังนี้ สำนักงานจังหวัด มีหน้าที่เกี่ยวกับราชการทั่วไปของจังหวัดนั้น มีผู้ว่าราชการจังหวัดเป็น ผู้ปกครองบังคับบัญชาและรับผิดชอบส่วนต่าง ๆ ซึ่งกระทรวง ทบวง กรม ได้ตั้งขึ้น มีหน้าที่เกี่ยวกับราชการของกระทรวง ทบวง กรม นั้น ๆ มีหัวหน้าส่วนราชการประจำจังหวัดนั้น ๆ เป็นผู้ปกครองบังคับบัญชาและรับผิดชอบ” โดยมีอำนาจหน้าที่ ดังนี้

1) แปลงยุทธศาสตร์การพัฒนาระดับชาติไปเป็นยุทธศาสตร์การพัฒนาจังหวัดในพื้นที่

2) พัฒนาระบบข้อมูลสารสนเทศเพื่อการบริหาร ระบบสารสนเทศภูมิศาสตร์เพื่อการวางแผน และเครือข่ายสารสนเทศของจังหวัด โดยเป็นศูนย์สารสนเทศของจังหวัด เพื่อการบริหารและวางแผนพัฒนาจังหวัด

3) จัดทำแผนพัฒนาจังหวัด ดำเนินการตามแผน กำกับและติดตามผลการดำเนินงานตามยุทธศาสตร์ นโยบาย และแผนพัฒนาจังหวัด รวมทั้งประสานการจัดทำแผนพัฒนากลุ่มจังหวัด

4) จัดทำแผนปฏิบัติราชการประจำปีของจังหวัดหรือคำของบประมาณของจังหวัด และประสานการจัดทำแผนปฏิบัติราชการประจำปีของกลุ่มจังหวัดหรือคำของบประมาณของกลุ่มจังหวัด

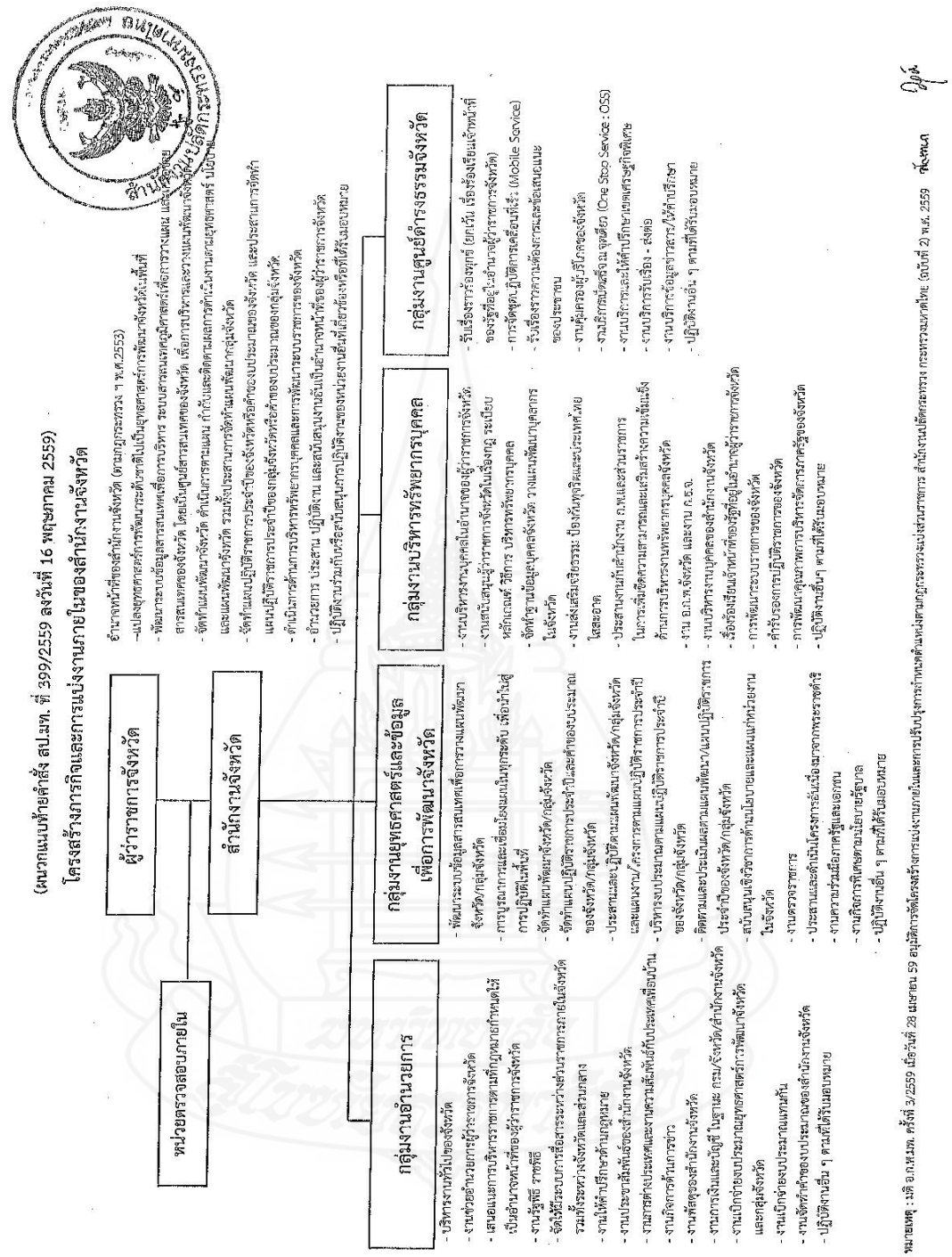
5) ดำเนินการด้านการบริหารทรัพยากรบุคคลและการพัฒนาระบบราชการของจังหวัด

6) อำนวยการ ประสาน ปฏิบัติงาน และสนับสนุนงานอันเป็นอำนาจหน้าที่ของผู้ว่าราชการจังหวัด

7) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นทีเกี่ยวข้อง

โดยแบ่งการบริหารออกเป็น 4 กลุ่ม ดังนี้

1) กลุ่มงานอำนวยการ
2) กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
3) กลุ่มงานบริหารทรัพยากรบุคคล
4) กลุ่มงานศูนย์ดำรงธรรมจังหวัด



ภาพที่ 2.7 การแบ่งส่วนราชการสำนักงานปลัดกระทรวงมหาดไทย พ.ศ. 2559

ที่มา: http://www.moi.go.th

2. งานวิจัยที่เกี่ยวข้อง

วีระวัฒน์ จิรัญดร (2556) ได้ศึกษาเรื่อง การยอมรับกรอบมาตรฐาน ISO/IEC 27001 เพื่อการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศของมหาวิทยาลัยเอกชนในกรุงเทพมหานครและปริมณฑล โดยมีวัตถุประสงค์เพื่อศึกษาการยอมรับกรอบมาตรฐาน ISO/IEC 27001 และปัจจัยที่มีอิทธิพลต่อการยอมรับกรอบมาตรฐาน ISO/IEC 27001 เพื่อการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศของมหาวิทยาลัยเอกชนในกรุงเทพมหานครและปริมณฑล โดยใช้ตัวแบบการยอมรับเทคโนโลยี (TAM) เป็นกรอบแนวคิดในการวิจัย กลุ่มตัวอย่างคือผู้ที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัยเอกชนในกรุงเทพมหานครและปริมณฑล จำนวน 57 คน จากมหาวิทยาลัย 19 แห่ง โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูล ได้รับแบบสอบถามกลับคืนร้อยละ 80.70 ผลการวิจัยพบว่า ผู้ตอบแบบสอบถามส่วนใหญ่มีระดับการยอมรับกรอบมาตรฐาน ISO/IEC 27001 โดยรวมอยู่ในระดับมาก (3.92, 0.33) การรับรู้ประโยชน์อยู่ในระดับมาก (4.11, 0.47) ความง่ายต่อการใช้อยู่ในระดับปานกลาง (3.41, 0.45) ทัศนคติที่มีต่อการใช้อยู่ในระดับมาก (4.07, 0.31) ความตั้งใจที่จะใช้อยู่ในระดับมาก (3.96, 0.426) จากการทดสอบสมมติฐานด้วยสถิติอ้างอิง Multiple Regression พบว่ามีปัจจัยทั้งสิ้น 38 ปัจจัย คือ กลุ่มปัจจัยความง่ายต่อการใช้กรอบมาตรฐาน ISO/IEC 27001 จำนวน 10 ปัจจัย กลุ่มปัจจัยจ่ายต่อการใช้กรอบมาตรฐาน ISO/IEC 27001 จำนวน 7 ปัจจัย กลุ่มปัจจัยทัศนคติที่มีต่อการใช้กรอบมาตรฐาน ISOIEC 27001 จำนวน 10 ปัจจัย กลุ่มปัจจัยทัศนคติที่มีต่อการใช้กรอบมาตรฐาน ISO/IEC 27001 จำนวน 11 ปัจจัย เป็นปัจจัยที่มีอิทธิพลระดับสูงมากต่อการยอมรับกรอบมาตรฐาน ISO/IEC 27001 เมื่อพยากรณ์โดยเพศของผู้ตอบแบบสอบถาม, ระดับการศึกษา, ตำแหน่งงาน, ระยะเวลาทำงานในองค์กร และการรู้เกี่ยวกับมาตรฐาน ISO/IEC 27001 ได้สมการแสดงระดับอิทธิพล จำนวน 5 สมการ

พลสิริ วรรณวิโรจน์ (2556) ได้ศึกษาระดับอิทธิพลของมาตรการการจัดการความมั่นคงปลอดภัยตามกรอบมาตรฐาน ISO/IEC 27001 ต่อการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ บริษัท วี จี ไอ โกลบอล มีเดีย จำกัด (มหาชน) โดยการวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาระดับอิทธิพลของมาตรการการจัดการความมั่นคงปลอดภัยตามกรอบมาตรฐาน ISO/IEC 27001 ต่อการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ บริษัท วี จี ไอ โกลบอล มีเดีย จำกัด (มหาชน) 2) เขียนแผนปฏิบัติการรองรับความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ บริษัท วี จี ไอ โกลบอล มีเดีย จำกัด (มหาชน) ตาม

กรอบมาตรฐาน ISO/IEC 27001 ตามระดับอิทธิพลในข้อ 1 วิธีดำเนินการวิจัยเป็นเชิงสำรวจ โดยใช้แบบสอบถามในการเก็บข้อมูลจากผู้บริหารและพนักงานบริษัท วี จี ไอ โกลบอล มีเดีย จำกัด (มหาชน) จำนวน 430 คน และวิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนานาคือ ค่าร้อยละ ค่าเฉลี่ยเลขคณิต และส่วนเบี่ยงเบนมาตรฐาน และสถิติทดสอบสมมติฐานคือ การวิเคราะห์ถดถอยพหุ (Multiple Regression) ผลการวิจัยพบว่าผู้บริหารและพนักงานส่วนใหญ่มีความคิดเห็นว่า มาตรการการจัดการความมั่นคลปลอดภัยตามกรอบมาตรฐาน ISO/IEC 27001 ทั้ง 10 มาตรการ มีอิทธิพลต่อการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท วี จี ไอ โกลบอล มีเดีย จำกัด (มหาชน) ในระดับมาก และมาตรการการจัดการความมั่นคงปลอดภัยตามกรอบมาตรฐาน ISO/IEC 27001 ทั้ง 30 ด้าน มีอิทธิพลต่อการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท วี จี ไอ โกลบอล มีเดีย จำหัด (มหาชน) เมื่อพญากรณ์โดยเพศ ระดับการศึกษา ตำแหน่งการทำงาน และประสบการณ์ทำงาน อย่างมีนัยสำคัญทางสถิติที่ระดับ .05

สุพรรณี ชาติสุข (2556) ได้วิเคราะห์และประเมินความเสี่ยงด้วยมาตรฐาน ISO/IEC 27001 เพื่อบริหารจัดการระบบเทคโนโลยีสารสนเทศภายในองค์กร กรณีศึกษาศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค โดยมีวัตถุประสงค์ เพื่อต้องการตรวจสอบช่องโหว่/จุดอ่อนของระบบเทคโนโลยีสารสนเทศและต้องการให้ทราบถึงระดับความเสี่ยง/ภัยคุกคาม เพื่อนำมาพัฒนาปรับปรุงร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยนำผลการวิเคราะห์และประเมินความเสี่ยงในครั้งนี้ ซึ่งมีทั้งก่อนดำเนินโครงการและหลังดำเนินโครงการ มาใช้กำหนดกลยุทธ์และแนวทางในการบริหารจัดการศูนย์เทคโนลีสารสนเทศขององค์กรด้านต่าง ๆ เช่น กรณีผลการวิเคราะห์และประเมินความเสี่ยงก่อนการดำเนินโครงการ ได้นำมาพัฒนาปรับปรุงร่างนโยบายความมั่นคงปลอดภัยและปรับปรุงระบบเครือข่ายให้มีความปลอดภัยมากยิ่งขึ้น ส่วนกรณีผลการวิเคราะห์และประเมินความเสี่ยงหลังจากดำเนินโครงการ นำมาประยุกต์ใช้ เพื่อหาแนวทางบริหารความเสี่ยงที่เหมาะสม จัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร เป็นต้น การจัดทำโครงการดังกล่าว ในครั้งนี้เป็นจุดเริ่มต้นของการตรวจสอบความปลอดภัยของระบบสารสนเทศ เพื่อนำจุดอ่อน มาวางแผน พัฒนาและปรับปรุงระบบให้มีประสิทธิภาพ ให้รองรับการเข้าสู่การให้บริการในการระดับสากลมาตรฐาน ISO/IEC 27001 และสามารถให้องค์กรนำมาใช้เป็นเครื่องมือและกลไกสนับสนุนการดำเนินงานให้สอดคล้องกับภารกิจหลักขององค์กรเพื่อมุ่งสู่ความเป็นเลิศในการบริการประชาชน ทั้งเป็นการเตรียมความพร้อมในด้าน ICT รองรับการเข้าสู่ประชาคมอาเซียน ซึ่งมีเป้าหมายในการพัฒนาและปรับปรุงระบบมีโครงการต่าง ๆ ดังนี้ คือ โครงการจัดทำแผนแม่บทเทคโนโลยี

สารสนเทศและการสื่อสาร ฉบับที่ 2 ปี 2557 – 2560 โครงการจัดทำแผนปฏิบัติราชการ 4 ปี (ด้านเทคโนโลยีสารสนเทศ) โครงการพัฒนาปรับปรุงการจัดทำนโยบายเพื่อความมั่นคงปลอดภัยสารสนเทศและโครงการจัดทำแผนบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

กรกฎ สราญสุทธิ์ (2556) ได้พัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO27001 ของกรมทรัพยากรน้ำบาดาล พร้อมประเมินความเสี่ยงและจัดทำรายงานผลกระทบรายงานวิธีการจัดการกับความเสี่ยง โดยดำเนินการศึกษาข้อมูลด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล วิเคราะห์และประเมินความเสี่ยงระบบความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศของศูนย์ข้อมูล ในการวิเคราะห์ความเสี่ยงนั้นได้ระบุรายการความเสี่ยง ระดับความเสี่ยงแยกเป็นรายอุปกรณ์พร้อมกับการกำหนดรายการควบคุมตามมาตรฐาน ISO27001 ผลการวิเคราะห์ความเสี่ยงก่อนการดำเนินการพบว่าส่วนใหญ่อยู่ในระดับกลางและต่ำ จากนั้นดำเนินการจัดการความเสี่ยง โดยจัดทำนโยบายด้านความมั่นคงปลอดภัยมาตรฐาน ISO27001 ให้กรม ประกอบด้วย นโยบายการควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน นโยบายการเข้าถึงระบบปฏิบัติการ แนวปฏิบัติการจัดทาระบบสารองและแผนเตรียมความพร้อมกรณีฉุกเฉิน แนวปฏิบัติการประเมินความเสี่ยง แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ จากนั้นปรับปรุงระบบระบบเทคโนโลยีสารสนเทศเพื่อลดช่องโหว่ทั้งฮาร์ดแวร์และซอฟต์แวร์ และอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยให้ผู้ใช้งาน สุดท้ายดำเนินการประเมินทบทวน วิเคราะห์ความเสี่ยงหลังจากดำเนินการ พบว่าหน่วยงานมีความเสี่ยงระดับกลางลดลง และความเสี่ยงที่เหลืออยู่ส่วนใหญ่เป็นความเสี่ยงในระดับต่ำ ซึ่งผู้จัดทำได้มีข้อเสนอแนะให้ตรวจสอบ ทบทวน และปรับปรุงระบบอยู่เสมอ เพื่อลดความเสี่ยง ช่องโหว่ และโอกาสที่จะถูกโจมตีต่อภัยคุกคามต่าง ๆ

ประกิจ อินทรักษ์ (2556) พัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001:2005 กรณีศึกษาสำหรับ สถาบันวิจัยแห่งหนึ่ง เพื่อใช้เป็นแนวทางในการปฏิบัติงาน รวมถึงการวิเคราะห์ และการประเมินความเสี่ยงให้กับองค์กร เพื่อให้องค์กรได้ทราบถึงระดับของความเสี่ยงที่องค์กรมีอยู่ และจัดทำแผนการบริหารจัดการความเสี่ยงลดระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ มีแนวทางดำเนินงานคือ การกำหนดขอบเขตในการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยแบ่งทรัพย์สินขององค์กรเป็น 5 ประเภท คือ ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล คน และงานบริการ จากนั้นกำหนดวิธีวิเคราะห์ประเมินความเสี่ยงตามรายการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Control Checklist) ของ ISO/IEC27001:2005 และกำหนด

นโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร ได้แก่ นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต นโยบายความมั่นคงปลอดภัยของอีเมล์ นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ นโยบายการบริหารจัดการทรัพย์สิน นโยบายด้านการปฏิบัติตามกฎหายและข้อบังคับนโยบายด้านความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย พร้อมจัดทำเอกสาร SOA (Statement Of Applicability) และตรวจสอบผลการดำเนินงาน พบว่ามีสามารถขจัดระดับความเสี่ยงสูงได้หมด ระดับความเสี่ยงปานกลางลดลง เหลือระดับความเสี่ยงต่ำซึ่งอยู่สภาพที่องค์กรรับได้

ไพศาล จันทร์เลื่อน (2557) ได้พัฒนาความความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO 27001 กรณีศึกษา ศูนย์พัฒนาและบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพระนคร เพื่อลดความเสี่ยงที่จะเกิดขึ้นกับหน่วยงาน โดยการกำหนดขอบเขตระบบเทคโนโลยีสารสนเทศที่จะดำเนินการ และวิเคราะห์ความเสี่ยงก่อนดำเนินการ จากนั้นกำหนดมาตการควบคุมความเสี่ยง และจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยการจัดทำเอกสาร Statement of Applicability (SOA) ประกอบด้วย นโยบาย 8 ด้าน ได้แก่ นโยบายความมั่นคงปลอดภัยสารสนเทศที่กำหนดให้ต้องมีการทบทวนทุก ๆ ปี นโยบายโครงสร้างความมั่นคงปลอดภัยสารสนเทศ ที่กำหนดถึงหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง นโยบายการบริหารจัดการทรัพย์สิน กำหนดผู้ดูแลทรัพย์สิน นโยบายการควบคุมการเข้าถึง นโยบายความมั่นคงปลอดภัยทางสภาพแวดล้อม นโยบายการใช้งานเครื่องคอมพิวเตอร์ และนโยบายการใช้งานระบบเครือข่ายไร้สาย จากนั้น ได้ดำเนินการะการอบรมเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ จากนั้น ประเมินความเสี่ยงหลังดำเนินงานและนำผลที่ได้เสนอผู้บริหาร เพื่อพิจารณาตรวจสอบ ซึ่งจากการประเมินความเสี่ยงพบว่า ความเสี่ยงสูงได้รับการจัดการ เหลือเพียงความเสี่ยงสูงเรื่องของซอฟต์แวร์ผิดกฎหมายเท่านั้น ในส่วนของมาตรการควบคุมก็ยังไม่สามารถดำเนินการใช้ทั้งหมดตามที่เลือกในเอกสาร SOA เนื่องด้วยเวลาอันกำจัดของการดำเนินงาน

จุติชัย ทองกระจาย (2557) ได้พัฒนาระบบตรวจจับการบุกรุกเครือข่ายกรณีศึกษา บริษัท เวนด้า ซอฟแวร์ ดีเวลอปเมนท์ จำกัด เพื่อตรวจจับภัยคุกคามที่เกิดขึ้นต่อระบบเครือข่ายของบริษัท และปรับปรุงระบบเครือข่ายของบริษัทให้มีความมั่นคงปลอดภัย โดยทำการเก็บข้อมูลจากระบบเครือข่ายที่ได้พัฒนาขึ้น ตรวจจับภัยคุกคาม ปรับปรุงซิกเนเจอร์ของระบบ และแสดงผลรายงานผ่านเว็บแอพพลิเคชัน ผลจากการดำเนินงานพบว่า ระบบที่พัฒนาขึ้นสามารถตรวจจับการบุกรุกและการโจมตีบนเครือข่ายได้จริง ผู้ดูแลระบบสามารถนำไปใช้เฝ้าดูสถานการณ์ที่เกิดขึ้นบน

ระบบเครือข่ายได้อย่างทันท่วงที และสามารถนำผลจากการตรวจจับไปใช้ในการปรับปรุงไฟร์วอลล์และระบบเครือข่ายของบริษัท เพื่อเพิ่มความมั่นคงปลอดภัยด้านเครือข่ายของบริษัทให้มากยิ่งขึ้น

อัจฉรา เวียงสิมา (2559) ได้ทบทวนและพัฒนานโยบายการบริหารจัดการความมั่นคงของระบบสารสนเทศภายใต้มาตรฐาน ISO/IEC 27001:2013 เพื่อทบทวนและการพัฒนานโยบายการบริหารจัดการความมั่นคงของระบบสารสนเทศของบริษัท ที-เน็ต จำกัด ให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 ที่ได้ปรับปรุงให้เป็นไปตามมาตรฐานสากล และเพื่อปรับปรุงนโยบายการบริหารจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ รวมถึงให้องค์กรมีมาตรฐานและการพัฒนากระบวนการบริหารจัดการความมั่นคงทางสารสนเทศ ให้เป็นไปตามแนวทางขององค์กร โดยนำกระบวนการดังกล่าวมาพัฒนาและประยุกต์ใช้ในการดำเนินของแต่ละส่วนงาน ให้มีการปฏิบัติเป็นไปตามข้อกำหนดที่ได้กำหนดไว้ ประกอบกับส่งเสริมบุคลากรภายในองค์กรให้มีความพร้อมและปฏิบัติหน้าที่ไปในทิศทางเดียวกัน

ธนวรรธน์ ว่องพิบูลย์ (2559) ทำการศึกษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงภายใต้มาตรฐาน ISO/IEC 27001:2013 ของ บริษัท แปซิฟิค เฮลธ์แคร์ (ไทยแลนด์) จำกัด จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อจัดทำร่างนโยบายความปลอดภัยทางเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงาน รวมถึงการวิเคราะห์และประเมินความเสี่ยง (Risk Management) ซึ่งจะช่วยลดผลกระทบและสามารถบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และเป็นการเพิ่มประสิทธิภาพในการทำงานของระบบเทคโนโลยีสารสนเทศภายในองค์กรให้มีมาตรฐานเพิ่มมากขึ้น

ณัทรัฏฐ์ มณีรัสยากร (2559) ทำการศึกษาและพัฒนานโยบายด้านความปลอดภัยภายใต้มาตรฐาน ISO27001 ของ บริษัท เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น จำกัด จัดทำขึ้นโดยมีวัตถุประสงค์ในการปรับปรุงพัฒนานโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้แก่องค์กรเพื่อใช้แนวทางสร้างความมั่นคงปลอดภัยและยกระดับระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยเป็นมาตรฐานสากลโดยมี มาตรฐาน ISO/IEC 27001: 2013 เป็นเครื่องมือในการพัฒนาเพื่อให้องค์กรดำเนินงานได้อย่างมีประสิทธิภาพ

จากการศึกษาทฤษฎี แนวคิด และงานวิจัยที่เกี่ยวข้องนั้น ผู้จัดทำจึงมีแนวคิดในการพัฒนาระบบจัดการความมั่นคงปลอดภัยด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามกรอบมาตรฐาน ISO/IEC 27001:2013 สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ขึ้น เพื่อใช้เป็นเครื่องมือและเป็นแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ และช่วยยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงานของรัฐให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงการดำเนินงานตามกรอบมาตรฐานสากล ISO/IEC 2001 และยังช่วยให้หน่วยงานสามารถลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจจะทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นงปลอดภัยถูกคุกคาม ตลอดจนช่วยให้สามารถฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว

บทที่ 3

วิธีดำเนินการวิจัย

สำหรับงานวิจัยในครั้งนี้ ผู้วิจัยมีแนวคิดที่จะพัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย โดยการวิจัยเดินการตามลำดับดังต่อไปนี้

1. ประชากรและกลุ่มตัวอย่าง

ขอบเขตของสินทรัพย์ที่ครอบคลุมในการประเมินความเสี่ยงในครั้งนี้ ประกอบด้วยสินทรัพย์ด้านสารสนเทศหลักของสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย โดยแบ่งกลุ่มของสินทรัพย์ตามแผนกและลักษณะงานได้ดังนี้

1.1 สินทรัพย์เกี่ยวกับงานระบบบริหารการเงินการคลังภาครัฐ (GFMIS) กลุ่มงานอำนวยการ

1.2 สินทรัพย์เกี่ยวกับงานระบบติดตามประเมินผลแผนงาน (Padme) กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด

1.3 สินทรัพย์เกี่ยวกับงานระบบสารสนเทศทรัพยากรบุคคลระดับจังหวัด (PPIS) กลุ่มงานบริหารทรัพยากรบุคคล

1.4 สินทรัพย์เกี่ยวกับงานระบบร้องเรียน ร้องทุกข์ ศูนย์ดำรงธรรมจังหวัด กลุ่มงานศูนย์ดำรงธรรมจังหวัด

2. ขั้นตอนการวิจัย

2.1 จัดทำทะเบียนสินทรัพย์และกำหนดค่าของสินทรัพย์ (Asset Identification and Valuation)

2.1.1 กำหนดแผนการประเมินความเสี่ยงต้องอย่างน้อยปีละ 1 ครั้ง และประเมินความเสี่ยงเพิ่มเติมในกรณีที่มีการเปลี่ยนแปลงสำคัญที่เกิดขึ้นกับสารสนเทศโดยการเปลี่ยนแปลงที่สำคัญที่ต้องนำมาพิจารณามีดังต่อไปนี้

2.1.1.1 การเปลี่ยนแปลงนโยบาย วัตถุประสงค์ หรือกระบวนการปฏิบัติงาน

2.1.1.2 การเปลี่ยนแปลงที่เกิดขึ้นกับผลิตภัณฑ์ เทคนิค เทคโนโลยี หรือกระบวนการ เพื่อเพิ่มความมีประสิทธิภาพและประสิทธิผลของวิธีการบริหาร และควบคุมความเสี่ยงสารสนเทศของหน่วยงาน

2.1.1.3 การมีภัยคุกคามใหม่เกิดขึ้น หรือการที่ภัยคุกคามมีความร้ายแรงมากขึ้น หรือการค้นพบจุดอ่อนใหม่ที่ไม่ได้มีการแจ้งเตือนมาก่อน

2.1.1.4 การเปลี่ยนแปลงจากปัจจัยภายนอก เช่น การเปลี่ยนกฎหมาย กฎระเบียบและข้อบังคับในสัญญาที่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน

2.1.2 จัดทำเกณฑ์ (Criteria) สำหรับการประเมินค่าของสินทรัพย์ (ซึ่งต้องได้รับความเห็นชอบจากหัวหน้าส่วนราชการ) โดยวัดจากระดับความเสียหายที่เกิดขึ้นกับความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งได้แก่ การสูญเสียความลับ (Loss of Confidentiality) การสูญเสียความถูกต้องครบถ้วน (Loss of Integrity) และการสูญเสียสภาพความพร้อมใช้งาน (Loss of Availability) โดยในแต่ละมิติสามารถจัดแบ่งประเภทความเสียหายได้ดังตัวอย่างต่อไปนี้

2.1.2.1 ทำให้องค์กรไม่สามารถปฏิบัติงานตามปกติได้ (Disruption of Service)

2.1.2.2 ทำให้องค์กรเสียชื่อเสียงและความเชื่อมั่น (Loss of Creditability)

2.1.2.3 ทำให้องค์กรละเมิดกฎหมาย ระเบียบข้อบังคับ และสัญญา (Violation of Law, Regulation and Contract)

2.1.2.4 ทำให้องค์กรมีความเสียหายเป็นจำนวนเงิน (Financial Loss)

2.1.2.5 ทำให้เกิดอันตรายต่อบุคลากรและผู้ใช้งานในองค์กร (Endangerment of Personal Safety)

2.1.3 ทำทะเบียนสินทรัพย์โดยกรอกข้อมูลลงในทะเบียนสินทรัพย์ แยกตามประเภทของสินทรัพย์ โดยเริ่มจากสินทรัพย์หลักและสินทรัพย์ประกอบตามลำดับ ซึ่งมีข้อมูลสินทรัพย์ในแต่ละประเภทที่ต้องระบุดังนี้

2.1.3.1 ระบุชื่อสินทรัพย์ ชื่อกระบวนการ ชื่อบุคลากร

2.1.3.2 ระบุรายละเอียดของสินทรัพย์ กระบวนการ/บุคลากร

2.1.3.3 ระบุชื่อผู้ดูแลสินทรัพย์ ผู้รับผิดชอบ ผู้บังคับบัญชา

2.1.3.4 ระบุรายละเอียดของกฎหมาย ระเบียบข้อบังคับ และสัญญาที่เกี่ยวข้องกับสินทรัพย์

2.1.3.5 ข้อมูลอื่น ๆ ที่เกี่ยวข้องกับสินทรัพย์

2.1.4 ประเมิน “ค่าของสินทรัพย์แยกตามประเภทความเสียหาย” โดยระบุค่าของสินทรัพย์แยกตามประเภท (CIA Value) โดยพิจารณาแยกตามแต่ละมิติซึ่งประกอบด้วย Confidentiality (C) Integrity (I) และ Availability (A) ตามประเภท และเกณฑ์ที่กำหนดไว้โดยใช้ค่าของสินทรัพย์ที่มีค่าสูงสุดในแต่ละประเภทความเสียหายมาเป็นค่าของสินทรัพย์ในแต่ละมิติ ดังนี้

ตารางที่ 3.1 ค่าของสินทรัพย์

ประเด็นในการพิจารณาความเสียหาย	**ค่าของสินทรัพย์/ระดับคะแนน**				
	สูงมาก = 5	**สูง = 4**	**ปานกลาง = 3**	**ต่ำ = 2**	**ต่ำมาก = 1**
ทำให้องค์กรไม่สามารถปฏิบัติงานตามปกติได้ (Disruption of services : DS)	มีผลให้สำนักงานจังหวัดต้องหยุดการปฏิบัติภารกิจมากกว่า 8 ชั่วโมง	มีผลให้สำนักงานจังหวัดต้องหยุดการปฏิบัติภารกิจไม่เกิน 8 ชั่วโมง	มีผลให้สำนักงานจังหวัดต้องหยุดการปฏิบัติภารกิจไม่เกิน 4 ชั่วโมง	มีผลให้สำนักงานจังหวัดปฏิบัติภารกิจไม่สะดวก	มีผลให้สำนักงานจังหวัดปฏิบัติภารกิจไม่ได้เลย

ตารางที่ 3.1 (ต่อ)

ประเด็นในการพิจารณาความเสียหาย	ค่าของสินทรัพย์/ระดับคะแนน				
	สูงมาก = 5	**สูง = 4**	**ปานกลาง = 3**	**ต่ำ = 2**	**ต่ำมาก = 1**
ทำให้องค์กรเสียชื่อเสียงและความเชื่อมั่น (Loss of Creditability: LC)	กระทบกับภาพลักษณ์ขององค์กร ทำให้เกิดความไม่เชื่อมั่นในการทำงานของสำนักงานจังหวัด	กระทบกับภาพลักษณ์ของสำนักงานจังหวัด ทำให้เกิดความไม่เชื่อมั่นในการปฏิบัติงานของพนักงานและเจ้าหน้าที่	กระทบกับภาพลักษณ์ของหน่วยงานย่อยในสำนักงานจังหวัด	กระทบกับภาพลักษณ์ของสำนักงานจังหวัดเล็กน้อย ไม่เป็นข่าวในสื่อ	กระทบภาพลักษณ์ของสำนักงานจังหวัดน้อยมาก
ทำให้องค์กรละเมิดกฎหมาย ระเบียบข้อบังคับและสัญญา (Violation Of Law, Regulation and Contract : VL)	ส่งผลให้ ต้องรับผิดชอบตามกฎหมาย ระเบียบข้อบังคับและสัญญา	ส่งผลให้ผู้บริหารระดับสูงรับผิดชอบตามกฎหมาย ระเบียบข้อบังคับ ระเบียบและสัญญา	ส่งผลให้เจ้าหน้าที่ที่เกี่ยวข้องต้องรับผิดชอบตามกฎหมาย ระเบียบข้อบังคับ ระเบียบและสัญญา	ส่งผลให้เจ้าหน้าที่ที่เกี่ยวข้องได้รับการตักเตือนหรือมีโทษทางวินัยเล็กน้อย	ส่งผลให้เจ้าหน้าที่ที่เกี่ยวข้องได้รับการตักเตือน

ตารางที่ 3.1 (ต่อ)

ประเด็นในการพิจารณาความเสียหาย	ค่าของสินทรัพย์/ระดับคะแนน				
	สูงมาก = 5	**สูง = 4**	**ปานกลาง = 3**	**ต่ำ = 2**	**ต่ำมาก = 1**
ทำให้องค์กรมีความเสียหายเป็นจำนวนเงิน (Financial Loss : FL)	มากกว่า 10 ล้านบาท	มากกว่า 5 ล้านบาท แต่ไม่เกิน 10 ล้านบาท	มากกว่า 1 ล้านบาท แต่ไม่เกิน 5 ล้านบาท	น้อยกว่า 1 ล้านบาท	น้อยกว่า 5 แสนบาท
ทำให้เกิดอันตรายต่อบุคลากรและผู้ใช้งานในองค์กร (Endangerment Of Personal Safety : ES)	มีผู้เสียชีวิต 1 คนขึ้นไป	บาดเจ็บสาหัสจนทำให้พิการหรือทุพลภาพ	บาดเจ็บสาหัสหรือทรัพย์สินบุคลากรเสียหาย	บาดเจ็บเล็กน้อย	ไม่บาดเจ็บ

2.2 กำหนดภัยคุกคามต่อสินทรัพย์ (Threat Identification)

2.2.1 จัดทำรายงานภัยคุกคาม (Threat List) ที่สามารถเกิดขึ้นกับสินทรัพย์ทั้งหมด โดยใช้ข้อมูลจากภัยคุกคามที่เคยเกิดขึ้นในอดีต และแหล่งข้อมูลที่น่าเชื่อถือ ทั้งนี้ ภัยคุกคามที่นำมาพิจารณาสามารถแยกได้ดังนี้

ตารางที่ 3.2 รายการภัยคุกคามและมติด้าน CIA

รายการภัยคุกคามและมติด้าน CIA

	Threat	**Basic Parameter**
T 0.01	เพลิงไหม้ (Fire)	I,A
T 0.02	สภาพภูมิอากาศไม่เอื้ออำนวย (Unfavorable climatic conditions)	I,A

ตารางที่ 3.2 (ต่อ)

	Threat	Basic Parameter
T 0.03	น้ำ (Water)	I,A
T 0.04	มลพิษฝุ่นละอองการกัดกร่อน (Pollution, dust, corrosion)	I,A
T 0.05	ภัยพิบัติทางธรรมชาติ (Natural disasters)	A
T 0.06	ภัยพิบัติทางสิ่งแวดล้อม (Environmental disasters)	A
T 0.07	เหตุการณ์สำคัญในสิ่งแวดล้อม (Major events in the environment)	C,I,A
T 0.08	ความล้มเหลวหรือการหยุดชะงักของแหล่งจ่ายไฟ (Failure or disruption of the power supply)	I,A
T 0.09	ความล้มเหลวหรือการหยุดชะงักของเครือข่ายการสื่อสาร (Failure or disruption of communication networks)	I,A
T 0.10	ความล้มเหลวหรือการหยุดชะงักของแหล่งจ่ายไฟ (Failure or disruption of mains supply)	A
T 0.11	ความล้มเหลวหรือการหยุดชะงักของผู้ให้บริการ (Failure or disruption of service providers)	C,I,A
T 0.12	รังสีรบกวน (Interfering radiation)	I,A
T 0.13	การขัดขวางการปล่อยมลพิษ (Intercepting compromising emissions)	C
T 0.14	การสกัดกั้นข้อมูล / การจารกรรม (Interception of information / espionage)	C
T 0.15	แอบฟัง (Eavesdropping)	C
T 0.16	การโจรกรรมอุปกรณ์สื่อเก็บข้อมูลและเอกสาร (Theft of devices, storage media and documents)	C,A
T 0.17	การสูญเสียอุปกรณ์สื่อเก็บข้อมูลและเอกสาร (Loss of devices, storage media and documents)	C,A
T 0.18	การวางแผนที่ไม่ดีหรือการปรับตัว (Bad planning or lack of adaptation)	C,I,A
T 0.19	การเปิดเผยข้อมูลที่สำคัญ (Disclosure of sensitive information)	C
T 0.20	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	C,I,A
T 0.21	การจัดการฮาร์ดแวร์และซอฟต์แวร์ (Manipulation of hardware and software)	C,I,A
T 0.22	การจัดการข้อมูล (Manipulation of information)	I

ตารางที่ 3.2 (ต่อ)

	Threat	Basic Parameter
T 0.23	การเข้าถึงระบบไอทีโดยไม่ได้รับอนุญาต (Unauthorized access to IT systems)	C,I
T 0.24	การทำลายอุปกรณ์หรือสื่อเก็บข้อมูล (Destruction of devices or storage media)	A
T 0.25	ความล้มเหลวของอุปกรณ์หรือระบบ (Failure of devices or systems)	A
T 0.26	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or systems)	C,I,A
T 0.27	ขาดแคลนทรัพยากร (Lack of resources)	A
T 0.28	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors	C,I,A
T 0.29	การละเมิดกฎหมายหรือข้อบังคับ (Violation of laws or regulations)	C,I,A
T 0.30	การใช้หรือการจัดการอุปกรณ์และระบบโดยไม่ได้รับอนุญาต (Unauthorized use or administration of devices and systems)	C,I,A
T 0.31	การใช้หรือการจัดการอุปกรณ์และระบบอย่างไม่ถูกต้อง (Incorrect use or administration of devices and systems)	C,I,A
T 0.32	การใช้อำนาจอนุมัติ (Abuse of authorizations)	C,I,A
T 0.33	การขาดบุคลากร (Absence of personnel)	A
T 0.34	โจมตี (Attack)	C,I,A
T 0.35	การบังคับขู่กรรโชกหรือการทุจริต (Coercion, extortion or corruption)	C,I,A
T 0.36	โจรกรรม (Identity theft)	C,I,A
T 0.37	การปฏิเสธการกระทำ (Repudiation of actions)	C,I
T 0.38	การใช้ข้อมูลส่วนบุคคล (Abuse of personal data)	C
T 0.39	ซอฟต์แวร์ที่เป็นอันตราย (Malicious software)	C,I,A
T 0.40	การปฏิเสธบริการ (Denial of service)	A
T 0.41	การก่อวินาศกรรม (Sabotage)	A
T 0.42	วิศวกรรมทางสังคม (Social Engineering)	C,I
T 0.43	การเล่นซ้ำของข้อความ (Replay of messages)	C,I
T 0.44	การเข้าสถานที่โดยไม่ได้รับอนุญาต (Unauthorized entry to premises)	C,I,A
T 0.45	ข้อมูลสูญหาย (Data loss)	A
T 0.46	สูญเสียข้อมูลที่ละเอียดอ่อน (Loss of integrity of sensitive information)	I

ที่มา: Overview of the elementary threats ของ supplement to BSI Standard 100-3

2.3 กำหนดจุดอ่อนของสินทรัพย์ (Vulnerability Identification)

2.3.1 พิจารณารายการจุดอ่อนซึ่งเอื้อให้เกิดภัยคุกคามแต่ละรายการที่สร้างความเสียหายให้กับสินทรัพย์ โดยประเภทของจุดอ่อนที่นำมาพิจารณา มีดังต่อไปนี้

2.3.1.1 จุดอ่อนที่เกี่ยวกับซอฟต์แวร์ เช่น โปรแกรมมีจุดอ่อนซึ่งเป็นสาเหตุให้ระบบคอมพิวเตอร์ถูกเจาะ (Hack) หรือการไม่ติดตั้งซอฟต์แวร์ Anti-virus เป็นสาเหตุให้เกิดปัญหาไวรัสแพร่ระบาด

2.3.1.2 จุดอ่อนที่เกี่ยวกับฮาร์ดแวร์ เช่น ไม่มีขั้นตอนควบคุมการปรับค่า Configuration ของสินทรัพย์ อาจทำให้ปรับแต่งค่าผิดและระบบมีปัญหา หรือในเครือข่ายการสื่อสารไม่มีการเข้ารหัสข้อมูลที่เป็นความลับ ซึ่งอาจทำให้ข้อมูลที่เป็นความลับถูกเปิดเผย

2.3.1.3 จุดอ่อนที่เกี่ยวข้องกับตัวบุคคล เช่น ไม่มีการฝึกอบรมเพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรที่เกี่ยวข้อง ซึ่งทำให้มีการปฏิบัติงานที่ผิดพลาด

2.3.1.4 จุดอ่อนที่เกี่ยวกับบริหารโครงสร้างพื้นฐานที่สนับสนุนระบบสารสนเทศ เช่น ไม่มีระบบควบคุมเพลิงไหม้ ซึ่งหากเกิดเพลิงไหม้ก็จะไม่สามารถควบคุมเพลิงได้ หรือไม่มีแนวปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน ซึ่งทำให้ไม่สามารถยืนยันตัวบุคคลของผู้ใช้งานและทำให้เกิดการสวมสิทธิการใช้งาน

2.3.2 พิจารณาถึงจุดอ่อนซึ่งเอื้อให้เกิดภัยคุกคามแต่ละรายการ หลังจากนั้นให้ระบุรายการของ “จุดอ่อน” ที่เกี่ยวข้องลงไป แบบฟอร์มรายงานการประเมินความเสี่ยงสินทรัพย์ ให้ถูกต้องและเป็นปัจจุบัน โดยข้อมูลของจุดอ่อนและภัยคุกคามที่เกี่ยวข้องต้องอยู่ในแถวเดียวกัน

2.4 วิเคราะห์มาตรการป้องกันที่มีอยู่ (Existing Control Analysis)

2.4.1 พิจารณามาตรการป้องกันที่มีอยู่ในปัจจุบัน ที่ใช้ในการแก้ไขจุดอ่อน หรือลดความเป็นไปได้ หรือลดความรุนแรงของภัยคุกคามต่อสินทรัพย์ หรือป้องกันไม่ให้ภัยคุกคามสร้างความเสียหายให้กับสินทรัพย์

2.4.2 พิจารณาได้แล้วให้ปรับปรุงข้อมูลของมาตรการป้องกันในแบบฟอร์มรายการประเมินความเสี่ยงสินทรัพย์ (Risk Assessment Report) ให้ถูกต้องและเป็นปัจจุบัน

2.5 ประเมินระดับความเป็นไปได้ (Likelihood Determination)

2.5.1 ผู้ดูแลสินทรัพย์ประเมินระดับความเป็นไปได้ (Likelihood) โดยประเมินค่าความเป็นไปได้ที่ภัยคุกคามอาจกระทำความเสียหายต่อสินทรัพย์ได้สำเร็จ โดยต้องพิจารณา 2 ปัจจัยหลักดังนี้

2.5.1.1 แนวโน้มการเกิดขึ้นของภัยคุกคาม พิจารณาจากแรงจูงใจหรือค่าทางสถิติที่มีการบันทึกไว้ เช่น สินทรัพย์ที่มีราคาสูงและเคลื่อนย้ายง่ายจะมีแนวโน้มที่จะถูกขโมยได้มากกว่าสินทรัพย์ทั่วไป หรือภัยคุกคามประเภทภัยธรรมชาติต่าง ๆ จะมีแนวโน้มการเกิดต่อเมื่อดูจากสถิติที่เคยเกิดขึ้น ถ้าแนวโน้มการเกิดของภัยคุกคามสูง ความเป็นไปได้ที่ภัยคุกคามนั้นจะกระทำความเสียหายต่อสินทรัพย์ได้สำเร็จจะสูงกว่าภัยคุกคามที่มีแนวโน้มการเกิดต่อ

2.5.1.2 ความยากง่ายที่ภัยคุกคามจะสำเร็จ พิจารณาจากจุดอ่อนที่มีอยู่และเครื่องมือควบคุมในปัจจุบัน หากมีจุดอ่อนมาก แต่ไม่มีเครื่องมีควบคุมเลย โอกาสที่ภัยคุกคามจะเกิดขึ้นกับสินทรัพย์ได้ก็จะสูงกว่าในกรณีที่มีเครื่องมือควบคุม

2.5.2 เมื่อประเมินค่าได้แล้วให้ปรับปรุงค่าความเป็นไปได้ รายงานการประเมินความเสี่ยงสินทรัพย์ (Risk Assessment Report) ให้เป็นปัจจุบัน ระดับความเป็นไปได้แบ่งออกเป็น ๕ ระดับ ตามตารางต่อไปนี้

ตารางที่ 3.3 ความเป็นไปได้ระดับความเสี่ยง

ระดับ	ความเป็นไปได้	คำอธิบายและหลักเกณฑ์
5	สูงมาก	ภัยคุกคามมีโอกาสสร้างความเสียหายได้สูงมาก หรืออาจเกิดขึ้นได้ทุกสัปดาห์หรือบ่อยกว่านั้น
4	สูง	ภัยคุกคามมีโอกาสสร้างความเสียหายได้สูง หรืออาจเกิดขึ้นได้ประมาณเดือนละครั้ง
3	ปานกลาง	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ปานกลาง หรืออาจเกิดขึ้นได้ประมาณปีละครั้ง
2	ต่ำ	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ต่ำ หรือในรอบสิบปีอาจเกิดขึ้นได้ 1 – 2 ครั้ง
1	ต่ำมาก	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ต่ำมาก หรือในรอบร้อยปีอาจเกิดขึ้นได้สักครั้ง หรือแทบเป็นไปไม่ได้ที่จะเกิดขึ้น

2.6 ประเมินผลกระทบและความเสียหาย (Impact Analysis)

2.6.1 ผู้ดูแลสินทรัพย์ประเมินผลกระทบ (Impact) ซึ่งเกิดจากภัยคุกคามลงในรายงานการประเมินความเสี่ยงสินทรัพย์ (Risk Assessment Report) โดยพิจารณาจากมิติของความ

มั่นคงปลอดภัยสารสนเทศที่ได้รับความเสียหายจากภัยคุกคาม และค่าของสินทรัพย์ในแต่ละมิติของความมั่นคงปลอดภัยสารสนเทศ ซึ่งได้แก่ การสูญเสียความลับ (Loss of Confidentiality) การสูญเสียความถูกต้องครบถ้วน (Loss of Integrity) และการสูญเสียสภาพความพร้อมใช้งาน (Loss of Availability)

2.7 ประเมินระดับความเสี่ยง

2.7.1 ***ผู้ดูแลสินทรัพย์ประเมินค่าระดับความเสี่ยงจากผลกระทบ (Impact) และโอกาสที่จะเกิด (Likelihood)*** โดยพิจารณาจากผลกระทบแยกตามมิติของความมั่นคงปลอดภัยสารสนเทศ ซึ่งได้แก่ การสูญเสียความลับ (Loss of Confidentiality) การสูญเสียความถูกต้องครบถ้วน (Loss of Integrity) และการสูญเสียสภาพความพร้อมใช้งาน (Loss of Availability) และใช้ระดับความเสี่ยงที่มากที่สุดที่ประเมินได้ในแต่ละด้านเป็นความเสี่ยงของภัยคุกคามนั้น ๆ ต่อสินทรัพย์การประเมินค่าระดับความเสี่ยงให้อ้างอิงจากตารางต่อไปนี้

ตารางที่ 3.4 ผลกระทบและโอกาสที่จะเกิดความเสี่ยง

โอกาสที่จะเกิด/ระดับความเสี่ยง	**ผลกระทบ/ระดับความรุนแรง**				
	1 = ต่ำมาก (Very Low)	**2 = ต่ำ (Low)**	**3 = ปานกลาง (Medium)**	**4 = สูง (High)**	**5 = สูงมาก (Very Hight)**
5 = โอกาสเกิดสูงมาก	5 (ต่ำมาก)	10 (ต่ำ)	15 (ปานกลาง)	20 (สูง)	25 (สูงมาก)
4 = โอกาสเกิดสูง	4 (ต่ำมาก)	8 (ต่ำ)	12 (ปานกลาง)	16 (สูง)	20 (สูง)
3 = โอกาสเกิดปานกลาง	3 (ต่ำมาก)	6 (ต่ำ)	9 (ต่ำ)	12 (ปานกลาง)	15 (ปานกลาง)
2 = โอกาสเกิดน้อย	2 (ต่ำมาก)	4 (ต่ำมาก)	6 (ต่ำ)	8 (ต่ำ)	10 (ต่ำ)
1 = โอกาสเกิดน้อยมาก	1 (ต่ำมาก)	2 (ต่ำมาก)	3 (ต่ำมาก)	4 (ต่ำมาก)	5 (ต่ำมาก)

การคิดค่าของระดับความเสี่ยงสามารถคำนวณได้ดังนี้

ระดับความเสี่ยงโดยรวม (Risk Value) = โอกาสที่จะเกิด (Likelihood) X ผลกระทบ (Impact)

การนำระดับความเสี่ยงที่ระบุไว้มาประเมินโอกาสที่จะเกิด (Likelihood) และการประเมินระดับของผลกระทบ (Impact) ตามเกณฑ์การประเมินความเสี่ยงขององค์กร ซึ่งได้กำหนดเกณฑ์ความเสี่ยงไว้ 5 ระดับ ดังนี้

ระดับความเสี่ยง 1 – 5 = ต่ำมาก (Very Low)
ระดับความเสี่ยง 6 – 10 = ต่ำ (Low)
ระดับความเสี่ยง 11 – 15 = ปานกลาง (Medium)
ระดับความเสี่ยง 16 – 20 = สูง (High)
ระดับความเสี่ยง 21 – 25 = สูงมาก (Very High)

2.7.2 ผลลัพธ์ในตารางข้างต้นสำหรับช่องที่ถูกแรเงาแบ่งตามสีนั้นเป็นกรณีที่ต้องนำไปดำเนินการหาวิธีแก้ไขความเสี่ยง ความหมายของความเสี่ยงในแต่ละระดับตามตารางข้างต้น มีความหมายดังนี้

ตารางที่ 3.5 ระดับความเสี่ยง

ระดับความเสี่ยง	การดำเนินการที่เหมาะสม
สูงมาก (Very Hight)	ความเสี่ยงในระดับสูง ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง และดำเนินการทันที
สูง (High)	ความเสี่ยงในระดับค่อนข้างสูง ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยงและดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสม
ปานกลาง (Medium)	ความเสี่ยงในระดับปานกลาง ควรพิจารณาแก้ไขความเสี่ยง แต่หากมีเหตุจำเป็นก็สามารถพิจารณายอมรับความเสี่ยงได้
ต่ำ (Low)	ความเสี่ยงในระดับที่ต่ำมาก สามารถยอมรับได้โดยไม่ต้องดำเนินการใด ๆ เพิ่มเติม
ต่ำมาก (Very Low)	ความเสี่ยงในระดับที่ต่ำมาก สามารถยอมรับได้เลย

2.8 ประเมินปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO 27001 สำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

2.9 พัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

2.9.1 แนวคิดในการออกแบบและพัฒนาระบบ

ในการพัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย จะพัฒนาตามสถาปัตยกรรม Web Application ซึ่งเป็นการพัฒนาระบบงานบนเว็บ โดยใช้ภาษา PHP ในการพัฒนา และใช้ My SQL เป็นฐานข้อมูล โดย Web Application มีข้อดีคือ ข้อมูลต่าง ๆ ในระบบมีการไหลเวียนในแบบ Online ทั้งแบบ Local (ภายในวงLAN) และ Global (ออกไปยังเครือข่ายอินเตอร์เน็ต) ทำให้เหมาะสำหรับงานที่ต้องการข้อมูลแบบ Real Time ระบบมีประสิทธิภาพ แต่ใช้งานง่าย เหมือนกำลังท่องเว็บ ระบบงานที่พัฒนาขึ้นมาจะตรงกับความต้องการกับหน่วยงาน ซึ่งแตกต่างจากโปรแกรมสำเร็จรูปทั่วไป ที่มักจะจัดทำระบบในแบบกว้าง ๆ ซึ่งมักจะไม่ตรงกับความต้องการที่แท้จริง ระบบสามารถโต้ตอบกับผู้ใช้บริการแบบ Real Time ทำให้เกิดความประทับใจ และเครื่องที่ใช้งานไม่จำเป็นต้องติดตั้งโปรแกรมใด ๆ เพิ่มเติมทั้งสิ้น

ลักษณะการทำงานของ Web Application นั้นโปรแกรมส่วนหนึ่งจะวางตัวอยู่บน Rendering Engine ซึ่งตัว Rendering Engine จะทำหน้าที่หลักๆ คือนำเอาชุดคำสั่งหรือรูปแบบโครงสร้างข้อมูลที่ใช้ในการแสดงผล นำมาแสดงผลบนพื้นที่ส่วนหนึ่งในจอภาพ โปรแกรมส่วนที่วางตัวอยู่บน Rendering Engine จะทำหน้าที่หลักๆ คือการเปลี่ยนแปลงแก้ไขสิ่งที่แสดงผล จัดการตรวจสอบข้อมูลที่รับเข้ามาเบื้องต้นและการประมวลบางส่วนแต่ส่วนการทำงานหลักๆ จะวางตัวอยู่บนเซอร์เวอร์ ในลักษณะ Web Application แบบเบื้องต้น

ฝั่งเซิร์ฟเวอร์จะประกอบไปด้วยเว็บเซิร์ฟเวอร์ซึ่งทำหน้าที่เชื่อมต่อกับไคลเอนต์ตามโพรโทคอล (Protocol) HTTP/HTTPS โดยนอกจากเว็บเซิร์ฟเวอร์จะทำหน้าที่ส่งไฟล์ที่เกี่ยวเนื่องกับการแสดงผลตามมาตรฐาน HTTP ตามปกติทั่วไปแล้ว เว็บเซิร์ฟเวอร์จะมีส่วนประมวลผลซึ่งอาจจะเป็นตัวแปลภาษา เช่น Script Engine ของภาษา PHP หรืออาจจะมีการติดตั้ง .NET Framework ซึ่งมีส่วนแปลภาษา CLR (Common Language Runtime) ที่ใช้แปลภาษา intermediate จากโค้ดที่เขียนด้วย VB.NET หรือ C#.NET หรืออาจจะเป็น J2EE ที่มีส่วนแปลไบต์โค้ดของคลาสที่ได้จากโปรแกรมภาษาจาวา เป็นต้น

2.9.2 คุณสมบัติของระบบ

โดยกำหนดความต้องการของระบบ ดังนี้

1. *สำหรับผู้ใช้งานทั่วไป*

1) ระบบสามารถแสดงรายละเอียดตามข้อกำหนดของ ISO/IEC 27001:2013 เฉพาะด้านการควบคุมการเข้าถึง (Access Control)

2) ผู้ใช้งานสามารถร้องขอการลงทะเบียน เพื่อขอเข้าใช้งานระบบ

2. สำหรับผู้ใช้งานที่ลงชื่อเข้าใช้งาน

1) ผู้ใช้งานต้องทำการลงทะเบียนเพื่อเข้าใช้งานระบบ และต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งานเสมอ

2) ผู้เข้าใช้งานระบบที่ได้รับอนุญาตให้ใช้งาน ต้องทำการลงชื่อเข้าใช้งานระบบทุกครั้ง และระบบจะทำการออกจากระบบโดยอัตโนมัติเมื่อไม่มีการใช้งานเป็นระยะเวลานานเกิน 10 นาที

3) ระบบต้องแสดงฟังก์ชันหลัก 2 ส่วน ดังนี้

3.1) รายการควบคุม (Control List) ระบบสามารถแสดงรายละเอียดตามข้อกำหนดตามมาตรฐาน ISO/IEC 27001:2013 โดยแบ่งหัวข้อการแสดงผลอย่างชัดเจนตามข้อกำหนดหลัก 14 โดเมน

3.2) รายการตรวจสอบ (Checklist) ระบบสามารถแสดงรายละเอียด ตามข้อกำหนด และเอกสารที่เกี่ยวข้องของแต่ละข้อกำหนดที่สอดคล้องกับการพัฒนาระบบ โดยแยกแสดงผลอย่างชัดเจน

3.3) การแสดงผล (Assessment) ระบบสามารถประเมินความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013 เฉพาะด้านการควบคุมการเข้าถึง (Access Control) ดังนี้

+ ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)

- นโยบายการควบคุมการเข้าถึง (Access control policy)
- การเข้าถึงเครือข่ายและบริหารเครือข่าย (Access to networks and network services)

+ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

- การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and deregistration)

- การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)

- การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

- การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)

- การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

- การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)

+ **หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)**

- การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of secret authentication information)

+ **การควบคุมการเข้าถึงระบบ (System and application access control)**

- การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

- ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

- ระบบบริหารจัดการหัสผ่าน (Password management system)

- การใช้โปรแกรมอรรถประโยชน์ (User of privileged utility programs)

- การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

โดยในแต่ละข้อจะประกอบไปด้วย รายการตรวจสอบ (Checklist) ดังต่อไปนี้

- ระเบียบ/ข้อกำหนด
  - มี/แนบเอกสาร ผลการประเมินเท่ากับ 100%
  - มี/ไม่แนบเอกสาร ผลการประเมินเท่ากับ 50 %
  - ไม่มี ผลการประเมินเท่ากับ 0%
- การปฏิบัติตามระเบียบ/ข้อกำหนด
  - ปฏิบัติ/แนบเอกสาร ผลการประเมินเท่ากับ 100%
  - ปฏิบัติ/ไม่แนบเอกสาร ผลการประเมินเท่ากับ 50%
  - ไม่ปฏิบัติ ผลการประเมินเท่ากับ 0%

เมื่อทำการประเมินครบทุกข้อ ระบบสามารถแสดงสรุปผลการประเมินแยกเป็นข้อ และ % พร้อมแสดงแถบสี ดังนี้

สีเขียว	ผลการประเมิน 100%	ผ่าน
สีเหลือง	ผลการประเมิน 50 – 99%	ปรับปรุง
สีแดง	ผลการประเมิน 0 – 49%	ไม่ผ่าน

บทที่ 4

ผลการวิจัย

1. ข้อมูลพื้นฐานของสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย

1.1 ระบบเครือข่ายที่มีอยู่

รายการอุปกรณ์ระบบเครือข่ายของสำนักงานจังหวัด ประกอบด้วย

1) Nortel Network/Passport 7480 (ATM) ทำหน้าที่เป็นอุปกรณ์หลักในการรับสัญญาณเครือข่ายอินเทอร์เน็ตจากสำนักงานปลัดกระทรวงมหาดไทย ด้วยความเร็ว 10/100 Mpbs

2) Nortel Network Baystack 425-24T (Layer 2 Switch) เป็นอุปกรณ์หลักในการกระจายสัญญาณในอาคารศาลากลางจังหวัด และ Nortel Network/Baystack 425-24T_C1 (Layer 2 Switch) เป็นอุปกรณ์หลักในการกระจายสัญญาณไปยังระบบการประชุมทางไกลกระทรวงมหาดไทยและจังหวัด (VDO Conference)

3) Fortigate60 Firewall อุปกรณ์ป้องกันการบุกรุกระบบเครือข่าย

4) TP-Link 8 port อุปกรณ์กระจายสัญญาณไปยังสำนักงานจังหวัด

5) D-Link 8 port อุปกรณ์กระจายสัญญาณไปแต่ละกลุ่มงานภายในสำนักงานจังหวัด

6) เครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการข้อมูลจังหวัดและกระทรวงมหาดไทย (MOC) เครื่องคอมพิวเตอร์แม่ข่ายข้อมูลบุคลากรภาครัฐของสำนักงานจังหวัด

7) ระบบสำรองไฟฟ้าทำหน้าที่จ่ายไฟให้กับ ATM Access และ Nortel Network/Baystack 425-24T ประกอบด้วย

(1) DC Power Supply (Delta MCS1800) 1 ชุด

(2) MGE UPS Systems Pulsar Extreme 2000 VA 1 ชุด

(3) MGE UPS Systems Pulsar Evolution 500 VA 1 ชุด

8) ระบบปรับอากาศในห้องสื่อสาร ประกอบด้วย แอร์ ขนาด 800 BTU จำนวน 2 ตัว

ระบบเครือข่ายที่ติดตั้ง ณ สำนักงานจังหวัดใช้ระบบ ATM Access รับสัญญานไฟเบอร์ออฟติกจากกระทรวงมหาดไทย เข้ามายังศาลากลางจังหวัด จากนั้นใช้อุปกรณ์ Layer 2 Switch กระจายสัญญาณไปยังชั้นและห้องต่าง ๆ ภายในอาคารศาลากลางจังหวัด รวมถึงสำนักงานจังหวัด จากนั้นต่อเข้าไฟร์วอลล์ และกระจายสัญญาณไปยังกลุ่มงานต่าง ๆ ภายในสำนักงานจังหวัด

1.2 ปัญหาที่พบ

1) อุปกรณ์ที่ติดตั้งเป็นอุปกรณ์รุ่นเก่า เช่น ไฟร์วอลล์ ไม่สามารถรองรับภัยคุกคามคอมพิวเตอร์หรือการโจมตีรูปแบบใหม่ ๆ ได้ ส่งผลให้ระบบเครือข่ายในหน่วยงานช้า ขาดเสถียรภาพในการใช้งาน

2) เครื่องคอมพิวเตอร์แม่ข่ายสามารถเข้าถึงได้โดยตรง โดยไม่มีไฟร์วอลล์กั้นอยู่

3) การเชื่อมต่อสวิตซ์หลายตัวแบบเชื่อมต่อกันไปเรื่อย ๆ ส่งผลให้เป็นการลดทอนสัญญาณ ส่งผลให้ประสิทธิภาพในการทำงานช้าลง

4) ไม่สามารถบริหารจัดการระบบเครือข่ายได้ เนื่องจากขาดอุปกรณ์ในการควบคุมและการบริหารจัดการระบบเครือข่ายที่ดี

5) ปัญหาความเร็วที่จำกัด แบบด์วิดท์ในการใช้งานอินเทอร์เน็ต และเมื่อหากมีการประชุมทางไกลจากกระทรวงมหาดไทยถึงจังหวัด จะส่งผลให้ระบบเครือข่ายช้าลงไปอีก

1.3 ระบบเทคโนโลยีสารสนเทศภายในองค์กร

1) กลุ่มงานอำนวยการ สินทรัพย์เกี่ยวกับงานระบบ คือ ระบบการบริหารงานการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ หรือ ระบบ GFMIS ซึ่งเป็นการดำเนินงานปรับปรุงระบบการจัดการด้านการเงินการคลังของภาครัฐให้มีความทันสมัยและมีประสิทธิภาพยิ่งขึ้น โดยนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ เพื่อปรับกระบวนการดำเนินงานและการจัดการภาครัฐด้านการ งบประมาณ การบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร ให้เป็นไปในทิศทางเดียวกับนโยบายปฏิรูปราชการที่เน้นประสิทธิภาพและความคล่องตัวในการดำเนินงาน รวมทั้งมุ่งหวังให้เกิดการใช้ทรัพยากรภายในองค์กรอย่างคุ้มค่าเพื่อให้ได้มาซึ่งข้อมูลสถานภาพการคลังภาครัฐที่ถูกต้องรวดเร็ว สามารถตอบสนองนโยบายการบริหารเศรษฐกิจของประเทศ

2) กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สินทรัพย์เกี่ยวกับงานระบบคือ ระบบติดตามประเมินผลแผนงาน (Padme) เพื่อใช้สำหรับบริหารจัดการแผนงาน/โครงการจากทุกแหล่งงบประมาณที่ดำเนินการในพื้นที่

3) กลุ่มงานบริหารทรัพยากรบุคคล สินทรัพย์เกี่ยวกับงานระบบคือ ระบบสารสนเทศทรัพยากรบุคคลระดับจังหวัด (PPIS) เป็นโปรแกรมที่พัฒนาขึ้นตั้งแต่ปี พ.ศ. 2531 เพื่อเป็นเครื่องมือช่วยในการบริหารจัดการเกี่ยวกับข้าราชการและลูกจ้างประจำระดับจังหวัด มีการพัฒนาและปรับปรุงหลายครั้ง เพื่อให้ทันกับความต้องการ กฎ ระเบียบและเทคโนโลยีที่เปลี่ยนแปลง ในปัจจุบันได้พัฒนาและปรับปรุงโปรแกรม Version 5.0 ให้สามาถจัดเก็บข้อมูลของลูกจ้างชั่วคราว

ปรับปรุงการเก็บข้อมูลบุคคลได้ถึงระดับต่ำกว่าสำนัก/กอง 5 ระดับ การใช้งานตามโครงสร้างตามมองหมายงาน เพื่อให้สามารถใช้งานในการบริหารงานบุคคลให้แก่ส่วนราชการได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

4) กลุ่มงานศูนย์ดำรงธรรมจังหวัด สินทรัพย์เกี่ยวกับงานระบบ คือ ระบบงานรับและติดตามเรื่องราวร้องทุกข์ของศูนย์ดำรงธรรม

2. ทะเบียนสินทรัพย์และกำหนดค่าของสินทรัพย์ (Asset Identification and Valuation)

ขอบเขตของสินทรัพย์ที่ครอบคลุมในการประเมินความเสี่ยงในครั้งนี้ ประกอบด้วยสินทรัพย์ด้านสารสนเทศหลักของสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย โดยแบ่งกลุ่มของสินทรัพย์ตามแผนกและลักษณะงานได้ดังนี้

(1) สินทรัพย์เกี่ยวกับงานระบบบริหารการเงินการคลังภาครัฐ (GFMIS) กลุ่มงานอำนวยการ

(2) สินทรัพย์เกี่ยวกับงานระบบติดตามประเมินผลแผนงาน (Padme) กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด

(3) สินทรัพย์เกี่ยวกับงานระบบสารสนเทศทรัพยากรบุคคลระดับจังหวัด (PPIS) กลุ่มงานบริหารทรัพยากรบุคคล

(4) สินทรัพย์เกี่ยวกับงานระบบร้องเรียน ร้องทุกข์ ศูนย์ดำรงธรรมจังหวัด กลุ่มงานศูนย์ดำรงธรรมจังหวัด

โดยประเมินรายการสินทรัพย์ด้านเทคโนโนลีสารสนเทศแบ่งออกเป็น 6 ด้าน คือ

(1) กระบวนการทางธุรกิจ (Business Processes)

(2) ข้อมูล (Information Assets)

(3) ซอฟต์แวร์ (Software Assets)

(4) ฮาร์ดแวร์ (Hardware Assets)

(5) บุคคล (Propel Assets)

(6) บริการโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร (Infrastructure Assets)

3. ประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัด ตามกรอบมาตรฐาน ISO /IEC 27001:2013 ข้อ A9 การควบคุมการเข้าถึง (Access Control)

ตารางที่ 4.1 ประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

ประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัด ตามกรอบมาตรฐาน ISO /IEC 27001:2013 A9 การควบคุมการเข้าถึง (Access Control)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.1 ความต้องการทางธุรกิจสำหรับควบคุมการเข้าถึง (Business requirements of access control) วัตถุประสงค์ เพื่อกำจัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ								
A9.1.1	นโยบายควบคุมการเข้าถึง (Access control policy)	- ไม่มีการกำหนดสิทธิ ระยะเวลาการให้อำนาจในการเข้าออกพื้นที่เพื่อควบคุมการเข้าถึง - ไม่มีนโยบายควบคุมการเข้าถึงระบบสารสนเทศจากผู้บริหาร - ไม่มีแนวทางการจัดทำนโยบายควบคุมการเข้าถึงระบบสารสนเทศแต่ผู้ปฏิบัติงานปฏิบัติตามขอบเขตงานตนเอง	- การไม่มีนโยบายการควบคุมการเข้าถึงระบบ ทำให้ผู้ใช้งานในหน่วยงานไม่เห็นความสำคัญของการปฏิบัติตามนโยบาย หรือแนวทาง อาจส่งผลให้ระบบถูกโจมตีจากผู้ไม่หวังดีได้	3	5	15 (ปานกลาง)	สีส้ม	นโยบายควบคุมการเข้าถึงต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร และทบทวนตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.1.2	การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to network and network services)	- มีการพิสูจน์ตัวจริงบนเครือข่าย แต่ยังไม่ครอบคลุมทุกอุปกรณ์ - ไม่มีนโยบายและแนวทางการเข้าถึงเครือข่ายและบริการเครือข่าย	- การเข้าใช้งานเครือข่ายหน่วยงานโดยไม่ได้รับอนุญาตอาจทำให้ข้อมูลถูกทำลายหรือถูกละเมิดสิทธิจากการปกป้องได้	3	4	12 (ปานกลาง)	สีส้ม	ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุญาตการเข้าถึงเท่านั้น

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) วัตถุประสงค์ เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยมิได้รับอนุญาต								
A9.2.1	การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and deregistration)	- ขาดการควบคุม ให้ / ถอน สิทธิการใช้งานอย่างเป็นทางการ - ไม่มีนโยบายและแนวทางการลงทะเบียนและถอดถอนสิทธิ์ - ไม่มีการแสดงตารางสิทธิในการเข้าถึงระบบ - ไม่มีแนวทางการปฏิบัติการเพิกถอนลงทะเบียนสิทธิผู้ใช้งานและรายงานการเพิกถอนทะเบียน	- การขาดหลักฐานการลงทะเบียนผู้ใช้งาน หรือถอดถอนสิทธิทำให้ไม่สามารถทราบประวัติการใช้งาน - การไม่มีรายการเพิกถอนสิทธิผู้ใช้งาน อาจมีการแอบเข้าใช้งานของพนักงานที่ลาออกจากงานไปแล้ว	3	4	12 (ปานกลาง)	สีส้ม	กระบวนการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อเป็นการใช้สิทธิการเข้าถึง

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.2.2	การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)	- ทำตามดุลพินิจของผู้ดูแลระบบโดยผู้บริหารไม่จำเป็นต้องอนุมัติ - ไม่มีนโยบายและแนวทางการจัดการสิทธิการเข้าถึงของผู้ใช้งาน	- อาจทำให้มีการแอบอ้างการใช้งานจากผู้ไม่ได้รับอนุญาต	3	4	12 (ปานกลาง)	สีส้ม	กระบวนการจัดการสิทธิการเข้าถึงของผู้ใช้งานต้องมีการปฏิบัติตาม ทั้งให้และถอดถอนสิทธิการเข้าถึงสำหรับผู้ใช้งานทุกประเภททุกระบบและบริการทั้งหมดขององค์กร

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.2.3	การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)	- มีการจัดลำดับความสำคัญในการเข้าถึงข้อมูลของผู้ใช้แต่ละระดับโดยผู้ดูแลระบบ - ไม่มีนโยบายการบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ	- ทำให้ผู้ใช้งานละเมิดสิทธิการใช้งานของผู้อื่นนอกเหนือจากสิทธิการใช้งานของตนเอง ทำให้อาจมีการเปลี่ยนแปลงข้อมูลที่สำคัญขององค์กรได้	2	5	10 (ต่ำ)	สีเหลือง	การให้และใช้สิทธิการเข้าถึงตามระดับสิทธิต้องมีการจำกัดและควบคุม
A9.2.4	การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)	- ไม่มีกระบวนการการควบคุมการมอบข้อมูลการพิสูจน์ตัวจริงของผู้ใช้งาน - ไม่มีนโยบายการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน	- ผู้ไม่ได้รับอนุญาตในการเข้าถึงข้อมูลอาจมีการแอบอ้างสิทธิการใช้งาน	4	3	12 (ปานกลาง)	สีส้ม	การมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ ต้องมีการควบคุมโดยผ่านกระบวนการบริหารจัดการที่เป็นทางการ

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.2.5	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	- มีการทบทวนสิทธิ์ แต่ไม่ได้กำหนดเวลาไว้อย่างชัดเจน - ไม่มีนโยบายและแนวทางการทบทวนสิทธิการเข้าถึงผู้ใช้งาน - ไม่มีการรายงานการสอบทานรายชื่อผู้ใช้	- ผู้ที่ถูกยกเลิกสิทธิการเข้าถึงระบบงาน อาจมีการแอบอ้างเพื่อเข้าใช้งาน ทำให้เกิดความเสียหายต่อระบบ	3	4	12 (ปานกลาง)	สีส้ม	เจ้าของทรัพย์สินต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนดไว้

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.2.6	การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)	- ไม่มีการระบุขั้นตอนปรับปรุงสิทธิการเข้าถึงอย่างเป็นทางการ - ไม่มีนโยบายและแนวทางการถอดถอนและสิทธิการใช้งาน	- ผู้ที่ถูกยกเลิกสิทธิการเข้าถึงระบบงาน อาจมีการแอบอ้างเพื่อเข้าใช้งาน ทำให้เกิดความเสี่ยงต่อระบบงานได้	3	4	12 (ปานกลาง)	สีส้ม	สิทธิการเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญาหรือสิ้นสุดข้อตกลงการจ้าง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนการจ้างงาน

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน								
A9.3.1	การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of secret authentication information)	- ไม่ได้กำหนดวิธีปฏิบัติการใช้ข้อมูลการพิสูจน์ตัวจริงซึ่งเป็นความลับ - ไม่มีรายงานการถอดถอนสิทธิ - ไม่มีนโยบายการใช้งานข้อมูลการพิสูจน์ตัวตน ซึ่งเป็นข้อมูลลับ	- อาจเป็นช่องทางให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงระบบงานได้ จนเกิดความเสียหายต่อระบบงาน	4	5	20 (สูง)	ชมพู	ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ
A9.4 **การควบคุมการเข้าถึงระบบ (System and application access control)** วัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต								
A9.4.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	- มีการกำหนดรหัสผ่านการเข้าใช้งานระบบสารสนเทศ - ไม่มีนโยบายการจำกัดการเข้าถึงระบบสารสนเทศ	- อาจเป็นช่องทางให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงระบบงานได้	3	3	9 (ต่ำ)	สีเหลือง	การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.4.2	ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)	- เป็นที่รับทราบเฉพาะผู้ดูแลระบบสำหรับขั้นตอนการล็อกอินเข้าระบบ - ไม่มีนโยบายและแนวทางสำหรับการล็อกอินเข้าระบบ ที่มีความมั่นคงปลอดภัย	- การใช้งานจากที่สาธารณะต้องระมัดระวังการใช้งานรหัสผ่านและคงค้างรหัสไว้ ผู้อื่นอาจมาใช้งานต่อได้	3	2	6 (ต่ำ)	สีเหลือง	กรณีมีการกำหนดโดยนโยบายควบคุมการเข้าถึงการเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย
A9.4.3	ระบบบริหารจัดการหัสผ่าน (Password management system)	- มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน แต่ไม่เป็นทางการ - ไม่มีนโยบายและแนวทางการบริหารจัดการรหัสผ่าน	- ผู้ใช้งานที่ไม่ได้รับอนุญาตอาจคาดเดารหัสผ่านได้โดยง่ายจนสามารถเข้าใช้งานระบบได้	3	2	6 (ต่ำ)	สีเหลือง	ระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มีคุณภาพ

ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.4.4	การใช้โปรแกรมอรรถประโยชน์ (User of privileged utility programs)	- ไม่มีการควบคุมการใช้งาน การติดตั้งโปรแกรมอรรถประโยชน์ - ไม่มีนโยบายและแนวทางการใช้และขอติดตั้งโปรแกรมอรรถประโยชน์ - ไม่มีแบบฟอร์มขอติดตั้งโปรแกรมอรรถประโยชน์	- ผู้ใช้งานอาจมีการติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต จนอาจเกิดความเสียหายต่อระบบสารสนเทศได้	3	5	9 (ต่ำ)	สีเหลือง	การใช้ประโยชน์อรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

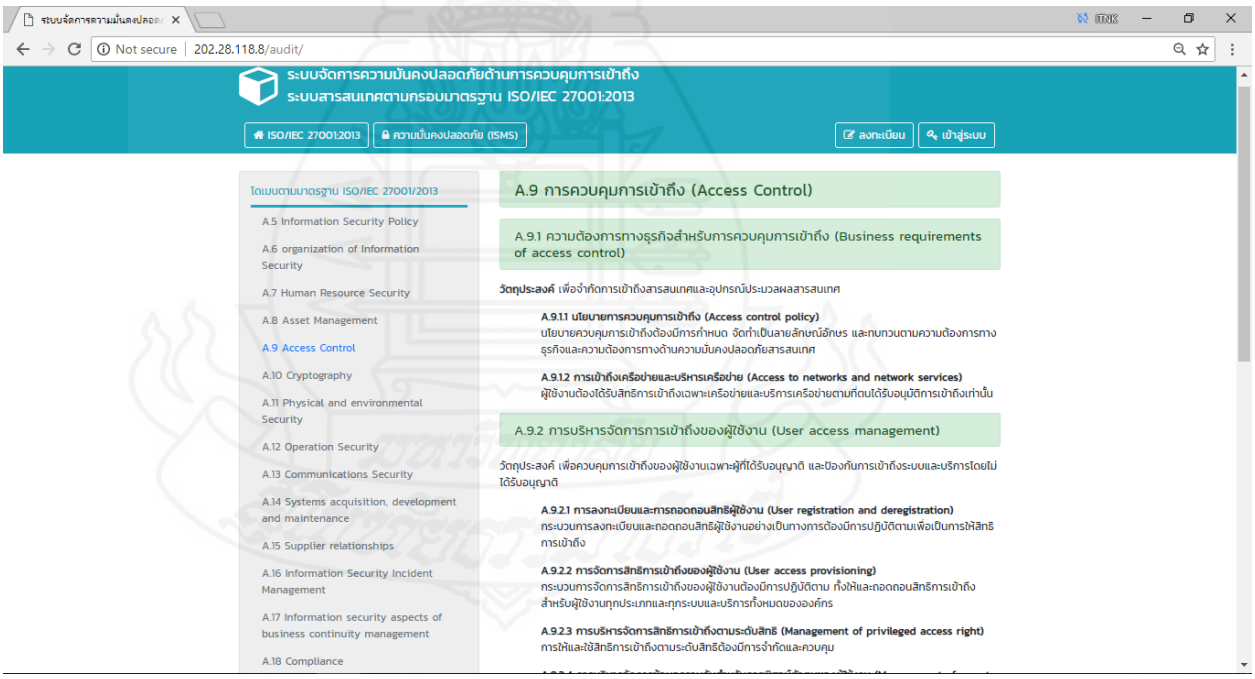
ตารางที่ 4.1 (ต่อ)

ข้อ	มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013	สถานะปัจจุบัน	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ	ผลกระทบ	โอกาส	ระดับความเสี่ยง	KPI	ข้อเสนอแนะ
A9.4.5	การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)	- มีการควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ กำหนดการเข้ารหัสและรหัสผ่าน - ไม่มีนโยบายและแนวทางการควบคุมการเข้าถึงซอสโค้ดของโปรแกรม - ไม่มีแบบฟอร์มร้องขอการเปลี่ยนแปลง	- ผู้ใช้งานอาจมีการเข้าถึงซอสโค้ดของระบบโดยไม่ได้รับอนุญาต จนอาจเกิดความเสียหายต่อระบบสารสนเทศได้	2	3	6 (ต่ำ)	สีเหลือง	การเข้าถึงซอร์สโค้ดของโปรแกรมต้องมีการจำกัดและควบคุม

จากการประเมินค่าความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัด ตามมาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013จำนวน 14 รายการ สรุปได้ดังนี้

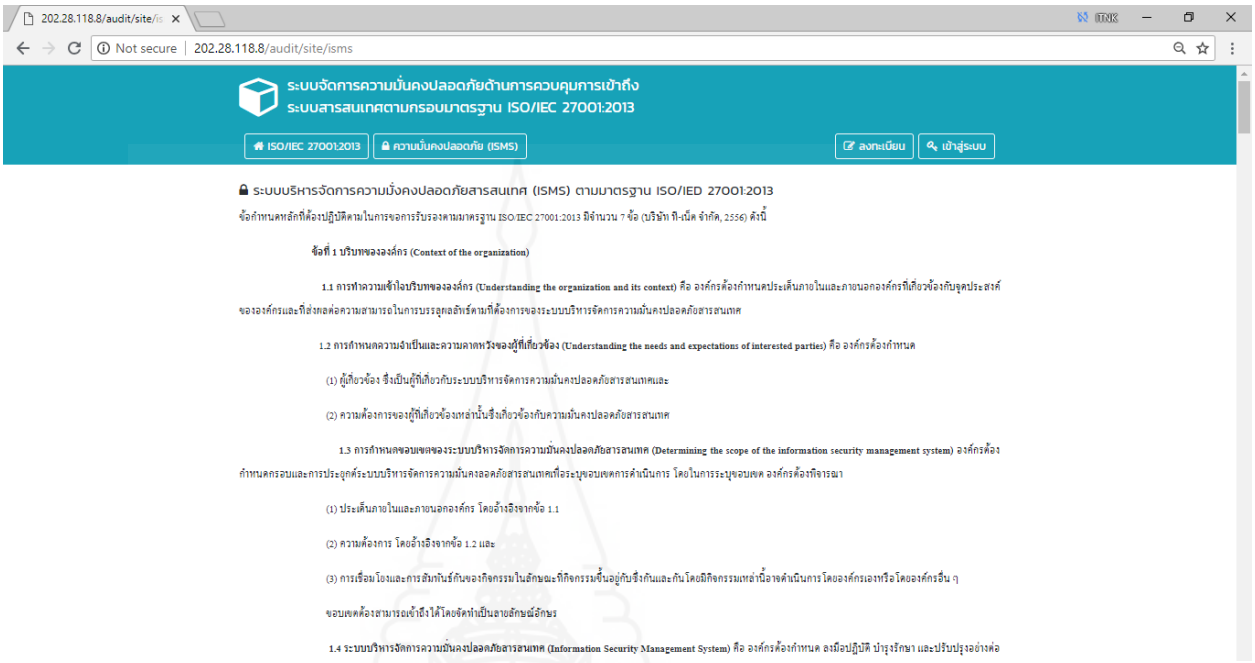
ระดับความเสี่ยงสูงมาก	สีแดง	จำนวน 0 รายการ
ระดับความเสี่ยงสูง	สีชมพู	จำนวน 1 รายการ
ระดับความเสี่ยงปานกลาง	สีสม	จำนวน 7 รายการ
ระดับความเสี่ยงต่ำ	สีเหลือง	จำนวน 6 รายการ
ระดับความเสี่ยงต่ำมาก	สีเขียว	จำนวน 0 รายการ

4. ระบบสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามกรอบมาตรฐาน ISO/IEC 27001:2013 สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย



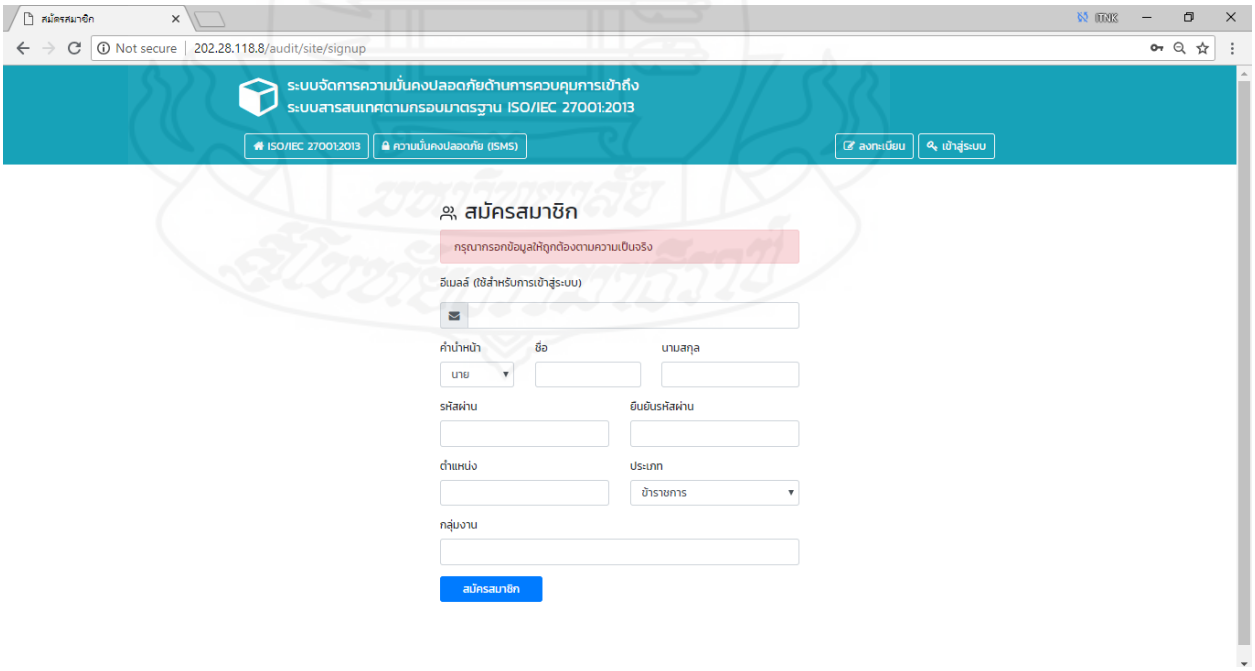
ภาพที่ 4.1 หน้าหลัก

4.1. ระบบสามารถแสดงรายละเอียดตามข้อกำหนดของ ISO/IEC 27001:2013 เฉพาะด้านการควบคุมการเข้าถึง (Access Control)



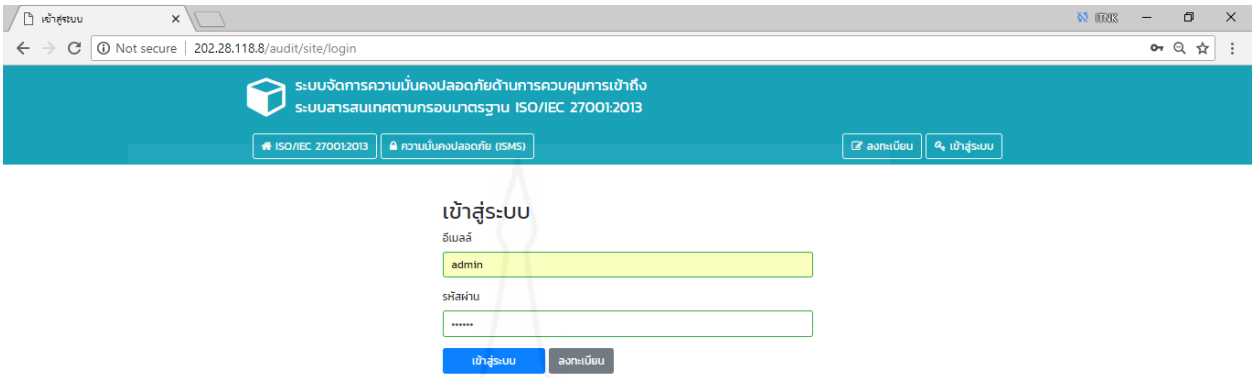
ภาพที่ 4.2 แนวทางการประเมิน

4.2 ผู้ใช้งานต้องทำการลงทะเบียนเพื่อเข้าใช้งานระบบ และต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งานเสมอ

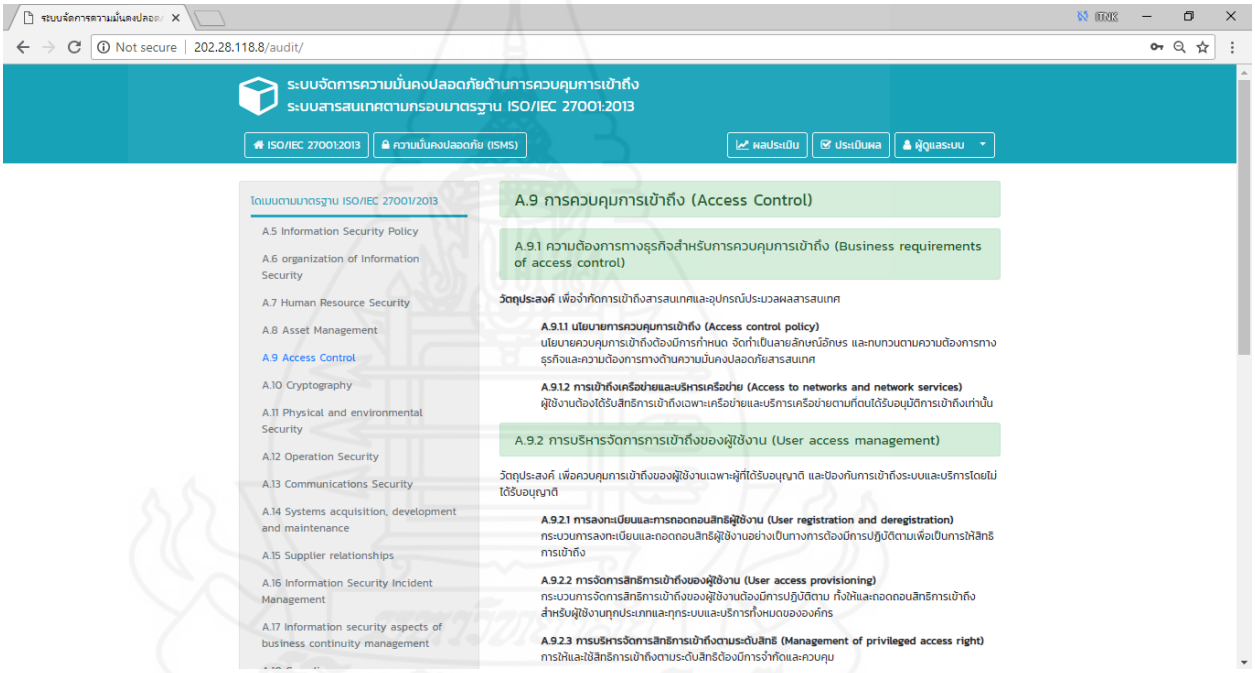


ภาพที่ 4.3 ลงทะเบียนผู้ใช้งาน

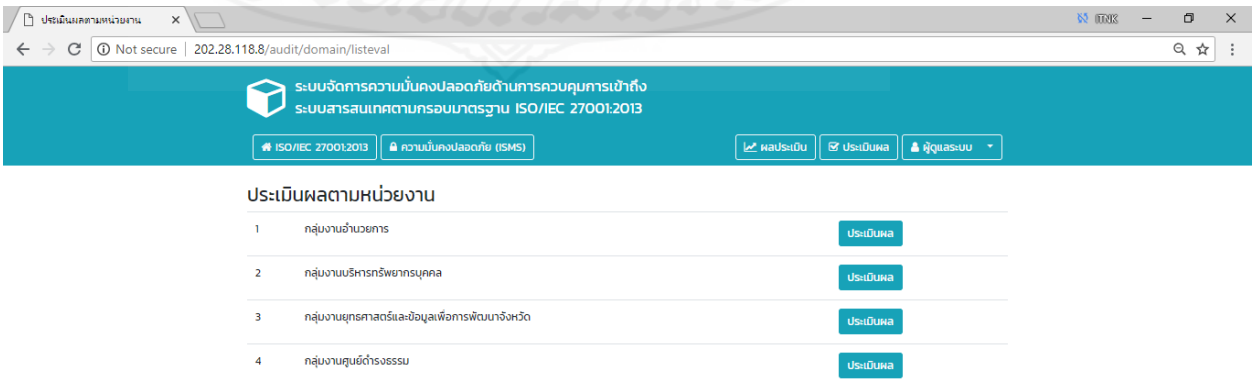
4.3 ผู้เข้าใช้งานระบบที่ได้รับอนุญาตให้ใช้งาน ต้องทำการลงชื่อเข้าใช้งานระบบทุกครั้ง และระบบจะทำการออกจากระบบโดยอัตโนมัติเมื่อไม่มีการใช้งานเป็นระยะเวลานานเกิน 10 นาที



ภาพที่ 4.4 ลงชื่อเข้าสู่ระบบ

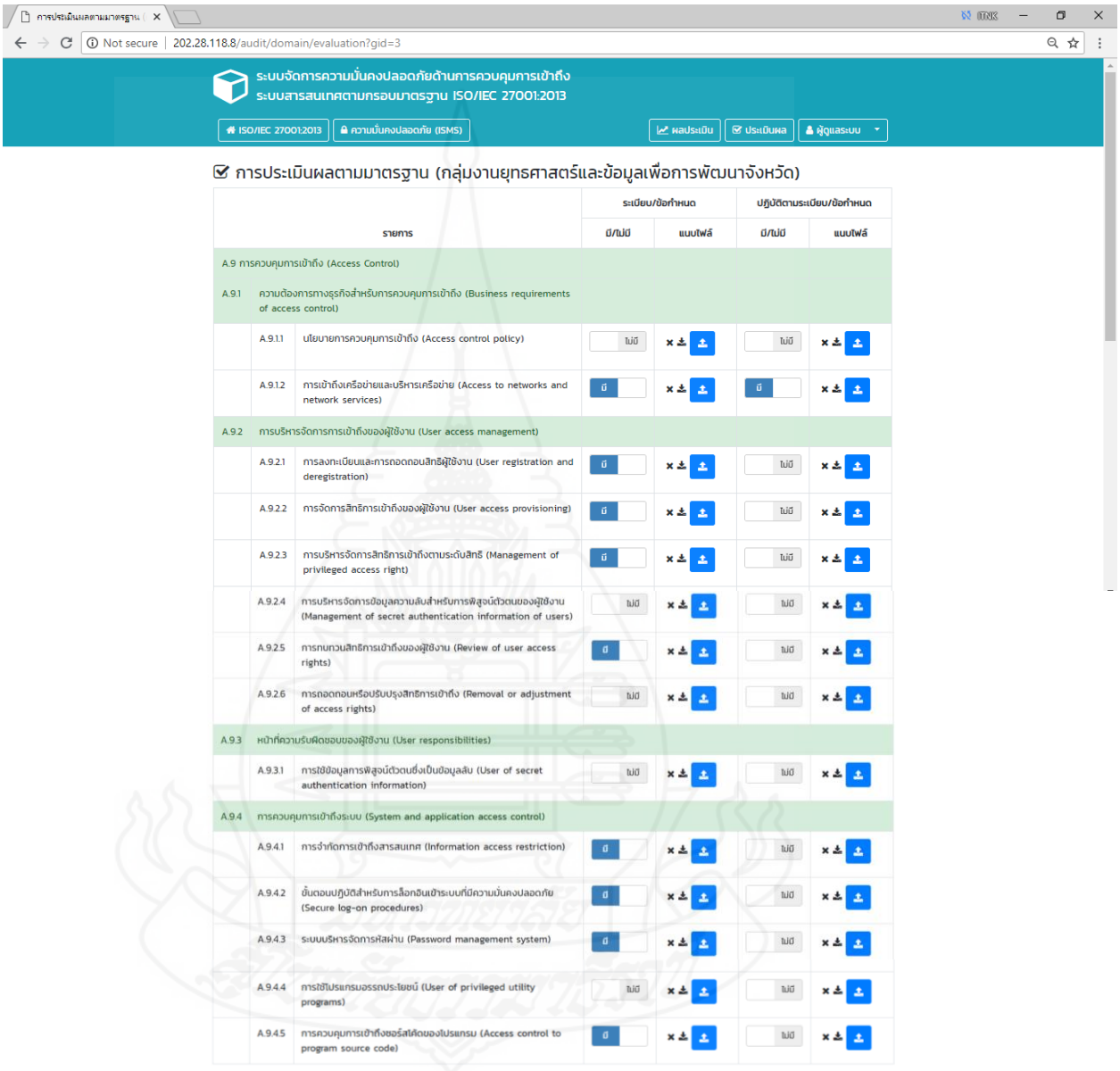


ภาพที่ 4.5 เข้าสู่ระบบ



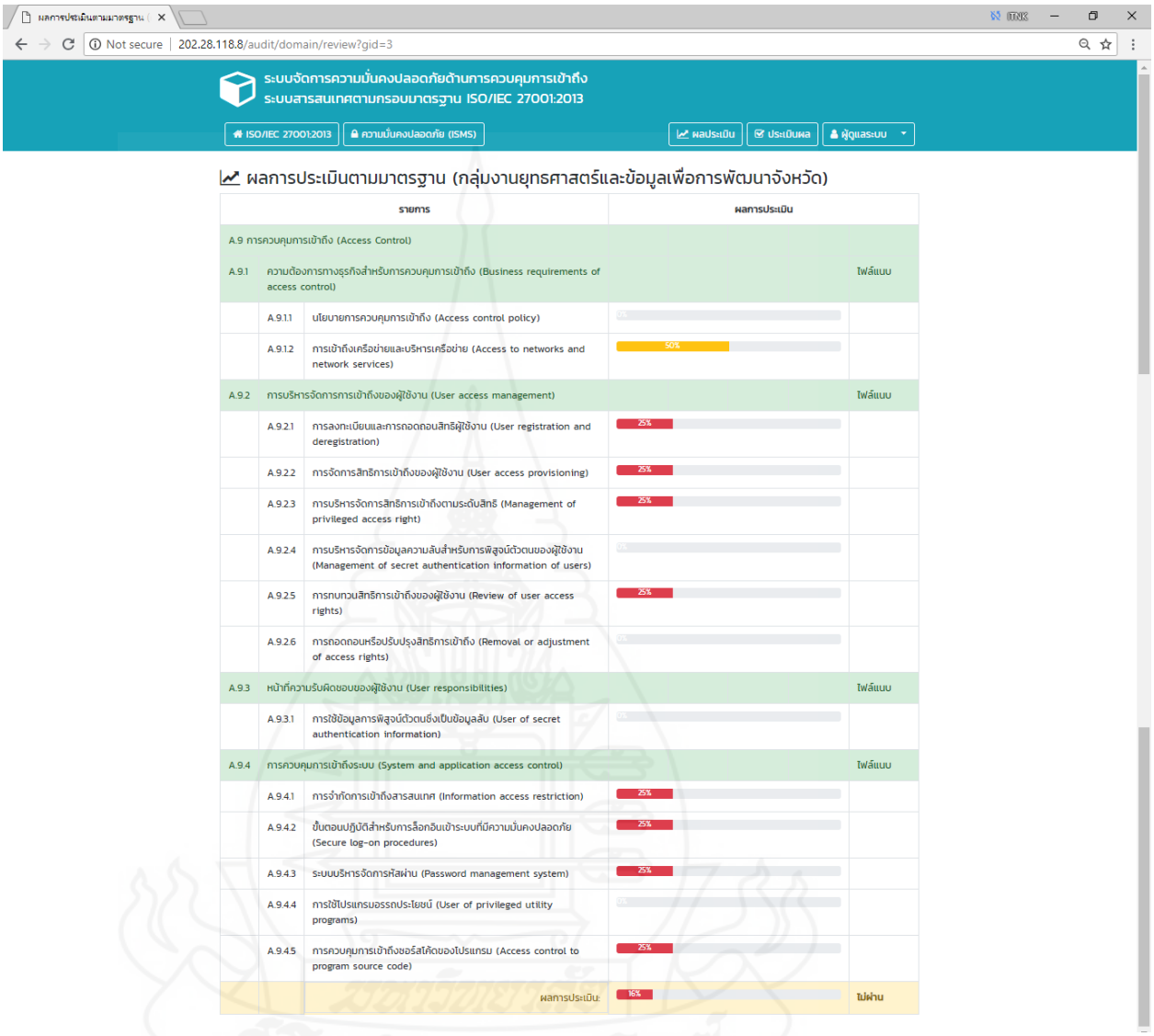
ภาพที่ 4.6 ประเมินระบบแยกตามหน่วยงาน

4.4 ผู้ใช้งานสามารถประเมินตัวเองผ่านระบบได้ด้วยตัวเอง และสามารถแนบไฟล์เอกสารที่ดำเนินการเรียบร้อยแล้วเก็บไว้ในระบบเพื่อสะดวกในการตรวจสอบต่อไป



ภาพที่ 4.7 ประเมินระบบสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศตามกรอบมาตรฐาน ISO/IEC 27001:2013

4.5 หลังจากที่กรอกข้อมูลครบถ้วนตามกรอบมาตรฐาน ระบบจะทำการประเมินผลออกมาในรูปเปอร์เซ็นต์ (%)



รายการ			ผลการประเมิน	
A.9 การควบคุมการเข้าถึง (Access Control)				
A.9.1		ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)		ไฟล์แนบ
	A.9.1.1	นโยบายการควบคุมการเข้าถึง (Access control policy)	0%	
	A.9.1.2	การเข้าถึงเครือข่ายและบริหารเครือข่าย (Access to networks and network services)	50%	
A.9.2		การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)		ไฟล์แนบ
	A.9.2.1	การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and deregistration)	25%	
	A.9.2.2	การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)	25%	
	A.9.2.3	การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)	25%	
	A.9.2.4	การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)	0%	
	A.9.2.5	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	25%	
	A.9.2.6	การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)	0%	
A.9.3		หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)		ไฟล์แนบ
	A.9.3.1	การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of secret authentication information)	0%	
A.9.4		การควบคุมการเข้าถึงระบบ (System and application access control)		ไฟล์แนบ
	A.9.4.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	25%	
	A.9.4.2	ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)	25%	
	A.9.4.3	ระบบบริหารจัดการรหัสผ่าน (Password management system)	25%	
	A.9.4.4	การใช้โปรแกรมอรรถประโยชน์ (User of privileged utility programs)	0%	
	A.9.4.5	การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)	25%	
		ผลการประเมิน:	16%	ไม่ผ่าน

ภาพที่ 4.8 สรุปผล

โดยในแต่ละข้อจะประกอบไปด้วย รายการตรวจสอบ (Checklist) ดังต่อไปนี้

- ระเบียบ/ข้อกำหนด
  - มี/แนบเอกสาร ผลการประเมินเท่ากับ 100%
  - มี/ไม่แนบเอกสาร ผลการประเมินเท่ากับ 50 %
  - ไม่มี ผลการประเมินเท่ากับ 0%

- การปฏิบัติตามระเบียบ/ข้อกำหนด
  - ปฏิบัติ/แนบเอกสาร ผลการประเมินเท่ากับ 100%
  - ปฏิบัติ/ไม่แนบเอกสาร ผลการประเมินเท่ากับ 50%
  - ไม่ปฏิบัติ ผลการประเมินเท่ากับ 0%

เมื่อทำการประเมินครบทุกข้อ ระบบสามารถแสดงสรุปผลการประเมินแยกเป็นข้อ และ % พร้อมแสดงแถบสี ดังนี้

สีเขียว	ผลการประเมิน 100%	ผ่าน
สีเหลือง	ผลการประเมิน 50 – 99%	ปรับปรุง
สีแดง	ผลการประเมิน 0 – 49%	ไม่ผ่าน

บทที่ 5

สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

1. สรุปผลการวิจัย

การพัฒนาระบบจัดการความมั่นคงปลอดภัยตามกรอบมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย มีวัตถุประสงค์เพื่อ 1. ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ตามมาตรฐาน ISO/IEC 27005 2. พัฒนากระบวนการบริหารจัดการความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC 27001 เพื่อควบคุมการเข้าถึง สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย 3. พัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ในการนี้ ผู้วิจัยจึงขอสรุปผลการวิจัยเพื่อให้สอดคล้องกับวัตถุประสงค์ของการวิจัย ดังต่อไปนี้

1.1 การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ตามมาตรฐาน ISO/IEC 27005

สรุปผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้ง 6 ด้าน ของสำนักงานจังหวัด ดังนี้

1.1.1 **กลุ่มงานอำนวยการ สินทรัพย์เกี่ยวกับงานระบบบริหารการเงินการคลังภาครัฐ (GFMIS)**

1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Process) มีทั้งหมด 11 รายการ ระดับความเสี่ยงต่ำ 10 รายการ ระดับความเสี่ยงปานกลาง 1 รายการ

2) รายการสินทรัพย์ข้อมูล (Information Assets) มีทั้งหมด 6 รายการ ระดับความเสี่ยงปานกลาง ทั้ง 6 รายการ

3) รายการสินทรัพย์ซอฟต์แวร์ (Software Assets) มีทั้งหมด 2 รายการ ระดับความเสี่ยงต่ำ ทั้ง 2 รายการ

4) รายการสินทรัพย์ฮาร์ดแวร์ (Hardware Assets) มีทั้งหมด 3 รายการ ระดับความเสี่ยงปานกลาง ทั้ง 3 รายการ

5) รายการสินทรัพย์บุคคล (Propel Assets) มีทั้งหมด 2 รายการ ระดับความเสี่ยงสูง ทั้ง 2 รายการ

6) รายการสินทรัพย์บริการโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร (Infrastructure Assets) มีทั้งหมด 6 รายการ ระดับความเสี่ยงปานกลาง 3 รายการ ระดับความเสี่ยงสูง 2 รายการ และระดับความเสี่ยงสูงมาก 1 รายการ

1.1.2 **กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สินทรัพย์เกี่ยวกับงานระบบติดตามประเมินผลแผนงาน (Padme)**

1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Process) มีทั้งหมด 9 รายการ ระดับความเสี่ยงต่ำ ทั้ง 9 รายการ

2) รายการสินทรัพย์ข้อมูล (Information Assets) มีทั้งหมด 1 รายการ ระดับความเสี่ยงปานกลาง ทั้ง 1 รายการ

3) รายการสินทรัพย์ซอฟต์แวร์ (Software Assets) มีทั้งหมด 2 รายการ ระดับความเสี่ยงต่ำ ทั้ง 2 รายการ

4) รายการสินทรัพย์ฮาร์ดแวร์ (Hardware Assets) มีทั้งหมด 3 รายการ ระดับความเสี่ยงปานกลาง ทั้ง 3 รายการ

5) รายการสินทรัพย์บุคคล (Propel Assets) มีทั้งหมด 2 รายการ ระดับความเสี่ยงสูง ทั้ง 2 รายการ

6) รายการสินทรัพย์บริการโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร (Infrastructure Assets) มีทั้งหมด 6 รายการ ระดับความเสี่ยงปานกลาง 3 รายการ ระดับความเสี่ยงสูง 2 รายการ และระดับความเสี่ยงสูงมาก 1 รายการ

1.1.3 **กลุ่มงานบริหารทรัพยากรบุคคล สินทรัพย์เกี่ยวกับงานระบบสารสนเทศทรัพยากรบุคคลระดับจังหวัด (PPIS)**

1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Process) มีทั้งหมด 14 รายการ ระดับความเสี่ยงต่ำ ทั้ง 14 รายการ

2) รายการสินทรัพย์ข้อมูล (Information Assets) มีทั้งหมด 1 รายการ ระดับความเสี่ยงปานกลาง ทั้ง 1 รายการ

3) รายการสินทรัพย์ซอฟต์แวร์ (Software Assets) มีทั้งหมด 2 รายการ ระดับความเสี่ยงต่ำ ทั้ง 2 รายการ

4) รายการสินทรัพย์ฮาร์ดแวร์ (Hardware Assets) มีทั้งหมด 3 รายการ ระดับความเสี่ยงปานกลาง ทั้ง 3 รายการ

5) รายการสินทรัพย์บุคคล (Propel Assets) มีทั้งหมด 2 รายการ ระดับความเสี่ยงสูง ทั้ง 2 รายการ

6) รายการสินทรัพย์บริการโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร (Infrastructure Assets) มีทั้งหมด 6 รายการ ระดับความเสี่ยงปานกลาง 3 รายการ ระดับความเสี่ยงสูง 2 รายการ และระดับความเสี่ยงสูงมาก 1 รายการ

1.1.4 **กลุ่มงานศูนย์ดำรงธรรมจังหวัด สินทรัพย์เกี่ยวกับงานระบบร้องเรียน ร้องทุกข์ ศูนย์ดำรงธรรมจังหวัด**

1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Process) มีทั้งหมด 9 รายการ ระดับความเสี่ยงต่ำ ทั้ง 9 รายการ

2) รายการสินทรัพย์ข้อมูล (Information Assets) มีทั้งหมด 1 รายการ ระดับความเสี่ยงปานกลาง ทั้ง 1 รายการ

3) รายการสินทรัพย์ซอฟต์แวร์ (Software Assets) มีทั้งหมด 2 รายการ ระดับความเสี่ยงต่ำ ทั้ง 2 รายการ

4) รายการสินทรัพย์ฮาร์ดแวร์ (Hardware Assets) มีทั้งหมด 3 รายการ ระดับความเสี่ยงปานกลาง ทั้ง 3 รายการ

5) รายการสินทรัพย์บุคคล (Propel Assets) มีทั้งหมด 2 รายการ ระดับความเสี่ยงสูง ทั้ง 2 รายการ

6) รายการสินทรัพย์บริการโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร (Infrastructure Assets) มีทั้งหมด 6 รายการ ระดับความเสี่ยงปานกลาง 3 รายการ ระดับความเสี่ยงสูง 2 รายการ และระดับความเสี่ยงสูงมาก 1 รายการ

ตารางที่ 5.1 สรุปผลการประเมินความเสี่ยง สำนักงานจังหวัดทั้ง 6 ด้าน

รายการสินทรัพย์	จำนวน (รายการ)	ระดับความเสี่ยง				
		สูงมาก	สูง	ปานกลาง	ต่ำ	ต่ำมาก
- กระบวนการทางธุรกิจหรือกิจกรรม (Business Process)	43	-	-	1	42	-
- ข้อมูล (Information Assets)	9	-	-	9	-	-

ตารางที่ 5.1 (ต่อ)

รายการสินทรัพย์	จำนวน (รายการ)	ระดับความเสี่ยง				
		สูงมาก	สูง	ปานกลาง	ต่ำ	ต่ำมาก
- ซอฟต์แวร์ (Software Assets)	8	-	-	-	8	-
- ฮาร์ดแวร์ (Hardware Assets)	12	-	-	12	-	-
- บุคคล (Propel Assets)	8	-	8	-	-	-
- บริการโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร (Infrastructure Assets)	24	4	8	12	-	-

หลังจากที่ทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ตามมาตรฐาน ISO/IEC 27005 ตามตารางที่ 5.1 สรุปได้ดังนี้

ระดับความเสี่ยงต่ำมาก จำนวน 0 รายการ
ระดับความเสี่ยงต่ำ จำนวน 50 รายการ
ระดับความเสี่ยงปานกลาง จำนวน 34 รายการ
ระดับความเสี่ยงสูง จำนวน 16 รายการ
ระดับความเสี่ยงสูงมาก จำนวน 4 รายการ

จะเห็นได้ว่าสถานะความเสี่ยงของสำนักงานจังหวัดในแต่ละด้านนั้นอยู่ในระดับความเสี่ยงที่ ต่ำ ถึง ปานกลาง ดังนั้น เพื่อให้สอดคล้องกับนโยบายของสำนักงานปลัดกระทรวงมหาดไทย และนโยบายของภาครัฐในระดับประเทศ ผู้วิจัยจึงได้พัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย เพื่อเป็นเครื่องมือหนึ่งที่จะช่วยในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ให้เป็นไปตามมาตรฐานขั้นต่ำที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553 ประกาศ ณ วันที่ 31 พฤษภาคม พ.ศ.2553 โดยที่การดำเนินงานดังกล่าว จะเป็นมาตรการหนึ่งที่ช่วยยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงานของรัฐ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงการดำเนินงานตามกรอบมาตรฐานสากล ISO/IEC 27001 ภายใต้

แนวทางที่เป็นมาตรฐานขั้นต่ำซึ่งเพียงพอต่อการดำเนินงาน และไม่สร้างภาระให้หน่วยงานมากเกินความจำเป็น และช่วยให้หน่วยงานสามารถลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือถูกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม ตลอดจนช่วยให้สามารถฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว

โดยในการพัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ที่จัดทำขึ้นในครั้งนี้ มีวัตถุประสงค์เพื่อ ใช้งานในองค์กรเพื่อใช้เป็นต้นแบบ โดยได้ทำการทดสอบและประเมินความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของสำนักงานจังหวัด โดย นักวิชาการคอมพิวเตอร์ของสำนักงานจังหวัด ซึ่งระบบสามารถใช้งานได้และสามารถประมวลผลได้ตามความต้องการ แต่มีข้อจำกัดที่ระบบถูกพัฒนามาเพื่อเป็นการประเมินเบื้องต้น ว่าเอกสารครบถ้วนตามกรอบมาตรฐาน ISO/IEC 27001 หรือไม่ ส่วนคุณภาพของเอกสาร ผู้รับผิดชอบต้องตรวจสอบอีกครั้งว่าคุณภาพครบตามแนวทางและมาตรฐานที่กำหนดหรือไม่

ตารางที่ 5.2 ผลการทดสอบการประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO 27001 ด้านการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

ลำดับ	หัวข้อประเมิน	คุณภาพ (ร้อยละ)	หมายเหตุ
1	**ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)**		
1.1	นโยบายการควบคุมการเข้าถึง (Access control policy)	0	- ไม่มีการกำหนดสิทธิ ระยะเวลาการให้อำนาจในการเข้าออกพื้นที่เพื่อควบคุมการเข้าถึง - ไม่มีนโยบายควบคุมการเข้าถึงระบบสารสนเทศจากผู้บริหาร - ไม่มีแนวทางการจัดทำนโยบายควบคุมการเข้าถึงระบบสารสนเทศ แต่ผู้ปฏิบัติงานปฏิบัติตามขอบเขตงานตนเอง

ตารางที่ 5.2 (ต่อ)

ลำดับ	หัวข้อประเมิน	คุณภาพ (ร้อยละ)	หมายเหตุ
1.2	การเข้าถึงเครือข่ายและบริหารเครือข่าย (Access to networks and network services)	50	- มีการพิสูจน์ตัวจริงบนเครือข่าย แต่ยังไม่ครอบคลุมทุกอุปกรณ์ - ไม่มีนโยบายและแนวทางการเข้าถึงเครือข่ายและบริการเครือข่าย
2	**การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)**		
2.1	การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and deregistration)	25	- ขาดการควบคุม ให้ / ถอน สิทธิการใช้งานอย่างเป็นทางการ - ไม่มีนโยบายและแนวทางการลงทะเบียนและถอดถอนสิทธิ์ - ไม่มีการแสดงตารางสิทธิในการเข้าถึงระบบ - ไม่มีแนวทางการปฏิบัติการเพิกถอนลงทะเบียนสิทธิผู้ใช้งานและรายงานการเพิกถอนทะเบียน
2.2	การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)	25	- ทำตามดุลพินิจของผู้ดูแลระบบโดยผู้บริหารไม่จำเป็นต้องอนุมัติ - ไม่มีนโยบายและแนวทางการจัดการสิทธิการเข้าถึงของผู้ใช้งาน
2.3	การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)	25	- มีการจัดลำดับความสำคัญในการเข้าถึงข้อมูลของผู้ใช้แต่ละระดับโดยผู้ดูแลระบบ - ไม่มีนโยบายการบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ

ตางรางที่ 5.2 (ต่อ)

ลำดับ	หัวข้อประเมิน	คุณภาพ (ร้อยละ)	หมายเหตุ
2.4	การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)	0	- ไม่มีกระบวนการการควบคุมการมอบข้อมูลการพิสูจน์ตัวจริงของผู้ใช้งาน - ไม่มีนโยบายการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน
2.5	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	25	- มีการทบทวนสิทธิ์ แต่ไม่ได้กำหนดเวลาไว้อย่างชัดเจน - ไม่มีนโยบายและแนวทางการทบทวนสิทธิการเข้าถึงผู้ใช้งาน - ไม่มีการรายงานการสอบทานรายชื่อผู้ใช้
2.6	การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)	0	- ไม่มีการระบุขั้นตอนปรับปรุงสิทธิการเข้าถึงอย่างเป็นทางการ - ไม่มีนโยบายและแนวทางการถอดถอนและสิทธิการใช้งาน
3	**หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)**		
3.1	การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of secret authentication information)	0	- ไม่ได้กำหนดวิธีปฏิบัติการใช้ข้อมูลการพิสูจน์ตัวจริงซึ่งเป็นความลับ - ไม่มีรายงานการถอดถอนสิทธิ - ไม่มีนโยบายการใช้งานข้อมูลการพิสูจน์ตัวตน ซึ่งเป็นข้อมูลลับ

ตารางที่ 5.2 (ต่อ)

ลำดับ	หัวข้อประเมิน	คุณภาพ (ร้อยละ)	หมายเหตุ
4	**การควบคุมการเข้าถึงระบบ (System and application access control)**		
4.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	25	- มีการกำหนดรหัสผ่านการเข้าใช้งานระบบสารสนเทศ - ไม่มีนโยบายการจำกัดการเข้าถึงระบบสารสนเทศ
4.2	ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)	25	- เป็นที่รับทราบเฉพาะผู้ดูแลระบบสำหรับขั้นตอนการล็อกอินเข้าระบบ - ไม่มีนโยบายและแนวทางสำหรับการล็อกอินเข้าระบบ ที่มีความมั่นคงปลอดภัย
4.3	ระบบบริหารจัดการหัสผ่าน (Password management system)	25	- มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน แต่ไม่เป็นทางการ - ไม่มีนโยบายและแนวทางการบริหารจัดการรหัสผ่าน
4.4	การใช้โปรแกรมอรรถประโยชน์ (User of privileged utility programs)	0	- ไม่มีการควบคุมการใช้งาน การติดตั้งโปรแกรมอรรถประโยชน์ - ไม่มีนโยบายและแนวทางการใช้และขอติดตั้งโปรแกรมอรรถประโยชน์ - ไม่มีแบบฟอร์มขอติดตั้งโปรแกรมอรรถประโยชน์

ตารางที่ 5.2 (ต่อ)

ลำดับ	หัวข้อประเมิน	คุณภาพ (ร้อยละ)	หมายเหตุ
4.5	การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)	25	- มีการควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ กำหนดการเข้ารหัสและรหัสผ่าน - ไม่มีนโยบายและแนวทางการควบคุมการเข้าถึงซอสโค้ดของโปรแกรม - ไม่มีแบบฟอร์มร้องขอการเปลี่ยนแปลง

จากการประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ สำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ตามมาตรฐาน ISO 27001 ด้านการควบคุมการเข้าถึงระบบสารสนเทศ (Access control) โดยผลของการประเมินอยู่ที่ ร้อยละ 16 ซึ่งถือว่าอยู่ในเกณฑ์ที่ต่ำมาก และส่งผลให้ทราบว่ารายการใดบ้างที่หน่วยงานต้องรีบดำเนินการ หรือปรับปรุงแก้ไขเพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์กรมีความปลอดภัยมากยิ่งขึ้น และเป็นไปตามมาตรฐานสากล

จะเห็นได้ว่าการพัฒนาระบบจัดการความมั่นคงปลอดภัยด้านตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย จะช่วยให้หน่วยงานมีแบบแผนในการดำเนินงานอย่างเป็นระบบ และส่งผลให้สามารถลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือถูกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม ตลอดจนช่วยให้สามารถฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว ซึ่งงานวิจัยนี้สามารถนำไปใช้เป็นต้นแบบให้กับส่วนราชการอื่น ๆ และนำไปเป็นกรณีศึกษาถึงแนวทางการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศในเชิงการนำไปปฏิบัติจริงให้เกิดผล เพื่อรองรับกับสถานการณ์ที่จะเกิดขึ้นทั้งในปัจจุบันและอนาคต เนื่องจากโลกมีการขับเคลื่อนด้วยเทคโนโลยีและการเชื่อมโยงถึงกันด้วยความเร็วสูง การละเมิดข้อมูลการจู่โจมทางไซเบอร์ยังคงเป็นการจู่โจมที่มีนัยสำคัญต่อองค์กร และการขาดความตระหนักในเรื่องของความเสี่ยงก็ยังคงเป็นสิ่งที่ต้องถูกตำหนิ การปกป้องความมั่นคงปลอดภัยของข้อมูล จึงเป็นสิ่งที่ต้องทำภายใต้การดูแลให้ความสำคัญอย่างใกล้ชิด

จึงสรุปได้ว่า ระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ส่งผลให้หน่วยงานสามารถปฏิบัติตามนโยบายของรัฐบาลได้อย่างเป็นรูปธรรม และถือเป็นแนวทางปฏิบัติที่ดีในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2. อภิปรายผล

จากการที่ได้ทำการวิจัยและพัฒนาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทยนั้น การพัฒนาตามการวิจัยดังกล่าว สอบคล้องกับผลการศึกษาของ สุพรรณี ชาติสุข (2556) ที่ได้ทำการวิเคราะห์และประเมินความเสี่ยงด้านมาตรฐาน ISO/IEC 27001 เพื่อบริหารจัดการระบบเทคโนโลยีสารนเทศภายในองค์กร กรณีศึกษาศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค เพื่อตรวจสอบช่องโหว่/จุดอ่อนของระบบเทคโนโลยีสารสนเทศและต้องการให้ทราบถึงระดับความเสี่ยง/ภัยคุกคาม เพื่อนำมาพัฒนาปรับปรุงร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ, กรกฎ สราญสุทธิ์ (2556) ได้พัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001 ของกรมทรพยากรน้ำบาดาล เพื่อดำเนินการจัดการความเสี่ยง โดยจัดทำนโยบายด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 ให้กรมทรัพยากรน้ำบาดาล, ประกิจ อินทรักษ์ (2556) พัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001:2005 กรณีศึกษาสำหรับ สถาบันวิจัยแห่งหนึ่ง เพื่อใช้เป็นแนวทางในการปฏิบัติงาน รวมถึงการวิเคราะห์ และการประเมินความเสี่ยงให้กับองค์กร เพื่อให้องค์กรได้ทราบถึงระดับของความเสี่ยงที่องค์กรมีอยู่ และจัดทำแผนการบริหารจัดการความเสี่ยงลดระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ และไพศาล จันทร์เลื่อน (2557) ได้พัฒนาความความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO 27001 กรณีศึกษา ศูนย์พัฒนาและบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพระนคร เพื่อลดความเสี่ยงที่จะเกิดขึ้นกับหน่วยงาน

สำหรับการดำเนินการทั้งหมด ส่งผลให้สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย มีเครื่องมือในการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ให้เป็นไปตามมาตรฐานขั้นต่ำที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้ และเพื่อให้สอดคล้องกับนโยบายของสำนักงานปลัดกระทรวงมหาดไทย และนโยบายของภาครัฐในระดับประเทศ

3. ข้อเสนอแนะ

จากการวิจัยดังกล่าว ผู้วิจัยจึงมีข้อเสนอแนะว่า

3.1 หน่วยงานควรเร่งจัดทำระบบบริหารความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สามารถรองรับเหตุการณ์ด้านความมั่นคงปลอดภัยภายในองค์กร รวมทั้งเพื่อให้บุคลากรในหน่วยงานทราบถึงรูปแบบการดำเนินการที่เป็นรูปธรรม รวมถึงระเบียบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดย มอบหมายผู้รับผิดชอบในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานอย่างเป็นรูปธรรม และดำเนินการดังต่อไปนี้

3.1.1 แต่งตั้งคณะกรรมการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ
และการสื่อสาร

3.1.2 กำหนดนโยบายหรือแนวทางการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

3.1.3 แต่งตั้งคณะทำงานบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อดำเนินการดังต่อไปนี้

1) กำหนดโครงสร้างการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2) ดำเนินการตามกระบวนการบริหารความเสี่ยงด้านระบบสารสนเทศ คือ

(1) ระบุความเสี่ยง

(2) วิเคราะห์และประเมินความเสี่ยง

(3) จัดลำดับความสำคัญของปัจจัยเสี่ยง

(4) กำหนดกิจกรรมบริหารความเสี่ยง

(5) จัดทำแผนบริหารความเสี่ยงของแต่ละปัจจัยเสี่ยงที่อยู่ในระดับที่มีนัยสำคัญ

(6) สื่อสารทำความเข้าใจเกี่ยวกับแผนบริหารความเสี่ยงให้บุคลากรของหน่วยงาน เพื่อให้สามารถนำไปปฏิบัติได้จริง

(7) รายงานสรุปผล ข้อดีข้อเสีย ปัญหา อุปสรรค และข้อเสนอแนะของการดำเนินการตามแผนบริหารความเสี่ยงต่อประธานคณะกรรมการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

3.2 หน่วยงานราชการต่างๆ สามารถนำกรอบวิธีปฏิบัตินี้ไปประยุกต์ใช้กับหน่วยงานได้

ทั้งนี้ สำหรับการนำเอามาตรฐาน ISO/IEC 27001 เข้ามาใช้ในหน่วยงานนั้นต้องได้รับการสนับสนุน เห็นชอบจากผู้บริหารระดับสูงของหน่วยงานเนื่องจากปัญหาที่เกิดขึ้นในองค์กรส่วนใหญ่ก็คือ ผู้บริหารระดับสูงมักจะมอง “IT Risk” เป็นเรื่องของฝ่ายเทคโนโลยีสารสนเทศโดยมองเป็นเรื่องเทคนิคเพียงอย่างเดียวแต่ไม่มองถึงผลกระทบจากความเสี่ยงที่เกิดจากการใช้งานระบบสารสนเทศอย่างไม่ปลอดภัย หรือไม่ได้ให้ความสนใจเพียงพอกับเรื่องความมั่นคงปลอดภัยสารสนเทศหรือ “Information Security” ขณะนี้เป็นที่ยอมรับกันทั่วโลกแล้วว่า เรื่องความมั่นคงปลอดภัยสารสนเทศนั้น มีความสำคัญและมีส่วนเกี่ยวข้องโดยตรงกับความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร และต้องได้รับความความร่วมมือจากบุคคลากรของหน่วยงานทุกระดับชั้นด้วย

บรรณานุกรม

บรรณานุกรม

กรกฎ สราญสุทธิ์. (2556). *นโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO27001 ของกรมทรัพยากรน้ำบาดาล* (สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช. (2554). *แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ*. สืบค้นจาก www.dnp.go.th/isms/ISMS2557.pdf

การแบ่งส่วนราชการสำนักงานปลัดกระทรวงมหาดไทย พ.ศ. 2559 สืบค้นจาก www.moi.go.th

จุติชัย ทองกระจาย. (2557). *ระบบตรวจจับการบุกรุกเครือข่ายกรณีศึกษา บริษัท เวนด้า ซอฟแวร์ดีเวลอปเมนท์ จำกัด* (สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

ณัทรัฏฐ์ มณีรัสยากร. (2559). *ทำการศึกษาและพัฒนานโยบายด้านความปลอดภัยภายใต้มาตรฐาน ISO27001 ของ บริษัท เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น จำกัด*. (สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

ธนภัทร์ นรเศรษฐ์ตระกูล. (2557). *การควบคุมการเข้าถึงข้อมูลและระบบข้อมูลสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย*

ธนวรรธน์ ว่องพิบูลย์. (2559). *ศึกษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงภายใต้มาตรฐาน ISO/IEC 27001:2013 ของ บริษัท แปซิฟิค เฮลธ์แคร์ (ไทยแลนด์) จำกัด.* (สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

นโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย สืบคืนจาก http://ictsgp.moi.go.th/ictsgp/ICTsecurity.php

บริษัท ที-เน็ต จำกัด. (2556). *เอกสารเผยแพร่ มาตรฐาน ISO/IEC 27001:2013,* สืบคืนจาก http://www.tnetsecurity.com/content_audit/27001-2013.pdf

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553

แผนปฏิบัติการดิจิทัลศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย พ.ศ.2557 – 2561

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544. ราชกิจจานุเบกษา. เล่ม 118. ตอนที่ 112ก. หน้า 26. วันที่ 4 ธันวาคม 2544.

พระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. 2495. ราชกิจจานุเบกษา. เล่ม 69. ตอนที่ 16. หน้า 286. วันที่ 11 มีนาคม 2495.

พลสิริ วรรณวิโรจน์. (2556). *ระดับอิทธิพลของมาตรการการจัดการความมั่นคงปลอดภัยตามกรอบมาตรฐาน ISO/IEC 27001 ต่อการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ บริษัท วี จี ไอ โกลบอล มีเดีย จำกัด (มหาชน)* (วิทยานิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยรังสิต, กรุงเทพฯ.

ไพศาล จันทร์เลื่อน. (2557). *การพัฒนาความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO 27001 กรณีศึกษา ศูนย์พัฒนาและบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพระนคร* (สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

ประกิจ อินทรักษ์. (2556). *นโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001:2005 กรณีศึกษาสำหรับ สถาบันวิจัยแห่งหนึ่ง* (สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

ระบบบริหารจัดการความปลอดภัยสำหรับสารสนเทศ สืบค้นจาก http://prowcharinrat.blogspot.com/

รัตนา จรุญศักดิ์สิทธิ์. (2557). *การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ภายใต้ พรบ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544*. กรุงเทพฯ สืบค้นจาก http://www.mdes.go.th

วีระวัฒน์ จิรัญดร. (2556). *การยอมรับกรอบมาตรฐาน ISO/IEC 27001 เพื่อการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศของมหาวิทยาลัยเอกชนในกรุงเทพมหานครและปริมณฑล* (วิทยานิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยรังสิต, กรุงเทพฯ.

สุพรรณี ชาติสุข. (2556). *วิเคราะห์และประเมินความเสี่ยงด้วยมาตรฐาน ISO/IEC 27001 เพื่อบริหารจัดการระบบเทคโนโลยีสารสนเทศภายในองค์กร กรณีศึกษาศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค* (สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยธุรกิจบัณฑิตย์, กรุงเทพฯ.

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2557). *คู่มือการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ*. กรุงเทพฯ. สืบค้นจาก http://www.mdes.go.th

อัจฉรา เวียงสิมา. (2559). *การทบทวนและพัฒนานโยบายการบริหารจัดการความมั่นคงของระบบสารสนเทศภายใต้มาตรฐาน ISO/IEC 27001:2013*. (สารนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ

อัจฉรินทร์ พัฒนพันธ์ชัยและคณะ. (2559). *นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร*. สืบค้นจาก http://www.boi.go.th/upload/%E0...A2_ICT_(P_IT_SP_01)_37229.pdf.

Club27001 Information Security สืบค้นจาก http://www.club27001.com/2013/08/normal-0-false-false-false-en-us-x-none.html

International Standard ISO/IEC 27001 First edition 2005-10-15 Information technology – Security techniques – information security management systems – Requirements

International Strandard ISO/IEC 27001 Information technology – Secrity techniques – Information security management systems - Requirements

ISO สืบค้นจาก https://www.iso.org

Kuo-Hsiung Liao, Hao-En Chueh. (2555). Medical Organization Information Security Management Based on ISO27001 Information Security Standard Information Management Department. JOURNAL OF SOFTWARE, 7(4), 792-797.

BSI UK. (2013). ISO/IEC 27001 Mapping guide, United kingdom. Retrived 31 August 2014. From http://bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf

ภาคผนวก

4.2.1 ทะเบียนสินทรัพย์และกำหนดค่าของสินทรัพย์ (Asset Identification and Valuation

4.2.1.1 กลุ่มงานอำนวยการ สินทรัพย์เกี่ยวกับงานระบบ คือ ระบบการบริหารงานการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ หรือ ระบบGFMIS

(1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-1-1-1	รับเอกสารการเบิกจากหน่วยตรวจ		1					1				3	3			2	1	1	3	ผอ.อำนวยการ
1-1-1-2	จัดทำใบสำคัญตั้งหนี้ (PV) และใบสำคัญจ่าย (DV) ผ่านระบบ ERP		1					1				3		1		1	1	1	3	ผอ.อำนวยการ
1-1-1-3	เสนอหัวหน้างานการเงินและหัวหน้าสำนักงานจังหวัดลงนามอนุมัติ							3					3				0	3	3	ผอ.อำนวยการ
1-1-1-4	จัดทำทะเบียนบันทึก		1					1				3		1		1	1	1	3	ผอ.อำนวยการ
1-1-1-5	ดำเนินการขอเบิก							3				3	3				0	3	3	ผอ.อำนวยการ
1-1-1-6	อนุมัติการขอเบิก							3				3	3				0	3	3	ผอ.อำนวยการ
1-1-17	ตรวจสอบการประมวลสั่งจ่ายเงิน							3				3	3				0	3	3	ผอ.อำนวยการ
1-1-1-8	จัดทำเช็คและทะเบียนการจ่ายเช็คพร้อมหนังสือรังรองภาษีหัก ณ ที่จ่าย							3				3	3				0	3	3	ผอ.อำนวยการ
1-1-1-9	ดำเนินการจ่ายเช็คให้กับผู้มีสิทธิ							3		3		3	3				0	3	3	ผอ.อำนวยการ
1-1-1-10	ดำเนินการขอจ่าย (PM53)							3					3				0	3	3	ผอ.อำนวยการ
1-1-1-11	ประทับตรา "จ่ายเงินแล้ว" พร้อมลงลายมือชื่อและวันเดือนปีที่จ่ายเงิน ในเอกสารการเบิก							3					3				0	3	3	ผอ.อำนวยการ

(2) รายการสินทรัพย์ประเภทข้อมูลสารสนเทศ (Information Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-1-2-1	เอกสารการเบิก							3					3				0	3	3	ผอ.อำนวยการ
1-1-2-2	ใบสำคัญตั้งหนี้ (PV)							3					3				0	3	3	ผอ.อำนวยการ
1-1-2-3	ใบสำคัญจ่าย (DV)							3					3				0	3	3	ผอ.อำนวยการ
1-1-2-4	ทะเบียนการจ่ายเช็ค							3					3				0	3	3	ผอ.อำนวยการ
1-1-2-5	เช็ค							3		4			3				0	4	3	ผอ.อำนวยการ
1-1-2-6	หนังสือรับรองภาษีหัก ณ ที่จ่าย							3					3				0	0	3	ผอ.อำนวยการ

(3) รายการสินทรัพย์ประเภทซอฟต์แวร์ (Software Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-1-3-1	Microsoft Windows 8.1											3					0	0	3	ผอ.อำนวยการ
1-1-3-2	Micorsoft Office 2013											3					0	0	3	ผอ.อำนวยการ

(4) รายการสินทรัพย์ประเภทฮาร์ดแวร์ (Hardware Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-1-4-1	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ											3					0	0	3	ผอ.อำนวยการ
1-1-4-2	เครื่องปริ้นเตอร์											3					0	0	3	ผอ.อำนวยการ
1-1-4-3	เครื่องแสกนเนอร์											3					0	0	3	ผอ.อำนวยการ

(5) รายการสินทรัพย์ประเภทบุคลากร (People Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-1-5-1	นักวิชาการเงินและบัญชี											3					0	0	3	ผอ.อำนวยการ
1-1-5-2	เจ้าพนักงานการเงินและบัญชี											3					0	0	3	ผอ.อำนวยการ

(6) รายการสินทรัพย์ประเภทโครงสร้างพื้นฐาน (Infrastructure Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-1-6-1	ห้องกลุ่มงานอำนวยการ	2	2									3	2				2	0	3	ผอ.อำนวยการ
1-1-6-2	ระบบไฟฟ้า											3					0	0	3	ผอ.อำนวยการ
1-1-6-3	ระบบโทรศัพท์											2					0	0	2	ผอ.อำนวยการ
1-1-6-4	ระบบอินเทอร์เน็ต											3					0	0	3	ผอ.อำนวยการ
1-1-6-5	ระบบเครื่องปรับอากาศ											1					0	0	1	ผอ.อำนวยการ
1-1-6-6	อุปกรณ์ดับเพลิง						4	4	4	4	4	4	4	4	4	4	0	4	4	ผอ.อำนวยการ

4.2.1 ทะเบียนสินทรัพย์และกำหนดค่าของสินทรัพย์ (Asset Identification and Valuation

4.2.1.2 กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สินทรัพย์เกี่ยวกับงานระบบ คือ ระบบติดตามประเมินผลแผนงาน (Padme)

(1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C					I					A					C	I	A	
		เมื่อสินทรัพย์สูญเสียความลับ					เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน								
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-2-1-1	รับเอกสารโครงการ							3					3				0	3	3	ผอ.ยุทธศาสตร์
1-2-1-2	บันทึกข้อมูลแผนงาน/โครงการ							3					3				0	3	3	ผอ.ยุทธศาสตร์
1-2-1-3	บันทึกข้อมูลรายละเอียดแผนงาน/โครงการ							3					3				0	3	3	ผอ.ยุทธศาสตร์
1-2-1-4	บันทึกข้อมูลรายการเบิกจ่ายงบประมาณ							3					3				0	3	3	ผอ.ยุทธศาสตร์
1-2-1-5	บันทึกข้อมูลเอกสาร/รูปภาพประกอบ							3					3				0	3	3	ผอ.ยุทธศาสตร์
1-2-1-6	บันทึกข้อมูลปัญหา ข้อเสนอแนะ ข้อสั่งการ							3					3				0	3	3	ผอ.ยุทธศาสตร์
1-2-1-7	บันทึกข้อมูลผลการตรวจสอบข้อมูล							3					3				0	3	3	ผอ.ยุทธศาสตร์
1-2-1-8	บันทึกข้อมูลเงินเหลือจ่าย							3					3				0	3	3	ผอ.ยุทธศาสตร์
1-2-1-9	รายงานผู้บริหาร							3					3				0	3	3	ผอ.ยุทธศาสตร์

(2) รายการสินทรัพย์ประเภทข้อมูลสารสนเทศ (Information Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-2-2-1	ข้อมูลโครงการ							3					3				0	3	3	ผอ.ยุทธศาสตร์

(3) รายการสินทรัพย์ประเภทซอฟต์แวร์ (Software Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-2-3-1	Microsoft Windows 8.1											3					0	0	3	ผอ.ยุทธศาสตร์
1-2-3-2	Micorsoft Office 2013											3					0	0	3	ผอ.ยุทธศาสตร์

(4) รายการสินทรัพย์ประเภทฮาร์ดแวร์ (Hardware Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-2-4-1	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ											3					0	0	3	ผอ.ยุทธศาสตร์
1-2-4-2	เครื่องปริ้นเตอร์											3					0	0	3	ผอ.ยุทธศาสตร์
1-2-4-3	เครื่องแสกนเนอร์											3					0	0	3	ผอ.ยุทธศาสตร์

(5) รายการสินทรัพย์ประเภทบุคลากร (People Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-2-5-1	นักวิเคราะห์นโยบายและแผน											3					0	0	3	ผอ.ยุทธศาสตร์
1-2-5-2	พนักงานวิเคราะห์นโยบายและแผน											3					0	0	3	ผอ.ยุทธศาสตร์

(6) รายการสินทรัพย์ประเภทโครงสร้างพื้นฐาน (Infrastructure Assets) Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-2-6-1	ห้องกลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด	2	2									3	2				2	0	3	ผอ.ยุทธศาสตร์
1-2-6-2	ระบบไฟฟ้า											1					0	0	1	ผอ.ยุทธศาสตร์
1-2-6-3	ระบบโทรศัพท์											2					0	0	2	ผอ.ยุทธศาสตร์
1-2-6-4	ระบบอินเทอร์เน็ต											2					0	0	2	ผอ.ยุทธศาสตร์
1-2-6-5	ระบบเครื่องปรับอากาศ											1					0	0	1	ผอ.ยุทธศาสตร์
1-2-6-6	อุปกรณ์ดับเพลิง						4	4	4	4	4	4	4	4	4	4	0	4	4	ผอ.ยุทธศาสตร์

4.2.1 ทะเบียนสินทรัพย์และกำหนดค่าของสินทรัพย์ (Asset Identification and Valuation

4.2.1.3 กลุ่มงานบริหารทรัพยากรบุคคล สินทรัพย์เกี่ยวกับงานระบบ คือ ระบบสารสนเทศทรัพยากรบุคคลระดับจังหวัด(PPIS)

(1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-3-1-1	รับเอกสาร กพ.7							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-2	บันทึกข้อมูลบุคคล							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-3	บันทึกข้อมูลการบรรจุ/แต่งตั้ง/โอน							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-4	บันทึกข้อมูลการย้าย/เลื่อนตำแหน่ง							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-5	บันทึกข้อมูลเงินเดือน							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-6	บันทึกข้อมูลการออกจากราชการ							3					3				0	3	3	ผอ.ทรัพยากร
1-3-2-7	บันทึกข้อมูลการลา/สาย							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-8	บันทึกข้อมูลการดำเนินการทางวินัย							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-9	บันทึกข้อมูลการศึกษาต่อ/ฝึกอบรม							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-10	บันทึกข้อมูลหนังสือรับรอง							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-11	บันทึกข้อมูลการถ่ายโอนข้อมูล							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-12	บันทึกข้อมูลระบบจ่ายตรงค่ารักษาพยาบาล							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-13	บันทึกข้อมูลการรักษาราชการแทน/รักษาการในตำแหน่งช่วยราชการ							3					3				0	3	3	ผอ.ทรัพยากร
1-3-1-14	รายงานผู้บริหาร							3					3				0	3	3	ผอ.ทรัพยากร

(2) รายการสินทรัพย์ประเภทข้อมูลสารสนเทศ (Information Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-3-2-1	ข้อมูล กพ.7							3					3				0	3	3	ผอ.ทรัพยากร

(3) รายการสินทรัพย์ประเภทซอฟต์แวร์ (Software Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-3-3-1	Microsoft Windows 8.1											3					0	0	3	ผอ.ทรัพยากร
1-3-3-2	Micorsoft Office 2013											3					0	0	3	ผอ.ทรัพยากร

(4) รายการสินทรัพย์ประเภทฮาร์ดแวร์ (Hardware Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-3-4-1	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ											3					0	0	3	ผอ.ทรัพยากร
1-3-4-2	เครื่องปริ้นเตอร์											3					0	0	3	ผอ.ทรัพยากร
1-3-4-3	เครื่องแสกนเนอร์											3					0	0	3	ผอ.ทรัพยากร

(5) รายการสินทรัพย์ประเภทบุคลากร (People Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-3-5-1	นักทรัพยากรบุคคล											3					0	0	3	ผอ.ทรัพยากร
1-3-5-2	พนักงานทรัพยากรบุคคล											3					0	0	3	ผอ.ทรัพยากร

(6) รายการสินทรัพย์ประเภทโครงสร้างพื้นฐาน (Infrastructure Assets) Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-3-6-1	ห้องกลุ่มงานบริหารทรัพยากรบุคคล	2	2									3	2				2	0	3	ผอ.ทรัพยากร
1-3-6-2	ระบบไฟฟ้า											1					0	0	1	ผอ.ทรัพยากร
1-3-6-3	ระบบโทรศัพท์											2					0	0	2	ผอ.ทรัพยากร
1-3-6-4	ระบบอินเทอร์เน็ต											2					0	0	2	ผอ.ทรัพยากร
1-3-6-5	ระบบเครื่องปรับอากาศ											1					0	0	1	ผอ.ทรัพยากร
1-3-6-6	อุปกรณ์ดับเพลิง						4	4	4	4	4	4	4	4	4	4	0	4	4	ผอ.ทรัพยากร

4.2.1 ทะเบียนสินทรัพย์และกำหนดค่าของสินทรัพย์ (Asset Identification and Valuation

4.2.1.4 กลุ่มงานศูนย์ดำรงธรรมจังหวัด คือ ระบบร้องเรียน ร้องทุกข์ ศูนย์ดำรงธรรมจังหวัด

(1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C					I					A					C	I	A	
		เมื่อสินทรัพย์สูญเสียความลับ					เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน								
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-4-1-1	รับเรื่องร้องเรียน/ร้องทุกข์							3					3				0	3	3	ผอ.ดำรงธรรม
1-4-1-2	ปริ้นเอกสารเรื่องร้อนเรียน/ร้องทุกข์							3					3				0	3	3	ผอ.ดำรงธรรม
1-4-1-3	ลงรับเรื่องร้องเรียน/ร้องทุกข์							3					3				0	3	3	ผอ.ดำรงธรรม
1-4-1-4	วินิจฉัยประเด็น							3					3				0	3	3	ผอ.ดำรงธรรม
1-4-1-5	สรุปประเด็นแจ้งส่วนราชการที่เกี่ยวข้อง							3					3				0	3	3	ผอ.ดำรงธรรม
1-4-1-6	รับรายงานผลการร้องเรียน							3					3				0	3	3	ผอ.ดำรงธรรม
1-4-1-7	เสนอผู้ว่าราชการจังหวัด							3					3				0	3	3	ผอ.ดำรงธรรม
1-4-1-8	ยุติเรื่องร้องเรียน/ร้องทุกข์							3					3				0	3	3	ผอ.ดำรงธรรม
1-4-1-9	รายงาน ปมท.และผู้ร้อง							3					3				0	3	3	ผอ.ดำรงธรรม

(2) รายการสินทรัพย์ประเภทข้อมูลสารสนเทศ (Information Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-4-2-1	ข้อมูลเรื่องร้องเรียนร้องทุกข์							3					3				0	3	3	ผอ.ดำรงธรรม

(3) รายการสินทรัพย์ประเภทซอฟต์แวร์ (Software Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-4-3-1	Microsoft Windows 8.1											3					0	0	3	ผอ.ดำรงธรรม
1-4-3-1	Micorsoft Office 2013											3					0	0	3	ผอ.ดำรงธรรม

(4) รายการสินทรัพย์ประเภทฮาร์ดแวร์ (Hardware Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-4-4-1	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ											3					0	0	3	ผอ.ดำรงธรรม
1-4-4-2	เครื่องปริ้นเตอร์											3					0	0	3	ผอ.ดำรงธรรม
1-4-4-3	เครื่องแสกนเนอร์											3					0	0	3	ผอ.ดำรงธรรม

(5) รายการสินทรัพย์ประเภทบุคลากร (People Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-4-5-1	นิติกร											3					0	0	3	ผอ.ดำรงธรรม
1-4-5-2	นักวิเคราะห์นโยบายและแผน											3					0	0	3	ผอ.ดำรงธรรม

(6) รายการสินทรัพย์ประเภทโครงสร้างพื้นฐาน (Infrastructure Assets) Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
เลขที่	ชื่อกระบวนการ/รายละเอียดกระบวนการ	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องสมบูรณ์ครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมให้ใช้งาน					C	I	A	
		DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-4-6-1	ห้องกลุ่มงานศูนย์ดำรงธรรมจังหวัด	2	2									3	2				2	0	3	ผอ.ดำรงธรรม
1-4-6-2	ระบบไฟฟ้า											1					0	0	1	ผอ.ดำรงธรรม
1-4-6-3	ระบบโทรศัพท์											2					0	0	2	ผอ.ดำรงธรรม
1-4-6-4	ระบบอินเทอร์เน็ต											2					0	0	2	ผอ.ดำรงธรรม
1-4-6-5	ระบบเครื่องปรับอากาศ											1					0	0	1	ผอ.ดำรงธรรม
1-4-6-6	อุปกรณ์ดับเพลิง						4	4	4	4	4	4	4	4	4	4	0	4	4	ผอ.ดำรงธรรม

4.2.2 ตารางรายงานการประเมินความเสี่ยงของสินทรัพย์ (Asset Identification and Valuation)

4.2.2.1 กลุ่มงานอำนวยการ สินทรัพย์เกี่ยวกับงานระบบ คือ ระบบการบริหารงานการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ หรือ ระบบ GFMIS

(1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Proces

เลขที่	สินทรัพย์					ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-1-1-1	รับเอกสารการเบิกจากหน่วยตรวจ	1	1	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-1-1-2	จัดทำใบสำคัญตั้งหนี้ (PV) และใบสำคัญจ่าย (DV) ผ่านระบบ ERP	1	1	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-1-1-3	เสนอหัวหน้างานการเงินและหัวหน้าสำนักงานจังหวัดลงนามอนุมัติ	0	3	3	การใช้อำนาจอนุมัติ (Abuse of authorisations)	Y	Y	Y	3	3	3	1	M	M	M	วิไลวรรณ
2-1-1-4	จัดทำทะเบียนบันทึก	1	1	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-1-1-5	ดำเนินการขอเบิก	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-1-1-6	อนุมัติการขอเบิก	0	3	3	การใช้อำนาจอนุมัติ (Abuse of authorisations)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-1-1-7	ตรวจสอบการประมวลสั่งจ่ายเงิน	0	3	3	การใช้อำนาจอนุมัติ (Abuse of authorisations)	Y	Y	Y	2	2	2	1	L	L	L	วิไลวรรณ
2-1-1-8	จัดทำเช็คและทะเบียนการจ่ายเช็คพร้อมหนังสือรังรองภาษีหัก ณ ที่จ่าย	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-1-1-9	ดำเนินการจ่ายเช็คให้กับผู้มีสิทธิ	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-1-1-10	ดำเนินการขอจ่าย (PM53)	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-1-1-11	ประทับตรา "จ่ายเงินแล้ว" พร้อมลงลายมือชื่อและวันเดือนปีที่จ่ายเงิน	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ

(2) รายการสินทรัพย์ประเภทข้อมูลสารสนเทศ (Information Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-1-2-1	เอกสารการเบิก	1	1	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ
2-1-2-2	ใบสำคัญตั้งหนี้ (PV)	1	1	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ
2-1-2-3	ใบสำคัญจ่าย (DV)	0	3	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ
2-1-2-4	ทะเบียนการจ่ายเช็ค	1	1	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ
2-1-2-5	เช็ค	0	3	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ
2-1-2-6	หนังสือรับรองภาษีหัก ณ ที่จ่าย	0	3	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ

(3) รายการสินทรัพย์ประเภทซอฟต์แวร์ (Software Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-1-3-1	Microsoft Windows 8.1	0	0	3	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors)	Y	Y	Y	4	4	4	1	L	L	L	วิไลวรรณ
2-1-3-2	Micorsoft Office 2013	0	0	3	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors)	Y	Y	Y	4	4	4	1	L	L	L	วิไลวรรณ

(4) รายการสินทรัพย์ประเภทฮาร์ดแวร์ (Hardware Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นไปได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-1-4-1	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ
2-1-4-2	เครื่องปริ้นเตอร์	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ
2-1-4-3	เครื่องแสกนเนอร์	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ

(5) รายการสินทรัพย์ประเภทบุคลากร (People Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นไปได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-1-5-1	นักวิชาการเงินและบัญชี	0	0	3	การขาดบุคลากร (Abseence of personnel)	N	N	Y			1	1			H	วิไลวรรณ
2-1-5-2	เจ้าพนักงานการเงินและบัญชี	0	0	3	การขาดบุคลากร (Abseence of personnel)	N	N	Y			1	1			H	วิไลวรรณ

(6) รายการสินทรัพย์ประเภทโครงสร้างพื้นฐาน (Infrastructure Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-1-6-1	ห้องกลุ่มงานอำนวยการ	2	0	3	การเข้าสถานที่โดยไม่ได้รับอนุญาต (Unauthorised entry to premises)	Y	Y	Y	1	1	1	1	M	M	M	วิไลวรรณ
2-1-6-2	ระบบไฟฟ้า	0	0	3	ความล้มเหลวหรือการหยุดชะงักของแหล่งจ่ายไฟ (Failure or disruption of communication networks)	N	Y	Y	0	1	1	1		H	H	วิไลวรรณ
2-1-6-3	ระบบโทรศัพท์	0	0	2	ความล้มเหลวหรือการหยุดชะงักของผู้ให้บริการ (Failure of disruption of mains supply)	Y	Y	Y	1	1	1	1	M	M	M	วิไลวรรณ
2-1-6-4	ระบบอินเทอร์เน็ต	0	0	3	ความล้มเหลวหรือการหยุดชะงักของเครือข่ายการสื่อสาร (Failure of disruption of communication networks)	N	Y	Y	0	1	1	1		H	H	วิไลวรรณ
2-1-6-5	ระบบเครื่องปรับอากาศ	0	0	1	สภาพภูมิอากาศไม่เอื้ออำนวย (Unfavourable climatic conditions)	N	Y	Y	0	1	1	1		M	M	วิไลวรรณ
2-1-6-6	อุปกรณ์ดับเพลิง	0	4	4	เพลิงไหม้ (Fire)	N	Y	Y	5	5	5	1		VH	VH	วิไลวรรณ

4.2.2 ตารางรายงานการประเมินความเสี่ยงของสินทรัพย์ (Asset Identification and Valuation)

4.2.2.2 กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สินทรัพย์เกี่ยวกับงานระบบ คือ ระบบติดตามประเมินผลแผนงาน (Padme)

(1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Proces

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นไปได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-2-1-1	รับเอกสารโครงการ	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-2-1-2	บันทึกข้อมูลแผนงานโครงการ	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-2-1-3	บันทึกข้อมูลรายละเอียด	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-2-1-4	บันทึกข้อมูลการเบิกจ่ายงบประมาณ	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-2-1-5	บันทึกข้อมูลความก้าวหน้า/ผลการดำเนินการ	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-2-1-6	บันทึกข้อมูลเอกสาร/รูปภาพ	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-2-1-7	บันทึกข้อมูลผลการตรวจสอบข้อมูล	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-2-1-8	บันทึกข้อมูลเหลือจ่าย/ยกเลิก	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-2-1-9	รายงานผู้บริหาร	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ

(2) รายการสินทรัพย์ประเภทข้อมูลสารสนเทศ (Information Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นไปได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-2-2-1	ข้อมูลโครงการ	0	3	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ

(3) รายการสินทรัพย์ประเภทซอฟต์แวร์ (Software Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นไปได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-2-3-1	Microsoft Windows 8.1	0	0	3	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors)	Y	Y	Y	4	4	4	1	L	L	L	วิไลวรรณ
2-2-3-2	Micorsoft Office 2013	0	0	3	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors)	Y	Y	Y	4	4	4	1	L	L	L	วิไลวรรณ

(4) รายการสินทรัพย์ประเภทฮาร์ดแวร์ (Hardware Assets)

เลขที่	สินทรัพย์					ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-2-4-1	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ
2-2-4-2	เครื่องปริ้นเตอร์	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ
2-2-4-3	เครื่องแสกนเนอร์	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ

(5) รายการสินทรัพย์ประเภทบุคลากร (People Assets)

เลขที่	สินทรัพย์					ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-2-5-1	นักวิเคราะห์นโยบายและแผน	0	0	3	การขาดบุคลากร (Abseence of personnel)	N	N	Y			1	1			H	วิไลวรรณ
2-2-5-2	พนักงานวิเคราะห์นโยบายและแผน	0	0	3	การขาดบุคลากร (Abseence of personnel)	N	N	Y			1	1			H	วิไลวรรณ

(6) รายการสินทรัพย์ประเภทโครงสร้างพื้นฐาน (Infrastructure Assets)

เลขที่	สินทรัพย์					ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นไปได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-2-6-1	ห้องกลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด	2	0	3	การเข้าสถานที่โดยไม่ได้รับอนุญาต (Unauthorised entry to premises)	Y	Y	Y	1	1	1	1	M	M	M	วิไลวรรณ
2-2-6-2	ระบบไฟฟ้า	0	0	3	ความล้มเหลวหรือการหยุดชะงักของแหล่งจ่ายไฟ (Failure or disruption of communication networks)	N	Y	Y	0	1	1	1		H	H	วิไลวรรณ
2-2-6-3	ระบบโทรศัพท์	0	0	2	ความล้มเหลวหรือการหยุดชะงักของผู้ให้บริการ (Failure of disruption of mains supply)	Y	Y	Y	1	1	1	1	M	M	M	วิไลวรรณ
2-2-6-3	ระบบอินเทอร์เน็ต	0	0	3	ความล้มเหลวหรือการหยุดชะงักของเครือข่ายการสื่อสาร (Failure of disruption of communication networks)	N	Y	Y	0	1	1	1		H	H	วิไลวรรณ
2-2-6-4	ระบบเครื่องปรับอากาศ	0	0	1	สภาพภูมิอากาศไม่เอื้ออำนวย (Unfavourable climatic conditions)	N	Y	Y	0	1	1	1		M	M	วิไลวรรณ
2-2-6-5	อุปกรณ์ดับเพลิง	0	4	4	เพลิงไหม้ (Fire)	N	Y	Y	5	5	5	1		VH	VH	วิไลวรรณ

4.2.2 ตารางรายงานการประเมินความเสี่ยงของสินทรัพย์ (Asset Identification and Valuation)

4.2.2.3 กลุ่มงานบริหารทรัพยากรบุคคล สินทรัพย์เกี่ยวกับงานระบบ คือ ระบบสารสนเทศทรัพยากรบุคคลระดับจังหวัด (PPIS)

(1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Proces

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-3-1-1	รับเอกสาร คพ.7	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-2	บันทึกข้อมูลบุคคล	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-3	บันทึกข้อมูลการบรรจุ/แต่งตั้ง/โอน	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-4	บันทึกข้อมูลการย้าย/เลื่อนตำแหน่ง	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-5	บันทึกข้อมูลเงินเดือน	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-6	บันทึกข้อมูลการออกจากราชการ	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-7	บันทึกข้อมูลการลา/ลาย	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-8	บันทึกข้อมูลการดำเนินการทางวินัย	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-9	บันทึกข้อมูลการศึกษาต่อ/ฝึกอบรม	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-10	บันทึกข้อมูลหนังสือรับรอง	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-11	บันทึกข้อมูลการถ่ายโอนข้อมูล	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-12	บันทึกข้อมูลระบบจ่ายตรงค่ารักษาพยาบาล	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-13	บันทึกข้อมูลการรักษาราชการแทน/รักษาการในตำแหน่งช่วยราชการ	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-3-1-14	รายงานผู้บริหาร	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ

(2) รายการสินทรัพย์ประเภทข้อมูลสารสนเทศ (Information Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-3-2-1	ข้อมูล คพ.7	0	3	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ

(3) รายการสินทรัพย์ประเภทซอฟต์แวร์ (Software Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-3-3-1	Microsoft Windows 8.1	0	0	3	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors)	Y	Y	Y	4	4	4	1	L	L	L	วิไลวรรณ
2-3-3-2	Micorsoft Office 2013	0	0	3	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors)	Y	Y	Y	4	4	4	1	L	L	L	วิไลวรรณ

(4) รายการสินทรัพย์ประเภทฮาร์ดแวร์ (Hardware Assets)

เลขที่	สินทรัพย์					ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-3-4-1	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ
2-3-4-2	เครื่องปริ้นเตอร์	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ
2-3-4-3	เครื่องแลกนเนอร์	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ

(5) รายการสินทรัพย์ประเภทบุคลากร (People Assets)

เลขที่	สินทรัพย์					ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-3-5-1	นักทรัพยากรบุคคล	0	0	3	การขาดบุคลากร (Absence of personnel)	N	N	Y			1	1			H	วิไลวรรณ
2-3-5-2	พนักงานทรัพยากรบุคคล	0	0	3	การขาดบุคลากร (Absence of personnel)	N	N	Y			1	1			H	วิไลวรรณ

(6) รายการสินทรัพย์ประเภทโครงสร้างพื้นฐาน (Infrastructure Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-3-6-1	ห้องคลุ่มงานบริหารทรัพยากรบุคคล	2	0	3	การเข้าสถานที่โดยไม่ได้รับอนุญาต (Unauthorised entry to premises)	Y	Y	Y	1	1	1	1	M	M	M	วิไลวรรณ
2-3-6-2	ระบบไฟฟ้า	0	0	3	ความล้มเหลวหรือการหยุดชะงักของแหล่งจ่ายไฟ (Failure or disruption of communication networks)	N	Y	Y	0	1	1	1		H	H	วิไลวรรณ
2-3-6-3	ระบบโทรศัพท์	0	0	2	ความล้มเหลวหรือการหยุดชะงักของผู้ให้บริการ (Failure of disruption of mains supply)	Y	Y	Y	1	1	1	1	M	M	M	วิไลวรรณ
2-3-6-4	ระบบอินเทอร์เน็ต	0	0	3	ความล้มเหลวหรือการหยุดชะงักของเครือข่ายการสื่อสาร (Failure of disruption of communication networks)	N	Y	Y	0	1	1	1		H	H	วิไลวรรณ
2-3-6-5	ระบบเครื่องปรับอากาศ	0	0	1	สภาพภูมิอากาศไม่เอื้ออำนวย (Unfavourable climatic conditions)	N	Y	Y	0	1	1	1		M	M	วิไลวรรณ
2-3-6-6	อุปกรณ์ดับเพลิง	0	4	4	เหตุไหม้ (Fire)	N	Y	Y	5	5	5	1		VH	VH	วิไลวรรณ

4.2.2 ตารางรายงานการประเมินความเสี่ยงของสินทรัพย์ (Asset Identification and Valuation)

4.2.2.4 กลุ่มงานศูนย์ดำรงธรรมจังหวัด คือ ระบบร้องเรียน ร้องทุกข์ ศูนย์ดำรงธรรมจังหวัด

(1) รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Proces

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นไปได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-4-1-1	รับเรื่องร้องเรียน/ร้องทุกข์	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-4-1-2	ปริ้นเอกสารเรื่องร้อนเรียน/ร้องทุกข์	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-4-1-3	ลงรับเรื่องร้องเรียน/ร้องทุกข์	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-4-1-4	วินิจฉัยประเด็น	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-4-1-5	สรุปประเด็นแจ้งส่วนราชการที่เกี่ยวข้อง	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-4-1-6	รับรายงานผลการร้องเรียน	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-4-1-7	เสนอผู้ว่าราชการจังหวัด	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-4-1-8	ยุติเรื่องร้องเรียน/ร้องทุกข์	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ
2-4-1-9	รายงาน ปมท.และผู้ร้อง	0	3	3	ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ (Information from an unreliable source)	Y	Y	Y	1	1	1	1	L	L	L	วิไลวรรณ

(2) รายการสินทรัพย์ประเภทข้อมูลสารสนเทศ (Information Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-4-2-1	ข้อมูลเรื่องร้องเรียนร้องทุกข์	0	3	3	ข้อมูลสูญหาย (Data loss)	N	N	Y			3	1			M	วิไลวรรณ

(3) รายการสินทรัพย์ประเภทซอฟต์แวร์ (Software Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-4-3-1	Microsoft Windows 8.1	0	0	3	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors)	Y	Y	Y	4	4	4	1	L	L	L	วิไลวรรณ
2-4-3-2	Micorsoft Office 2013	0	0	3	ช่องโหว่หรือข้อผิดพลาดของซอฟต์แวร์ (Software vulnerabilities or errors)	Y	Y	Y	4	4	4	1	L	L	L	วิไลวรรณ

(4) รายการสินทรัพย์ประเภทฮาร์ดแวร์ (Hardware Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-4-4-1	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ
2-4-4-2	เครื่องปริ้นเตอร์	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ
2-4-4-3	เครื่องแสกนเนอร์	0	0	3	ความผิดปกติของอุปกรณ์หรือระบบ (Malfunction of devices or system)	Y	Y	Y	4	4	4	1	M	M	M	วิไลวรรณ

(5) รายการสินทรัพย์ประเภทบุคลากร (People Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-4-5-1	นิติกร	0	0	3	การขาดบุคลากร (Abseence of personnel)	N	N	Y			1	1			H	วิไลวรรณ
2-4-5-2	นักวิเคราะห์นโยบายและแผน	0	0	3	การขาดบุคลากร (Abseence of personnel)	N	N	Y			1	1			H	วิไลวรรณ

(6) รายการสินทรัพย์ประเภทโครงสร้างพื้นฐาน (Infrastructure Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			ความเป็นได้	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-4-6-1	ห้องกลุ่มงานศูนย์คำรงธรรมจังหวัด	2	0	3	การเข้าสถานที่โดยไม่ได้รับอนุญาต (Unauthorised entry to premises)	Y	Y	Y	1	1	1	1	M	M	M	วิไลวรรณ
2-4-6-2	ระบบไฟฟ้า	0	0	3	ความล้มเหลวหรือการหยุดชะงักของแหล่งจ่ายไฟ (Failure or disruption of communication networks)	N	Y	Y	0	1	1	1		H	H	วิไลวรรณ
2-4-6-3	ระบบโทรศัพท์	0	0	2	ความล้มเหลวหรือการหยุดชะงักของผู้ให้บริการ (Failure of disruption of mains supply)	Y	Y	Y	1	1	1	1	M	M	M	วิไลวรรณ
2-4-6-4	ระบบอินเทอร์เน็ต	0	0	3	ความล้มเหลวหรือการหยุดชะงักของเครือข่ายการสื่อสาร (Failure of disruption of communication networks)	N	Y	Y	0	1	1	1		H	H	วิไลวรรณ
2-4-6-5	ระบบเครื่องปรับอากาศ	0	0	1	สภาพภูมิอากาศไม่เอื้ออำนวย (Unfavourable climatic conditions)	N	Y	Y	0	1	1	1		M	M	วิไลวรรณ
2-4-6-6	อุปกรณ์ดับเพลิง	0	4	4	เพลิงไหม้ (Fire)	N	Y	Y	5	5	5	1		VH	VH	วิไลวรรณ

ประวัติผู้วิจัย

ชื่อ	นางสาววิไลวรรณ ทาน้อย	
วัน เดือน ปีเกิด	15 มกราคม 2526	
สถานที่เกิด	อำเภอเมืองอุดรธานี จังหวัดอุดรธานี	
ประวัติการศึกษา	ปริญญาตรี บธ.บ (คอมพิวเตอร์ธุรกิจ)	มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ
	ปริญญาตรี ร.บ. (บริหารรัฐกิจ)	มหาวิทยาลัยรามคำแหง
สถานที่ทำงาน	ก.พ. 2550 – ก.ย. 2551	สำนักงานจังหวัดนครพนม
	ต.ค. 2551 – ปัจจุบัน	สำนักงานจังหวัดหนองคาย
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ชำนาญการ	