การพัฒนาแนวปฏิบัติที่ดีและเครื่องมือในการบริหารความเสี่ยง ของระบบเทคโนโลยีสารสนเทศสำหรับสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ ฝั่งอ่าวไทยตามหลักการ COSO

นางสาวประภาศรี รักษ์บางแหลม

การศึกษาค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2561

Development of the Best Practices and Tool for Risk Management in Information Technology System of Governor's Office at the Office of the Southern Gulf of Thailand Based on COSO.

Miss Prapasri Rakbanglaem

An Independent Study Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science Information and Communication Technology

School of Science and Technology

Sukhothai Thammathirat Open University

2018

หัวข้อการศึกษาค้นคว้าอิสระ	การพัฒนาแนวปฏิบัติที่ดีและเครื่องมือในการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศสำหรับสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทยตามหลักการ COSO
ชื่อและนามสกุล	นางสาวประภาศรี รักษ์บางแหลม
แขนงวิชา	เทคโนโลยีสารสนเทศและการสื่อสาร
สาขาวิชา	วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์

การศึกษาค้นคว้าอิสระนี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษา ตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 25 มกราคม 2561

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์)

..... กรรมการ
(อาจารย์ ดร.ดวงดาว วิชาดากุล)

.....
(อาจารย์ ดร.สิทธิชัย รัชยศโยธิน)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

การศึกษาค้นคว้าอิสระ การพัฒนาแนวปฏิบัติที่ดีและเครื่องมือในการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศสำหรับสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทยตามหลักการ COSO

ผู้ศึกษา นางสาวประภาศรี รักษ์บางแหลม **รหัสนักศึกษา** 2559600289

ปริญญา วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร)

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์ **ปีการศึกษา** 2561

บทคัดย่อ

งานวิจัยครั้งนี้ มีวัตถุประสงค์เพื่อ (1) พัฒนาแนวทางปฏิบัติเพื่อประเมินความเสี่ยง ตามหลักการของ COSO สำหรับสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทยในด้านเทคโนโลยีสารสนเทศ (2) พัฒนาระบบสำหรับการประเมินความเสี่ยงตามแนวทางปฏิบัติของ COSO ในด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทย

วิธีดำเนินงานวิจัยประกอบด้วยรายละเอียดดังนี้ (1) ศึกษาแนวทาง COSO ในการประเมินความเสี่ยงในด้านเทคโนโลยีสารสนเทศ (2) วิเคราะห์ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดโดยใช้รายการภัยคุกคามเป็นตัวกำหนด (จำนวน 25 รายการ) และใช้สูตรในการประเมินความเสี่ยง (ค่าความเสี่ยง = โอกาสที่จะเกิด x ผลกระทบ) (3) พัฒนาระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เครื่องมือที่พัฒนาระบบ ได้แก่ PHP และ Mysql จัดทำเป็น Web application โดยมีรายการตรวจสอบตามภัยคุกคาม และคำนวณเป็นค่าความเสี่ยง นำเสนอเป็นกราฟสีเขียวสำหรับความเสี่ยงต่ำ สีเหลือง สำหรับความเสี่ยงปานกลาง และสีแดง สำหรับความเสี่ยงสูง

ผลการวิจัยพบว่า (1) สถานะความเสี่ยงของสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทย มีระดับความเสี่ยงปานกลางถึงสูง (2) ระบบการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทยที่พัฒนาขึ้น สามารถประเมินความเสี่ยงของแต่ละจังหวัดให้สามารถรู้ถึงระดับความเสี่ยงในปัจจุบันได้ จากผลการดำเนินงานดังกล่าว ควรมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และให้ความรู้กับผู้บริหาร ผู้ดูแลระบบ และผู้ปฏิบัติงานในการจัดทำแนวทางปฏิบัติด้วยมาตรฐานใหม่ๆ เพื่อการปฏิบัติงานที่มีประสิทธิภาพยิ่งขึ้น

คำสำคัญ COSO การบริหารความเสี่ยง การประเมินความเสี่ยง ระบบเทคโนโลยีสารสนเทศ

Independent Study title : Development of the Best Practices and Tool for Risk Management in Information Technology System of Governor's Office at the Office of the Southern Gulf of Thailand Based on COSO.

Author: Miss Prapasri Rakbanglaem; **ID:** 2559600289;

Degree: Master of Science (Information and Communication Technology);

Independent Study advisor: Dr.Vipa Jaroenpuntaruk, Associate Professor;

Academic year: 2018

Abstract

The objectives of this research were: (1) to develop the best practices of information technology risk management for the Office of the Southern Gulf of Thailand based on risk management of COSO, and (2) to develop the risk estimation system of information technology for the office of the Southern Gulf of Thailand based on risk management of COSO.

The research method included: (1) studying details of risk management of COSO; (2) analyzing and evaluating information technology risks of provincial office by using threats listed as determination (amount 25 items) and using formulas for risk assessment whereas Risk = Likelihood x Impact; (3) developing the web application using PHP and Mysql for information technology risk assessment with threat-based checklists. The indicator for risk assessment represented in colors as of green for low risk, yellow for medium risk or fair, and red for high risk.

The results of the research were as follows: (1) the risk status of the Governor's Office at the Office of the Southern Gulf of Thailand was in a medium to high level of risk. (2) the developed system for information technology risk assessment of the Governor's Office at the Office of the Southern Gulf of Thailand was able to provided the current status of risk level. Form the experimental results, it was demonstrated that system should be evaluated at least once a year. Moreover, the Executives, administrators and operators should update knowledge in new standard of best practice to improve operation more efficiently.

Keywords: COSO, Risk Management, Risk Assessment, Information Technology System

กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระนี้ได้ดำเนินการจัดทำจนสำเร็จได้ด้วยดี ด้วยได้รับความกรุณาเป็นอย่างยิ่งจาก รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์ อาจารย์ที่ปรึกษา สาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช ที่ได้กรุณาให้คำแนะนำและอดทนติดตามการศึกษาค้นคว้าอิสระของลูกศิษย์คนนี้มาตลอด ผู้ศึกษาขอกราบขอบพระคุณอาจารย์เป็นอย่างสูง

ขอบพระคุณครอบครัว มารดา ที่คอยสนับสนุนและให้กำลังใจในการศึกษาครั้งนี้ เพื่อนนักศึกษาที่คอยให้ความช่วยเหลือ ผู้เกี่ยวข้องในการศึกษาค้นคว้าอิสระครั้งนี้ เจ้าหน้าที่ของสาขาทุกท่านที่ได้กรุณาให้การสนับสนุนช่วยเหลือตลอดมา ขอขอบพระคุณอย่างยิ่ง

ประภาศรี รักษ์บางแหลม

มกราคม 2561

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันระบบเทคโนโลยีสารสนเทศกลายเป็นหัวใจหลักของระบบบริหารจัดการภาครัฐล้วนนำระบบเทคโนโลยีสารสนเทศมาใช้ในองค์กรอย่างกว้างขวาง ซึ่งหน่วยงานภาครัฐที่มีระบบเทคโนโลยีสารสนเทศที่รับผิดชอบและให้บริการประชาชน มีการใช้งานจากบุคคลภายนอกหรือแม้กระทั่งภายในองค์กร ก็ทำให้มีความเสี่ยงในการใช้งาน ความเสี่ยงในการเข้าถึงข้อมูลมากขึ้นด้วย ดังนั้น ปัญหาที่หลายองค์กรกำลังเผชิญอยู่ในปัจจุบันคือ ปัญหาความเสี่ยงของความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ที่อาจเกิดจากผู้ไม่ประสงค์ดี หรือการขาดความรู้ในการใช้งานจากพนักงานในองค์กรเอง อาจส่งผลกระทบต่อการดำเนินงานและภาพรวมขององค์กรนั้น ๆ จึงควรนำมาตรฐานการบริหารความเสี่ยงเข้ามาบริหารจัดการความเสี่ยงของระบบเทคโนโลยีสารสนเทศภายในองค์กรให้สามารถทำงานตามปกติต่อไป

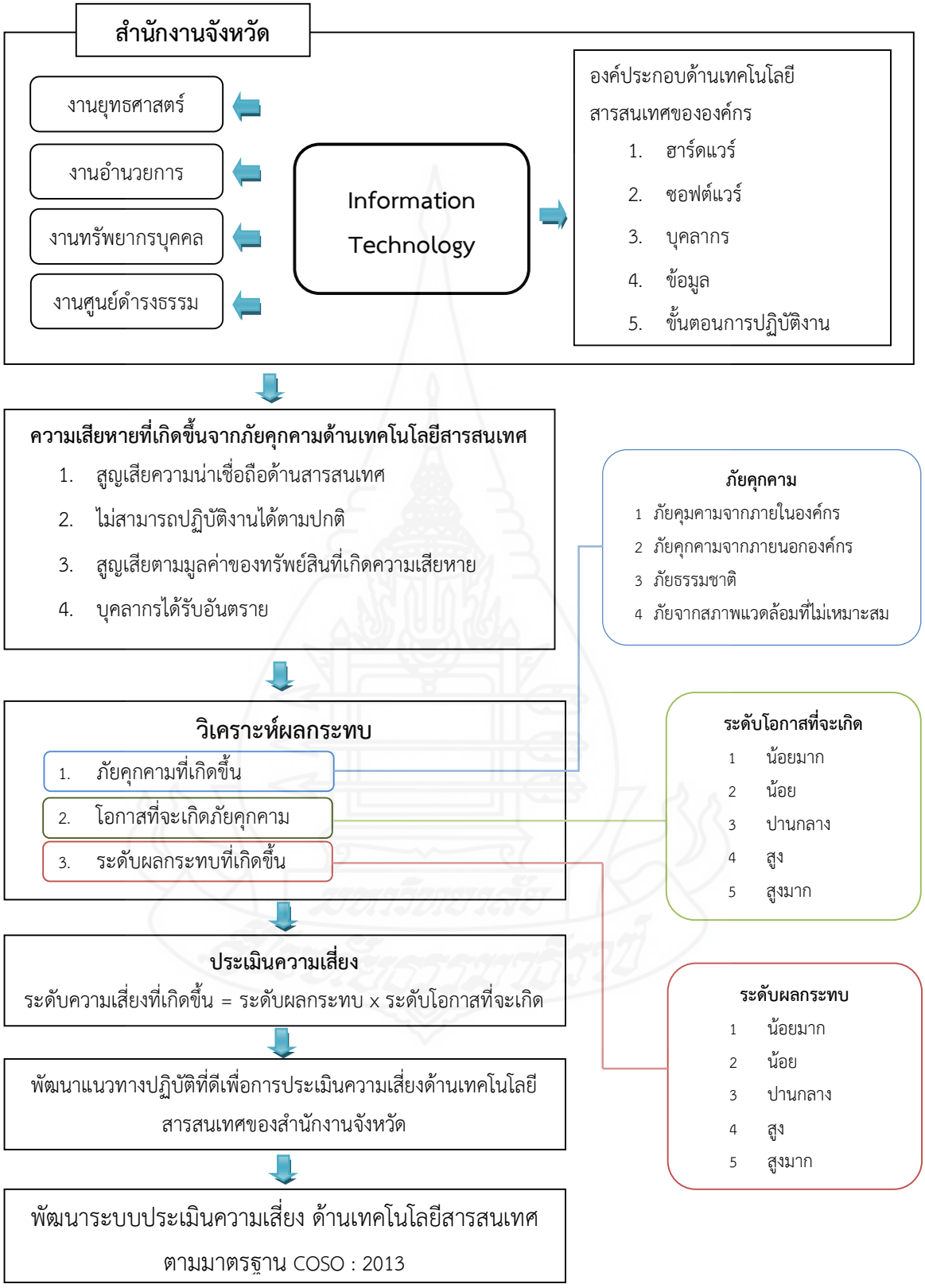
สำนักงานจังหวัด เป็นเสมือนสำนักงานของผู้ว่าราชการจังหวัด มีหน้าที่รวบรวมข้อมูลในด้านต่าง ๆ สำหรับผู้บริหารระดับสูง เพื่อใช้ในการบริหารงานราชการจังหวัด ควรที่ผู้บริหารระดับสูงจะให้ความสำคัญกับการบริหารความเสี่ยงในทุกด้าน โดยเฉพาะด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นเครื่องมือที่สำคัญอย่างยิ่งในการขับเคลื่อนการทำงาน ผู้วิจัยจึงมีแนวคิดที่จะการพัฒนาแนวปฏิบัติด้านในการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ เพื่อเป็นมาตรฐานสำหรับสำนักงานจังหวัดเพื่อเป็นต้นแบบในการทำงาน โดยยึดตามแนวทางปฏิบัติของ COSO (Committee of Sponsoring Organizations) มาพัฒนาแนวทางปฏิบัติให้เกิดรูปธรรมมากขึ้น โดย COSO ได้ออกแบบกรอบการควบคุมความเสี่ยงและสามารถนำมาประยุกต์ใช้กับด้านเทคโนโลยีสารสนเทศได้

2. วัตถุประสงค์การวิจัย

2.1 เพื่อพัฒนาแนวทางปฏิบัติที่ดี เพื่อประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทย ตามแนวทางปฏิบัติของ COSO

2.2 เพื่อพัฒนาระบบการประเมินความเสี่ยง ประยุกต์ใช้ตามแนวทางปฏิบัติของ COSO ด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทย

3. กรอบแนวคิดการวิจัย



ภาพที่ 1.1 กรอบแนวคิดการศึกษา

4. ขอบเขตการวิจัย

4.1 หลักการกรอบแนวคิด COSO : 2013 ประกอบด้วย 5 องค์ประกอบ 17 หลักการ ซึ่งผู้ศึกษาใช้องค์ประกอบที่ 2 ประกอบการศึกษาครั้งนี้

4.1.1 องค์ประกอบที่ 1: สภาพแวดล้อมการควบคุม (Control Environment)

4.1.2 องค์ประกอบที่ 2: การประเมินความเสี่ยง (Risk Assessment)

4.1.3 องค์ประกอบที่ 3: กิจกรรมการควบคุม (Control Activities)

4.1.4 องค์ประกอบที่ 4: สารสนเทศและการสื่อสาร (Information and Communication)

4.1.5 องค์ประกอบที่ 5: กิจกรรมการกำกับติดตามและประเมินผล (Monitoring Activities)

4.2 องค์ประกอบด้านเทคโนโลยีสารสนเทศเพื่อใช้การประเมินความเสี่ยง แบ่งออกเป็น 5 ด้าน คือ

4.2.1 ขั้นตอนการปฏิบัติงาน (processes)

4.2.2 ข้อมูล (Information)

4.2.3 ซอฟต์แวร์ (Software)

4.2.4 ฮาร์ดแวร์ (Hardware)

4.2.5 บุคลากร (People)

4.3 กลุ่มเป้าหมายในการประเมินและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ สำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทย จำนวน 5 จังหวัด คือ ชุมพร สุราษฎร์ธานี นครศรีธรรมราช พัทลุง และสงขลา โดยมีลักษณะงาน ดังนี้

4.3.1 งานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด

4.3.2 งานอำนวยการ

4.3.3 งานทรัพยากรบุคคล

4.3.1 งานศูนย์ดำรงธรรม

5. วิธีการดำเนินการวิจัย

5.1 ศึกษากรอบแนวคิดตามมาตรฐาน COSO ตามองค์ประกอบที่ 2 การประเมินความเสี่ยง (Risk Assessment) โดยผู้ศึกษาได้ทำความเข้าใจในหลักการภายใต้องค์ประกอบที่ 2 ว่ามีการกำหนดเป้าหมาย วิเคราะห์และประเมินความเสี่ยงอย่างไร โดยศึกษาจาก

- ศึกษาเอกสารมาตรฐานการควบคุมภายใน COSO 2013
- ศึกษาการวิจัยที่เกี่ยวข้อง

5.2 ศึกษาการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร ประกอบไปด้วย ภัยคุกคาม ผลกระทบ โอกาสที่จะเกิดความเสี่ยง และระดับความเสี่ยง ผู้ศึกษาจะทำการประเมินและวิเคราะห์ความเสี่ยงโดยมีขั้นตอน ดังนี้

- กำหนดภัยคุกคาม (Threat Identification)
- วิเคราะห์ผลกระทบ (Impact Analysis)
- ระดับโอกาสที่จะเกิดขึ้น (Likelihood)
- ประเมินระดับความเสี่ยง (Risk assessment)

5.3 พัฒนาระบบประเมินความเสี่ยงโดยจัดทำเป็นเว็บ แอปพลิเคชั่น เพื่อใช้ในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด ประกอบด้วย

- ระบบบริหารจัดการผู้ใช้งานระบบ สามารถสมัครผู้ใช้งานผ่านหน้าเว็บ และ login เข้าสู่ระบบได้
- ระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศตามภัยคุกคามที่กำหนด โดยจัดทำเป็น checklist เพื่อประเมินความพร้อม และกำหนด KPI แสดงเป็นสีเขียว เหลือง แดง เพื่อง่ายต่อการทำความเข้าใจ ซึ่งสีเขียวหมายถึง ความเสี่ยงต่ำ สีเหลืองหมายถึง ความเสี่ยงปานกลาง และสีแดงหมายถึง ความเสี่ยงสูง
- ระบบออกรายงาน โดยสามารถรายงานผลการประเมินความเสี่ยงเป็นรูปแบบกราฟ แยกเป็นแต่ละด้านที่ทำการประเมิน โดยแสดงค่าความเสี่ยงแยกเป็นสีเขียว สีเหลือง สีแดง หมายถึง ค่าความเสี่ยงต่ำ ปานกลาง สูง

6. นิยามศัพท์

6.1 องค์ประกอบด้านเทคโนโลยีสารสนเทศ หมายถึง สิ่งที่มีความสำคัญต่อองค์กรที่ใช้ในการประเมินความเสี่ยงและการรักษาความปลอดภัย ทั้งที่มีมูลค่าความเสียหายเชิงปริมาณ และเชิงคุณภาพ ซึ่งหมายรวมถึงในรูปแบบของข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์

สารสนเทศ ซึ่งในการศึกษานี้ คือ 1) ขั้นตอนการปฏิบัติงาน (processes) 2) ข้อมูล (Information) 3) ซอฟต์แวร์ (Software) 4) ฮาร์ดแวร์ (Hardware) และ 5) บุคลากร (People)

6.2 ภัยคุกคาม (Threat) หมายถึง ปัจจัยที่อาจทำร้ายหรือก่อให้เกิดความเสียหาย ต่อองค์ประกอบด้านเทคโนโลยีสารสนเทศ หรือทรัพย์สินขององค์กร ที่ส่งผลกระทบทำให้องค์กรไม่สามารถปฏิบัติงานได้ตามปกติ ภัยคุกคามสามารถแบ่งได้หลายประเภท คือ ภัยคุกคามจากภายนอกองค์กร ภัยคุกคามจากภายในองค์กร ภัยธรรมชาติ และภัยคุกคามจากสภาพแวดล้อมที่ไม่เหมาะสม

6.3 เป้าหมาย (Target) หมายถึง การโจมตีของภัยคุกคามเพื่อวัตถุประสงค์ใด ซึ่งจะมุ่งเน้นไปที่การรักษาความปลอดภัย คือ ความลับ ความคงสภาพ และความพร้อมใช้งาน

6.4 ความเสี่ยง (Risk) หมายถึง ความน่าจะเป็น ที่จะเกิดภัยคุกคามใด ๆ ขึ้น และก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สินขององค์กร ระดับความรุนแรงของผลกระทบที่เกิด ขึ้นอยู่กับความสำคัญของข้อมูลและทรัพย์สินนั้น ๆ

6.5 ผลกระทบ (Impact) หมายถึง ความเสียหายที่เกิดขึ้นจากภัยคุกคาม อาจเกิดในรูปแบบของจำนวนเงิน หรือความน่าเชื่อถือขององค์กร หรือการเสียโอกาส เป็นต้น

6.6 โอกาสที่จะเกิดขึ้น (Likelihood) หมายถึง จำนวนความถี่ที่ภัยคุกคามอาจเกิดขึ้นกระทำความเสียหายต่อทรัพย์สิน ซึ่งอาจเกิดจากแรงจูงใจ การไม่มีความรู้ หรือการเข้าถึงได้ง่ายเกินไป

ระดับความเสี่ยง เขียว เหลือง แดง หมายถึง รูปแบบสีที่นำมาแทนค่าความเสี่ยงที่เกิดขึ้นในแต่ละภัยคุกคาม ซึ่งสีเขียวหมายถึง ความเสี่ยงต่ำ สีเหลืองหมายถึง ความเสี่ยงปานกลาง และสีแดงหมายถึง ความเสี่ยงสูง

7. ประโยชน์ที่จะได้รับ

7.1 ได้แนวทางในการปฏิบัติเรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

7.2 ได้ Web application ระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด เพื่อใช้เป็นต้นแบบให้กับจังหวัดอื่นต่อไป

บทที่ 2
วรรณกรรมที่เกี่ยวข้อง

1. ทฤษฎีที่เกี่ยวข้อง

ปัจจุบันการนำเทคโนโลยีสารสนเทศมาใช้งานในองค์กร ถือว่าเป็นการอำนวยความสะดวกให้การทำงานในองค์กรมีประสิทธิภาพมากขึ้น ในขณะเดียวกันหากไม่มีการควบคุมที่ดี ก็สามารถเป็นช่องทางในการถูกโจมตีจากทั้งภายในและภายนอกองค์กรได้ ระบบควบคุมภายในขององค์กร ไม่ได้เป็นแต่เพียงข้อกำหนดทางวิชาการเท่านั้น แต่หากสามารถใช้ในการบริหารจัดการองค์กรได้ เป็นการปฏิบัติที่สามารถตรวจสอบได้ถึงตัวบุคคลทุกระดับขององค์การ ตั้งแต่ผู้บริหารระดับสูงจนถึงผู้ปฏิบัติงานระดับล่าง การที่องค์กรมีระบบการควบคุมภายในที่มีมาตรฐานที่ดีนั้นย่อมแสดงได้ว่าองค์การนั้น ๆ ตระหนักถึงการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์ของหน่วยงาน ทำให้หน่วยงานที่มีการจัดวางระบบการควบคุมภายในและการประเมินผลการควบคุมภายใน จะสามารถลดภาระงานตลอดจนปัญหาอุปสรรคต่าง ๆ ของการปฏิบัติงานลงได้ มีการพัฒนาระบบการควบคุมภายในให้สามารถปฏิบัติได้จริงและมีความทันสมัยของการบริหารจัดการองค์การอยู่เสมอ เพราะฉะนั้นองค์กรควรมีระบบมาตรฐานในการควบคุมภายในที่ดี เพื่อลดความเสี่ยงจากการปฏิบัติการ ผู้ศึกษาจึงได้แนวคิดในการบริหารจัดการความเสี่ยงโดยใช้มาตรฐานการควบคุมภายในมาใช้ในการศึกษาค้นคว้าครั้งนี้

- มาตรฐานการควบคุมภายใน COSO : 2013
- การบริหารจัดการความเสี่ยงด้านเทคโนโลยี
- การประเมินความเสี่ยงด้านเทคโนโลยี

2. กรอบแนวคิดของ COSO

COSO คือ กรอบแนวคิดการควบคุมภายในองค์กร เพื่อช่วยให้ผู้ปฏิบัติงานบรรลุเป้าหมาย ทั้งเรื่องของการปฏิบัติงานอย่างมีประสิทธิภาพ ประสิทธิผล ความถูกต้องครบถ้วน และการปฏิบัติตามกฎเกณฑ์ที่กำหนด การบริหารและการจัดการกับความเสี่ยงตามหลักการของ COSO สามารถประยุกต์ใช้ในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบต่อองค์กร

COSO ย่อมาจาก **Committee of Sponsoring of the Treadway Commission** เป็นคณะทำงาน ที่ก่อตั้งขึ้น โดยคณะกรรมาธิการของประเทศสหรัฐอเมริกา ที่ชื่อว่า Treadway Commission ในปี 1985 โดยจัดตั้งขึ้น เพื่อศึกษาและพัฒนาแนวทางการบริหารความเสี่ยง รูปแบบ

การควบคุมภายในที่มีประสิทธิผล ค.ศ. 2013 COSO ได้ประกาศแนวทางการควบคุมภายใน ซึ่งยังคงยึดกรอบแนวคิดเดิมของปี ค.ศ.1992 (**Internal Control – Integrated Framework**) ที่กำหนดให้การควบคุมภายในมีองค์ประกอบหลัก 5 องค์ประกอบ แต่เพิ่มเติมในส่วนอื่น ๆ ให้ชัดเจนขึ้น เรียกกันว่า *COSO 2013* ซึ่งใช้กันในปัจจุบัน

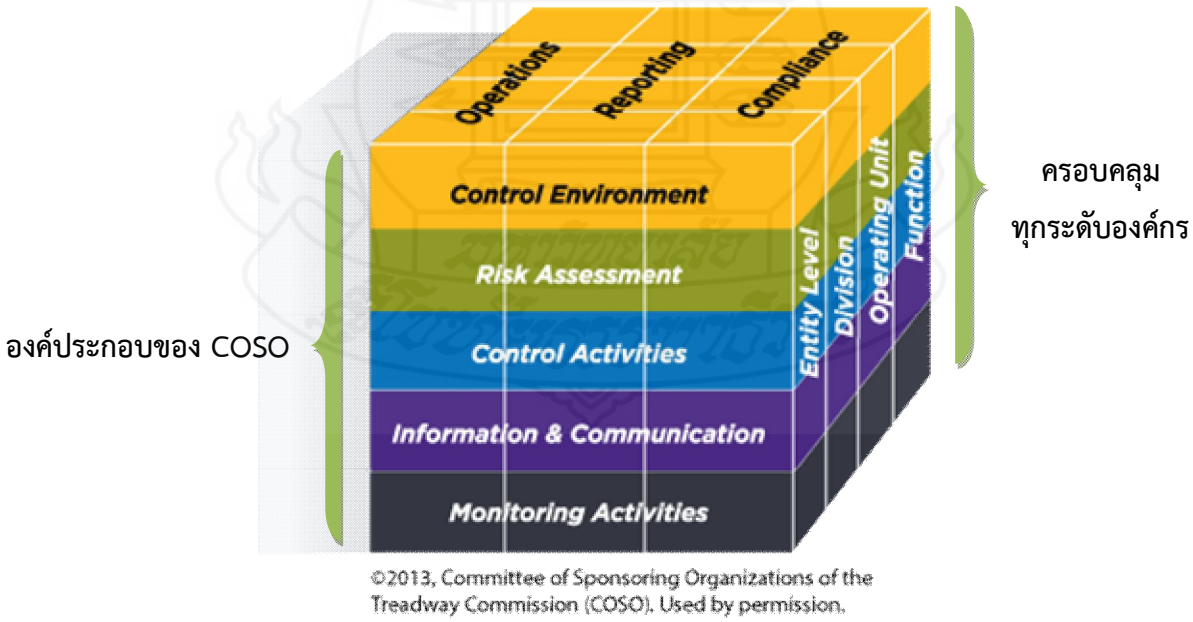
องค์ประกอบตามกรอบแนวคิดของ COSO มี 5 องค์ประกอบหลัก คือ

1. Control Environment สภาพแวดล้อมการควบคุม
2. Risk Assessment การประเมินความเสี่ยง [ซึ่งใช้ในการศึกษาครั้งนี้]
3. Control Activities กิจกรรมการควบคุม
4. Information and Communication สารสนเทศและการสื่อสาร
5. Monitoring Activities การติดตามและประเมินผล

ซึ่งทั้ง 5 องค์ประกอบนั้น ใช้เป็นเกณฑ์ในการควบคุมทุกระดับ คือ

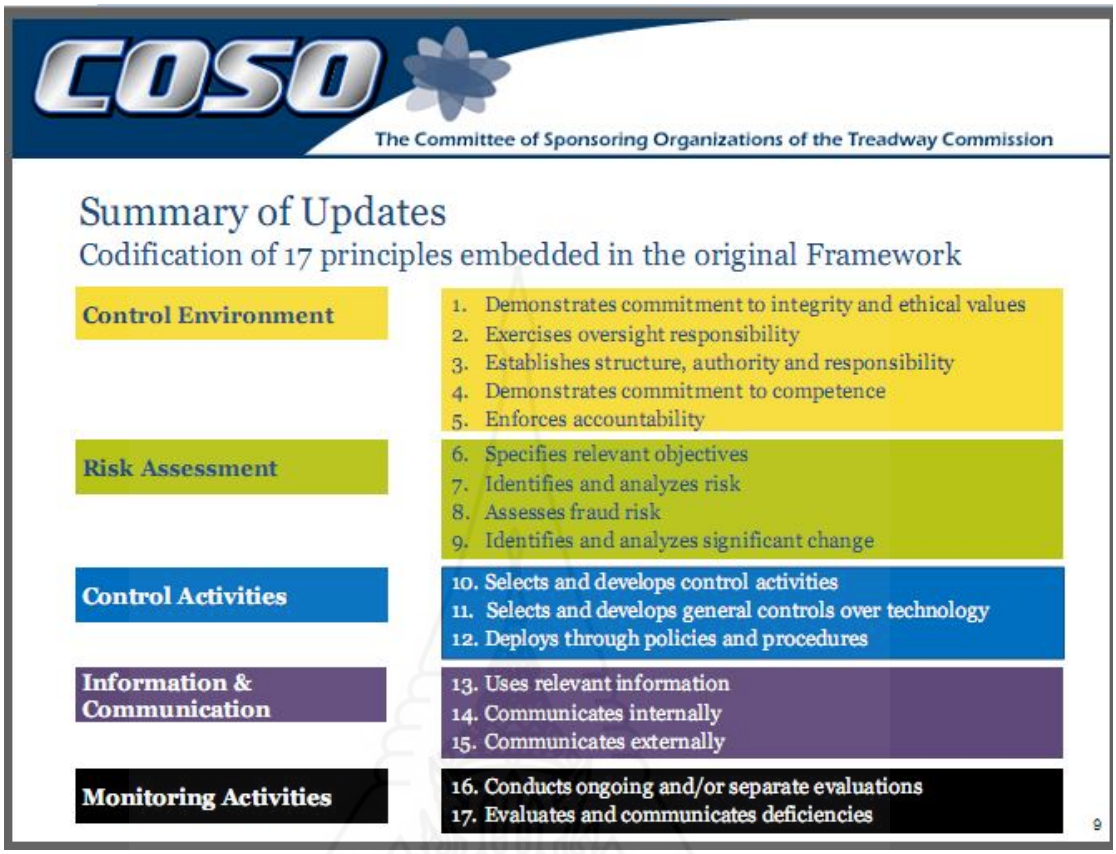
- ระดับองค์กร (Entity Level)
- ระดับหน่วยงาน (Division)
- ระดับหน่วยการปฏิบัติการ (Operating Unit)
- ระดับหน่วยงานย่อย (Function)

โดยองค์ประกอบตามกรอบแนวคิดของ COSO นั้น สามารถอธิบายได้ตามรูปภาพ ดังนี้



ภาพที่ 2.1 ภาพรวมองค์ประกอบ COSO (COSO Cube)

ที่มา www.protiviti.com



ภาพที่ 2.2 หลักการของ COSO Framework

ที่มา www.protiviti.com

ประกอบด้วย 5 องค์ประกอบ 17 หลักการ

องค์ประกอบที่ 1: สภาพแวดล้อมการควบคุม (Control Environment)

หลักการที่ 1 - องค์กรยึดหลักความซื่อตรงและจริยธรรม

หลักการที่ 2 - คณะกรรมการแสดงออกถึงความรับผิดชอบต่อการกำกับดูแล

หลักการที่ 3 - คณะกรรมการและฝ่ายบริหาร มีอำนาจการสั่งการชัดเจน

หลักการที่ 4 - องค์กร จูงใจ รักษาไว้ และจูงใจพนักงาน

หลักการที่ 5 – องค์กรผลักดันให้ทุกตำแหน่งรับผิดชอบต่อการควบคุมภายใน

องค์ประกอบที่ 2: การประเมินความเสี่ยง (Risk Assessment)

หลักการที่ 6 - กำหนดเป้าหมายชัดเจน

หลักการที่ 7 - ระบุและวิเคราะห์ความเสี่ยงอย่างครอบคลุม

หลักการที่ 8 - พิจารณาโอกาสที่จะเกิดการทุจริต

หลักการที่ 9 – ระบุและประเมินความเปลี่ยนแปลงที่จะกระทบต่อการควบคุมภายใน

องค์ประกอบที่ 3: กิจกรรมการควบคุม (Control Activities)

หลักการที่ 10 - ควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

หลักการที่ 11 - พัฒนาระบบเทคโนโลยีที่ใช้ในการควบคุม

หลักการที่ 12 – ควบคุมให้นโยบายสามารถปฏิบัติได้

องค์ประกอบที่ 4: สารสนเทศและการสื่อสาร (Information and Communication)

หลักการที่ 13 - องค์กรมีข้อมูลที่เกี่ยวข้องและมีคุณภาพ

หลักการที่14 - มีการสื่อสารข้อมูลภายในองค์กร ให้การควบคุมภายในดำเนินต่อไปได้

หลักการที่ 15 - มีการสื่อสารกับหน่วยงานภายนอก ในประเด็นที่อาจกระทบต่อการควบคุมภายใน

องค์ประกอบที่ 5: กิจกรรมการกำกับติดตามและประเมินผล (Monitoring Activities)

หลักการที่ 16 - ติดตามและประเมินผลการควบคุมภายใน

หลักการที่ 17 - ประเมินและสื่อสารข้อบกพร่องของการควบคุมภายในทันเวลา และเหมาะสม

วงจรพัฒนาระบบ (System Development Life Cycle : SDLC)

เป็นวงจรที่แสดงถึงกิจกรรมต่างๆ ที่เป็นลำดับขั้นตอนในการพัฒนาระบบ ซึ่ง SDLC ประกอบด้วยกิจกรรม 7 ระยะด้วยกัน ดังนี้

ภาพที่ 2.3 ภาพรวมวงจรการพัฒนาระบบ SDLC

1. การกำหนดปัญหา

การพัฒนาระบบต้องตอบสนองกับปัญหาที่เกิดขึ้นว่า สามารถแก้ไขปัญหาได้หรือไม่ เพราะฉะนั้น ในการกำหนดปัญหาต้องชัดเจนและตรงประเด็นว่า มีปัญหาในการทำงานอย่างไร และต้องการให้แก้ปัญหาในจุดใด ซึ่งแนวทางที่ดีที่สุดในการแก้ไขปัญหา คือการพัฒนาระบบที่ตอบตรงปัญหามากที่สุด ไม่จำเป็นต้องใช้งบประมาณที่สูง แต่เป็นการจัดวางแนวทางที่เหมาะสมสำหรับสถานการณ์นั้น ๆ มากกว่า โดยสรุป คือ

- รับรู้สภาพของปัญหาที่เกิดขึ้น
- ค้นหาต้นเหตุของปัญหา รวบรวมปัญหาของระบบงานเดิม
- ศึกษาความเป็นไปได้ของโครงการพัฒนาระบบ
- ลงมือดำเนินการ

2. การวิเคราะห์

การวิเคราะห์เป็นการรวบรวมข้อมูลความต้องการ (Requirements) ต่าง ๆ มาให้มากที่สุด ซึ่งการสืบค้นความต้องการของผู้ใช้สามารถดำเนินการได้จากการรวบรวมเอกสารการสัมภาษณ์ การออกแบบสอบถาม และการสังเกตการณ์บนสภาพแวดล้อมการทำงานจริง ในการทำงานครั้งนี้ ผู้เขียนได้รวบรวมจากการปฏิบัติงานจริง เมื่อวิเคราะห์สรุปเป็นความต้องการที่ชัดเจนแล้ว ก็นำข้อกำหนดเหล่านั้นไปพัฒนาเป็นความต้องการของระบบใหม่ ด้วยการพัฒนาเป็นแบบจำลอง (Model) โดยสรุป คือ

- วิเคราะห์ระบบงานปัจจุบัน
- รวบรวมความต้องการ และกำหนดความต้องการของระบบใหม่
- วิเคราะห์ความต้องการเพื่อสรุปเป็นข้อกำหนด
- สร้างแผนภาพ DFD และแผนภาพ E-R

3. การออกแบบ

เป็นการนำผลจากการวิเคราะห์มาออกแบบเชิงกายภาพ ว่าระบบที่พัฒนาขึ้นมาต้องการจัดทำอะไรบ้าง เช่น ข้อมูลที่นำเข้า ฐานข้อมูล รายงาน หน้าจอที่ใช้ติดต่อกับผู้ใช้ (User Interface) เป็นต้น โดยสรุป คือ

- พิจารณาแนวทางในการพัฒนาระบบ
- ออกแบบสถาปัตยกรรมระบบ
- ออกแบบรายงาน
- ออกแบบหน้าจออินพุตข้อมูล
- ออกแบบผังงานระบบ
- ออกแบบฐานข้อมูล

- การสร้างต้นแบบ
- การออกแบบโปรแกรม

4. การพัฒนา

เป็นการพัฒนาโปรแกรม โดยพัฒนาตามที่ได้ออกแบบไว้ เป็นการกำหนดขอบเขตการพัฒนาโปรแกรมให้ตรงจุดที่ต้องการทำเท่านั้น โดยสรุป คือ

- พัฒนาโปรแกรม
- เลือกภาษาโปรแกรมที่เหมาะสม
- สามารถนำเครื่องมือมาช่วยพัฒนาโปรแกรมได้
- สร้างเอกสารประกอบโปรแกรม

5. การทดสอบ

เมื่อพัฒนาโปรแกรมขึ้นมาแล้ว ยังไม่สามารถใช้งานระบบได้ทันที เนื่องจากต้องดำเนินการทดสอบระบบก่อนที่จะนำไปใช้งานจริงเสมอ ควรมีการทดสอบข้อมูลเบื้องต้นก่อน ด้วยการสร้างข้อมูลจำลองนำเข้าในระบบ เพื่อใช้ตรวจสอบการทำงานของระบบงาน หากพบข้อผิดพลาดก็ปรับปรุงแก้ไขให้ถูกต้อง การทดสอบระบบจะตรวจสอบว่าระบบตรงกับความต้องการของผู้ใช้หรือไม่ โดยสรุป คือ

- ทดสอบไวยากรณ์ภาษาคอมพิวเตอร์
- ทดสอบความถูกต้องของผลลัพธ์ที่ได้
- ทดสอบว่าระบบที่พัฒนาตรงตามความต้องการของผู้ใช้หรือไม่

6. การนำระบบไปใช้

เมื่อทดสอบระบบจนมั่นใจว่าระบบที่ได้รับการทดสอบนั้นพร้อมที่จะนำไปติดตั้งเพื่อใช้งานบนสถานการณ์จริง และเมื่อระบบสามารถรันได้จนเป็นที่น่าพอใจทั้งสองฝ่าย ก็จะต้องจัดทำเอกสารคู่มือระบบ รวมถึงการฝึกอบรมผู้ใช้

- ศึกษาสภาพแวดล้อมของพื้นที่ก่อนที่จะนำระบบไปติดตั้ง
- ติดตั้งระบบให้เป็นไปตามสถาปัตยกรรมที่ออกแบบไว้
- จัดทำคู่มือระบบ
- ฝึกอบรมผู้ใช้
- ดำเนินการใช้ระบบงานใหม่
- ประเมินผลการใช้งานของระบบใหม่

7. การบำรุงรักษา

ขั้นตอนการบำรุงรักษาอาจเกิดขึ้นหลังใช้งานระบบ ทั้งนี้ข้อบกพร่องในด้านการทำงานของโปรแกรมอาจเพิ่งค้นพบได้ เป็นข้อบกพร่องที่ไม่ได้พบในช่วงการทดสอบระบบ ซึ่งจะต้อง

ดำเนินการแก้ไขให้ถูกต้องรวมถึงกรณีที่ข้อมูลที่จัดเก็บมีปริมาณที่มากขึ้นต้องวางแผนการรองรับเหตุการณ์นี้ด้วย นอกจากนี้งานบำรุงรักษายังเกี่ยวข้องกับการเขียนโปรแกรมเพิ่มเติมกรณีที่ผู้ใช้มีความต้องการเพิ่มขึ้น

- กรณีเกิดข้อผิดพลาดขึ้นจากระบบ ให้ดำเนินการแก้ไขให้ถูกต้อง
- อาจจำเป็นต้องเขียนโปรแกรมเพิ่มเติม กรณีที่ผู้ใช้มีความต้องการเพิ่มเติม
- วางแผนรองรับเหตุการณ์ที่อาจเกิดขึ้นในอนาคต
- บำรุงรักษาระบบงาน และอุปกรณ์

3. การประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยง (Risk) ความเสี่ยง คือ โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริหาร

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

โอกาสที่จะเกิด (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ ความเสี่ยง

ผลกระทบ (Impact) หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง

ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น 5 ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก

ปัจจัยความเสี่ยง หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการความเสี่ยง ในภายหลังได้อย่างถูกต้อง

4. งานวิจัยที่เกี่ยวข้อง

พลภัทร สุนทรทิวกร (2560) ทำการศึกษาพัฒนาระบบประเมินความเสี่ยงและความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของเนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ ตามหลัก CIA Triad และพัฒนาระบบการควบคุมความมั่นคงปลอดภัย ด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ของเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์ ผลการวิจัยพบว่า เมื่อทำการทดสอบระบบที่พัฒนาขึ้น ทำให้ประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของเนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ อยู่ในระดับต่ำถึงปานกลาง

วิไลวรรณ ทาน้อย (2560) ทำการศึกษาระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานตามมาตรฐาน ISO/IEC 27005 พัฒนากระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ตามมาตรฐาน ISO/IEC 27001 ประเมินกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย ผลการวิจัยพบว่า ผลการประเมินความพร้อม ด้านการควบคุมการเข้าถึงระบบอยู่ในระดับต่ำกว่าเกณฑ์ ดังนั้นหน่วยงานควรเร่งจัดทำระบบบริหารความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สามารถรองรับเหตุการณ์ด้านความมั่นคงปลอดภัยภายในองค์กร

สุชาติ บัวดำ (2555) ทำการศึกษาด้านการประเมินการควบคุมภายในตามแนว COSO กระบวนการปฏิบัติงานสินไหมทดแทน บริษัทวัชระประกันภัย จำกัด มีวัตถุประสงค์เพื่อประเมินระบบการควบคุมภายในกระบวนการปฏิบัติงานสินไหมทดแทน และ เสนอแนะแนวทางปรับปรุง แก้ไข โดยทำการประเมินการควบคุมภายใน 5 องค์ประกอบ ตามกรอบแนวคิดของ COSO ซึ่งประกอบด้วยสภาพแวดล้อมการควบคุม การประเมินความเสี่ยง กิจกรรมการควบคุมสารสนเทศและการสื่อสาร การติดตามและประเมินผลการศึกษา ผลการศึกษาพบว่า ระบบการควบคุมภายในควรปรับปรุง เกี่ยวกับนโยบายวิธีบริหารทรัพยากรบุคคล เรื่องการประเมินผลการปฏิบัติงานให้มีความชัดเจน ควรจัดให้มีเครื่องมือและวิธีการประเมินความเสี่ยงอย่างมีระบบ มีการกำหนดเกณฑ์เพื่อประเมินปัจจัยความเสี่ยงในด้านผลกระทบและโอกาสที่จะเกิดขึ้นต่อกระบวนการปฏิบัติงานโดยกำหนดกรอบและนโยบายบริหารความเสี่ยงภัยให้สอดคล้องกับแนวทางการบริหารความเสี่ยงภัยตามแนวทางสากลและ ระบุประเมินความเสี่ยงอย่างสม่ำเสมอ

นางสาวสุวินชา การพัดชี (2555) ทำการศึกษาการวิเคราะห์ประสิทธิภาพระบบการควบคุมภายในของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ ศึกษาปัจจัยด้านประชากรศาสตร์ ที่มีผลต่อประสิทธิภาพการควบคุมภายในตามแนวคิดของ COSO และประสิทธิภาพในการดำเนินงานศึกษาความสัมพันธ์ระหว่างปัจจัยด้านการบริหาร กับประสิทธิภาพการควบคุมภายในและประสิทธิภาพการดำเนินงาน ศึกษาความสัมพันธ์ระหว่างประสิทธิการควบคุมภายในตามแนวคิดของ COSO กับประสิทธิภาพการดำเนินงาน ผลการวิจัยพบว่า ปัจจัยด้านประชากรศาสตร์ อายุ ประสบการณ์การทำงาน มีผลต่อประสิทธิภาพการควบคุมภายในตามแนวคิดของ COSO ในด้านการประเมินความเสี่ยง ด้านสารสนเทศและการสื่อสาร และการติดตามประเมินผล

ปิญะธิดา อมรภิญโญ (2560) ทำการศึกษาการควบคุมภายในเพื่อความสำเร็จอย่างยั่งยืนของวิสาหกิจการผลิตขนาดย่อมในภาคตะวันออกเฉียงเหนือตอนบนประเทศไทย วัตถุประสงค์ของงานวิจัยนี้คือ เพื่อศึกษาลักษณะการใช้การควบคุมภายใน (ในระดับหลักการและข้อปฏิบัติ) และเพื่อศึกษาผลกระทบของการควบคุมภายในที่ส่งผลต่อความสำเร็จอย่างยั่งยืนของวิสาหกิจการผลิตขนาดย่อมในภาคตะวันออกเฉียงเหนือตอนบนประเทศไทย โดยศึกษาการควบคุมภายในตามแนวคิด COSO 2013 ประกอบด้วยองค์ประกอบ 5 ด้านหลักการการควบคุมภายใน 17 หลักการและใช้ COSO 2013 เป็นแนวทางในการกำหนดข้อปฏิบัติการควบคุมภายในของแต่ละหลักการ ผลการวิจัยพบว่า หลักการการควบคุมภายในที่ถูกนำไปปฏิบัติมากที่สุดคือการจัดโครงสร้างองค์กรกำหนดอำนาจสั่งการและความรับผิดชอบที่ชัดเจน อันดับสองคือระบุและวิเคราะห์ความเสี่ยงอย่างครอบคลุมและอันดับสามคือกิจกรรมการควบคุมผ่านทางนโยบาย และพบว่าการควบคุมภายในของ COSO 2013 มีอิทธิพลต่อความสำเร็จอย่างยั่งยืน

นางสาวปิยพร บรรดาศักดิ (2555) ทำการศึกษา ระบบการควบคุมภายในตามแนว COSO ด้านรายรับ - รายจ่าย กรณีศึกษากองทุนสุขภาพ โดยมีวัตถุประสงค์ในการศึกษาเพื่อทราบระบบการควบคุมภายในด้านรายรับ - รายจ่าย เพื่อสามารถเสนอแนะแนวทางการควบคุมภายในด้านรายรับ – รายจ่ายที่มีประสิทธิภาพและเหมาะสมกับการดำเนินงาน จากการศึกษาพบว่า ด้านการประเมินความเสี่ยง ระดับการควบคุมอยู่ในเกณฑ์ที่ควรปรับปรุง ประเด็นการควบคุมที่ยังไม่มีความเหมาะสม คือ ควรจัดทำแผนการประเมินความเสี่ยงสำหรับระบบงานต่างๆ ที่สำคัญ

กิตติพงศ์ โภชนะสมบัติ (2557) ทำการศึกษาถึงการประเมินผลระบบควบคุมภายในตามแนวคิด COSO กรณีศึกษาหน่วยงานในสังกัดสำนักงานปลัดกระทรวงศึกษาธิการ โดยมีวัตถุประสงค์ในการศึกษาคือ เพื่อประเมินผลการควบคุมภายในตามแนวคิด COSO ของหน่วยงานในสังกัดสำนักงานปลัดกระทรวงศึกษาธิการและเพื่อศึกษาปัญหาและอุปสรรคในการควบคุมภายในตามแนวคิด COSO ผลการศึกษาในภาพรวมผลการประเมินผลระบบควบคุมภายในของหน่วยงานในสังกัดสำนักงานปลัดกระทรวงศึกษาธิการตามแนวคิด COSO พบว่า หน่วยงานในสังกัดสำนักงานปลัดกระทรวงศึกษาธิการมีระบบควบคุมภายในที่ดี ปัญหาและอุปสรรคในการควบคุมภายในของหน่วยงานในสังกัดสำนักงานปลัดกระทรวงศึกษาธิการตามแนวคิด COSO ด้านสภาพแวดล้อมของการควบคุม พบว่า บุคลากรบางส่วนยังไม่ตระหนักถึงความสำคัญของการควบคุมภายในเท่าที่ควร ทำให้กิจกรรมควบคุมที่มีอยู่ลดประสิทธิภาพประสิทธิผลลง ด้านการประเมินความเสี่ยง พบว่า การประเมินความเสี่ยงในบางหน่วยงานยังไม่ครอบคลุมทุกกิจกรรมที่มีอยู่

ลีลาศ คุณฟอง (2557) ทำการศึกษากระบวนการบริหารความเสี่ยงตามกรอบแนวคิดการบริหารความเสี่ยงทั่วทั้งองค์กร COSO-ERM กรณีศึกษา: บริษัท เด สเต โค (เอเชีย) จำกัด โดยมีวัตถุประสงค์เพื่อศึกษาระบบการบริหารความเสี่ยงตามกรอบแนวคิดการบริหารเสี่ยงทั่วทั้งองค์กร (COSO-ERM) และเสนอแนวทางการพัฒนาระบบการบริหารความเสี่ยงภายใต้องค์ประกอบทั้ง 8 องค์ประกอบตามแนวทาง COSO-ERM ผลการศึกษาพบว่า กระบวนการบริหารความเสี่ยงของบริษัท เด สเต โค (เอเชีย) จำกัด มีความสอดคล้องและคล้ายคลึงกับแนวทาง COSO-ERM อยู่ในระดับที่ดี ด้านความเสี่ยงองค์กรต้องมั่นใจว่าพนักงานทุกระดับ มีความรู้ความเข้าใจการบริหารความเสี่ยงอย่างเพียงพอโดยจะต้องมีการประเมินจากแบบทดสอบหรือการจัดกิจกรรมที่เหมาะสม

ฐิติโชค พันศิริพัฒน์ (2558). ทำการศึกษาองค์ประกอบที่มีผลต่อการนำระบบการควบคุมภายในมาใช้ในองค์กร : กรณีศึกษา สำนักงานป้องกันควบคุมโรคที่ 5 จังหวัดราชบุรี จัดทำขึ้น โดยมีวัตถุประสงค์เพื่อศึกษาองค์ประกอบที่มีต่อการนำระบบควบคุมภายในมาใช้ในองค์กร ผลการวิจัยพบว่า องค์ประกอบของการควบคุมภายใน มี 3 ตัวแปรหลัก ประกอบด้วย ปัจจัยด้านสารสนเทศและการติดตามผล ปัจจัยด้านกิจกรรมการควบคุมและการประเมินความเสี่ยง และปัจจัยด้านสภาพแวดล้อมของการควบคุม

บทที่ 3
วิธีดำเนินการวิจัย

การพัฒนาระบบประเมินความเสี่ยง ด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด มีความสำคัญในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เนื่องจากจะทำให้รู้ได้ว่าปัจจุบันองค์กรมีความมั่งคงปลอดภัยด้านเทคโนโลยีสารสนเทศอยู่ในระดับใด ภัยคุกคามใดที่ต้องควรระวัง เมื่อเกิดขึ้นแล้วจะเกิดความเสียหายมากน้อยเพียงใด และสามารถกำหนดแนวทางปฏิบัติในการทำงาน เพื่อลดความเสี่ยงในการทำงานได้ในอนาคต

ผู้ศึกษาได้ทำการศึกษาเกี่ยวกับการควบคุมภายในตามมาตรฐาน COSO : 2013 และการบริหารจัดการความเสี่ยงเป็นแนวทางในการศึกษามาประยุกต์ใช้ในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร คือ สำนักงานจังหวัด ซึ่งทำการศึกษาเฉพาะในส่วน องค์ประกอบที่ 2 : การประเมินความเสี่ยง (Risk Assessment) โดยเฉพาะ

1. เครื่องมือที่ใช้ในการวิจัย

1.1 จัดทำ Web Application เพื่อใช้เป็นระบบต้นแบบในการประเมินความเสี่ยง ประกอบด้วย

1.1.1 Web Server ในการจัดเก็บฐานข้อมูลและโปรแกรมระบบ

1.1.2 โปรแกรมจัดการบริหารเว็บไซต์ (Joomla) ซึ่งเป็นโปรแกรมระบบเปิดเพื่อใช้ในการบริหารจัดการเว็บไซต์

1.1.3 Google chart , Fusion Chart เพื่อใช้ในการกำหนดรูปแบบรายงานแบบ Info graphic

2. ขั้นตอนการดำเนินงาน

2.1 ศึกษากรอบการควบคุมภายในตามมาตรฐาน COSO : 2013 ตามองค์ประกอบที่ 2 การประเมินความเสี่ยง (Risk Assessment) และประยุกต์ให้สอดคล้องกับการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ 4 หลักการ คือ

2.1.1 หลักการที่ 1 – กำหนดเป้าหมายชัดเจน

องค์กรกำหนดเป้าหมายในการพัฒนาด้านเทคโนโลยีสารสนเทศอย่างชัดเจน ว่าต้องการให้พัฒนาไปในทิศทางใด เพื่อที่จะได้ปฏิบัติไปในแนวทางเดียวกัน ทั้งนี้หมายรวมถึงผู้บริหารองค์กร ต้องให้ความสำคัญในการพัฒนาด้านเทคโนโลยีสารสนเทศด้วย กำหนดเป็นนโยบายหลักเพื่อที่จะสื่อสารภายในองค์การให้ทราบทั่วกัน

2.1.2 หลักการที่ 2 – ระบุและวิเคราะห์ความเสี่ยงอย่างครอบคลุม

สำรวจภัยคุกคามที่จะทำให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทุกประเภท ทุกกลุ่มงาน ทุกกระบวนงานที่เกี่ยวข้อง ปัจจัยความเสี่ยงทั้งภายนอก และภายในองค์กร และให้ผู้บริหารมีส่วนร่วมในทุกระดับชั้น ประเมินความสำคัญของความเสี่ยงที่ระบุ และกำหนดแนวทางแก้ไขในแต่ละความเสี่ยงนั้น

2.1.3 หลักการที่ 3 – พิจารณาโอกาสที่จะเกิด

ประเมินโอกาสที่จะเกิดขึ้นของความเสี่ยงที่ได้ระบุไว้ทุกกรณี ความร้ายแรงหากเกิดเหตุ ประเมินความเสียหาย นำเรียนให้ผู้บริหารรับทราบ และมอบนโยบายการป้องกันและการแก้ไข แนวทางปฏิบัติ หากเกิดความเสี่ยงขึ้นจริง และต้องสื่อสารให้บุคลากรในองค์กรรับทราบ พร้อมรับมือกับทุกสถานการณ์หากเกิดเหตุขึ้นจริง

2.1.4 หลักการที่ 4 – ระบุและประเมินความเปลี่ยนแปลงที่จะกระทบต่อองค์กร

ประเมินการเปลี่ยนแปลงสภาพแวดล้อมขององค์กร หากไม่อยากให้เกิดความเสี่ยงขึ้นอีก ทั้งสภาพแวดล้อมภายใน ภายนอก ขั้นตอนการทำงาน ด้านข้อมูล ด้านอุปกรณ์ Hardware Software และบุคลากรเอง และทัศนคติของผู้บริหารองค์กร

2.2 ศึกษาความมั่นคงและปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร ปัจจุบัน องค์กรที่ใช้เป็นกรณีศึกษา คือ สำนักงานจังหวัด ยังไม่มีแนวทางในการปฏิบัติเกี่ยวกับความมั่นคงและปลอดภัยด้านเทคโนโลยีสารสนเทศ เนื่องจากเป็นองค์กรที่มีหน้าที่รับผิดชอบหลากหลาย และมีบุคลากรด้านเทคโนโลยีสารสนเทศน้อยมาก จึงยังไม่มีการปฏิบัติด้านการควบคุมภายใน หรือการบริหารความเสี่ยงในองค์กร

2.3 ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร ขอบเขตของการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร ครอบคลุมด้านเทคโนโลยีสารสนเทศขององค์กร โดยแบ่งกลุ่มงานตามลักษณะงาน แบ่งเป็น 4 กลุ่มงาน คือ 1.) กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด 2.) กลุ่มงานอำนวยการ 3.) กลุ่มงานบริหารทรัพยากรบุคคล และ 4.) ศูนย์ดำรงธรรมจังหวัด

2.3.1 งานตามองค์ประกอบของเทคโนโลยีสารสนเทศ 5 ด้าน ดังนี้

1.) ขั้นตอนการปฏิบัติงาน (Processes)

2.) ข้อมูล (Information)

3.) ซอฟต์แวร์ (Software)

4.) ฮาร์ดแวร์ (Hardware)

5.) บุคลากร (People)

2.3.2 จัดทำรายการภัยคุกคาม (Threat List) ที่สามารถเกิดขึ้นได้ โดยภัยคุกคามที่นำมาพิจารณาแยกเป็นประเภทตามสาเหตุที่เกิดขึ้น เช่น ภัยคุกคามที่เกิดจากธรรมชาติ, ภัยคุกคามที่เกิดจากภายในองค์กร, ภัยคุกคามที่เกิดจากภายนอกองค์กร และ ภัยคุกคามที่เกิดจากสภาพแวดล้อมที่ไม่เหมาะสม โดยอ้างอิงรายการภัยคุกคามของ Supplement to BSI Standard 100-3,Version 2.5 โดยอ้างอิงรายการภัยคุกคาม มีภัยคุกคามหลัก 46 รายการ แต่มีภัยคุกคามส่วนที่เกี่ยวข้องการศึกษาครั้งนี้มี 25 รายการ **(รายละเอียดภาคผนวก ก)**

2.3.3. ประเมินระดับโอกาสที่จะเกิดขึ้น (Likelihood)

ระดับโอกาสที่จะเกิดขึ้น (Likelihood) โดยประเมินค่าโอกาสที่จะเกิดขึ้นที่ภัยคุกคามจะกระทำความเสียหายต่อองค์กรได้ พิจารณาจากแนวโน้มการเกิดขึ้นของภัยคุกคาม ซึ่งอาจเกิดจากแรงจูงใจหรือความรู้ของผู้ใช้งาน ระดับโอกาสที่จะเกิดขึ้น แบ่งออกเป็น 5 ระดับ ตามตารางด้านล่างนี้

ตารางที่ 3.1 ระดับโอกาสที่จะเกิดขึ้น

โอกาสที่จะเกิดขึ้น	**คำอธิบายและหลักเกณฑ์**
สูงมาก (5)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้สูงมาก หรืออาจเกิดขึ้นได้**ทุกสัปดาห์หรือบ่อยกว่า**นั้น
สูง (4)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้สูง หรืออาจเกิดขึ้นได้ประมาณ**เดือนละครั้ง**
ปานกลาง (3)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ปานกลาง หรืออาจเกิดขึ้นได้ประมาณ**ปีละครั้ง**
ต่ำ (2)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ต่ำ หรือในรอบ**ปีอาจเกิดขึ้นได้ 1-2 ครั้ง**
ต่ำมาก (1)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ต่ำมาก หรือในรอบหลาย**ปีอาจเกิดขึ้นได้สักครั้ง หรือแทบเป็นไปไม่ได้ที่จะเกิดขึ้น**

2.3.4 ประเมินผลกระทบ (Impact) จากภัยคุกคาม โดยพิจารณาความรุนแรงที่ได้รับความเสียหายจากภัยคุกคาม ระดับโอกาสที่จะเกิดขึ้น แบ่งออกเป็น 5 ระดับ ตามตารางด้านล่างนี้

ตารางที่ 3.2 ระดับผลกระทบที่จะเกิดขึ้น

ผลกระทบที่จะเกิดขึ้น	**คำอธิบายและหลักเกณฑ์**
สูงมาก (5)	ผลกระทบมีความรุนแรงสูงมาก สร้างความเสียหายสูงมาก
สูง (4)	ผลกระทบมีความรุนแรงสูง สร้างความเสียหายสูง
ปานกลาง (3)	ผลกระทบมีความรุนแรงปานกลาง สร้างความเสียหายปานกลาง
ต่ำ (2)	ผลกระทบมีความรุนแรงต่ำ สร้างความเสียหายต่ำ
ต่ำมาก (1)	ผลกระทบมีความรุนแรงต่ำมาก สร้างความเสียหายต่ำมาก

2.3.5 ประเมินระดับความเสี่ยง

ประเมินระดับความเสี่ยง คำนวณได้จากผลคูณของระดับของผลกระทบ (Impact) และระดับโอกาสที่จะเกิดความเสี่ยงขึ้น (Likelihood)

ระดับความเสี่ยง = ระดับผลกระทบ x ระดับโอกาสที่จะเกิด

ค่าระดับความเสี่ยงให้อ้างอิงจาก ตารางด้านล่างนี้

ตารางที่ 3.3 ตารางแสดงระดับความเสี่ยง

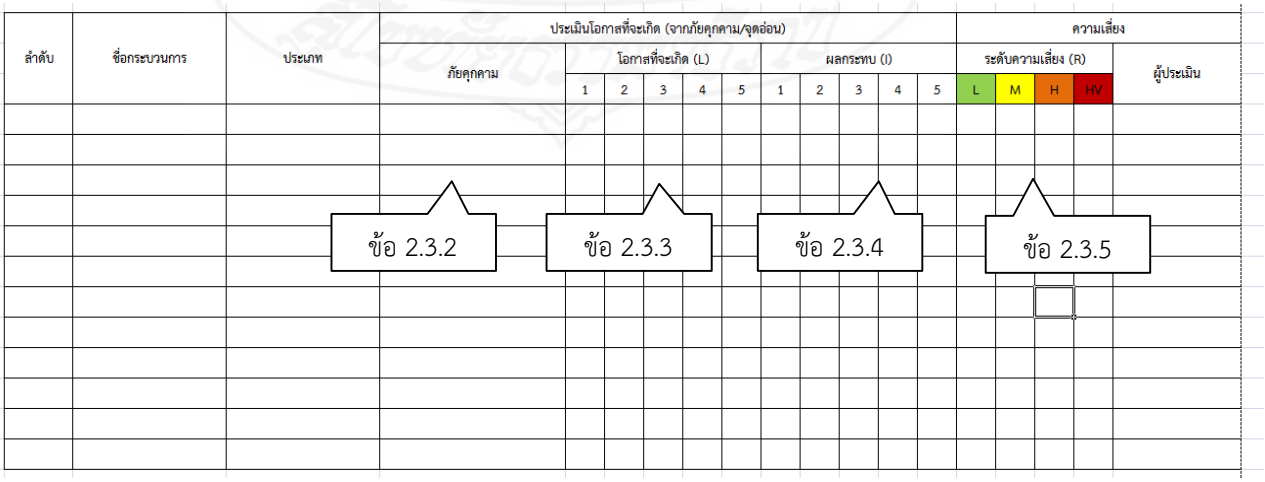
โอกาสที่จะเกิดขึ้น	**ระดับผลกระทบ**				
	(1) = (very Low) ต่ำมาก	(2) = (Low) ต่ำ	(3) = (Medium) ปานกลาง	(4) = (High) สูง	(5) = (Very High) สูงมาก
สูงมาก (5)	(1) x (5) ปานกลาง	(2) x (5) สูง	(3) x (5) สูงมาก	(4) x (5) สูงมาก	(5) x (5) สูงมาก
สูง (4)	(1) x (4) ปานกลาง	(2) x (4) สูง	(3) x (4) สูง	(4) x (4) สูงมาก	(5) x (4) สูงมาก
ปานกลาง (3)	(1) x (3) ปานกลาง	(2) x (3) ปานกลาง	(3) x (3) สูง	(4) x (3) สูง	(5) x (3) สูง
น้อย (2)	(1) x (2) ต่ำ	(2) x (2) ปานกลาง	(3) x (2) ปานกลาง	(4) x (2) สูง	(5) x (2) สูง
น้อยมาก (1)	(1) x (1) ต่ำ	(2) x (1) ต่ำ	(3) x (1) ปานกลาง	(4) x (1) ปานกลาง	(5) x (1) ปานกลาง

ค่าสีในตารางข้างต้นสำหรับช่องที่ถูกแรเงาแบ่งตามสีนั้นเป็นกรณีที่ต้องนำไปดำเนินการหาวิธีแก้ไขความเสี่ยง ความหมายของความเสี่ยงในแต่ละระดับตามตารางที่ 3.3 มีความหมายดังนี้

ตารางที่ 3.4 ตารางแสดงเกณฑ์ในการยอมรับความเสี่ยง

ระดับความเสี่ยง	รายละเอียดความเสี่ยง / เกณฑ์การยอมรับ
สูงมาก (VH) 100 15-25 คะแนน คิดเป็น 57 – 100%	ความเสี่ยงในระดับสูงมาก ไม่สามารถยอมรับได้ ต้องดำเนินการแก้ไขโดยเร็ว
สูง (H) (8-14 คะแนน) คิดเป็น 29 – 56%	ความเสี่ยงในระดับสูง ไม่สามารถยอมรับได้ สามารถดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสม
ปานกลาง (M) (4-7 คะแนน) คิดเป็น 13 – 28%	ความเสี่ยงในระดับปานกลาง ควรพิจารณาแก้ไขความเสี่ยง หากมีเหตุผลความจำเป็น ก็สามารถยอมรับได้
ต่ำ (L) 12 (1-3 คะแนน) คิดเป็น 1 – 12%	ความเสี่ยงในระดับที่ต่ำ ควรพิจารณาแก้ไขความเสี่ยง แต่สามารถยอมรับได้โดยไม่ต้องดำเนินการใดๆ

ตารางที่ 3.5 ตารางสรุปขั้นตอนในการประเมินความเสี่ยง หัวข้อที่ 2.3.2 – 2.3.5



2.3.6 การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับกาประเมินความสำคัญแล้วต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ อาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้(Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

การหลีกเลี่ยง (Terminate)

เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกกิจกรรมที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้น

การยอมรับ (Take)

เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในภาวะที่องค์กรยอมรับได้

การควบคุม (Treat)

เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า

การถ่ายโอน (Transfer)

การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

2.4 พัฒนาระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

2.4.1 แนวคิดในการออกแบบและพัฒนาระบบ

1) ออกแบบและจัดทำ Web Application เพื่อใช้ในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

2) ทดสอบการใช้งานระบบ

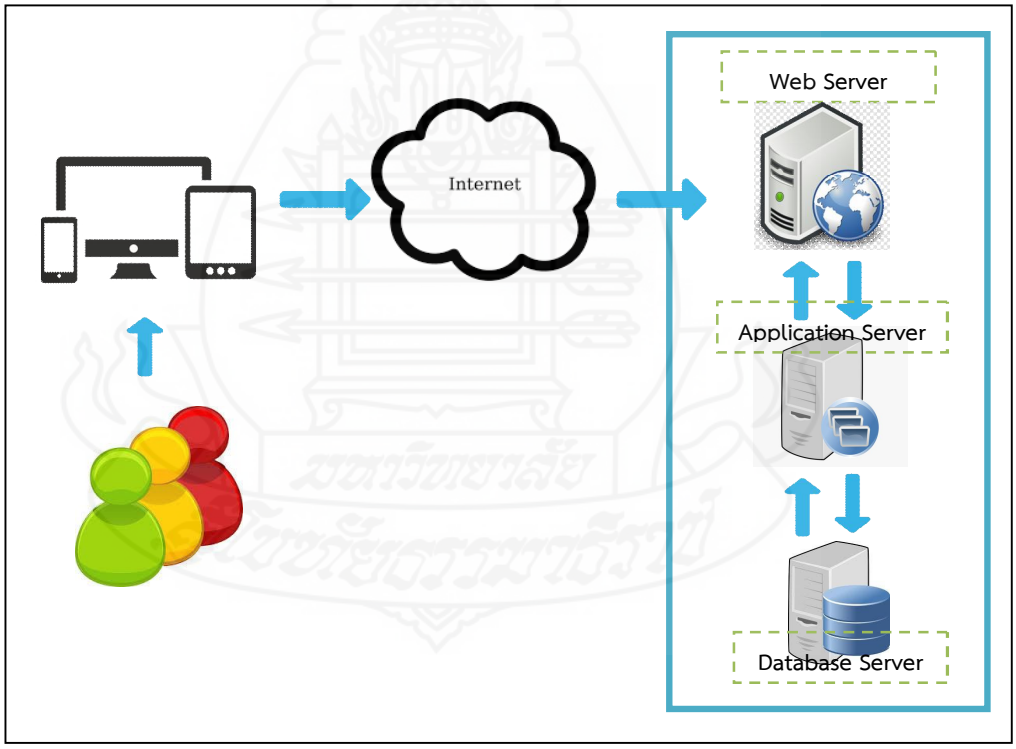
2.4.2 ภาษาและเครื่องมือที่ใช้ในการพัฒนาระบบ

1) ใช้โปรแกรม CMS (Joomla) โดยมีฐานเป็นภาษา PHP ในการพัฒนาระบบซึ่งงานต่อการบริหารจัดการ มีประสิทธิภาพและมีความยืดหยุ่นสูง

2) ใช้โปรแกรม Adobe Dreamweaver ในการออกแบบและจัดการ User Interface

3) ใช้โปรแกรม Adobe Photoshop ตกแต่งและออกแบบเว็บไซต์

4) ใช้ My SQL เป็น Database สำหรับจัดเก็บข้อมูล



ภาพที่ 3.1 โครงสร้างการทำงานของระบบประเมินความเสี่ยง

2.4.3 ฟังก์ชั่นการทำงานของระบบ

1) ระบบบริหารจัดการการเข้าใช้งานสำหรับผู้ใช้งาน
2) ระบบประเมินความเสี่ยง ด้านเทคโนโลยีสารสนเทศ
3) ระบบแสดงผล และรายงานการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักงานจังหวัด
4) แสดงเอกสารและดาวน์โหลดเอกสารแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ

บทที่ 4
ผลการดำเนินการวิจัย

1. ข้อมูลพื้นฐานองค์กร

สำนักงานจังหวัด ถือเป็นส่วนราชการส่วนภูมิภาคประจำจังหวัด สังกัดสำนักงานปลัดกระทรวงมหาดไทย เป็นเสมือนสำนักงานของผู้ว่าราชการจังหวัด แบ่งออกเป็น 4 กลุ่มงาน คือ 1) กลุ่มงานอำนวยการ 2) กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด 3) กลุ่มงานบริหารทรัพยากรบุคคล และ 4) กลุ่มงานศูนย์ดำรงธรรมจังหวัด มีหน้าที่คือ

- แปลงยุทธศาสตร์การพัฒนาระดับชาติไปเป็นยุทธศาสตร์การพัฒนาจังหวัดในพื้นที่
- พัฒนาระบบข้อมูลสารสนเทศเพื่อบริหาร ระบบสารสนเทศภูมิศาสตร์เพื่อการวางแผน และเครือข่ายสารสนเทศของจังหวัดและเป็นศูนย์สารสนเทศของจังหวัดเพื่อการบริหารและการวางแผนพัฒนาจังหวัด
- จัดทำแผนพัฒนาจังหวัดและดำเนินการตามแผน
- กำกับและติดตามผลการดำเนินงานตามแผนยุทธศาสตร์การพัฒนาจังหวัด
- อำนวยการ ประสานและปฏิบัติตามอำนาจหน้าที่ของผู้ว่าราชการจังหวัด
- ดำเนินการในภารกิจที่ได้รับมอบหมาย กรณีที่ไม่มีการจัดตั้งส่วนราชการขึ้นรับผิดชอบ ในระดับจังหวัด
- ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

2. โครงสร้างการบริหารงานสำนักงานจังหวัด

สำนักงานจังหวัด มีอำนาจหน้าที่และโครงสร้างภารกิจและการแบ่งงานภายในของสำนักงานจังหวัด เป็นกลุ่มงานต่าง ๆ 1) กลุ่มงานอำนวยการ 2) กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด 3) กลุ่มงานบริหารทรัพยากรบุคคล และ 4) กลุ่มงานศูนย์ดำรงธรรมจังหวัด ตามภาพด้านล่างนี้

ภาพที่ 4.1 โครงสร้างการบริหารงานสำนักงานจังหวัด

ที่มา มติ อ.ก.พ.มท. ครั้งที่ 3/2559 เมื่อวันที่ 28 เมษายน 2559

2.1 โครงสร้างการบริหารงานด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

สำนักงานจังหวัด มีการบริหารจัดการงานเทคโนโลยี โดยมีนักวิชาการคอมพิวเตอร์ 1 คน สังกัดกลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด เสนอผ่านหัวหน้าสำนักงานจังหวัด รองผู้ว่าราชการจังหวัด (CIO) และผู้ว่าราชการจังหวัด แผนผัง ดังนี้

โครงสร้างการบริหารงาน
ด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

ภาพที่ 4.2 โครงสร้างการบริหารงานด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

2.2 โครงสร้างพื้นฐานและทรัพยากรด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

2.2.1 ระบบเครือข่ายที่มีอยู่

1) เครือข่าย MOI Net เป็นเครือข่ายอินเตอร์เน็ตภายในของกระทรวงมหาดไทย (Ministry Of Interior) ซึ่งรับสัญญาณมาจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงมหาดไทย โดยผ่านสายใยแก้วนำแสง (Fiber Optic) มายังศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เขต 10 สุราษฎร์ธานี และกระจายมายังสำนักงานจังหวัดสุราษฎร์ธานี โดยจำกัดความเร็วในการใช้งานอินเตอร์เน็ต

2) เครือข่าย GIN (Government Information Network) หรือ เครือข่ายสารสนเทศภาครัฐ เครือข่ายความเร็วสูงที่มีประสิทธิภาพและคุณภาพ มีความปลอดภัยสูง เพื่อรองรับ

งานให้บริการประชาชน และการเชื่อมโยงระหว่างหน่วยงานภาครัฐทั้งหมด อันเป็นโครงสร้างพื้นฐานระบบแรกของโครงการ e-Government การบริการประชาชนจะมีความ**สะดวก รวดเร็ว** ในการติดต่อหน่วยงานภาครัฐ ซึ่งสำนักงานจังหวัดสุราษฎร์ธานี ใช้เพื่อการให้บริการข้อมูลข่าวสารผ่านเว็บไซต์จังหวัดสุราษฎร์ธานี (www.suratthani.go.th)

2.2.2 รายการอุปกรณ์ระบบเครือข่ายของสำนักงานจังหวัด ประกอบด้วย

1) ระบบ ATM (Asynchronous Transfer Mode) คือระบบสื่อสารข้อมูลความเร็วสูง ซึ่งสามารถใช้รับส่งข้อมูลได้ทุกรูปแบบ (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) ระบบสำรองไฟฟ้า

8) ระบบปรับอากาศในห้องศูนย์ปฏิบัติการจังหวัด ประกอบด้วยเครื่องปรับอากาศแบบแขวน ขนาด 32,000 BTU จำนวน 4 ตัว

ระบบเครือข่ายที่ติดตั้ง ณ สำนักงานจังหวัดใช้เครือข่ายภายในของกระทรวงมหาดไทย (MOI Net) โดยใช้ระบบ ATM Access รับสัญญาณผ่านสายไฟเบอร์ออฟติกจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เขต 10 สุราษฎร์ธานี เข้ามายังศาลากลางจังหวัด ใช้อุปกรณ์ Layer 2 Switch กระจายสัญญาณอินเตอร์เน็ตไปยังสำนักงานภายในอาคารศาลากลางจังหวัด รวมถึงภายในสำนักงานจังหวัดด้วย

2.2.3 ปัญหาที่พบ

1) อุปกรณ์ที่ใช้งานในปัจจุบันเป็นอุปกรณ์รุ่นเก่า ไม่สามารถรองรับภัยคุกคามคอมพิวเตอร์หรือการโจมตีรูปแบบใหม่ ๆ ได้ ส่งผลให้การใช้งานระบบเครือข่ายในหน่วยงานไม่มีประสิทธิภาพ

2) เครื่องคอมพิวเตอร์แม่ข่าย (Server) สามารถเข้าถึงได้โดยตรง

3) การเชื่อมต่อสวิตซ์หลายตัวแบบเชื่อมต่อกันไปเรื่อย ๆ ส่งผลให้ประสิทธิภาพในการทำงานช้าลง และไม่มีความปลอดภัยในการใช้งาน

4) ไม่สามารถบริหารจัดการระบบเครือข่ายได้ เนื่องจากขาดอุปกรณ์ในการควบคุมและการบริหารจัดการระบบเครือข่ายที่ดี

5) ปัญหาความเร็วที่จำกัด ในการใช้งานอินเทอร์เน็ต หากมีการประชุมทางไกลจากกระทรวงมหาดไทยถึงจังหวัด จะส่งผลกระทบทำให้ระบบเครือข่ายอินเตอร์เน็ตช้าลง

2.2.4 ระบบเทคโนโลยีสารสนเทศภายในองค์กร

- กลุ่มงานอำนวยการ มีระบบงาน คือ

1) ระบบสารบรรณอิเลกทรอนิกส์ของจังหวัด เป็นระบบงานที่ใช้สำหรับการรับ-ส่งหนังสือราชการภายในจังหวัดสุราษฎร์ธานี เป็นระนาบเดียวกัน เพื่อการเผยแพร่ข้อมูลข่าวสารจากผู้ว่าราชการจังหวัดด้วยความรวดเร็ว ถูกต้อง และเป็นไปในแนวทางเดียวกัน ทั้งนี้สามารถประหยัดงบประมาณในการจัดซื้อกระดาษ และค่าจัดส่งเอกสารทางไปรษณีย์

2) ระบบจองห้องประชุมออนไลน์ เป็นระบบงานในการบริหารจัดการการใช้งานห้องประชุมโดยผ่านระบบออนไลน์ ซึ่งหน่วยงานภายนอกสามารถเข้าจองห้องประชุมหรือตรวจสอบการใช้งานห้องประชุมภายในศาลากลางจังหวัดได้

3) ระบบจัดเก็บทะเบียนทรัพย์สิน เป็นระบบงานที่ใช้รวบรวมข้อมูลครุภัณฑ์ของสำนักงานจังหวัด โดยระบุถึงชื่อทรัพย์สิน วันที่ได้มา เลขครุภัณฑ์ ผู้ครอบครอง และมูลค่าทรัพย์สินปัจจุบัน

4) ระบบจัดซื้อจัดจ้างภาครัฐ (e-GP) เป็นระบบบริหารจัดการการจัดซื้อจัดจ้างตามระเบียบของกรมบัญชีกลาง โดยสามารถประกาศหาผู้ค้าได้โดยผ่านระบบออนไลน์ ซึ่งผู้ค้าสามารถเข้ามาดูข้อมูลได้เอง และยื่นเอกสารผ่านระบบได้ทันที

5) ระบบการบริหารงานการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ หรือ ระบบ GFMIS ซึ่งเป็นการดำเนินงานบริหารจัดการด้านการเงินการคลังของภาครัฐให้มีความทันสมัยและมีประสิทธิภาพยิ่งขึ้น โดยนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ เพื่อปรับกระบวนการดำเนินงานและการจัดการภาครัฐด้านการ งบประมาณ การบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหาร

ทรัพยากร ให้เป็นไปในทิศทางเดียวกับนโยบายปฏิรูปราชการที่เน้นประสิทธิภาพและความคล่องตัวในการดำเนินงาน

- กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด ระบบงานคือ ระบบติดตามประเมินผลแผนงาน/โครงการตามแผนปฏิบัติการจังหวัด ประจำปีงบประมาณ (PADME) เพื่อใช้สำหรับบริหารจัดการแผนงาน/โครงการจากทุกแหล่งงบประมาณที่ดำเนินการในพื้นที่
- กลุ่มงานบริหารทรัพยากรบุคคล ระบบงานคือ ระบบสารสนเทศทรัพยากรบุคคลระดับจังหวัด (PPIS) เป็นเครื่องมือช่วยในการบริหารจัดการเกี่ยวกับข้าราชการและลูกจ้างประจำระดับจังหวัด เพื่อให้สามารถใช้งานในการบริหารงานบุคคลให้แก่ส่วนราชการได้อย่างมีประสิทธิภาพมากยิ่งขึ้น
- กลุ่มงานศูนย์ดำรงธรรมจังหวัด ระบบงาน คือ ระบบงานรับและติดตามเรื่องราวร้องทุกข์ของศูนย์ดำรงธรรม

ตารางที่ 4.1 ระบบเทคโนโลยีสารสนเทศภายในองค์กร

กลุ่มงานอำนวยการ	
ระบบเทคโนโลยีสารสนเทศ	รายละเอียด
1. ระบบสารบรรณอิเล็กทรอนิกส์	- ติดตั้ง server เอง ใช้ Window Server 2013 - ขออนุเคราะห์ระบบมาจากกระทรวงมหาดไทย - ทำการดูแลรักษาเอง โดยบุคลากรในสำนักงาน
2: ระบบจองห้องประชุมออนไลน์	- ติดตั้ง server เอง ใช้ Window Server 2013 - จัดทำระบบเอง - ทำการดูแลรักษาเอง โดยบุคลากรในสำนักงาน
3. ระบบจัดเก็บทะเบียนทรัพย์สิน	- ใช้ MS Excel ในการจัดเก็บข้อมูล - ผู้ใช้งานดูแลได้เอง
4. ระบบจัดซื้อจัดจ้างภาครัฐ ด้วยระบบอิเล็กทรอนิกส์ e-GP	- ปฏิบัติงานผ่าน Website ของกรมบัญชีกลาง - มี user/password ในการเข้าใช้งานระบบ
5. ระบบ GFMIS	- ปฏิบัติงานผ่านเครื่อง Terminal ที่ติดตั้งไว้ที่สำนักงาน - มี key card และ password ในการระบุตัวตน

ตารางที่ 4.1 (ต่อ)

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด	
ระบบเทคโนโลยีสารสนเทศ	รายละเอียด
6. ระบบติดตามและประเมินผลโครงการ (PADME)	- ปฏิบัติงานผ่าน Website ของกระทรวงมหาดไทย - มี user/password ในการเข้าใช้งานระบบ

กลุ่มงานบริหารทรัพยากรบุคคล	
ระบบเทคโนโลยีสารสนเทศ	รายละเอียด
7. ระบบสารสนเทศทรัพยากรบุคคลระดับจังหวัด (PPIS)	- ติดตั้ง server เอง ใช้ Window Server 2013 - ขออนุเคราะห์ระบบมาจาก กพ. - ทำการดูแลรักษาเอง โดยบุคลากรในสำนักงาน

กลุ่มงานศูนย์ดำรงธรรมจังหวัด	
ระบบเทคโนโลยีสารสนเทศ	รายละเอียด
8. ระบบงานรับและติดตามเรื่องร้องทุกข์ของศูนย์ดำรงธรรม	- ติดตั้ง server เอง ใช้ Window Server 2013 - ขออนุเคราะห์ระบบมาจากกระทรวงมหาดไทย - ทำการดูแลรักษาเอง โดยบุคลากรในสำนักงาน

3. การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร

ผลการประเมินความเสี่ยงด้านเทคโนโลยีขององค์กร โดยใช้เครื่องมือในบทที่ 3 ตามภาพที่ 3.4 ได้ผลลัพธ์ดังตัวอย่างตามตารางนี้ (รายละเอียดผนวก ข) ตามตัวอย่างเป็นการประเมินความเสี่ยงในระบบสารบรรณอิเล็กทรอนิกส์ของสำนักงานจังหวัดสุราษฎร์ธานี

ตารางที่ 4.2 การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร

ลำดับ	ภัยคุกคาม	ประเภท	ประเมินโอกาสที่จะเกิด (จากภัยคุกคาม/จุดอ่อน)										ความเสี่ยง				
			โอกาสที่จะเกิด (L)					ผลกระทบ (I)					ระดับความเสี่ยง (R)				ผู้ประเมิน
			1	2	3	4	5	1	2	3	4	5	L	M	H	HV	
1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง	ข้อมูล (Information)		2						3				6			ประภาศรี
2	การล้วงความลับหรือข้อมูลจากระบบ	ข้อมูล (Information)	1							3			3				ประภาศรี
3	ความลับถูกเปิดเผย	ข้อมูล (Information)	1							3			3				ประภาศรี
4	ข้อมูลขาดความน่าเชื่อถือ	ข้อมูล (Information)	1									5		5			ประภาศรี
5	การจัดการข้อมูลไม่ดี	ข้อมูล (Information)	1									5		5			ประภาศรี
6	การปฏิเสธความรับผิดชอบ	ขั้นตอนการปฏิบัติงาน (Processes)	1							3			3				ประภาศรี
7	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	ขั้นตอนการปฏิบัติงาน (Processes)	1							3			3				ประภาศรี
8	ไม่มีการวางแผนและการปรับปรุงแผนงาน	ขั้นตอนการปฏิบัติงาน (Processes)			3					3					9		ประภาศรี
9	การละเมิดกฎหมาย หรือข้อบังคับ	ขั้นตอนการปฏิบัติงาน (Processes)	1							3			3				ประภาศรี
10	ช่องโหว่ของซอฟต์แวร์	ซอฟต์แวร์ (Software)	1									5		5			ประภาศรี
11	การถูกโจมตี	ซอฟต์แวร์ (Software)	1									5		5			ประภาศรี
12	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	บุคลากร (People)	1									5		5			ประภาศรี
13	การเข้าถึงสถานที่หรือบริเวณต้องห้าม	บุคลากร (People)		2								5			10		ประภาศรี
14	การเข้าถึงระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			ประภาศรี
15	การจัดการอุปกรณ์หรือระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			ประภาศรี
16	การจัดการดูแลอุปกรณ์หรือระบบโดยไม่ถูกต้อง	บุคลากร (People)	1									5		5			ประภาศรี
17	ขาดแคลนบุคลากร	บุคลากร (People)				4						5				20	ประภาศรี
18	เพลิงไหม้	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศรี
19	ความเสียหายจากน้ำ	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศรี
20	ฝุ่น สนิม มลพิษ	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศรี
21	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	ฮาร์ดแวร์ (Hardware)		2						3				6			ประภาศรี
22	หยุดทำงานเนื่องจากบริการพื้นฐาน (Mains supply)	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศรี
23	การจัดการฮาร์ดแวร์และซอฟ์ฟแวร์ไม่ดี	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศรี
24	ความผิดปกติ/ความล้มเหลวของอุปกรณ์หรือระบบ	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศรี
25	ขาดแคลนทรัพยกร	ฮาร์ดแวร์ (Hardware)			3					3					9		ประภาศรี

4. พัฒนาระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด

ฟังก์ชันการทำงานของระบบ

4.1 ระบบบริหารจัดการการเข้าใช้งาน

4.1.1 สำหรับผู้ใช้งานทั่วไป

1) ระบบสามารถแสดงรายละเอียดมาตรฐาน COSO : 2013 (5 องค์ประกอบ 17 หลักการ)
2) ระบบสามารถดาวน์โหลดข้อมูล เกี่ยวกับวัตถุประสงค์ของการใช้งานระบบ แนวทางปฏิบัติที่เกี่ยวข้อง
3) ผู้ใช้งานทั่วไปสามารถขอลงทะเบียน เพื่อเข้าใช้งานระบบเฉพาะผู้ที่ได้ทำการลงทะเบียนแล้ว

4.1.2 สำหรับผู้ใช้งานที่ลงชื่อเข้าใช้งาน

1) ผู้ใช้งานต้องทำการลงทะเบียนเพื่อเข้าใช้งานระบบ และต้องได้รับการอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งาน
2) ผู้ที่ได้รับอนุญาตต้องลงชื่อเข้าใช้ระบบทุกครั้งที่ทำการใช้งาน และออกจากระบบอัตโนมัติเมื่อไม่มีการใช้งานเป็นระยะเวลาเกิน 15 นาที (900 วินาที)

4.2 ระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำหรับผู้ใช้งานที่ลงทะเบียนเข้าใช้งานระบบ แสดงหน้าหลัก 3 ส่วนคือ เกณฑ์การประเมิน, ระบบประเมินความเสี่ยง และ รายงาน

4.2.1 เมนูเกณฑ์การประเมิน

ระบบแสดงเกณฑ์การประเมิน ค่าคะแนนความเสี่ยง เขียว เหลือง แดง ช่วงคะแนนที่กำหนด

4.2.2 เมนูระบบประเมินความเสี่ยง

ระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยสามารถ checklist ตามภัยคุกคามที่มีโอกาสเกิดขึ้นในระบบต่าง ๆ ได้หรือไม่ ซึ่งเป็นภัยคุกคามที่เกี่ยวกับด้านขั้นตอนการทำงาน, ด้านข้อมูล ,ด้านฮาร์ดแวร์, ซอฟต์แวร์ และด้านบุคลากร พร้อมคำนวณระดับความเสี่ยงที่ได้จากการประเมินความเสี่ยง

4.2.3 เมนูแสดงรายงานผล

เป็นการแสดงผลและรายงานการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด ซึ่งแสดงผลเป็นรูปกราฟ ง่ายต่อการเปรียบเทียบ

ภาพที่ 4.3 หน้าหลักระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

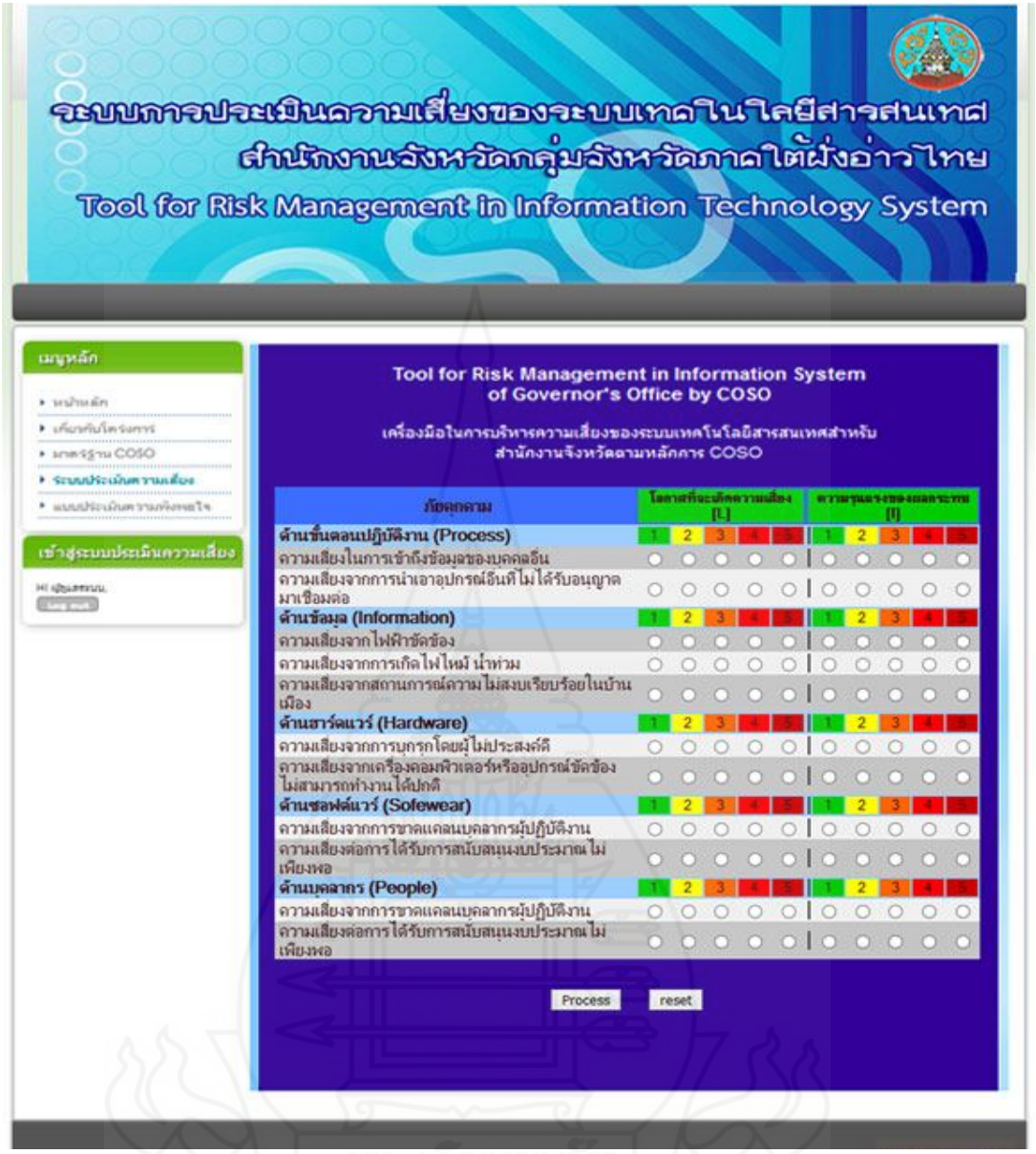
หน้านี้สามารถเข้าดูรายละเอียดเกี่ยวกับโครงการ มาตรฐาน COSO แนวทางในการปฏิบัติที่ถูกต้อง และการลงทะเบียนสำหรับผู้ใช้รายใหม่

ภาพที่ 4.4 หน้าลงทะเบียนผู้ใช้งาน

เมื่อทำการคลิกที่ ลงทะเบียน จะสามารถเข้ามากรอกข้อมูลผู้ใช้งาน Username และรหัสผ่าน Password โดยที่ผู้ใช้งานสามารถกำหนดได้เอง

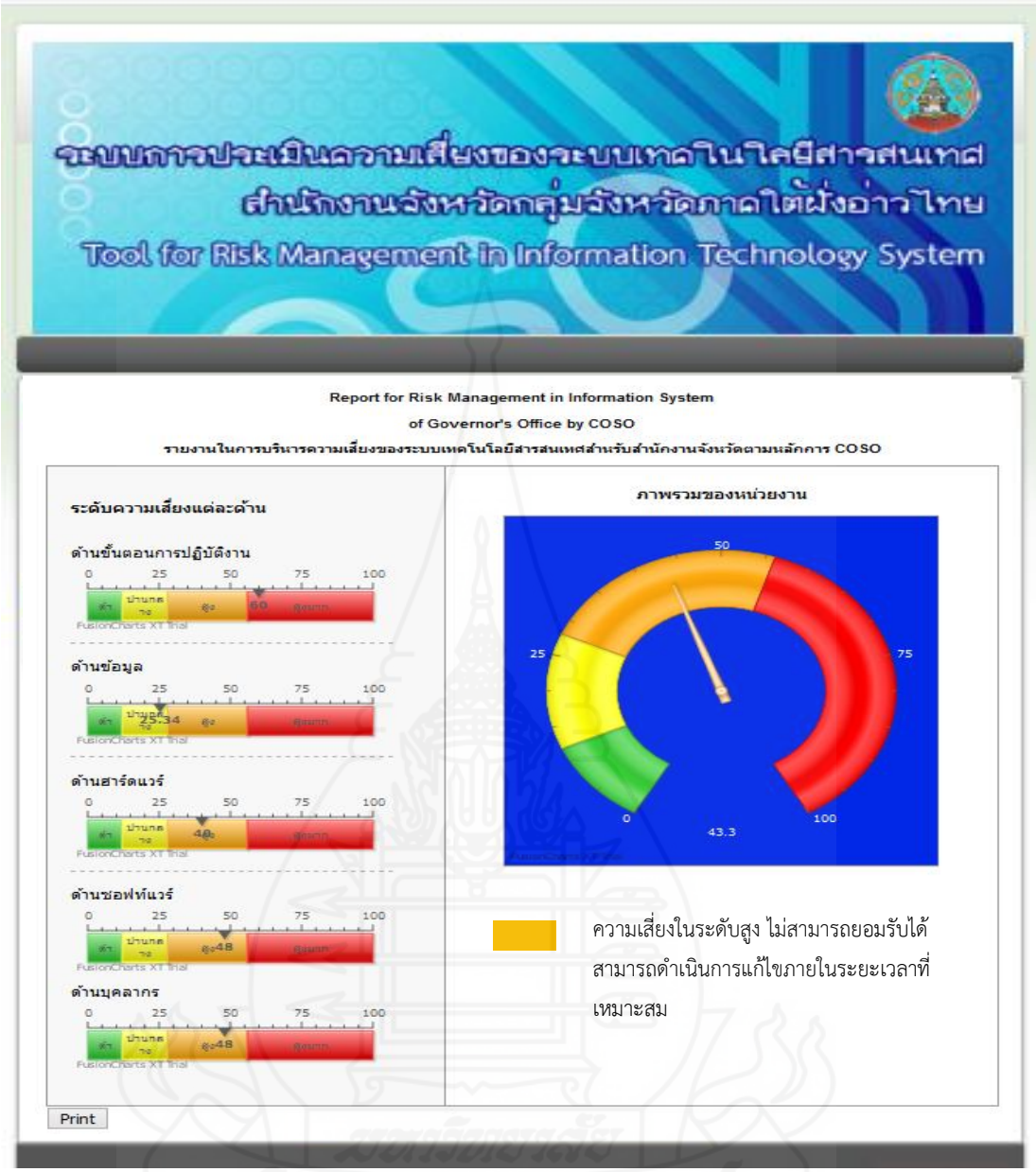
ภาพที่ 4.5 หน้าเข้าสู่ระบบ

เมื่อทำการลงทะเบียนแล้ว สามารถเข้าใช้งานระบบ login ได้ทันที ทางช่องเมนูด้านซ้ายมือ ใส่ Username และ password ที่ผู้ใช้กำหนดไว้ แล้วคลิกที่ปุ่ม login



ภาพที่ 4.6 หน้าประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เมื่อ login เข้าสู่ระบบแล้ว ระบบจะกำหนดให้มาที่หน้าแบบประเมินเป็นหน้าแรก ผู้ใช้งานสามารถคลิกเพื่อประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรได้ทันที โดยแยกการประเมินตามภัยคุกคามแบ่งออกเป็น 5 ด้าน คือ ด้านขั้นตอนการปฏิบัติงาน ด้านข้อมูล ด้านฮาร์ดแวร์ ด้านซอฟท์แวร์ และด้านบุคลากร ผู้ใช้งานสามารถเลือกโอกาสที่จะเกิด และผลกระทบเมื่อเกิดภัยคุกคาม ระดับคะแนน 1-5 1 2 3 4 5 สีเขียว คือ ต่ำ สีแดง คือ สูง จากนั้นคลิกที่ปุ่ม Process เพื่อให้ระบบทำการประมวลผลเพื่อคำนวณค่าความเสี่ยง หรือหากต้องการคลิกเลือกใหม่ สามารถคลิกที่ปุ่ม reset ได้ทันที



ภาพที่ 4.7 หน้ารายงานผลการประเมินความเสี่ยง

เมื่อทำการคลิกปุ่ม Process แล้ว ระบบจะทำการประมวลผลแล้วแสดงค่าความเสี่ยงออกมาเป็นรายงานในรูปแบบของกราฟ แยกออกเป็นแต่ละด้านรวม 5 ด้าน คือ ด้านขั้นตอนการปฏิบัติงาน ด้านข้อมูล ด้านฮาร์ดแวร์ ด้านซอฟท์แวร์ และด้านบุคลากร และสรุปภาพรวมขององค์กรโดยแบ่งเป็นเกณฑ์สี พร้อมคำอธิบายว่า อยู่ในค่าระดับความเสี่ยงเท่าใด และควรปฏิบัติอย่างไร

บทที่ 5
สรุปผลการวิจัยอภิปรายผลและข้อเสนอแนะ

1. สรุปผลการวิจัย

จากการที่ได้ทำการศึกษาและพัฒนาระบบประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศเพื่อทำการประเมินความเสี่ยงของสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทย มีวัตถุประสงค์เพื่อพัฒนาแนวทางปฏิบัติในการประเมินความเสี่ยงระบบเทคโนโลยี และพัฒนาระบบประเมินความเสี่ยงระบบเทคโนโลยีให้กับสำนักงานจังหวัดในการประเมินตนเองสถานะตนเองจากภัยคุกคามด้านต่าง ๆ จึงขอสรุปผลการศึกษา ดังนี้

1.1 สรุปผลการประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศตามหลัก COSO

การประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศขององค์กรทำให้ทราบถึงสถานะความเสี่ยงขององค์กรว่าอยู่ในระดับปานกลางถึงสูง โดยได้พบความเสี่ยงขององค์กรแต่ละจังหวัดในแต่ละด้าน ดังตารางด้านล่างนี้

ตารางที่ 5.1 ตารางสรุปผลการประเมินความเสี่ยงแยกรายจังหวัด

จังหวัด	ค่าระดับความเสี่ยงในแต่ละด้าน																			
	ขั้นตอนการปฏิบัติงาน				ข้อมูล				ซอฟต์แวร์				ฮาร์ดแวร์				บุคลากร			
	L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
สุราษฎร์ธานี	3		1		2	3				2				7	1			4	1	1
ชุมพร	2		2			2	3			1	1			2	4	2		6		
สงขลา		2	2		1	3	1				2			1	7			5	1	
นครศรีธรรมราช		2	1	1		1	2	2				2		4	1	3		5		1
พัทลุง		3	1			2	3			1	1			7	1			4	2	

หลังจากที่ทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัด ในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทยตามตาราง สรุปได้ดังนี้

- จังหวัดสุราษฎร์ธานี

ความเสี่ยงต่ำ	5	รายการ
ความเสี่ยงปานกลาง	16	รายการ
ความเสี่ยงสูง	3	รายการ
ความเสี่ยงสูงมาก	1	รายการ

- จังหวัดชุมพร

ความเสี่ยงต่ำ	2	รายการ
ความเสี่ยงปานกลาง	11	รายการ
ความเสี่ยงสูง	16	รายการ
ความเสี่ยงสูงมาก	2	รายการ

- จังหวัดสงขลา

ความเสี่ยงต่ำ	1	รายการ
ความเสี่ยงปานกลาง	11	รายการ
ความเสี่ยงสูง	13	รายการ
ความเสี่ยงสูงมาก	-	รายการ

- จังหวัดนครศรีธรรมราช

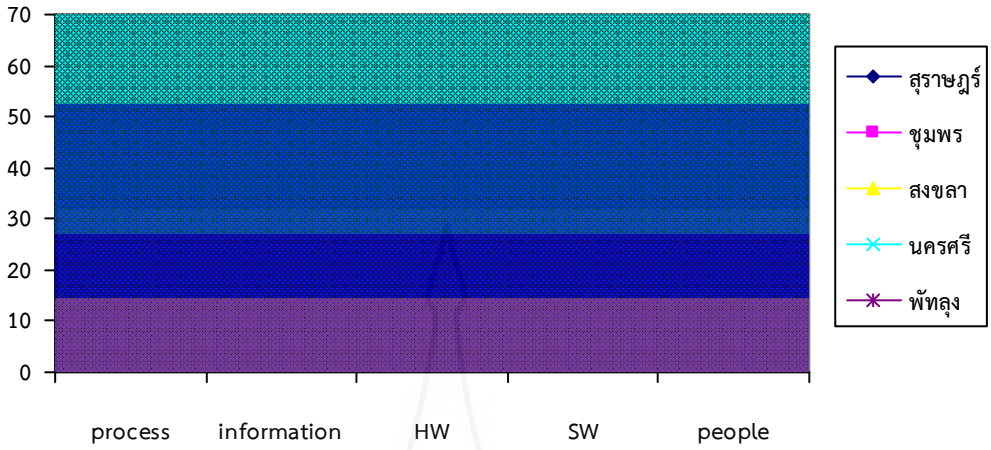
ความเสี่ยงต่ำ	-	รายการ
ความเสี่ยงปานกลาง	12	รายการ
ความเสี่ยงสูง	4	รายการ
ความเสี่ยงสูงมาก	9	รายการ

- จังหวัดพัทลุง

ความเสี่ยงต่ำ	-	รายการ
ความเสี่ยงปานกลาง	17	รายการ
ความเสี่ยงสูง	8	รายการ
ความเสี่ยงสูงมาก	-	รายการ

1.2 สรุปผลการประเมินความเสี่ยงด้านเทคโนโลยี

จากการพัฒนาระบบการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ มาใช้ประเมินความเสี่ยงของสำนักงานจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทยนั้น ปรากฏว่าเป็นการประเมินความเสี่ยงตนเอง ซึ่งทำให้รู้ถึงศักยภาพของสำนักงานจังหวัดว่ามีความพร้อมในการดูแลระบบด้านเทคโนโลยีสารสนเทศของแต่ละจังหวัดมากน้อยเพียงใด ซึ่งผลการประเมินมีรายละเอียดดังนี้



ภาพที่ 5.1 กราฟแสดงผลการประเมินความเสี่ยงรายจังหวัด

จากการประเมินจะเห็นได้ว่า ผู้ดูแลระบบในแต่ละจังหวัดในกลุ่มจังหวัดภาคใต้ฝั่งอ่าวไทย ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของตนเองเป็นค่าความเสี่ยงปานกลางถึงสูง สามารถวิเคราะห์ได้ว่า

1. สำนักงานจังหวัดไม่มีระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นมาตรฐานเดียวกันทั้งหมด
2. ผู้ดูแลระบบ ไม่มีการประสานงาน หรือซักซ้อมแนวทางให้เข้าใจไปในทิศทางเดียวกัน หรือต่างคน ต่างทำงานไม่ได้บูรณาการงานร่วมกัน
3. หน่วยงานต้นสังกัดไม่ได้ตีกรอบหรือกำหนดแนวทางให้ถูกต้อง จึงทำให้ประเมินความเสี่ยงออกมาที่ค่อนข้างแตกต่างกัน

2. ข้อเสนอแนะ

1. เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศมีความปลอดภัยในการใช้งานระบบควรมีการพัฒนานโยบายและแนวทางการปฏิบัติงานที่เกี่ยวข้องให้ครอบคลุมตามแนวทางของมาตรฐาน COSO ตามที่ได้จัดทำขึ้น อย่างน้อยปีละ 1 ครั้ง เพื่อให้ทราบสถานะความเสี่ยงในปัจจุบัน
2. เทคโนโลยีในปัจจุบันมีการพัฒนาอย่างรวดเร็ว ความเสี่ยงด้านเทคโนโลยีก็สูงตามไปด้วย ดังนั้น การจัดทำนโยบายการรักษาความปลอดภัยสารสนเทศเพื่อบริหารความเสี่ยง จึงจำเป็นต้องมีการพัฒนาและปรับปรุงอยู่เสมอ เพื่อให้ทันต่อเหตุการณ์เหมาะสมต่อเทคโนโลยี
3. ผู้ดูแลระบบ ผู้จัดทำ และผู้บริหาร ควรมีความรู้ ความใส่ใจในการตั้งนโยบายหรือแนวทางปฏิบัติในการบริหารความเสี่ยงของด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเข้าใจในกระบวนการจัดทำโดยสมบูรณ์ ครบถ้วน และเข้าใจไปในแนวทางเดียวกัน

ทั้งนี้ สำหรับการนำเอาแนวทางมาตรฐาน COSO เข้ามาใช้ในหน่วยงานนั้นต้องได้รับการสนับสนุน จากผู้บริหารระดับสูงของหน่วยงาน เนื่องจากปัญหาที่เกิดขึ้นส่วนใหญ่ คือ ผู้บริหารระดับสูงมักจะไม่เห็นความสำคัญของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยมองเป็นเรื่องไกลตัว ไม่ได้คำนึงถึงผลกระทบที่เกิดจากความเสี่ยงด้านสารสนเทศ ว่าดำเนินการอย่างปลอดภัยหรือไม่ และต้องเผยแพร่ความรู้ เพื่อความเข้าใจของบุคลากรภายในองค์กร และได้รับความร่วมมือจากบุคลากรขององค์กรทุกระดับชั้นด้วย

บรรณานุกรม

บรรณานุกรม

พลภัทร สุนทรทิวกร, ดร.วิภา เจริญภัณฑารักษ์. (2560). *การพัฒนาระบบประเมินความเสี่ยงและความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์* (รายงานการศึกษาค้นคว้าอิสระ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยสุโขทัยธรรมาธิราช, นนทบุรี.

วิไลวรรณ ทาน้อย, ดร.วิภา เจริญภัณฑารักษ์. (2560). *ระบบจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 เพื่อควบคุมการเข้าถึงระบบสารสนเทศ สำหรับสำนักงานจังหวัด สำนักงานปลัดกระทรวงมหาดไทย* (รายงานการศึกษาค้นคว้าอิสระ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยสุโขทัยธรรมาธิราช, นนทบุรี.

สุชาติ บัวดำ, สุตาภัทร ทิพย์รังศรี. (2555) *การประเมินการควบคุมภายในตามแนว COSO กระบวนการปฏิบัติงานสินไหมทดแทน วัชระประกันภัย.* มหาวิทยาลัยหอการค้าไทย : กรุงเทพมหานคร.

นางสาวสุวินชา การพัดชี, รศ.อภิรดา สุทธิสานนท์ (2555) *ทำการศึกษาการวิเคราะห์ประสิทธิภาพระบบการควบคุมภายในของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร.* มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี, ปทุมธานี.

ปิญะธิดา อมรภิญโญ (2560) การใช้การควบคุมภายในเพื่อความสำเร็จอย่างยั่งยืนของวิสาหกิจการผลิตขนาดย่อมในภาคตะวันออกเฉียงเหนือตอนบนประเทศไทย (ตีพิมพ์เอกสารวิชาการ มหาวิทยาลัยฟาร์อีสเทอร์น ,11(1),186-204. มกราคม 2560 - มีนาคม 2560) มหาวิทยาลัยราชภัฏอุดรธานี, อุดรธานี

นางสาวปิยพร บรรดาศักดิ์, ผศ.อรพิน เหล่าประเสริฐ (2555) *ระบบการควบคุมภายในตามแนว COSO ด้านรายรับ - รายจ่าย กรณีศึกษากองทุนสุขภาพ.* มหาวิทยาลัยหอการค้าไทย, กรุงเทพมหานคร

กิตติพงศ์ โภชนะสมบัติ, ดร.กิจฐเชต ไกรวาส (2557) *การประเมินผลระบบควบคุมภายในตามแนวคิด COSO กรณีศึกษาหน่วยงานในสังกัดสำนักงานปลัดกระทรวงศึกษาธิการ.* มหาวิทยาลัยบูรพา, ชลบุรี

ลีลาศ คุณฟอง, ดร.พัทธนันท์ เพชรเชิดชู (2557) *กระบวนการบริหารความเสี่ยงตามกรอบแนวคิดการบริหารความเสี่ยงทั่วทั้งองค์กร COSO-ERM กรณีศึกษา: บริษัท เด สเต โค (เอเชีย) จำกัด.* มหาวิทยาลัยธุรกิจบัณฑิต, กรุงเทพมหานคร

ธิติโชค พันศิริพัฒน์, ดร.ศิริเดช คำสุพรหม. (2559). *การศึกษาองค์ประกอบที่มีผลต่อการนำระบบการควบคุมภายในมาใช้ในองค์กร : กรณีศึกษา สำนักงานป้องกันควบคุมโรคที่ 5 จังหวัดราชบุรี.* มหาวิทยาลัยธุรกิจบัณฑิต, กรุงเทพมหานคร.

Guidance on Internal Control— Integrated Framework (2013) สืบค้นเมื่อ 13 มกราคม 2561 จาก https://www.coso.org/Pages/ic.aspx

The 2013 COSO Framework & SOX Compliance: One Approach to an Effective Transition สืบค้นเมื่อ 13 มกราคม 2561 จาก https://www.coso.org/documents/COSO McNallyTransition Article-Final COSO Version Proof_5-31-13.pdf

COSO INTERNAL CONTROL-INTEGRATED FRAMEWORK. An Implementation Guide for the Healthcare Provider Industry by Crowe สืบค้นเมื่อ 13 มกราคม 2561 จาก https://www.coso.org/Documents/COSO-CROWE-COSO-Internal-Control-Integrated-Framework.pdf

นวัตกรรมการควบคุมภายใน (2560). หลักการและแนวคิดเกี่ยวกับ COSO สืบค้นเมื่อ 5 มกราคม 2561 จากhttps://sites.google.com/site/innovationinternalcontrol1/1-2-hlak-kar-laea-naewkhid

Bundesamt für Sicherheit in der Informationstechnik. (2554). Supplement to BSI-Standard 100-3, Version 2.5Application of the Elementary Threats from the IT-Grundschutz Catalogues forPerforming Risk Analyses. สืบค้นเมื่อ 5 มกราคม 2561 จาก https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/supplement_to_100-3.pdf?__blob=publicationFile&v=1

Protiviti Inc. (2019) สืบค้นเมื่อ มกราคม 2562 จาก https://www.protiviti.com/CA-en/insights/bulletinv5-i3

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2559). *แผนบริหารความเสี่ยง สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. 2559.* สืบค้นเมื่อ 21 พฤษภาคม 2561 จากhttp://www.mdes.go.th/assets/portals/1/files/590816_%E0%B9%81%E0%B8%9C%E0%B8%99%E0%B8%9A%E0%B8%A3%E0%B8%B4%E0%B8%AB%E0%B8%B2%E0%B8%A3%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B9%80%E0%B8%AA%E0%B8%B5%E0%B9%88%E0%B8%A2%E0%B8%87.pdf

สำนักงานปลัดกระทรวงมหาดไทย. (2551). *นโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย* สืบค้นเมื่อ มิถุนายน 2561 จาก http://ictsgp.moi.go.th/ictsgp/ICTsecurity.php

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. (2556). *แผนปฏิบัติการดิจิทัลศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย พ.ศ.2557 – 2561* สืบค้นเมื่อ มิถุนายน 2561 จาก http://www.ict.moi.go.th/PDF/plant_ict_moi.pdf

ภาคผนวก

ภาคผนวก ก

รายการภัยคุกคาม 25 รายการ

ตารางนี้เป็นภาพรวมของภัยคุกคามเบื้องต้น จำนวน 25 รายการ สำหรับใช้ในการศึกษาครั้งนี้

อ้างอิงจาก : Supplement to BSI Standard 100-3,Version 2.5

ลำดับ	ภัยคุกคาม	C	I	A
1	เพลิงไหม้	N	Y	Y
2	ความเสียหายจากน้ำ	N	Y	Y
3	ฝุ่น สนิม มลพิษ	N	Y	Y
4	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง	N	Y	N
5	การปฏิเสธความรับผิดชอบ	Y	Y	N
6	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	N	Y	Y
7	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y
8	การล้วงความลับหรือข้อมูลจากระบบ	Y	N	N
9	ความลับถูกเปิดเผย	Y	N	N
10	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	Y	N	Y
11	หยุดทำงานเนื่องจากบริการพื้นฐาน (Mains supply)	N	N	Y
12	การเข้าสู่สถานที่หรือบริเวณต้องห้าม	Y	Y	Y
13	ไม่มีการวางแผนและการปรับปรุงแผนงาน	Y	Y	Y
14	ข้อมูลขาดความน่าเชื่อถือ	Y	Y	Y
15	การจัดการฮาร์ดแวร์และซอฟท์แวร์	Y	Y	Y
16	การจัดการข้อมูล	N	Y	N
17	การเข้าสู่ระบบโดยไม่ได้รับอนุญาต	Y	Y	N
18	ความผิดปกติ/ความล้มเหลวของอุปกรณ์หรือระบบ	N	N	Y
19	ขาดแคลนทรัพยากร	N	N	Y
20	ช่องโหว่ของซอฟท์แวร์	Y	Y	Y
21	การละเมิดกฎหมาย หรือข้อบังคับ	Y	Y	Y
22	การจัดการอุปกรณ์หรือระบบโดยไม่ได้รับอนุญาต	Y	Y	Y
23	การจัดการดูแลอุปกรณ์หรือระบบโดยไม่ถูกต้อง	Y	Y	Y
24	ขาดแคลนบุคลากร	N	N	Y
25	การถูกโจมตี	Y	Y	Y

ภาคผนวก ข

ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศรายจังหวัด

ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศสำนักงานจังหวัดสุราษฎร์ธานี

ลำดับ	ภัยคุกคาม	ประเภท	ประเมินโอกาสที่จะเกิด (จากภัยคุกคาม/จุดอ่อน)										ความเสี่ยง				
			โอกาสที่จะเกิด (L)					ผลกระทบ (I)					ระดับความเสี่ยง (R)				ผู้ประเมิน
			1	2	3	4	5	1	2	3	4	5	L	M	H	HV	
1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง	ข้อมูล (Information)		2						3				6			ประภาศิริ
2	การล้วงความลับหรือข้อมูลจากระบบ	ข้อมูล (Information)	1							3			3				ประภาศิริ
3	ความลับถูกเปิดเผย	ข้อมูล (Information)	1							3			3				ประภาศิริ
4	ข้อมูลขาดความน่าเชื่อถือ	ข้อมูล (Information)	1									5		5			ประภาศิริ
5	การจัดการข้อมูลไม่ดี	ข้อมูล (Information)	1									5		5			ประภาศิริ
6	การปฏิเสธความรับผิดชอบ	ขั้นตอนการปฏิบัติงาน (Processes)	1							3			3				ประภาศิริ
7	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	ขั้นตอนการปฏิบัติงาน (Processes)	1							3			3				ประภาศิริ
8	ไม่มีการวางแผนและการปรับปรุงแผนงาน	ขั้นตอนการปฏิบัติงาน (Processes)			3					3					9		ประภาศิริ
9	การละเมิดกฎหมาย หรือข้อบังคับ	ขั้นตอนการปฏิบัติงาน (Processes)	1							3			3				ประภาศิริ
10	ช่องโหว่ของซอฟต์แวร์	ซอฟต์แวร์ (Software)	1									5		5			ประภาศิริ
11	การถูกโจมตี	ซอฟต์แวร์ (Software)	1									5		5			ประภาศิริ
12	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	บุคลากร (People)	1									5		5			ประภาศิริ
13	การเข้าถึงสถานที่หรือบริเวณต้องห้าม	บุคลากร (People)		2								5			10		ประภาศิริ
14	การเข้าถึงระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			ประภาศิริ
15	การจัดการอุปกรณ์หรือระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			ประภาศิริ
16	การจัดการดูแลอุปกรณ์หรือระบบโดยไม่ถูกต้อง	บุคลากร (People)	1									5		5			ประภาศิริ
17	ขาดแคลนบุคลากร	บุคลากร (People)				4						5				20	ประภาศิริ
18	เพลิงไหม้	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศิริ
19	ความเสียหายจากน้ำ	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศิริ
20	ฝุ่น สกปรก บดทึบ	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศิริ
21	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	ฮาร์ดแวร์ (Hardware)		2						3				6			ประภาศิริ
22	หยุดทำงานเนื่องจากบริการพื้นฐาน (Mains supply)	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศิริ
23	การจัดการฮาร์ดแวร์และซอฟต์แวร์ไม่ดี	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศิริ
24	ความผิดปกติ/ความล้มเหลวของอุปกรณ์หรือระบบ	ฮาร์ดแวร์ (Hardware)	1									5		5			ประภาศิริ
25	ขาดแคลนทรัพยากร	ฮาร์ดแวร์ (Hardware)			3					3					9		ประภาศิริ

ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศสำนักงานจังหวัดนครศรีธรรมราช

ลำดับ	ภัยคุกคาม	ประเภท	ประเมินโอกาสที่จะเกิด (จากภัยคุกคาม/จุดอ่อน)										ความเสี่ยง				
			โอกาสที่จะเกิด (L)					ผลกระทบ (I)					ระดับความเสี่ยง (R)				ผู้ประเมิน
			1	2	3	4	5	1	2	3	4	5	L	M	H	HV	
1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง	ข้อมูล (Information)			3					3					9		นวก.คอมพิวเตอร์
2	การล้วงความลับหรือข้อมูลจากระบบ	ข้อมูล (Information)		2							4				8		นวก.คอมพิวเตอร์
3	ความลับถูกเปิดเผย	ข้อมูล (Information)			3							5				15	นวก.คอมพิวเตอร์
4	ข้อมูลขาดความน่าเชื่อถือ	ข้อมูล (Information)			3							5				15	นวก.คอมพิวเตอร์
5	การจัดการข้อมูลไม่ดี	ข้อมูล (Information)	1									5		5			นวก.คอมพิวเตอร์
6	การปฏิเสธความรับผิดชอบ	ขั้นตอนการปฏิบัติงาน (Processes)			3							5				15	นวก.คอมพิวเตอร์
7	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	ขั้นตอนการปฏิบัติงาน (Processes)	1									5		5			นวก.คอมพิวเตอร์
8	ไม่มีการวางแผนและการปรับปรุงแผนงาน	ขั้นตอนการปฏิบัติงาน (Processes)	1									5		5			นวก.คอมพิวเตอร์
9	การละเมิดกฎหมาย หรือข้อบังคับ	ขั้นตอนการปฏิบัติงาน (Processes)			3						4				12		นวก.คอมพิวเตอร์
10	ช่องโหว่ของซอฟต์แวร์	ซอฟต์แวร์ (Software)			3							5				15	นวก.คอมพิวเตอร์
11	การถูกโจมตี	ซอฟต์แวร์ (Software)			3							5				15	นวก.คอมพิวเตอร์
12	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
13	การเข้าถึงสถานที่หรือบริเวณต้องห้าม	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
14	การเข้าถึงระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
15	การจัดการอุปกรณ์หรือระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
16	การจัดการดูแลอุปกรณ์หรือระบบโดยไม่ถูกต้อง	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
17	ขาดแคลนบุคลากร	บุคลากร (People)					5					5				25	นวก.คอมพิวเตอร์
18	เพลิงไหม้	ฮาร์ดแวร์ (Hardware)			3							5				15	นวก.คอมพิวเตอร์
19	ความเสียหายจากน้ำ	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
20	ฝุ่น สกปรก มลพิษ	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
21	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
22	หยุดทำงานเนื่องจากบริการพื้นฐาน (Mains supply)	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
23	การจัดการฮาร์ดแวร์และซอฟท์แวร์ไม่ดี	ฮาร์ดแวร์ (Hardware)			3							5				15	นวก.คอมพิวเตอร์
24	ความผิดปกติ/ความลับเหลวของอุปกรณ์หรือระบบ	ฮาร์ดแวร์ (Hardware)			3							5				15	นวก.คอมพิวเตอร์
25	ขาดแคลนทรัพยากร	ฮาร์ดแวร์ (Hardware)			3					3					9		นวก.คอมพิวเตอร์

ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุง

ลำดับ	ภัยคุกคาม	ประเภท	ประเมินโอกาสที่จะเกิด (จากภัยคุกคาม/จุดอ่อน)										ความเสี่ยง				
			โอกาสที่จะเกิด (L)					ผลกระทบ (I)					ระดับความเสี่ยง (R)				ผู้ประเมิน
			1	2	3	4	5	1	2	3	4	5	L	M	H	HV	
1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง	ข้อมูล (Information)			3					3					9		นวก.คอมพิวเตอร์
2	การล้วงความลับหรือข้อมูลจากระบบ	ข้อมูล (Information)		2							4				8		นวก.คอมพิวเตอร์
3	ความลับถูกเปิดเผย	ข้อมูล (Information)			3							5				15	นวก.คอมพิวเตอร์
4	ข้อมูลขาดความน่าเชื่อถือ	ข้อมูล (Information)			3							5				15	นวก.คอมพิวเตอร์
5	การจัดการข้อมูลไม่ดี	ข้อมูล (Information)	1									5		5			นวก.คอมพิวเตอร์
6	การปฏิเสธความรับผิดชอบ	ขั้นตอนการปฏิบัติงาน (Processes)			3							5				15	นวก.คอมพิวเตอร์
7	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	ขั้นตอนการปฏิบัติงาน (Processes)	1									5		5			นวก.คอมพิวเตอร์
8	ไม่มีการวางแผนและการปรับปรุงแผนงาน	ขั้นตอนการปฏิบัติงาน (Processes)	1									5		5			นวก.คอมพิวเตอร์
9	การละเมิดกฎหมาย หรือข้อบังคับ	ขั้นตอนการปฏิบัติงาน (Processes)			3						4				12		นวก.คอมพิวเตอร์
10	ช่องโหว่ของซอฟต์แวร์	ซอฟต์แวร์ (Software)			3							5				15	นวก.คอมพิวเตอร์
11	การถูกโจมตี	ซอฟต์แวร์ (Software)			3							5				15	นวก.คอมพิวเตอร์
12	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
13	การเข้าถึงสถานที่หรือบริเวณต้องห้าม	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
14	การเข้าถึงระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
15	การจัดการอุปกรณ์หรือระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
16	การจัดการดูแลอุปกรณ์หรือระบบโดยไม่ถูกต้อง	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
17	ขาดแคลนบุคลากร	บุคลากร (People)					5					5				25	นวก.คอมพิวเตอร์
18	เพลิงไหม้	ฮาร์ดแวร์ (Hardware)			3							5				15	นวก.คอมพิวเตอร์
19	ความเสียหายจากน้ำ	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
20	ฝุ่น สิ่งปนเปื้อน	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
21	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
22	หยุดทำงานเนื่องจากบริการพื้นฐาน (Mains supply)	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
23	การจัดการฮาร์ดแวร์และซอฟต์แวร์ไม่ดี	ฮาร์ดแวร์ (Hardware)			3							5				15	นวก.คอมพิวเตอร์
24	ความผิดปกติ/ความล้มเหลวของอุปกรณ์หรือระบบ	ฮาร์ดแวร์ (Hardware)			3							5				15	นวก.คอมพิวเตอร์
25	ขาดแคลนทรัพยากร	ฮาร์ดแวร์ (Hardware)			3					3					9		นวก.คอมพิวเตอร์

ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศสำนักงานจังหวัดสงขลา

ลำดับ	ภัยคุกคาม	ประเภท	ประเมินโอกาสที่จะเกิด (จากภัยคุกคาม/จุดอ่อน)										ความเสี่ยง				
			โอกาสที่จะเกิด (L)					ผลกระทบ (I)					ระดับความเสี่ยง (R)				ผู้ประเมิน
			1	2	3	4	5	1	2	3	4	5	L	M	H	HV	
1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง	ข้อมูล (information)	1									5		5			นวก.คอมพิวเตอร์
2	การล้วงความลับหรือข้อมูลจากระบบ	ข้อมูล (information)		2								5			10		นวก.คอมพิวเตอร์
3	ความลับถูกเปิดเผย	ข้อมูล (information)	1									5		5			นวก.คอมพิวเตอร์
4	ข้อมูลจากความน่าเชื่อถือ	ข้อมูล (information)	1								4			4			นวก.คอมพิวเตอร์
5	การจัดการข้อมูลไม่ดี	ข้อมูล (information)	1							3			3				นวก.คอมพิวเตอร์
6	การปฏิเสธความรับผิดชอบ	ขั้นตอนการปฏิบัติงาน (Processes)	1									5		5			นวก.คอมพิวเตอร์
7	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	ขั้นตอนการปฏิบัติงาน (Processes)	1									5		5			นวก.คอมพิวเตอร์
8	ไม่มีการวางแผนและการปรับปรุงแผนงาน	ขั้นตอนการปฏิบัติงาน (Processes)		2								5			10		นวก.คอมพิวเตอร์
9	การละเมิดกฎหมาย หรือข้อบังคับ	ขั้นตอนการปฏิบัติงาน (Processes)			3						4				12		นวก.คอมพิวเตอร์
10	ช่องโหว่ของซอฟต์แวร์	ซอฟต์แวร์ (Software)			3							5				15	นวก.คอมพิวเตอร์
11	การถูกโจมตี	ซอฟต์แวร์ (Software)			3							5				15	นวก.คอมพิวเตอร์
12	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	บุคลากร (People)			3							5				15	นวก.คอมพิวเตอร์
13	การเข้าถึงสถานที่หรือบริเวณต้องห้าม	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
14	การเข้าถึงระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
15	การจัดการอุปกรณ์หรือระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1								4			4			นวก.คอมพิวเตอร์
16	การจัดการดูแลอุปกรณ์หรือระบบโดยไม่ถูกต้อง	บุคลากร (People)	1								4			4			นวก.คอมพิวเตอร์
17	ขาดแคลนบุคลากร	บุคลากร (People)	1								4			4			นวก.คอมพิวเตอร์
18	เพลิงไหม้	ฮาร์ดแวร์ (Hardware)	1								4			4			นวก.คอมพิวเตอร์
19	ความเสียหายจากน้ำ	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
20	ฝุ่น สิ่งปนเปื้อน	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
21	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
22	หยุดทำงานเนื่องจากบริการพื้นฐาน (Mains supply)	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
23	การจัดการฮาร์ดแวร์และซอฟท์แวร์ไม่ดี	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
24	ความผิดปกติ/ความสับเหลวของอุปกรณ์หรือระบบ	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
25	ขาดแคลนทรัพยากร	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์

ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศสำนักงานจังหวัดชุมพร

ลำดับ	ภัยคุกคาม	ประเภท	ประเมินโอกาสที่จะเกิด (จากภัยคุกคาม/จุดอ่อน)										ความเสี่ยง				
			โอกาสที่จะเกิด (L)					ผลกระทบ (I)					ระดับความเสี่ยง (R)				ผู้ประเมิน
			1	2	3	4	5	1	2	3	4	5	L	M	H	HV	
1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง	ข้อมูล (Information)	1									5		5			นวก.คอมพิวเตอร์
2	การล้วงความลับหรือข้อมูลจากระบบ	ข้อมูล (Information)	1									5		5			นวก.คอมพิวเตอร์
3	ความลับถูกเปิดเผย	ข้อมูล (Information)		2							4				8		นวก.คอมพิวเตอร์
4	ข้อมูลขาดความน่าเชื่อถือ	ข้อมูล (Information)		2							4				8		นวก.คอมพิวเตอร์
5	การจัดการข้อมูลไม่ดี	ข้อมูล (Information)		2							4				8		นวก.คอมพิวเตอร์
6	การปฏิเสธความรับผิดชอบ	ขั้นตอนการปฏิบัติงาน (Processes)		2							4				8		นวก.คอมพิวเตอร์
7	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	ขั้นตอนการปฏิบัติงาน (Processes)		2								5			10		นวก.คอมพิวเตอร์
8	ไม่มีการวางแผนและการปรับปรุงแผนงาน	ขั้นตอนการปฏิบัติงาน (Processes)	1							3			3				นวก.คอมพิวเตอร์
9	การละเมิดกฎหมาย หรือข้อบังคับ	ขั้นตอนการปฏิบัติงาน (Processes)	1							3			3				นวก.คอมพิวเตอร์
10	ช่องโหว่ของซอฟต์แวร์	ซอฟต์แวร์ (Software)		2							4				8		นวก.คอมพิวเตอร์
11	การถูกโจมตี	ซอฟต์แวร์ (Software)	1								4			4			นวก.คอมพิวเตอร์
12	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	บุคลากร (People)	1								4			4			นวก.คอมพิวเตอร์
13	การเข้าถึงสถานที่หรือบริเวณต้องห้าม	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
14	การเข้าถึงระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
15	การจัดการอุปกรณ์หรือระบบโดยไม่ได้รับอนุญาต	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
16	การจัดการดูแลอุปกรณ์หรือระบบโดยไม่ถูกต้อง	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
17	ขาดแคลนบุคลากร	บุคลากร (People)	1									5		5			นวก.คอมพิวเตอร์
18	เพลิงไหม้	ฮาร์ดแวร์ (Hardware)	1									5		5			นวก.คอมพิวเตอร์
19	ความเสียหายจากน้ำ	ฮาร์ดแวร์ (Hardware)		2								5		10			นวก.คอมพิวเตอร์
20	ฝุ่น สนิม บลทิษ	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
21	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
22	หยุดทำงานเนื่องจากบริการพื้นฐาน (Mains supply)	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
23	การจัดการฮาร์ดแวร์และซอฟท์แวร์ไม่ดี	ฮาร์ดแวร์ (Hardware)		2								5			10		นวก.คอมพิวเตอร์
24	ความผิดปกติ/ความล้มเหลวของอุปกรณ์หรือระบบ	ฮาร์ดแวร์ (Hardware)			3							5				15	นวก.คอมพิวเตอร์
25	ขาดแคลนทรัพยากร	ฮาร์ดแวร์ (Hardware)			3							5				15	นวก.คอมพิวเตอร์

ประวัติผู้ศึกษา

ชื่อ	นางสาวประภาศรี รักษ์บางแหลม
วัน เดือน ปีเกิด	12 ตุลาคม 2519
สถานที่เกิด	อำเภอเมือง จังหวัดสุราษฎร์ธานี
ประวัติการศึกษา	บริหารธุรกิจบัณฑิต มหาวิทยาลัยศรีปทุม พ.ศ.2541
สถานที่ทำงาน	สำนักงานจังหวัดสุราษฎร์ธานี สำนักงานปลัดกระทรวงมหาดไทย
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ชำนาญการ