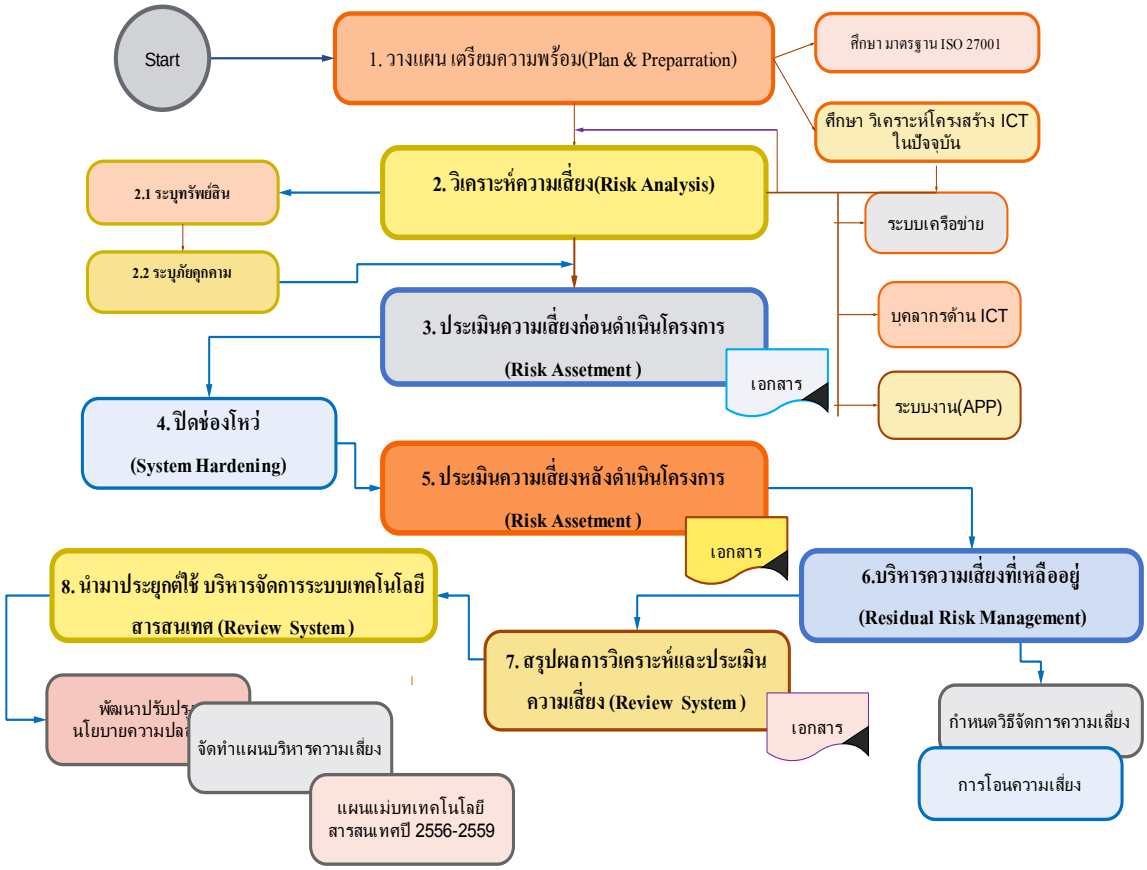
บทที่ 4
การวิเคราะห์และประเมินความเสี่ยง

จากการวิเคราะห์ปัญหา และออกแบบขั้นตอนและวิธีการดำเนินงาน ในบทนี้จะกล่าวถึง การวิเคราะห์และประเมินความเสี่ยง โดยการนำมาตรฐานสากล ISO/IEC 27001 มาใช้เป็นกรอบในการกำหนดขอบเขต การวิเคราะห์และประเมินความเสี่ยงให้ตรงตามวัตถุประสงค์ของการดำเนินงานโครงการและนำผลการวิเคราะห์และประเมินความเสี่ยง ไปใช้บริหารจัดการระบบเทคโนโลยีสารสนเทศภายในองค์กรประกอบด้วยขั้นตอนต่างๆ ของกระบวนการวิเคราะห์และประเมินความเสี่ยง ดังภาพที่ 4.1



ภาพที่ 4.1 กระบวนการวิเคราะห์และประเมินความเสี่ยง

การวิเคราะห์และประเมินความเสี่ยงตามที่ได้มีการวิเคราะห์ออกแบบไว้ในบทที่ 3 มีรายละเอียดต่างๆ ดังนี้ การศึกษา วิเคราะห์ การบริหารจัดการความเสี่ยงภายใต้มาตรฐาน ISO/IEC 270001 เป็นขั้นตอนศึกษาวิเคราะห์ความเสี่ยงของทรัพย์สินสารสนเทศ ในแง่ของโอกาสที่จะเกิดหรือเหตุการณ์ (Event) ว่ามีโอกาสที่จะเกิดมากน้อยแค่ไหนและเมื่อเกิดขึ้นแล้วมีผลกระทบ (Impact) ความรุนแรงเสียหายอย่างไรบ้างมีขั้นตอนและรายละเอียด ตามข้อ 4.1-4.6 อธิบายรายละเอียดดังนี้

4.1 การวางแผนเตรียมความพร้อม

4.2 การวิเคราะห์ความเสี่ยงโดยการนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้

4.3 การประเมินความเสี่ยงก่อนดำเนินโครงการ

4.4 วิเคราะห์ ตามตารางประเมินความเสี่ยงที่ได้ตรวจสอบปิดช่องโหว่ของระบบ

4.5 วิเคราะห์และประเมินความเสี่ยงหลังดำเนินโครงการ

4.6 การจัดการความเสี่ยง (Risk Management) มีวิธีจัดการความเสี่ยงได้หลายวิธี ได้แก่ การลดความเสี่ยง การหลีกเลี่ยงความเสี่ยง การถ่ายโอนความเสี่ยง การยอมรับความเสี่ยงที่มีอยู่ (Accept Risk)

4.7 สรุปผลการวิเคราะห์และประเมินความเสี่ยง วิเคราะห์เปรียบเทียบตารางความเสี่ยงก่อนดำเนินโครงการและหลังดำเนินโครงการ นำผลการวิเคราะห์และประเมินความเสี่ยงไปใช้วางแผน เพื่อดำเนินงานต่างๆ ด้านเทคโนโลยีและการสื่อสาร(ICT) ขององค์กร

4.8 นำมาประยุกต์ใช้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศ เช่น จัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับที่ 2 ปี 2556-2559 การพัฒนาปรับปรุงนโยบายความปลอดภัยของหน่วยงานและการจัดทำแผนบริหารความเสี่ยง

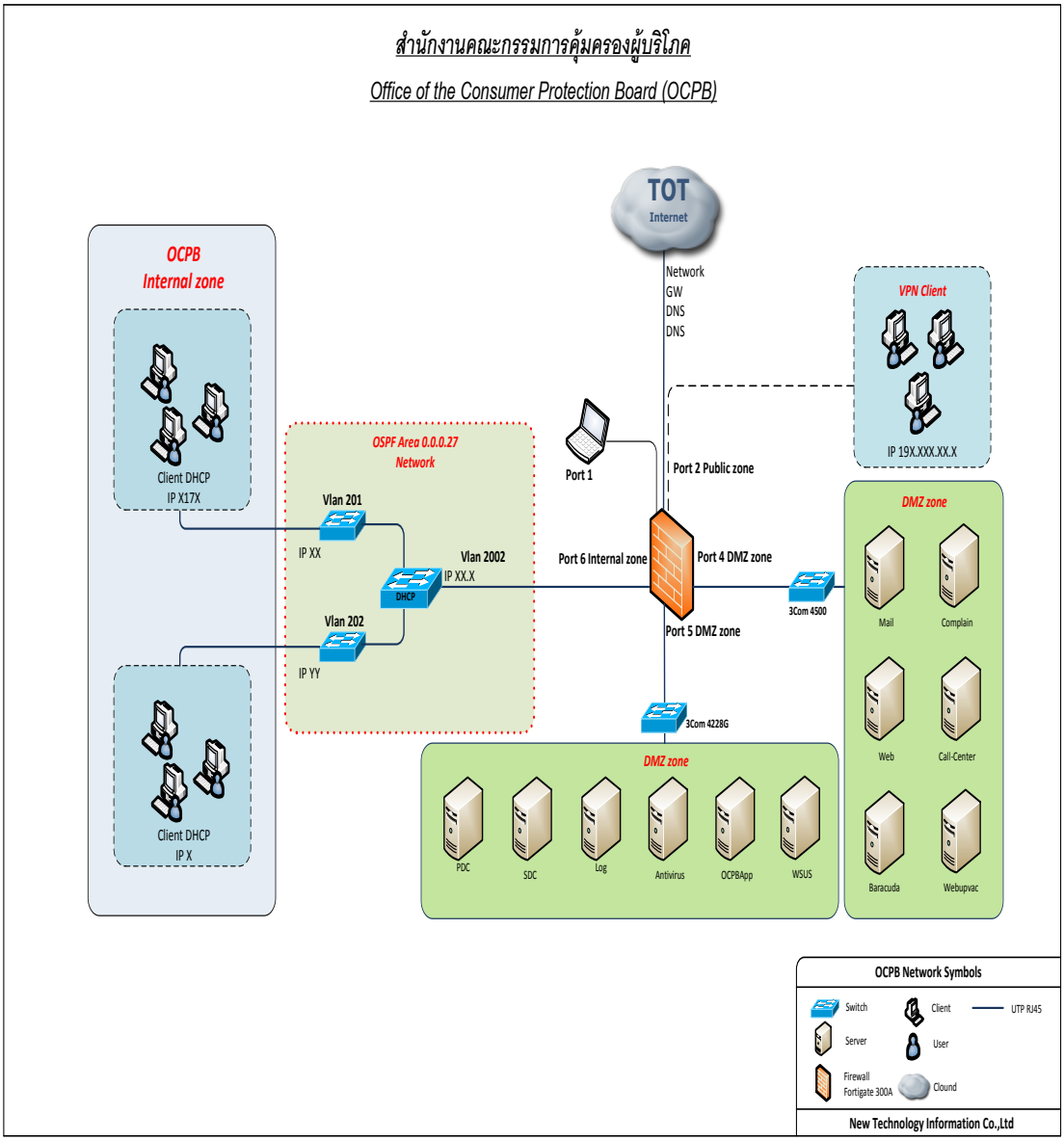
4.1 การวางแผนเตรียมความพร้อม ต้องมีการวางแผนเตรียมความพร้อมใน การศึกษา วิเคราะห์ข้อมูลด้านความปลอดภัยของระบบสารสนเทศ เพื่อมีการเตรียมพร้อมในการวิเคราะห์และประเมินความเสี่ยง

4.1.1 ศึกษาข้อมูลด้านความปลอดภัยตามมาตรฐาน ISO/IEC 27001 เพื่อเป็นแนวทางในการวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศ และกำหนดขอบเขต ระบุภัยคุกคาม/ความเสี่ยงที่อาจเกิดขึ้น ทำความเข้าใจขั้นตอนการวิเคราะห์ความเสี่ยง ศึกษาผลกระทบ เป็นต้น

4.1.2 ศึกษา การบริหารความเสี่ยง ภัยคุกคาม/ช่องโหว่ การศึกษาวิเคราะห์ด้านการจัดการความเสี่ยงการใช้งานระบบสารสนเทศและอุปกรณ์ในปัจจุบัน การวิเคราะห์และประเมินความเสี่ยงต้องมีการระบุปัจจัยเสี่ยงอะไรบ้าง ศึกษาการบริหารความเสี่ยง เพื่อบริหารจัดการด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นต้น

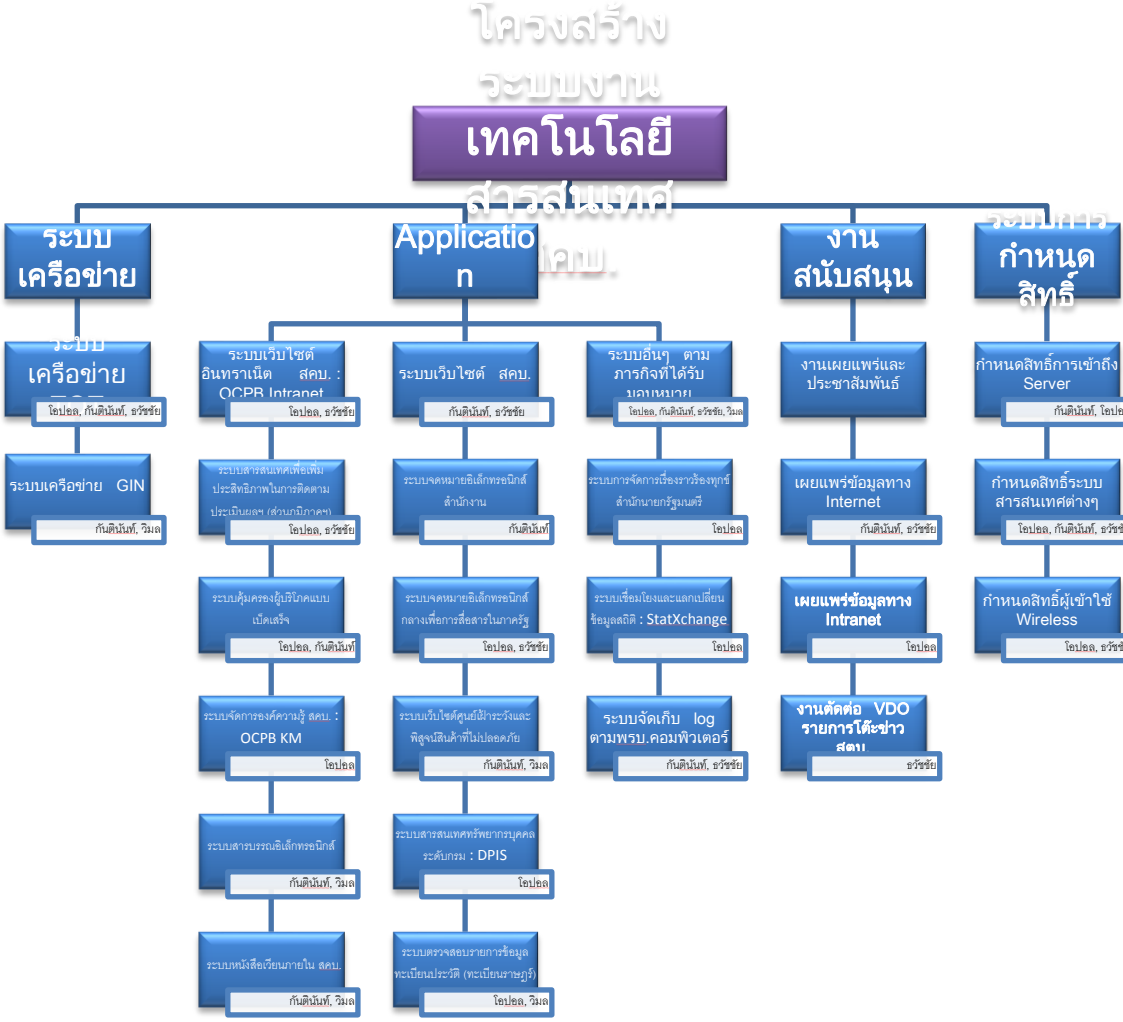
4.1.3 ศึกษาโครงสร้างขององค์กร ในการศึกษาโครงสร้างขององค์กรในด้านต่างๆ ทำให้ทราบขั้นตอนการทำงานและ กระบวนงานหลัก กระบวนงานสนับสนุน เพื่อข้อมูลนำมาวิเคราะห์และประเมินความเสี่ยงให้กับระบบ เช่น ระบุขอบเขตดำเนินงาน ระบุทรัพย์สิน มีการศึกษาระบบเครือข่าย กระบวนการ และโครงสร้างของระบบงานต่างๆ ได้แก่

4.1.3.1 ศึกษาโครงสร้างระบบเครือข่ายและอุปกรณ์ต่อพ่วง เพื่อนำมาวิเคราะห์ความปลอดภัยและการควบคุมการเข้าถึงข้อมูล รายละเอียดตามภาพที่ 4.2



ภาพที่ 4.2 ระบบเครือข่าย (Network System)

4.1.3.2 ศึกษาโครงสร้างระบบงานเทคโนโลยีสารสนเทศ



ภาพที่ 4.3 โครงสร้างระบบงานสารสนเทศ

4.1.3.2 ศึกษากระบวนการ (Process) ศึกษาถึงกระบวนการต่างๆ เช่น กระบวนการและขั้นตอนในการติดตั้ง เครื่องแม่ข่ายใหม่เพิ่มเติม วิเคราะห์โครงสร้างระบบเครือข่ายและอุปกรณ์ต่อพ่วงของระบบเทคโนโลยีสารสนเทศตามความเป็นจริง เพื่อนำไปใช้ในการวิเคราะห์และประเมินความเสี่ยง เช่น การจัดการความเสี่ยงการใช้งานระบบสารสนเทศและอุปกรณ์ กรณีห้องเซิร์ฟเวอร์ เน้นหัวข้อสร้างความมั่นคงปลอดภัยทางกายภาพและควบคุมการเข้าถึง การระบุขอบเขตดำเนินงาน ระบุถึงทรัพย์สินความไม่มั่นคงของระบบและภัยคุกคามต่างๆ เป็นการรวบรวมข้อมูลหรือ สัมภาษณ์บุคคลที่เกี่ยวข้องและดูจากสถานที่จริง โดยผู้จัดทำได้แบ่งชนิดระบบสารสนเทศเฉพาะที่เกี่ยวข้องกับการดำเนินโครงงาน สามารถแบ่งได้หลายประเภท ได้แก่ กลุ่มเครื่องเซิร์ฟเวอร์

ที่ติดตั้งภายในห้องเซิร์ฟเวอร์ของหน่วยงานประกอบไปด้วย รายละเอียดและประเภทของเซิร์ฟเวอร์ตามลักษณะการใช้งานต่างๆ

4.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)

จากการศึกษา รวบรวมข้อมูล ด้วยวิธีการต่างๆ นำมาวิเคราะห์และประเมินความเสี่ยง โดยมีการระบุขอบเขตการดำเนินงาน ระบุถึงทรัพย์สินความไม่มั่นคงปลอดภัยของระบบและภัยคุกคามต่างๆ จากการรวบรวมข้อมูล หรือ สัมภาษณ์บุคคลที่เกี่ยวข้อง และ ดูจากสถานที่จริงโดยผู้จัดทำได้แบ่งชนิดระบบสารสนเทศที่เกี่ยวข้องกับการดำเนินโครงงาน เพื่อการวิเคราะห์ให้ใกล้เคียงความเป็นจริงมากที่สุด

การวิเคราะห์ความเสี่ยงในโครงงานนี้ เป็นการวิเคราะห์สถานะภาพของระบบเทคโนโลยีสารสนเทศ และศึกษากระบวนการจัดการความเสี่ยง เพื่อตรวจสอบและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศขององค์กรทำให้ทราบสาเหตุ ปัจจัย และเพื่อวัดผลกระทบของความเสี่ยงที่อาจจะเกิดขึ้นและนำไปใช้สร้างเกณฑ์กำหนดระดับในการประเมินความเสี่ยง (Risk Model) โดยจะต้องกำหนดเกณฑ์การประเมินผลกระทบต่อระดับของความปลอดภัย เกณฑ์การประเมินโอกาสในการเกิดภัยคุกคามความเสี่ยง และเกณฑ์ในการประเมินความเสี่ยง ซึ่งกระบวนวิเคราะห์ความเสี่ยงประกอบด้วย ขั้นตอนต่างๆ ประกอบด้วย การบ่งชี้ความไม่มั่นคงปลอดภัย (Vulnerability Identification) จัดกลุ่มทรัพย์สินกำหนดเกณฑ์ระดับการประเมินความเสี่ยงของระบบสารสนเทศที่จะประเมินความเสี่ยง การกำหนดประเภทภัยคุกคาม ซึ่งมีรายละเอียดดังนี้

4.2.1 การบ่งชี้ความไม่มั่นคงปลอดภัย (Vulnerability Identification) ของระบบสารสนเทศที่จะประเมินความเสี่ยง ซึ่งได้จากการรวบรวมจากการวิเคราะห์ ศึกษา สภาพ ICT ตามความเป็นจริงที่มี เช่น การระบุภัยคุมคาม/ช่องโหว่ระบบ ได้จาก

4.2.1.1 การสัมภาษณ์การใช้งานจาก ผู้ดูแลระบบ ผู้ใช้งานระบบ ผู้บริหาร

4.2.1.2 ติดตั้ง Software เพื่อตรวจสอบพฤติกรรมของผู้ใช้งานระบบ Internet Scanner เพื่อค้นหาช่องโหว่ ได้แก่ Nessus เพื่อค้นหาช่องโหว่ของระบบ Lancope เพื่อตรวจจับตรวจสอบช่องโหว่ของ Server ระบบงาน

4.2.1.3 ระบบเครือข่าย

4.2.14 ภัยคุกคามจากธรรมชาติ เช่น น้ำท่วม ไฟไหม้ ไฟฟ้าดับ

การศึกษา วิเคราะห์ จากแหล่งข้อมูลต่างๆ ของสถานะภาพด้าน ICT ที่อาจบ่งชี้ถึงความไม่มั่นคงปลอดภัยของระบบสารสนเทศ สรุปรายละเอียดตามตารางที่ 4.1

ตารางที่ 4.1 ตารางบ่งชี้ความไม่มั่นคงปลอดภัยของระบบสารสนเทศ

ลำดับ	ความเสี่ยงไม่มั่นคงปลอดภัยของระบบสาสนเทศ
1.	ขาดการป้องกันทางกายภาพของประตูเข้า- ออก
2.	มีความรู้เกี่ยวกับความปลอดภัยระบบสารสนเทศไม่เพียงพอ
3.	ไม่มีนโยบายการใช้งานเครือข่ายบริการที่ชัดเจน
4.	ไม่มีการทบทวนสิทธิของผู้ใช้งานการเข้าถึงของผู้ใช้ระบบ
5.	ขาดการตรวจสอบระบบจากหน่วยงานภายนอก
6.	ไม่มีการลงทะเบียน ในการใช้ระบบอินเตอร์เนต ออกสู่ภายนอก
7.	ไม่มีนโยบายความปลอดภัยสารสนเทศที่ชัดเจนสำหรับภายในองค์กร
8.	ขาดบุคลากรทางด้าน IT
9.	การดูแลระบบงานขาดผู้รับผิดชอบที่ชัดเจน
10.	บุคลากรทางด้าน IT ขาดทักษะและความเชี่ยวชาญในการวิเคราะห์ระบบ
11.	ปริมาณแบนด์วิดที่ไม่เพียงพอ
12.	การโจมตีระบบจากภายในระบบเครือข่าย
13.	ระบบปฏิบัติการเครื่องไคลน์เอนด์ไม่ได้รับการปรับปรุง
14.	ระบบสำรองไฟฟ้าที่ไม่สามารถรองรับทำการเพื่ออุปกรณ์ในอนาคต
15.	การเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต เนื่องจากมีการป้องกันที่ไม่เหมาะสม
16.	การเข้าถึงระบบโดยใช้ User และ Password ของคนก่อน
17.	การปฏิเสธความรับผิดชอบ จากลักษณะงานหรือหน้าที่ความรับผิดชอบไม่ชัดเจน
18.	ไม่มีระบบเครือข่ายสำรองใช้งาน(Backup Line) เมื่อระบบเครือข่ายหลักล่ม
19.	ไม่มีคู่มือแสดงขั้นตอนการปฏิบัติงานของระบบเครือข่าย
20.	อุปกรณ์สำรองข้อมูล มีไม่เพียงพอ เช่น ขนาดความจุของ Hard Disk Storage
21.	เซิร์ฟเวอร์ Active Directory ที่ทำหน้าที่ตรวจสอบบัญชีของผู้ใช้กรุณาเข้าสู่ระบบบางเครื่องไม่ทำการ Join Domain
22.	ผู้ดูแลระบบงานต่างๆยังไม่สามารถทำงาน ในการวิเคราะห์ปัญหาจากการใช้งานระบบได้ ทำให้ขาดความต่อเนื่องในการปฏิบัติงานและไม่สามารถทำงานแทนกันได้อย่างต่อเนื่อง

ตารางที่ 4.1 (ต่อ)

ลำดับ	ความเสี่ยงไม่มั่นคงปลอดภัยของระบบสาสนเทศ
23.	การกำหนด ไฟร์วอลล์ ไม่รัดกุม เป็นแบบอนุญาตทั้งหมด ซึ่งมีความเสี่ยงที่จะทำให้ถูกโจมตีจากภายนอก และทำให้ระบบเซิร์ฟเวอร์ และเน็ตเวิร์กได้รับความเสียหายได้อาจส่งผลให้ระบบข้อมูลที่มีความสำคัญมีความเสียหายได้
24.	ความเสี่ยงเรื่องโครงสร้างระบบเครือข่ายเนื่องจากทางบริษัทไม่มีการแบ่งโซนแยกกันระหว่าง เซิร์ฟเวอร์ และไคลเอ็น
25.	สิทธิ์ในการรีโมทเข้าเครื่อง เซิร์ฟเวอร์ ไม่มีการควบคุม
26.	พบพนักงานสามารถการติดตั้งซอฟต์แวร์เองได้
27.	พบบัญชีรายชื่อ ของพนักงานที่ลาออกไปแล้วยังอยู่ในระบบ
28.	พบบัญชีรายชื่อที่มีการตั้งรหัส แบบไม่มีวันหมดอายุ (Password Never Expire)
29.	ไม่มี่การกำหนดสิทธิ์การเข้าใช้งานระบบอินเตอร์เน็ตแล้วกำหนดสิทธิ์ ช่วงเวลาในการเข้าใช้งานของผู้ใช้
30.	ระบบฐานข้อมูลไม่มีการกำหนดสิทธิ์ในการเข้าใช้งาน
31.	เครื่องแม่ข่าย (Server) มีอายุการใช้งานเกิน 5 ปี

การระบุภัยประเภทภัยคุกคาม จากการวิเคราะห์สถานะด้านระบบเทคโนโลยีสารสนเทศ เช่น น้ำท่วม ไฟไหม้ ไฟฟ้าดับ ภัยคุกคามจากช่องโหว่ของอุปกรณ์ต่างๆ เป็นต้น สรุปได้ตามตารางที่ 4.2 ดังนี้

ตารางที่ 4.2 ตารางบ่งชี้ประเภทภัยคุกคามของระบบสารสนเทศ

ลำดับที่	ประเภทของภัยคุกคาม
1.	ภัยคุกคามที่เกิดจากการละเมิดทรัพย์สินทางปัญญา
2.	ภัยคุกคามจากการบุกรุก การเจาะระบบ
3.	ภัยคุกคามจากไม่มีนโยบายการใช้งานเครือข่ายบริการ
4.	ภัยคุกคามจากไม่มีการทบทวนสิทธิของผู้ใช้งาน การเข้าถึงของผู้ใช้
5.	ภัยคุกคามจากการขาดการตรวจสอบระบบบ่อยๆ
6.	ภัยคุกคามจากไม่มีการลงทะเบียน ในการออกสู่ระบบอินเตอร์เน็ตภายนอก
7.	ภัยคุกคามจากไม่มีนโยบายความปลอดภัยสารสนเทศที่ชัดเจน
8.	ภัยคุกคามจากขาดบุคลากรทางด้าน IT ที่มีประสิทธิภาพ
9.	ภัยคุกคามจากภัยธรรมชาติ
10.	ภัยคุกคามจากคุณภาพการให้บริการ
11.	ภัยคุกคามจากการโจรกรรมข้อมูล
12.	ภัยคุกคามจากการโจมตีซอฟต์แวร์
13.	ภัยคุกคามจากข้อผิดพลาดทางด้านฮาร์ดแวร์
14.	ภัยคุกคามจากการใช้เทคโนโลยีที่ทันสมัย
15.	ภัยคุกคามจากการขาดการกำกับ ดูแลระบบที่ดีในการควบคุมบริษัท Outsource ในการบำรุงรักษาระบบงานต่างๆ
16.	ภัยคุกคามจาก การไม่มีเอกสารในการจัดทำ Process เช่น ข้อกำหนดรายละเอียด เอกสารการออกแบบระบบ

4.2.2 ระบุทรัพย์สินด้าน ICT ที่จะประเมินความเสี่ยง /การกำหนดประเภทรายการทรัพย์สิน

การสำรวจและระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของหน่วยงาน ต้องมีการระบุทรัพย์สินสารสนเทศ เพื่อนำมาวิเคราะห์และประเมินความเสี่ยง ซึ่งมีการแบ่งหมวดหมู่และรายละเอียดของทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Asset Inventory) ที่จำเป็นของทรัพย์สินตลอดจนแนวนโยบายด้านความมั่นคงปลอดภัยคงสารสนเทศขององค์กรที่อาจมีผลต่อองค์กรและระบุภัยคุกคามที่มีต่อแต่ละทรัพย์สิน แบ่งรายการทรัพย์สินต่างๆได้ 5 ประเภท โดยแยกตามองค์ประกอบของระบบงานคอมพิวเตอร์ ได้แก่ ทรัพย์สินประเภทฮาร์ดแวร์และอุปกรณ์ต่อพ่วง (Hardware Assets) ทรัพย์สินประเภทโปรแกรม (Software Assets) ทรัพย์สินประเภทบุคลากร

(People Assets) ทรัพย์สินด้านข้อมูล (Information Assets) และทรัพย์สินประเภทบริการ (Service Assets) มีรายละเอียด ดังนี้

4.2.2.1 ทรัพย์สินกลุ่มประเภทฮาร์ดแวร์และอุปกรณ์ต่อพ่วงต่างๆ (Hardware Assets) จัดกลุ่มย่อย ๆ ได้แก่ กลุ่มเครื่องแม่ข่าย กลุ่มอุปกรณ์เครือข่าย รายละเอียดตามตารางข้างล่าง

(1) กลุ่มเครื่องแม่ข่าย

ตารางที่ 4.3 รายชื่อทรัพย์สิน กลุ่มเครื่องแม่ข่าย

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
1. Active Directory Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
2. Domain Name Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
3. File Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
4. Mail Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
5.Mail Gateway	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
6.Anti Virus Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
7. Proxy Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
8. Intranet Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
9. Log Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
10.เครื่องคอมพิวเตอร์แม่ข่ายระบบเบ็ดเสร็จ	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
11. เครื่องคอมพิวเตอร์แม่ข่ายระบบเรื่องราวร้องทุกข์ 1166	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
12.เครื่องคอมพิวเตอร์แม่ข่ายระบบงานสารบรรณ	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
13.เครื่องคอมพิวเตอร์ แม่ข่ายระบบรายงานผล ส่วนภูมิภาค	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
14.เครื่องคอมพิวเตอร์ แม่ข่ายระบบเว็บไซต์	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ

(2) กลุ่มอุปกรณ์เครือข่ายประกอบด้วยรายละเอียด ดังนี้

ตารางที่ 4.4 กลุ่มอุปกรณ์เครือข่าย

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
1. ตู้ Rack	กลุ่มอุปกรณ์เครือข่าย	สำนัก/กอง/ฝ่ายงานต่างๆ
2.Firewall	กลุ่มอุปกรณ์เครือข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
3 Core Switch	กลุ่มอุปกรณ์เครือข่าย	บริษัท ทีโอที จำกัดมหาชน
4.Access Switch	กลุ่มอุปกรณ์เครือข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
5. Patch Panel	กลุ่มอุปกรณ์เครือข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
6. Core Switch	กลุ่มอุปกรณ์เครือข่าย	บริษัท ทีโอที จำกัดมหาชน
7. Router ISP	กลุ่มอุปกรณ์เครือข่าย	บริษัท ทีโอที จำกัดมหาชน

(3) กลุ่มอุปกรณ์สื่อสารโทรคมนามและอื่นๆ รายละเอียด ดังนี้

ตารางที่ 4.5 กลุ่มอุปกรณ์สื่อสารโทรคมนาคมและอื่นๆ

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
1. เครื่องคอมพิวเตอร์ (PC) จำนวน 228 เครื่อง	เครื่องลูกข่าย	สำนัก/กอง/ฝ่ายงานต่างๆ
2.เครื่องคอมพิวเตอร์ /Notebook	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
3. KVM Switch	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
4. UPS	อุปกรณ์	ฝ่ายเทคโนโลยีสารสนเทศ
5. ตู้ PBX	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
6. WiFi Access Control	อุปกรณ์สื่อสาร	บริษัท ทีโอที จำกัดมหาชน
7. สาย Fireber Optic E1	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
8. Central Copper wire	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
9. Lease line link	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ

4.2.2.2 ทรัพย์สินประเภทโปรแกรม (Software Assets) จัดแบ่งประเภทของโปรแกรมต่างๆ ที่เป็นทรัพย์สินโดยแยกตามลักษณะความจำเป็นในการใช้งาน ได้แก่ รายละเอียดตามตาราง 4.6 ข้างล่างนี้

ตารางที่ 4.6 รายชื่อทรัพย์สินประเภทโปรแกรม (Software)

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
ระบบงานคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ	โปรแกรมประยุกต์	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบ 1166	โปรแกรมประยุกต์	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบงานติดตามประเมินผลภูมิภาคและท้องถิ่น	โปรแกรมประยุกต์	ฝ่ายเทคโนโลยีสารสนเทศ
Microsoft Office	โปรแกรมพื้นฐานทั่วไป	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบสารบรรณอิเล็กทรอนิกส์	โปรแกรมประยุกต์	ฝ่ายเทคโนโลยีสารสนเทศ
OS Microsoft window XP Profession	ระบบปฏิบัติการ	ฝ่ายเทคโนโลยีสารสนเทศ
OS Microsoft window 2005	ระบบปฏิบัติการ	ฝ่ายเทคโนโลยีสารสนเทศ
OS Microsoft window 2008	ระบบปฏิบัติการ	ฝ่ายเทคโนโลยีสารสนเทศ
Microsorft Exchange 2008	โปรแกรม	ฝ่ายเทคโนโลยีสารสนเทศ
KapeskyAnti Virus	โปรแกรม	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบฐานข้อมูล SQL Server 2008	ระบบฐานข้อมูล SQL	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบฐานข้อมูล SQL Server 2012	ระบบฐานข้อมูล SQL	ฝ่ายเทคโนโลยีสารสนเทศ
โปรแกรมป้องกันไวรัส	โปรแกรม	ฝ่ายเทคโนโลยีสารสนเทศ

4.2.2.3 ทรัพย์สินประเภทบุคลากร (People Assets) จัดแบ่งประเภทโปรแกรมต่างๆ ที่เป็นทรัพย์สินโดยแยกตามลักษณะความจำเป็นในการใช้งาน รายละเอียดตามตารางที่ 4.7 ข้างล่างนี้

ตารางที่ 4.7 รายชื่อทรัพย์สินทางด้านบุคลากร (People Assets)

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
บุคลากร	ผู้บริหารระดับสูง	ฝ่ายการเจ้าหน้าที่
บุคลากร	ผู้บริหารระดับกลาง	ฝ่ายการเจ้าหน้าที่
บุคลากร	อำนวยการระดับสูง	ฝ่ายการเจ้าหน้าที่
บุคลากร	อำนวยการระดับต้น	ฝ่ายการเจ้าหน้าที่
บุคลากร	ชำนาญการพิเศษ	ฝ่ายการเจ้าหน้าที่
บุคลากร	ชำนาญการ	ฝ่ายการเจ้าหน้าที่
บุคลากร	ปฏิบัติการ	ฝ่ายการเจ้าหน้าที่
บุคลากร	พนักงานทั่วไป	ฝ่ายการเจ้าหน้าที่
บุคลากร	พนักงานราชการ	ฝ่ายการเจ้าหน้าที่
บุคลากร	ลูกจ้างโครงการ	กอง/สำนัก

4.2.2.4 ทรัพย์สินข้อมูล (Information Assets) จัดแบ่งประเภทของข้อมูลต่างๆที่เป็นทรัพย์สินโดยแยกตามลักษณะความจำเป็นในการใช้งาน รายละเอียดตามตารางที่ 4.8 ข้างล่างนี้

ตารางที่ 4.8 รายชื่อทรัพย์สินประเภทข้อมูล (Information Assets)

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
ระบบเว็บไซต์	ระบบฐานข้อมูล Access	ศูนย์เทคโน ฯ
ระบบ 1166	ระบบฐานข้อมูล SQL	ศูนย์เทคโน ฯ
ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ	ระบบฐานข้อมูล SQL	ศูนย์เทคโน ฯ
ระบบสารบรรณอิเล็กทรอนิกส์	ระบบฐานข้อมูล Oracle	ศูนย์เทคโน ฯ
ระบบ Dpis (บุคลากร)	ข้อมูลบุคลากร	ศูนย์เทคโน ฯ
ระบบ e-Mail	ข้อมูลภายใน	ศูนย์เทคโน ฯ
ระบบหนังสือเวียน	ข้อมูลภายใน เฉพาะ	ศูนย์เทคโน ฯ

4.2.2.5 ทรัพย์สินประเภทบริการ (Service Assets) สามารถจัดแบ่งประเภทการบริการต่างๆ ที่เป็นทรัพย์สินโดยแยกตามลักษณะความจำเป็นในการใช้งานรายละเอียด ดังนี้

ตารางที่ 4.9 รายชื่อทรัพย์สินด้านงานบริการ

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
งานบริการ Internet	ให้บริการเผยแพร่ข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการ Intranet	ให้บริการเผยแพร่ข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการ ตัดต่อภาพ แปลง File	ให้บริการ	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการติดตั้ง บำรุงรักษา อุปกรณ์เครื่อง PC	บำรุงรักษา(Outsource)	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการติดตั้ง บำรุงรักษา โปรแกรมคอมพิวเตอร์	บำรุงรักษา (Outsource)	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริหารจัดการสิทธิ ในการเข้าถึงข้อมูล การเข้าใช้งานระบบต่างๆ	Computing (Admin)	ฝ่ายเทคโนโลยีสารสนเทศ
งานบำรุงรักษาระบบเครื่องแม่ข่าย	บำรุงรักษา(Outsource)	ฝ่ายเทคโนโลยีสารสนเทศ
งานบำรุงรักษา ระบบเครือข่าย	บำรุงรักษา(Outsource)	ฝ่ายเทคโนโลยีสารสนเทศ

4.2.3 กำหนดเกณฑ์การประเมินระดับความเสี่ยงของระบบด้วย Risk Assessment Matrix ได้แก่ ระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) รายละเอียดแสดงได้ ดังนี้

4.2.3.1 ระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) ตามตารางที่ 4.10 ดังนี้

ตารางที่ 4.10 ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood)		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสเกิดขึ้นสูงมาก
4	สูง	มีโอกาสเกิดขึ้นค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	มีโอกาสเกิดขึ้นบางครั้ง
2	น้อย	อาจจะมีโอกาสเกิดขึ้นแต่นานๆครั้ง
1	น้อยมาก	อาจจะไม่มีโอกาสเกิดขึ้นเลย

4.2.3.2 ระดับความรุนแรงของผลกระทบ (Impact) ตามตารางที่ 4.11

ตารางที่ 4.11 เกณฑ์การประเมินผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (Impact)

	ระดับความรุนแรงของผลกระทบของความเสี่ยง(Impact)	
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	มีผลกระทบมาก ระบบเสียหายทั้งหมดไม่สามารถใช้งานอีกต่อไป/ข้อมูลที่สำคัญเสียหายทั้งหมด ทำให้องค์กรเสียหายมาก
4	สูง	มีผลกระทบต่อความปลอดภัยของระบบเสียหายบางส่วน ไม่สามารถใช้งานได้ตามปกติ/ข้อมูลที่เป็นความลับ ถูกเปิดเผยมีผลกระทบร้ายแรงต่อองค์กรมากต้องใช้ระยะเวลาในการกู้คืนระบบ
3	ปานกลาง	มีผลกระทบต่อความปลอดภัยของระบบเสียหายหายทั้งหมดบางส่วน ไม่สามารถใช้งานชั่วคราวได้ตามปกติ/ข้อมูลที่เป็นความลับ ถูกเปิดเผยมีผลกระทบร้ายแรงต่อองค์กรมาก
2	ต่ำ	มีผลกระทบต่อความปลอดภัยเล็กน้อย ระบบสามารถใช้งานได้ตามปกติ/ข้อมูลที่เปิดเผยไม่มีผลกระทบหรือไม่สำคัญต่อองค์กรมีไม่มากนัก
1	ต่ำมาก	มีผลกระทบต่อความปลอดภัยเล็กน้อย ระบบสามารถใช้งานได้ตามปกติ/ข้อมูลที่เปิดเผยไม่มีผลกระทบหรือไม่สำคัญต่อองค์กร

การวิเคราะห์ความเสี่ยง (Risk Analysis) และเกณฑ์ในการประเมินความเสี่ยง ในโครงงานนี้จะนำผลของการประเมินความเสี่ยงประยุกต์ใช้ในการบริหารจัดการด้านเทคโนโลยีสารสนเทศและวางแผนการบริหารจัดการความเสี่ยง พร้อมทั้งจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค ฉบับที่ 2 ประจำปี 2556-2559 (ซึ่งอยู่ระหว่างดำเนินการจัดทำ) และแผนปฏิบัติราชการ 4 ปี โดยศึกษาวิเคราะห์ระบบเทคโนโลยีสารสนเทศขององค์กรทั้งหมดในปัจจุบัน เพื่อหาสาเหตุ ปัจจัย และวัดผลกระทบของความเสี่ยงที่อาจจะเกิดขึ้นและหาแนวทางแก้ไข พร้อมทั้งวางแผนจัดเตรียมการวิเคราะห์ เพื่อของบประมาณด้าน ICT ประจำปี ตามเหตุผลความจำเป็นที่หน่วยงานต้องการปิดช่องโหว่ของระบบและแก้ไข ป้องกันปัญหาที่อาจจะเกิดขึ้นได้จากการวิเคราะห์และประเมินความเสี่ยง

4.3 การประเมินความเสี่ยงก่อนการดำเนินโครงการ

การประเมินความเสี่ยง (Risk Assessment) หมายถึง การคาดคะเนหรือคำนวณโอกาสที่จะเกิดเหตุการณ์ที่นำไปสู่ความเสียหายและมีการสูญเสียเกิดขึ้น จากการที่มีกระบวนการ/ขั้นตอนจากการระบุ/สินทรัพย์ เรียบร้อยแล้วก็นำมาสู่หลักการของประเมินความเสี่ยง(Risk Assessment) และคำนวณค่าความเสี่ยงโดยรวมซึ่งประกอบด้วย ขั้นตอนการวิเคราะห์ การประเมินและการจัดระดับความเสี่ยง เพื่อการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศขององค์กร เช่น ต้องการทราบว่ามีอะไรบ้างที่จะเป็นจุดอ่อน หรือช่องโหว่ เป็นสาเหตุให้เกิดภัยคุกคามซึ่งนำมาให้เกิดความเสียหายและผลกระทบต่อองค์กร เมื่อถูกโจมตีจุดอ่อน หรือช่องโหว่ที่มีอยู่ หรือมูลค่าทรัพย์สินขององค์กรเสียหาย มีอะไรบ้างและจำนวนเท่าไร เราจะป้องกันหรือแก้ไขช่องโหว่ หรือจุดอ่อนได้อย่างไร

ในการพิจารณาจากระดับความสำคัญของทรัพย์สิน ซึ่งผลลัพธ์การประเมินจะทำให้ทราบระดับความเสี่ยงต่อทรัพย์สินแต่ละอย่าง ทั้งที่ยอมรับได้และยอมรับไม่ได้ ซึ่งจะทำให้ได้แผนงานในการดำเนินงาน การเตรียมรับมือ ป้องกันความเสี่ยงที่เกิดขึ้น โดยจะต้องผ่านการอนุมัติจากผู้บริหารขององค์กร โดยกำหนดมาตรการที่เหมาะสมอ้างอิงตามมาตรฐานความปลอดภัยสากล ISO/IEC 17799, BS7799 และ ISO/IEC 27001 ทำให้ทราบถึงความสำคัญของความเสี่ยงที่แตกต่างกันและใช้ในการพิจารณากำหนดจุดควบคุมความเสี่ยงที่มีนัยสำคัญ การประเมินความเสี่ยงเป็นกระบวนการ ที่ประกอบด้วย การวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานขององค์กรก่อนที่จะทำการประเมินความเสี่ยงเพื่อให้เกิดความชัดเจนในการประเมิน ประกอบด้วยขั้นตอนและข้อมูลต่างๆ ซึ่งสามารถสรุปได้ดังต่อไปนี้

(1) ระบุปัจจัยในกระบวนการประเมินความเสี่ยงซึ่ง ได้แก่ ทรัพย์สิน (Assets) ช่องโหว่ (Vulnerabilities) ภัยคุกคาม (Treats) ผลกระทบต่อธุรกิจ (Business Impact) และการควบคุม (Controls) จากการวิเคราะห์ความเสี่ยงเพื่อการนำข้อมูลที่ได้มาประเมินความเสี่ยง ดังนี้

การประเมินความเสี่ยงก่อน การดำเนินโครงการ จะใช้ Risk Calculation

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

Risk Value = ค่าความเสี่ยง

Likelihood = โอกาสที่จะเกิด

Impact = ผลกระทบ

(2) การประเมินโอกาสและผลกระทบของความเสี่ยง วิเคราะห์ระดับความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงที่ระบุไว้มาประเมินโอกาสที่จะเกิดความเสียหาย (Likelihood) และประเมินระดับความรุนแรงของผลกระทบ (Impact) ตามเกณฑ์การประเมินความเสี่ยงขององค์กรตามระดับของความเสี่ยง (Degree of Risk) ที่แตกต่างกัน กำหนดเกณฑ์ระดับความเสี่ยงไว้ 3 ระดับ ได้แก่ ต่ำ ปานกลาง สูง ดังนี้

ระดับความเสี่ยง 1 – 8 ต่ำ (Low)

ระดับความเสี่ยง 9 – 16 กลาง (Medium)

ระดับความเสี่ยง 17 – 25 สูง (High)

รายละเอียด การคำนวณประเมินความเสี่ยง (Risk Value) ตามตารางข้างล่างนี้

ตารางที่ 4.12 การคำนวณประเมินความเสี่ยง (Risk Value)

Risk Value		Likelihood				
		Very Low	Low	Medium	High	Very High
	Very low	1	2	3	4	5
	Low	2	4	6	8	10
	Medium	3	6	9	12	15
	High	4	8	12	16	20
	Very High	5	10	15	20	25

(3) การวัดและประเมิน เพื่อให้ผู้บริหารเข้าใจและรับรู้ถึงความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศและมีการกำหนดแผนปฏิบัติในการลดความเสี่ยงดังกล่าว ให้อยู่ในระดับที่ยอมรับได้ (Risk Acceptance Level)

(4) ขั้นตอนในการวิเคราะห์ หาวิธีการในการควบคุมความเสี่ยง (Control Analysis) หลังจากได้ทำการรวบรวมข้อมูลและศึกษาข้อมูลเกี่ยวกับระบบ ตลอดจนสามารถระบุภัยคุกคามและช่องโหว่ต่างๆ ของระบบได้แล้ว ขั้นตอนต่อไปคือวิเคราะห์วิธีการหรือแนวทางใน การควบคุมความเสี่ยงที่หน่วยงาน มีการดำเนินการอยู่แล้วในปัจจุบันหรือมีแผนที่จะดำเนินการกิจกรรมโครงการใน อนาคตอันใกล้ โดยอาศัย การควบคุมความมั่นคงปลอดภัย (Control Checklist) ของ ISO/IEC 27001 ที่ได้จากการประเมินความเสี่ยง

4.3.1 การประเมินความเสี่ยง (Risk Assessment) ก่อนการดำเนินโครงการ มีการจัดทำตารางวิเคราะห์และประเมินความเสี่ยงก่อนดำเนินโครงการ รายละเอียดดังนี้

4.3.1.1 ตารางระบุขอบเขตประเมินความเสี่ยงตามกลุ่มทั้ง 11 โดเมน ด้วยมาตรฐาน ISO/IEC 27001 วิเคราะห์ตามวัตถุประสงค์ที่จำเป็น ตามรายละเอียด (ภาคผนวก ก)

4.3.1.2 ตารางประเมินความเสี่ยงแยกตามกลุ่มสินทรัพย์ ในการประเมินทรัพย์สินและบริหารความเสี่ยงโดยแบ่งระบุสินทรัพย์ได้ 5 ประเภท โดยแยกตามองค์ประกอบของระบบงานคอมพิวเตอร์ ได้แก่ (1) ทรัพย์สินประเภทฮาร์ดแวร์และอุปกรณ์ต่อพ่วง (Hardware Assets) (2) ทรัพย์สินประเภทซอร์ฟแวร์ (Software Assets) (3) ทรัพย์สินข้อมูล (Information Assets)

(4) ทรัพย์สินประเภทบริการ (Service Assets) (5) ทรัพย์สินประเภทบุคคลากร(People Assets) ตามรายละเอียด (ภาคผนวก ข)

4.3.2 การตรวจสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยตรวจสอบช่องโหว่ หรือจุดอ่อนด้วยโปรแกรมต่างๆ ที่มีการโจมตีทั้งจากภายในและภายนอก ได้แก่ (1) ด้วยโปรแกรม Nessus (2)โปรแกรม Lancope (3) การจัดลำดับความสำคัญของความเสี่ยง

4.4 ปิดช่องโหว่ของระบบ(Hardening) และดำเนินการปรับปรุงให้ระบบมีความปลอดภัยมากขึ้น

จากการวิเคราะห์และประเมินความเสี่ยง ก่อนการดำเนินโครงการ แล้วนำผลวิเคราะห์มาทบทวนพิจารณาและมีการตรวจสอบ ช่องโหว่/ จุดอ่อนของระบบ เพื่อควบคุม แก้ไขปัญหาความเสี่ยงเบื้องต้นที่สามารถจัดการได้โดย ยังไม่มีการใช้งบประมาณ เมื่อองค์กรได้ดำเนินการและทราบผลการประเมินความเสี่ยงก่อนและนำมาปรับปรุง ก็จะทำการประเมินความเสี่ยงอีกครั้ง เพื่อนำผลที่ได้มาวิเคราะห์เปรียบเทียบ และปิดช่องโหว่ ของระบบเทคโนโลยีสารสนเทศ ที่สามารถดำเนินการได้ในแบบพื้นฐานสำคัญ ดังนี้

4.4.1 การควบคุมการเข้าถึงระบบ ทบทวนแนวปฏิบัติพื้นฐาน เพื่อให้เกิดความปลอดภัยของระบบในเบื้องต้น ได้แก่

4.4.1.1 การตรวจสอบระบบต่างๆ ได้แก่ ป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต ป้องกันการให้บริการทางเครือข่าย ป้องกันการเข้าใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต ตรวจจับเหตุการณ์ที่ผิดหรือไม่ได้รับอนุญาต

4.4.1.2 ควบคุมการเข้าถึงข้อมูล

4.4.1.3 มีการควบคุมการเข้าออก (Physical entry Control)

4.4.2 มีการระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of Assets) มีการจัดทำฉลากให้ทราบผู้รับผิดชอบทรัพย์สินต่างๆ

4.4.2.1 เพื่อกำหนดผู้รับผิดชอบให้ชัดเจน ได้แก่ การลดความเสี่ยงที่อาจเกิดเนื่องจากความผิดพลาดของคน การขโมย การฉ้อโกงหรือหลอกลวง การใช้งานระบบในทางที่ผิด

4.4.2.2 เพื่อให้มั่นใจว่าผู้ใช้มีความระมัดระวังเกี่ยวการรักษาความปลอดภัยของข้อมูลและมีระบบป้องกัน เช่น รองรับนโยบายทางด้านการรักษาความปลอดภัยในการปฏิบัติงานปกติของพนักงาน การวางแผนความเสี่ยงเพื่อลดความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์การทำงานที่ผิดพลาดของระบบ

4.4.3 จัดทำเอกสารแสดงนโยบาย ISMS

4.4.3.1 เอกสารข้อกำหนดรายละเอียดของระบบงาน

4.4.3.2 จัดทำคู่มือวิธีการปฏิบัติงาน และการควบคุมเพื่อสนับสนุนต่อ ISMS

4.4.3.3 รายงานต่างๆ ที่จำเป็น

4.4.3.4 เอกสารวิธีการปฏิบัติงานที่จำเป็นสำหรับองค์กร เพื่อให้มั่นใจได้ถึงความมีประสิทธิผลในการวางแผนการดำเนินงาน

4.5 การประเมินความเสี่ยงหลังดำเนินโครงการ

มีการตรวจสอบ ช่องโหว่/ จุดอ่อนของระบบ เพื่อควบคุม แก้ไข ปัญหาความเสี่ยงเบื้องต้นที่สามารถจัดการได้โดย ยังไม่มีการใช้งบประมาณ เมื่อองค์กร ได้ดำเนินการและทราบผลการประเมินความเสี่ยงก่อนและนำมาปรับปรุง ก็จะทำการประเมินความเสี่ยงอีกครั้ง เพื่อนำผลที่ได้มาวิเคราะห์เปรียบเทียบ ระหว่างการวิเคราะห์และประเมินความเสี่ยง ทั้งก่อน-หลังการดำเนินโครงการ

4.6 การจัดการความเสี่ยง(Risk Management)

โดยควบคุม แก้ไข ปัญหาการจัดการความเสี่ยง เมื่อองค์กร ได้ดำเนินการและทราบผลการประเมินความเสี่ยงก็จะได้รับทราบประกอบด้วยขั้นตอนและข้อมูลต่างๆ ซึ่งมีการบริหารความเสี่ยงได้หลายวิธี ได้แก่ การลดความเสี่ยง การหลีกเลี่ยงความเสี่ยง การถ่ายโอนความเสี่ยง การยอมรับความเสี่ยงที่เหลืออยู่มีรายละเอียด ดังนี้

4.6.1 การลดความเสี่ยง

4.6.1.1 จัดทำ Check List ตามมาตรฐาน ISO 27001 เพื่อตรวจสอบและเก็บข้อมูลจากผู้มีส่วนได้เสียและผู้ที่เกี่ยวข้องในการใช้งานและมีผลกระทบระบบ ICT

4.6.1.2 นำผลการวิเคราะห์ นำเสนอที่ประชุมผู้บริหาร หรือคณะกรรมการ ICT ของสำนักงาน เพื่อรับข้อเสนอแนะ จากผู้เชี่ยวชาญด้าน ICT มาวิเคราะห์และจัดหมวดหมู่ จัดกลุ่มแยกประเภท เพื่อการบริหารจัดการความเสี่ยงในด้าน ICT ภายใต้การควบคุม

การควบคุม หมายถึง ความเสี่ยงที่ยอมรับได้แต่ต้องมีการแก้ไขเกี่ยวกับการควบคุมที่มีอยู่ในปัจจุบัน เพื่อให้มีการควบคุมที่เพียงพอและเหมาะสม เช่น จัดทำแผนการดำเนินงาน จัดทำแผนงานบริหารความเสี่ยง จัดทำแผนฉุกเฉิน เป็นต้น

4.6.1.3 นำข้อมูลเบื้องต้นด้านอื่นๆ ที่เกี่ยวข้อง รวมทั้ง Check List มาวิเคราะห์ เพื่อหาแนวทาง จัดทำข้อเสนอในการบริหารจัดการความเสี่ยงด้าน ICT เพื่อให้มีการทบทวน ปรับปรุง จัดทำนโยบายความปลอดภัยระบบสารสนเทศ (Policy) และนำมาจัดทำแผนฉุกเฉิน

4.6.2 หลีกเลี่ยง หรือ ยกเลิกความเสี่ยง หมายถึง ความเสี่ยงที่ไม่สามารถยอมรับได้และต้องจัดการให้ความเสี่ยงนั้นอยู่นอกเหนือเงื่อนไขการดำเนินงาน โดยต้องมีวิธีการจัดการความเสี่ยงในกลุ่มนี้ให้เหมาะสม อาจจะเกี่ยวข้องกับงบประมาณในการดำเนินการ

4.6.3 ถ่ายโอนความเสี่ยง คือการถ่ายโอนความเสี่ยงให้กับบุคคลภายนอกรับผิดชอบแทน แต่ในกรณีของหน่วยงานภาครัฐ จะมีปัจจัยหลายอย่างที่เกี่ยวข้อง เช่น ข้อจำกัดด้านงบประมาณ ความเหมาะสมตามภารกิจ ข้อจำกัดด้านบุคลากร

4.6.4 ยอมรับความเสี่ยงที่มีอยู่ (Accept Risk) คือความเสี่ยงที่เกิดขึ้นสามารถยอมรับได้ ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องมีการดำเนินการใดๆ

4.6.5 วางแผนฉุกเฉิน ต้องมีแผนการในการจัดทำแผนฉุกเฉินเพื่อรองรับความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งมีผลกระทบต่อการให้การบริการประชาชน

4.7 สรุปผลการวิเคราะห์และประเมินความเสี่ยง

จากการวิเคราะห์ความเสี่ยงระบบสารสนเทศของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค โดยพิจารณาจาก การให้ความสำคัญของระดับของผลกระทบ และโอกาสในการเกิดภัยคุกคาม รวมทั้งชนิดของภัยคุกคามที่อาจเกิดขึ้น ซึ่งได้แยกการพิจารณาตามประเภทของทรัพย์สินสารสนเทศขององค์กร

4.8 นำมาประยุกต์ใช้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศ

ผลที่ได้จากการวิเคราะห์ความเสี่ยงระบบสารสนเทศของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค นำมาพัฒนาปรับปรุงนโยบายความปลอดภัยระบบสารสนเทศ ใช้ในการวางแผนการจัดการดำเนินงานต่างๆ จัดทำแผนงานบริหารความเสี่ยงของหน่วยงาน รวมทั้งการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 2) ปี 2556-2559