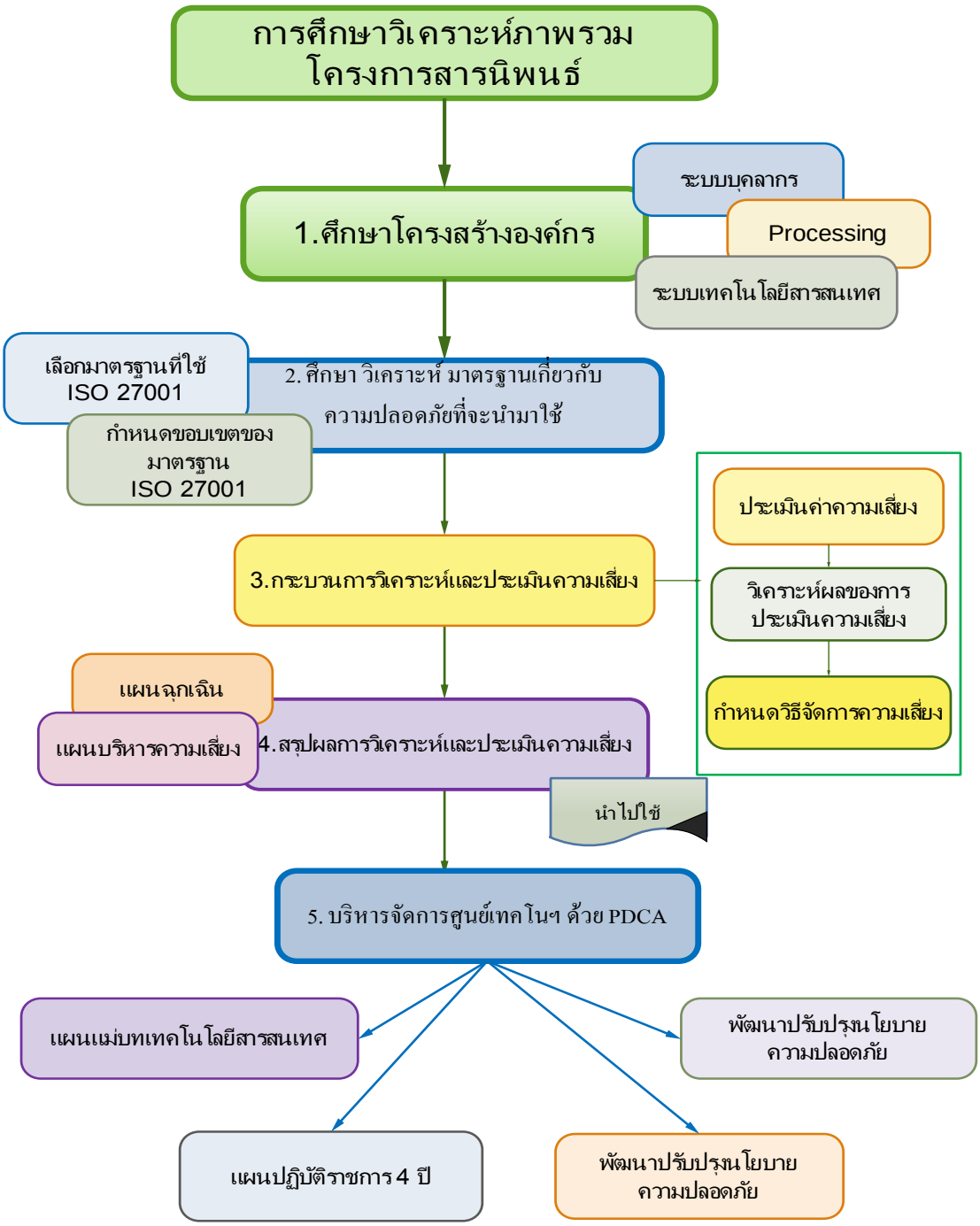
บทที่ 3
วิธีการและขั้นตอนการดำเนินงาน

ในการจัดทำโครงงานสารนิพนธ์จะกล่าวถึง วิธีการและขั้นตอนการดำเนินงานในการศึกษาวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค เพื่อให้สอดคล้องกับวัตถุประสงค์ของโครงงาน ที่ได้กำหนดไว้ ซึ่งรายละเอียดขั้นตอนในการดำเนินงาน(Process) มีความสำคัญอย่างมาก ซึ่งเป็นการศึกษาวิเคราะห์ถึงปัญหาและสาเหตุความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศขององค์กร เพื่อต้องการทราบจุดอ่อนหรือช่องโหว่ของระบบเทคโนโลยีสารสนเทศ เพื่อจะได้หาวิธีการ จัดการแก้ปัญหาและพัฒนาปรับปรุงระบบให้ดีขึ้น ทั้งนี้ในการจัดทำและนำเสนอขั้นตอนต่างๆ ให้ชัดเจนทำให้หน่วยงานภาครัฐที่เป็นองค์กรเล็ก ๆ ด้าน ICT สามารถวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรด้วยตัวเอง โดยเลือกใช้มาตรฐานสากล ISO/IEC 27001 ที่เน้นในด้านความปลอดภัยของระบบสารสนเทศที่ยอมรับทั่วไป โดยศึกษาและกำหนดขั้นตอนการดำเนินงานให้ชัดเจน วิธีการศึกษาวิเคราะห์ให้เหมาะสมกับลักษณะงานขององค์กรนั้นๆ เพื่อนำมาปรับปรุงช่องโหว่หรือจุดอ่อนด้าน ICT โดยไม่ต้องเสียงบประมาณ ในการบริหารจัดการหรือสามารถใช้เป็นกรณีศึกษาในการบริหารจัดการด้านความปลอดภัยของระบบสารสนเทศและนำไปใช้ในการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีวิธีการและขั้นตอนในการดำเนินงานและรายละเอียด ดังนี้

3.1 ศึกษาภาพรวมการดำเนินงานโครงการ
3.2 แหล่งที่มาและวิธีการเก็บรวบรวมข้อมูล
3.3 ศึกษาวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและภัยคุกคาม
3.4 อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย
3.5 วิธีการวิเคราะห์และประเมินความเสี่ยง
3.6 ระยะเวลาในการดำเนินการวิจัย
3.7 ขั้นตอนวิธีการดำเนินการศึกษาและวิเคราะห์ความเสี่ยง

3.1 ศึกษาภาพรวมการดำเนินงานโครงการ

การศึกษาภาพรวมวิธีการและขั้นตอนในการดำเนินงานการวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศ ขั้นตอนตามภาพที่ 3.1



ภาพที่ 3.1 วิธีการดำเนินงาน

การศึกษาวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศเพื่อนำผลการวิเคราะห์และประเมินความเสี่ยงมาบริหารจัดการระบบสารสนเทศของหน่วยงานให้สอดคล้องกับวัตถุประสงค์ของโครงงานที่ได้กำหนดไว้ เพื่อให้การดำเนินงานโครงการมีประสิทธิภาพสะท้อนปัญหาหรือจุดอ่อนที่แท้จริงของการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศโดยได้กำหนดกรอบแนวคิดในการศึกษา 4 หัวข้อ ดังนี้

3.1.1 ศึกษา วิเคราะห์ สถานะของระบบเทคโนโลยีสารสนเทศในปัจจุบัน เพื่อรับทราบปัญหาและความเสี่ยงด้าน ICT ในปัจจุบันขององค์กร โดยศึกษาผลกระทบความเสี่ยงด้านต่างๆ วิธีการแก้ปัญหา จากผู้มีส่วนเกี่ยวข้องโดยศึกษาวิเคราะห์ สังเกต สัมภาษณ์ จากระบบทั้งหมดที่เป็น Work Flow ต่างๆ ได้แก่

3.1.1.1 สัมภาษณ์บุคคลที่เกี่ยวข้อง ได้แก่

ผู้บริหาร (CIO) เพื่อทราบถึง พันธกิจ วิสัยทัศน์และกลยุทธ์ในการดำเนินงานด้าน ICT เพื่อหาโอกาสในการแก้ปัญหา

บุคลากรด้าน ICT เพื่อรับทราบปัญหา ในการปฏิบัติงาน สถานปัจจุบันของระบบสารสนเทศของหน่วยงาน

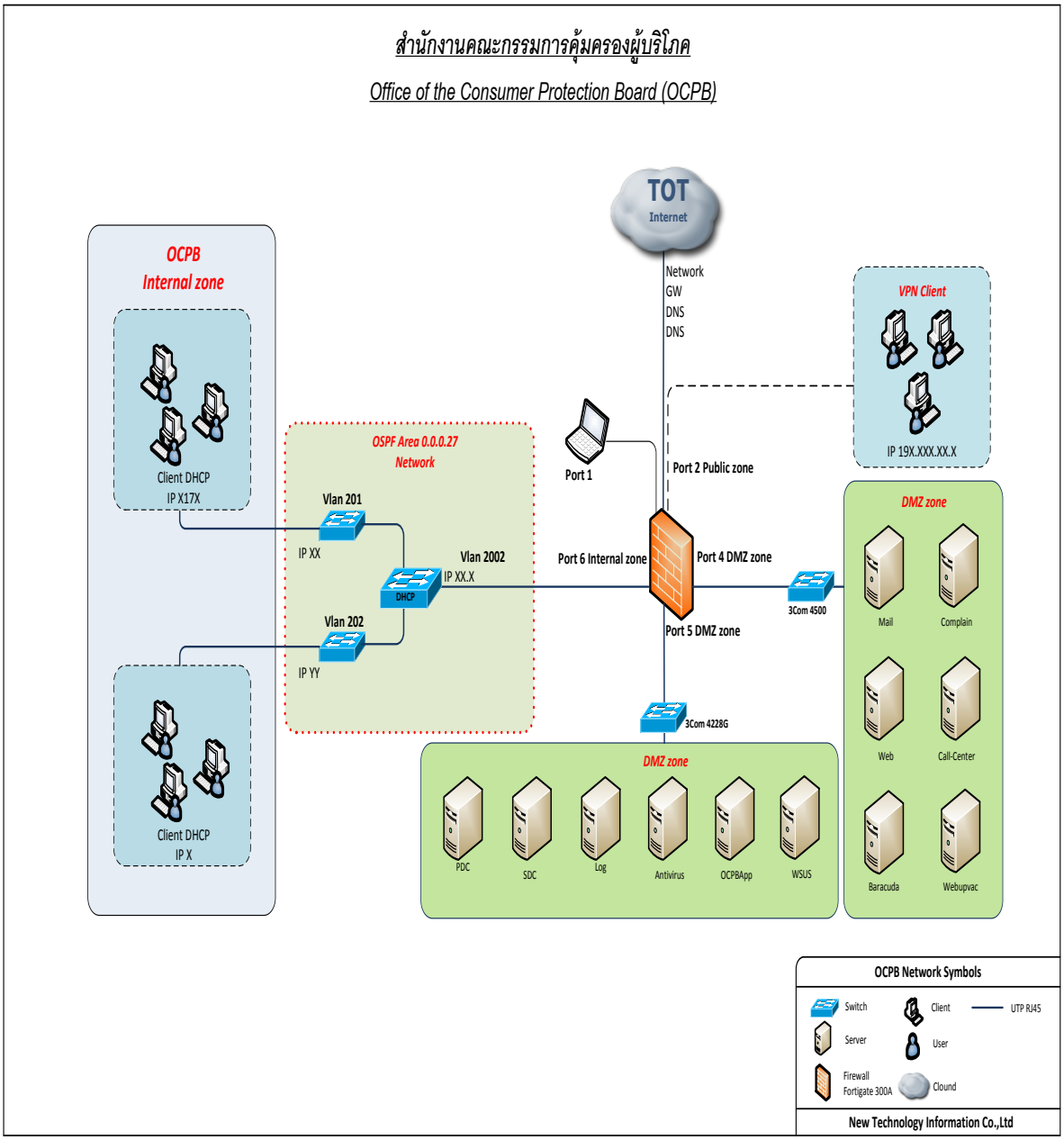
ผู้ใช้ระบบ (User) ทำให้ทราบปัญหาต่างๆ ในการใช้งาน เช่น ระบบช้า หน้าจอผู้ใช้งานซับซ้อนเกินไป ระบบเครือข่ายหลุดบ่อยๆ

3.1.1.2 ศึกษาจากเอกสารคู่มือต่างๆ

เอกสารผู้ดูแลระบบ เพื่อให้ทราบถึงขั้นตอนในการทำงานของระบบด้าน ICT เพื่อหาวิเคราะห์ปัญหาที่กระทบต่อระบบ

เอกสารคู่มือผู้ใช้ระบบด้าน ICT เพื่อรับทราบปัญหา ในการปฏิบัติงานสถานะปัจจุบันขอบระบบสารสนเทศของหน่วยงาน

3.1.2 ศึกษาโครงสร้างของระบบเครือข่าย เพื่อวิเคราะห์สถานะการณ์ในการดำเนินงานด้าน ICT ในปัจจุบัน การวางแผนด้านระบบเครือข่าย วางแผนในด้านการจัดหาเครื่องแม่ข่ายเพื่อรองรับการขยายงานที่เพิ่มขึ้น การดูแลความปลอดภัยด้านกายภาพของ โครงสร้างระบบเครือข่ายและอุปกรณ์ต่อพ่วง เพื่อนำมาวิเคราะห์ ความปลอดภัยและการควบคุมการเข้าถึงข้อมูลมีไดอะแกรมรายละเอียด ตามภาพที่ 3.2



ภาพที่ 3.2 ระบบเครือข่าย (Network System)

ที่มา : ศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

3.1.3 ศึกษาเรื่องของความเสี่ยงและการประเมินความเสี่ยง เพื่อนำมาการวิเคราะห์ปัญหาที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศ ซึ่งแต่ละองค์กรจะมีความเสี่ยงไม่เหมือนกันแล้วแต่ภารกิจหลักและบริบทต่างๆ เพื่อให้รู้ปัญหาต่างๆ มีดังนี้

3.1.3.1 เหตุการณ์ความเสี่ยง (Risks) หมายถึง เหตุการณ์ต่างๆ ที่มีโอกาสเกิดขึ้นได้ซึ่งเป็นภัยคุกคามและความเสียหายเกิดขึ้นจะเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กรและส่งผลเสียหายทั้งเป็นเงินและไม่เป็นตัวเงิน หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายองค์กร จุดอ่อน (Vulnerability) คือ ช่องโหว่ที่มี โดยจุดอ่อนต่างๆ อาจอยู่ในโครงสร้างขององค์กร ในเรื่องของขั้นตอนการปฏิบัติงาน บุคลากรขาดความสามารถ ไม่มีการบริหารจัดการด้านการรักษาความปลอดภัยของสารสนเทศที่ดีพอ จุดอ่อนเรื่องฮาร์ดแวร์ซึ่งอาจจะรุ่น เสียบ่อยๆ และการให้บริการหลังการขายมีช่องว่างในการใช้งาน หรือมีข้อบกพร่องมาจากโรงงาน จุดอ่อนเรื่องซอฟท์แวร์ ซึ่งอาจมีข้อบกพร่องมาจากโรงงาน ซึ่งจุดอ่อนในตัวมันเองมักไม่ก่อให้เกิดอันตรายถ้าไม่มีภัยคุกคาม (Threat) เช่น ถ้าไม่ล็อคประตูบริเวณแถวนั้นไม่มีโจรของก็ไม่หาย ไวรัสทำให้ข้อมูลเสียหายข้อมูลสำคัญถูกขโมยซึ่งอาจทำให้องค์กรสูญเสียข้อได้เปรียบด้านการแข่งขัน หรือหน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้องค์กรเสียชื่อเสียง

3.1.3.2 การประเมินความเสี่ยง (Risk assessment) หมายถึง การกำหนดเหตุการณ์ความเสี่ยงที่มีโอกาสเกิดขึ้นได้ กำหนดระดับของผลกระทบหากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้นจริง และกำหนดค่าความเสี่ยงของเหตุการณ์ความเสี่ยงนั้น การประเมินความเสี่ยงมีจุดประสงค์เพื่อคาดการณ์ว่ามีเหตุการณ์ความเสี่ยงใดบ้างที่เกี่ยวข้องกับทรัพย์สินสารสนเทศหนึ่ง และมีระดับความเสี่ยงมากน้อยเพียงใด ทั้งนี้เพื่อจะได้เตรียมการป้องกันไว้ก่อน ก่อนที่เหตุการณ์ความเสี่ยงนั้นจะเกิดขึ้นจริงและทำให้องค์กรเกิดความเสียหาย

การประเมินความเสี่ยง (Risk Assessment) เป็นการประเมินความเสี่ยงขององค์กรว่ามีวัตถุประสงค์อะไร และมีความเสี่ยงอะไรบ้าง ที่ทำให้ไม่บรรลุวัตถุประสงค์และความเสี่ยงนั้นมีนัยสำคัญเพียงใด โดยการจัดลำดับความเสี่ยง และหาแนวทางการควบคุม (กิจกรรมที่ปฏิบัติ) เพื่อป้องกัน หรือลดความเสี่ยงนั้นๆ มีขั้นตอนดังนี้

การระบุปัจจัยเสี่ยง (Risk Identification) ทั้งนี้จะต้องศึกษาวัตถุประสงค์และเป้าหมายขององค์กรซึ่งจะสอดคล้องกับภารกิจ (Mission) ซึ่งแบ่งเป็น 2 ระดับ คือ

1. วัตถุประสงค์ระดับองค์กร (Entity – Ievel Objectives) เป็นวัตถุประสงค์ตามแผนกลยุทธ์ขององค์กร หรือแผนปฏิบัติราชการ 4 ปี (พ.ศ. 2555 – 2558)

2. วัตถุประสงค์ระดับกิจกรรม (Activity–Ievel Objectives) เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจง สำหรับแต่ละกิจกรรมในแต่ละหน่วยงาน ซึ่งต้องสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การวัดและประเมินความเสี่ยง (Risk Measurement) ทั้งนี้ต้องศึกษาก่อน ว่าอะไรเป็นปัจจัยเสี่ยงและมีความเสี่ยงอย่างไร ด้านการดำเนินงาน งบประมาณ กลยุทธ์ในการวิเคราะห์จะดูถึง

สาเหตุ (Cause) ของการเกิดนั้นมีโอกาส (Opportunity) มากน้อยเพียงใดและเมื่อเกิดแล้วจะมีผลกระทบ (Effect) มากน้อยเพียงใด

การจัดลำดับความเสี่ยง (Risk Prioritization) เมื่อเทียบความเสี่ยง โอกาสและผลกระทบแล้วจะต้องมาจัดลำดับว่าความเสี่ยงนนั้ มีนัยสำคัญเพียงใด โดยการจัดลำดับความเสี่ยง จากมากไปหาน้อย หรือเลือกเทคนิคการวิเคราะห์ความเสี่ยงที่เหมาะสม โดยอาจจะวิเคราะห์ในรูปตัวเลขก็ได้ มีขั้นตอนการในการวิเคราะห์ ดังนี้

1. ประเมินระดับความสำคัญของปัจจัยเสี่ยง คือปัจจัยเสี่ยงแต่ละปัจจัย หากเกิดขึ้นแล้วมีผลกระทบต่อองค์กรมากน้อยเพียงใด

2. ประเมินความเสี่ยงที่ปัจจัยเสี่ยงจะเกิดขึ้นคือพิจารณาว่าปัจจัยเสี่ยงที่เรียงลำดับความสำคัญแล้วมีโอกาสที่จะเกิดขึ้น มากน้อยเพียงใด

3.1.3.3 ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk) หมายถึง ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง มีค่าน้อยกว่าค่าที่ยอมรับได้นี้ จะถือว่าทรัพย์สินสารสนเทศที่เกี่ยวข้องกับเหตุการณ์ฯ มีความมั่นคงปลอดภัยเพียงพอ (และผู้ประเมินความเสี่ยงไม่จำเป็นต้องนำเสนอแผนการลดความเสี่ยงใดๆ เพิ่มเติม)

3.1.3.4 แผนการลดความเสี่ยง (Risk treatment plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานเพื่อพิจารณาอนุมัติก่อน

3.1.3.5 ภัยคุกคาม (Threat) คือเรื่องในทางลบต่อองค์กร ซึ่งยังไม่ได้เกิดขึ้น หรือหากเกิดขึ้นอาจเกิดจากจุดอ่อนหรือช่องโหว่ของระบบสารสนเทศ เช่น ไวรัสโจมตี ข้อมูลเปลี่ยนแปลงโดยไม่ได้รับอนุญาต DoS (Denial of Service) ข้อมูลไม่สามารถดึงมาใช้งานได้ เป็นต้น

3.1.3.6 การจัดการความเสี่ยง (Risk Management) หมายถึง การบริหารจัดการด้านต่างๆ ในด้านการวางแผนจัดองค์กร การบังคับบัญชา และการควบคุมการปฏิบัติงานขององค์กร เพื่อลดผลเสียหายของความไม่แน่นอนที่จะเกิดขึ้นกับองค์กร เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์ตามที่กำหนดในการบริหารความเสี่ยง จะต้องมีต้นทุนทรัพยากรและบุคคล ดังนั้นจะต้องคำนึงถึงผลประโยชน์ที่จะได้รับด้วยว่าคุ้มค่าหรือไม่ ในการลดความเสี่ยงเหล่านั้น เพราะเหตุว่าความเสี่ยงนั้นมีการเปลี่ยนแปลงอยู่ตลอดเวลา แล้วแต่บริบทของเหตุการณ์นั้นๆ เมื่อวิเคราะห์และจัดลำดับความเสี่ยงตามโอกาสที่เกิดความเสี่ยงและวิเคราะห์สาเหตุที่ทำให้เกิดความเสี่ยงรวมทั้งพิจารณาหาวิธีหรือกำหนดกิจกรรมการต่างๆ เพื่อควบคุมความเสี่ยงนั้นๆ วิธีการมีหลายวิธี เช่น หลีกเลี่ยง

ยอมรับ ควบคุม หรือถ่ายโอนความเสี่ยง ในการบริหารความเสี่ยงต้องพิจารณาด้านงบประมาณในการใช้จ่าย รวมทั้งความคุ้มค่าและความเหมาะสม

3.1.4 ศึกษาทำความเข้าใจมาตรฐาน ISO/IEC 27001 โดยศึกษา วิเคราะห์กระบวนการและจัดเตรียมความพร้อม จัดทำขอบเขตของการบริหารความเสี่ยงตามแนวทางมาตรฐาน ISO/IEC 270001 เพื่อการบริหารจัดการความเสี่ยงของระบบสารสนเทศซึ่งประกอบด้วย ขั้นตอนต่างๆ ผู้เขียนได้จัดทำโครงการศึกษาได้จัดทำในรูปแบบมีขั้นตอนที่ชัดเจน(Process) เพื่อง่ายต่อการทำความเข้าใจ มี 11 โดเมน 133 Control Objective มีรายละเอียด ดังนี้

3.1.4.1 Security Policy-A5 (นโยบายการรักษาความปลอดภัย) เป็นสิ่งแรกที่สำคัญและจำเป็นสำหรับองค์กรที่ต้องมีเพื่อเป็นแนวทาง และสนับสนุนการรักษาความปลอดภัยของระบบสารสนเทศ

3.1.4.2 Organizing Information Security-A6 (การจัดโครงสร้างระบบการรักษาด้านความปลอดภัยขององค์กร) มีจุดประสงค์เพื่อการบริหารความปลอดภัยของข้อมูลภายในองค์กร และดูแลควบคุมระบบการรักษาความปลอดภัยของข้อมูลและระบบที่ต้องมีการเข้าถึงจากภายนอกองค์กร

3.1.4.3 Asset Management-A7 (การจัดการทรัพย์สิน) เป็นสิ่งที่มีความจำเป็นสำหรับการดูแล และควบคุมการเข้าถึงข้อมูลที่มีชั้นความลับ

3.1.4.4 Human Resource Security-A8 (การรักษาความปลอดภัยในระดับบุคลากร) โดยมีจุดมุ่งหมายดังนี้

(1) เพื่อลดความเสี่ยงที่อาจเกิดเนื่องจากความผิดพลาดของคน การขโมย การฉ้อโกง หรือหลอกลวง และการใช้งานระบบในทางที่ผิด

(2) เพื่อทำให้มั่นใจว่า ผู้ใช้มีความระมัดระวังเกี่ยวกับภัยคุกคามต่อการรักษาความปลอดภัยของข้อมูลและมีระบบป้องกัน และรองรับนโยบายทางด้านการรักษาความปลอดภัยในการปฏิบัติงานปกติของพนักงาน

(3) ลดความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์ การทำงานที่ผิดพลาดของระบบ และเรียนรู้จากบทเรียนต่างๆ

3.1.4.5 Physical and Environmental Security–A9 (การรักษาความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม) มีจุดมุ่งหมายเพื่อ

(1) ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อจะทำลายหรือขัดขวางการดำเนินธุรกิจขององค์กร

(2) ป้องกันการสูญเสีย และการขัดขวางการดำเนินธุรกิจขององค์กร

(3) ป้องกันการขโมยข้อมูล และการใช้ทรัพยากรขององค์กร

3.1.4.6 Communications and Operations Management-A10 (การสื่อสารและการบริหารการปฏิบัติงาน) มีจุดมุ่งหมายดังนี้

(1) เพื่อทำให้แน่ใจว่าระบบจัดการข้อมูลนั้นทำงานอย่างถูกต้องและปลอดภัย

(2) ลดความเสี่ยงในการที่ระบบล่ม

(3) รักษาความคงสภาพ และมั่นคงของซอฟต์แวร์และข้อมูล

(4) เพื่อรักษาความคงสภาพ และความพร้อมใช้งานของระบบสื่อสารข้อมูล และระบบจัดการข้อมูล

(5) เพื่อป้องกันและรักษาความปลอดภัยข้อมูลบนเครือข่าย และการป้องกันโครงสร้างของระบบ

(6) ป้องกันการสูญเสียต่อทรัพย์สิน และการขัดขวางต่อการดำเนินธุรกิจ

(7) ป้องกันการสูญเสีย การดัดแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดเมื่อต้องมีการแลกเปลี่ยนข้อมูลระหว่างองค์กร

3.1.4.7 Access Cotrol-A11 (การควบคุมการเข้าถึงระบบ) มีจุดมุ่งหมายเพื่อการควบคุมการเข้าถึงข้อมูล

(1) ป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

(2) ป้องกันการให้บริการทางเครือข่าย

(3) ป้องกันการเข้าใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต

(4) ตรวจจับเหตุการณ์ที่ผิดหรือไม่ได้รับอนุญาตมีระบบรักษาความปลอดภัยเมื่อมีการใช้งานอุปกรณ์เคลื่อนที่ และการใช้งานการสื่อสารทางด้านโทรคมนาคม

3.1.4.8 Information systems acquisition, development and maintenance-A12 (การดูแลและพัฒนาระบบ) มีวัตถุประสงค์ดังนี้

(1) เพื่อให้แน่ใจว่าระบบที่พัฒนาหรือสร้างนั้นมีความปลอดภัยเพียงพอสำหรับการใช้งานจริง

(2) ป้องกันการสูญเสีย หรือมีการเปลี่ยนแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดในแอพพลิเคชัน

(3) ป้องกันความลับ การพิสูจน์ทราบตัวตน และความคงสภาพของข้อมูล

(4) ทำให้แน่ใจว่าโครงการต่างๆนั้นให้ความสำคัญกับการรักษาความปลอดภัย

(5) ดูแลรักษาความปลอดภัยของแอพพลิเคชันและข้อมูล

3.1.4.9 Information security incident management - A13 (การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย) ซึ่งมีมาตรการ 2 ส่วนคือ

(1) การรายงานเหตุการณ์ จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความปลอดภัย

(2) การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย เพื่อให้มีความรวดเร็วและมีประสิทธิภาพ

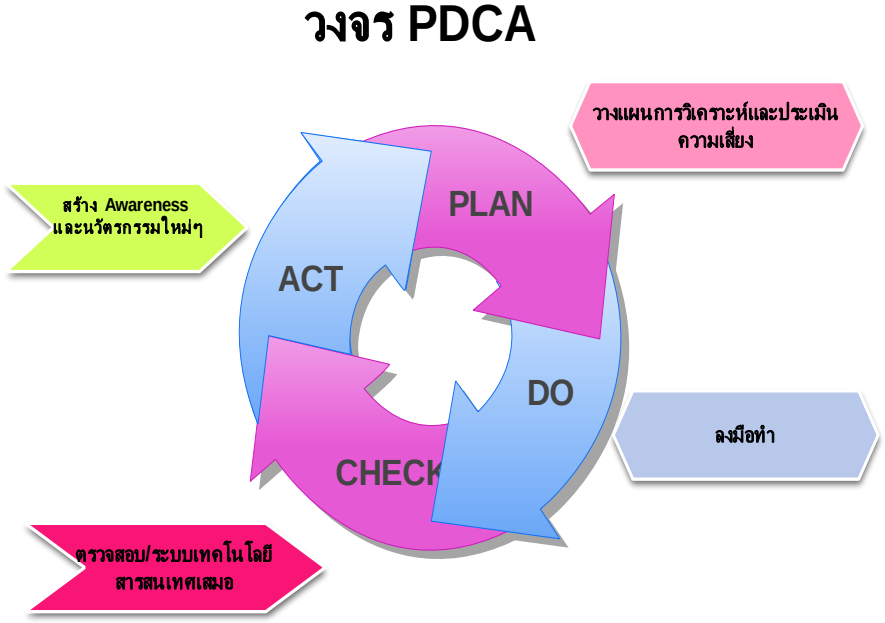
3.1.4.10 Business Continuity Management-A14 (การบริหารความต่อเนื่องของธุรกิจ) เพื่อป้องกันเหตุการณ์ที่จะขัดขวางการดำเนินธุรกิจจากเหตุการณ์ล้มเหลวขนาดใหญ่หรือภัยธรรมชาติ

3.1.4.11 Compliance-A15 (ไม่ขัดต่อกฎหมาย) มีวัตถุประสงค์เพื่อ

(1) ป้องกันการขัดต่อกฎหมายแพ่งและอาญา กฎ ระเบียบ และสัญญาต่างๆ

(2) เพื่อทำให้แน่ใจว่าระบบไม่ขัดต่อนโยบายการรักษาความปลอดภัยขององค์กรหรือมาตรฐานที่เลือกใช้

3.1.5 ศึกษา รูปแบบการดำเนินการแบบ Plan-Do-Check-Act (PDCA) เพิ่มเติมมาตรฐาน ISO/IEC 27001 ซึ่งศึกษามองเห็นว่าเป็นรูปแบบการดำเนินงานที่สำคัญ เพื่อนำมาพัฒนาระบบการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ จึงเป็นแนวทางพื้นฐานเพื่อที่จะสร้างระบบควบคุมเพื่อให้องค์กรให้สามารถบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้และเพื่อให้ระบบต่างๆได้รับการพัฒนาปรับปรุงอย่างต่อเนื่องหรือทบทวน อย่างน้อยปีละ 1 ครั้ง เมื่อถึงเวลา มีรายละเอียดของวงจร PDCA ตามระบบบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 หัวใจหลักของกระบวนการ ซึ่งประกอบด้วย 4 ขั้นตอนหลัก รายละเอียด ดังภาพที่ 3.3



ภาพที่ 3.3 หัวใจหลักกระบวนการ PDCA

ที่มา : บทความ Plan-Do-Check-Act (12)

เมื่อวิเคราะห์และพิจารณาแล้ว หัวใจหลักของ การเพิ่มประสิทธิภาพในการดำเนินงานกิจกรรมใดๆ ต้องมีกระบวนการ PDCA แทรกอยู่เสมอ ได้แก่

1) การวางแผน (Establish the ISMS (เทียบเท่ากับ Plan)) ถ้าหากหน่วยงานยังไม่มีการวางแผนงานสำหรับกิจกรรมใดๆ ที่อาจเกิดขึ้น

2) การดำเนินการตามแผน (Do) Implement and operate the ISMS (เทียบเท่ากับ Do) หมายถึงการดำเนินงานตามแผนที่ได้วางไว้

3) การเฝ้าระวังและติดตามการดำเนินการตามแผน (Monitor and Review the ISMS (เทียบเท่ากับ Check)) มีการตรวจสอบการทำงาน ตรวจสอบแผนงาน

4) การดำเนินการเพิ่มเติมตามสมควร (Maintain and Improve the ISMS (เทียบเท่ากับ Act)) ทบทวน ปรับปรุงงานให้ดีขึ้น แก้ไขให้ตรงตามความต้องการ

อธิบายรายละเอียด แนวทางในการดำเนินการตาม PDCA ได้ ดังนี้

3.1.5.1 การวางแผน (Plan) คือการวางแผนหรือ Plan เป็นการประเมินความเสี่ยงที่มีต่อทรัพย์สินสารสนเทศซึ่งส่วนใหญ่จะหมายถึงทรัพย์สินสารสนเทศใหม่ที่กำลังนำเข้ามาสู่การใช้งานที่จะต้องมีแผนในการประเมินความเสี่ยง เพื่อเตรียมการป้องกันก่อนเริ่มต้นใช้งานทรัพย์สินใหม่

เหล่านั้น เช่น กรณีมีโครงการจัดทำระบบงาน E-Meeting ที่ต้องดำเนินการให้แล้วเสร็จในปีงบประมาณนี้ ทรัพย์สินสารสนเทศใหม่ของโครงการนี้อาจประกอบด้วย

(1) วางแผนในการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยระบบสารสนเทศระบบงาน E-Meeting ฮาร์ดแวร์ของระบบงาน E-Meeting ซอฟต์แวร์ต่างๆ ของระบบงาน E-mail เช่น ระบบปฏิบัติการ Windows ระบบฐานข้อมูล

(2) การกำหนดแนวทางในการประเมินความเสี่ยงสำหรับองค์กรที่เหมาะสมต้องสอดคล้องกับการบริหารความเสี่ยงเชิงกลยุทธ์ขององค์กร กำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยงและได้รับการอนุมัติโดยฝ่ายบริหาร

(3) วางแผนงานเพื่อวิเคราะห์ความเสี่ยง ซึ่งประกอบด้วย การระบุทรัพย์สิน ระบุภัยคุกคามที่มีต่อทรัพย์สิน ระบุผลกระทบ การค้นหาจุดอ่อนการประเมินถึงโอกาสในการเกิดขึ้นของความล้มเหลวที่มี่ต่อความมั่นคงปลอดภัยระบบสารสนเทศ

(4) วางแผนกำหนดแนวทางมาตรการควบคุมสำหรับองค์กรที่เหมาะสม เช่น กำหนดมาตรการควบคุมที่เหมาะสม การยอมรับความเสี่ยงที่เกิดขึ้น การหลีกเลี่ยงความเสี่ยง การโอนย้ายความเสี่ยง

(5) วางแผน การจัดเตรียมเอกสาร มีเอกสารแสดงการประยุกต์ใช้งาน หรือ Statement of Applicability (SOA) โดยเป็นเอกสารที่อธิบายถึงรายการของหัวข้อควบคุม (Control) วัตถุประสงค์การควบคุม (Control objectives) ที่ได้เลือกไว้ และเหตุผลของการเลือก รวมถึงหัวข้อควบคุมและวัตถุประสงค์ควบคุมที่มีอยู่ วางแผน Base line control ในกรณีที่หัวข้อการควบคุมอะไร

3.1.5.2 การลงมือทำ (DO) คือการดำเนินการตามแผนที่วางไว้ DO ในขั้นตอนของการลงมือทำจะประกอบด้วย

(1) จัดทำแผนเกี่ยวกับความมั่นคงปลอดภัยระบบสารสนเทศ เช่น วางแผนกำหนดผู้รับผิดชอบทรัพยากร

(2) จัดลำดับความสำคัญในการดำเนินงาน สำหรับการจัดการกับความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศการจัดฝึกอบรมและการสร้างการรับรู้ขึ้นภายในองค์กร

(3) ดำเนินการตามมาตรการควบคุมที่กำหนดไว้เพื่อให้ได้ตามวัตถุประสงค์ของการควบคุมการบริหารงาน ISMSการจัดการทรัพยากรสำหรับ ISMS(4)การดำเนินงานตามวิธีการปฏิบัติงาน และการควบคุมอื่นๆ เพื่อให้สามารถตรวจสอบเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยและการตอบสนองต่อเหตุการณ์นั้นๆ

3.1.5.3 การตรวจสอบ (Check) องค์กรจะต้องมีการดำเนินการต่างๆ ประกอบด้วย

(1) การดำเนินการเฝ้าติดตาม และทบทวนวิธีการปฏิบัติงาน และการควบคุมต่างๆ ระบุถึงการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ต่างๆ ที่เกิดขึ้น ช่วยให้ฝ่ายบริหารสามารถระบุถึงการดำเนินการความมั่นคงที่ได้มอบหมายให้บุคลากรต่างๆ เป็นไปตามที่คาดหมายไว้ ช่วยในการตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยโดยการใช้ดัชนีวัดที่เหมาะสม โดยพิจารณาถึงความมีประสิทธิผลในการดาเนินการเพื่อแก้ไขการละเมิดความมั่นคงปลอดภัย

(2) การดำเนินการทบทวนความมีประสิทธิผลของ ISMS อย่างสม่าเสมอ โดยพิจารณาถึงของการตรวจประเมินความมั่นคงปลอดภัย (Audit) เหตุการณ์ที่เกิดขึ้น ผลของการวัดความมีประสิทธิผล ข้อเสนอแนะ และข้อมูลแจ้งกลับจากหน่วยงานต่างๆ ที่เกี่ยวข้อง การวัดความมีประสิทธิผลของการควบคุมเพื่อทวนสอบถึงความสอดคล้องตามข้อกำหนดความมั่นคงปลอดภัย และทบทวนการประเมินความเสี่ยงตามแผนที่ได้กาหนดไว้ รวมถึงทบทวนความเสี่ยงที่เหลืออยู่และระดับของความเสี่ยงที่สามารถยอมรับได้ โดยคำนึงถึงการเปลี่ยนแปลงในองค์กรด้านเทคโนโลยี

(3) การปรับปรุงงานกิจกรรมต่างๆ เกี่ยวกับระบบสารสนเทศและการควบคุมต่าง การดำเนินการทบทวนโดยฝ่ายบริหาร เพื่อดูแลความเพียงพอของขอบเขต และการดำเนินการปรับปรุงกระบวนการ ISMS การปรับปรุงแผนความมั่นคงปลอดภัย โดยคำนึงถึงสิ่งที่พบจากการเฝ้าติดตามการทบทวน การบันทึกผลการดำเนินการ และเหตุการณ์ที่อาจส่งผลต่อความมีประสิทธิผลหรือผลการดำเนินงานของ ISMS

(4) การตรวจสอบ ดูแลว่าการปรับปรุงเป็นไปตาม วัตถุประสงค์ที่วางไว้ คู่มือการปฏิบัติงานเป็นปัจจุบัน มีการทบทวนตรวจสอบความครบถ้วนสมบูรณ์ของกระบวนการที่อาจส่งผลต่อความมีประสิทธิผล หรือผลการดำเนินงานของ ISMS

3.1.5.4 การปรับปรุงแก้ไข (Act) ในขั้นตอนการของการปรับปรุงและแก้ไขระบบต่างๆ อาจจะประกอบด้วย

(1) การดำเนินการปรับปรุง ISMS ตามที่กำหนดไว้ ปรับปรุงเอกสารให้ถูกต้องการปฏิบัติการแก้ไขและการป้องกันอย่างเหมาะสม รวมถึงการนำบทเรียนจากประสบการณ์ความมั่นคงปลอดภัยขององค์กรอื่นๆ ขององค์กรมาปรับใช้ให้เหมาะสม

(2) การสื่อสารการปรับปรุง ISMS ตามที่กำหนดไว้ การสื่อสารแนวปฏิบัติการที่แก้ไขและการปรับปรุงไปยังหน่วยงานต่างๆ ที่เกี่ยวข้องทั้งหมด การสื่อสารแผนบริหารความเสี่ยงให้เข้าใจทั่วทั้งองค์กรรวมทั้งการจัดทำรายงานต่างๆ นำเสนอผู้บริหาร

3.2 แหล่งที่มาและวิธีการเก็บรวบรวมข้อมูล

3.2.1 ศึกษาจากเอกสาร (Document) ต้องศึกษา จากเอกสารต่างๆที่เกี่ยวข้องทั้งแนวคิดและทฤษฎีที่เกี่ยวข้อง ได้แก่ ศึกษามาตรฐาน ISO/IEC 27001 ศึกษาสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศขององค์กรพร้อมทำความเข้าใจเพื่อใช้เป็นข้อเพื่อประกอบการวิเคราะห์ เช่น ศึกษาจากขั้นตอนการทำงานและกระบวนการทำงาน ศึกษาขั้นตอนการปฏิบัติงานเป็นหลัก ศึกษาจากเอกสารจากงานวิจัยที่เกี่ยวข้อง บทความด้านความปลอดภัยสารสนเทศจากแหล่งข้อมูลต่างๆ เพื่อนำมาใช้เป็นแนวทางในการวิเคราะห์ผลการจัดทำโครงงาน

3.2.2 สังเกต (Observation) ทำให้เกิดความเข้าใจในการศึกษา วิเคราะห์ระบบสารสนเทศของหน่วยงาน สังเกตการปฏิบัตงานเชิงนโยบาย ลักษณะการบริหารงาน เทคนิคกลยุทธ์เพื่อสร้างให้เกิดจินตนาการในการวิเคราะห์ระบบและนำข้อมูลพื้นฐานไปประเมินและวิเคราะห์ความเสี่ยงต่อไป

3.2.3 การประชุม/สัมมนา เพื่อเก็บรวบรวม รายละเอียดของข้อมูลที่จะศึกษา การบริหารความเสี่ยงของโครงการเพื่อรวบรวมข้อมูลพื้นฐานในการจัดทำโครงการด้าน ICT นำมาศึกษาแนวคิดของเจ้าหน้าที่ทั้งระดับบริหาร และระดับปฏิบัติงานของหน่วยงาน

3.2.4 การสัมภาษณ์ (Interview) ผู้ที่มีส่วนเกี่ยวข้อง ได้แก่ ระดับผู้บริหารของหน่วยงานเจ้าหน้าที่ที่ปฏิบัติงาน ตลอดจนถึงผู้รับบริการ เพื่อค้นหาทิศทาง วิสัยทัศน์ พันธกิจในการตอบสนองวัตถุประสงค์ขององค์กร นำมาเลือกใช้เทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือสนับสนุนการทำงานให้เหมาะสมและสอดคล้องกับภารกิจหลักขององค์กร รวมทั้งกำหนดขอบเขตในการดำเนินงานด้าน ICT การแก้ปัญหาในปัจจุบันและวางแผนในอนาคต

3.3 ศึกษาวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและภัยคุกคาม

3.3.1 จุดแข็งขององค์กร

1. เป็นองค์กรภาครัฐที่ให้การบริการประชาชนทั่วประเทศในการคุ้มครองผู้บริโภค
2. การให้บริการอย่างทั่วถึงของพื้นที่ที่รับผิดชอบ มีประสิทธิภาพและคุณภาพ
3. มีการขยายตัวขององค์กรเพื่อรองรับการก้าวสู่ประชาคมอาเซียน

3.3.2 จุดอ่อนขององค์กร

1. วัฒนธรรมองค์กรแบบเฉพาะที่เปลี่ยนแปลงได้ยากในการประสานงาน
2. บุคลากรและเจ้าหน้าที่ยังขาดความรู้ความเข้าใจด้าน ICT ในการถ่ายทอดความรู้และประสบการณ์หรือไม่ได้รับการฝึกอบรม
3. ระบบเทคโนโลยีสารสนเทศ ถือเป็นโครงสร้างพื้นฐานรองรับที่สาคัญ แต่ยังไม่ได้รับการสนับสนุนและขาดการพัฒนาอย่างต่อเนื่องยังมีช่องโหว่ของระบบเทคโนโลยีสารสนเทศและ

มีความเสี่ยงต่อการล้มเหลวของระบบทาให้การปฏิบัติงานเกิดความขัดข้อง เช่น ระบบรักษาความมั่นคงปลอดภัยที่ต้องได้มาตรฐานเป็นที่เชื่อถือได้

3.3.3 โอกาสขององค์กร

1. รัฐบาลมีนโยบายชัดเจน ด้านการคุ้มครองผู้บริโภคในประเทศไทยและอาเซียน โดยเฉพาะด้านเทคโนโลยีสารสนเทศ

2. มีโอกาสพัฒนาระบบสารสนเทศให้สามารถรองรับความต้องการใช้บริการได้อย่างพอเพียงและมีประสิทธิภาพ

3. องค์กรมีบทบาทในด้านความก้าวหน้าทางเทคโนโลยีเพื่อรองรับการคุ้มครองผู้บริโภคก้าวสู่อาเซียน

4. การวิจัยพัฒนาเกี่ยวกับการคุ้มครองผู้บริโภคด้วยประสบการณ์ที่ยาวนาน

3.3.4 ภัยคุกคามขององค์กร

1. ภัยคุกคามต่อระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในระบบเครือข่ายสื่อสารคอมพิวเตอร์ และระบบปัจจุบันอาจทำให้ระบบชะงัก หรืออาจถูกขโมยข้อมูลได้

2. การเปลี่ยนแปลงทางการเมืองบ่อยๆ ทำให้ขาดความต่อเนื่องในการทำงานต้องมาเริ่มต้นใหม่จึงทำให้พัฒนาได้ช้า

3.4 อุปกรณ์และเครื่องมือที่ใช้ในการศึกษาวิจัย

3.4.1 เครื่องมือที่ใช้ในการศึกษาวิจัย ได้แก่ มาตรฐานสากล ISO/IEC 27001 PDCA Model การบริหารความเสี่ยง (Risk Management)

3.4.2 เครื่องมือที่ใช้ในการตรวจสอบ (Tools) การเก็บข้อมูลของปัญหา โดยเครื่องมือการตรวจสอบช่องโหว่ และเอกสาร Checklist เพื่อให้ทราบถึงสภาพโครงสร้างระบบเครือข่ายภายในองค์กรที่ใช้เป็นกรณีศึกษา และสามารถทราบถึงปัญหาที่ตรวจพบในระบบเทคโนโลยีสารสนเทศเพื่อหาแนวทางป้องกันมีดังนี้

3.4.2.1 Super Scan โปรแกรมสแกนพอร์ตแบบฟรีแวร์ (Freeware) เป็นโปรแกรม Super Scan ที่มีชื่อเสียงและจุดเด่นในด้านการสแกนพอร์ตได้อย่าง รวดเร็วและมีประสิทธิภาพ

3.4.2.2 Nmap (Network Mapping) เป็นโปรแกรม Open source ที่ใช้สแกนเครือข่ายและตรวจสอบความปลอดภัยซึ่ง Nmap สามารถทำการสแกนเครือข่ายขนาดใหญ่ได้อย่างรวดเร็วโดยการสแกนไอพีแอดเดรส เพื่อที่จะรายงาน Port Application OS และ Firewall ในปัจจุบัน Nmap มีการประมวลผลได้กับระบบปฏิบัติการ(OS) ทุกประเภท สามารถเลือกใช้งานได้ทั้งแบบผ่าน Command และแบบ Graphic GUI ซึ่งไม่จำเป็นต้องจำคำสั่งต่างๆ

3.4.2.3 เป็นเครื่องมือสำหรับการตรวจสอบการบุกรุกซึ่งใช้สำหรับการสแกนช่องโหว่ Nessus สามารถแสดงรายงานออกมาว่าแต่ละเครื่องมี ช่องโหว่อะไรบาง ระดับความเสี่ยงที่จะถูกโจมตีมี มาก-น้อย แค่ไหน วิธีป้องกันทำได้อย่างไรบ้าง

3.4.2.4 SQL Scan เป็นเครื่องมือสำหรับทำการตรวจสอบว่าเครื่องไหนบ้างภายในเครือข่ายได้ติดตั้ง โปรแกรม Microsoft Sql Server

3.4.2.5 SQL Dict เป็นเครื่องมือสำหรับถอดรหัส Microsoft Sql Server โดยเทียบจากคำศัพท์ จากไฟล์ดิกชั่นนารี

3.4.2.6 Pwdump3v2 เป็นเครื่องมือสำหรับดัมพ์เอารหัสผ่านจาก Registry ของเครื่องเหยื่อออกมาเป็นไฟล Text

3.5 วิธีการวิเคราะห์และประเมินความเสี่ยง

หลังจากผ่านกระบวนการศึกษา รวบรวมข้อมูล และมีการจัดเตรียมข้อมูล วางแผนงาน ทำความเข้าใจศึกษาข้อกำหนดในมาตรฐานที่เลือกใช้ทำการเปรียบเทียบข้อมูลพื้นฐานต่างๆ การระบุทรัพย์สิน การประเมินความเสี่ยงของทำการพัฒนานโยบายสารสนเทศแต่ละหัวข้อด้วยขั้นตอนดังต่อไปนี้

3.5.1 นำข้อมูลพื้นฐานมาจัดลำดับความสำคัญ เพื่อกำหนดลำดับในการจัดกลุ่มทรัพย์สินของระบบสารสนเทศ โดยจัดทำตารางการให้คะแนนอัตราความเสียหายที่จะเกิดขึ้นกับข้อมูล โดยแยกเป็นอัตราความเสี่ยงที่มีต่อการรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมให้บริการ (Availability) นำคะแนนต่างๆ ที่ได้จากการประเมินความเสี่ยงมารวมกันแล้วนำคะแนนมาวิเคราะห์และจัดลำดับความเสี่ยง

3.5.2 ศึกษาข้อกำหนดและวิธีการโดยละเอียด โดยใช้ข้อมูลจากเอกสาร ISO/IEC 27001 เพื่อระบุว่าจะต้องบรรจุ หัวข้ออะไรบ้างลงในการวิเคราะห์และประเมินความเสี่ยง

3.5.3 ระบุทรัพย์สิน นำข้อมูลที่ได้จาก การรวบรวม สัมภาษณ์ มาจัดกลุ่มแยกประเภทเพื่อวิเคราะห์ ตรวจสอบหาจุดอ่อน จุดแข็งและ ช่องโหว่

3.5.4 แยกการวิเคราะห์ออกเป็นหัวข้อย่อย ตามมาตรฐาน ISO ทั้ง 11 Domain ซึ่งในแต่ละกระบวนการอาจแยกได้มากกว่า 1 หัวข้อ ขึ้นอยู่กับความต้องการในการแบ่งแยกชนิดของการควบคุม เช่น กระบวนการสร้างความปลอดภัยให้กับระบบสารสนเทศ อาจแยกออกเป็นการควบคุมการเข้าถึงข้อมูล นโยบายด้านความปลอดภัยของเซิร์ฟเวอร์(server) เป็นต้น ข้อมูลในแต่ละตารางประกอบไปด้วย หมายเลขนโยบาย ชื่อนโยบาย วัตถุประสงค์ หลักการและเหตุผล หน้าที่รับผิดชอบ รายละเอียดของนโยบายความปลอดภัย

3.5.5 เพิ่มขั้นตอนของวิธีการของ PDCA เพื่อให้ครอบคลุมข้อกำหนดตามกระบวนการของมาตรฐาน ISO/IEC 27001

3.5.6 นำผลการวิเคราะห์และการประเมินความเสี่ยงที่พัฒนาเสร็จแล้วแต่ละกระบวนการปรึกษากับอาจารย์ที่ปรึกษา เพื่อทำการตรวจสอบและแก้ไขและปรับปรุงเพิ่มเติมความครบถ้วนให้มีความสมบูรณ์ยิ่งขึ้น

3.5.7 ทำตามขั้นตอนตั้งแต่ข้อ 3 จนถึงข้อ 7 เรียงตามลำดับจนครบทุกกระบวนการ

3.5.8 จัดทำผลสรุป เพื่อรวบรวม วางแผน จัดทำแผนงานพัฒนา ICT แผนแม่บทเทคโนโลยีสารสนเทศ ฉบับที่ 2 ปี 2557-2560 ส่งรายงานสรุปต่อให้ผู้บริหารองค์กรพิจารณา

3.6 ระยะเวลาในการดำเนินการศึกษาวิจัย

ระยะเวลาในการดำเนินการวิจัยตั้งแต่ ตุลาคม 2555 – มิถุนายน 2556 เพื่อการศึกษาวิเคราะห์วางแผนการดำเนินงานตามตารางข้างล่างนี้

ตารางที่ 3.1 ระยะเวลาในการดำเนินงานศึกษาวิจัย

ระยะเวลาดำเนินงาน (เม.ย.- กันยายน)	ต.ค	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.
1. ศึกษา รวบรวมข้อมูลที่เกี่ยวข้องระบบสารสนเทศภายในองค์กร									
2. จัดหมวดหมู่ของทรัพย์สินสารสนเทศ									
3. วิเคราะห์ประเมินความเสี่ยงทางระบบสารสนเทศ									
4. กำหนดมาตรการป้องกันและวิเคราะห์									
5. สรุปผลการ วิจัยและข้อเสนอแนะ									
6. เรียบเรียงงานค้นคว้าอิสระให้สมบูรณ์/เสนอจบ									

3.7 ขั้นตอนวิธีการดำเนินการศึกษาและวิเคราะห์ความเสี่ยง

จากวิธีการและการออกแบบขั้นตอนการทำงานในภาพรวม สามารถกำหนดข้อมูลที่ใช้ในการวิเคราะห์และประเมินความเสี่ยง ซึ่งมีขั้นตอนการดำเนินงาน(รายละเอียดในบทที่4) มีดังต่อไปนี้

1. รวบรวม ศึกษาข้อมูลและระบบสารสนเทศภายในองค์กรทั้งหมด
2. จัดหมวดหมู่ แยกประเภทสารสนเทศแยกตามประเภทระบบงาน
3. วิเคราะห์องค์กร จุดแข็ง จุดอ่อน โอกาสและภัยคุกคามขององค์กร
4. วิเคราะห์การใช้งานระบบสารสนเทศและอุปกรณ์ในปัจจุบัน
5. ประเมินความเสี่ยงและผลกระทบต่อองค์กร
6. กำหนดมาตรการป้องกันที่สามารถจัดการได้ ในด้านความปลอดภัยขององค์กร
7. สรุปผลการวิเคราะห์และประเมินความเสี่ยง
8. แนวทางในการนำไปใช้การวิจัยและข้อเสนอแนะ