บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ความเจริญก้าวหน้าด้านเทคโนโลยีและการสื่อสารอย่างไร้พรหมแดนยุคโลกาภิวัตน์ทำให้มีนวัตกรรมใหม่ๆ เกิดขึ้น เพื่อนำมาใช้สนับสนุนการทำงานตามภารกิจหลักของหน่วยงานต่างๆ หรือตอบสนองธุรกิจทั้งภาครัฐและเอกชน ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่หน่วยงานต้องตระหนักถึงความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ทั้งภาครัฐและเอกชน จึงมีแนวคิดในการบริหารจัดการด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงาน ความเจริญก้าวหน้าทางเทคโนโลยีใหม่ๆ ก็จะมีความเสี่ยงในการถูกบุกรุกจากผู้ไม่ประสงค์ดีด้วยวิธีการใหม่ ๆ มากยิ่งขึ้น

จากปัญหาที่เกิดขึ้น คือระบบเว็บไซต์ของหน่วยงาน ถูกโจมตีและบุกรุกจากบุคคลภายนอกโดยไม่ได้รับอนุญาตแสดงให้เห็นว่าระบบเทคโนโลยีสารสนเทศของหน่วยงานยังมีจุดอ่อนอยู่ ซึ่งเป็นสาเหตุของปัญหาอย่างหนึ่ง ในหลายๆข้อจำกัด ทำให้ผู้จัดทำโครงการเกิดแนวคิดเพื่อที่จะศึกษา วิเคราะห์ ปัญหาดังกล่าวที่เกิดขึ้น จึงเป็นความตั้งใจของผู้วิจัยที่จะศึกษาวิเคราะห์และประเมินความเสี่ยงระบบสารสนเทศขององค์กร เพื่อค้นหาจุดอ่อนและช่องโหว่ของระบบสารสนเทศภายในองค์กร โดยใช้มาตรฐานสากล ISO/IEC 27001 เพื่อนำไปใช้ในองค์กรและนำไปสู่การวางแผนดำเนินงาน แผนรับมือกับความเสี่ยงที่เกิดขึ้นและแผนการกรณีฉุกเฉิน นำไปสู่การดำเนินงานและการบริหารจัดการศูนย์เทคโนโลยีสารสนเทศ

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อตรวจสอบภัยคุกคามและช่องโหว่ของระบบสารสนเทศที่อาจเกิดความเสี่ยงต่อองค์กรได้ด้วยมาตรฐานสากล ISO/IEC 27001

2. เพื่อทบทวนและกำหนดแนวทางแก้ไขเบื้องต้นด้านความปลอดภัยของระบบสารสนเทศและหาแนวทางป้องกันได้อย่างมีระบบและมีประสิทธิภาพ

3. เพื่อนำไปพัฒนาปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

4. นำผลการวิเคราะห์และประเมินความเสี่ยงมาประยุกต์ใช้งานด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนภารกิจหลักขององค์กร

1.3 ขอบเขตของการศึกษาวิจัย

ขอบเขตของการศึกษาวิจัย มีดังต่อไปนี้

1. ศึกษา วิเคราะห์และการจัดการความเสี่ยงสำหรับระบบสารสนเทศในองค์กรด้วยมาตรฐานสากล ISO/IEC 270001 โดยใช้มาตรการป้องกันตามแนวทางของมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2)ประจำปี 2550 เป็นแนวทางเปรียบเทียบ เพื่อหาถึงภัยคุกคามหรือปัญหาและจุดอ่อน ที่เกิดขึ้นและจัดทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. จัดทำกระบวนการจัดการประเมินความเสี่ยงตามมาตรฐานสากล

3. วิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในด้านต่างๆ เช่น

1) ด้านระบบโปรแกรมประยุกต์(Application)

2) ด้านระบบเครือข่าย (Network)

3) ด้านสถาปัตยกรรมของระบบ

4. นำผลการวิเคราะห์และประเมินความเสี่ยงไปพัฒนาและปรับปรุงการจัดทำนโยบายความมั่นคงปลอดภัย เพื่อใช้เป็นแนวทางของเจ้าหน้าที่ใช้งานในระบบงานเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย โดยจะมีนโยบายที่มีไว้ให้ปฏิบัติตามดังต่อไปนี้

1) ด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

2) ด้านระบบการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์

3) ด้านระบบการรักษาความมั่นคงปลอดภัยระบบปฏิบัติการคอมพิวเตอร์

4) ด้านระบบการรักษาความมั่นคงปลอดภัยของข้อมูลระบบเครือข่าย

5) ด้านการเข้าถึงระบบงาน สิทธิการเข้าถึงข้อมูลต่างๆ

5. นำเสนอแผนการประเมินความเสี่ยงต่อผู้บริหารขององค์กร เพื่อให้เห็นความสำคัญของความปลอดภัยของระบบสารสนเทศพื้นฐานที่จำเป็น ดังนี้

1) ประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่ใช้ในปัจจุบันโดยอ้างอิงเกณฑ์จาก ISO27001/17799 (Risk Assessment)

2) ทบทวนนโยบายโดยยึดเป้าหมายและจุดประสงค์ ตามแนวทางของหน่วยงานโดยนำข้อกำหนดในมาตรฐาน ISO27001/17799 ซึ่งเป็นมาตรฐานมาปรับใช้เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลระบบสารสนเทศ

1.4 ปัญหาและอุปสรรค

จากปัญหาที่เกิดขึ้นและมีผลกระทบต่อหน่วยงานคือระบบเว็บไซต์ของหน่วยงานถูกโจมตีและถูกบุกรุกจากบุคคลภายนอกโดยไม่ได้รับอนุญาตมีการเข้าถึงข้อมูลของระบบโดยผู้ไม่มีสิทธิ์ แสดงให้เห็นว่าระบบสารสนเทศของหน่วยงานยังมีจุดอ่อน/ช่องโหว่ จึงจำเป็นต้องศึกษาวิเคราะห์ถึงปัญหาดังกล่าวและกำหนดแนวทางในการแก้ไขปัญหา ทั้งนี้หน่วยงานไม่มีงบประมาณในด้านการบริหารจัดการระบบความปลอดภัยระบบเทคโนโลยีสารสนเทศสนับสนุน

1.5 กรณีศึกษา

งานค้นคว้าอิสระเล่มนี้ กรณีศึกษาศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค ซึ่งปัจจุบันได้นำระบบเทคโนโลยีสารสนเทศมาใช้งานเพื่อสนับสนุนภารกิจหลัก ผู้ศึกษาวิจัย เป็นผู้กำกับ ดูแลและบริหารงานด้านเทคโนโลยีสารสนเทศ โดยตรงในตำแหน่งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ซึ่งมีความต้องการเผยแพร่แนวคิด และวิธีการนำไปประยุกต์ใช้งานในหน่วยงานภาครัฐอื่นๆ เพื่อให้มีการนำเทคนิคการวิเคราะห์และประเมินความเสี่ยงไปใช้การวางแผนด้านเทคโนโลยีสารสนเทศ ให้เกิดประสิทธิภาพสูงในเรื่องความเชื่อถือได้ (Reliability) ความมั่นคงปลอดภัย (Security) และคุณภาพ (Quality) รวมทั้งสนับสนุนระบบเพิ่มเติมในอนาคต

สำหรับการวิเคราะห์ SWOT ขององค์กรในจุดแข็ง (Strength) จุดอ่อน (Weakness) โอกาส (Opportunity) และภัยคุกคาม(Threat) จากปัจจัยต่างๆ ซึ่งไม่เป็นเพียงแต่ในด้านความมั่นคงปลอดภัยด้านสารสนเทศเท่านั้นแต่เป็นในภาพรวมขององค์กร ซึ่งมีผลต่อความมั่นคงปลอดภัยสารสนเทศของทั้งระบบ ดังรายละเอียดต่อไปนี้

1. จุดแข็งขององค์กร

1.1 เป็นองค์กรภาครัฐที่ให้การบริการประชาชนทั่วประเทศในการคุ้มครองผู้บริโภค

1.2 กำลังมีการขยายตัวขององค์กร เพื่อรองรับการก้าวสู่ประชาคมอาเซียน

2. จุดอ่อนขององค์กร

2.1 วัฒนธรรมองค์กรแบบเฉพาะที่เปลี่ยนแปลงได้ยาก การประสานงานในแต่ละฝ่ายจึงไม่ง่ายนัก

2.2 บุคลากรและเจ้าหน้าที่ยังขาดความเข้าใจด้าน ICT ในการถ่ายทอดความรู้และประสบการณ์

2.3 ระบบเทคโนโลยีสารสนเทศ ถือเป็นโครงสร้างพื้นฐานรองรับที่สำคัญแต่ขาดการพัฒนาอย่างต่อเนื่องยังมีช่องโหว่ของระบบเทคโนโลยีสารสนเทศ และมีความเสี่ยงต่อการล้มเหลวของระบบทำให้การปฏิบัติงานเกิดความขัดข้อง เช่น ความมั่นคงปลอดภัยของระบบต้องได้มาตรฐานเป็นที่เชื่อถือได้

3. โอกาสขององค์กร

3.1 รัฐบาลมีนโยบายชัดเจนด้านการคุ้มครองผู้บริโภคในประเทศไทยและประเทศในกลุ่มอาเซียนและสากล

3.2 มีโอกาสพัฒนาระบบสารสนเทศให้สามารถรองรับความต้องการใช้บริการได้อย่างพอเพียงและมีประสิทธิภาพ

3.3 องค์กรมีบทบาทในด้านความก้าวหน้าทางเทคโนโลยีสารสนเทศ

3.4 การวิจัยพัฒนาเกี่ยวกับการคุ้มครองผู้บริโภคด้วยประสบการณ์ที่ยาวนาน

4. ภัยคุกคามขององค์กร

4.1 ภัยคุกคามต่อระบบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศในระบบเครือข่ายสื่อสารคอมพิวเตอร์และระบบปัจจุบันอาจทำให้ระบบชะงัก หรืออาจถูกขโมยข้อมูลได้

4.2 การเปลี่ยนแปลงทางการเมืองบ่อยๆ ทำให้ขาดความต่อเนื่องในการทำงาน ต้องมาเริ่มต้นใหม่จึงทำให้พัฒนาได้ช้า

1.6 แนวทางการแก้ปัญหา

แนวทางการแก้ปัญหา เพื่อการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ เป็นการเตรียมพร้อมรับมือกับความเสี่ยง หรือความเสียหายให้แก่ ระบบสารสนเทศขององค์กรโดยไม่คาดคิด เพื่อลดความเสียหายให้ลดน้อยลงที่สุด โดยการวางแผนดำเนินงานมีขั้นตอนดังต่อไปนี้

1. วิเคราะห์มาตรฐานด้านความมั่นคงปลอดภัยและนโยบายที่เหมาะสมกับองค์กร การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อเป็นกรอบการรักษาความมั่นคงปลอดภัยและเป็นแนวทางปฏิบัติสาหรับบุคลากรทุกภาคส่วนในองค์กร โดยครอบคลุมทุกกระบวนงานที่เกี่ยวเนื่องกับระบบเทคโนโลยีสารสนเทศ

2. ศึกษาโครงสร้างขององค์กร ศึกษาการดำเนินงานและประสานงานของฝ่ายเทคโนโลยีสารสนเทศ โดยศึกษาในแต่ละเรื่องเพื่อการวางแผนรองรับเหตุการณ์ฉุกเฉินในปัจจุบัน หากเกิดปัญหาขึ้นจะกระทบกับฝ่ายอื่นหรือไม่

3. วางแผนรองรับสถานการณ์ฉุกเฉินที่เหมาะสม หากมีปัญหาที่อาจเกิดขึ้นและมีผลกระทบทางด้านธุรกิจ ถ้าระบบล้มเหลว ควรนำแผนรองรับสถานการณ์ฉุกเฉินมาใช้ทันที เช่น Incident Response Planning,Disaster Recovery Planning Business Continuity Planning ให้เหมาะสมกับสถานะการณ์ฉุกเฉินนั้นๆ ได้อย่างทันท่วงที

4. ทดสอบ และวิเคราะห์ปัญหา รวมถึงการปรับปรุงการฝึกอบรม การทดสอบแผนงานจะช่วยให้ทราบถึงข้อบกพร่องของการวางแผน ส่วนการฝึกอบรมก็เป็นการเตรียมความพร้อมให้พนักงานดำเนินงานได้อย่างคล่องตัว ส่งผลให้การนำแผนงานไปใช้อย่างมีประสิทธิผล

5. บำรุงรักษาแผนงานทบทวนและปรับปรุงข้อมูลแผนงานให้เป็นปัจจุบัน โดยประสานงานกับหน่วยงานภายในและหน่วยงานภายนอกที่เกี่ยวข้อง เพื่อควบคุมการเผยแพร่เอกสารแผนงานและควบคุมการเปลี่ยนแปลงแผนงาน ซึ่งในแต่ละหัวข้อมีรายละเอียดที่มีความเกี่ยวเนื่องกันเพื่อผลสัมฤทธิในการจัดทำแผนเพื่อให้เกิดประสิทธิภาพและประสิทธิผล

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1. ผู้บริหารสามารถใช้เป็นข้อมูลในการวิเคราะห์และตัดสินใจและประเมินความเสี่ยงขององค์กรเพื่อบริหารจัดการและการวางแผนรับมือกับความเสี่ยงที่เกิดขึ้น

2. ลดความเสี่ยงที่อาจเกิดขึ้นและมีผลต่อระบบเทคโนโลยีสารสนเทศที่ใช้งานภายในองค์กร สร้างความคล่องตัวในการให้บริการแก่ประชาชน

3. นำผลการวิเคราะห์และประเมินความเสี่ยงมาประยุกต์ใช้งานด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนภารกิจหลักขององค์กรในอนาคต

4. สร้างความเชื่อมั่นให้แก่ประชาชนผู้ใช้บริการและเพิ่มประสิทธิภาพในการใช้บริการให้แก่ประชาชนในภาพรวมมากยิ่งขึ้น

5. สร้างความน่าเชื่อถือให้องค์กรที่มีการป้องกันความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่อาจก่อให้เกิดผลกระทบกับการดำเนินงานในองค์กร