บทที่ 6
บทสรุปและข้อเสนอแนะ

6.1 ผลการวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศ

ตามที่ผู้จัดทำโครงงานได้ดำเนินการศึกษาวิเคราะห์และประเมินความเสี่ยงการจัดการด้านความปลอดภัยของระบบสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001:2005 ซึ่งเป็นการเพิ่มประสิทธิภาพในการบริหารจัดการศูนย์คอมพิวเตอร์และข้อมูลภายในองค์กร เพื่อสร้างมาตรฐานความปลอดภัยของระบบสารสนเทศและแก้ไขช่องโหว่/จุดอ่อนที่มีอยู่ พร้อมทั้งปรับปรุงระบบเดิมให้ดียิ่งขึ้น โดยสรุปผลการดำเนินงานได้ดังนี้

6.1.1 ทำให้ได้รับทราบ จุดอ่อนหรือช่องโหว่ ที่อาจทำให้เกิดความเสี่ยงต่อองค์กร และสามารถหาวิธีการแก้ปัญหาได้อย่างเหมาะสม

6.1.2 นำมาพัฒนาปรับปรุงการจัดทำนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งในขณะนี้ได้ดำเนินการจัดทำร่างนโยบายเรียบร้อยแล้ว (ภาคผนวก จ)

6.1.3 นำผลวิเคราะห์และประเมินความเสี่ยง มาประกอบการจัดทำโครงการจัดซื้อจัดจ้างอุปกรณ์ป้องกันการบุกรุกความปลอดภัย เพื่อปรับปรุงระบบเครือข่ายขององค์กร

6.1.4 จากผลการวิเคราะห์ สามารถปิดช่องโหว่ของระบบต่างๆ เช่น การทดสอบการโจมตีทำให้รู้ถึงโครงสร้างหลักการและวิธีการทำงานของการทดสอบโจมตี รวมถึงวิธีการเลือกเป้าหมายและเครื่องมือต่างๆ ที่ใช้ในการทดสอบการโจมตีรวมถึงขั้นตอนการดำเนินงานการปิดช่องโหว่รวมถึงแนวทางในการป้องกัน

6.2 แนวทางการนำไปประยุกต์ใช้ ในการบริหารจัดการศูนย์เทคโนโลยีสารสนเทศ

เมื่อได้นำผลการวิเคราะห์และประเมินความเสี่ยงก่อนและหลัง การดำเนินงานโครงการมาเปรียบเทียบจะผ่านขั้นตอนการวิเคราะห์และการปิดช่องโหว่ของระบบและทบทวนจุดอ่อนด้านความปลอดภัยสารสนเทศที่องค์กรมีอยู่และสามารถดำเนินการปรับปรุงได้ทันทีโดยไม่ต้องใช้งบประมาณ เช่น การปรับค่าการติดตั้งสำหรับค่าของ Operating System ต่างๆ การจัดทำคู่มือเอกสารต่างๆ เพื่อให้ระบบมีความปลอดภัยมากยิ่งขึ้น ซึ่งมีการเปรียบเทียบผลการวิเคราะห์และประเมินความเสี่ยงก่อนและหลังดำเนินโครงการรายละเอียดตามตารางที่ 6.1 ดังนี้

ตารางที่ 6.1 การเปรียบเทียบผลการวิเคราะห์และประเมินความเสี่ยงก่อน-หลังดำเนินโครงการ

Domain	ระดับความเสี่ยงสูง		ระดับความเสี่ยงกลาง		ระดับความเสี่ยงต่ำ	
	ก่อน	หลัง	ก่อน	หลัง	ก่อน	หลัง
1.นโยบายความมั่นคงปลอดภัย (Secur Policy) – A5	2	1	-	-	-	1
2.โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security) – A6	3	1	2	3	-	1
3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) – A7	2	-	4	4	-	2
4.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security) – A8	1	-	7	-	2	-
5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental) – A9	1	-	5	3	5	7
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communicate and Operations Management) – A10	5	3	2	3	1	2
7.การควบคุมการเข้าถึง (Access Control) –A11	2	-	4	5	-	2
8.การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ(Information systems acquisition, development and maintenance) – A12	3	1	3	5	1	1
9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ขององค์กร (Information security incident management) – A13	-	-	2	2	-	-
10.บริหาร การความต่อเนื่องในการดำเนินงานขององค์กร(Business continuity) – A14	4	3	-	1	-	-
11.การปฏิบัติตามข้อกำหนด (Compliance) – A15	3	1	-	2	-	-
รวมทั้งหมด	24	10	31	27	9	21

จากการเปรียบเทียบผลการวิเคราะห์และประเมินความเสี่ยงก่อนและหลังดำเนินโครงการ ที่ผ่าน มาสามารถนำไปประยุกต์ใช้โดยรู้ถึงความเสี่ยงที่อาจจะเกิดขึ้น เพื่อนำมากำหนดแนวทางแก้ไขพร้อมรับมือกับความเสี่ยงที่อาจจะเกิดขึ้นหรือกำหนดแนวทางป้องกัน ดังนี้

6.2.1 ทำให้ได้รับทราบจุดอ่อนหรือช่องโหว่ ที่อาจทำให้เกิดความเสี่ยงต่อองค์กรและสามารถหาวิธีการแก้ปัญหาได้อย่างเหมาะสม

6.2.2 นำผลที่ได้ใช้กำหนดทิศทาง (Roadmap) สำหรับการพัฒนาปรับปรุงนโยบายความปลอดภัยภายในองค์กรด้วยมาตรฐาน ISO/IEC 27001

6.2.3 นำผลการวิเคราะห์ที่ได้มาจัดทำแผนการดำเนินงานประจำปี แผนปฏิบัติราชการ 4 ปี รวมทั้งการจัดทำแผนแม่บทด้านเทคโนโลยีสารสนเทศ

6.2.4 วางแผนพัฒนาระบบสารสนเทศ เพื่อรองรับการขยายงานขององค์กรก้าวสู่ประชาคมอาเซียนในการคุ้มครองผู้บริโภคสู่สากล พร้อมทั้งสร้างมาตรฐานข้อมูลในการติดต่อแลกเปลี่ยนข้อมูลระหว่างองค์กร ดังนั้นการรักษาความปลอดภัยข้อมูล การประเมินและการบริหารความเสี่ยงที่เกิดขึ้นจึงถือเป็นสิ่งสำคัญในการบริหารงานองค์กรให้มีประสิทธิภาพ

6.3 ปัจจัยความสำเร็จ ที่สำคัญในการประยุกต์ใช้มาตรฐาน ISO/IEC 27001 ในองค์กรมีดังนี้

6.3.1 การสนับสนุนจากฝ่ายบริหาร (Management Support) เนื่องจากการบริหารจัดการด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศให้สำเร็จต้องได้รับความร่วมมือร่วมใจ จากบุคลากรในหน่วยงานที่เกี่ยวข้องทุกส่วนงาน ได้แก่ ด้านงบประมาณ ด้านผู้ใช้ระบบ

6.3.2 ความร่วมมือของบุคลากรภายในองค์กร (Internal Approach)

6.3.3 การสื่อสารภายในองค์กร(Document Control) การประสานงานและการติดต่อสื่อสารภายในองค์กร ต้องชัดเจนและก้าวไปในทิศทางเดียวกัน

6.3.4 ขอบเขตการดำเนินงาน (Scope of Work) ต้องมีความชัดเจน

6.4 ปัญหาอุปสรรค

ต้องมีการวางแผนการดำเนินงานที่ดี ทำงานซ้ำซ้อนในช่วงแรกที่มีการเริ่มดำเนินการโครงการทำให้ไม่ได้รับความร่วมมือจากเจ้าหน้าที่ปฏิบัติเท่าที่ควร ต้องมีการสื่อสารให้เจ้าหน้าที่/หรือบุคลากรในองค์เข้าใจถึง การจัดการดำเนินงานด้านความปลอดภัยของระบบเทคโนโลยี และมีความตระหนักในการการจัดทำ

6.5 ข้อเสนอแนะ

6.5.1 การปฏิบัติตามมาตรฐาน ISO/IEC 27001:2005 ซึ่งเป็นที่ยอมรับตามมารตฐานสากล หากหน่วยงานของรัฐหรือภาคเอกชน นำมาประยุกต์ใช้ให้เหมาะสมกับสภาพแวดล้อมหรือบริบทของลักษณะงานและวัฒนธรรมขององค์กร จะสามารถทำให้องค์กรพัฒนาและสร้างความศรัทธาและเชื่อมั่นจากผู้ใช้บริการได้และสามารถใช้เป็นเครื่องมือในการพัฒนาองค์กรให้ก้าวสู่ความเป็นเลิศได้อย่างมีประสิทธภาพ

6.5.2 การฝึกอบรมสำหรับนักพัฒนาโปรแกรมหรือนักพัฒนาแอพพลิเคชันนั้น ควรเป็นส่วนหนึ่งที่เพิ่มจากการฝึกอบรมพนักงานทั่วไป โดยส่วนที่เพิ่มขึ้นมานั้นควรเป็นเรื่องเกี่ยวกับเทคนิคการเขียนโปรแกรมอย่างไรเพื่อให้มีความปลอดภัย นอกจากนี้ก็ควรจะอธิบายถึงเหตุผลและหน้าที่ของฝ่ายรักษาความปลอดภัย ในระหว่างที่ได้มีการพัฒนา กระบวนการรักษาความปลอดภัยสำหรับโครงการใหม่ฝ่ายรักษาความปลอดภัยนั้น ควรที่จะมีส่วนร่วมในระหว่างการออกแบบด้วย ซึ่งเป็นการเปิดโอกาส ให้ฝ่ายการรักษาความปลอดภัยได้มีการพิจารณาเกี่ยวกับ เรื่องความปลอดภัย ก่อนที่จะผลิตในระหว่างการอบรมนั้น ควรจะอธิบายให้นักพัฒนาโปรแกรมทราบถึงคุณค่าของความปลอดภัยในช่วงต้นของการผลิตซอฟต์แวร์

6.5.3 การตรวจสอบการปฏิบัติตามนโยบายนั้น ไม่ควรที่จะเน้นในเฉพาะระบบคอมพิวเตอร์เท่านั้น ควรให้ความสำคัญกับข้อมูลที่มีอยู่ในรูปแบบอื่นด้วย ควรตรวจสอบด้วยว่านโยบายข้อมูลนั้นมีการปฏิบัติตามเคร่งครัดแค่ไหน หรือเอกสารที่มีข้อมูลที่สำคัญมีการจัดเก็บหรือรับส่งอย่างไร

การตรวจสอบควรกระทำปีละครั้ง อาจทำโดยเจ้าหน้าที่จากฝ่ายรักษาความปลอดภัย หรืออาจจะเป็นฝ่ายตรวจสอบต่างหาก หรืออาจจ้างบริษัทข้างนอก ซึ่งมีความชำนาญทางด้านนี้โดยเฉพาะมาทำงานให้ การรักษาความปลอดภัยนั้นเกี่ยวกับการบริหารจัดการความเสี่ยง ถ้าระบบไม่มีความเสี่ยงก็ไม่จำเป็นต้องมีระบบการรักษาความปลอดภัย แต่ถ้าระบบมีความเสี่ยงก็จำเป็นต้องรู้ว่าเสี่ยงมากน้อยแค่ไหน และต้องออกแบบและติดตั้งระบบอะไร เพื่อที่จะช่วยลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และงบประมาณเพียงพอ