บทที่ 5
ผลการดำเนินงาน

จากการศึกษาวิจัย ตามขั้นตอนในบทที่ 4 ได้นำผลการวิเคราะห์และประเมินความเสี่ยงมาจัดหมวดหมู่แยกประเภทตามมาตรฐาน ISO/IEC 27001 ทั้ง 11 โดเมนโดยสรุปตามระดับของความเสี่ยงที่ประเมินได้ 3 ระดับ ได้แก่ ต่ำ ปานกลาง สูง ดังนี้

ระดับความเสี่ยง 1 – 8 คือ ระดับความเสี่ยงต่ำ (Low) ยังไม่จำเป็นต้องมีการจัดการในขณะนี้ก็ได้ไม่มีผลกระทบต่อการทำงานขององค์กรมากนัก แต่ควรมีแผนการดำเนินงานหรือพัฒนาปรับปรุงงานให้มีประสิทธิภาพยิ่งขึ้น

ระดับความเสี่ยง 9 – 16 คือ ระดับความเสี่ยงกลาง (Medium) องค์กรเริ่มมองว่าเป็นระดับความเสี่ยงที่มีความสำคัญ ควรมีการปรับปรุงแต่ยังไม่เร่งด่วน แต่ควรอยู่ในแผนการดำเนินงานขององค์กรในระยะยาว ซึ่งต้องมีการวางแผนการดำเนินงานไว้ล่วงหน้า

ระดับความเสี่ยง 17 – 25 คือ ระดับความเสี่ยงสูง (High) องค์กรต้องมองว่าเป็นระดับความเสี่ยงที่มีสำคัญมาก มีโอกาสเกิดความเสียหายที่เกิดขึ้นสูง ต้องมีการจัดการอย่างเร่งด่วน ควรกำหนดอยู่ให้อยู่ในแผนการดำเนินงานระยะสั้น แผนการดำเนินงานทั้งระยะกลางและระยะยาว ซึ่งแสดงให้เห็นถึงความจำเป็นอย่างยิ่งและต้องมีการบริหารจัดการโดยเร็ว เพื่อป้องกันความเสียหายที่จะเกิดขึ้น

มีผลการดำเนินงานสรุปได้ 3 ระยะ ได้แก่ ผลการวิเคราะห์และประเมินความเสี่ยง (ก่อนการดำเนินโครงการ) นำผลการวิเคราะห์มาดำเนินการปรับปรุงระบบสารสนเทศ และ มีการวิเคราะห์และประเมินความเสี่ยง(หลังดำเนินโครงการ) โดยมีผลการดำเนินงาน ดังนี้

5.1 ผลการวิเคราะห์และประเมินความเสี่ยง(ก่อนการดำเนินโครงการ)

วัตถุประสงค์

1. เพื่อให้ทราบถึงความเสี่ยงของระบบเทคโนโลยีสารสนเทศขององค์กรที่อาจจะเกิดขึ้น
2. เพื่อทราบถึงช่องโห่ว/จุดอ่อน ด้านเทคโนโลยีสารสนเทศในปัจจุบัน
3. เพื่อนำผลการวิเคราะห์และประเมินความเสี่ยงไปประยุกต์ใช้งานต่างๆ

จากการวิเคราะห์และประเมินความเสี่ยงด้วยมาตรฐาน ISO/IEC 27001 ก่อนการดำเนินโครงการทำให้ศูนย์เทคโน ฯ ทราบถึงความเสี่ยง จุดอ่อน/ช่องโหว่ ของระบบและเครือข่ายที่มีอยู่ในปัจจุบัน ซึ่งสรุปผลการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ 11 หัวข้อ (Domain) รายละเอียด ภาคผนวก ค ตารางผลการวิเคราะห์และประเมินความเสี่ยง(ก่อนดำเนินโครงการ) ได้ผลสรุปตามตารางที่ 5.1 ดังนี้

ตารางที่ 5.1 สรุปผลการวิเคราะห์และประเมินความเสี่ยง (ก่อนดำเนินโครงการ)

11 หัวข้อ(ก่อนดำเนินโครงการ)	**ระดับความเสี่ยง**		
	สูง	**กลาง**	**ต่ำ**
1.นโยบายความมั่นคงปลอดภัย (Security policy) –A5	3	-	-
2.โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) –A6	3	2	-
3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)-A7	1	4	-
4.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources ecurity) – A8	1	6	2
5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) – A9	2	5	2
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and operations management) – A10	5	2	1
7.การควบคุมการเข้าถึง (Access control) – A11	4	1	1
8.การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) – A12	4	2	1

ตารางที่ 5.1 (ต่อ)

11 หัวข้อ(ก่อนดำเนินโครงการ)	ระดับความเสี่ยง		
	สูง	กลาง	ต่ำ
9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management) – A13	-	2	-
10.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity) – A14	4	-	-
11.การปฏิบัติตามข้อกำหนด (Compliance) – A15	-	1	2
รวม	27	25	9

การสรุปข้อมูลจากรายละเอียดใน (ภาคผนวก ค) ขออธิบายเพิ่มเติมถึงวิธีการผลสรุปผลที่ได้ตามตารางที่ 5.1 ดังตามตัวอย่างที่ 1 ข้างล่างนี้ เพื่อความเข้าใจที่ชัดเจน

ตัวอย่างที่ 1. ผลการวิเคราะห์จากรายละเอียดในภาคผนวก ค สรุปได้ตาราง 5.1 ข้อ 1 นโยบายความมั่นคงปลอดภัยสำหรับองค์กร(Security Policy) – A5 และตามมาตรฐาน ISO/IEC 27001 ดังนี้

ตารางที่ 5.2 ตารางการวิเคราะห์และประเมินความเสี่ยงข้อ 1 (ก่อนดำเนินโครงการ) ตามภาคผนวก ค

ข้อ 1	ประเด็นความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส	ผลการวิเคราะห์	ระดับความเสี่ยง
1.1	ยังไม่มีการประกาศใช้นโยบายด้านความปลอดภัยเป็นทางการ	ยังไม่ได้จัดทำนโยบายด้านความมั่นคงปลอดภัยระบบ	5	5	25	สูง
1.2	ไม่มีการกำหนดหน้าที่และความรับผิดชอบในการจัดทำนโยบายความปลอดภัยและแนวปฏิบัติ	ไม่มีการกำหนดหน้าที่และผู้รับผิดชอบดูแลระบบสารสนเทศอย่างชัดเจน	5	5	25	สูง

ตารางที่ 5.2 (ต่อ)

ข้อ 1	ประเด็นความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส	ผลการวิเคราะห์	ระดับความเสี่ยง
1.3	ไม่มีการทบทวนปรับปรุงการจัดทำนโยบายความมั่นคงปลอดภัย	มีการละเมิดด้านความมั่นคงปลอดภัยขององค์กร	4	5	20	สูง

ผลสรุปได้ ตามหัวข้อที่ 1 ตารางที่ 5.1 ระดับความเสี่ยงสูง = 3 หัวข้อย่อย ได้แก่ 1.1-1.3 ตัวอย่างที่ 2. นำผลการวิเคราะห์จากรายละเอียดในภาคผนวก ค สรุปได้ในตาราง 5.1 ในข้อ 2 ของโครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร(Organization of information security) – A6 ตามมาตรฐาน ISO/IEC 27001 ได้ตามตารางที่ 5.3 รายละเอียดดังนี้

ตารางที่ 5.3 ตารางการวิเคราะห์และประเมินความเสี่ยง ข้อ2 (ก่อนดำเนินโครงการ) ในภาคผนวก ค

ข้อ 2	ประเด็นความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส	ผลการวิเคราะห์	ระดับความเสี่ยง
2.1	ไม่สามารถผลักดันนโยบายด้านความปลอดภัยให้ชัดเจน	ขาดการกำหนดประสานงานด้านความมั่นคงปลอดภัยระบบจากสำนัก/กอง	5	4	20	สูง
2.2	ระบบสารสนเทศไม่มีความมั่นคงปลอดภัยเนื่องจากขาดผู้รับผิดชอบและดูแลอย่างจริงจัง	ไม่มีการกำหนดหน้าที่และผู้รับผิดชอบดูแลระบบสารสนเทศอย่างชัดเจน	5	4	20	สูง

ตารางที่ 5.3 (ต่อ)

ข้อ 2	ประเด็นความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส	ผลการวิเคราะห์	ระดับความเสี่ยง
2.3	การเข้าถึงระบบและข้อมูลสำคัญโดยไม่ได้รับอนุญาต	มีการระบุข้อกำหนดหรือเงื่อนไขในการเข้าถึงระบบงานหรือสารสนเทศขององค์กร	5	2	10	กลาง
2.4	ข้อมูลสำคัญรั่วไหลหรือถูกเปิดเผยโดยบุคคลผู้ไม่มีสิทธิ์ทั้งภายในและนอกองค์กร	ไม่มีการจัดทำข้อตกลงการไม่เปิดเผยความลับด้านข้อมูลและเอกสารขององค์กร	5	4	20	สูง
2.5	ไม่มีการจัดทำแผนฉุกเฉิน กรณีระบบมีปัญหา	ไม่สามารถกู้ระบบได้ตามเวลาที่เหมาะสมอาจส่งผลกระทบต่อการทำงาน	4	4	16	กลาง

ผลสรุป ตามหัวข้อที่ 2 ตารางที่ 5.1 ข้างบน ระดับความเสี่ยงสูง = 3 ได้แก่ หัวข้อ 2.1, 2.2 และ 2.4 ระดับความเสี่ยงกลาง = 2 ได้แก่หัวข้อ 2.3 และ 2.5

5.2 นำผลการวิเคราะห์และประเมินความเสี่ยง (ก่อนดำเนินโครงการ) เพื่อการบริหารจัดการศูนย์เทคโนโลยีสารสนเทศ โดยดำเนินการ ดังนี้

5.2.1 นำมาพัฒนาและปรับปรุงแนวคิดในการจัดทำนโยบายด้านความปลอดภัย (Security Policy Development) ตามมาตรฐานและแนวปฏิบัติของมาตรฐาน ISO/IEC 27001 โดยนำผลการวิเคราะห์และประเมินความเสี่ยง เข้าประชุมคณะกรรมการด้านระบบสารสนเทศเพื่อคัดเลือกหัวข้อ

ที่จะใช้ กำหนดนโยบายด้านความปลอดภัย ซึ่งประกอบด้วย 11 หัวข้อ (Domain) สรุปได้ตามตารางที่ 5.4 ดังนี้

ตารางที่ 5.4 สรุปผลการจัดทำนโยบายความปลอดภัย

หัวข้อ(Domain)	**จัดทำนโยบายความปลอดภัย**	
	ทำ	**ไม่ทำ**
1. A5-นโยบายความมั่นคงปลอดภัย (Security policy)	/	
2. A6 -โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)		/
3. A7 -การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)		/
4.A8-ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources ecurity)	/	
5.A-9 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)	/	
6. A-10 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and operations management)	/	
7.A-11 การควบคุมการเข้าถึง (Access control)	/	
8.A-12 การจัดหา การพัฒนา และการบำรุงรักษาระบบ การจัดหาการพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)	/	
9.A-13 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ขององค์กร (Information security incident management)		/
10.A-14 บริหาร การความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity)	/	
11.A-15 การปฏิบัติตามข้อกำหนด (Compliance)		/
รวม	7	4

สามารถนำมาจัดหมวดหมู่แยกตามประเด็นความเสี่ยงสิ่งที่ต้องจัดทำก่อนได้ หลังจากนั้นนำผลการวิเคราะห์และการเลือกหัวข้อ สิ่งที่ต้องปรับปรุงนโยบายความปลอดภัยระบบสารสนเทศและแนวปฏิบัติตามมาตรฐาน ISO/IEC 27001 ปี 2556 สรุปได้ 7 หัวข้อประกอบด้วย

1. A5 - นโยบายความมั่นคงปลอดภัย (Security Policy)

2. A8 - ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resource security)

3. A9 - การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

4. A10 - การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายสารสนเทศขององค์กร(Communications and operations management)

5. A11- การควบคุมการเข้าถึง (Access control)

6. A12- การจัดหา การพัฒนา และการบำรุงรักษาระบบ การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ(Information systems acquisition, development and maintenance)

7. A14 - การบริหาร ความต่อเนื่องในการดำเนินงานขององค์กร(Business continuity)

จากหัวข้อดังกล่าวข้างต้นคณะกรรมการ ICT ได้เลือก มีความสอดคล้องตามข้อกำหนดในการจัดทำนโยบายของกระทรวง ICT (สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,กันยายน 2556, น 4) มีรายละเอียดเกี่ยวกับความเสี่ยงที่ต้องบริหารจัดการอย่างเร่งด่วนและมีความจำเป็น ซึ่งผู้ศึกษาวิจัยได้ร่วมจัดทำและตรวจสอบนโยบายที่ได้ปรับปรุงเรียบร้อยแล้วรายละเอียดตาม (ภาคผนวก จ)

ส่วนหัวข้อที่ไม่ๆได้เลือกในการพัฒนาปรับปรุงและจัดทำนโยบาย ความปลอดภัยระบบสารสนเทศและแนวปฏิบัติตามมาตรฐาน ISO/IEC 27001 ในครั้งนี้ก็มีความสำคัญแต่จะพิจารณาจากความเร่งด่วน โดยอาจจะพัฒนาในปี 2557-2558 สรุปได้ 4 หัวข้อประกอบด้วย

1. A6 – โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร(Organization of information security)

2. A7 - การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

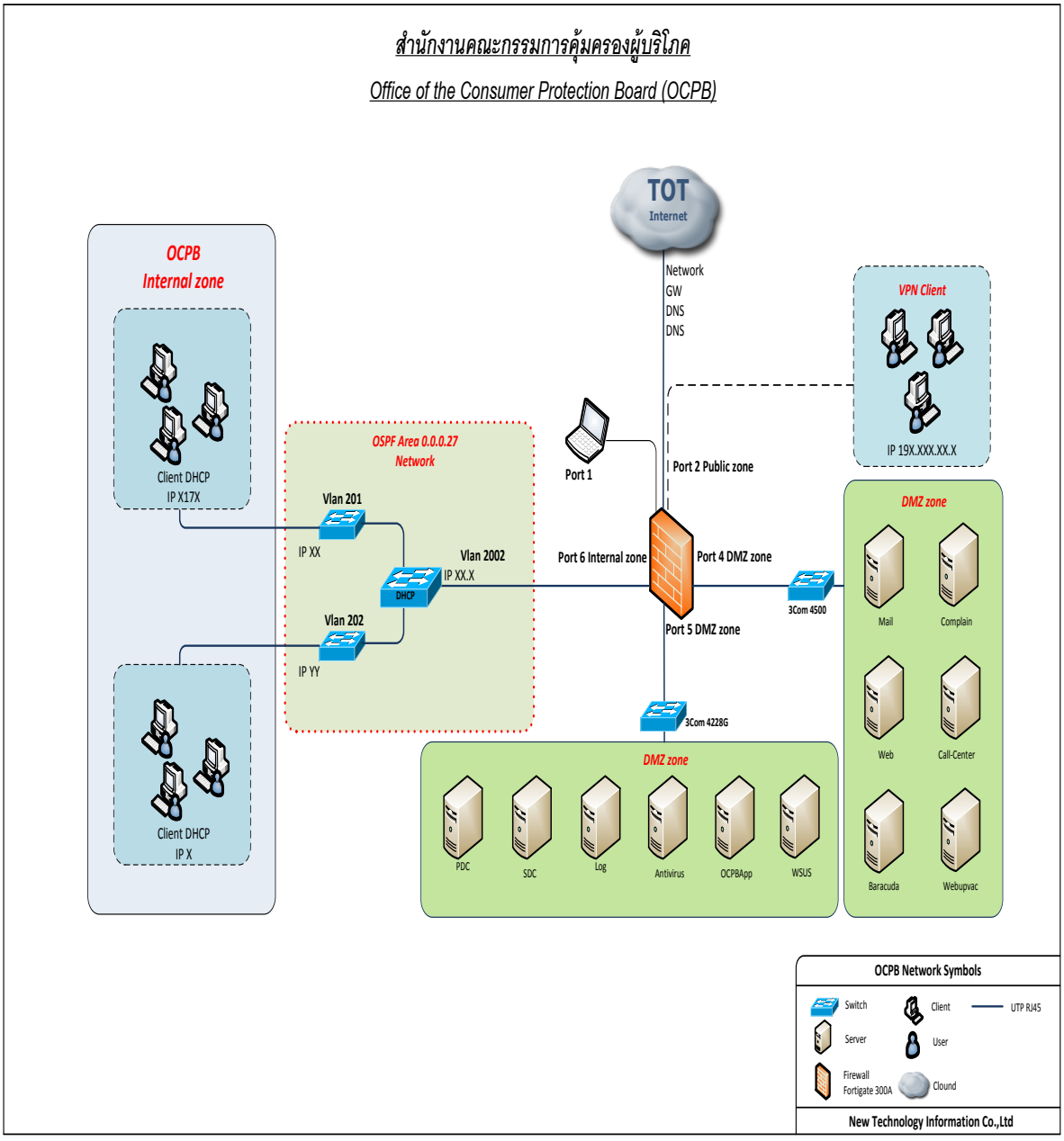
3. A13 -การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

4. A15- การปฏิบัติตามข้อกำหนด (Compliance)

5.2.2 นำมาพัฒนาและปรับปรุงด้านความปลอดภัยระบบสารสนเทศของหน่วยงานเพื่อจัดทำโครงการจัดซื้ออุปกรณ์ป้องกันการบุกรุกระบบเครือข่าย และสามารถดำเนินการเพิ่ม

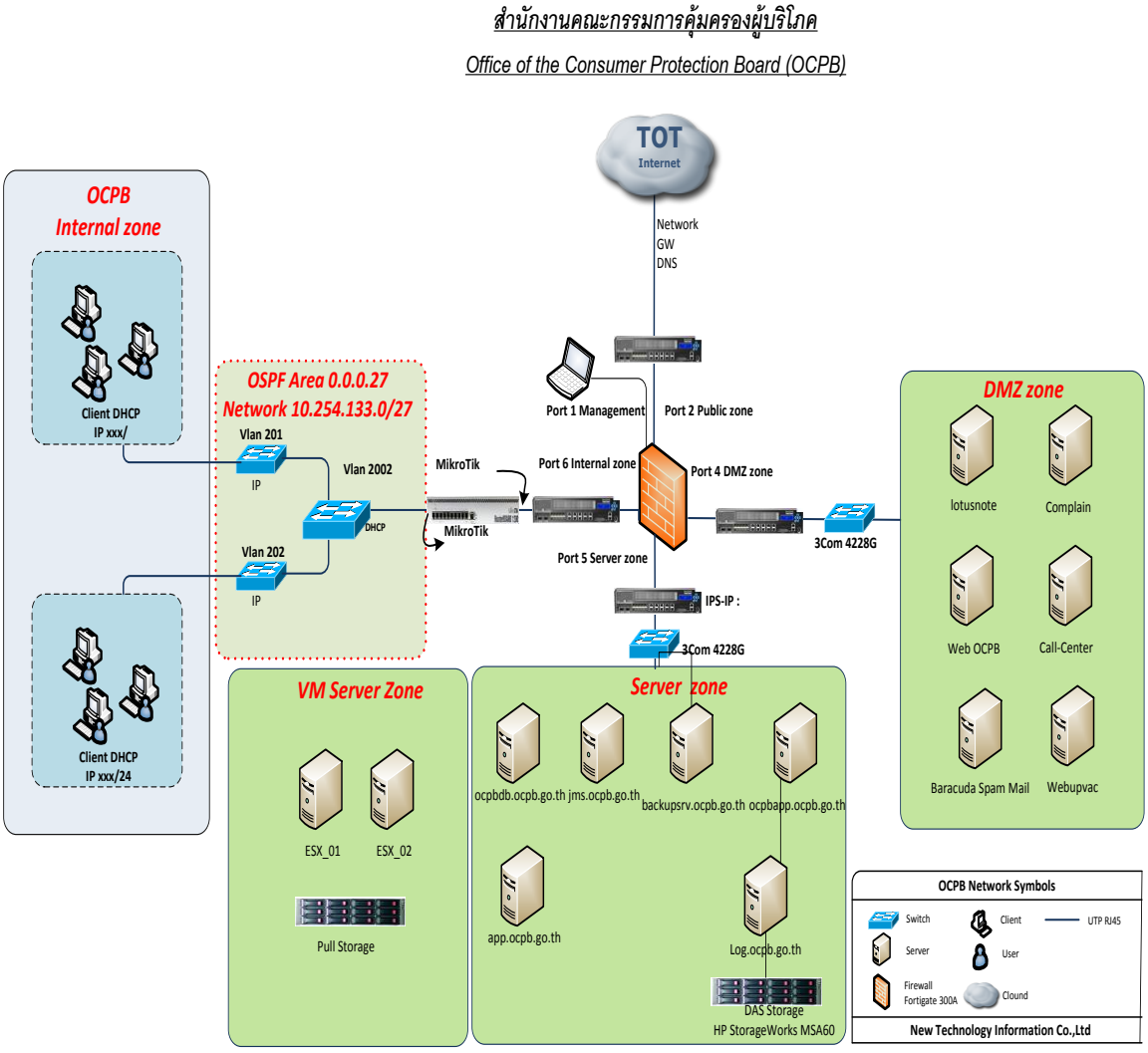
ความปลอดภัยให้กับระบบเครือข่ายได้ สามารถดำเนินการปรับปรุงระบบเครือข่ายเพื่อให้ระบบมีความปลอดภัยมากยิ่งขึ้น ดังนี้

5.2.2.1 โครงสร้างของระบบเครือข่ายเดิม ขณะที่ดำเนินการวิเคราะห์และประเมินความเสี่ยง ก่อนการดำเนินการโครงการรายละเอียด ดังภาพที่ 5.1



ภาพที่ 5.1 ระบบเครือข่ายภายในองค์กรก่อนที่มีการปรับปรุง

5.2.2.2 ได้มีการปรับปรุงระบบเครือข่าย จากผลการวิเคราะห์และประเมินความเสี่ยง (ภาคผนวก ค) ในข้อ 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operating Management- A10) หัวข้อย่อย 6.2 ผลการวิเคราะห์และประเมินความเสี่ยง = 25/ ระดับสูง และได้ดำเนินการปรับปรุงระบบเครือข่ายใหม่รายละเอียด ดังภาพที่ 5.2



ภาพที่ 5.2 ระบบเครือข่ายภายในองค์กรที่มีการปรับปรุงแล้วในปัจจุบัน

จากการวิเคราะห์และปรับปรุงระบบเครือข่าย โดยปกติมีการแบ่งโซนของระบบเครือข่ายให้เหมาะสมตามอุปกรณ์ต่างๆ เพื่อไม่ให้เกิดความเสี่ยงในการโจมตีระบบ ทั้งภายนอกและภายใน จากการนำเสนอผลการวิเคราะห์และประเมินความเสี่ยงก่อนการดำเนินการโครงการ

เข้าสู่ที่ประชุมผู้บริหาร ได้รับการจัดสรรงบประมาณเพื่อจัดซื้ออุปกรณ์ป้องกันการบุกรุก (IPS) เพื่อสร้างความปลอดภัยของระบบเพิ่มขึ้น ในการเข้าถึงระบบเครือข่ายและการเข้าถึงข้อมูล โดยให้มีการแบ่งโซน ดังนี้

1. DMZ Zone (DMZ) ใช้สำหรับเชื่อมต่อกับอุปกรณ์ Server และ Log เพื่อให้เกิดการควบคุมและป้องกันการเข้าถึงเครื่อง Server และการแก้ไข Log

2. Server Zone ใช้สำหรับเชื่อมต่อกับอุปกรณ์ไปยัง Server เพื่อให้การทำงานของระบบเครือข่ายสามารถควบคุมการเข้าถึงข้อมูลได้

3. Internal Zone ใช้สำหรับเชื่อมต่อกับเครือข่ายภายใน Office ของผู้ใช้งานเพื่อให้เกิดความปลอดภัยและป้องกันการเข้าออกของข้อมูล

4. IPS-IP : ใช้สำหรับเชื่อมต่อกับ Server Zone และ DMZ Zone ใช้สำหรับการตรวจสอบความปลอดภัยในของระบบเครือข่าย ที่ได้จัดซื้อเพิ่มเติมตามโครงการนี้

5.2.3 การตรวจสอบความปลอดภัยของระบบเครือข่ายสารสนเทศโดยตรวจสอบช่องโหว่หรือจุดอ่อนด้วยโปรแกรม Nessus

การดำเนินการตามข้อนี้ได้ดำเนินการทดสอบจาก เครื่องแม่ข่ายที่สำคัญหลายเครื่อง แต่นำเสนอเพียงบางตัวเท่านั้นเพื่อสร้างความเข้าใจในการตรวจสอบระบบเครือข่าย ตามตัวอย่างที่ 5.3 ตัวอย่างที่ 5.3 รายงานการตรวจสอบช่องโหว่เครื่องคอมพิวเตอร์แม่ข่ายปีงบประมาณ 2555 มีดังนี้ รายละเอียดเครื่องคอมพิวเตอร์แม่ข่าย ดังรูปหน้าถัดไป

ตารางที่ 5.5 ผลการตรวจสอบช่องโหว่ (Vulnerabilities)

Hostname : www.ocpb.go.th Private IP Address : 172.16.106.3

Public IP Address : 180.180.240.36 Date Scan : 30 Aug 2012

WWW.OCPB.GO.TH	
Scan Time	
Start time:	Tue Aug 30 18:18:17 2012
End time:	Tue Aug 30 18:24:12 2012
Number of vulnerabilities	
High	8
Medium	5
Low	123
Remote Host Information	
Operating System:	Microsoft Windows Server 2008 R2 Standard
NetBIOS name:	WEB
DNS name:	www.ocpb.go.th
IP address:	172.16.106.3
MAC address:	e4:1f:13:1c:19:08

จะเห็นได้ว่า Number of Vulnerabilities รายละเอียดในการตรวจสอบช่องโหว่ของระบบของ Plugin ID ในระดับต่างๆ

5.3 ผลการวิเคราะห์และประเมินความเสี่ยง (หลังการดำเนินโครงการ)

วัตถุประสงค์

1. เพื่อให้รู้ว่าความเสี่ยงของระบบเทคโนโลยีสารสนเทศขององค์กรมีอะไรบ้าง ที่ต้องปรับปรุง และต้องจัดการความเสี่ยงทรัพย์สินสารสนเทศ

2. นำผลการวิเคราะห์และการประเมินความเสี่ยงมาวางแผนการบริหารความเสี่ยงที่ยังเหลืออยู่

สรุปผลการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ จากรายละเอียดใน (ภาคผนวก ง) ตารางผลการวิเคราะห์และประเมินความเสี่ยง(หลังดำเนินโครงการ) ผลสรุปตามตารางที่ 5.6 มีรายละเอียด ดังนี้

ตารางที่ 5.6 สรุปผลการวิเคราะห์และประเมินความเสี่ยง (หลังการดำเนินโครงการ)

11 หัวข้อ (หลังดำเนินโครงการ)	ระดับความเสี่ยง		
	สูง	กลาง	ต่ำ
1.นโยบายความมั่นคงปลอดภัย (Security policy) –A5	1	-	1
2.โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) –A6	1	3	1
3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) - A7	-	4	2
4.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resource security) – A8	-	4	5
5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) – A9	-	3	7
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and operations management) – A10	3	3	2
7.การควบคุมการเข้าถึง (Access control) – A11	-	5	2
8.การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) – A12	1	5	1
9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management) – A13	-	2	-
10.บริหาร การความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity) – A14	3	1	-
11.การปฏิบัติตามข้อกำหนด (Compliance) – A15	1	2	-
รวม	26	27	10

จากการวิเคราะห์และประเมินความเสี่ยงด้วยมาตรฐาน ISO/IEC 27001 อีกครั้งหลังการดำเนินโครงการทำให้องค์กรทราบถึงความเสี่ยงของระบบที่ยังมีอยู่ในปัจจุบันและนำผลที่ได้ประยุกต์ใช้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศต่อไป