Information Security Risk Management Handbook

คู่มือการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ประจำปีงบประมาณ

2566

Submitted by:
MWA Digital

การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

คู่มือการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

Information Security Risk Management Handbook

หมายเลขเอกสาร	
ปรับปรุงครั้งที่	
วันที่มีผลบังคับใช้	15 กันยายน 2566
ประเภทเอกสาร	ภายใน
เจ้าของเอกสาร	ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล
ทบทวนโดย	ทีมงานดำเนินการข้อ 5.2
มีผลบังคับใช้กับ	ผู้ปฏิบัติงาน
อนุมัติโดย	ผู้ช่วยผู้ว่าการ (เทคโนโลยีดิจิทัล)

ประวัติการแก้ไขเอกสาร

ครั้งที่	รายละเอียดการแก้ไข	วันที่มีผลบังคับใช้
1	- นำคู่มือหลักวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO 27001 มาเป็นเอกสารอ้างอิงในการทำคู่มือฉบับนี้ - กระบวนการและการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ - การสื่อสารและการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ - การวัด ติดตาม วิเคราะห์ ประเมินผล ตัววัดผลลัพธ์ กระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ - การนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล/ จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) การนำผลที่ได้จากการประเมินไปเรียนรู้และจัดการความรู้เพื่อนำไปปรับปรุงและทำนวัตกรรม	15 กันยายน 2566

การอนุมัติเอกสาร

ผู้จัดทำ	
ชื่อ นายทรงศักดิ์ ศรีโดวัน ตำแหน่ง ผอ. กขม. ฝคท. วันที่ 13 ก.ย. 66	ลงชื่อ ..... ((นายทรงศักดิ์ ศรีโดวัน) ผอ.กขม.ฝคท.)
ผู้สอบทาน	
ชื่อ นายภาคภูมิ พิระชัย ตำแหน่ง ผอ. ฝคท. วันที่ 13 ก.ย. 66	ลงชื่อ ..... ((นายภาคภูมิ พิระชัย) ผอ.ฝคท.)
ผู้อนุมัติ	
ชื่อ นายธำรง บูรณะตระกูล ตำแหน่ง รวก.(ท) วันที่ 14 ก.ย. 66	ลงชื่อ ..... ((นายธำรง บูรณะตระกูล) รองผู้ว่าการ (เทคโนโลยีดิจิทัล))

สารบัญ

สารบัญตาราง

1. วัตถุประสงค์

การประเมินความเสี่ยงเป็นกระบวนการสำคัญที่ใช้ในการพิสูจน์หาปัจจัยที่ก่อให้เกิดความเสี่ยง ทั้งนี้ผลการประเมินความเสี่ยงจะถูกนำมาใช้ในการจัดการความเสี่ยง โดยพิจารณาจากระดับความเสี่ยง และเกณฑ์ในการยอมรับความเสี่ยง การประเมินความเสี่ยงจำเป็นต้องมีหลักการ และขั้นตอนปฏิบัติที่แน่ชัดเพื่อทำให้การประเมินความเสี่ยงนั้นมีประสิทธิภาพ มีความสม่ำเสมอ สามารถเปรียบเทียบ และเชื่อถือได้ โดยมีวัตถุประสงค์ดังนี้

- เป็นกรอบในการประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของกปน. เพื่อให้การประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของกปน. เป็นไปอย่างเป็นระบบ และสอดคล้องกับมาตรฐานสากล
- เพื่อใช้จัดการกับความไม่แน่นอนที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ และอยู่ในระดับที่ยอมรับได้

2. ขอบเขต

อ้างอิงจากเอกสารคู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual) (IS.HBK.002)

3. นิยามและคำจำกัดความ

ภายใต้เอกสารหลักวิธีการประเมินความเสี่ยงฉบับนี้ ได้กำหนดนิยามและคำจำกัดความดังนี้

1. **ทรัพย์สินสารสนเทศ** หมายถึง สิ่งที่มีความสำคัญต่อกปน. ซึ่งอาจได้รับผลกระทบจากเหตุการณ์ความเสี่ยง และส่งผลกระทบต่อการดำเนินกิจกรรม

2. **เหตุการณ์ความเสี่ยง** หมายถึง เหตุการณ์ที่มีความไม่แน่นอนในอนาคต มีผลกระทบเชิงลบต่อระบบสารสนเทศ ข้อมูลสารสนเทศ รวมไปถึงทรัพย์สินสารสนเทศ/ทรัพยากรอื่น ๆ ของกปน. และส่งผลต่อวัตถุประสงค์ด้านปลอดภัยสารสนเทศทำให้กระบวนการดำเนินธุรกิจล่าช้าหรือหยุดชะงัก

3. **ภัยคุกคาม** หมายถึง ปัจจัยที่ไม่พึงประสงค์ซึ่งมีความเป็นไปได้ที่จะส่งผลให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศ ระบบเทคโนโลยีสารสนเทศหรือองค์กร ความเสียหายเหล่านี้เกิดขึ้นจากการที่ทรัพย์สินสารสนเทศนั้นถูกกระทำหรือโจมตี

4. **ช่องโหว่** หมายถึง จุดอ่อนของทรัพย์สินสารสนเทศ หรือมาตรการที่ภัยคุกคามสามารถอาศัยเป็นช่องทางใช้เป็นประโยชน์หรือเจาะช่องโหว่นั้น สร้างความเสียหายต่อทรัพย์สินสารสนเทศ ระบบเทคโนโลยีสารสนเทศหรือองค์กรได้

5. **การประเมินความเสี่ยง** หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อทรัพย์สินสารสนเทศ โดยผลลัพธ์แสดงให้เห็นถึงระดับของความเสี่ยงที่มีผลต่อทรัพย์สินสารสนเทศ

6. **ผู้กระทำ** หมายถึง ผู้ที่สร้างภัยคุกคามหรือผู้ที่ใช้ประโยชน์จากช่องโหว่ที่เกิดขึ้น ผู้กระทำอาจจะเป็นทั้งคนภายในองค์กรหรือคนภายนอกองค์กร ทั้งนี้อาจรวมถึงการกระทำที่ไม่ใช่มนุษย์

7. **ผลกระทบ** หมายถึง ผลจากเหตุการณ์ความเสี่ยงสามารถเป็นได้ทั้งบวกและลบต่อวัตถุประสงค์การดำเนินการทางธุรกิจหรือในการปฏิบัติงาน

8. **โอกาสเกิด** หมายถึง โอกาสที่น่าจะเป็นไปได้ (Probability) หรือความถี่ (Frequency) ที่เหตุการณ์จะเกิดขึ้น

9. มาตรการควบคุม หมายถึง มาตรการที่ใช้สำหรับจัดการ หรือควบคุมความเสี่ยง โดยรวมถึงกระบวนการ นโยบาย การปฏิบัติ หรือการกระทำใด ๆ ที่ควบคุมความเสี่ยง ซึ่งอาจเป็นรูปแบบการจัดการด้านเทคนิค ด้านการดำเนินการจัดการ ด้านบริหารจัดการ หรือด้านกฎหมาย

10. การตอบสนองความเสี่ยง หมายถึง การคัดเลือกแนวทางการตอบสนองความเสี่ยงประกอบด้วย การหลีกเลี่ยงไม่ให้เกิดความเสี่ยง (ยกเลิก) การยอมรับความเสี่ยง การควบคุมความเสี่ยง (ควบคุม) และการถ่ายโอนความเสี่ยง

11. แผนจัดการความเสี่ยง หมายถึง แผนดำเนินการเพื่อบริหารความเสี่ยงโดยการควบคุม จัดการ หรือปรับลดความเสี่ยง สำหรับรายการความเสี่ยงที่อยู่ในระดับที่ต้องควบคุมเพื่อจัดการความเสี่ยง

12. ความเสี่ยงที่เหลืออยู่ หมายถึง ระดับความเสี่ยงที่เหลือในปัจจุบัน หลังจากมีการตอบสนองต่อความเสี่ยง เพื่อลดโอกาสเกิดหรือผลกระทบของความเสี่ยงแล้ว

13. ผู้มีอำนาจตัดสินใจ หมายถึง ผู้มีหน้าที่ในการตัดสินใจเกี่ยวกับเหตุการณ์ความเสี่ยงที่เกิดขึ้น โดยในขอบเขตของการดำเนินการนั้น หมายถึงผู้บริหารระดับสูง (ในกรณีที่เป็นระดับความเสี่ยงสูงมาก) และคณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001 (ในกรณีที่เป็นระดับความเสี่ยงสูง ปานกลาง และต่ำ) อย่างไรก็ตาม หากเหตุการณ์ความเสี่ยงที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับฝ่ายอื่น ๆ ฝ่ายที่เกี่ยวข้องจะต้องร่วมตัดสินใจเกี่ยวกับเหตุการณ์ความเสี่ยงที่เกิดขึ้น

14. เจ้าของความเสี่ยง หมายถึง คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001 บุคคล หรือกลุ่มบุคคล ที่ได้รับผลกระทบจากความเสี่ยงโดยตรงและมีอำนาจหน้าที่ในการตัดสินใจเกี่ยวกับเหตุการณ์ความเสี่ยงที่เกิดขึ้น

4. หน้าที่ความรับผิดชอบ

ลำดับที่	ตำแหน่ง	หน้าที่ความรับผิดชอบ
1	คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001	■ พิจารณากำหนดวิธีการและเกณฑ์การประเมินความเสี่ยง ■ พิจารณารายงานผลการประเมินความเสี่ยง ■ พิจารณาแผนจัดการความเสี่ยง ■ พิจารณาผลการจัดการความเสี่ยง ■ รับทราบความคืบหน้าของแผนจัดการความเสี่ยงในการประชุม ISMS Committee
2	คณะทำงานความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001	■ กำหนดวิธีการและเกณฑ์การประเมินความเสี่ยง ■ รวบรวมรายการทรัพย์สินสารสนเทศ ■ กำหนดเหตุการณ์ความเสี่ยง ■ ประเมินความเสี่ยง ■ จัดทำรายงานผลการประเมินความเสี่ยง ■ พิจารณาความเสี่ยง ■ จัดทำแผนจัดการความเสี่ยง ■ ปฏิบัติตามแผนจัดการความเสี่ยง

ลำดับที่	ตำแหน่ง	หน้าที่ความรับผิดชอบ
		▪ ดำเนินการตามแผนการจัดการความเสี่ยง ▪ ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง ▪ แจ้งความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง ▪ ตรวจสอบการดำเนินงานตามแผนจัดการความเสี่ยง ▪ ดำเนินการปรับปรุงแก้ไขตามแผนจัดการความเสี่ยง ▪ ปรับปรุงข้อมูลการดำเนินการในแผนจัดการความเสี่ยง ▪ นำเสนอความคืบหน้าของแผนจัดการความเสี่ยงในการประชุม ISMS Committee

5. กระบวนการและการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ

SIPOC กระบวนการารบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

Supplier	Input	Process	Output	Customer
1.คณะทำงาน ISMS 2.คณะความเสี่ยงสายงาน	1.ปัจจัยภายใน/ภายนอก ที่ส่งผลกระทบต่อระบบ ISMS 2.เกณฑ์การประเมินความเสี่ยงขององค์กร 3. ความเสี่ยงที่ยอมรับได้ขององค์กร (Risk Appetite) 4. ผลการประเมินความเสี่ยงในปีที่ผ่านมา	1. กำหนดวิธีการและเกณฑ์การประเมินความเสี่ยง - ขอบเขตการประเมินความเสี่ยง (คณะทำงาน ISMS)	- วิธีการและเกณฑ์การประเมินความเสี่ยง - ขอบเขตการประเมินความเสี่ยง	คณะกรรมการ ISMS

Supplier	Input	Process	Output	Customer
คณะกรรมการ ISMS	วิธีการและเกณฑ์การประเมินความเสี่ยง	2. พิจารณาเห็นชอบ/ไม่เห็นชอบวิธีการและเกณฑ์การประเมินความเสี่ยง (คณะกรรมการ ISMS) - เห็นชอบ ดำเนินการต่อ - ไม่เห็นชอบ กลับไปกระบวนการทบทวน และจัดทำวิธีการและเกณฑ์การประเมินความเสี่ยงใหม่	วิธีการและเกณฑ์การประเมินความเสี่ยงที่ได้รับความเห็นชอบ	คณะทำงาน ISMS
คณะทำงาน ISMS	1. รายการทะเบียนทรัพย์สินสารสนเทศ 2. วิธีการและเกณฑ์การประเมินความเสี่ยงที่ได้รับความเห็นชอบ	3. รวบรวมทรัพย์สินสารสนเทศ (คณะทำงาน ISMS)	ทะเบียนรายการทรัพย์สินสารสนเทศ	คณะทำงาน ISMS
คณะทำงาน ISMS	1. ทะเบียนรายการทรัพย์สินสารสนเทศ 2. ปัจจัยภายใน/ภายนอก ที่ส่งผลกระทบต่อระบบ ISMS	4. กำหนดเหตุการณ์ประเมินความเสี่ยง (คณะทำงาน ISMS)	Risk Scenario	คณะทำงาน ISMS
คณะทำงาน ISMS	Risk Scenario	5. ประเมินความเสี่ยงและจัดทำรายงานผลกระทบการประเมินความเสี่ยง (คณะทำงาน ISMS)	1. ผลการประเมิน 2. รายงานผลการประเมินความเสี่ยง	คณะกรรมการ ISMS

Supplier	Input	Process	Output	Customer
คณะกรรมการ ISMS	รายงานผลการประเมินความเสี่ยง	6. พิจารณาเห็นชอบ/ไม่เห็นชอบ รายงานผลการประเมินความเสี่ยง (คณะกรรมการ ISMS) - เห็นชอบ ดำเนินการต่อ - ไม่เห็นชอบ กลับไปกระบวนการทบทวน และจัดทำรายงานผลการประเมินความเสี่ยงใหม่	รายงานผลการประเมินความเสี่ยงที่ผ่านการเห็นชอบ	คณะทำงาน ISMS
คณะทำงาน ISMS	1. รายงานผลการประเมินความเสี่ยงที่ผ่านการเห็นชอบ 2. Risk Scenario	7. จัดทำแผนจัดการความเสี่ยง (คณะทำงาน ISMS)	แผนจัดการความเสี่ยง	ฝยท.,ฝคท.,ฝพท.,ฝกง.,ฝบส.,สตส.,สายงานบริการ
คณะทำงาน ISMS	แผนจัดการความเสี่ยง	8. ปฏิบัติตามแผนจัดการความเสี่ยง (คณะทำงาน ISMS, ฝยท.,ฝคท.,ฝพท.,ฝกง.,ฝบส.,สตส.,สายงานบริการ)	รายงานผลการจัดการความเสี่ยง	คณะทำงาน ISMS, ฝยท.,ฝคท.,ฝพท.,ฝกง.,ฝบส.,สตส.,สายงานบริการ

RACI กระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

	ROLES	คณะกรรมการ ISMS	คณะทำงาน ISMS	คณะความเสี่ยงสายงาน	ฝคท.	ฝพท.	ฝยท.	ฝบส.	ฝกง.	ฝบส.	สคส.	สายงานปฏิบัติการ
	Key Management Practice **Status**											
1	**กำหนดวิธีการเกณฑ์การประเมินความเสี่ยง และขอบเขตการประเมินความเสี่ยง**											
	- วิธีการและเกณฑ์การประเมินความเสี่ยง - ขอบเขตการประเมินความเสี่ยง		C	C/R	C							
2	**พิจารณาเห็นชอบ/ไม่เห็นชอบวิธีการและเกณฑ์การประเมินความเสี่ยง**											
	วิธีการและเกณฑ์การประเมินความเสี่ยงที่ได้รับความเห็นชอบ		A	R								
3	**รวบรวมทรัพย์สินสารสนเทศ**											
	ทะเบียนรายการทรัพย์สินสารสนเทศ			C/R								
4	**กำหนดเหตุการณ์ประเมินความเสี่ยง**											
	Risk Scenario			C/R								
5	**ประเมินความเสี่ยงและจัดทำรายงานผลกระทบการประเมินความเสี่ยง**											
	- ผลการประเมิน - รายงานผลการประเมินความเสี่ยง		I	C/R								
6	**พิจารณาเห็นชอบ/ไม่เห็นชอบ รายงานผลการประเมินความเสี่ยง**											
	รายงานผลการประเมินความเสี่ยงที่ผ่านการเห็นชอบ		A/R	C								
7	**จัดทำแผนจัดการความเสี่ยง**											
	แผนจัดการความเสี่ยง			C		R	R	R	R	R	R	R	R
8	**ปฏิบัติตามแผนจัดการความเสี่ยง**											
	รายงานผลการดำเนินงานตามมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและไซเบอร์			C/R		R	R	R	R	R	R	R	R

R	Responsible	Assigned to complete the task or deliverable.
A	Accountable	Has final decision-making authority and accountability for completion. Only 1 per task.
C	Consulted	An adviser, stakeholder, or subject matter expert who is consulted before a decision or action.
I	Informed	Must be informed after a decision or action.
I/C		

6. องค์ประกอบ

6.1 ทรัพย์สินสารสนเทศ

การบริหารจัดการทรัพย์สินสารสนเทศที่ถูกต้องเหมาะสมเพื่อให้ดำรงอยู่ถือเป็นสิ่งสำคัญสูงสุดขององค์กร และถือเป็นหน้าที่ของฝ่ายบริหารทุกระดับ โดยทรัพย์สินสารสนเทศที่จำเป็นต้องรักษาความมั่นคงปลอดภัย เช่น

- ทรัพย์สินสารสนเทศทางกายภาพ เช่น เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ ห้องดาต้าเซ็นเตอร์ อาคารสำนักงาน
- สารสนเทศ/ข้อมูล เช่น เอกสาร สัญญา ฐานข้อมูล
- ซอฟต์แวร์
- บุคลากร

การบำรุงรักษาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สมบูรณ์นั้นจำเป็นต้องมีการระบุถึงทรัพย์สินสารสนเทศที่ชัดเจน โดยทรัพย์สินสารสนเทศที่จำเป็นต้องรวบรวมในการประเมินความเสี่ยงประกอบด้วย

1. กระบวนการ (Process)
   - กระบวนการที่หากเสียหายหรือสูญเสียไปแล้วจะมีผลต่อการปฏิบัติตามภารกิจขององค์กร
   - กระบวนการที่ซึ่งหากมีการแก้ไขแล้วจะส่งผลกระทบต่อการปฏิบัติภารกิจขององค์กร
   - กระบวนการที่มีกระบวนการสำคัญอันเป็นความลับหรือกระบวนที่เกี่ยวกับเทคโนโลยีที่มีสิทธิ์ความเป็นเจ้าของกระบวนการที่สำคัญสำหรับองค์กรที่จำเป็นต้องมีเพื่อปฏิบัติตามกฎหมาย กฎระเบียบ หรือข้อผูกพันตามสัญญา
2. ข้อมูล (Information)
   - ข้อมูลสำคัญในระบบสารสนเทศ
   - สารสนเทศที่เป็นข้อมูลบุคคล
   - สารสนเทศที่เป็นข้อมูลเกี่ยวกับยุทธศาสตร์หรือกลยุทธ์ขององค์กร
   - สารสนเทศสำคัญที่มีมูลค่าสูงที่ต้องจัดเก็บรักษา
3. โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure)
   - อุปกรณ์ประมวลผลหลัก
   - อุปกรณ์ที่จัดเก็บข้อมูล
   - อุปกรณ์ที่ในการประมวลผลหรือทำรายการประมวลผล
   - อุปกรณ์ต่อพ่วงระบบคอมพิวเตอร์
   - อุปกรณ์สื่อบันทึกข้อมูล/สื่อจัดเก็บข้อมูล
   - เครือข่ายเชื่อมต่อการสื่อสาร
   - สื่อสัญญาณ
   - อุปกรณ์เครือข่าย

- สื่ออื่น ๆ

4. แอปพลิเคชัน (Applications)
   - ระบบปฏิบัติการ (Operating system)
   - ระบบงานทางธุรกิจ (Business application)
   - ซอฟต์แวร์สำเร็จรูป (Package Software)
   - ซอฟต์แวร์บริการ (Service software)
   - ซอฟต์แวร์สนับสนุนที่ใช้ในการบริหารจัดการและบำรุงรักษาระบบ (Supporting software)
5. บุคลากรและทักษะ (People and skills)
   - ผู้มีอำนาจตัดสินใจ
   - ผู้ใช้งานระบบสารสนเทศ
   - ผู้ปฏิบัติงาน
   - ผู้ดูแลระบบ
   - ผู้พัฒนาระบบ
6. โครงสร้างพื้นฐานทางกายภาพ (Physical Infrastructure)
   - อาคาร สถานที่ตั้ง สภาพแวดล้อมทางกายภาพ
   - พื้นที่การแบ่งเขตโซนภายในสถานที่
   - ระบบสนับสนุนในการดูแลอาคารสถานที่
   - ระบบหรือบริการที่สำคัญ
   - ระบบการสื่อสารโทรคมนาคม
   - อุปกรณ์เครื่องมือสนับสนุนต่าง ๆ
7. โครงสร้าง (Organizational structure)
   - โครงสร้างองค์กรตามสายบังคับบัญชา
   - โครงการหรือระบบภายในองค์กร
   - คณะทำงานหรือบุคคลที่ได้รับมอบหมาย
   - ผู้ให้บริการภายนอก (ผู้ผลิต ผู้ให้บริการ ที่ปรึกษา ฯลฯ)

6.2 เหตุการณ์ความเสี่ยง (Risk Scenario)

เหตุการณ์ความเสี่ยงที่เป็นไปได้หากเหตุการณ์ที่เกิดขึ้นจะมีผลกระทบด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศ ข้อมูลสารสนเทศ รวมไปถึงทรัพย์สินสารสนเทศ/ทรัพยากรอื่น ๆ ขององค์กร และส่งผลให้กระบวนการดำเนินธุรกิจล่าช้าหรือหยุดชะงัก โดยเหตุการณ์ความเสี่ยงประกอบไปด้วย

- ผู้กระทำ (Actor) หมายถึง ผู้ที่สร้างภัยคุกคามหรือผู้ที่ใช้ประโยชน์จากช่องโหว่ที่เกิดขึ้น ผู้กระทำอาจจะเป็นทั้งคนภายในองค์กรหรือคนภายนอกองค์กร

- ประเภทภัยคุกคาม (Threat Type) หมายถึง ชนิดภัยคุกคามซึ่งเป็นปัจจัยที่ไม่พึงประสงค์ที่อาจก่อให้เกิดความเสี่ยง หรือความเสียหายแก่องค์กร ซึ่งภัยคุกคามอาจเกิดจาก สิ่งแวดล้อม มนุษย์ ธรรมชาติ และอาจเกิดจากความตั้งใจหรืออุบัติเหตุ
- เหตุการณ์ (Event) คือ การเกิดหรือการเปลี่ยนแปลงของส่วนหนึ่งส่วนใดของสภาพการณ์/สถานการณ์
- ทรัพย์สินสารสนเทศ/ทรัพยากรต้นเหตุ (Asset (Cause)) คือ ทรัพย์สินสารสนเทศ/ทรัพยากรต้นเหตุที่ทำให้เกิดความเสี่ยง
- ทรัพย์สินสารสนเทศ/ทรัพยากรที่เกิดผลกระทบ (Asset (Effect)) คือ ทรัพย์สินสารสนเทศ/ทรัพยากรที่ได้รับผลกระทบจากความเสี่ยงที่เกิดขึ้น
- เวลา (Time) คือ ช่วงเวลาที่เกิดเหตุการณ์

6.3 ผลกระทบ

ผลกระทบ คือ ผลลัพธ์ของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นจากภัยคุกคาม ซึ่งมีผลกระทบต่อธุรกิจ ผลกระทบนี้อาจสร้างความเสียหายกับทรัพย์สินสารสนเทศในด้านต่างๆ การประเมินผลกระทบอาศัยการประเมินในเชิงคุณภาพซึ่งบอกถึงระดับผลกระทบที่เกิดขึ้นต่อธุรกิจ โดยประเมินแยกในแต่ละด้านทั้งหมด 7 ด้านดังนี้

1. ผลกระทบด้านกลยุทธ์

	ระดับ 1 ต่ำมาก/ เล็กน้อยมาก	ระดับ 2 ต่ำ/เล็กน้อย	ระดับ 3 ปานกลาง	ระดับ 4 สูง/สำคัญ	ระดับ 5 สูงมาก/ รุนแรงมาก
ด้านกลยุทธ์	ไม่มีผลกระทบต่อการบรรลุเป้าหมายเชิงยุทธศาสตร์ของหน่วยงาน	มีผลกระทบเล็กน้อยต่อการบรรลุเป้าหมาย เชิงยุทธศาสตร์ของหน่วยงาน	มีผลกระทบปานกลางต่อการบรรลุเป้าหมายเชิงยุทธศาสตร์ของหน่วยงาน แต่มีแนวทางในการแก้ไขที่สามารถทำได้อย่างรวดเร็ว	ไม่สามารถบรรลุเป้าหมายเชิงยุทธศาสตร์ของหน่วยงาน และมีหรือไม่มีแนวทางแก้ไขในระยะปานกลาง	ไม่สามารถบรรลุเป้าหมายเชิงยุทธศาสตร์ของหน่วยงาน และอาจส่งผลกระทบต่อเป้าหมายเชิงยุทธศาสตร์ขององค์กร

2. ผลกระทบด้านการเงิน

	ระดับ 1 ต่ำมาก/ เล็กน้อยมาก	ระดับ 2 ต่ำ/เล็กน้อย	ระดับ 3 ปานกลาง	ระดับ 4 สูง/สำคัญ	ระดับ 5 สูงมาก/ รุนแรงมาก
ความเสียหายต่อครั้ง จากเหตุการณ์ที่เกิดขึ้น	น้อยกว่าหรือเท่ากับ 1 หมื่นบาท	มากกว่า 1 หมื่น ถึง 5 หมื่นบาท	มากกว่า 5 หมื่น ถึง 3 แสนบาท	มากกว่า 3 แสน ถึง 6 แสนบาท	มากกว่า 6 แสนบาท

3. ผลกระทบด้านชื่อเสียง

	ระดับ 1 ต่ำมาก/ เล็กน้อยมาก	ระดับ 2 ต่ำ/เล็กน้อย	ระดับ 3 ปานกลาง	ระดับ 4 สูง/สำคัญ	ระดับ 5 สูงมาก/ รุนแรงมาก
ชื่อเสียงองค์กร	มีการเผยแพร่ข่าวในวงจำกัดภายในองค์กร แต่ไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กร	มีการเผยแพร่ข่าวในวงจำกัด และมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กรบ้างเล็กน้อย	มีการเผยแพร่ข่าวในวงกว้างสำหรับสื่อต่างๆ และมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กร ซึ่งสามารถชี้แจงหรือแก้ไขได้ในระยะสั้น	มีการเผยแพร่ข่าวในวงกว้างสำหรับสื่อต่างๆ และมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กร ซึ่งสามารถชี้แจงหรือแก้ไขได้ในระยะปานกลาง	มีการพาดหัวข่าวในสื่อต่างๆ อย่างต่อเนื่องและมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กรในระดับสูงมาก ซึ่งไม่สามารถชี้แจงหรือแก้ไขได้

4. ผลกระทบด้านเทคโนโลยีสารสนเทศ

	ระดับ 1 ต่ำมาก/ เล็กน้อยมาก	ระดับ 2 ต่ำ/เล็กน้อย	ระดับ 3 ปานกลาง	ระดับ 4 สูง/สำคัญ	ระดับ 5 สูงมาก/ รุนแรงมาก
ระยะเวลาที่ระบบงาน IT หยุดชะงัก	ระบบงาน IT มีปัญหาที่ไม่สำคัญมีการหยุดชะงักน้อยกว่าครึ่ง ชม. โดยไม่ต้องพึ่งระบบสำรอง/แผนความต่อเนื่องทางธุรกิจด้าน IT	ระบบงาน IT มีปัญหาเล็กน้อย ทำให้หยุดชะงักครึ่ง ชม. ถึง 4 ชม. โดยสามารถใช้ระบบสำรอง/แผนความต่อเนื่องทางธุรกิจด้าน IT	ระบบงาน IT มีปัญหา/เสียหายทำให้ต้องหยุดชะงักมากกว่า 4 ถึง 8 ชม. โดยสามารถใช้ระบบสำรอง/แผนความต่อเนื่องทางธุรกิจด้าน IT ได้เริ่มหาวิธีการจัดการในการติดต่อกับผู้ให้บริการ	ระบบงาน IT มีปัญหา/เสียหายมากทำให้ต้องหยุดชะงักมากกว่า 8 ชม. โดยต้องไปใช้ศูนย์คอมพิวเตอร์สำรอง/แผนความต่อเนื่องทางธุรกิจด้าน IT	ระบบงาน IT มีปัญหา/เสียหายอย่างรุนแรงโดยไม่สามารถใช้ระบบสำรองและศูนย์คอมพิวเตอร์สำรองแต่ยังคงใช้แผนความต่อเนื่องทางธุรกิจด้าน IT ได้

5. ผลกระทบด้านกฎหมาย / กฎระเบียบ

	ระดับ 1 ต่ำมาก/ เล็กน้อยมาก	ระดับ 2 ต่ำ/เล็กน้อย	ระดับ 3 ปานกลาง	ระดับ 4 สูง/สำคัญ	ระดับ 5 สูงมาก/ รุนแรงมาก
ด้านกฎหมาย/กฎระเบียบ	ไม่ปฏิบัติตามกฎหมาย/กฎระเบียบ หรือข้อสัญญาเล็กน้อยและสามารถแก้ไขได้ในระยะเวลาอันสั้น โดยหน่วยงานตนเอง	ไม่ปฏิบัติตามกฎหมาย/กฎระเบียบ หรือข้อสัญญาที่มีความสำคัญ แต่สามารถแก้ไขได้โดยต้องร่วมมือกับหน่วยงานอื่น	ไม่ปฏิบัติตามกฎหมาย/กฎระเบียบ หรือข้อสัญญาที่มีความสำคัญ และเป็นเหตุให้ต้องเสียค่าปรับ/เงินเพิ่ม	ไม่ปฏิบัติตามกฎหมาย/กฎระเบียบ หรือข้อสัญญาที่มีความสำคัญ และผลกระทบต่อองค์กรทั้งในด้านการเงินและชื่อเสียง	ไม่ปฏิบัติตามกฎหมาย/กฎระเบียบ หรือข้อสัญญาที่มีความสำคัญ และผลกระทบต่อองค์กรอย่างรุนแรง ทั้งในด้านการเงินและชื่อเสียง

6. ผลกระทบด้านการดำเนินงาน

	ระดับ 1 ต่ำมาก/ เล็กน้อยมาก	ระดับ 2 ต่ำ/เล็กน้อย	ระดับ 3 ปานกลาง	ระดับ 4 สูง/สำคัญ	ระดับ 5 สูงมาก/ รุนแรงมาก
ด้านการดำเนินงาน	มีผลกระทบต่อกระบวนการดำเนินงานในระดับส่วนงาน	มีผลกระทบต่อกระบวนการดำเนินงาน และส่งผลกระทบระดับกอง	มีผลกระทบต่อกระบวนการดำเนินงาน และส่งผลกระทบต่อระดับหน่วยงาน และ/หรือเริ่มส่งผลกระทบต่อผู้ใช้น้ำ	มีผลกระทบต่อกระบวนการดำเนินงาน และส่งผลกระทบต่อหน่วยงานอื่นภายในองค์กร และ/หรือผู้ใช้น้ำ	มีผลกระทบต่อกระบวนการดำเนินงาน และส่งผลกระทบต่อหน่วยงานอื่น ทั้งภายในและภายนอกองค์กร และ/หรือผู้ใช้น้ำอย่างรุนแรง

7. ผลกระทบด้านความปลอดภัยและสุขอนามัย

	ระดับ 1 ต่ำมาก/ เล็กน้อยมาก	ระดับ 2 ต่ำ/เล็กน้อย	ระดับ 3 ปานกลาง	ระดับ 4 สูง/สำคัญ	ระดับ 5 สูงมาก/ รุนแรงมาก
ด้านความปลอดภัยและสุขอนามัย	เกิดเหตุการณ์ แต่ไม่ก่อให้เกิดการบาดเจ็บ	ก่อให้เกิดการบาดเจ็บเล็กน้อยที่สามารถรักษาได้ในระดับปฐมพยาบาล	เกิดการบาดเจ็บโดยต้องนำส่งโรงพยาบาล	อาจเป็นเหตุให้เกิด/เกิดการบาดเจ็บสาหัสหรือพิการ	อาจเป็นเหตุให้เกิด/เกิดการเสียชีวิต

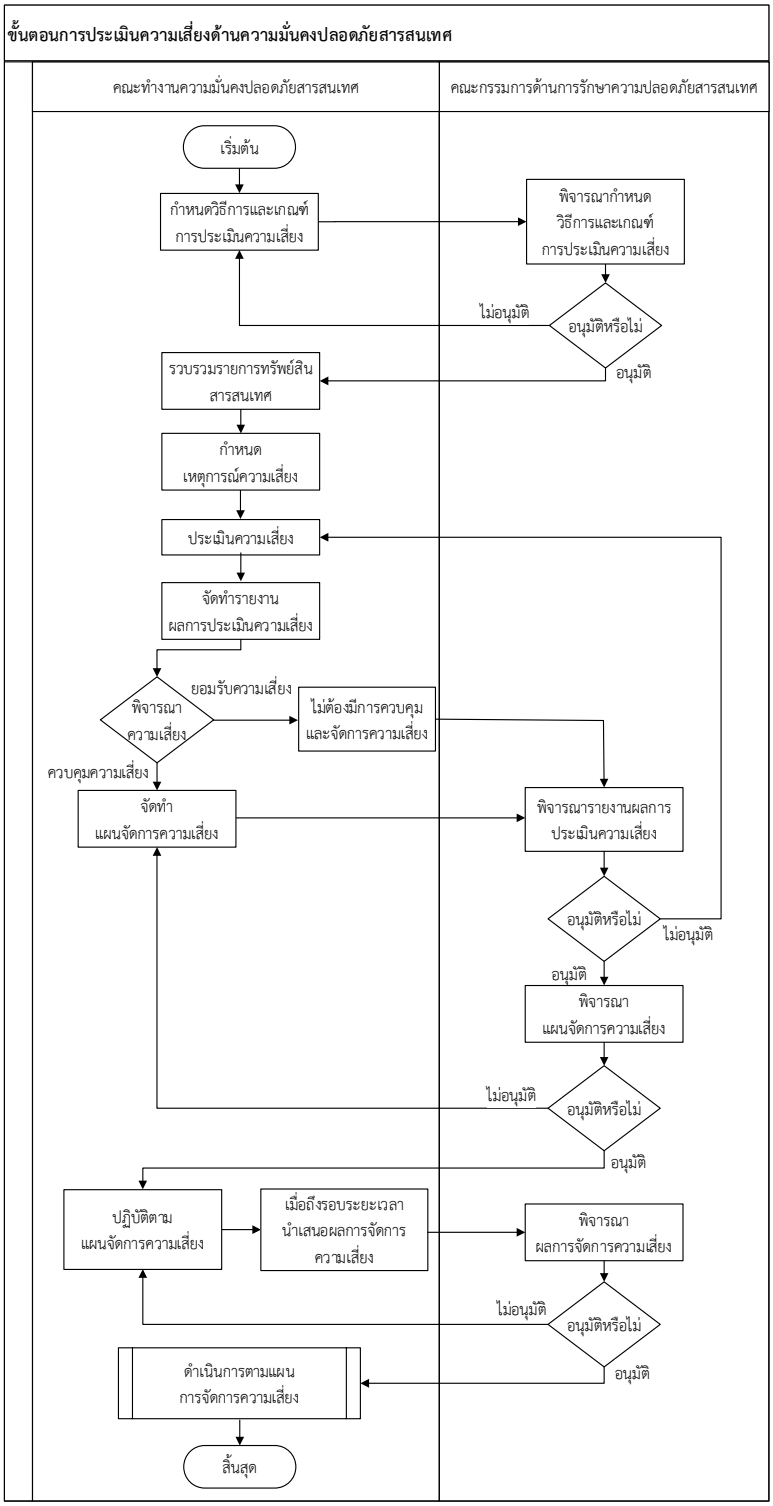
6.4 การประเมินความเสี่ยง

การประเมินความเสี่ยงประกอบด้วยองค์ประกอบสององค์ประกอบ คือ องค์ประกอบที่หนึ่ง: โอกาสเกิด และผลกระทบจากเหตุการณ์ความเสี่ยง ดังนั้น การเรียนรู้หรือรับทราบถึงการเปลี่ยนแปลงใด ที่เกิดขึ้นจะทำให้มีโอกาสในการดำเนินการจัดการกับความเสี่ยงมากยิ่งขึ้น ซึ่งทางเลือกสำหรับการจัดการกับความเสี่ยง มีทั้งการหลีกเลี่ยงไม่ให้เกิดความเสี่ยง การยอมรับความเสี่ยง การควบคุมความเสี่ยง และการถ่ายโอนความเสี่ยง

เมื่อระบุระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ทำให้ความเสี่ยงจากการประเมินสามารถแบ่งออกได้เป็นความเสี่ยงที่ยอมรับได้และความเสี่ยงที่ไม่สามารถยอมรับได้ เมื่อกำหนดแนวทางในการจัดการแล้วพบว่าระดับความเสี่ยงยังคงมากกว่าระดับความเสี่ยงที่ยอมรับได้ เราจึงเรียก ความเสี่ยงนั้นว่า “ความเสี่ยงที่เหลืออยู่” (Residual Risk)

7. ขั้นตอนการดำเนินงาน

7.1 ขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ



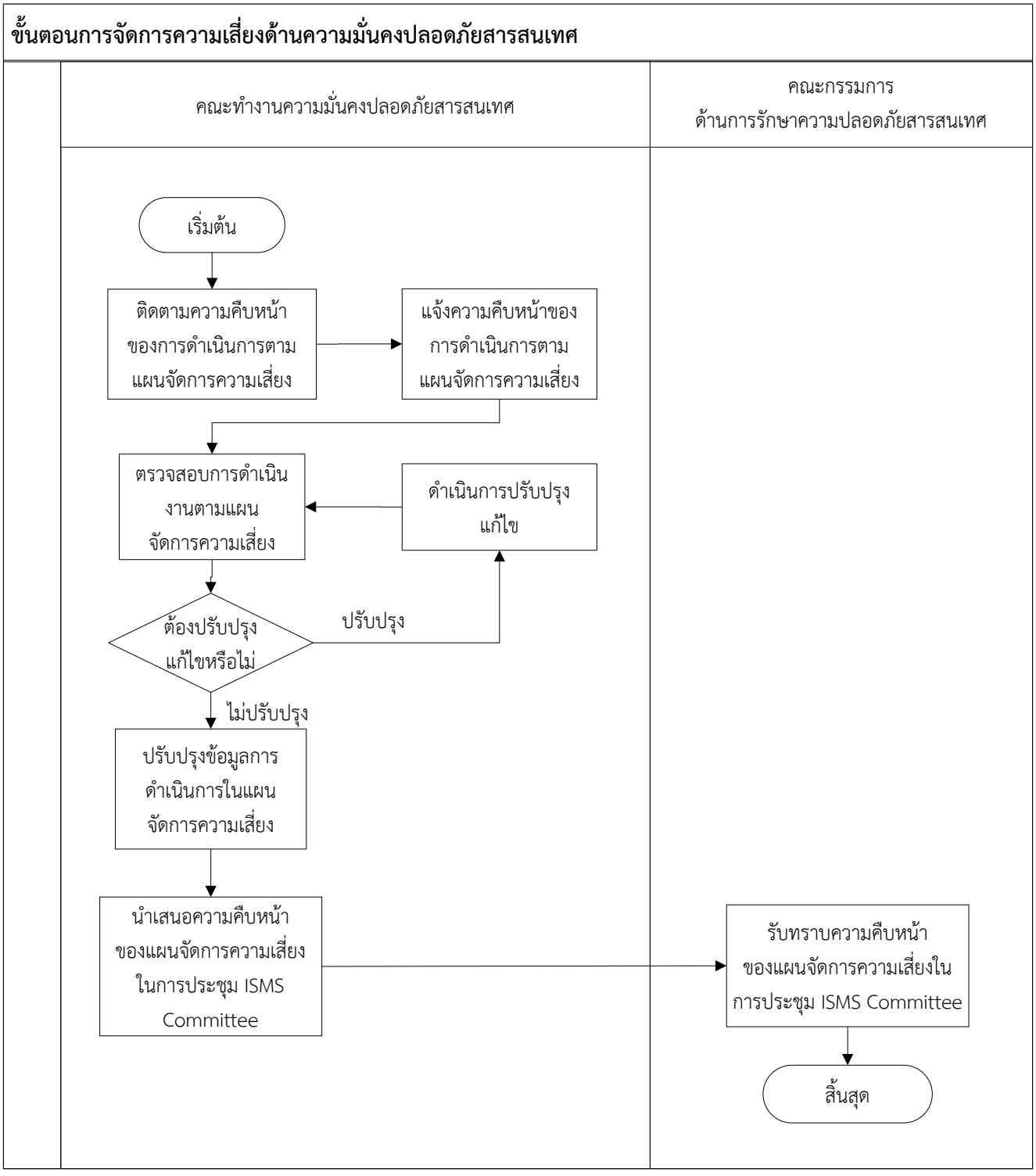
7.2 คำอธิบายขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ลำดับที่	ขั้นตอน	คำอธิบาย
1	กำหนดวิธีการและเกณฑ์การประเมินความเสี่ยง	คณะทำงานฯกำหนดวิธีการและเกณฑ์การประเมินความเสี่ยง เมื่อถึงรอบการประเมินความเสี่ยงหรือเมื่อมีการเปลี่ยนแปลงที่เป็นนัยสำคัญ รวมถึงเมื่อมีปัจจัยภายในหรือภายนอกที่ส่งผลกระทบต่อระบบ ISMS อย่างมีนัยสำคัญ
2	พิจารณากำหนดวิธีการและเกณฑ์การประเมินความเสี่ยง	คณะกรรมการฯพิจารณาวิธีการและเกณฑ์การประเมินความเสี่ยง
3	พิจารณาอนุมัติหรือไม่	คณะกรรมการฯพิจารณาอนุมัติหรือไม่ ▪ หากไม่อนุมัติเกณฑ์การประเมินความเสี่ยง ให้ดำเนินการตามข้อ 1 ▪ หากอนุมัติเกณฑ์การประเมินความเสี่ยง ให้ดำเนินการตามข้อ 4
4	รวบรวมทรัพย์สินสารสนเทศ	คณะทำงานฯดำเนินการรวบรวมทรัพย์สินสารสนเทศที่อยู่ภายในขอบเขต อ้างอิงขั้นตอนการประเมินความเสี่ยงข้อ 8.1
5	กำหนดเหตุการณ์ความเสี่ยง	คณะทำงานฯดำเนินการกำหนดเหตุการณ์ความเสี่ยง (Risk Scenario) อ้างอิงขั้นตอนการประเมินความเสี่ยงข้อ 8.2
6	ประเมินความเสี่ยง	คณะทำงานฯดำเนินการประเมินความเสี่ยง ดังนี้ 1. ระบุการควบคุมปัจจุบัน (Existing Control) โดยอ้างอิงขั้นตอนการประเมินความเสี่ยงข้อ 8.3 2. ประเมินหาค่าผลกระทบที่สูงสุดจากผลการประเมินผลกระทบทั้ง 7 ด้าน อ้างอิงขั้นตอนการประเมินความเสี่ยงข้อ 8.4 3. ประเมินโอกาสเกิดเหตุการณ์ (Likelihood) เพื่อหาค่าระดับความเสี่ยง (Risk Level) อ้างอิงขั้นตอนการประเมินความเสี่ยงข้อ 8.5 4. จัดลำดับความเสี่ยง อ้างอิงขั้นตอนการประเมินความเสี่ยงข้อ 8.6

		5. พิจารณาระดับความเสี่ยงกับเกณฑ์การยอมรับความเสี่ยง อ้างอิงขั้นตอนการประเมินความเสี่ยง ข้อ 8.7
7	จัดทำรายงานผลการประเมินความเสี่ยง	คณะทำงานฯจัดทำรายงานผลการประเมินความเสี่ยง
8	พิจารณาความเสี่ยง	คณะทำงานฯพิจารณาความเสี่ยงที่ยอมรับได้หรือต้องควบคุม โดยอ้างอิงขั้นตอนการประเมินความเสี่ยงข้อ 8.6 ■ หากเป็นความเสี่ยงที่ต้องควบคุม ให้ดำเนินการตามข้อ 9 ■ หากเป็นความเสี่ยงที่ยอมรับได้ ไม่ต้องมีการควบคุมและจัดการความเสี่ยง
9	จัดทำแผนจัดการความเสี่ยง	คณะทำงานฯจัดทำแผนจัดการความเสี่ยง
10	พิจารณารายงานผลการประเมินความเสี่ยง	คณะกรรมการฯพิจารณารายงานผลการประเมินความเสี่ยง
11	พิจารณาอนุมัติหรือไม่	คณะกรรมการฯพิจารณาอนุมัติหรือไม่ ■ หากไม่อนุมัติรายงานผลการประเมินความเสี่ยง ให้ดำเนินการตามข้อ 6 ■ หากอนุมัติรายงานผลการประเมินความเสี่ยง ให้ดำเนินการตามข้อ 12
12	พิจารณาแผนจัดการความเสี่ยง	คณะกรรมการฯพิจารณาแผนจัดการความเสี่ยง
13	พิจารณาอนุมัติหรือไม่	คณะกรรมการฯพิจารณาอนุมัติหรือไม่ ■ หากไม่อนุมัติแผนจัดการความเสี่ยง ให้ดำเนินการตามข้อ 9 ■ หากอนุมัติแผนจัดการความเสี่ยง ให้ดำเนินการตามข้อ 14
14	ปฏิบัติตามแผนจัดการความเสี่ยง	คณะทำงานฯปฏิบัติตามแผนจัดการความเสี่ยง
15	เมื่อถึงรอบระยะเวลานำเสนอผลการจัดการความเสี่ยง	คณะทำงานฯนำเสนอผลการจัดการความเสี่ยง
16	พิจารณาผลการจัดการความเสี่ยง	คณะกรรมการฯพิจารณาผลการจัดการความเสี่ยง

17	พิจารณาอนุมัติหรือไม่	คณะกรรมการฯพิจารณาอนุมัติหรือไม่ ■ หากไม่อนุมัติผลการจัดการความเสี่ยง ให้ดำเนินการตามข้อ 14 ■ หากอนุมัติผลการจัดการความเสี่ยง ให้ดำเนินการตามข้อ 18
18	ดำเนินการตามแผนการจัดการความเสี่ยง	คณะทำงานฯดำเนินการตามแผนการจัดการความเสี่ยง

7.3 ขั้นตอนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ



7.4 คำอธิบายขั้นตอนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ลำดับที่	ขั้นตอน	คำอธิบาย
1	ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	คณะทำงานฯติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง
2	แจ้งความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	คณะทำงานฯแจ้งความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง
3	ตรวจสอบการดำเนินงานตามแผนจัดการความเสี่ยง	คณะทำงานฯตรวจสอบการดำเนินงานตามแผนจัดการความเสี่ยง
4	ต้องปรับปรุงแก้ไขหรือไม่	คณะทำงานพิจารณาว่าต้องปรับปรุงแก้ไขหรือไม่ ▪ หากต้องปรับปรุงแก้ไข ให้ดำเนินการตามข้อ 5 คณะทำงานดำเนินการปรับปรุงแก้ไขตามแผนจัดการความเสี่ยงใหม่อีกครั้ง ▪ หากไม่ต้องปรับปรุงแก้ไข ให้ดำเนินการตามข้อ 6
5	ดำเนินการปรับปรุงแก้ไข	คณะทำงานฯดำเนินการปรับปรุงแก้ไขตามแผนจัดการความเสี่ยง
6	ปรับปรุงข้อมูลการดำเนินการในแผนจัดการความเสี่ยง	คณะทำงานฯปรับปรุงข้อมูลการดำเนินการในแผนจัดการความเสี่ยง
7	นำเสนอความคืบหน้าของแผนจัดการความเสี่ยงในการประชุม ISMS Committee	คณะทำงานฯนำเสนอความคืบหน้าของแผนจัดการความเสี่ยงในการประชุม ISMS Committee
8	รับทราบความคืบหน้าของแผนจัดการความเสี่ยงในการประชุม ISMS Committee	คณะกรรมการฯรับทราบความคืบหน้าของแผนจัดการความเสี่ยงในการประชุม ISMS Committee

8. ขั้นตอนการประเมินความเสี่ยง

8.1 รวบรวมรายการทรัพย์สินสารสนเทศ

การรวบรวมข้อมูลและจัดกลุ่มรายการทรัพย์สินสารสนเทศที่อยู่ในขอบเขตการประเมินความเสี่ยง โดยสามารถจัดรายชื่อเดียวกันในส่วนของกลุ่มรายการทรัพย์สินที่ทำงานในลักษณะเดียวกันหรือเป็นทรัพย์สินประเภทเดียวกัน และการระบุประเภททรัพย์สินโดยอ้างอิง 5.1

ตารางที่ 1 แสดงตัวอย่างรายการทรัพย์สินสารสนเทศ

ลำดับ	ทะเบียนทรัพย์สิน	กลุ่มรายการทรัพย์สิน	ประเภททรัพย์สิน	สถานที่	หน่วยงาน
No.	Asset Inventory	Identification of Asset	Types of Asset	Location	Asset Owner
1	ข้อมูล Network Diagram	ข้อมูล Diagram	Information	ศูนย์คอมพิวเตอร์หลัก	กองบริหารเครื่องแม่ข่าย
2	HP ProLiant DL380 GS for CIS (Report)	เครื่องแม่ข่าย	IT Infrastructure	ศูนย์คอมพิวเตอร์หลัก	กองบริหารเครื่องแม่ข่าย

8.2 กำหนดเหตุการณ์ความเสี่ยง (Risk Scenario)

เหตุการณ์ความเสี่ยงที่เป็นไปได้ที่ก่อให้เกิดเหตุการณ์ที่สร้างความเสียหายต่อทรัพย์สินสารสนเทศ โดยเหตุการณ์ความเสี่ยงจะเกิดขึ้นนั้นโดยอ้างอิง 5.2

ตารางที่ 2 แสดงตัวอย่างการกำหนดเหตุการณ์ความเสี่ยง

ลำดับ	ผู้กระทำ	ประเภทภัยคุกคาม/ช่องโหว่	เหตุการณ์	ทรัพย์สินต้นเหตุ	ทรัพย์สินที่เกิดผลกระทบ	เวลา	เหตุการณ์ความเสี่ยง
No.	Actor	Threat/ Vulnerability Type	Event	Asset (Cause)	Asset (Effect)	Time	Risk Scenario
1	ผู้ปฏิบัติงาน	ไม่มีการสื่อสารที่ดีต่อผู้ปฏิบัติงาน	ผู้ปฏิบัติงานไม่ทราบถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จนทำให้เกิดการเสียหายต่ออุปกรณ์รักษาความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม อุปกรณ์รักษาความมั่นคงปลอดภัยทางเครือข่าย อุปกรณ์เครือข่าย เครื่องแม่ข่ายของระบบสารสนเทศลูกค้า (CIS) ,ระบบ SAP และระบบสารบรรณอิเล็กทรอนิกส์ จนกระทบกับผู้ใช้บริการ	Process : 1.นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของการประปานครหลวง พ.ศ.๒๕๕๘ People and skills : 1. เจ้าหน้าที่กองบริหารเครื่องแม่ข่าย 2. เจ้าหน้าที่กองบริหารเครือข่ายสื่อสารและความมั่นคงสารสนเทศ 3. ผู้ดูแลห้องดาต้าเซ็นเตอร์ (เจ้าหน้าที่ส่วนจัดการศูนย์คอมพิวเตอร์)	Information : 1.ข้อมูลการตั้งค่าระบบ 2.ข้อมูลสำรองของระบบ 3.ข้อมูล Diagram Applications : 1.ระบบปฏิบัติการ 2.โปรแกรมสำรองข้อมูล IT Infrastructure : 1.เครื่องแม่ข่าย 2..Storage 3. Switch (CORE) Physical Infrastructure : 1.Access Control 2.ระบบกล้องวงจรปิด	เวลาที่เกิดเหตุเป็นช่วงเวลาที่สำคัญเพราะมีผู้เข้าใช้งานในระบบ การแก้ไขปัญหาต้องใช้เวลานาน ทราบถึงผลกระทบได้ทันที	ผู้ปฏิบัติงานไม่ทราบถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จนทำให้เกิดการเสียหายต่ออุปกรณ์รักษาความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม อุปกรณ์รักษาความมั่นคงปลอดภัยทางเครือข่าย อุปกรณ์เครือข่าย เครื่องแม่ข่ายของระบบสารสนเทศลูกค้า (CIS) ,ระบบ SAP และระบบสารบรรณอิเล็กทรอนิกส์ เพราะสาเหตุไม่มีการสื่อสารที่ดีต่อผู้ปฏิบัติงาน

8.3 ระบุการควบคุมปัจจุบัน (Existing Control)

ดำเนินการระบุการควบคุมปัจจุบันที่รองรับเหตุการณ์ความเสี่ยงที่กำหนดไว้

ตารางที่ 3 แสดงตัวอย่างการระบุการควบคุมปัจจุบัน

เหตุการณ์ความเสี่ยง	การควบคุมปัจจุบัน
Risk Scenario	Existing Control
ผู้ปฏิบัติงานไม่ทราบถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จนทำให้เกิดการเสียหายต่ออุปกรณ์รักษาความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม อุปกรณ์รักษาความมั่นคงปลอดภัยทางเครือข่าย อุปกรณ์เครือข่าย เครื่องแม่ข่ายของระบบสารสนเทศลูกค้า (CIS) ,ระบบ SAP และระบบสารบรรณอิเล็กทรอนิกส์ เพราะสาเหตุไม่มีการสื่อสารที่ดีต่อผู้ปฏิบัติงาน	เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของการประปานครหลวง พ.ศ.๒๕๕๘ จะมีการนำเสนอว่าผู้มีอำนาจ เพื่อเสนอขออนุมัติและประกาศใช้ โดยผู้ปฏิบัติงานจะทราบหลังจากมีการประกาศใช้ เพื่อนำมาปฏิบัติและควบคุมต่อไป โดยนโยบายจะมีการทบทวนตามรอบที่กำหนดไว้

8.4 ประเมินค่าผลกระทบ

ดำเนินการประเมินค่าผลกระทบ 7 ด้านโดยอ้างอิง 5.3 โดยนำค่าผลกระทบที่สูงที่สุดมาเป็นค่าผลกระทบหลักของเหตุการณ์ความเสี่ยงนั้น

ตารางที่ 4 แสดงตัวอย่างการประเมินค่าผลกระทบ

เหตุการณ์ความเสี่ยง	การควบคุมปัจจุบัน	ผลกระทบแต่ละด้าน							ระดับผลกระทบ
Risk Scenario	Existing Control	กลยุทธ์	การเงิน	ชื่อเสียง	เทคโนโลยีสารสนเทศ	กฎหมาย/กฎระเบียบ	การดำเนินงาน	ความปลอดภัยและสุขอนามัย	Impact
ผู้ปฏิบัติงานไม่ทราบถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จนทำให้เกิดการเสียหายต่ออุปกรณ์รักษาความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม อุปกรณ์รักษาความมั่นคงปลอดภัยทางเครือข่าย อุปกรณ์เครือข่าย เครื่องแม่ข่ายของระบบสารสนเทศลูกค้า (CIS) , ระบบ SAP และระบบสารบรรณอิเล็กทรอนิกส์ เพราะสาเหตุไม่มีการสื่อสารที่ดีต่อผู้ปฏิบัติงาน	เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของการประปานครหลวง พ.ศ.๒๕๕๘ จะมีการนำเสนอว่าผู้มีอำนาจ เพื่อเสนอขออนุมัติและประกาศใช้ โดยผู้ปฏิบัติงานจะทราบหลังจากมีการประกาศใช้ เพื่อนำมาปฏิบัติและควบคุมต่อไป โดยนโยบายจะมีการทบทวนตามรอบที่กำหนดไว้	2	2	2	2	2	2	-	2

8.5 ประเมินโอกาสเกิดเหตุการณ์

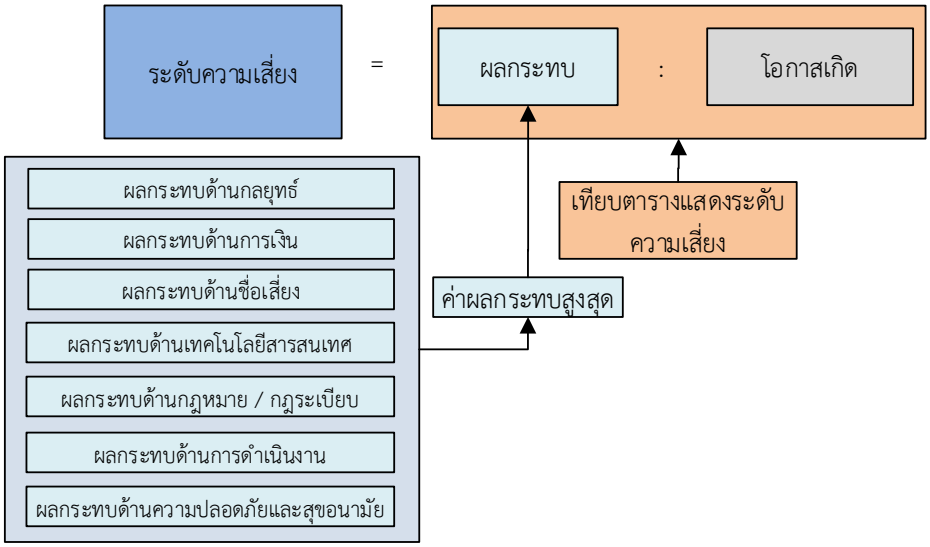
กำหนดโอกาสเกิด (Likelihood) แบ่งเป็น 5 ระดับ ดังตารางต่อไปนี้

ตารางที่ 5 แสดงระดับโอกาสเกิด

คะแนน (Score)	โอกาสเกิดเหตุการณ์ (Likelihood)
5 - สูงมาก	มีโอกาสเกิดเหตุการณ์มากกว่า 12 ครั้งต่อปี
4 - สูง	มีโอกาสเกิดเหตุการณ์ตั้งแต่ 5 ถึง 12 ครั้งต่อปี
3 - ปานกลาง	มีโอกาสเกิดเหตุการณ์ตั้งแต่ 3 ถึง 4 ครั้งต่อปี
2 - น้อย	มีโอกาสเกิดเหตุการณ์ไม่เกิน 2 ครั้งต่อปี
1 - น้อยมาก	มีโอกาสเกิดเหตุการณ์ 1 ครั้งต่อปี

8.6 ระดับความเสี่ยง

ระดับความเสี่ยง (Risk Level) เกิดจากโอกาสเกิดเหตุการณ์เมื่อทรัพย์สินสารสนเทศได้รับผลกระทบ สามารถประเมินได้จากสมการ ดังนี้



ซึ่งสามารถสรุปได้ดังตารางต่อไปนี้

ตารางที่ 6 แสดงระดับความเสี่ยงที่มีผลต่อทรัพย์สินสารสนเทศ

ระดับความเสี่ยง (RISK EXPOSURE)		โอกาสเกิด (LIKELIHOOD)				
		1 - น้อยมาก	2 - น้อย	3 - ปานกลาง	4 - สูง	5 - สูงมาก
ผลกระทบ (IMPACT)	5 - สูงมาก	M5	H10	E15	E20	E25
	4 - สูง	M4	M8	H12	E16	E20
	3 - ปานกลาง	L3	M6	M9	H12	H15
	2 - น้อย	L2	L4	L6	M8	M10
	1 - น้อยมาก	L1	L2	L3	L4	L5

ระดับความเสี่ยงที่ยอมรับได้

เกณฑ์ระดับความเสี่ยง		การจัดการความเสี่ยง	เกณฑ์ระดับความเสี่ยง
E :Extremely	ระดับความเสี่ยงสูงมาก	กำหนดแผนจัดการความเสี่ยง	E15, E16, E20, E25
H : High	ระดับความเสี่ยงสูง	กำหนดแผนจัดการความเสี่ยง	H10, H12, H15
M : Moderate	ระดับความเสี่ยงปานกลาง	กำหนดแผนจัดการความเสี่ยง	M4, M5, M6, M8, M9, M10
L : Low	ระดับความเสี่ยงต่ำ	ยอมรับความเสี่ยง	L1, L2, L3, L4, L5, L6

ตารางที่ 7 แสดงตัวอย่างการประเมินโอกาสเกิดเหตุการณ์และการจัดลำดับความเสี่ยง

ระดับผลกระทบ	โอกาสเกิดเหตุการณ์	ระดับความเสี่ยง
Impact	Likelihood	Risk Level
2	1	L2

8.7 พิจารณาระดับความเสี่ยงกับเกณฑ์การยอมรับความเสี่ยง

เมื่อได้ค่าของระดับความเสี่ยงจากทรัพย์สินสารสนเทศต่างๆ แล้ว คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001 จะต้องพิจารณาระดับความเสี่ยงที่ยอมรับได้

ในที่นี้คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001 ได้ลงมติร่วมกันยอมรับความเสี่ยงที่คำนวณได้ระดับ L1, L2, L3, L4, L5, L6 และเป็นความเสี่ยงที่มีการควบคุม ดังนั้นระบุในช่อง “การตอบสนองความเสี่ยง” ว่า “ยอมรับ (TAKE)”

หากระดับความเสี่ยงที่คำนวณได้ M4, M5, M6, M8, M9, M10, H10, H12, H15, E15, E16, E20, E25 หรือความเสี่ยงนั้นไม่มีการดำเนินการควบคุมในปัจจุบัน ให้พิจารณาทางเลือกสำหรับการตอบสนองความเสี่ยง และระบุในช่อง “การตอบสนองความเสี่ยง” ทางเลือกสำหรับการจัดการความเสี่ยง มีดังนี้

1. ยอมรับ (TAKE)
2. จัดการ (TREAT)
3. ถ่ายโอน (TRANSFER)
4. หลีกเลี่ยง (TERMINATE)

8.8 กำหนดแผนจัดการความเสี่ยง

การจัดลำดับความสำคัญของการตอบสนองความเสี่ยงนิยามไว้ ดังนี้

- หากระดับความเสี่ยงอยู่ในระดับสีแดง เป็นความเสี่ยงสูงมาก ต้องดำเนินการจัดการเป็นอับดับแรก ซึ่งโดยต้องเริ่มต้นการปรับปรุงนั้นทันที หรือไม่เกิน 1 เดือน นับจากวันที่ได้รับอนุมัติแผนจัดการความเสี่ยง
- หากระดับความเสี่ยงอยู่ในระดับสีส้ม เป็นความเสี่ยงสูง ควรเริ่มต้นดำเนินการภายใน 2 เดือน นับจากวันที่ได้รับอนุมัติแผนจัดการความเสี่ยง
- หากระดับความเสี่ยงอยู่ในระดับสีเหลือง เป็นความเสี่ยงปานกลาง ควรเริ่มต้นดำเนินการภายใน 3 เดือนนับจากวันที่ได้รับอนุมัติแผนจัดการความเสี่ยง
- หากระดับความเสี่ยงอยู่ในระดับสีเขียว เป็นความเสี่ยงระดับต่ำ อยู่ในระดับที่ยอมรับได้โดยไม่ต้องมีการบริหารจัดการความเสี่ยงเพิ่มเติม

หากพบว่า ความเสี่ยงอยู่ในระดับเดียวกันเป็นจำนวนมาก ให้ดำเนินการจัดการความเสี่ยง สำหรับความเสี่ยงที่มีค่าผลกระทบ (Impact) สูงก่อนและดำเนินการตามระดับของค่าผลกระทบเป็นหลัก หากแผนจัดการความเสี่ยงใดสามารถดำเนินการได้ ให้ดำเนินการตามแผนจัดการความเสี่ยงนั้นทันที

ทั้งนี้สำหรับระดับความเสี่ยงใดที่ไม่ได้กำหนดให้ต้องมีการควบคุมระดับความเสี่ยง ไม่ต้องกำหนดแผนจัดการความเสี่ยงและไม่ต้องวัดระดับความเสี่ยงที่เหลืออยู่

8.9 ระดับความเสี่ยงที่หลงเหลือ

กรณีที่มีการจัดการ (TREAT) ด้วยการควบคุม (Controlling) หรือหลีกเลี่ยง (TERMINATE) ไม่ให้เกิดความเสี่ยง หรือหลีกเลี่ยง (TERMINATE) ความเสี่ยง ภายหลังจากการกำหนดแผนการจัดการความเสี่ยงแล้วให้ทำการคำนวณค่าความเสี่ยงที่เหลืออยู่อีกครั้งโดยการกรอกข้อมูลเกี่ยวกับ

1. ระดับความเสียหายหลังทำการจัดการความเสี่ยง
2. โอกาสเกิดเหตุการณ์หลังทำการจัดการความเสี่ยง

หากภายหลังการควบคุมความเสี่ยงแล้ว ระดับความเสี่ยงคำนวณได้ระดับ L1, L2, L3, L4, L5, L6 ให้ถือว่าระดับความเสี่ยงอยู่ในเกณฑ์ที่ยอมรับได้ ระดับความเสี่ยงที่นอกเหนือจากนี้ให้ถือเป็นความเสี่ยงที่เหลืออยู่ และต้องนำความเสี่ยงที่คงเหลือเสนอคณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001 เพื่อพิจารณาและรับทราบ

9. การสื่อสารและการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ

ผู้ถ่ายทอดสาร/ผู้รับผิดชอบ	ผู้รับสาร	ประเด็นสื่อสาร	ระดับการเข้าร่วม	รูปแบบ/วิธีการ/ช่องทางการสื่อสาร			การประเมินการรับรู้	
				ภายใน	ภายนอก	กำหนดเวลา	วิธีการประเมิน	กำหนดเวลา
คณะทำงาน ISMS, ฝคท.	- คณะกรรมการ ISMS	- ทบทวนแผนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	- การให้คำปรึกษา - การให้ข้อมูล	การประชุม		เมื่อมีการทบทวนและปรับปรุงแผนการประเมินความเสี่ยงอย่างน้อยปีละครั้ง	รายงานการประชุมคณะทำงานฯ และคณะกรรมการฯ	ไตรมาสที่ 2
คณะทำงาน ISMS, ฝคท.	- คณะความเสี่ยงสายงาน	- รายงานผลการประเมินและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	- การให้ข้อมูล - การมีส่วนร่วม	- ประชุม		ปีละ 1 ครั้ง	รายงานการประชุมสรุปรายงานผลการประเมินและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	ไตรมาสที่ 3

10. การวัด ติดตาม วิเคราะห์ ประเมินผล ตัววัดผลลัพธ์ กระบวนการการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

การประเมินประสิทธิผลของกระบวนการการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยสารสนเทศขององค์กร ดังต่อไปนี้

10.1 ตัวชี้วัด การบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร (Output)

ตัวชี้วัดที่ 1	คณะทำงานได้ทำการ**ทบทวนแผนการประเมิน**ความเสี่ยงแล้วเสร็จตามกำหนด
ผู้ติดตาม วัดผล	คณะความเสี่ยงสายงานเทคโนโลยีดิจิทัล
ข้อมูลประกอบตัววัด	รายงานการประชุมการทบทวนแผนการประเมินความเสี่ยง
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	ทบทวนแล้วเสร็จในไตรมาสที่ 2

10.2 ตัวชี้วัด การบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร (Output)

ตัวชี้วัดที่ 1	คณะทำงานได้**รายงานผล**การบริหารและจัดการความเสี่ยงตามเวลาที่กำหนด
ผู้ติดตาม วัดผล	คณะความเสี่ยงสายงานเทคโนโลยีดิจิทัล
ข้อมูลประกอบตัววัด	รายงานผลการบริหารและจัดการความเสี่ยง
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	ทบทวนแล้วเสร็จในไตรมาสที่ 3

หมายเหตุ : Output เป็นการวัดเชิงปริมาณ

11. การนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล/ จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) การนำผลที่ได้จากการประเมินไปเรียนรู้และจัดการความรู้เพื่อนำไปปรับปรุงและทำนวัตกรรม

11.1 นำผลที่ได้จากรายงานการประเมินความเสี่ยงมาทบทวน นำกระบวนการไปใช้กับการประเมินความเสี่ยงในระบบอื่นๆ ที่อาจจะเกิดผลกระทบต่อการดำเนินงานต่อไป

11.2 นำรายงานการประเมินความเสี่ยงที่เป็นผลลัพธ์ในข้อ 10 รายงานต่อคณะกรรมการด้านความมมั่นคงปลอดภัยสารสนเทศและไซเบอร์

11.3 นำผลที่ได้จากการประเมินไปเรียนรู้และจัดการความรู้ โดยการจัดประชุมเพื่อแลกเปลี่ยนความรู้ นำไปปรับปรุงกระบวนการและจัดทำนวัตกรรมของกระบวนการ ปีละครั้ง

12. สรุป

จากขั้นตอนวิธีการทั้งหมดที่ได้กล่าวมาในเอกสารคู่มือหลักวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศนี้ เป็นเพียงกรอบการดำเนินการประเมินความเสี่ยงซึ่งยังคงต้องรับการพัฒนาอย่างต่อเนื่อง เพราะด้วยเหตุที่ว่าการประเมินความเสี่ยงอาจยังมีจุดบกพร่องหรืออาจไม่มีประสิทธิผลที่เพียงพอหรือเพิ่มเติมเปลี่ยนแปลงอุปกรณ์หรือ

ขอบเขต ดังนั้นหากมีการนำไปใช้งานแล้วและพบว่าหลักวิธีการนี้ยังไม่มีประสิทธิผลเพียงพอ อาจนำหลักวิธีการนี้ไปปรับปรุงต่อได้ในอนาคต

13. โปรแกรมประกอบการประเมิน

วิธีการประเมินความเสี่ยงที่กำหนดมานี้ให้ใช้โปรแกรมประเมินความเสี่ยง ซึ่งจัดทำในรูปแบบไมโครซอฟต์เอ็กเซล อ้างอิงตามเอกสาร Information Security Risk Assessment Sheet เพื่อประเมินความเสี่ยง

14. เอกสารที่เกี่ยวข้อง

1. บริบทองค์กร (Context of the organization) (IS.REF.002)
2. คู่มือหลักวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (IS.HBK.001)
3. รายงานการประเมินความเสี่ยง (Risk Assessment Report) (IS.RPT.001)

15. เอกสารสำหรับบันทึก

1. Information Security Risk Assessment Sheet (IS.FRM.001)