การประเมินความเสี่ยงข้อมูลสารสนเทศ

โดย นายวุฒิไกร พิมพ์หล่อ
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ฝ่ายเทคโนโลยีและสารสนเทศ

ความเสี่ยง

- เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้น ภายในสถานการณ์ที่ไม่แน่นอน และส่งผลกระทบและความเสียหายหรือ ความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อเป้าหมาย และ วัตถุประสงค์ที่กหนด

“ความเสี่ยงของระบบฐานข้อมูลสารสนเทศ”

โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่าหรือเหตุการณ์ซึ่งไม่พึงประสงค์

ขั้นตอนในการประเมินความเสี่ยงข้อมูลสารสนเทศ

- ระบุทรัพย์สินและกระบวนการที่เกี่ยวข้องกับการให้บริการ
- ระบุความเสี่ยงที่อาจเกิดขึ้นและแจกแจงที่มาของความเสี่ยง
- วิเคราะห์ผลกระทบของความเสี่ยงต่อระบบ
- พิจารณาการดำเนินการต่อความเสี่ยง
- สรุปผลการจัดการความเสี่ยงและแผนการตอบสนองความเสี่ยง

ระบุทรัพย์สินและกระบวนการที่เกี่ยวข้องกับการให้บริการ

- การระบุทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ
  - ระบบคอมพิวเตอร์
  - ระบบสนับสนุน
  - ระบบเครือข่าย
  - อื่นๆ

ระบุความเสี่ยงที่อาจเกิดขึ้นและแจกแจงที่มาของความเสี่ยง

- ความเสี่ยงที่ส่งผลกระทบให้กับทรัพย์ที่ระบุไว้
  - การทำงานขัดข้อง
  - การเสียงหาย
  - การสูญหาย
  - ความลับรั่วไหล

วิเคราะห์ผลกระทบของความเสี่ยงต่อระบบ

- พิจารณาจาก ความถี่ที่เกิดหรือโอกาสที่สามารถเกิดเหตุการณ์นั้นขึ้นมาได้
- พิจารณาจาก ระดับความรุนแรง ความเสียหายที่พบเมื่อเกิดเหตุการณ์นั้นขึ้นมาจริงๆ
- ประเมินความเสี่ยงที่มีความสำคัญเร่งด่วน

ตารางแสดงความรุนแรงของความเสี่ยงที่เกิด

ตารางอ้างอิง Impact Level

ผลกระทบหากสูญเสียในด้าน C,I,A					
Impact Level	คะแนน	ความต่อเนื่องของธุรกิจ (I1)	ภาพลักษณ์องค์กร (I2)	ผลกระทบกับระบบอื่นๆ ที่เกี่ยวข้อง ((I3)	กฎหมายหรือข้อบังคับ (I4)
Very High	5	ไม่สามารถให้บริการได้ตามปกติมากกว่า 48 ชม.	ภาพลักษณ์สูญเสียถาวร ผู้รับบริการ หมดความเชื่อถือ ออกสื่อต่างประเทศ	มีผลกระทบกับ มากกว่า 2 ระบบขึ้นไป ไม่สามารถทำงานได้	ขัดต่อข้อกฎหมายหรือพระราชบัญญัติคอมพิวเตอร์
High	4	ไม่สามารถให้บริการได้ตามปกติมากกว่า 24 ถึง 48 ชม.	ส่งผลกับภาพลักษณ์ขององค์กรค่อนข้างสูง ออกสื่อภายในประเทศ	มีผลกระทบกับ 2 ระบบ ไม่สามารถทำงานได้	ขัดต่อนโยบายหรือข้อปฏิบัติขององค์กร
Medium	3	ไม่สามารถให้บริการได้ตามปกติมากกว่า 4 ถึง 24 ชม.	กระทบกับภาพลักษณ์ขององค์กรเล็กน้อย สู่ภายนอก	มีผลกระทบกับ 1 ระบบ ไม่สามารถทำงานได้	ขัดต่อข้อปฏิบัติของหน่วยงาน
Low	2	ไม่สามารถให้บริการได้ตามปกติมากกว่า 2 ถึง 4 ชม.	แทบจะไม่กระทบภาพลักษณ์ขององค์กร รู้กันภายในองค์กร	มีผลกระทบทำให้ระบบอื่นทำงานช้าลง	ขัดต่อกระบวนการในการปฏิบัติงานเฉพาะในทีม
Very Low	1	ไม่สามารถให้บริการได้ตามปกติน้อยกว่า 2 ชม.	ไม่กระทบภาพลักษณ์	ไม่มีผลกระทบกับระบบอื่น	ไม่ขัดต่อกฎข้อบังคับต่างๆ รวมถึงนโยบายและระเบียบปฏิบัติ

ตารางแสดงความถี่ หรือ โอกาสความน่าจะเป็นที่สามารถเกิดความเสี่ยงได้

ตารางอ้างอิง Probability

Probability	คะแนน	Criteria / Description
Almost Certain	5	Threat มีความน่าจะเป็นที่จะเกิดขึ้นได้ประจำ ทุกสัปดาห์หรือบ่อยกว่า
Likely	4	Threat มีความน่าจะเป็นที่จะเกิดขึ้นได้บ่อย ประมาณเดือนละครั้ง
Possible	3	Threat มีความน่าจะเป็นที่จะเกิดขึ้นปานกลาง ประมาณ 3-5 ครั้งในรอบปี
Unlikely	2	Threat มีความน่าจะเป็นที่จะเกิดขึ้นได้ยาก ประมาณ 1–2 ครั้งในรอบปี
Rare	1	Threat มีความน่าจะเป็นที่จะเกิดขึ้นได้ยากมากอาจจะเกิดขึ้น 1-2 ครั้งในรอบ 3 ปี

การคำนวนค่าความเสี่ยง

ตารางอ้างอิง Risk Level

Impact	Rare(1)	Unlikely(2)	Possible(3)	Likely(4)	Almost Certain(5)
Very High(5)	Medium (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
High(4)	Low (4)	Medium (8)	High (12)	High (16)	Extreme (20)
Medium(3)	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)
Low(2)	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)
Very Low(1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

Probability

Risk Level	Required Action
Extreme	**ความเสี่ยงในระดับสูง** ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง และดำเนินการทันที
High	**ความเสี่ยงในระดับค่อนข้างสูงไม่สามารถยอมรับได้** ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง และดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสม
Medium	**ความเสี่ยงในระดับปานกลาง** ทำการติดตามผลความเสี่ยง และพิจารณาปรับปรุงมาตรการควบคมปัจจุบันที่มีอยู่ แต่หากมีเหตุจำเป็นก็สามารถพิจารณายอมรับความเสี่ยงได้
Low	**ความเสี่ยงในระดับที่ต่ำมาก** สามารถยอมรับได้โดยไม่ต้องดำเนินการใดๆ เพิ่มเติมที่มีในปัจจุบัน

การดำเนินการต่อความเสี่ยง

- การดำเนินใดๆต่อความเสี่ยงที่พอ เพื่อลดหรือกำจัดเสี่ยงที่ยังมา

แผนดำเนินการความเสี่ยง Risk Treatment Plan						
Treatment ID	Treatment Explanation	Responsible Person/Dept.	Duration		Status	Actual Filnish Date
			Start	Finish		
	กล้องวงจรปิด ขออนุมัติติดตั้งกล้องวงจรปิดในห้อง Server และดำเนินการติดตั้งกล้องวงจรปิดในห้อง Server	ฝ่ายเทคโนโลยีและสารสนเทศ	21/3/65	8/4/65	กำลังดำเนินการ	5/4/1965
	ไฟฟ้าดับหรือกระชาก จัดทำ QP-ISMS-13 การบริหารจัดการความต่อเนื่องในการดำเนินงานขององค์กร (BCP) และซ่อมแผนแบบ Table Top	ฝ่ายเทคโนโลยีและสารสนเทศ / อาคารสถานที่	21/3/65	30/4/65	กำลังดำเนินการ	22/4/1965
	รหัสผ่าน จัดทำ QP-ISMS-06 การลงทะเบียนผู้ใช้งาน และดำเนินการตรวจสอบ Username และ Password ให้เป็นไปตามมาตรฐาน	ฝ่ายเทคโนโลยีและสารสนเทศ	21/3/65	4/4/65	กำลังดำเนินการ	4/4/1965

ขอบพระคุณครับ