กระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศ
โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ
(Information Asset Inventory)
โรงพยาบาลสันกำแพง

การประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศ เป็นกระบวนการที่สำคัญในการระบุและประเมินความเสี่ยงที่อาจส่งผลกระทบต่อความปลอดภัยและความน่าเชื่อถือของระบบสารสนเทศ โดยมีการวิเคราะห์โอกาสที่จะเกิดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น เพื่อนำไปสู่การจัดการความเสี่ยงอย่างเหมาะสม

ขั้นตอนการประเมินและให้คะแนนความเสี่ยง:

1. การระบุความเสี่ยง (Risk Identification):

ขั้นตอนนี้เกี่ยวข้องกับการระบุเหตุการณ์หรือสถานการณ์ที่อาจเป็นภัยคุกคามต่อระบบสารสนเทศ. ตัวอย่างเช่น การรั่วไหลของข้อมูล, การโจมตีทางไซเบอร์, หรือความล้มเหลวของระบบ

2. การวิเคราะห์ความเสี่ยง (Risk Analysis):

ขั้นตอนนี้เกี่ยวข้องกับการประเมินโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

- **โอกาสที่จะเกิดความเสี่ยง (Likelihood):** การประเมินว่าเหตุการณ์ความเสี่ยงนั้นมีโอกาสเกิดขึ้นมากน้อยเพียงใด.
- **ผลกระทบ (Impact):** การประเมินผลกระทบที่อาจเกิดขึ้นหากความเสี่ยงนั้นเกิดขึ้นจริง.

3. การประเมินค่าความเสี่ยง (Risk Evaluation):

ขั้นตอนนี้เกี่ยวข้องกับการนำผลการวิเคราะห์ความเสี่ยงมาประเมินและจัดลำดับความสำคัญของความเสี่ยง

4. การจัดการความเสี่ยง (Risk Treatment):

ขั้นตอนนี้เกี่ยวข้องกับการกำหนดและดำเนินการตามมาตรการต่างๆ เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

5. การติดตามและทบทวน (Monitoring and Review):

ขั้นตอนนี้เกี่ยวข้องกับการติดตามและทบทวนผลการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามาตรการที่ดำเนินการยังคงมีประสิทธิภาพ

การให้คะแนนความเสี่ยง:

- การให้คะแนนความเสี่ยงมักจะใช้เมทริกซ์ความเสี่ยง (Risk Matrix) ที่แสดงความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
- ระดับความเสี่ยงมักถูกจัดแบ่งเป็นหลายระดับ เช่น ต่ำ ปานกลาง สูง หรือ สูงมาก เพื่อให้สามารถจัดลำดับความสำคัญของความเสี่ยงได้อย่างเหมาะสม

ตัวอย่าง:

ระดับความเสี่ยง	โอกาสที่จะเกิด	ผลกระทบ
ต่ำ (Low)	เกิดขึ้นน้อยมาก	น้อยมาก
ปานกลาง (Medium)	เกิดขึ้นปานกลาง	ปานกลาง
สูง (High)	เกิดขึ้นสูง	สูง
สูงมาก (Very High)	เกิดขึ้นสูงมาก	สูงมาก

ประโยชน์ของการประเมินและให้คะแนนความเสี่ยง:

- ช่วยให้องค์กรสามารถระบุและเข้าใจความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศได้.
- ช่วยให้องค์กรสามารถจัดลำดับความสำคัญของความเสี่ยงและจัดสรรทรัพยากรเพื่อจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ.
- ช่วยให้องค์กรสามารถลดความเสียหายที่อาจเกิดขึ้นจากความเสี่ยงได้.
- ช่วยให้องค์กรสามารถปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล.

การประเมินและให้คะแนนความเสี่ยงเป็นกระบวนการที่สำคัญในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่องและปลอดภัย.

รายงานความเสี่ยงในระบบ Back Office ของโรงพยาบาลสันกำแพง