แผนการบริหารจัดการความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
โรงพยาบาลสะบ้าย้อย

ปรับปรุงเมื่อเดือน กรกฎาคม 2567

สารบัญ

หัวข้อ **หน้า**

การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

โรงพยาบาลสะบ้าย้อยได้จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. 2566 - 2570 ด้วยการวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อที่จะบริหารจัดการความเสี่ยงตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Treadway Commission) โดยได้วิเคราะห์ความเสี่ยง ให้ครอบคลุมตามหลักธรรมาภิบาลและเป็นไปตามข้อกำหนดตามเกณฑ์การพัฒนาคุณภาพการบริหารจัดการ ภาครัฐ (PMQA) ซึ่งสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (ISO27001) แผนบริหารจัดการ ความเสี่ยงดังกล่าวจะใช้เป็นกรอบและแนวทำงานในการปฏิบัติงานของหน่วยงานต่างๆ ที่เกี่ยวข้อง ตลอดจน การกำกับดูแลการใช้งานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลสะบ้าย้อยในปี 2563-2567 เพื่อให้เทคโนโลยีสารสนเทศของโรงพยาบาลสะบ้าย้อย สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและมีความมั่นคงปลอดภัยสูงสุด ทั้งนี้จะมีการตรวจสอบและประเมินความเสี่ยงที่มีแนวโน้มอาจจะเกิดขึ้นเพื่อบริหารจัดการได้อย่างถูกต้อง ไม่เกิดเหตุการณ์ความเสียหาย

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของโรงพยาบาล
2. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
3. เพื่อให้เกิดการบริหารความเสี่ยงในโรงพยาบาลในด้านเทคโนโลยีสารสนเทศ
4. เพื่อลดความเสี่ยงลงให้มากที่สุด

กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยง เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความ เสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ในการดำเนินงานขององค์กร รวมทั้งการจัดทำแผนบริหารจัดการ ความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งกลุ่มงาน สารสนเทศทางการแพทย์ มีขั้นตอนหรือกระบวนการบริหารความเสี่ยง ดังนี้

1.การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

1.1 ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ ประกอบไปด้วยปัจจัยดังนี้

1. จุดอ่อน หรือ ช่องโหว่
2. ภัยคุกคาม

<u>จุดอ่อน</u> หมายถึง ข้อบกพร่องทางด้าน กายภาพ การจัดระบบ ขั้นตอนการทำงาน บุคลากร การบริหารจัดการ ครุภัณฑ์โปรแกรม หรือข้อมูลสารสนเทศสำคัญ ดังตัวอย่างต่อไปนี้

- ไม่มีระบบสำรองข้อมูลและการกู้คืนจากภัยพิบัติ
- ห้องแม่ข่าย (Server) แยกอาคาร
- บุคลากรไม่ทำตามระเบียบปฏิบัติด้านการตั้งรหัสผ่าน
- ไม่มีการดำเนินการควบคุมความมั่นคงปลอดภัย
- ติดตั้งโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ตได้โดยอิสระ

ภัยคุกคาม หมายถึง ภัยอันตรายต่างๆ ทั้งที่มีสาเหตุมาจากมนุษย์และสาเหตุอื่นๆ อันมีโอกาสจะทำให้เกิดความ เสียหายต่อระบบเทคโนโลยีสารสนเทศ ดังอย่างต่อไปนี้

- ไฟไหม้
- ฟ้าผ่า
- ขโมย
- ไวรัสคอมพิวเตอร์
- กระแสไฟฟ้าขัดข้อง

1.2 การระบุความเสี่ยง (Risk identification)

การค้นหาความเสี่ยง

1. จากอุบัติการณ์ในปีที่ผ่านมา
2. การวิเคราะห์กระบวนการทำงานและคาดการณ์ว่ามีความเสี่ยงที่จะเกิดอุบัติการณ์
3. จากเหตุการณ์ที่เกิดผลกระทบจากที่อื่นๆ

การแบ่งประเภทของความเสี่ยง

1. ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

1.1 ความเสี่ยงต่อระบบ Hardware

1) การหยุดชะงักของระบบ Server (Server Down)

2) Switch crash

3) เครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นชำรุด / ขัดข้อง ไม่สามารถใช้งานได้

4) อุปกรณ์เครือข่ายขัดข้อง / ชำรุดใช้งานไม่ได้

1.2 ความเสี่ยงในระบบ Software

1) HoSXP XE Client ขัดข้อง

2) LIS ไม่สามารถเชื่อมต่อกับ HIS

3) โปรแกรมสนับสนุน(INVC,RMC,BackOffice) ขัดข้อง

1.3 ความเสี่ยงต่อระบบ Network

1) ระบบเครือข่ายหยุดชะงัก (Network failure)

1.4 ความเสี่ยงต่อระบบฐานข้อมูล (Database)

1) ฐานข้อมูลสูญหาย

2) ฐานข้อมูลเสียหาย

2. ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ทำให้เกิดความบกพร่องในการรักษาผู้ป่วย

2.1 ข้อมูลผู้ป่วยที่ถูกบันทึก ผิดพลาด/ไม่ครบถ้วน

2.2 เวชระเบียนซ้ำซ้อนในผู้ป่วยรายเดียวกัน

2.3 เวชระเบียนที่ถูก scan เข้าระบบ ผิดพลาด/ไม่ครบถ้วน

3. ความเสี่ยงต่อการเปิดเผยข้อมูลผู้ป่วย

3.1 การเข้าถึงเวชระเบียนโดยผู้ที่ไม่ได้รับอนุญาต

3.2 เวชระเบียนสูญหาย

3.3 การส่งข้อมูลทาง social media ที่ไม่ถูกต้อง

4. ความเสี่ยงในการดำเนินงานตามแผนแม่บทและการปฏิบัติตามนโยบายด้าน IT

4.1 แผนแม่บท IT ไม่ตอบสนองยุทธศาสตร์โรงพยาบาล

4.2 งบประมาณที่ตั้งไว้ไม่เพียงพอ

5. ความเสี่ยงจากภัยคุกคามภายนอกและภัยพิบัติ

5.1 อัคคีภัย

5.2 อุปกรณ์ได้รับความเสียหายจากระบบไฟฟ้าขัดข้อง

5.3 ระบบไฟฟ้าภายในขัดข้อง

5.4 ระบบไฟฟ้าภายนอกขัดข้อง

5.5 การโจรกรรม / ลักขโมย

5.6 ฟ้าผ่า

1.3 การวิเคราะห์ความเสี่ยง (Risk analysis)

แนวทางการวิเคราะห์ความเสี่ยงของโรงพยาบาล

การประเมินความเสี่ยงโอกาสที่จะเกิดความเสี่ยงและผลเสียหาย จะประเมินค่าเป็นระดับ 1-5 ดังนี้

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่าได้เป็น

1. ต่ำมาก ไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก
2. ต่ำมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ 1 ปี
3. ปานกลาง มีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ 1 ครั้ง
4. สูง มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
5. สูงมาก มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆ สัปดาห์

ประเมินความรุนแรงผลกระทบ มีค่าได้เป็น

1. ต่ำมาก ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
2. ต่ำ มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
3. ปานกลาง มีผลกระทบต่อการให้บริการของโรงพยาบาลใน 1 -2 แผนก
4. สูง มีผลกระทบต่อการให้บริการของโรงพยาบาล 3 -4 แผนก
5. สูงมาก มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

หลังจากนั้นให้ประเมินคะแนนความเสี่ยง คำนวณได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15 เมื่อคำนวณคะแนนความเสี่ยงแล้ว ให้นำคะแนนความเสี่ยงมาพิจารณา ตามแผนผังประเมินความเสี่ยง ดังนี้

ค่าความเสี่ยง (ระดับ)		**โอกาสที่เกิดจากความเสี่ยง (Probability/Likelihood : P)**				
		ต่ำมาก (1)	**ต่ำ (2)**	**ปานกลาง (3)**	**สูง (4)**	**สูงมาก (5)**
ความรุนแรงผลกระทบ (Impact :I)	**สูงมาก (5)**	5	10	15	20	25
	สูง (4)	4	8	12	16	20
	ปานกลาง(3)	3	6	9	12	15
	ต่ำ (2)	2	4	6	8	10
	ต่ำมาก (1)	1	2	3	4	5

มีความเสี่ยงสูงมาก
มีความเสี่ยงสูง
มีความเสี่ยงปานกลาง
มีความเสี่ยงต่ำ

ระดับการประเมินความเสี่ยง

ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง	คำอธิบาย
1-3	ต่ำ (Low)	เป็นระดับความเสี่ยงที่องค์กรสามารถยอมรับได้
4-9	ปานกลาง (Medium)	เป็นระดับความเสี่ยงที่องค์กรพอสามารถยอมรับ แต่ต้องมีมาตรการควบคุมความเสี่ยง/ปรับปรุงความเสี่ยงในระดับที่องค์กรยอมรับได้
10-16	สูง (High)	ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
17-25	สูงมาก (Very High)	เป็นระดับที่องค์กรไม่สามารถยอมรับได้/มีการปรับปรุงอย่างเร่งด่วน

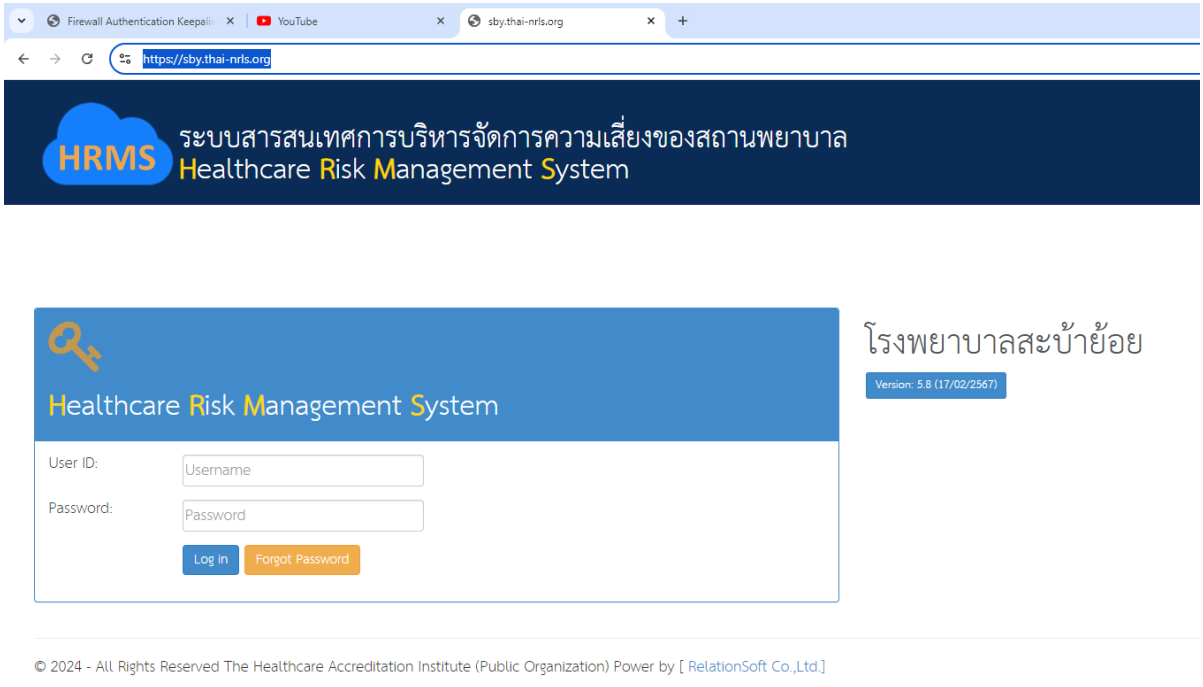
จากการใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยงและการจัดลำดับความสำคัญของเหตุการณ์ที่ทาให้เกิดความเสี่ยงโดยค่าที่มีความเสี่ยงสูงมาก (17- 25) จะถือว่าเป็นความเสี่ยงที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ให้ยอมรับได้โดยทันที จึงต้องเขียนแผนจัดการความเสี่ยงเหตุการณ์ระดับนี้โดยกำหนดลำดับความสำคัญเป็นลำดับแรก ส่วนเหตุการณ์ที่มีคะแนนความเสี่ยงสูง ปานกลางและต่ำ จะกำหนดลำดับความสำคัญไว้เป็นลำดับต่อมา

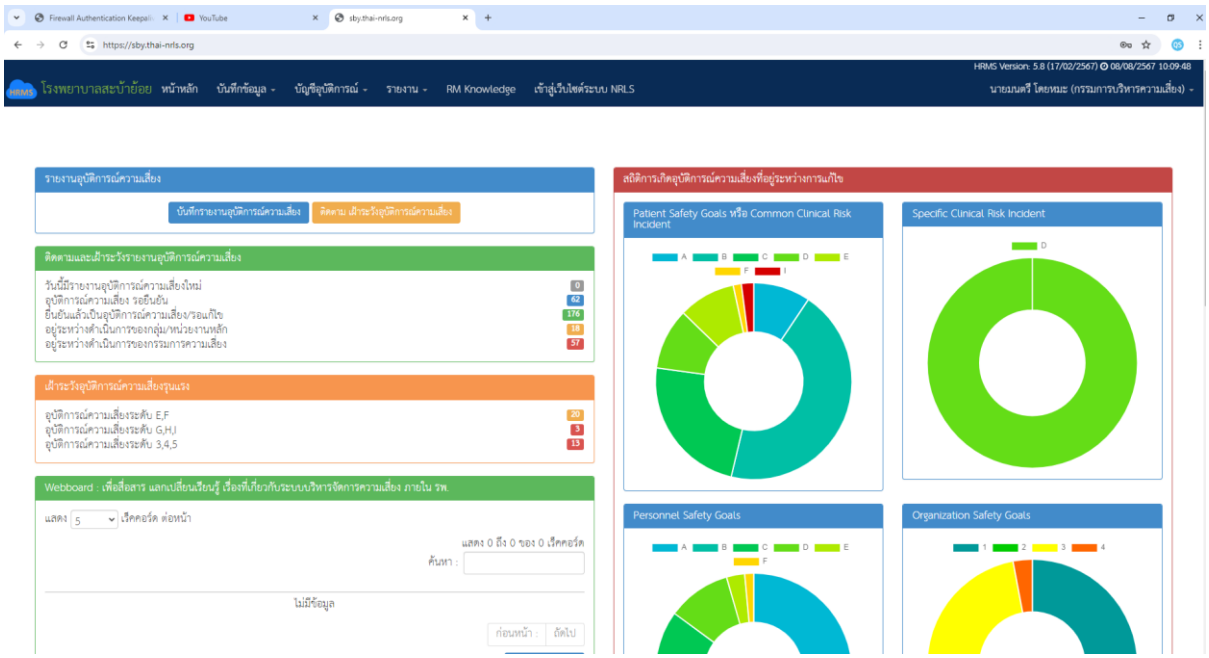
มีการกำหนดวิธีแก้ไขความเสี่ยง ให้กับเหตุการณ์ต่างๆ และมีแผนจัดการเหตุการณ์ไม่ปกติ ซึ่งการกำหนดแนวทางการปฏิบัติอย่างชัดเจน ทำให้มั่นใจได้ว่าผลการประเมินถูกต้องและสามารถนำผลการประเมินมาใช้ได้




ภาพผนวก

โปรแกรมความเสี่ยง




https://sby.thai-nrls.org
HRMS Version: 5.8 (17/02/2567) 08/08/2567 10:09:48
โรงพยาบาลสะบ้าย้อย หน้าหลัก บันทึกข้อมูล บัญชีอุบัติการณ์ รายงาน RM Knowledge เข้าสู่เว็บไซต์ระบบ NRLS
นายมนตรี โตยหมะ (กรรมการบริหารความเสี่ยง)
รายงานอุบัติการณ์ความเสี่ยง
บันทึกรายงานอุบัติการณ์ความเสี่ยง
ติดตาม เฝ้าระวังอุบัติการณ์ความเสี่ยง
ติดตามและเฝ้าระวังรายงานอุบัติการณ์ความเสี่ยง
วันนี้มีรายงานอุบัติการณ์ความเสี่ยงใหม่ 0
อุบัติการณ์ความเสี่ยง รอยืนยัน 62
ยืนยันแล้วเป็นอุบัติการณ์ความเสี่ยง/รอแก้ไข 176
อยู่ระหว่างดำเนินการของกลุ่ม/หน่วยงานหลัก 18
อยู่ระหว่างดำเนินการของกรรมการความเสี่ยง 57
เฝ้าระวังอุบัติการณ์ความเสี่ยงรุนแรง
อุบัติการณ์ความเสี่ยงระดับ E,F 20
อุบัติการณ์ความเสี่ยงระดับ G,H,I 3
อุบัติการณ์ความเสี่ยงระดับ 3,4,5 13
Webboard : เพื่อสื่อสาร แลกเปลี่ยนเรียนรู้ เรื่องที่เกี่ยวกับระบบบริหารจัดการความเสี่ยง ภายใน รพ.
แสดง 5 เร็คคอร์ด ต่อหน้า
แสดง 0 ถึง 0 ของ 0 เร็คคอร์ด
ค้นหา :
ไม่มีข้อมูล
ก่อนหน้า : ถัดไป
สถิติการเกิดอุบัติการณ์ความเสี่ยงที่อยู่ระหว่างการแก้ไข
Patient Safety Goals หรือ Common Clinical Risk Incident
A B C D E F I
Specific Clinical Risk Incident
D
Personnel Safety Goals
A B C D E F
Organization Safety Goals
1 2 3 4

ผลการวิเคราะห์ความเสี่ยง

ลำดับ	ชื่อความเสี่ยง	ประเภท	P			I	ค่าคะแนน (P*I)	ระดับความเสี่ยง	ระดับความเสี่ยงด้านคลินิก	หมายเหตุ
			จำนวนอุบัติการณ์ปีที่ผ่านมา (2566)	จำนวนอุบัติการณ์ 9 เดือนที่ผ่านมา	คะแนน P					
1	การหยุดชะงักของระบบ Server (Server Down)	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	0	0	1	5	5	ปานกลาง	ปานกลาง	
2	Switch crash	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1	1	1	5	5	ปานกลาง	ปานกลาง	
3	คอมพิวเตอร์ หรืออุปกรณ์อื่น ชำรุด/ขัดข้อง ไม่สามารถใช้งานได้ (Work Station)	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	40	20	4	3	12	สูง	สูง	
4	อุปกรณ์เครือข่ายขัดข้อง / ชำรุดใช้งานไม่ได้	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	21	12	4	2	8	ปานกลาง	ปานกลาง	
5	HOSxP XE Client ขัดข้อง	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	40	35	5	2	10	สูง	สูง	
6	LIS ไม่เชื่อมกับ HIS	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	3	1	1	4	4	ปานกลาง	ปานกลาง	
7	โปรแกรมสนับสนุน(INVC,RMC,BackOffice)	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	7	1	1	3	3	ต่ำ	ต่ำ	
8	ระบบเครือข่ายหยุดชะงัก (Network failure)	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	9	5	2	5	10	สูง	สูง	
9	ฐานข้อมูลสูญหาย	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	0	0	1	1	1	ต่ำ	ต่ำ	
10	ฐานข้อมูลเสียหาย	ความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	0	1	1	3	3	ต่ำ	ต่ำ	
11	ข้อมูลผู้ป่วยถูกบันทึกผิดพลาด/ ไม่ครบถ้วน	ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ทำให้เกิดความบกพร่องในการรักษาผู้ป่วย	15	9	2	4	8	ปานกลาง	ปานกลาง	
12	เวชระเบียนซ้ำซ้อนในผู้ป่วยรายเดียวกัน	ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ทำให้เกิดความบกพร่องในการรักษาผู้ป่วย	2	1	1	5	5	ปานกลาง	ปานกลาง	

ลำดับ	ชื่อความเสี่ยง	ประเภท	P			I	ค่าคะแนน (P*I)	ระดับความเสี่ยง	ระดับความเสี่ยงด้านคลินิก	หมายเหตุ
			จำนวนอุบัติการณ์ปีที่ผ่านมา (2566)	จำนวนอุบัติการณ์ 9 เดือนที่ผ่านมา	คะแนน P					
13	เวชระเบียนถูก scan ไม่ครบ / ผิดพลาด	ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ทำให้เกิดความบกพร่องในการรักษาผู้ป่วย	5	3	1	2	2	ต่ำ	ต่ำ	
14	การเข้าถึงเวชระเบียนโดยไม่ได้รับอนุญาต	ความเสี่ยงต่อการเปิดเผยข้อมูลผู้ป่วย	0	0	1	2	2	ต่ำ	ต่ำ	
15	เวชระเบียนสูญหาย	ความเสี่ยงต่อการเปิดเผยข้อมูลผู้ป่วย	0	0	1	2	2	ต่ำ	ต่ำ	
16	การส่งข้อมูลทาง Social Media ที่ไม่ถูกต้อง	ความเสี่ยงต่อการเปิดเผยข้อมูลผู้ป่วย	7	5	2	3	6	ปานกลาง	ปานกลาง	
17	แผนแม่บท IT ไม่ตอบสนองยุทธศาสตร์โรงพยาบาล	ความเสี่ยงในการดา เนินงานตามแผนแม่บทและการปฏิบัติตามนโยบายด้าน IT	0	0	1	2	2	ต่ำ	ต่ำ	
18	งบประมาณที่ตั้งไว้ไม่เพียงพอ	ความเสี่ยงในการดา เนินงานตามแผนแม่บทและการปฏิบัติตามนโยบายด้าน IT	0	1	1	2	2	ต่ำ	ต่ำ	
19	อัคคีภัย	ความเสี่ยงจากภัยคุกคามภายนอกและภัยพิบัติ	0	1	1	5	5	ปานกลาง	ปานกลาง	
20	อุปกรณ์ได้รับความเสียหายจากระบบไฟฟ้าขัดข้อง	ความเสี่ยงจากภัยคุกคามภายนอกและภัยพิบัติ	15	11	4	3	12	สูง	สูง	
21	ระบบไฟฟ้าภายในขัดข้อง	ความเสี่ยงจากภัยคุกคามภายนอกและภัยพิบัติ	1	2	1	5	5	ปานกลาง	ปานกลาง	
22	ระบบไฟฟ้าภายนอกขัดข้อง	ความเสี่ยงจากภัยคุกคามภายนอกและภัยพิบัติ	0	0	1	2	2	ต่ำ	ต่ำ	
23	การโจรกรรม/ลักขโมย	ความเสี่ยงจากภัยคุกคามภายนอกและภัยพิบัติ	0	0	1	2	2	ต่ำ	ต่ำ	
24	ฟ้าผ่า	ความเสี่ยงจากภัยคุกคามภายนอกและภัยพิบัติ	0	0	1	1	1	ต่ำ	ต่ำ	

Risk Evaluation การประเมินความเสี่ยง

ความรุนแรงผลกระทบ(Impact :I)

5	01/02/12/19/21	08/11			
4	06				
3	07/10	16		03/20	
2	13/14/15/17/18/22/23			04	05
1	09/24				
คะแนน	1	2	3	4	5

โอกาสที่เกิดจากความเสี่ยง (Probability/Likelihood : P)

2.การกำหนดกลยุทธ์และแนวทางการจัดการความเสี่ยง (Risk management)

กลยุทธ์ในการจัดการความเสี่ยง

กลยุทธ์ที่ 1 การยอมรับความเสี่ยง (Take)

กลยุทธ์ที่ 2 การควบคุมความเสี่ยง (Treat)

กลยุทธ์ที่ 3 การถ่ายโอนความเสี่ยง (Transfer)

กลยุทธ์ที่ 4 การหลีกเลี่ยงความเสี่ยง (Terminate)

แนวทางการจัดการความเสี่ยง

ลำดับ	ชื่อความเสี่ยง	คะแนน	ระดับความเสี่ยง	สาเหตุ/ปัจจัย	กลยุทธ์	แนวทางการจัดการ / มาตรการป้องกัน
1	คอมพิวเตอร์ หรืออุปกรณ์อื่นชำรุด/ขัดข้อง ไม่สามารถใช้งานได้ (Work Station)	12	สูง	- อายุการใช้งานของคอมพิวเตอร์ - ระบบการ share	ถ่ายโอนความเสี่ยง (Transfer)	- จัดหาเครื่องคอมพิวเตอร์หรือครุภัณฑ์คอมพิวเตอร์ทดแทนเครื่องอายุเกิน 5 ปี - จัดทำแผน maintenance เครื่องคอมพิวเตอร์หรืออุปกรณ์อื่น
2	อุปกรณ์ได้รับความเสียหายจากระบบไฟฟ้าขัดข้อง	12	สูง	- ไฟฟ้าดับ / ไฟฟ้ากระชาก	ควบคุมความเสี่ยง (Treat)	- มีระบบไฟฟ้าสำรอง - มีอุปกรณ์ป้องกัน Power surge ในอุปกรณ์ที่สำคัญ - จัดหาสำรองไฟ
3	HOSxP XE Client ขัดข้อง	10	สูง	- เครื่องคอมพิวเตอร์ลูกข่ายติดไวรัส - ระบบปฏิบัติการ windows ไม่มีลิขสิทธิ์	ควบคุมความเสี่ยง (Treat)	- จัดหา Anti-virus สำหรับใช้งานในเครื่องคอมพิวเตอร์ลูกข่าย - ติดตั้งระบบ firewall ประสิทธิภาพสูง
ลำดับ	**ชื่อความเสี่ยง**	**คะแนน**	**ระดับความเสี่ยง**	**สาเหตุ/ปัจจัย**	**กลยุทธ์**	**แนวทางการจัดการ / มาตรการป้องกัน**
4	ระบบเครือข่ายหยุดชะงัก (Network failure)	10	สูง	- ขนาดของข้อมูลและapplication สูงขึ้น	ควบคุมความเสี่ยง (Treat)	- ปรับปรุงระบบเครือข่ายเพื่อรองรับความเร็ว 10 Gbps - จัดหาอุปกรณ์เครือข่ายทดแทนอุปกรณ์เดิมที่มีอายุการใช้งานเกิน 5 ปี - นโยบายความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ - ปรับปรุง เปลี่ยน Network switch ที่มีอายุการใช้งานมากกว่า 5 ปี - บำรุงรักษาตามระยะเวลา

5	ข้อมูลผู้ป่วยถูกบันทึกผิดพลาด/ ไม่ครบถ้วน	8	ปานกลาง	- ความรู้ความเข้าใจในการบันทึกเวชระเบียน - การออกแบบระบบการบันทึกให้สะดวกต่อผู้ใช้งาน	ควบคุมความเสี่ยง (Treat)	- ตรวจสอบคุณภาพเวชระเบียน และสื่อสารไปยังองค์กรแพทย์ / พยาบาล - ปรับปรุงระบบการบันทึกข้อมูลการตรวจร่างกายโดยแพทย์
6	อุปกรณ์เครือข่ายขัดข้อง / ชำรุดใช้งานไม่ได้	8	ปานกลาง	-	ถ่ายโอนความเสี่ยง (Transfer)	-
7	การส่งข้อมูลทาง Social Media ที่ไม่ถูกต้อง	6	ปานกลาง	- การออกนโยบาย/ ระเบียบปฏิบัติ - ระบบกำกับติดตาม	ควบคุมความเสี่ยง (Treat)	- นโยบายการส่งข้อมูลผ่าน Line - นโยบายความมั่นคงปลอดภัย
8	การหยุดชะงักของระบบ Server (Server Down)	5	ปานกลาง	- อายุการใช้งานของ server - ขนาดของข้อมูลเพิ่มขึ้น - การเพิ่มฐานข้อมูล	ถ่ายโอนความเสี่ยง (Transfer)	- จัดการ server แยกฐานข้อมูลตามลำดับความสำคัญ - จัดหา server ประสิทธิภาพสูงใหม่มาทดแทน
9	Switch crash	5	ปานกลาง	- อายุการใช้งานของอุปกรณ์ switch - คุณภาพของ Switch	ควบคุมความเสี่ยง (Treat)	- ปรับปรุงเปลี่ยน switch ที่มีอายุการใช้งานมากกว่า 5 ปี - บำรุงรักษาตามระยะเวลา
ลำดับ	**ชื่อความเสี่ยง**	**คะแนน**	**ระดับความเสี่ยง**	**สาเหตุ/ปัจจัย**	**กลยุทธ์**	**แนวทางการจัดการ / มาตรการป้องกัน**
10	เวชระเบียนซ้ำซ้อนในผู้ป่วยรายเดียวกัน	5	ปานกลาง	- ความรู้ความเข้าใจในการบันทึกเวชระเบียน - ผู้ป่วยทำประวัติใหม่โดยไม่แจ้ง/ไม่ทราบว่ามีประวัติเดิม	ควบคุมความเสี่ยง (Treat)	- จัดทำแผนตรวจสอบคุณภาพเวชระเบียน
11	อัคคีภัย	5	ปานกลาง	- สภาพสิ่งแวดล้อม - ระบบการ monitor	ควบคุมความเสี่ยง (Treat)	- จัดทำและซ้อมแผนอัคคีภัยเป็นประจำทุกปี - ติดตั้งอุปกรณ์ควบคุมอัคคีภัย
12	ระบบไฟฟ้าภายในขัดข้อง	5	ปานกลาง		ควบคุมความเสี่ยง (Treat)	- มีระบบไฟฟ้าสำรอง - มีอุปกรณ์ป้องกัน Power surge ในอุปกรณ์ที่สำคัญ
13	LIS ไม่เชื่อมกับ HIS	4	ปานกลาง	- LIS connecting server ค้าง	ควบคุมความเสี่ยง (Treat)	-เปลี่ยนระบบ LIS และ ทำการ monitor
14	โปรแกรมสนับสนุน(INVC, RMC, BackOffice)	3	ต่ำ		ควบคุมความเสี่ยง (Treat)	- ใช้ Software ลิขสิทธิ์ถูกต้อง - Update Program สม่ำเสมอ

15	ฐานข้อมูลเสียหาย	3	ต่ำ	- ไม่มีการสำรองข้อมูล - ไม่มีแผนตรวจการทำงานของ server - ไม่มีแผน maintenance server	ควบคุมความเสี่ยง (Treat)	- จัดทำแผน maintenance server
16	เวชระเบียนถูก scan ไม่ครบ / ผิดพลาด	2	ต่ำ	- การตรวจสอบความผิดพลาดขณะทำการ scan	ควบคุมความเสี่ยง (Treat)	- มีการสุ่มตรวจความถูกต้องของไฟล์ scan ในระบบทุกวัน
17	การเข้าถึงเวชระเบียนโดยไม่ได้รับอนุญาต	2	ต่ำ	- ระบบการป้องกันการเข้าถึง	ควบคุมความเสี่ยง (Treat)	- ให้มีการเข้าระบบโดย log in ใช้รหัสผ่านเฉพาะบุคคล - ไม่สามารถดูข้อมูล และบันทึกเวชระเบียนย้อนหลังในโปรแกรมได้ - นโยบายความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ
ลำดับ	**ชื่อความเสี่ยง**	**คะแนน**	**ระดับความเสี่ยง**	**สาเหตุ/ปัจจัย**	**กลยุทธ์**	**แนวทางการจัดการ / มาตรการป้องกัน**
						- มีระบบเก็บข้อมูล log การเข้าดูเวชระเบียนเมื่อเปลี่ยนไปใช้ server ใหม่
18	เวชระเบียนสูญหาย	2	ต่ำ	- ระบบการคืนเวชระเบียนจากห้องตรวจ OPD	ควบคุมความเสี่ยง (Treat)	- OPD ใช้ระบบ paperless 100%
19	แผนแม่บท IT ไม่ตอบสนองยุทธศาสตร์ โรงพยาบาล	2	ต่ำ	- การวิเคราะห์ปัจจัยแห่งความสำเร็จ - แผนแม่บทไม่ตอบสนองความต้องการของแผนยุทธศาสตร์	ควบคุมความเสี่ยง (Treat)	- จัดทำแผนแม่บทโดยการมีส่วนร่วมของผู้รับผิดชอบแผนปฏิบัติการทุกกลยุทธ์
20	งบประมาณที่ตั้งไว้ไม่เพียงพอ	2	ต่ำ	- การวางแผนงบประมาณ	ควบคุมความเสี่ยง (Treat)	- การปรับแผนงบประมาณ
21	ระบบไฟฟ้าภายนอกขัดข้อง	2	ต่ำ		ควบคุมความเสี่ยง (Treat)	- มีระบบไฟฟ้าสำรอง - มีอุปกรณ์ป้องกัน Power surge ในอุปกรณ์ที่สำคัญ
22	การโจรกรรม/ลักขโมย	2	ต่ำ	- การเข้าถึงอุปกรณ์ต่างๆ - ระบบความปลอดภัย	ควบคุมความเสี่ยง (Treat)	- มีระบบการป้องกันการเข้าถึง ในระบบที่สำคัญ - มีระบบ CCTV
23	ฐานข้อมูลสูญหาย	1	ต่ำ	- ข้อมูลไม่ได้สำรองอย่างเป็นระบบ	ควบคุมความเสี่ยง (Treat)	- จัดระบบการสำรองและกู้คืนข้อมูล (DR-Site , Offline backup)

				- ข้อมูลสำรองโดยผู้ดูแลระบบเพียงคนเดียว		- จัดระบบสำรองข้อมูลทุกๆวันโดยแยกตัวจัดเก็บเป็นรายวัน
24	ฟ้าผ่า	1	ต่ำ		ควบคุมความเสี่ยง (Treat)	

3.อันดับความเสี่ยงสำคัญในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลสะบ้าย้อย

ลำดับ	ความเสี่ยง	Risk Profile
1	คอมพิวเตอร์ หรืออุปกรณ์อื่น ชำรุด/ขัดข้อง ไม่สามารถใช้งานได้ (Work Station)	12
2	อุปกรณ์ได้รับความเสียหายจากระบบไฟฟ้าขัดข้อง	12
3	HOSxP XE Client ขัดข้อง	10
4	ระบบเครือข่ายหยุดชะงัก (Network failure)	10
5	อุปกรณ์เครือข่ายขัดข้อง / ชำรุดใช้งานไม่ได้	8
6	การหยุดชะงักของระบบ Server (Server Down)	5
7	Switch crash	5
8	ระบบไฟฟ้าภายในขัดข้อง	5

4.มีการดำเนินการตามแผนจัดการความเสี่ยง

ลำดับ	ชื่อความเสี่ยง	กลยุทธ์	Action Plan	ปีงบประมาณ 2567				ปีงบประมาณ 2568				ปีงบประมาณ 2569				ปีงบประมาณ 2570				ผู้รับผิดชอบ
				Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
1	คอมพิวเตอร์ หรืออุปกรณ์อื่น ชำรุด/ขัดข้อง ไม่สามารถใช้งานได้ (Work Station)	ถ่ายโอนความเสี่ยง	1.ตรวจสอบเครื่องคอมพิวเตอร์และอุปกรณ์อื่น 2.จัดทำแผนจัดหาเครื่องคอมพิวเตอร์ทดแทน 3.ดูแลและซ่อมบำรุงประจำเดือน	→				→				→				→			→	IT
2	อุปกรณ์ได้รับความเสียหายจากระบบไฟฟ้าขัดข้อง	ถ่ายโอนความเสี่ยง	1.ตรวจสอบการทำงานของเครื่องปั่นไฟ 2.ตรวจสอบเครื่องสำรองไฟ	→				→				→				→			→	IT และ ทีม ENV
3	HOSxP XE Client ขัดข้อง	ควบคุมความเสี่ยง	1.ตรวจสอบโปรแกรม HOSxP XE Client ทุกวัน 2.ตรวจสอบระบบปฏิบัติการ Windows 3.ตรวจสอบระบบเครือข่าย	→		→		→		→		→		→		→		→	→	IT
4	ระบบเครือข่ายหยุดชะงัก (Network failure)	ควบคุมความเสี่ยง	1.ตรวจสอบความพร้อมของระบบเครือข่าย 2.ตรวจสอบประสิทธิภาพ รวมทั้งขีดความสามารถของระบบเครือข่าย	→				→				→				→			→	IT
5	อุปกรณ์เครือข่ายขัดข้อง / ชำรุดใช้งานไม่ได้	ถ่ายโอนความเสี่ยง	1.ตรวจสอบความพร้อมใช้งานของอุปกรณ์ 2.ติดตั้งเครื่องสำรองไฟให้กับ Switch ทุกตัว 3.จัดทำระบบ network สำรอง กรณีเส้นทางใดเส้นทางหนึ่งใช้การไม่ได้	→				→				→				→				→	IT

ลำดับ	ชื่อความเสี่ยง	กลยุทธ์	Action Plan	ปีงบประมาณ 2567				ปีงบประมาณ 2568				ปีงบประมาณ 2569				ปีงบประมาณ 2570				ผู้รับผิดชอบ
				Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
6	การหยุดชะงักของระบบ Server (Server Down)	ถ่ายโอนความเสี่ยง	1.ตรวจสอบประสิทธิภาพของ Server 2.จัดหา Server ประสิทธิภาพสูง ใหม่ทดแทน	→	→	→	→	→	→	→	→	→	→	→	→	→	→	→	→	IT
7	Switch crash	ควบคุมความเสี่ยง	1.ตรวจสอบอุปกรณ์ Switch 2.จัดทำแผนซื้ออุปกรณ์ทดแทนที่เกิน 5 ปี 3.ดูแลซ่อมบำรุงตลอดทุกเดือน	→	→	→	→	→	→	→	→	→	→	→	→	→	→	→	→	IT
8	ระบบไฟฟ้าภายในขัดข้อง	ควบคุมความเสี่ยง	1.ตรวจสอบการทำงานของเครื่องปั่นไฟของโรงพยาบาล 2.ตรวจสอบเครื่องสำรองไฟทุกหน่วยงานตามแผนซ่อมบำรุงประจำปี 3.มีระบบไฟฟ้าสำรอง 4.มีอุปกรณ์ป้องกัน Power surge ในอุปกรณ์ที่สำคัญ	→	→	→	→	→	→	→	→	→	→	→	→	→	→	→	→	ทีม ENV

5.กระบวนการพัฒนาเพื่อจัดการความเสี่ยง

1.คอมพิวเตอร์ หรืออุปกรณ์อื่น ชำรุด/ขัดข้อง ไม่สามารถใช้งานได้ (Work Station)

ปี	2566	2567	2568	2569	2570
ระดับความเสี่ยง (คะแนน)					

บริบท

โรงพยาบาลสะบ้าย้อย มีเครื่องคอมพิวเตอร์ที่เป็นเครื่องที่จัดซื้อมาเองทั้งหมด และถูกใช้งานจนกว่าจะหมดสภาพการใช้งาน การซ่อมและเปลี่ยนอะไหล่ ส่วนใหญ่เป็นการเปลี่ยน Power supply รองลงมาจะเป็นการเปลี่ยน Hard disk ซึ่งสาเหตุหลักมาจากความไม่เสถียรของระบบไฟฟ้า ไฟตกและไฟดับบ่อย เครื่องสำรองไฟไม่พอใช้กับเครื่องคอมพิวเตอร์ที่มีอยู่ และเครื่องที่หมดสภาพจะถูกจาหน่ายและจัดซื้อทดแทน และมี Printer หลายชนิดไม่ว่าจะเป็น Printer Thermal , Printer Laser, Printer แบบฉีกกระดาษ โดยมีการ Share Printer เป็นสักส่วนใหญ่

Plan : กำหนดจัดทำแผนซ่อมบำรุง เมื่อเกิดปัญหาการใช้งานกับเครื่องคอมพิวเตอร์ และอุปกรณ์อื่นๆ เมื่อมีการแจ้งผ่าน service help desk และมีแผนจัดหาคอมพิวเตอร์ทดแทนสำหรับเครื่องเสื่อมสภาพหรือถึงอายุการใช้งาน

Do : มีการดำเนินการ โดยการส่งซ่อมและเปลี่ยนอะไหล่ แก้ปัญหาการใช้งานให้กับหน่วยงาน ในเมื่อมีหน่วยงานแจ้งผ่านระบบการแจ้งซ่อม

Check : เกิดอุบัติการณ์จำนวน----ครั้ง จากการวิเคราะห์ปัญหา พบสาเหตุดังนี้

- คอมพิวเตอร์มีอายุการใช้งานนานงาน
- Printer พบอุบัติการณ์พิมพ์ไม่ได้ จากการ update OS ทำให้ระบบที่ share printer ไว้ไม่ทำงาน

Action : การนำผลการวิเคราะห์ปัญหาจากการเกิดอุบัติกาณ์ มาปรับปรุงโดยการตรวจสอบอายุของครุภัณฑ์คอมพิวเตอร์ทั้งหมดก่อนถึงอายุการใช้งาน

2.อุปกรณ์ได้รับความเสียหายจากระบบไฟฟ้าขัดข้อง

ปี	2566	2567	2568	2570	
ระดับความเสี่ยง (คะแนน)					

Plan : ยังไม่ได้มีการวางแผนอย่างชัดเจน

Do : ยังไม่ได้กำหนดแนวทางป้องกันที่ชัดเจน

Check : พบอุบัติการณ์หลังจากไฟฟ้าขัดข้องดังนี้

- ทำให้อุปกรณ์เครือข่ายเสียหาย 1 เครื่อง
- ทำให้ Power supply เสียหาย 4 ตัว
- ทำให้จอ Monitor เสีย 2 ตัว
- ทำให้ Hard disk ได้รับความเสียหาย 1 ตัว

Action : 1. มีการวางแผนติดตั้งเครื่องสำรองไฟฟ้ากับครุภัณฑ์คอมพิวเตอร์ทุกชนิด

2. มีการสำรอง hard disk ที่เป็น ssd สำหรับทดแทนกรณี hard disk ที่เครื่องเดิมเสียเนื่องจาก hard disk ssd ซึ่งจะมีความทนต่อการเสียหายมากกว่า

3. มีการสำรองแบตเตอรี่สำรองไฟ

3.HOSxP XE Client ขัดข้อง

ปี	2566	2567	2568	2570	
ระดับความเสี่ยง (คะแนน)					

บริบท

Program HOSxP XE Client ซึ่งเป็นระบบปฏิบัติการ (HIS) ของโรงพยาบาลสะบ้าย้อย มีการพัฒนาเพิ่มเติมโดยบริษัท BMS ในเรื่องของ IPD Paperless, ER Paperless เพื่อให้เข้ากับบริบทและความต้องการของผู้ใช้งาน และแผนกผู้ป่วยนอกและแผนกอื่นๆมีการใช้ระบบเรียกคิวการรับบริการ เพื่อการรวดเร็วในการให้บริการผู้ป่วยและลดความแออัดในการรับบริการ

Plan : มีการวางแผนและกำหนดแนวทางในการ update โปรแกรม

Do : ได้ดำเนินการตามแนวทางที่วางไว้ โดยกำหนดผู้รับผิดชอบในฝ่าย IT สำหรับการ update

Check : พบอุบัติการณ์ HIS ขัดข้องจำนวน --- ครั้ง สาเหตุพบว่าเกิดจาก BUG ในกระบวนการพัฒนา Software และระบบที่ทำการปิดกั้นการ update Software ของเครื่อง

Action : เพิ่มความเข้มงวดในกระบวนการทดสอบโปรแกรมให้มากขึ้น จากแนวทางที่กำหนดไว้เดิม

4.ระบบเครือข่ายหยุดชะงัก (Network failure)

ปี	2566	2567	2568	2570	
ระดับความเสี่ยง (คะแนน)					

บริบท

Plan :

Do :

Check :

Action :

5.อุปกรณ์เครือข่ายขัดข้อง / ชำรุดใช้งานไม่ได้

ปี	2566	2567	2568	2570	
ระดับความเสี่ยง (คะแนน)					

บริบท

Plan :

Do :

Check :

Action :

6.การหยุดชะงักของระบบ Server (Server Down)

ปี	2566	2567	2568	2570	
ระดับความเสี่ยง (คะแนน)					

บริบท

Plan :

Do :

Check :

Action :

7.Switch crash

ปี	2566	2567	2568	2570	
ระดับความเสี่ยง (คะแนน)					

บริบท

Plan :

Do :

Check :

Action :

8. ระบบไฟฟ้าภายในขัดข้อง

ปี	2566	2567	2568	2570	

ระดับความเสี่ยง (คะแนน)					

บริบท

Plan :

Do :

Check :

Action :