5) ปัจจัยภายใน หมายถึง ปัจจัยสำคัญที่สามารถควบคุมได้ ที่มีโอกาสส่งผลให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ

6) ปัจจัยภายนอก หมายถึง ปัจจัยสำคัญที่ไม่สามารถควบคุมได้ ที่มีโอกาสส่งผลให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ

7) บัญชีรายการความเสี่ยง (Risk Profile) หมายถึง รายการความเสี่ยงที่อาจเกิดขึ้น ซึ่งผู้รับผิดชอบ/หน่วยงานได้รวบรวมจัดทำขึ้น โดยอาศัยการเรียนรู้จากประสบการณ์ข้อมูลในอดีต และหน่วยงานอื่นๆ ตลอดจนการทบทวนต่าง ๆ และการสำรวจภายในหน่วยงานของตนเอง เพื่อเป็นประเด็นสำคัญที่ควรมีการเฝ้าระวังโดยมีทั้งระดับโรงพยาบาล กลุ่มงาน/แผนก หน่วยงาน

การกำหนดเกณฑ์การประเมินความเสี่ยง

คะแนนความเสี่ยง

	คะแนนความเสี่ยง				
ประเมินโอกาสที่จะเกิดความเสี่ยง	1	2	3	4	5
(Probability)	ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก
ประเมินผลเสียหาย (Impact)	1	2	3	4	5
	ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก

การประเมินความเสี่ยง

ประเมินจุดอ่อนหรือโอกาสที่จะเกิดความเสี่ยง (P)	
1 (ต่ำมาก)	มีจุดอ่อนน้อยมาก หรือไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก
2 (ต่ำ)	มีจุดอ่อนน้อย หรือมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้งในรอบ 1 ปี
3 (ปานกลาง)	มีจุดอ่อนพอควร หรือมีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อยเดือนละ 1 ครั้ง
4 (สูง)	มีจุดอ่อนมาก หรือมีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
5 (สูงมาก)	มีจุดอ่อนรอบด้าน หรือมีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆสัปดาห์
ประเมินผลเสียหาย (I)	
1 (ต่ำมาก)	ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
2 (ต่ำ)	มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
3 (ปานกลาง)	มีผลกระทบต่อการให้บริการของโรงพยาบาล 1-2 แผนก
4 (สูง)	มีผลกระทบต่อการให้บริการของโรงพยาบาล 3-4 แผนก
5 (สูงมาก)	มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

การคำนวณคะแนนความเสี่ยง

คะแนนความเสี่ยง = คะแนนโอกาสที่จะเกิดความเสี่ยง (P) X คะแนนผลเสียหาย (I)

บทที่ 3 กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ขั้นตอนสำคัญในการจัดการความเสี่ยง

1) การค้นหาและประเมินความเสี่ยง (Risks Identification and Risks Assessment)

2) การวางแผนกลยุทธ์จัดการความเสี่ยง (Risks Management strategic Planning)

3) การดำเนินการจัดการความเสี่ยง (Risks Treatment)

การค้นหาและประเมินความเสี่ยง (Risks Identification and Risks Assessment)

โรงพยาบาลนาด้วงมีการค้นหาความเสี่ยงจากการรวบรวมนำเอาปัญหาที่อาจเกิดขึ้นและปัญหาในอดีตที่เคยเกิดขึ้นแล้วภายในโรงพยาบาล หรือปัญหาที่อาจเกิดขึ้น และปัญหาในอดีตที่เคยเกิดขึ้นแล้ว จากหน่วยงานอื่นๆ ซึ่งเป็นปัญหาสำคัญที่ควรมีการเฝ้าระวังที่อาจนำไปสู่ความขัดข้องของระบบคอมพิวเตอร์ที่ส่งผลให้การให้บริการผู้ป่วยสะดุด และการนำเข้าข้อมูลการรักษาผู้ป่วยขาดการต่อเนื่อง รวมไปถึงไม่สามารถนำข้อมูลไปใช้ หรือเผยแพร่ข้อมูลไม่ได้ มาเป็นเป็นบัญชีรายการความเสี่ยงโดยใช้แบบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตามมาตรฐาน TMI ในการรวบรวมรายการบัญชีความเสี่ยง และมีการนำบัญชีรายการความเสี่ยงโรงพยาบาลนาด้วงไปประเมินความเสี่ยงต่อไป

แบบประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล
พัฒนาโดยสมาคมเวชสารสนเทศไทย ปีพ.ศ. 2567

TMI Vulnerabilities Assessment

IT Components	Probability (P)	Impact (I)	Risk (P x I)	ระดับความเสี่ยง
1. IT - System Hardware				
1.1 Servers and Main Switches Crash or Failure	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
1.2 Network Switches Crash or Failure	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
1.3 Workstations and Printers Failure	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
2. T - System Software				
2.1 Operating System Failure	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
3. IT- Application				
3.1 Front Offices	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
3.2 Back Offices	1 2 3 4 5	1 2 3 4 5	1	ต่ำ

IT Components	Probability (P)	Impact (I)	Risk (P x I)	ระดับความเสี่ยง
4. T - Communications, Connectivity				
4.1 Intranet	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
4.2 Internet	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
5. IT - Operational (Human) error				
5.1 Backup Error	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
5.2 Data Loss Error	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
6. Data Loss and Privacy Breach				
6.1 Data Backup	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
6.2 Data Protection Policy and Regulations	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
6.3 PDPA Implementation	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
7. IT – Future Development				
7.1 No Data Dictionary	1 2 3 4 5	1 2 3 4 5	2	ต่ำ
7.2 No System Blueprint	1 2 3 4 5	1 2 3 4 5	2	ต่ำ
7.3 No Program Document or Comments	1 2 3 4 5	1 2 3 4 5	2	ต่ำ
8. IT – Vendor and Outsource Failure				
8.1 Vendor Stop Support	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
9. IT- Hacking Unauthorized Intrusions				
9.1 IT- Hacking Unauthorized Intrusions	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
10. Environment Factors				
10.1 Flooding –Internal	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
10.2 Flooding External	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
10.3 Fire – Internal	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
10.4 Fire – External	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
10.5 Utilities – Electricity	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
10.6 Criminal – Theft	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
10.7 Criminal - Break – ins	1 2 3 4 5	1 2 3 4 5	1	ต่ำ

IT Components	Probability (P)	Impact (I)	Risk (P x I)	ระดับความเสี่ยง
10.8 Civil Unrest – Protest, Mob	1 2 3 4 5	1 2 3 4 5	1	ต่ำ
11. Patient Risk due to IT Error/Misuse				
11.1 Patient Risk due to IT Error/Misuse	1 2 3 4 5	1 2 3 4 5	4	ปานกลาง

เมื่อคำนวณคะแนนความเสี่ยงแล้วให้นำคะแนนความเสี่ยงมาพิจารณาตามแผนผังประเมินความเสี่ยงดังนี้

Risk Value			Probability				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Impact	Very High	5	5	10	15	20	25
	High	4	4	8	12	16	20
	Medium	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Very Low	1	1	2	3	4	5

สูงมาก 17-25
สูง 10-16
ปานกลาง 4-9
ต่ำ 1-3

Risk Value			Probability				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Impact	Very High	5					
	High	4					
	Medium	3					
	Low	2		11.1			
	Very Low	1	1.1 1.2 1.3	7.1 7.2 7.3			

			2.1 3.1 3.2 4.1 4.2 5.1 5.2 6.1 6.2 6.3 8.1 9.1 10.1 10.2 10.3 10.4 10.5 10.6 10.7 10.8				

จากแผนผังประเมินความเสี่ยงจะเห็นว่า เหตุการณ์ที่มีค่าคะแนนความเสี่ยงตั้งแต่ 4 ถึง 9 จะเป็นเหตุการณ์ที่เราพอยอมรับได้ (แสดงในตารางเป็นเหลือง) ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยงตั้งแต่ 1-3 จะเป็นเหตุการณีที่ยังไม่ต้องเร่งรีบจัดการ

การวางแผนกลยุทธ์จัดการความเสี่ยง (Risks Management Strategic Planning)

เมื่อเสร็จสิ้นขั้นตอนการประเมินความเสี่ยงแล้ว ขั้นตอนต่อไปจะเป็นการวางแผนกลยุทธ์จัดการความเสี่ยง โดยเริ่มการจัดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยง โดยใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยงดังนี้

เกณฑ์ความสามารถในการยอมรับความเสี่ยง

แผนกลยุทธ์จัดการความเสี่ยง			
ความเสี่ยง	**คะแนน**	**แถบสี**	**เกณฑ์ความสามารถในการยอมรับความเสี่ยง**
ต่ำ	1-3		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง
ปานกลาง	4-9		ระดับที่พอยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	10-16		ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก	17-25		ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้ทันที

จากการใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยง เราจะสามารถเรียงลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้ดังนี้

ความเสี่ยงต่ำ(1-3)	ความเสี่ยงปานกลาง (4-9)	ความเสี่ยงสูง(10-16)	ความเสี่ยงสูงมาก (17-25)
1.1 Servers and Main Switches Crash or Failure	11.1 Patient Risk due to IT Error/Misuse		
1.2 Network Switches Crash or Failure			
1.3 Workstations and Printers Failure			
2.1 Operating System Failure			
3.1 Front Offices			
3.2 Back Offices			
4.1 Intranet			
4.2 Internet			
5.1 Backup Error			
5.2 Data Loss Error			
6.1 Data Backup			
6.2 Data Protection Policy and Regulations			
6.3 PDPA Implementation			

ความเสี่ยงต่ำ(1-3)	ความเสี่ยงปานกลาง (4-9)	ความเสี่ยงสูง(10-16)	ความเสี่ยงสูงมาก (17-25)
7.1 No Data Dictionary			
7.2 No System Blueprint			
7.3 No Program Document or Comments			
8.1 Vendor Stop Support			
9.1 IT- Hacking Unauthorized Intrusions			
10.1 Flooding –Internal			
10.2 Flooding External			
10.3 Fire – Internal			
10.4 Fire – External			
10.5 Utilities – Electricity			
10.6 Criminal – Theft			
10.7 Criminal - Break – ins			
10.8 Civil Unrest – Protest, Mob			

เมื่อกำหนดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้แล้ว ขั้นตอนต่อไปคือการ กำหนดวิธีแก้ไขความเสี่ยง (Risk Treatment) ให้กับเหตุการณ์ต่าง ๆ โดยมีทางเลือกกลยุทธ์ในการแก้ไขความเสี่ยงทั้งหมด 4 กลยุทธ์ดังนี้

- กลยุทธ์ที่ 1 การลดความเสี่ยง
- กลยุทธ์ที่ 2 การย้ายความเสี่ยง
- กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง
- กลยุทธ์ที่ 4 การยอมรับความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง เป็นการกำหนดมาตรการควบคุมให้โอกาสเกิดเหตุการณ์ที่ก่อให้เกิดความเสี่ยง ลดน้อยลง และ/หรือ ร่วมกับมาตรการควบคุมให้ผลเสียหายลดลง ดังนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	ระดับความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
11.1 Patient Risk due to IT Error/Misuse - ความเสี่ยงค่าวิกฤตที่อาจทำให้เกิดอันตรายต่อ ผู้ป่วย	4	ลดโอกาสที่จะเกิดเหตุการณ์	1. มีระบบแจ้งเตือนเมื่อพบค่าวิกฤต ของผู้ป่วย 2. มีการแจ้งเตือนผู้เกี่ยวข้องทันที 3. มีการตรวจสอบว่าระบบแจ้งเตือนทำงานได้ตามปกติ 4. มีระบบตรวจสอบการสั่งการรักษาที่เหมาะสม 5. มีระบบป้องกันความผิดพลาดในการบันทึกข้อมูล 6. มีระบบตรวจสอบบุคคลแบบ double check 7. อบรมบุคลากรให้มีความเข้าใจเรื่องการบันทึกข้อมูลที่ถูกต้อง พร้อมทั้งการแก้ไขข้อมูลเบื้องต้นเมื่อพบข้อผิดพลาด
		ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. บุคลากรสามารถแก้ไขข้อมูล เบื้องต้นเมื่อพบข้อผิดพลาด 2. แจ้งผู้ควบคุมข้อมูลแก้ไข ข้อผิดพลาดหากไม่สามารถแก้ไขได้ด้วยตนเอง

กลยุทธ์ที่ 2 การย้ายความเสี่ยง เป็นการย้ายผลเสียหายที่เกิดขึ้นจากเหตุการณ์ที่ทำให้เกิดความเสี่ยงไปสู่ บุคคลอื่น มักใช้ในกรณีที่องค์กรไม่สามารถลดความเสี่ยงได้หรือไม่คุ้มค่าที่จะลงทุนลดความเสี่ยง ดังนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	ระดับความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
-	-	-	-

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง เป็นการเปลี่ยนแปลงวิธีการทำงาน หรือกำหนดกิจกรรมเพิ่มเติมเพื่อให้ โอกาสเกิดเหตุการณ์ที่ทำให้เกิดความเสี่ยงลดน้อยลง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	ระดับความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
7.1 No Data Dictionary - ความเสี่ยงไม่มี พจนานุกรมข้อมูล	2	ปรับเปลี่ยนวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	จัดทำเอกสาร Data Dictionary
7.2 No System Blueprint - ความเสี่ยงไม่มีแบบจำลองระบบ	2	ปรับเปลี่ยนวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	จัดทำเอกสาร วิเคราะห์และ ออกแบบระบบ
7.3 No Program Document or Comments - ความเสี่ยงการควบคุม เวอร์ชันและการคอมเมนต์โค้ด	2	ปรับเปลี่ยนวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	จัดทำเอกสาร Version Control และ Source code comment

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง เป็นการบันทึกผลการวิเคราะห์และยอมรับความเสี่ยงในเรื่องที่มีโอกาส เกิดได้น้อยและ/หรือไม่คุ้มค่าที่จะลงทุนในการจัดการความเสี่ยง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	ระดับความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
-	-	-	-

การดำเนินการจัดการความเสี่ยง (Risks Treatment)

การดำเนินการจัดการความเสี่ยงประจำปีงบประมาณ 2567 เพื่อกำหนดช่วงเวลาการดำเนินกิจกรรมควบคุมหรือบรรเทาความเสี่ยง และบริหารทรัพยากรได้อย่างมีประสิทธิภาพ รายละเอียดตามตารางต่อไปนี้

ตารางแผนปฏิบัติการจัดการคำเสี่ยง													
ลำดับ	กิจกรรม	ปีงบประมาณ 2567											
		ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1	11.1 Patient Risk due to IT Error/Misuse												
	จัดทำระบบแจ้งเตือนผู้เกี่ยวข้อง เมื่อพบค่าวิกฤต ของผู้ป่วย							←	—	—	—	—	→
2	7.1 No Data Dictionary												
	จัดทำเอกสาร Data Dictionary	←	—	—	—	—	—	—	—	—	—	—	→
3	7.2 No System Blueprint												
	จัดทำเอกสาร วิเคราะห์และออกแบบระบบ	←	—	—	—	—	—	—	—	—	—	—	→
4	7.3 No Program Document or Comments												
	จัดทำเอกสารVersion Control และ Source code comment	←	—	—	—	—	—	—	—	—	—	—	→

แผนปฏิบัติการจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

ชื่อแผน พัฒนาระบบแจ้งเตือนค่าวิกฤต

กลยุทธ ลดความเสี่ยง

ตัวชี้วัด ระบบแจ้งเตือนถูกต้อง พร้อมใช้งาน

ประเภทความเสี่ยง	ระดับความเสี่ยง	โครงการ / แผนดำเนินการ	ระยะเวลาดำเนินการ	แนวทางการควบคุม	งบประมาณ (บาท)	ผู้รับผิดชอบ
11.1 Patient Risk due to IT Error/Misuse - ความเสี่ยงจากค่าวิกฤตที่อาจทำให้ เกิดอันตรายต่อผู้ป่วย	4	พัฒนาระบบแจ้งเตือน เมื่อพบค่าวิกฤต	เม.ย. 66 – ก.ย. 67	ระบบแจ้งเตือนสามารถปฏิบัติงานได้ หากพบค่าวิกฤตที่อาจทำให้ เกิดอันตรายต่อผู้ป่วย	-	นายพงษ์ปกรณ์ ศิริภาษณ์ นายศุภวิชญ์ ชัยสิทธิ์

ชื่อแผน จัดทำเอกสาร Data Dictionary

กลยุทธ หลีกเลี่ยงความเสี่ยง

ตัวชี้วัด มีเอกสาร Data Dictionary มีครบทุกตาราง

ประเภทความเสี่ยง	ระดับความเสี่ยง	โครงการ / แผนดำเนินการ	ระยะเวลาดำเนินการ	แนวทางการควบคุม	งบประมาณ (บาท)	ผู้รับผิดชอบ
7.1 No Data Dictionary - ความเสี่ยงไม่มี พจนานุกรมข้อมูล	2	จัดทำเอกสาร Data Dictionary	ต.ค. 66 – ก.ย. 67	เอกสาร Data Dictionary ครบทุกตารางในฐานข้อมูล	-	นายพงษ์ปกรณ์ ศิริภาษณ์ นายศุภวิชญ์ ชัยสิทธิ์

ชื่อแผน จัดทำเอกสาร วิเคราะห์และออกแบบระบบ

กลยุทธความเสี่ยง หลีกเลี่ยงความเสี่ยง

ตัวชี้วัด มีเอกสารวิเคราะห์และออกแบบระบบ ที่พัฒนาเองครบทุกระบบ

ประเภทความเสี่ยง	ระดับความเสี่ยง	โครงการ / แผนดำเนินการ	ระยะเวลาดำเนินการ	แนวทางการควบคุม	งบประมาณ (บาท)	ผู้รับผิดชอบ

7.2 ความเสี่ยงจาก No System Blueprint - ความเสี่ยงไม่มีแบบจำลองระบบ	2	จัดทำเอกสารวิเคราะห์และออกแบบระบบ	ต.ค. 66 – ก.ย. 67	เอกสารวิเคราะห์และออกแบบระบบครบทุกระบบที่พัฒนาเอง	-	นายพงษ์ปกรณ์ ศิริภาษณ์ นายศุภวิชญ์ ชัยสิทธิ์

ชื่อแผน จัดทำเอกสาร วิเคราะห์และออกแบบระบบ

กลยุทธความเสี่ยง หลีกเลี่ยงความเสี่ยง

ตัวชี้วัด มีเอกสารวิเคราะห์และออกแบบระบบ ที่พัฒนาเองครบทุกระบบ

ประเภทความเสี่ยง	ระดับความเสี่ยง	โครงการ / แผนดำเนินการ	ระยะเวลาดำเนินการ	แนวทางการควบคุม	งบประมาณ (บาท)	ผู้รับผิดชอบ
7.3 No Program Document or Comments - ความเสี่ยงการควบคุมเวอร์ชันและการคอมเมนต์โค้ด	2	จัดทำเอกสาร version control และ source code comment	ต.ค. 66 – ก.ย. 67	เอกสาร version control และ source code commentของผู้พัฒนาโปรแกรม	-	นายพงษ์ปกรณ์ ศิริภาษณ์ นายศุภวิชญ์ ชัยสิทธิ์

แผนการดำเนินการจัดการความเสี่ยง ปีงบประมาณ 2568

ระดับความเสี่ยง	ประเด็นความเสี่ยง	แนวทางการพัฒนา
ความเสี่ยงสูงมาก	-	-
ความเสี่ยงสูง	-	-
ความเสี่ยงปานกลาง	11.1 Patient Risk due to IT Error/Misuse	1. พัฒนาเพิ่มเติมระบบแจ้งเตือนค่าวิกฤตให้ครอบคลุม 2. พัฒนาระบบการแจ้งเตือนผู้เกี่ยวข้องทันที
ความเสี่ยงต่ำ	1.1 Servers and Main Switches Crash or Failure	
	1.2 Network Switches Crash or Failure	
	1.3 Workstations and Printers Failure	
	2.1 Operating System Failure	
	3.1 Front Offices	
	3.2 Back Offices	
	4.1 Intranet	ระบบเครือข่ายภายในมีทรัพยากรใช้งานเพียงพอ จึงยอมรับความเสี่ยง
	4.2 Internet	
	5.1 Backup Error	
	5.2 Data Loss Error	
	6.1 Data Backup	
	6.2 Data Protection Policy and Regulations	
	6.3 PDPA Implementation	
	ความเสี่ยงต่ำ(1-3)	
	7.1 No Data Dictionary	
	7.2 No System Blueprint	
	7.3 No Program Document or Comments	
	8.1 Vendor Stop Support	1. มีรายละเอียดให้ทางบริษัทจะต้องส่งมอบเอกสารสำคัญและข้อมูลทั้งหมดเมื่อหมดสัญญาให้ชัดเจน 2. ทำสัญญาส่งมอบเอกสารสำคัญและข้อมูล ทั้งหมดเมื่อหมดสัญญาให้ครบทุกบริษัท

	9.1 IT- Hacking Unauthorized Intrusions	แยกการใช้งานของเครื่องมือแพทย์และอุปกรณ์ คอมพิวเตอร์ออกจาก WIFI ที่ใช้ร่วมกัน
	10.1 Flooding –Internal	ตรวจสอบพื้นที่ที่เสี่ยงที่มีอุบัติการณ์น้ำรั่วไหล อย่างสม่ำเสมอ
	10.2 Flooding External	จัดซ้อมแผนเผชิญเหตุอุทกภัยในพื้นที่
	10.3 Fire – Internal	จัดซ้อมแผนปฏิบัติเมื่อเกิดอัคคีภัยในโรงพยาบาล
	10.4 Fire – External	จัดซ้อมแผนรับมืออัคคีภัยจากภายนอก
	10.5 Utilities – Electricity	ระบบเครื่องสำรองไฟป้องกันไม่ให้ไฟฟ้าสร้างความเสียหายต่อทรัพย์สิน IT จึงยอมรับความเสี่ยง
	10.6 Criminal – Theft	จัดทำแผนจัดซื้อกล้องวงจรปิดทดแทน
	10.7 Criminal - Break – ins	จัดทำแผนจัดซื้อกล้องวงจรปิด ทดแทน
	10.8 Civil Unrest – Protest, Mob	โรงพยาบาลมีเจ้าหน้าที่รักษาความปลอดภัย และมีแผนเผชิญเหตุจลาจล จึงยอมรับความเสี่ยง