มีกระบวนการประเมินและให้คะแนนความเสี่ยงของของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายได้ขอบเขตการให้บริการ สาธารณสุขของหน่วยงาน

แบบประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17

IT Components	Vulnerability		Score
- **IT - Hardware**			
1.1 Server and Main Switches Crash or Failure	อาจแยกประเมิน server แต่ละเครื่องหรือประเมินทั้งห้องร่วมกัน (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 4 = 5 5 – 7 = 4 8 – 11 = 3 12 – 14 = 2 15 – 16 = 1	● **กายภาพของห้อง server** - ระบบล็อคประตู => 1 - ระบบสลับการทำงานเครื่องปรับอากาศ => 1 - ระบบวัดอุณหภูมิ => 1 - ระบบตรวจจับควัน => 0 - ระบบแจ้งเตือนอัคคีภัย => 0 - ถังดับเพลิงที่เหมาะสม => 1 - ความสะอาด => 1 - การกำจัดสิ่งของไม่จำเป็นและเชื้อไฟออกจากห้อง => 1	6	**2**
	● **การจัดระเบียบสายสัญญาณและป้ายกำกับ** - สายสัญญาณด้านหน้า => 0 - สายสัญญาณด้านหลัง => 0 - ป้ายกำกับสายสัญญาณ => 1 - ป้ายกำกับ server => 1 - แผนผังตำแหน่งสายและช่องสัญญาณ => 1	3	
	● **การป้องกันการโจมตีพื้นฐาน** - มี firewall => 1 - เก็บ log => 1 - ตรวจสอบ log เป็นระยะ => 1	3	
1.2 Network Switches Crash or Failure	ประเมิน switches ที่อยู่ในจุดต่างๆ นอกห้อง (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 2 = 5 3 – 4 = 4 5 – 6 = 3 7 = 2 8 = 1	● **กายภาพของตู้ switches** - มีตู้ => 1 - ระบบล็อคประตู => 1 - ความสะอาด => 1 - การกำจัดสิ่งของไม่จำเป็น และเชื้อไฟออกจากตู้ => 1	4	**1**
	● **การจัดระเบียบสายสัญญาณและการป้องกันสัตว์กัดแทะ** - สายสัญญาณด้านหน้า => 1 - สายสัญญาณด้านหลัง => 1 - การป้องกันสัตว์กัดแทะ => 1	3	

IT Components	Vulnerability		Score
	● **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 0	0	
1.3 Workstation and Printers Failure	ประเมินภาพรวม PC ที่อยู่ในจุดต่าง ๆ ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 2 = 5 3 – 4 = 4 5 – 6 = 3 7 = 2 8 = 1	● **กายภาพของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง** - ระบบป้องกันสายไฟสายสัญญาณ => 0 - ระบบป้องกันไฟตกไฟกระชาก => 1 - ความสะอาด => 1 - การป้องกันน้ำและอาหารหกใส่ => 0 - ระบบป้องกันคนนอกเข้าถึง => 1	3	**3**
	● **ระบบปฏิบัติการและระบบขับเคลื่อน (driver)** - ถูกลิขสิทธิ์ทั้งหมด => 1 - เป็น version ที่ทันสมัยหรือเหมาะสมที่สุด => 1	2	
	● **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
2. IT – System Software			
2.1 Operating System Failure	ประเมินภาพรวม OS ที่อยู่ใน server ทั้งหมด ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 = 5 1 = 4 2 = 3 3 = 1	● **ระบบปฏิบัติการและระบบขับเคลื่อน (driver)** - ถูกลิขสิทธิ์ทั้งหมด => 1 - เป็น version ที่ทันสมัยหรือเหมาะสมที่สุด => 1	2	**1**
	● **แผ่นติดตั้งระบบปฏิบัติการ ในกรณี ต้องกู้คืนระบบ** - มีแผ่นติดตั้งครบทั้งหมด => 1	1	
3. IT- Applications			
3.1 Front Offices	ประเมินระบบ HIS ที่ใช้บริการส่วนหน้าทั้งหมดของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	● **การใช้ทรัพยากรของ server** - CPU ไม่ overload => 1 - หน่วยความจำยังไม่หมด => 1 - พื้นที่ hard disk ยังเพียงพอ => 1	3	**1**
	● **แผ่นติดตั้งระบบ HIS ในกรณี ต้องกู้คืนระบบ** - มีแผ่นติดตั้งครบทั้งหมด => 1	1	

IT Components	Vulnerability		Score
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
3.2 Back Offices	ประเมินระบบที่ใช้บริการส่วนหลังทั้งหมดของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **การใช้ทรัพยากรของ server** - CPU ไม่ overload => 1 - หน่วยความจำยังไม่หมด => 1 - พื้นที่ hard disk ยังเพียงพอ => 1	3	**1**
	• **แผ่นติดตั้งระบบ HIS ในกรณี ต้องกู้คืนระบบ** - มีแผ่นติดตั้งครบทั้งหมด => 1	1	
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
4. IT- Communication, Connectivity			
4.1 Intranet	ประเมินระบบเครือข่ายภายในของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **การใช้ทรัพยากรของระบบเครือข่าย** - traffic ไม่เกินร้อยละ 80 => 1 - bandwidth ไม่เกินร้อยละ 80 => 1	2	**1**
	• **การแยกวง เช่น vlan** - มีการแยกวงที่เหมาะสม => 1 - แยกระบบ HIS ออกจากระบบอินเทอร์เน็ต => 1	2	
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
4.2 Internet	ประเมินระบบเครือข่ายที่เชื่อมต่ออินเทอร์เน็ตของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **การใช้ทรัพยากรของระบบเครือข่าย** - Traffic ไม่เกินร้อยละ 80 => 1 - bandwidth ไม่เกินร้อยละ 80 => 1	2	**2**
	• **การเพิ่มสายสำรอง กรณีผู้ให้บริการหยุดชะงัก** - มีสายสำรองที่ 2 => 1 - มีสายสำรองที่ 3 => 0	1	
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
5. IT – Operational (Human) Error			
5.1 Backup Error	ประเมินระบบงานที่ทำให้การสำรองข้อมูลเกิดความผิดพลาด		

IT Components	Vulnerability		Score
	(เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **ขั้นตอนการปฏิบัติงานที่เหมาะสม** - มีขั้นตอนการปฏิบัติงานชัดเจน => 1 - ผู้สำรองข้อมูลเข้าใจและปฏิบัติได้ถูกต้อง => 1	2	**2**
	• **ระบบตรวจสอบข้อมูลสำรอง** - มีระบบตรวจสอบความครบถ้วนสมบูรณ์ => 1 - มีการทดลอง restore กลับ => 0	1	
	• **ระบบกำกับดูแลโดยผู้บังคับบัญชา** - กำกับดูแลเป็นประจำ => 1	1	
5.2 Data Loss Error	ประเมินระบบงานที่ทำให้ข้อมูลที่ผู้ใช้บันทึกไม่เกิดความผิดพลาด (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **ขั้นตอนการปฏิบัติงานที่เหมาะสม** - มีขั้นตอนการปฏิบัติงานชัดเจน => 1 - ผู้บันทึกข้อมูลเข้าใจและปฏิบัติได้ถูกต้อง => 1	2	**1**
	• **ระบบป้องกันข้อมูลสูญหายหรือผิดพลาด** - ปิดช่องว่างจากขั้นตอนการทำงาน => 1 - ปิดช่องว่างจากโปรแกรม => 1	2	
	• **ระบบกำกับดูแลโดยผู้บังคับบัญชา** - กำกับดูแลเป็นประจำ => 1	1	
6. Data Loss and Privacy Breach			
6.1 Data Backup	ประเมินระบบงานที่ทำให้ข้อมูลสำรองสูญหาย (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **ระบบ offline backup** - มีระบบ offline backup => 1 - อุปกรณ์เก็บข้อมูลสำรองมีจำนวนเพียงพอ => 1 - อุปกรณ์เก็บข้อมูลสำรองมีที่เก็บปลอดภัย => 1	3	**1**
	• **ระบบป้องกันข้อมูลสำรองถูกจารกรรม** - มีระบบห้ามบุคลากรนำข้อมูลสำรองออกสู่ภายนอก => 1	1	
	• **ระบบกำกับดูแลโดยผู้บังคับบัญชา** - กำกับดูแลเป็นประจำ => 1	1	
6.2 Data Protection Policy and Regulations	ประเมินการป้องกันความลับและความเป็นส่วนตัวของข้อมูล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4	• **ระบบห้ามการเข้าถึงข้อมูลที่บุคลากรไม่มีส่วนเกี่ยวข้อง** - มีระบบล็อคหรือมีระเบียบห้ามการเข้าถึงข้อมูลที่ตนเองไม่มีส่วนเกี่ยวข้อง => 1	1	**3**

IT Components	Vulnerability		Score
3 = 3 4 = 2 5 = 1	• **ระบบอภิบาลข้อมูล** - มีการสำรวจและจัดทำทะเบียนข้อมูลสำคัญ => 1 - มีการจัดประเภทข้อมูลที่ต้องปกปิด => 1 - มีขั้นตอนการจัดการข้อมูลสำคัญตั้งแต่ต้นทางจนถึงปลายทาง => 0	2	
	• **ระบบกำกับดูแลโดยผู้บังคับบัญชา** - กำกับดูแลเป็นประจำ => 0	0	
6.3 PDPA Implementation			
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	- ประเมินการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้คะแนน 0 ถึง 5 => 5	4	**2**
7. IT – Future Development			
7.1 No Data Dictionary	ประเมินเอกสารที่ใช้พัฒนาระบบต่อเนื่องในอนาคต (เลือก 0 หรือ 1)		
เกณฑ์คะแนน 0 = 5 1 = 1	- มีเอกสาร Data Dictionary ครบทุกตารางในฐานข้อมูล => 0	1	**1**
7.2 No System Blueprint	ประเมินเอกสารที่ใช้พัฒนาระบบต่อเนื่องในอนาคต (เลือก 0 หรือ 1)		
เกณฑ์คะแนน 0 = 5 1 = 1	- มีเอกสาร วิเคราะห์และออกแบบระบบที่พัฒนาเอง => 0	1	**1**
7.3 No System Document or Comments	ประเมินการบันทึก comment และ version ของผู้พัฒนาโปรแกรม (เลือก 0 หรือ 1)		
เกณฑ์คะแนน 0 = 5 1 = 1	- มีเอกสาร version control และ source code comment => 0	1	**1**
8. IT – Vendor and Outsource Failure			
8.1 Vendor stop Support	ประเมินสัญญาที่ทำกับบริษัทภายนอก (เลือก 0 หรือ 1)		
เกณฑ์คะแนน 0 = 5 1 = 1	- มีสัญญาที่บริษัทจะต้องส่งมอบเอกสารสำคัญและข้อมูลทั้งหมดเมื่อหมดสัญญา => 1	1	**1**
9. IT – Hacking Unauthorized Intrusions			
ประเมินภาพรวมจุดต่าง ๆ ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)			

IT Components	Vulnerability		Score
เกณฑ์คะแนน 0 – 2 = 5 3 – 4 = 4 5 – 6 = 3 7 = 2 8 – 9 = 1	• **เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง** - มีระบบหรือระเบียบล็อคหน้าจอเมื่อไม่มีผู้ใช้งาน => 1 - เข้ารหัสข้อมูลส่วนตัวผู้ป่วย => 0 - มีการป้องกันการถ่ายภาพหน้าจอในจุดที่คนนอกเข้าถึง => 0	1	**3**
	• **ระบบเครือข่าย** - ปิดสัญญาณช่องเชื่อมต่อเครือข่ายที่ไม่มีการใช้าน => 0 - มีการเข้ารหัสและตั้งรหัสผ่านการใช้ WIFI access => 1 - เปลี่ยนรหัส WIFI บ่อย ๆ => 0	1	
	• **ระเบียบปฏิบัติด้านความมั่นคงปลอดภัย** - ห้ามใช้ username ร่วมกัน => 1 - ตั้ง username และ password ซับซ้อน => 1 - ห้ามติด password ไว้ในที่เปิดเผย => 1	3	
10. Environment Factors			
เกณฑ์คะแนน 0 = 5 1 = 1	**10.1 Flooding – Internal** ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากน้ำรั่วในสำนักงาน (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้น้ำรั่วไหลลงสู่ทรัพย์สิน IT => 1	1	**1**
	10.2 Flooding – External ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากอุทกภัยในพื้นที่ (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้อุทกภัยสร้างความเสียหายต่อทรัพย์สิน => 0	0	**5**
	10.3 Fire – Internal ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟไหม้ในโรงพยาบาล (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้ไฟไหม้ทรัพย์สิน => 1 -	1	**1**
	10.4 Fire – External ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากอัคคีภัยในพื้นที่ (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้ไฟไหม้ทรัพย์สิน IT => 0	0	**5**
	10.5 Utilities – Electricity ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟฟ้าตกหรือกระชาก (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้ไฟฟ้าสร้างความเสียหายต่อทรัพย์สิน IT => 1	1	**1**
	10.6 Criminal – Theft ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากโจรกรรม (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้มีโจรหรือขโมยสร้างความเสียหายต่อทรัพย์สิน IT => 1	1	**1**
	10.7 Criminal – Break-ins ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากการงัดแงะหรือย่องเบา (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้มีโจรหรือขโมยสร้างความเสียหายต่อทรัพย์สิน IT => 1	1	**1**

IT Components	Vulnerability		Score
	10.8 Civil Unrest – Protest, Mob ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากเหตุจลาจล วัยรุ่นทะเลาะกัน (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้มีผู้สร้างความเสียหายต่อทรัพย์สิน IT => 0	0	**5**
11. Patient Risks due to IT Errors/Misuse			
ประเมินจุดอ่อนการใช้ IT ที่อาจทำให้เกินอันตรายต่อผู้ป่วย (เลือก 0 หรือ 1 แต่ละข้อ)			
เกณฑ์คะแนน 0 – 2 = 5 3 – 4 = 4 5 – 6 = 3 7 = 2 8 = 1	● **ระบบแจ้งเตือนเมื่อพบค่าวิกฤต** - มีระบบแจ้งเตือนเมื่อพบค่าวิกฤตของผู้ป่วย => 1 - มีการแจ้งเตือนผู้เกี่ยวข้องทันที => 1 - มีการตรวจสอบว่าระบบแจ้งเตือนทำงานได้ตามปกติ => 1	3	**2**
	● **ระบบตรวจสอบการสั่งการรักษาหรือไม่สั่งการรักษาที่เหมาะสม** - มีระบบตรวจสอบการไม่สั่งการรักษาที่เหมาะสมและแจ้งเตือน => 1 - มีระบบตรวจสอบการสั่งการรักษาที่เหมาะสม => 1	2	
	● **ระบบป้องกันความผิดพลาดในการบันทึกข้อมูล ตรวจสอบบุคคล หัวหน้าตรวจสอบ** - มีระบบป้องกันความผิดพลาดในการบันทึกข้อมูล => 1 - มีระบบตรวจสอบบุคคลแบบ double check => 1 - มีระบบหัวหน้ายืนยันการดำเนินการกรณีสำคัญยิ่งยวด => 0	2	

ผลการประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศ ปี พ.ศ.2567

IT Components	Probability (P)	Impact (I)	Risk = P x I
1. IT – Hardware			
1.1 Servers Crash or Failure	1 **2** 3 4 5	1 2 3 4 **5**	10
1.2 Network Switches Crash or Failure	**1** 2 3 4 5	1 2 3 **4** 5	4
1.3 Workstations Failure	1 2 **3** 4 5	**1** 2 3 4 5	3
2. IT – System Software			
2.1 Operating System Failure	**1** 2 3 4 5	1 **2** 3 4 5	2
3. IT – Applications			
3.1 Front Offices	**1** 2 3 4 5	**1** 2 3 4 5	1
3.2 Back Offices	**1** 2 3 4 5	1 2 3 **4** 5	4
4. IT – Communications, Connectivity			
4.1 Intranet	**1** 2 3 4 5	1 2 3 4 **5**	5
4.2 Internet	1 **2** 3 4 5	1 2 3 4 **5**	10
5. IT – Operational (Human) Error			
5.1 Backup Error	1 **2** 3 4 5	1 2 **3** 4 5	6
5.2 Data Loss Error	**1** 2 3 4 5	1 **2** 3 4 5	1
6. Data Loss and Privacy Breach			
6.1 Data Backup	**1** 2 3 4 5	1 2 **3** 4 5	3
6.2 Data Protection Policy and Regulations	1 2 **3** 4 5	1 **2** 3 4 5	6
6.3 PDPA Implementation	1 **2** 3 4 5	1 2 3 4 **5**	10
7. IT –Future Development			
7.1 No Data Dictionary	**1** 2 3 4 5	**1** 2 3 4 5	1
7.2 No System Blueprint	**1** 2 3 4 5	**1** 2 3 4 5	1
7.3 No Program Document or Comments	**1** 2 3 4 5	**1** 2 3 4 5	1
8. IT – Vendor and Outsource Failure			
8.1 Vendor Stop Support	**1** 2 3 4 5	**1** 2 3 4 5	1
9. IT – Hacking, Unauthorized Intrusions	1 2 **3** 4 5	1 2 3 4 **5**	15
10. Environment Factors			
10.1 Flooding – Internal	**1** 2 3 4 5	1 2 3 4 **5**	5
10.2 Flooding – External	**1** 2 3 4 5	1 2 3 4 **5**	5
10.3 Fire – Internal	**1** 2 3 4 5	1 2 3 4 **5**	5
10.4 Fire – External	**1** 2 3 4 5	1 2 3 4 **5**	5
10.5 Utilities – Electricity	**1** 2 3 4 5	1 2 3 4 **5**	5
10.6 Criminal – Theft	**1** 2 3 4 5	1 2 3 4 **5**	5
10.7 Criminal – Break-ins	**1** 2 3 4 5	1 2 3 4 **5**	5
10.8 Civil Unrest – Protest, Mob	1 2 3 4 **5**	1 2 3 4 **5**	25
11. Patient Risks due to IT Errors/Misuse	1 **2** 3 4 5	1 **2** 3 4 5	4
12. Other	1 2 3 4 5	1 2 3 4 5	

เมื่อคำนวณคะแนนความเสี่ยงแล้วนำคะแนนความเสี่ยงมาพิจารณาตามแผนผังประเมินความเสี่ยง ดังนี้

แผนผังประเมินความเสี่ยง

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

จากแผนผังประเมินความเสี่ยง จะเห็นว่า เหตุการณ์ที่มีค่าคะแนนความเสี่ยงตั้งแต่ 17 ถึง 25 จะเป็นเหตุการณ์ที่เร่งต้องจัดการความเสี่ยงโดยเร่งด่วน (แสดงในตารางเป็นสีแดง) ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยง ตั้งแต่ 1-3 จะเป็นเหตุการณ์ที่ยังไม่ต้องเร่งรีบจัดการ (แสดงในตารางเป็นสีเหลือง)