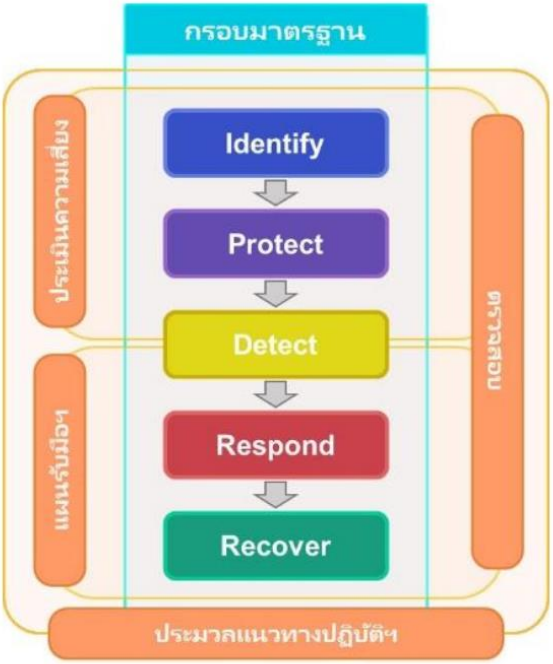
การประเมินความเสี่ยงและแผนรับมือเหตุภัยคุกคามทางไซเบอร์ โรงพยาบาลแคนดง

1. หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคง ปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล เพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การจัดทำประมวลแนวทางปฏิบัติ มีองค์ประกอบ ดังนี้

- แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์



รูปที่ 1 แสดงประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เอกสารฉบับนี้ เป็นการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การบริหารจัดการความเสี่ยงมีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ของหน่วยงานและยังรวมถึงการปกป้อง “ภารกิจ” ของหน่วยงานให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับ

เทคโนโลยีสารสนเทศอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงาน

หน่วยงานจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐานเพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยงและเพื่อความสามารถในการดำเนินภารกิจของหน่วยงานให้บรรลุผลสำเร็จไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเพียงเท่านั้น

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงของโรงพยาบาล โดยการประเมินความเสี่ยงทำให้สามารถ

- ระบุเหตุการณ์ความเสี่ยงที่เป็นภัยคุกคาม และอาจนำไปสู่กระทบต่อโรงพยาบาลในด้านต่างๆ
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมองค์กรเพื่อให้บุคลากรมีส่วนร่วมในการจัดการเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2. วัตถุประสงค์

1. เพื่อให้การจัดการภายในหน่วยงาน มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ
2. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของหน่วยงาน
3. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์
4. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และความมั่นคงปลอดภัยไซเบอร์
5. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

3. ขอบเขตการดำเนินงาน (SCOPE)

เอกสารฉบับนี้เป็นการดำเนินงาน เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

4. นิยาม

4.1 ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความหรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายของหน่วยงาน ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน งบประมาณ และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

4.2 ภัยคุกคามไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

4.3 การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ หมายถึง การดำเนินการในการป้องกันภัยคุกคามไซเบอร์โดยใช้มาตรการ และกระบวนการบริหารความเสี่ยง เพื่อวิเคราะห์ภัยคุกคามไซเบอร์ ประเมินความเสี่ยงที่อาจจะเกิดขึ้น โดยการจัดหา จัดทำมาตรการ จัดหาวัสดุอุปกรณ์ เพื่อป้องกันและลดผลกระทบจากภัยคุกคามไซเบอร์ความมั่นคงปลอดภัยไซเบอร์หมายถึง วิธีการ มาตรการ หรือการดำเนินการใดๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ การรักษาความครบถ้วน และสภาพพร้อมใช้งาน ของอุปกรณ์และข้อมูลภายในระบบสารสนเทศของโรงพยาบาล

4.4 ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด ทำไม และเกิดขึ้นได้อย่างไร ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

4.5 การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 5 ระดับ คือ สูงมาก สูง ปานกลาง ต่ำ และต่ำมาก

4.6 การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่หน่วยงานยอมรับได้ ซึ่งการจัดการความเสี่ยงอาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง ดังนี้

- **การยอมรับความเสี่ยง (Risk Acceptance)** เป็นการยอมรับความเสี่ยงที่เกิดขึ้นเนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง
- **การลด/การควบคุมความเสี่ยง (Risk Reduction)** เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้
- **การกระจายความเสี่ยงหรือการโอนความเสี่ยง (Risk Sharing)** เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้อื่นช่วยแบ่งความรับผิดชอบไป
- **การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)** เป็นการจัดการกับความเสี่ยงที่อยู่ในระดับสูงและหน่วยงานไม่อาจยอมรับได้ จึงต้องตัดสินใจยกเลิกโครงการ/กิจกรรมนั้นไป

4.7 การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ

- การควบคุมเพื่อการป้องกัน
- การควบคุมเพื่อให้ตรวจสอบ
- การควบคุมโดยการชี้แนะ
- การควบคุมเพื่อการแก้ไข

5. โครงสร้างการบริหารความเสี่ยงและการควบคุมภายในของโรงพยาบาล

เพื่อสร้างการมีส่วนร่วมในระบบการบริหารความเสี่ยงและการควบคุมภายในของโรงพยาบาล การจัดโครงสร้างการบริหารความเสี่ยงและการควบคุมภายในถือว่ามีความสำคัญมาก เนื่องจากต้องจัดให้ผู้ที่เกี่ยวข้องทั้งในระดับหน่วยงาน ระดับโรงพยาบาล และระดับนโยบาย ได้มีการแบ่งหน้าที่ความรับผิดชอบบทบาทหน้าที่ของแต่ละองค์ประกอบให้มีความชัดเจนมากที่สุด เพื่อให้เกิดความเชื่อมโยงการทำงานของแต่ละคณะโดยโครงสร้างการบริหารความเสี่ยงและการควบคุมภายในของโรงพยาบาล

ทั้งนี้การบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จะใช้โครงสร้างการบริหารความเสี่ยงและการควบคุมภายในของโรงพยาบาล ในการกกับดูแล โดยมีคณะทำงานบริหารความเสี่ยงและการควบคุม ภายในระดับหน่วยงาน เช่น ศูนย์คอมพิวเตอร์ ศูนย์นวัตกรรมและเทคโนโลยีการศึกษา สถานส่งเสริมและพัฒนาระบบสารสนเทศเพื่อการจัดการ (MIS) เป็นต้น เป็นผู้บริหารจัดการเความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และระบบเทคโนโลยีสารสนเทศ ที่หน่วยงานเป็นผู้รับผิดชอบ

6. หลักการบริหารความเสี่ยง

หลักการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Treadway Commission) และ ISO 27001 มีดังนี้

1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2. การระบุปัจจัยเสี่ยง (Event Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. การระบุวิธีการจัดการความเสี่ยง (Risk Response)
5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
7. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

6.1 การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

เพื่อให้โรงพยาบาลมีระบบในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล โดยสามารถดำเนินการอย่างมีประสิทธิภาพ และบรรลุเป้าหมายตามแผนยุทธศาสตร์ของโรงพยาบาล จึงได้ตั้งเป้าหมายในการดำเนินการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังตารางที่ 6.1

ตาราง 6.1 เป้าหมายในการดำเนินการบริหารความเสี่ยงตัวชี้วัดความสำเร็จ

เป้าหมายในการดำเนินการบริหารความเสี่ยง	ตัวชี้วัดความสำเร็จ
1. เพื่อให้โรงพยาบาลมีแผนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และดำเนินการตามแผนอย่างครบถ้วน	มีแผนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีการรายงานผล การดำเนินการตามแผนการบริหารความเสี่ยงใน ทุก ๆ ปีงบประมาณ
2.เพื่อให้ผู้บริหารและบุคลากรทุกระดับในโรงพยาบาล มีความรู้ ความเข้าใจกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	-ผู้บริหารและบุคลากรมีความรู้ความเข้าใจในหลักการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ -มีหลักสูตร e-courseware เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างความรู้ความเข้าใจให้บุคลากร นักเรียน นักศึกษาของโรงพยาบาล
3. เพื่อให้โรงพยาบาลสามารถบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ทันเวลา จนป้องกันและลดความเสี่ยงให้ อยู่ในระดับที่ยอมรับได้	มีการประเมินผลความสำเร็จในการดำเนินการตามแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ โดยระดับความเสี่ยงที่ เหลืออยู่ต้องอยู่ในระดับที่ยอมรับได้

6.2 การระบุปัจจัยเสี่ยง (Event Identification)

ปัจจัยเสี่ยง (Risk Factor) คือ สาเหตุที่มาของความเสี่ยง ที่ทำให้ไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่วางไว้ การระบุปัจจัยเสี่ยงควรมีความเชื่อมโยงกับผลความสำเร็จตามเป้าหมายของโรงพยาบาล โดยคำนึงถึง วัตถุประสงค์ตามแผนงานของหน่วยงาน และโอกาสของเหตุการณ์ที่อาจจะเกิดขึ้น อันจะส่งผลกระทบต่อหน่วยงาน ทำให้ไม่สามารถบรรลุวัตถุประสงค์นั้นได้ โรงพยาบาล ได้จัดประเภทของความเสี่ยงในการระบุความเสี่ยง ออกเป็น 9 ประเภทด้วยกัน และได้กำหนดเกณฑ์ดังกล่าว เพื่อใช้ในการระบุปัจจัยเสี่ยงแยกตามประเภท ความเสี่ยงของหน่วยงานทุกระดับในโรงพยาบาล ดังนี้

6.2.1 ประเภทของความเสี่ยง

1) **ความเสี่ยงด้านกลยุทธ์(Strategic Risk)** ตัวย่อ S ความเสี่ยงที่เกี่ยวกับการบรรลุเป้าหมาย และพันธกิจในภาพรวม โดยความเสี่ยงที่อาจจะเกิดขึ้นเป็นความเสี่ยงเนื่องจากการ เปลี่ยนแปลงของสถานการณ์และเหตุการณ์ภายนอก ส่งผลต่อกลยุทธ์ที่กำหนดไว้ ไม่สอดคล้องกับประเด็นยุทธศาสตร์/วิสัยทัศน์ หรือเกิดจากการกำหนดกลยุทธ์ที่ขาดการ มีส่วนร่วม ทำให้โครงการขาดการยอมรับและโครงการไม่ได้นำไปสู่การแก้ไขปัญหาหรือการตอบสนองต่อความต้องการของผู้รับบริการหรือผู้มีส่วนได้ส่วนเสียอย่างแท้จริง หรือเป็น ความเสี่ยงที่เกิดขึ้นจากการตัดสินใจผิดพลาด หรือนำการตัดสินใจนั้นมาใช้อย่างไม่ถูกต้อง

2) ความเสี่ยงด้านการเงินและทรัพย์สิน (Financial and Asset Risk) ตัวย่อ F ความเสี่ยงที่ เกี่ยวกับการเงินและทรัพย์สิน ซึ่งมีผลทำให้โรงพยาบาลต้องมีรายได้ลดน้อยลง หรือ ค่าใช้จ่ายเพิ่มขึ้น หรือความเสียหายต่อทรัพย์สินของโรงพยาบาล การจัดการความเสี่ยงจึงมีลักษณะของการปกป้องทรัพย์สิน การเงิน และมาตรการประหยัดค่าใช้จ่าย

3) ความเสี่ยงด้านปฏิบัติงาน (Operational Risk) ตัวย่อ O ความเสี่ยงที่เกิดขึ้นใน กระบวนการทำงานตามปกติทุกขั้นตอน โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับ กระบวนการ เทคโนโลยีสารสนเทศ วัสดุ/อุปกรณ์ บุคลากรที่ปฏิบัติงาน ฯลฯ ซึ่งจะส่งผลกระทบต่อ ความสำเร็จของการดำเนินงานตามแผนปฏิบัติการหรือแผนกลยุทธ์ของโรงพยาบาล

4) ความเสี่ยงด้านกฎระเบียบ (Compliance Risk) ตัวย่อ C ความเสี่ยงที่เกี่ยวข้องกับ การปฏิบัติตามกฎระเบียบต่าง ๆ โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยงเนื่องจาก ความไม่ชัดเจน ความไม่ทันสมัย หรือความไม่ครอบคลุมของกฎหมาย กฎระเบียบ ข้อบังคับ ต่าง ๆ รวมถึงการทำนิติกรรมสัญญา การร่างสัญญาที่ไม่ครอบคลุมการดำเนินงานจากเหตุการณ์ภายนอก

5) ความเสี่ยงด้านภาพลักษณ์และชื่อเสียง (Image and Reputation Risk) ตัวย่อ IM ภาพพจน์ของโรงพยาบาลอาจเกิดความเสียหาย เนื่องจากมีการเผยแพร่ข่าวสื่อเชิงลบ ในระดับจังหวัด ระดับชาติ และระดับนานาชาติ

6) ความเสี่ยงด้านสุขภาพและความปลอดภัย (Health and Safety Risk) ตัวย่อ HS ความเสี่ยง เกี่ยวกับการเกิดอุบัติเหตุ การบาดเจ็บ ความเจ็บป่วยที่เกิดขึ้นกับนักศึกษาและบุคลากร ของโรงพยาบาล

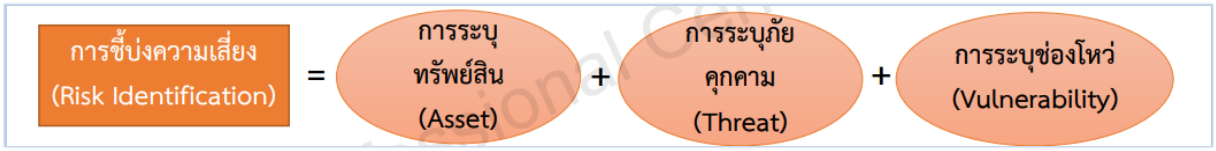
7) ความเสี่ยงด้านบุคลากร (Personnel Risk) ตัวย่อ P ความเสี่ยงที่เกี่ยวข้องกับพนักงาน ของโรงพยาบาล เป็นความเสี่ยงจากบุคลากรสายวิชาการ และบุคลากรสายปฏิบัติการ ความเสี่ยงนี้ครอบคลุมถึงการบริหารงานบุคคล เช่น อัตราการลาออกของพนักงานโรงพยาบาล

8) ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk) ตัวย่อ D เป็นความเสี่ยง เกี่ยวกับการจัดการเทคโนโลยีดิจิทัลของแต่ละหน่วยงานในการกำหนดให้มีการจัดการ ความเสี่ยงตามพื้นฐานความจำเป็นของงานแต่ละงาน เช่น การรักษาความปลอดภัยของ ข้อมูล การเรียกข้อมูลกลับคืน เป็นต้น

9) ความเสี่ยงด้านธรรมาภิบาลและอัตตาภิบาล (Good Governance and Self Governance Risk) ตัวย่อ G เป็นความเสี่ยงที่อาจเกิดขึ้นในกระบวนงานหลักขององค์กร เพื่อให้มั่นใจได้ว่าการดำาเนินการเป็นไปตามหลัก ธรรมาภิบาลและอัตตาภิบาล เช่น ความมี ประสิทธิภาพ ความคุ้มค่า โปร่งใส ตรวจสอบได้ เป็นต้น รวมถึงความเสี่ยงในการกำกับดูแลตนเองที่ดีด้วย

6.2.2 การชี้บ่งความเสี่ยง (Risk identification)

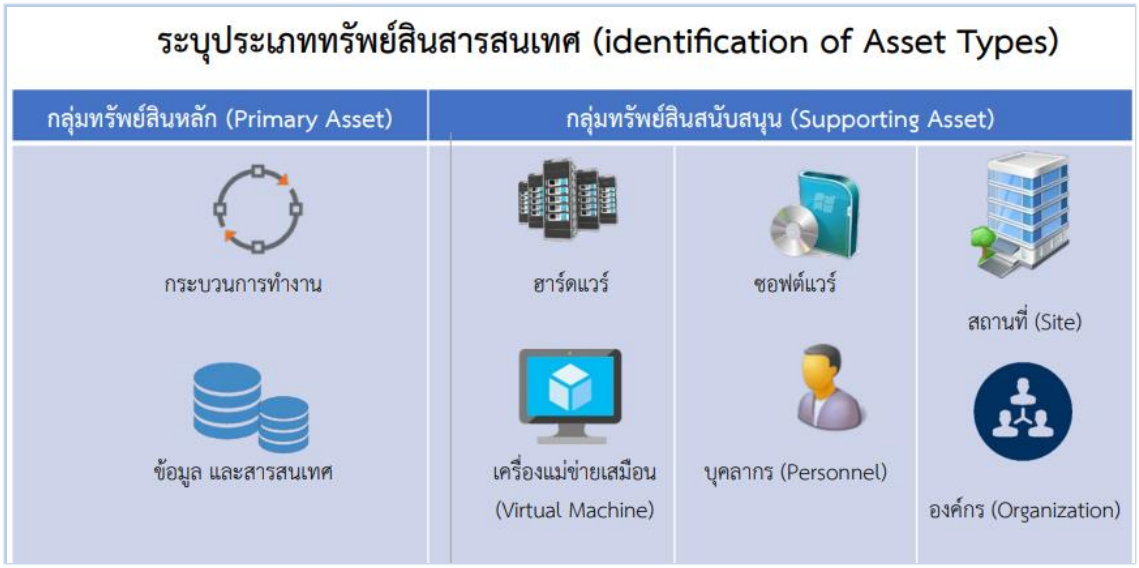
เป็นการระบุปัจจัยที่มีผลกระทบในเชิงลบต่อเป้าหมายขององค์กรหรือการปฏิบัติงานทั้งในระดับองค์กรและกิจกรรม เช่น ทรัพย์สิน ภัยคุกคาม ห่องโหว่ด้านความปลอดภัย



รูปที่6.2 แสดงการบ่งชี้ความเสี่ยงตามแนวทางของมาตรฐานสากล ISO/IEC 27005

1) สินทรัพย์สารสนเทศ

หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ ระบบเครือข่าย ซอฟต์แวร์ลิขสิทธิ์ เครื่องคอมพิวเตอร์แม่ข่าย กระบวนการทำงาน บุคลากร ข้อมูลและระบบสารสนเทศ เป็นต้น มีวัตถุประสงค์เพื่อบริหารกิจกรรมของโรงพยาบาล ให้บรรลุพันธกิจของโรงพยาบาล



รูปที่6.2.1 แสดงสินทรัพย์สารสนเทศ

(1) อาคารสถานที่

1) พื้นที่ตั้งสำนักงาน ศูนย์คอมพิวเตอร์ ณ โรงพยาบาลแคนดง

(2) รายการอุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย

ลำดับที่	รายละเอียด	จำนวน
1.	อุปกรณ์ให้บริการ Internet ได้แก่ - อุปกรณ์กระจายสัญญาณ Wifi (Accesspoint) - อุปกรณ์กระจายสัญญาณระบบ LAN (Switch) - Internet (Internet Gateway)	 20 ชุด 10 ชุด 2 ช่องทาง
2	อุปกรณ์ให้บริการจัดเก็บระบบสารสนเทศ ได้แก่ - ระบบจัดเก็บข้อมูลส่วนกลาง (Storage Server) - เครื่องคอมพิวเตอร์แม่ข่าย รองรับระบบ virtualization - ระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ - ระบบ monitor การทำงานอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย	 1 ชุด 2 เครื่อง 1 1
3	อุปกรณ์ให้บริการระบบโทรศัพท์ ได้แก่ - เครื่องแม่ข่าย - หัวเครื่องโทรศัพท์ -เครื่องโทรศัพท์ VoIP - หมายเลขโทรศัพท์	 1 ชุด 30 ชุด 100 เลขหมาย
4	Hardware ให้บริการที่สำคัญ ได้แก่ -เครื่องคอมพิวเตอร์พื้นฐาน	 75 ชุด

	- เครื่องพิมพ์ - เครื่องถ่ายเอกสาร	60 เครื่อง 1 เครื่อง
5	Software ให้บริการที่สำคัญ ได้แก่ - สำหรับรักษา - สำหรับสำนักงาน	 4 รายการ 1 รายการ

2) เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor) กระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP) ที่ใช้โดยผู้คุกคาม

- อาชญากรรมคอมพิวเตอร์ ผู้ก่อการร้ายทาง ไซเบอร์ การจารกรรมทางไซเบอร์
- **Ransomware (แรนซัมแวร์)** ซึ่งเป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความเชื่อถือในอุตสาหกรรมและองค์กรต่าง ๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์ได้มีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware
- **Phishing (ฟิชชิง)** คือการโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่าง ๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่นการส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่กรุณาคลิกลิงก์ด้านล่างนี้เพื่อ ยกเลิกการทำรายการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียงแค่กรอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีแล้วผู้ไม่หวังนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่น ๆ ของเป้าหมาย เช่นข้อมูลการเงิน ข้อมูลรหัสระบบต่าง ๆ ที่เป็นข้อมูลส่วนบุคคล
- **Malware (มัลแวร์)** หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น
- **Virus (ไวรัส)** เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศเป็นอย่างซึ่งโดยมุ่งเน้นในการโจมตีขัดขวางเพื่อไม่ให้ระบบสามารถใช้งานได้
- **Worms (เวิร์ม)** เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารเทศที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอกโดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่ายจนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้
- **Trojan (โทรจัน)** เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับเปลี่ยนแปลงแก้ไขข้อมูลซึ่งอาจส่งผลต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศหรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้

- **Spyware (สปายแวร์)** ซอฟต์แวร์ประสงค์ร้ายที่ทำงานอย่างลับๆ บนคอมพิวเตอร์และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล
- **Adware (แอดแวร์)** คือซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหากับระบบสารสนเทศได้ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัยได้
- **Data leaks (ข้อมูลรั่วไหล)** ข้อมูลรั่วไหลเกิดขึ้นเมื่อมีข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาจบันทึกผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้
- ภัยธรรมชาติได้แก่ น้ำท่วม แผ่นดินไหว พายุเข้า
- สภาพแวดล้อม ได้แก่ ระบบไฟฟ้าขัดข้อง อุณหภูมิไม่เหมาะสม ความชื้นจากเครื่องปรับอากาศ โครงสร้างนฐานถูกทำลาย

รูปที่ 6.2.1แสดงภัยคุคาม (Threat)

3) ช่องโหว่ (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สินหรือการควบคุมภายในของกระบวนการ เช่นช่องโหว่จาก hardware software ช่องจากความประมาทของบุคคล ช่องโหว่จากกระบวนการทำงาน ช่องโหว่ด้านการควบคุมการเข้าถึง เป็นต้น

รูปที่ 6.2.2 แสดงช่องโหว่ (Vulnerability)

6.3 การประเมินความเสี่ยง

การประเมินความเสี่ยง มีวัตถุประสงค์เพื่อทราบการจัดลำดับความสำคัญของความเสี่ยงในแต่ละประเด็น โดยอาศัยเกณฑ์มาตรฐานที่ได้กำหนดไว้ เพื่อใช้ประกอบการตัดสินใจของโรงพยาบาลในการที่จะดำเนินการเร่งป้องกันและแก้ไขบริหารจัดการก่อน หากเกิดเหตุการณ์ความเสี่ยงต่าง ๆ ขึ้น

6.3.1 การระบุค่าโอกาสของความเสี่ยง และค่าผลกระทบ

ขั้นตอนแรกของการบริหารความเสี่ยงในระดับหน่วยงาน หน่วยงานต้องทำการประเมิน **โอกาสของความเสี่ยง (Likelihood) ใช้ตัวย่อ L และ ผลกระทบ (Impact)** ใช้ตัวย่อ I

โอกาสของความเสี่ยง (Likelihood)หมายถึง ความเป็นไปได้ที่จะเกิดเหตุการณ์โดยพิจารณาจากความถี่ของเหตุการณ์ที่คาดว่าจะเกิดขึ้นในหนึ่งรอบปีงบประมาณ

ผลกระทบ (Impact) หมายถึง ระดับความรุนแรงและมูลค่าความเสียหายจากเหตุการณ์ที่คาดว่าจะเกิดขึ้น ตามประเภทของปัจจัยเสี่ยง

จากการระบุปัจจัยเสี่ยงแยกตามประเภทความเสี่ยงทั้ง 9 ประเภท คณะกรรมการบริหารความเสี่ยงและการควบคุมภายในโรงพยาบาล ได้ระบุเกณฑ์การให้คะแนนค่าโอกาส ของความเสี่ยง และค่าผลกระทบ ซึ่ง

สามารถกำหนดเกณฑ์ได้ทั้งในเชิงปริมาณและเชิงคุณภาพ ทั้งนี้ขึ้นอยู่กับ ข้อมูลและสภาพแวดล้อมของแต่ละหน่วยงาน ดังนี้

6.3.1.1 เกณฑ์การให้คะแนนค่าโอกาสของความเสี่ยง

คำอธิบาย ขั้นตอนนี้เป็นการระบุค่าโอกาสการเกิดเหตุการณ์ว่าจะอยู่ในระดับเป็นไปได้ มากหรือน้อยเพียงใด โดยจัดค่าโอกาสการเกิดเหตุการณ์ ออกเป็น 5 ระดับ ดังตารางที่ 2.3

ตารางที่ 5.3 เกณฑ์การให้คะแนนค่าโอกาสของความเสี่ยง

เชิงปริมาณ	เชิงคุณภาพ
1 = 0 – 1 ครั้งต่อปี	อาจเกิดขึ้นเฉพาะในสถานการณ์ที่ไม่ปกติบางกรณี
2 = 2 – 3 ครั้งต่อปี	อาจจะเกิดขึ้นน้อยมาก
3 = 4 – 5 ครั้งต่อปี	เป็นไปได้ ที่เกิดขึ้นในบางครั้ง
4 = 6 ครั้งต่อปี	เป็นไปได้มาก คาดหมายว่าจะเกิดขึ้นค่อนข้างบ่อย
5 = ตลอดทั้งปี (มากกว่า 6 ครั้งต่อปี)	ค่อนข้างแน่นอน คาดหมายว่าจะเกิดขึ้นในสถานการณ์ส่วนใหญ่

6.3.1.2 เกณฑ์การให้คะแนนค่าผลกระทบ

คำอธิบาย คณะกรรมการบริหารความเสี่ยงและการควบคุมภายในโรงพยาบาล ได้กำหนด เกณฑ์การหาค่าผลกระทบ ออกเป็น 5 ระดับ ตามประเภทของความเสี่ยง ไว้ทั้งหมด 9 ประเภท (ตามหัวข้อที 6.2.1) โดยเกณฑ์ การหาค่าผลกระทบที่ปรากฏในแต่ละประเภทนี้ เป็นกรอบหลักในการพิจารณา

1) เกณฑ์การให้คะแนนค่าผลกระทบด้านกลยุทธ์ (Strategic Risk)

ด้านกลยุทธ์		ความหมาย
1 =	ได้ผลงานตามเป้าหมาย มากกว่าร้อยละ 90 ขึ้นไป	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานมากกว่าร้อยละ 90 ขึ้นไป
2 =	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 81 – 90	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 81 – 90
3 =	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 71 – 80	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 71 – 80
4 =	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 61 – 70	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 61 – 70
5 =	ได้ผลงานตามเป้าหมายน้อยกว่าหรือเท่ากับร้อยละ 60	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานน้อยกว่าหรือเท่ากับร้อยละ 60

2) เกณฑ์การให้คะแนนค่าผลกระทบด้านการเงินและทรัพย์สิน (Financial and Asset Risk)

ด้านการเงิน		ความหมาย
1 =	มีการลดลงของรายได้ หรือมีค่าใช้จ่ายเพิ่มขึ้น หรือมีทรัพย์สินเสียหาย ไม่เกิน 50,000 บาท	กรณีที่ทาให้รายได้ลดลง/ค่าใช้จ่ายเพิ่มขึ้น / มีทรัพย์สินเสียหายไม่เกินจานวนเงิน 50,000 บาท
2 =	มีการลดลงของรายได้ หรือมีค่าใช้จ่ายเพิ่มขึ้น หรือมีทรัพย์สินเสียหาย ตั้งแต่ 50,001 – 100,000 บาท	กรณีที่ทาให้รายได้ลดลง/ค่าใช้จ่ายเพิ่มขึ้น / มีทรัพย์สินเสียหายจานวนเงินตั้งแต่ 50,001 – 100,000 บาท
3 =	มีการลดลงของรายได้ หรือมีค่าใช้จ่ายเพิ่มขึ้น หรือมีทรัพย์สินเสียหาย ตั้งแต่ 100,001 – 500,000 บาท	กรณีที่ทาให้รายได้ลดลง/ค่าใช้จ่ายเพิ่มขึ้น / มีทรัพย์สินเสียหายจานวนเงินตั้งแต่ 100,001 – 500,000 บาท
4 =	มีการลดลงของรายได้ หรือมีค่าใช้จ่ายเพิ่มขึ้น หรือมีทรัพย์สินเสียหาย ตั้งแต่ 500,001 – 1,000,000 บาท	กรณีที่ทาให้รายได้ลดลง/ค่าใช้จ่ายเพิ่มขึ้น / มีทรัพย์สินเสียหายจานวนเงินตั้งแต่ 500,001 – 1,000,000 บาท
5 =	มีการลดลงของรายได้ หรือมีค่าใช้จ่ายเพิ่มขึ้น หรือมีทรัพย์สินเสียหาย มากกว่า 1,000,0000 บาทขึ้นไป	กรณีที่ทาให้รายได้ลดลง/ค่าใช้จ่ายเพิ่มขึ้น / มีทรัพย์สินเสียหายจานวนเงิน มากกว่า 1,000,0000 บาทขึ้นไป

3) เกณฑ์การให้คะแนนค่าผลกระทบด้านปฏิบัติงาน (Operational Risk)

ด้านปฏิบัติงาน		**ความหมาย**
1 =	ได้ผลงานตามเป้าหมาย มากกว่าร้อยละ 90 ขึ้นไป	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนการปฏิบัติงาน ได้ผลงานมากกว่าร้อยละ 90 ขึ้นไป
2 =	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 81 – 90	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนการปฏิบัติงาน ได้ผลงานตั้งแต่ร้อยละ 81 – 90
3 =	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 71 – 80	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนการปฏิบัติงาน ได้ผลงานตั้งแต่ร้อยละ 71 – 80
4 =	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 61 – 70	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนการปฏิบัติงาน ได้ผลงานตั้งแต่ร้อยละ 61 – 70
5 =	ได้ผลงานตามเป้าหมายน้อยกว่าหรือเท่ากับ ร้อยละ 60	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนการปฏิบัติงาน ได้ผลงานน้อยกว่าหรือเท่ากับ ร้อยละ 60

4) เกณฑ์การให้คะแนนค่าผลกระทบด้านกฎระเบียบ (Compliance Risk)

ด้านกฎระเบียบ		ความหมาย
1 =	มีผลกระทบในระดับบุคลากร	มีการไม่ปฏิบัติตามกฎระเบียบ ระเบียบข้อบังคับที่ไม่มีนัยสำคัญ
2 =	มีผลกระทบภายในระดับงาน / ฝ่าย / สาขาวิชา	มีการละเมิดข้อกฎหมายที่ไม่มีนัยสำคัญ
3 =	มีผลกระทบในระดับสานักวิชา/ สถาบัน/ ศูนย์/ ส่วน/ หน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่า	มีการฝ่าฝืนกฎข้อกฎหมายที่สำคัญ ที่มีการสอบสวน หรือรายงาน ไปยังหน่วยงานที่เกี่ยวข้อง รวมทั้งการ ดำเนินคดีและ/หรือเรียกร้องค่าเสียหายหากเป็นไปได้
4 =	มีผลกระทบต่อโรงพยาบาล	มีการละเมิดข้อกฎหมายที่สำคัญ
5 =	มีผลกระทบต่อโรงพยาบาลและองค์กรภายนอก	มีการฟ้องร้องดำเนินคดี และ เรียกร้องค่าเสียหายที่สำคัญ ซึ่งเป็นคดีที่สำคัญมาก รวมถึงการฟ้องร้องที่เกิดจากการรวมตัวกันของผู้ที่ได้รับความเสียหาย

5) เกณฑ์การให้คะแนนค่าผลกระทบด้านภาพลักษณ์และชื่อเสียง (Image and Reputation Risk)

ด้านชื่อเสียง		ความหมาย
1 =	มีผลกระทบต่อชื่อเสียงในระดับหน่วยงาน	มีข่าวเชิงลบ แต่สามารถขจัดไปได้ตามกระบวนการบริหารปกติ
2 =	มีผลกระทบต่อชื่อเสียงในระดับภายในโรงพยาบาล	มีข่าวในเชิงลบจากสื่อภายในโรงพยาบาล เช่น การมีส่งจดหมายสนเท่ห์ในโรงพยาบาล
3 =	มีผลกระทบต่อชื่อเสียงของโรงพยาบาล ในระดับจังหวัด	มีข่าวในเชิงลบจากสื่อในจังหวัดนครราชสีมา
4 =	มีผลกระทบต่อชื่อเสียงของโรงพยาบาล ในระดับชาติ	มีการเผยแพร่ทางสื่อในเชิงลบในระดับชาติ ส่งผลต่อชื่อเสียงในระดับชาติ
5 =	มีผลกระทบต่อชื่อเสียงของโรงพยาบาล ในระดับนานาชาติ	มีการเผยแพร่ทางสื่อในเชิงลบ ในระดับนานาชาติ ส่งผลต่อชื่อเสียงในระดับนานาชาติ

6) เกณฑ์การให้คะแนนค่าผลกระทบด้านสุขภาพและความปลอดภัย (Health and Safety Risk)

ด้านสุขภาพและความปลอดภัย		ความหมาย
1 =	มีการบาดเจ็บเล็กน้อย	สามารถปฐมพยาบาลเบื้องต้นได้ทสี่ถานพยาบาล หรือมีความเจ็บป่วยที่ไม่มีผลต่อการทางาน
2 =	มีการบาดเจ็บหรือเจ็บป่วยไม่มาก	ได้รับการบาดเจ็บหรือเจ็บป่วยซึ่งต้องเข้ารับการรักษาจากแพทย์ และใช้ระยะเวลาในการรักษาตัวไม่เกิน 1 สัปดาห์
3 =	มีการบาดเจ็บหรือเจ็บป่วยมาก	ได้รับการบาดเจ็บหรือเจ็บป่วยซึ่งต้องเข้ารับการรักษาที่โรงพยาบาล และใช้ระยะเวลาในการรักษาตัวตั้งแต่ 1 สัปดาห์ แต่ไม่เกิน 1 เดือน
4 =	มีการบาดเจ็บหรือเจ็บป่วยที่รุนแรง	ได้รับการบาดเจ็บหรือเจ็บป่วยซึ่งต้องเข้ารับการรักษาที่โรงพยาบาล และใช้ระยะเวลานานในการรักษาตัวตั้งแต่ 1 เดือนขึ้นไป
5 =	มีการทุพพลภาพทางร่างกายในบริเวณสำคัญ หรือเสียชีวิต	มีการสูญเสียชีวิต หรือทุพพลภาพทางร่างกายในบริเวณสำคัญ จนไม่อาจปฏิบัติงานต่อไปได้

7) เกณฑ์การให้คะแนนค่าผลกระทบด้านบุคลากร (Personnel Risk)

ด้านบุคลากร		ความหมาย
1 =	มีผลกระทบในระดับบุคลากร	พนักงานโรงพยาบาล มีอัตราการออกหรือพ้นสภาพ ไม่เกินร้อยละ 1
2 =	มีผลกระทบภายในระดับงาน / ฝ่าย / สาขาวิชา	พนักงานโรงพยาบาล มีอัตราการออกหรือพ้นสภาพ ร้อยละ 2 - 4
3 =	มีผลกระทบในระดับสำนักวิชา/ สถาบัน/ ศูนย์/ ส่วน/ หน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่า	พนักงานโรงพยาบาล มีอัตราการออกหรือพ้นสภาพ ร้อยละ 5 - 9
4 =	มีผลกระทบต่อตัวชี้วัดของโรงพยาบาล	พนักงานโรงพยาบาล มีอัตราการออกหรือพ้นสภาพ ร้อยละ 10 - 14
5 =	มีผลกระทบต่อตัวชี้วัดขององค์กภายนอก เช่น สมศ. สกอ.	พนักงานโรงพยาบาล มีอัตราการออกหรือพ้นสภาพ ตั้งแต่ร้อยละ 15 ขึ้นไป

8) เกณฑ์การให้คะแนนค่าผลกระทบด้านเทคโนโลยีดิจิทัล (Digital Technology Risk)

ด้านเทคโนโลยีดิจิทัล		ความหมาย
1 =	มีการบริหารความเสี่ยงในหน่วยงานอย่างเป็นระบบ และมีการพิจารณากลยุทธ์เพื่อลดความเสี่ยงอยู่เสมอ	มีระบบการจัดการความเสี่ยงครอบคลุมทั้งหน่วยงาน และมีการจัดการความเสี่ยงที่ดี
2 =	มีการติดตามระดับความเสี่ยงด้านเทคโนโลยีดิจิทัล และจัดการให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้	มีกระบวนการจัดการความเสี่ยง และมีแผนการป้องกัน เหตุการณ์ที่อาจจะเกิดขึ้น
3 =	มีกระบวนการลดความเสี่ยงด้านเทคโนโลยีดิจิทัลที่สำคัญอย่างทันที เมื่อความเสี่ยงปรากฏ	มีกระบวนการจัดการรองรับความเสี่ยงหากเหตุการณ์เกิดขึ้น โดยระบุให้มีผู้รับผิดชอบไว้อย่างชัดเจน
4 =	เริ่มมีกระบวนการลดความเสี่ยงด้านเทคโนโลยีดิจิทัล	มีการวิเคราะห์ถึงความเสี่ยงด้านเทคโนโลยีดิจิทัลที่มีผลกระทบต่อการดำเนินงาน และมีการจัดการความเสี่ยงบ้างตามความจำเป็น
5 =	ไม่มีกระบวนการที่ใช้ในการจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล	มีการแก้ไขปัญหาจากการทำงานประจำวัน ซึ่งเป็นการแก้ไขปัญหาเป็นกรณีๆ ไป

9) เกณฑ์การให้คะแนนค่าผลกระทบด้านธรรมาภิบาลและอัตตาภิบาล (Good Governance and Self Governance Risk)

ด้านธรรมาภิบาลและอัตตาภิบาล		ความหมาย
1 =	มีการดำเนินงานตามมิติธรรมาภิบาลและอัตตาภิบาลอย่างเป็นระบบ และมีการพิจารณา การดำเนินงานเพื่อลดความเสี่ยงอยู่เสมอ	มีระบบการจัดการความเสี่ยงด้านธรรมาภิบาลและอัตตาภิบาลทคี่รอบคลุมทั้งหน่วยงาน และมีการจัดการความเสี่ยงที่ดี
2 =	มีการติดตามระดับความเสี่ยงด้านธรรมาภิบาลและอัตตาภิบาล และจัดการให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้	มีกระบวนการจัดการความเสี่ยง และมีแผนการป้องกันเหตุการณ์ที่อาจจะเกิดขึ้น
3 =	มีกระบวนการลดความเสี่ยงด้านธรรมาภิบาลและอัตตาภิบาลที่สาคัญอย่างทันที เมื่อความเสี่ยงปรากฏ	มีกระบวนการจัดการรองรับความเสี่ยงหากเหตุการณ์เกิดขึ้น โดยระบุให้มีผู้รับผิดชอบไว้อย่างชัดเจน
4 =	เริ่มมีกระบวนการลดความเสี่ยงด้านธรรมาภิบาลและอัตตาภิบาล	มีการวิเคราะห์ถึงความเสี่ยงด้านธรรมาภิบาลและอัตตาภิบาล ที่มีผลกระทบต่อการดาเนินงาน และมีการจัดการความเสี่ยงบ้างตามความจำเป็น

5 =	ไม่มีกระบวนการที่ใช้ในการจัดการความเสี่ยงด้านธรรมาภิบาลและอัตตาภิบาล	ไม่มีการวิเคราะห์ถึงความเสียงด้านธรรมาภิบาลและอัตตาภิบาล ที่มีผลกระทบต่อการดาเนินงาน

10.**เกณฑ์การให้คะแนนค่าผลกระทบด้านความมั่นคงปลอดภัยไซเบอร์ (CS:Cyber security risk)**

ด้านการรักษาความลับ (Confidentiality)		**ความหมาย**
1 =	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ไม่ส่งผลต่อความเสียหายแก่โรงพยาบาล	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน ทั้งนี้ไม่ส่งผลต่อความเสียหายแก่โรงพยาบาล
2 =	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ส่งผลต่อความเสียหายแก่โรงพยาบาล	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน ทั้งนี้ส่งผลต่อความเสียหายแก่โรงพยาบาล
3 =	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited)ทั้งนี้ส่งผลต่อความเสียหายแก่โรงพยาบาล และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)
4 =	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)
5 =	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)	มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)
ด้านการรักษาความถูกต้องครบถ้วน(Integrity)		**ความหมาย**
1 =	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด	มีผลกระทบต่อข้อมูลความถูกต้องของข้อมูลน้อย ทั้งนี้ไม่ส่งผลต่อความเสียหายแก่โรงพยาบาล

	(Limited)ทั้งนี้ไม่ส่งผลต่อความเสียหายแก่โรงพยาบาล	
2 =	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ส่งผลต่อความเสียหายแก่โรงพยาบาล	มีผลกระทบต่อข้อมูลความถูกต้องของข้อมูลน้อย และส่งผลต่อความเสียหายแก่โรงพยาบาล
3 =	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ส่งผลต่อความเสียหายแก่โรงพยาบาลและเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	มีผลกระทบต่อข้อมูลความถูกต้องของข้อมูลน้อย ส่งผลต่อความเสียหายแก่โรงพยาบาลและก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
4 =	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	มีผลกระทบต่อข้อมูลความถูกต้องของข้อมูลมาก ส่งผลต่อความเสียหายแก่โรงพยาบาลและก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
5 =	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)	มีผลกระทบต่อข้อมูลความถูกต้องของข้อมูลมากที่สุด ส่งผลต่อความเสียหายแก่โรงพยาบาลและก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

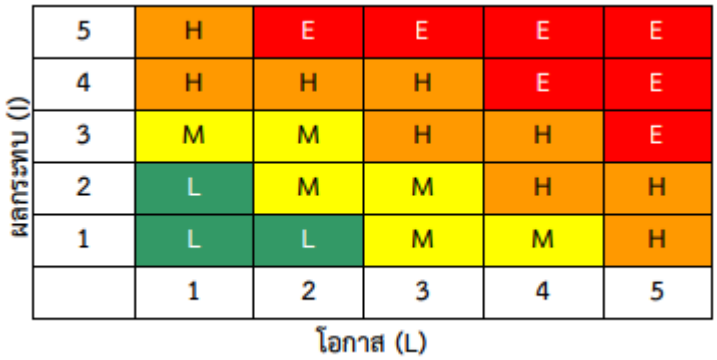
ด้านการรักษาสภาพพร้อมใช้งาน(Availability)		**ความหมาย**
1 =	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ไม่ส่งผลต่อความเสียหายแก่โรงพยาบาล	มีผลกระทบต่อสภาพความพร้อมใช้งานข้อมูลน้อย แต่ไม่ส่งผลต่อความเสียหายแก่โรงพยาบาล
2 =	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ส่งผลต่อความเสียหายแก่โรงพยาบาล	มีผลกระทบต่อสภาพความพร้อมใช้งานข้อมูลน้อย ส่งผลต่อความเสียหายแก่โรงพยาบาล
3 =	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ส่งผลต่อความเสียหายแก่โรงพยาบาล และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	มีผลกระทบต่อสภาพความพร้อมใช้งานข้อมูลน้อย ส่งผลต่อความเสียหายแก่โรงพยาบาลและก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

4 =	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	มีผลกระทบต่อสภาพความพร้อมใช้งานข้อมูลมาก ส่งผลต่อความเสียหายแก่โรงพยาบาลและก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
5 =	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)	มีผลกระทบต่อสภาพความพร้อมใช้งานข้อมูลมากที่สุด ส่งผลต่อความเสียหายแก่โรงพยาบาลและก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

เพื่อให้มีเครื่องมือในการพิจารณาความเสี่ยง ในภาพรวมว่า ความเสี่ยงต่างๆ นั้น มีการกระจายตัวของโอกาสการเกิดขึ้นของเหตุการณ์และมีผลกระทบ อย่างไร ความเสี่ยงใดควรได้รับการแก้ไขก่อนหลัง โดยการนำค่าโอกาสของความเสี่ยง (Likelihood) ใช้ตัวย่อ L และค่าผลกระทบ (Impact) ใช้ตัวย่อ I ไปบันทึกลงใน แผนผังเมทริกซ์(Risk Matrix) โดยกำหนดให้แกน X คือ ค่าโอกาสของความเสี่ยง และแกน Y คือ ค่าผลกระทบ ดังตารางที่ 5.3

ประโยชน์ของการจัดทำแผนผังเมทริกซ์ เพื่อช่วยให้หน่วยงานสามารถเรียงระดับความเสี่ยง (Degree of Risk) ของเหตุการณ์ต่างๆ ไว้ในแผนผังเดียวกัน และคณะกรรมการบริหารความเสี่ยงและ การควบคุมภายในโรงพยาบาล จักได้พิจารณาล าดับความสำคัญของความเสี่ยงได้สะดวกยิ่งขึ้น ซึ่งระดับ ความเสี่ยงของโรงพยาบาลมี 4 ระดับ ได้แก่ สูงมาก (Extreme) สูง (High) ปานกลาง (Medium) และต่ำ (Low) โดยใช้สีสื่อประกอบในรูปแบบคล้ายคลึงกับสัญญาณไฟจราจร

ตารางที่ 6.3 แผนผังเมทริกซ์แสดงผลการประเมินความเสี่ยง



คำอธิบาย

ขอบเขตพื้นที่	ความหมาย
= ความเสี่ยงสูงมาก (Extreme Risk, E)	ตกพื้นที่ซึ่งต้องมีแผนการบริหารความเสี่ยงเร่งด่วน
= ความเสี่ยงสูง (High Risk, H)	ตกพื้นที่ซึ่งต้องมีแผนการบริหารความเสี่ยง
= ความเสี่ยงปานกลาง (Medium Risk, M)	อยู่พื้นที่ซึ่งยอมรับความเสี่ยงได้
= ความเสี่ยงต่ำ (Low Risk, L)	อยู่พื้นที่ซึ่งยอมรับความเสี่ยงได้

6.4 กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

การจัดการความเสี่ยง เป็นการนำมาตรการหรือวิธีการมาใช้ปฏิบัติในหน่วยงาน เพื่อลดโอกาสและ ผลกระทบที่จะเกิดขึ้นจากความเสี่ยงในการดำเนินงานที่ยังไม่มีกิจกรรมควบคุม หรือที่มีอยู่แต่ยังไม่เพียงพอ วิธีการจัดการกับแต่ละความเสี่ยง โดยคณะกรรมการบริหารความเสี่ยงและการควบคุมภายในโรงพยาบาล และคณะทำงานบริหารความเสี่ยงและการควบคุมภายในประจำหน่วยงาน ควรคำนึงถึงต้นทุนและผลประโยชน์ที่ได้รับจากการตัดสินใจในการเลือกวิธีจัดการความเสี่ยง แนวทางการปฏิบัติในการจัดการความเสี่ยงมี 4 ลักษณะ ดังนี้

1) การยอมรับความเสี่ยง (Risk Acceptance) เมื่อทราบถึงความน่าจะเป็นของเหตุการณ์ ที่อาจจะเกิดขึ้นหรือผลกระทบเมื่อประเมินค่าความเสี่ยงแล้วมีค่าต่ำาหรือปานกลางหรือไม่คุ้มค่าในการลดความเสี่ยงเนื่องจากมีค่าใช้จ่ายในการดำเนินการ

2) การลดความเสี่ยง (Risk Reduction) เป็นการปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่เพื่อลดโอกาสความน่าจะเป็นของความเสี่ยงที่อาจจะเกิดขึ้น หรือผลกระทบที่อาจจะเกิดขึ้น

3) การถ่ายโอนความเสี่ยง (Risk Sharing) เป็นการแบ่งความรับผิดชอบ โดยการโอนความเสี่ยงไปให้บุคคลที่ 3 เช่น บริษัทประกันภัย หรือการว่าจ้างให้บุคคลภายนอกเป็นผู้กระทำกิจกรรมแทนในบางกิจกรรม (Outsourcing) เป็นต้น

4) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการยกเลิกกิจกรรมที่จะก่อให้เกิดความเสี่ยงนั้นซึ่งอาจจะเป็นสิ่งที่หน่วยงานไม่ถนัด หรืออาจมีความเสี่ยงอยู่ในระดับที่สูงมากซึ่งหน่วยงานไม่อาจยอมรับได้

มาตรการต่าง ๆ ข้างต้นจะช่วยปรับปรุงกลยุทธ์การบริหารความเสี่ยงให้มีประสิทธิภาพยิ่งขึ้นตามความเสี่ยงแต่ละประเภท ดังนั้น การระบุวิธีการจัดการความเสี่ยง ควรพิจารณาอย่างรอบคอบเพื่อเลือกใช้วิธีการจัดการความเสี่ยงได้อย่างเหมาะสม

ข้อแนะนำในการจัดการความเสี่ยง กรณีที่ผลประเมินความเสี่ยงเป็น ระดับ L หมายถึง มีระดับความเสี่ยงอยู่ในระดับต่ำ ควรใช้วิธีการจัดการความเสี่ยงโดยการยอมรับความเสี่ยง และปรับปรุงระบบการควบคุมภายในที่มีอยู่ให้มีประสิทธิภาพ กรณีที่ผลประเมินความเสี่ยงเป็น ระดับ M หมายถึง มีระดับความเสี่ยงที่ไม่

รุนแรง ควรใช้วิธีการ ยอมรับความเสี่ยงไว้ หรือการหลีกเลี่ยงความเสี่ยง โดยการยกเลิกกิจกรรมที่อาจจะทำให้มีความสูญเสีย หน่วยงานควรจัดให้มีการติดตามความเสี่ยงอย่างต่อเนื่องเป็นประจำทุก 6 เดือน กรณีที่มีผลประเมินความเสี่ยงเป็น ระดับ H หมายถึง มีระดับความเสี่ยงที่สูง จำเป็นต้องจัดการ ความเสี่ยง โดยวิธีลดความเสี่ยง หรือการถ่ายโอน ซึ่งต้องดำเนินการกำหนดให้มีแผนการบริหารความเสี่ยง หน่วยงานควรมีการติดตามความเสี่ยงเป็นประจำทุกไตรมาส และกรณีที่มีผลประเมินความเสี่ยงเป็น ระดับ E หมายถึง มีระดับความเสี่ยงที่รุนแรงมาก หน่วยงาน ควรจัดทำบันทึกข้อความพร้อมแผนการบริหารความเสี่ยง ประเภทแผนฉุกเฉิน และให้รายงานต่อประธานคณะกรรมการบริหารความเสี่ยงและการควบคุมภายในโรงพยาบาลทราบทันทีที่พบโดยตรง ประกอบกับ หน่วยงานควรมีการติดตามความเสี่ยงเป็นประจำทุกเดือน

6.5 กิจกรรมการบริหารความเสี่ยง (Control Activities)

กิจกรรมควบคุมหรือการควบคุมภายใน เป็นกิจกรรมที่กำหนดขึ้นเพื่อเป็นเครื่องมือช่วยควบคุมความเสี่ยง หรือปัจจัยเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของโรงพยาบาล ซึ่งกิจกรรมการควบคุมดังกล่าวหมายถึง กระบวนการ วิธีการปฏิบัติงานต่าง ๆ ที่จะทำให้มั่นใจได้ว่าผู้รับผิดชอบแต่ละกิจกรรมได้ ดำเนินการสอดคล้องกับทิศทางที่ต้องการ สามารถช่วยป้องกันและชี้ให้เห็นความเสี่ยงที่มีผลกระทบต่อ วัตถุประสงค์ได้โดยทั่วไป การปฏิบัติงานจะต้องมีการควบคุมโดยธรรมชาติ เป็นส่วนหนึ่งของการดำเนินงานอยู่แล้ว โดยเกิดขึ้นในทุกระดับ ทุกหน้าที่งาน ทั่งทั้งองค์กร เช่น การอนุมัติ การมอบหมายอำนาจหน้าที่ การลงความเห็น การตรวจสอบ การยืนยันความถูกต้อง การทบทวนประสิทธิภาพของการดำเนินงาน การจัดการทรัพยากร และการแบ่งหน้าที่ของบุคลากร เป็นต้น ทั้งนี้มีการแบ่งประเภทการควบคุมไว้ 4 ประเภท คือ

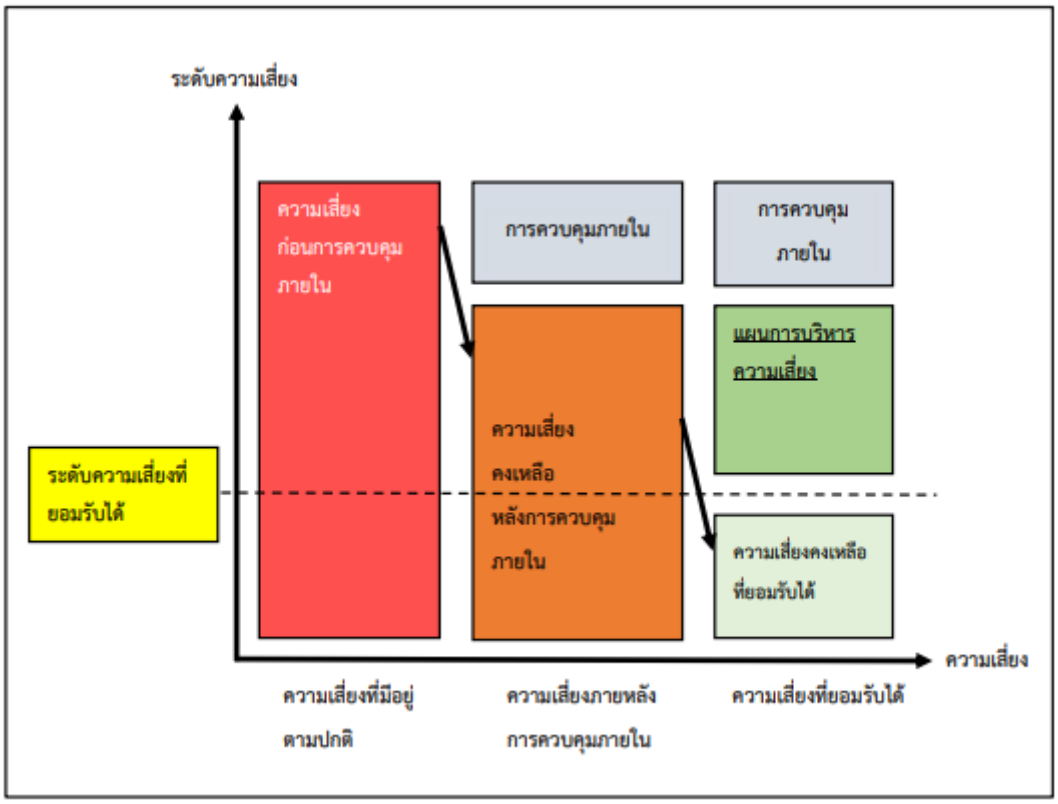
1) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อ ป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงการสร้างองค์กร การแบ่งแยกหน้าที่ การควบคุมการเข้าถึงเอกสาร ข้อมูล ทรัพย์สิน เป็นต้น

2) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อ ค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การสอบทาน การวิเคราะห์ การยืนยันยอด การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

3) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้ เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัลแก่ผู้มีผลงานดีเป็นต้น

4) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไข ข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต เช่น การจัดเตรียมเครื่องมือดับเพลิง เพื่อช่วยลดความรุนแรงของความเสียหายให้น้อยลง หากเกิดเพลิงไหม้ เป็นต้น

โดยกิจกรรมควบคุมหรือการควบคุมภายในซึ่งเป็นขั้นตอนที่สำคัญอันหนึ่งของการบริหารความเสี่ยงของโรงพยาบาล จะมีความเกี่ยวข้องกับค่าระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ดังภาพที่ 6.5 คณะกรรมการบริหารความเสี่ยงและการควบคุมภายในโรงพยาบาล และคณะทำงานบริหารความเสี่ยงและการควบคุมภายในประจำหน่วยงาน จำเป็นต้องกำหนด สัญญาณเตือนภัย (Warning Sign) สำหรับความ เสี่ยงแต่ละด้าน เพื่อเป็นการเตือนภัยว่าเหตุการณ์อาจจะเกิดขึ้นภายหลังจากที่มีการจัดการลดความเสี่ยงลงแล้ว โดยเหตุการณ์ดังกล่าวยังคงมีระดับความเสี่ยงเกินกว่าระบบการควบคุมภายในจะควบคุมไว้ได้และความเสี่ยงภายหลังการควบคุมภายในดังกล่าวเรียกว่า ความเสี่ยงที่ยังเหลืออยู่ (Residual Risk) คณะกรรมการบริหารความเสี่ยงและการควบคุมภายในโรงพยาบาลจะเป็นผู้อนุมัติระดับความเสี่ยงที่ยอมรับได้ในระดับหาวิทยาลัยและระดับหน่วยงาน การกำหนดระดับความเสี่ยงที่ยอมรับได้ควรกำหนดตามประเภทความเสี่ยงในแต่ละด้านใช้เป็นตัวชี้วัดความเสี่ยงขั้นต่ำที่กำหนดขึ้นเองในหน่วยงาน



ภาพที่ 6.5 การแสดงความสัมพันธ์ของระดับความเสี่ยงที่ยอมรับได้

ระดับความเสี่ยง	เขตสี	มาตรการในปัจจุบัน	มาตรการเพิ่มเติม
ยอมรับได้	เขียว	มาตรการในการจัดการความเสี่ยงในปัจจุบันเพียงพอหรือมีการควบคุมที่ดีมากแล้ว	ไม่จำเป็นต้องมีมาตรการจัดการความเสี่ยงเพิ่มเติมอีก หรืออาจจะผ่อนคลายมาตรการเดิม เพื่อให้มีประสิทธิภาพมากขึ้นโดยไม่เกิดการใช้ทรัพยากรมากเกินไป
	เหลือง	มาตรการในการจัดการความเสี่ยงในปัจจุบัน อาจจะเพียงพอแล้ว ให้ติดตามการดำเนินการเป็นระยะๆ	ไม่จำเป็นต้องมีมาตรการจัดการความเสี่ยงเพิ่มเติมอีก หรืออาจจะมีได้หากไม่ใช้ทรัพยากรเพิ่มเติมหรือมีแผนงานอื่นรองรับอยู่แล้ว
สูงกว่าระดับที่ยอมรับได้	แดง	ต้องเฝ้าระวังอย่างต่อเนื่อง และอาจเพิ่มเติมความเข้มข้นในการดำเนินการตามมาตรการในปัจจุบัน	จำเป็นต้องมีการเพิ่มเติมมาตรการ โดยหากมีข้อจำกัดด้านทรัพยากรในการจัดการความเสี่ยงให้มีความสำคัญในระดับที่สูงกว่า และผู้บริหารควรให้ความสำคัญในการติดตามการดำเนินการของมาตรการดังกล่าวอย่างต่อเนื่อง

6.6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

การสื่อสารทำความเข้าใจเกี่ยวกับแผนความเสี่ยงด้านสารสนเทศให้บุคลากรที่เกี่ยวข้องทราบสามารถนำไปปฏิบัติได้ และรายงานความก้าวหน้าของการดำเนินงานตามแผนบริหารความเสี่ยงด้านสารสนเทศตามมาตรฐานความมั่นคง ปลอดภัยสารสนเทศ (ISO/IEC 27001 : 2013) ใน 3 ด้าน คือ

1.ด้านบุคคล (People)

1) การสร้างความตระหนักของการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้บริหารและบุคลากรด้านเทคโนโลยีสารสนเทศ โดยการพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (People)

2). สร้างความตระหนักและการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Awareness) สำหรับผู้ใช้งาน (User) และวิธีการตรวจสอบช่องโหว่ Vulnerability Assessment (Web Application Hacking) และการเจาะระบบ (Penetration Testing) สำหรับผู้ดูแลระบบ (System Administrator)

3).การพัฒนากำลังคนผู้ปฏิบัติงานด้านการรักษาความปลอดภัยไซเบอร์

4) การพัฒนากำลังคนผู้ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy)

5) การฝึกซ้อมรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber drill) เพื่อให้บุคลากร และผู้บริหาร มีการเตรียมความพร้อมรับสถานการณ์การโจมตี (Cyber Drill) มีความเข้าใจและตระหนักถึงภัยจากการโจมตีทางอิเล็กทรอนิกส์ที่อยู่ใกล้ตัว เพราะเมื่อการโจมตีเกิดขึ้นจะได้ไม่ตกเป็นเหยื่อ โดยรู้เท่าไม่ถึงการณ์ที่การบริหาร

ความมั่นคงปลอดภัยขององค์การในอนาคตต้องมีรูปแบบเป็น “Cyber Resilience” ซึ่งหมายถึง ระบบต้องมีความสามารถในการรองรับการโจมตีและจะต้องสามารถทำงานหรือให้บริการได้อย่างต่อเนื่อง ไม่ทำให้เกิดความเสียหายต่อภารกิจและภาพลักษณ์ขององค์การ ภาพลักษณ์ของผู้บริหาร ดังนั้นแนวคิดของ Information Security Management ในรูปแบบเดิมๆ จึงไม่ครอบคลุม เพียงพอ จำเป็นต้องนำแนวคิด Cyber Security Resilience Framework (Cyber Security Centric and Cyber Resilience in Action) มาปรับใช้ในองค์กรด้วย

2 ด้านกระบวนการ (Process)

ขั้นตอน นโยบาย ระเบียบ ข้อบังคับและแนวปฏิบัติสำคัญต่าง ๆ ที่เป็นแนวทางในการปฏิบัติตนทั้งในสิ่งที่ต้องทำ ควรทำ และไม่ควรทำ รวมถึงการระบุบทบาทหน้าที่ความรับผิดชอบ เป็นส่วนสนับสนุนให้องค์กรสามารถทำงานได้อย่างราบรื่นและแก้ไขสถานการณ์หรือเหตุการณ์ที่ไม่ปกติที่เกิดขึ้นได้ เช่น ระบบหยุดทำงาน หรือเครือข่ายอินเทอร์เน็ตไม่สามารถใช้งานได้ หรือเหตุการณ์การโจมตีของผู้ไม่ประสงค์ดี รวมถึงมัลแวร์และไวรัสเรียกค่าไถ่ที่สามารถเกิดขึ้นได้หลากหลายช่องทาง หากองค์กรไม่มีการนโยบายในการใช้งาน และแนวทางการรับมือเหตุการณ์ต่าง ๆ ที่ดีเพียงพอ ก็จะส่งผลให้เกิดปัญหาเดิมซ้ำ ๆ และอาจจะยิ่งรุนแรงมากขึ้นเรื่อย ๆ สำหรับโรงพยาบาล มีประกาศโรงพยาบาล เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาล พ.ศ. 2554 และระเบียบ โรงพยาบาล ว่าด้วยการรักษาความปลอดภัย-ด้านเทคโนโลยีสารสนเทศ โรงพยาบาล พ.ศ. 2564 และหน่วยงาน ผู้ปฏิบัติงาน และผู้ใช้งาน ได้ยึดถือและปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.ด้านเทคโนโลยี (Technology) เทคโนโลยี ซอฟต์แวร์ ลิขสิทธิ์และการอัปเดต สิ่งจำเป็นในขั้นตอนนำมาปฏิบัติงานและช่วยในการทำงาน รวมถึงการปฏิบัติหน้าที่ ยังช่วยบริหารจัดการต่าง ๆ เพื่อให้บุคคลที่เกี่ยวข้องในการทำงาน สามารถติดตามและตรวจสอบเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้ นอกจากมีเทคโนโลยีที่ดี องค์กรต้องมีกระบวนการในการเฝ้าระวังและปรับปรุงแก้ไขช่องโหว่ และตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที

6.7. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

หลังจากจัดทำแผนบริหารความเสี่ยง และมีการดำเนินงานตามแผนแล้ว จะต้องมีการรายงานและติดตามผลเป็น ระยะๆ เพื่อให้เกิดความมั่นใจว่าได้มีการดำเนินงานไปอย่างถูกต้องและเหมาะสม โดยมีเป้าหมายในการติดตามผล คือ เป็น การประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการ ดำเนินการไปแล้วว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่

การติดตามผล

ตามประกาศโรงพยาบาล เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาล พ.ศ. 2554 กำหนดให้ ศูนย์คอมพิวเตอร์ หน่วยตรวจสอบภายใน และผู้ดูแลระบบที่ได้รับมอบหมาย ตรวจสอบและประเมินความเสี่ยงด้านสารสารเทศ โดยมีแนวปฏิบัติดังนี้

- ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ ปีละ1 ครั้ง

- ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยหน่วยตรวจสอบภายใน เพื่อให้โรงพยาบาลได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ
- มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง ปีละ 1 ครั้ง
- มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศปีละ 1 ครั้ง
- มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
- มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศปีละ 1 ครั้ง ต่อคณะกรรมการเทคโนดลยีสารสนเทศและการสื่อสาร และแจ้งคณะกรรมการบริหารความเสี่ยงของโรงพยาบาล
- มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบ และประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

7. การดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

การประเมินความเสี่ยงนั้นเกี่ยวกับการระบุความเสี่ยงที่เฉพาะเจาะจงกับสภาพแวดล้อม และการกำหนดระดับของความเสี่ยงที่ระบุ ขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินความเสี่ยง (Risk Evaluation)

รูปที่ 7.1 กระบวนการดำเนินการประเมินความเสี่ยง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	การประเมินค่าความเสี่ยงก่อนมีกิจกรรมควบคุม			กิจกรรมควบคุม	ระดับความเสี่ยงที่เหลืออยู่			วิธีการจัดการความเสี่ยง	สัญญาณเตือนภัย
			L	I	R1		L	I	R2		
1.ความเสี่ยงจากกระแสไฟฟ้า ขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ ผู้รับผิดชอบความเสี่ยง 1. ส่วนอาคารและสถานที่ 2. ศูนย์คอมพิวเตอร์ 3. MIS	O: Operation risk	การเกิดกระแสไฟฟ้าขัดข้องหรือเกิด แรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความ เสียหายจากแรงดัน ไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถ เปิดใช้งานได้โดยอัตโนมัติ	5	1	5	1 ทำแผน MA อุปกรณ์เครือข่ายและระบบสำรองไฟฟ้าห้อง Data Center อย่างต่อเนื่อง 2.ประสานหน่วยงานที่ดูแลระบบไฟฟ้าเข้ามาตรวจสอบระบบไฟฟ้าประจำอาคารอย่างต่อเนื่อง 3.จัดหาอุปกรณ์สำรอง เพื่อทดแทนอุปกรณ์เครือข่ายที่มีความสำคัญ 4.การทำประกันสำหรับทรัพย์สินด้านเทคโนโลยีสารสนเทศ (MA)	5	1	5	การลดความเสี่ยง Reduce การถ่ายโอนความเสี่ยง Transfer	1 ได้รับการแจ้งเตือนระบบเครือข่ายใช้งานไม่ได้จากผู้รับบริการ 2 อุปกรณ์เครือข่ายอยู่ในสถานะแจ้งเตือนความผิดปกติ 3. ระบบมอนิเตอร์แจ้งเตือนความผิดของอุปกรณ์ระบบเครือข่าย
	D: digital technology risk		5	2	10		5	1	5		
	CS: Cyber security risk (Availability)		5	2	10		5	1	5		
	F: financial Risk		2	2	4		1	2	2		

2.ความเสี่ยงจาก การถูกบุกรุก โดยผู้ไม่ประสงค์ดี (Hacker) ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์ 2.MIS 3.ศูนย์นวัตกรรมฯ 4.ศูนย์บริการการศึกษา 5.ส่วนการเงิน 6.ส่วนทรัพยากรบุคคล 7.โรงเรียนสุรวิวัฒน์ 8.โรงพยาบาลโรงพยาบาล	D:Digital technology risk	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย	5	2	10	1. กำหนด policy ให้ใช้รหัสผ่านแบบซับซ้อนเพื่อป้องกันการ hack account 2. มีมาตรการและอุปกรณ์ป้องกันการเจาะทำลายระบบ	5	1	5	การลดความเสี่ยง Reduce	1.ได้รับการแจ้งเตือนจากระบบ monitoring 2.ตรวจสอบพบการส่ง email ออกจากระบบจำนวนมากผิดปรกติ 3.ได้รับการแจ้งเตือน information leak จากระบบ cern
	CS: Cyber security risk (confidential)		5	2	10	3. มีการเฝ้าระวังและตรวจสอบระบบสารสนเทศอยู่เสมอ 4.มีการสำรองข้อมูลระบบสารสนเทศอยู่เสมอ	5	1	5		
	CS: Cyber security risk (Integritry)		5	2	10	5.จัดทำระบบ Authen แบบ 2 factor authen สำหรับระบบสารสนเทศที่มีความสำคัญ	5	1	5		
3.ผู้ใช้งาน-เครื่องคอมพิวเตอร์แม่ข่ายติด Ransomware (แรนซัมแวร์)-มัลแวร์ ติดRansomware	O: Operation risk	1.ผู้ใช้งานติด Ransomware (แรนซัมแวร์)-มัลแวร์ จาก Email phishing , การไปหน้าเว็บไซต์ที่อันตราย-ไม่มีโปรแกรม antivirus ป้องกัน	2	4	8	1.มีการสำรองข้อมูลระบบสารสนเทศอยู่เสมอ 2. มีการประชาสัมพันธ์ เฝ้าระวัง แจ้งเตือน ให้ความรู้	1	1	1	การลดความเสี่ยง Reduce	1.มีการแจ้งเตือนจากเครื่องคอมพิวเตอร์ ที่ระบุว่าติด Ransomware

(แรนซัมแวร์)-มัลแวร์ ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์ 2.โรงพยาบาล	IM: Image and Reputation Risk	2.เครื่องแม่ข่ายติด Ransomware (แรนซัมแวร์)-มัลแวร์ จากพฤติกรรมการใช้งานของผู้ดูแลระบบ การดาวน์โหลดไฟล์อันตราย-ไม่มีโปรแกรม antivirus ป้องกัน	2	1	2	ผู้ใช้งาน 3.มีแนวปฏิบัติเพื่อแก้ไขเหตุในเบื้องต้น 4.มีการ backup ข้อมูลสำคัญของเครื่องผู้ใช้งานสู่ระบบ backup อื่นๆ 5.มีการจัดทำระบบ system restore point สำหรับเครื่องผู้ใช้งาน 6.ติดตั้งโปรแกรมป้องกันไวรัสและpatch อย่างสม่ำเสมอ 7. ติดตั้งระบบป้องกัน และเตือนภัย Spam,Virus, Malware, Trojan 8.จัดหาอุปกรณ์เพื่อป้องกันเชิงรุก 9. ติดตั้ง patch ของระบบปฏิบัติการสม่ำเสมอ	1	1	1		เมื่อคุณเข้าสู่ระบบปฏิบัติการ 2.เมื่อผู้ใช้เจอไฟล์เอกสารอิเล็กทรอนิกส์มีนามสกุลต่อท้ายเป้น .crypted, .cryptor 3. เมื่อผู้ใช้ได้รับไฟล์ .txt หรือ .html เป็นข้อความระบุวิธีการจ่ายค่าไถ่บนหน้าจอ desktop
	D: Digital Technology Risk		2	3	6		1	1	1		
	CS: Cyber security risk (Availability)		2	2	4		1	1	1		

4.เกิดเหตุข้อมูลส่วนบุคคลรั่วไหล (Data leaks) ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์ 2.โรงพยาบาล	IM: Image and Reputation Risk	เกิดเหตุข้อมูลส่วนบุคคลรั่วไหล -จากการดำเนินงานของบุคคลากร -จากช่องโหว่ของระบบสารสนเทศ -จากการ hack ข้อมูล -จากการเข้าถึงข้อมูลส่วนบุคคลของคนอื่น	2	1	2	1.จัดหาอุปกรณ์เพื่อป้องกันเชิงรุก 2.มีแนวปฏิบัติเพื่อรองรับเหตุข้อมูลส่วนบุคคลรั่วไหล 3.มีนโยบายคุ้มครองข้อมูลส่วนบุคคล 4.จัดทำแนวปฏิบัติ สำหรับการนำอุปกรณ์ที่เชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่าย สำหรับระบบสารสนเทศที่มีความสำคัญ 5.สร้างความตระหนักและให้ความรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล 6. มีการเข้ารหัสข้อมูลที่สำคัญเพื่อป้องกันข้อมูลส่วนบุคคลรั่วไหล 7.มีการจัดทำสัญญาการประมวลผลข้อมูลระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล	1	1	1	การลดความเสี่ยง Reduce	1.เมื่อได้รับการแจ้งจากเจ้าของข้อมูลส่วนบุคคลตามช่องทางที่ประชาสัมพันธ์ 2.เมื่อผู้ดูแลระบบตรวจสอบพบข้อมูลส่วนบุคคลปรากฏในเว็บสาธารณะหรือเข้าถึงได้โดยสาธารณะ 3.ได้รับการแจ้งเตือน information leak จากระบบ cern
	D: Digital Technology Risk		2	2	4		1	1	1		
	CS: Cyber security risk (Confidential)		2	2	4		1	1	1		
	P: Personnel Risk		2	1	2		1	1	1		

5. ความเสี่ยงจากการเอาอุปกรณ์ที่ไม่ได้รับอนุญาตมาเชื่อมต่อ ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์	D: Digital Technology Risk	1.ผู้ใช้ขาดความระมัดระวังในการใช้งานระบบเครือข่าย เช่นการนำอุปกรณ์ switch hub access point มาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาลโดยมิได้รับอนุญาต ซึ่งมีผลกระทบระบบเครือข่ายของโรงพยาบาล เช่นระบบเครือข่ายไม่สามารถใช้งานได้ ลดทอนประสิทธิภาพการทำงานอุปกรณ์เครือข่าย เป็นต้น 2. ผู้ปฏิบัติงานนำ usb มาเชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่ายหรือระบบสารสนเทศที่มีความสำคัญ เป็นเหตุให้เกิดการติดไวรัส หรือเกิดการ	2	5	10	1.จัดทำแนวปฏิบัติ สำหรับการนำอุปกรณ์ที่เชื่อมต่อระบบเครือข่าย 2.จัดทำแนวปฏิบัติ สำหรับการนำอุปกรณ์ที่เชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่าย สำหรับระบบสารสนเทศที่มีความสำคัญ 3. จัดทำ Policy บน active directory (GPO) เพื่อ Block การใช้ Flash Drive/USB สำหรับระบบสารสนเทศที่สำคัญ	1	1	1	การลดความเสี่ยง Reduce	1.ระบบมอนิเตอร์แจ้งเตือนการพบ Rouge ap 2.ระบบเครือข่ายขัดข้องการเชื่อมต่อแบบ loop 3. ระบบมอนิเตอร์แจ้งเตือนระบบเครือข่ายทำงานผิดปรกติ
	CS: Cyber security risk (Confidential)		2	2	4		1	1	1		
	S: Strategic risk		2	5	10		1	1	1		

	P: Personnel Risk	นำข้อมูลที่มีความสำคัญออกจากระบบโดยไม่ได้รับอนุญาติ	2	1	2		1	1	1		
6. เกิดภัยคุกคามประเภท Phishing (ฟิชชิง) ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์	D: Digital Technology Risk	ผู้โจมตีส่งอีเมลฟิชชิ่งแบบเจาะจงกลุ่มเป้าหมายไปยังผู้ใช้งานระบบเมลล์ ซึ่งเมื่อคลิกแล้วจะทำให้บัญชีผู้ใช้โดน *hack*	5	3	15	1.อบรมและให้ความรู้แก่พนักงานในองค์กรให้ตระหนักถึงความอันตรายและการป้องกันตนเองจากภัยคุกคาม 2.จัดให้มีอุปกรณ์ หรือระบบป้องกันภัยคุกคาม	5	2	10	การลดความเสี่ยง Reduce	1.ตรวจพบการส่ง email phishing เข้าสู่ระบบเมลล์โรงพยาบาล 2.ตรวจพบการส่งemail phishing ออกจาก ระบบเมลล์โรงพยาบาล 3.ได้รับการแจ้งเตือนการพบเว็บไซต์ phishing ภายใต้โดเมนของโรงพยาบาล
	CS: Cyber security risk (Confidential)		5	2	10		5	1	5		
	P: Personnel Risk		5	1	5		5	1	5		

											จาก thaicert, สกมช. และองค์กรที่เกี่ยวข้อง
7. ทรัพย์สินด้านเทคโนโลยีสารสนเทศสูญหายจากการโจรกรรม ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์	F: Financial and Asset Risk	มีการลักขโมยทรัพย์สินด้านเทคโนโลยีสารสนเทศ เช่น การขโมยตัดสายสัญญาณระบบเครือข่าย การขโมยครุภัณฑ์เครือข่าย อุปกรณ์สารสนเทศได้รับ	2	2	4	1.มีการจัดทำทะเบียนครุภัณฑ์-มอบหมายผู้รับผิดชอบ 2.จัดให้มีระบบตรวจสอบการทำงานของอุปกรณ์เครือข่าย 3.ติดตั้งกล้องวงจรปิดสำหรับห้อง internet data center / ห้องเก็บข้อมูลสารสนเทศที่สำคัญ 4.รักษาความปลอดภัยของอาคารสถานที่ 5.เฝ้าระวังการลักลอบตัดสายสัญญาณระบบเครือข่าย-โทรศัพท์ 6.การทำประกันภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศ	1	1	1	การลดความเสี่ยง Reduce การถ่ายโอนความเสี่ยง Transfer	1.ระบบมอนิเตอร์ตรวจสอบพบอุปกรณ์เครือข่ายไม่ทำงาน ซึ่งอาจเป็นกรณีสูญหาย 2.ได้รับแจ้งจากงานรักษาความปลอดภัย 3.การหาครุภัณฑ์ไม่พบจากการตรวจสอบครุภัณฑ์ประจำปี
	D: Digital Technology Risk		2	2	4		1	1	1		
	O:Operation risk		2	3	6		1	1	1		

8. ระบบเครือข่ายคอมพิวเตอร์ไม่สามารถใช้งานได้ 24 ชั่วโมง ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์ 2.ส่วนอาคารสถานที่	CS: Cyber security risk (Availability)	1. มีสายใยแก้วนำแสง (fiber optic) สำรองไม่ครอบคลุมทุกอาคาร 2. สายสัญญาณระบบเครือข่ายมีอายุการใช้งานมายาวนานทำให้เกิดการเสื่อมสภาพ 3. อุปกรณ์ระบบเครือข่ายสำรองไม่เพียงพอ 4. ไฟฟ้าดับเป็นเวลานาน 5. ภัยธรรมชาติ (พายุ ฝนตก กระรอกกัด หนูกัด มดเข้าอุปกรณ์) 6. การปรับปรุงพื้นที่โดยไม่ได้ประสานกับศูนย์คอมพิวเตอร์	4	2	8	1. ของบประมาณเพื่อขยายสายใยแก้วนำแสง (Fiber Optic) ให้ครอบคลุมทุกอาคารที่ยังไม่มีเส้นสำรอง 2. ประสานหน่วยงานที่เกี่ยวข้องในการปรับภูมิทัศน์ไม่ให้กระทบกับสายสัญญาณ 3. ของบประมาณเพื่อจัดซื้ออุปกรณ์เครือข่ายที่จำเป็น 4. ของบประมาณในการจัดซื้อเครื่องสำรองไฟฟ้าให้เพียงพอ 5. ประสานงานกับหน่วยงานที่ดูแลความสะอาดภายในหน่วยงานอย่างสม่ำเสมอ 6. ประสานกับหน่วยงานที่เกี่ยวข้องในการปรับปรุงพื้นที่ที่มีผลกระทบกับหน่วยงาน 7.ของบประมาณเพื่อจัดทำป้ายระบุแนวสายสัญญาณระบบเครือข่าย เพื่อลดอุบัติเหตุจากการขุดเจาะพื้นที่โดนสายสัญญาณระบบเครือข่าย 8.การทำประกันภัยทรัพย์สิน	1	1	1	การลดความเสี่ยง Reduce การถ่ายโอนความเสี่ยง Transfer	1. ระบบเครือข่ายขัดข้องไม่สามารถใช้งานได้ 2.ระบบมอนิเตอร์ตรวจสอบพบอุปกรณ์เครือข่ายไม่ทำงาน 3.ระบบมอนิเตอร์ตรวจสอบพบสัญญาณ loss ของอุปกรณ์ระบบเครือข่าย
	D: Digital Technology Risk		4	3	12		1	2	2		
	O:Operation risk		4	4	16		1	3	3		

						ด้านเทคโนโลยีสารสนเทศ					
9. จำนวนบุคลากรด้านไซเบอร์ไม่เพียงพอ ผู้รับผิดชอบความเสี่ยง 1.ส่วนทรัพยากรบุคคล	O : Operational Risk	1.เจ้าหน้าที่ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ไม่เพียงพอ 2.ขาดหน่วยงานที่รับผิดชอบดูแลการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์โดยตรง	4	4	16	1.จัดทำแผนกำลังคนด้านความมั่นคงปลอดภัยไซเบอร์-วิเคราะห์อัตรากำลังอย่างเหมาะสม 2.สร้างบุคลากรเพื่อเป็นกำลังคนผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ 3.สร้างหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ (Security Operation Center) หรือ SOC	2	2	4	การลดความเสี่ยง Reduce	1.จำนวนภัยคุกคามทางไซเบอร์ที่มากขึ้น 2.การปฏิบัติงานของเจ้าหน้าที่ไม่สามารถทำงานในเชิงรุกได้
	P: Personnel Risk		4	4	16		2	1	2		
10.ความเสี่ยงต่อการได้รับงบประมาณสนับสนุน ไม่เพียงพอ ผู้รับผิดชอบความเสี่ยง 1.ส่วนแผนงาน	S : Strategic risk	ขาดแคลนงบประมาณในการดำเนินงานเพื่อสร้างความปลอดภัยทางไซเบอร์ , ความคงอยู่ของระบบสารสนเทศ	4	4	16	1.จัดหาแหล่งเงินทุนอื่นๆ นอกจากงบประมาณของโรงพยาบาล 2.มีกระบวนการในการพิจารณาระดับความสำคัญในการจัดสรรงบประมาณด้าน	3	2	6	การลดความเสี่ยง Reduce	1.การได้รับการจัดสรรงบประมาณด้านความมั่นคงปลอดภัยไซเบอร์ (งบประจำ)
	O : Operational Risk		4	4	16		3	2	6		

	F: Financial and Asset Risk		4	4	16	ความมั่นคงปลอดภัยไซเบอร์อย่างเพียงพอ	3	2	6		ลดลงทุกปี
11.การ Hack เว็บไซต์ ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์ 2.ทุกหน่วยงานภายในโรงพยาบาล	D: Digital Technology Risk	ผู้จัดทำเว็บไซต์ ปล่อยปละละเลยการให้ความสำคัญในการดูแลรักษาเว็บไซต์ให้ปลอดภัย -การตั้งค่า file folder ที่ไม่ปลอดภัย -เว็บไซต์มีช่องโหว่	5	3	15	1.ตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์อยู่เสมอ 2.สำรองข้อมูลอยู่เสมอ 3.patch ระบบความปลอดภัยของระบบสารสนเทศอยู่เสมอ 4.ใช้ password สำหรับผู้ดูแลระบบแบบซับซ้อน 5.ใช้ช่องทางการรหัสข้อมูลสำหรับระบบสารสนเทศที่มีความสำคัญ 6.เข้ารหัสข้อมูลในฐานข้อมูลเพื่อปกป้องfield ข้อมูลที่มีความสำคัญ 7.เก็บรักษา account ผู้ดูแลระบบ-ftp account เฉพาะผู้เกี่ยวข้องเท่านั้น 8.backup ข้อมูลระบบเว็บไซต์อยู่เสมอ 9.หมั่นตรวจสอบ malware spyware บนเครื่องคอมพิวเตอร์ส่วนบุคคล	3	1	3	การลดความเสี่ยง Reduce	1.ได้รับการแจ้งเตือน จากสกมช. 2.การตรวจสอบพบการเปิด permission ที่เหมาะสม 3.ได้รับการแจ้งเตือนจากผู้พบเห็น-หน่วยงานที่เกี่ยวข้อง
	IM: Image and Reputation Risk		5	2	10		3	1	3		
	CS: Cyber security risk (Confidential)		5	2	10		3	1	3		

12.ความเสี่ยงจากการปัญหาละเมิดลิขสิทธิ์ software ผู้รับผิดชอบความเสี่ยง 1.ศูนย์คอมพิวเตอร์ 2.โรงพยาบาล	F: Financial and Asset Risk	บุคลากร-นักศึกษาติดตั้งโปรแกรมละเมิดลิขสิทธิ์เนื่องจากความประสงค์เพื่อใช้งานส่วนตัว -โรงพยาบาล ไม่มีโปรแกรมลิขสิทธิ์สนับสนุนการใช้งานของบุคลากร-นศ อย่างทั่วถึง	4	5	20	1.รณรงค์ในการใช้ software ถูกลิขสิทธิ์ 2.จัดสรรงบประมาณเพื่อจัดซื้อ software สำหรับการเรียนการสอนอย่างเพียงพอ 3.จัดทำระบบบริการเข้าใช้งาน software ลิขสิทธิ์จากส่วนกลาง 4.รณรงค์-แนะนำการใช้softwareประเภท freeware	2	2	4	การลดความเสี่ยง Reduce การหลีกเลี่ยงความเสี่ยง Avoid	1.ผู้ดูแลระบบได้รับการแจ้งเตือนการละเมิด software ลิขสิทธิ์
	D: Digital Technology Risk		4	4	16		2	2	4		
	O : Operational Risk		4	3	12		2	1	2		
13.ความเสี่ยงจากเครื่องคอมพิวเตอร์ขัดข้อง ไม่สามารถใช้งานได้ตามปกติ	O : Operational Risk	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุด ด้วยสาเหตุทางเทคนิค	4	3	12	1.backup ข้อมูลเครื่องผู้ใช้งานอยู่เสมอ 2. มีเครื่องคอมพิวเตอร์สำรองทดแทนกรณีเครื่องคอมพิวเตอร์ขัดข้อง 3.จัดทำข้อกำหนด TOR เพื่อเช่าเหมาบริการเครื่อง	3	1	3	การลดความเสี่ยง Reduce การถ่ายโอนความ	1.ได้รับการแจ้งซ่อมในระบบติดตามงานเอกสารอิเล็กทรอนิกส์ภายในศูนย์คอมพิวเตอร์
	D: Digital Technology Risk		4	3	12		3	1	3		

						คอมพิวเตอร์ให้ครอบคลุมการซ่อมบำรุง-หรือการเปลี่ยนทดแทนกรณีเครื่องเกิดปัญหา				เสี่ยง 	E-Doc-Track (Electronic Document Tracking System) (https://dccs.sut.ac.th)
14.บุคคลากรยังไม่มีความรู้ความเข้าในในเรื่องความปลอดภัยไซเบอร์ ผู้รับผิดชอบความเสี่ยง 1.คณะกรรมการบริหารความเสี่ยงและการควบคุมภายในโรงพยาบาล 2.คณะกรรมการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ 3.ศูนย์คอมพิวเตอร์	P : Personnel Risk =	บุคลากรส่วนใหญ่ไม่มีความรู้พื้นฐานจากการป้องกันภัยคุกคามทางไซเบอร์	5	3	15	1. อบรมและให้ความรู้แก่พนักงานในองค์กรให้ตระหนักถึงความอันตรายและการป้องกันตนเองจากภัยคุกคามไซเบอร์	4	1	4	การลดความเสี่ยง 	1.การเกิดภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเพิ่มมากขึ้น 2.เกิดการ hack account สารสนเทศของบุคลากรโรงพยาบาล เพิ่มมากขึ้น
	C : Compliance risk		5	4	20		4	1	4		
	S : Strategic risk		5	4	20		4	2	8		

15.ขาดการทบทวนแนวปฏิบัติ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ผู้รับผิดชอบความเสี่ยง 1.คณะกรรมการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ 2.ศูนย์คอมพิวเตอร์ 3.หน่วยตรวจสอบภายใน 4.หน่วยงานด้านสารสนเทศอื่นๆ	P : Personnel Risk	ขาดการทบทวนแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ -ขาดการตรวจสอบ -ขาดการประเมินความเสี่ยง -ผู้รับผิดชอบหลัก ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	5	4	20	1.ทบทวนประกาศ มทส. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาล พ.ศ. 2554 2.จัดให้มีการตรวจสอบประเมิน-รายงานผลความเสี่ยงประจำทุกปี 3.ประชาสัมพันธ์ ประกาศ-นโยบาย เพื่อให้บุคลากรรับทราบและปฏิบัติ	1	1	1	การลดความเสี่ยง Reduce	1.การขาดการปฏิบัติตามประกาศ มทส. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 2.ขาดการติดตามผล-รายงานผลการปฏิบัติของหน่วยงานที่เกี่ยวข้อง
	C: Compliance risk		5	4	20		1	1	1		
	S : Strategic risk		5	4	20		1	1	1		