

แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
และการสื่อสารของหน่วยงาน

โรงพยาบาลทุ่งเสลี่ยม

LT Bird.

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. ความหมายและความสำคัญของการจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใน

สถานการณ์ที่ ไม่แน่นอน และจะส่งผลกระทบต่อหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิด ความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุ วัตถุประสงค์ที่กำหนดไว้โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนด มาตรการลด ความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะ ของ ความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้ โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยง ลดลง อยู่ในระดับที่องค์กรยอมรับได้ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลด ความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยง ตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) มีดังนี้

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

2. ความหมายของการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ กระบวนการการทำงานที่ช่วยให้ IT Managers สามารถสร้างความสมดุลของต้นทุนเชิงเศรษฐศาสตร์และการดำเนินธุรกิจ ระหว่าง มาตรการในการป้องกันและการบรรลุผลสำเร็จของพันธกิจ ด้วยการปกป้องระบบเทคโนโลยีสารสนเทศ และข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

2.1 Access Risk : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์โดยบุคคล ที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูล และระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่ได้รับผิดชอบ ซึ่งหากหน่วยงานไม่ได้มีวิธีการจัดการและ ควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจ หน้าที่ที่เกี่ยวข้องได้ล่วงรู้ ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ก็ อาจถูกแก้ไขเปลี่ยนแปลงได้ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถ เข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่ได้รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงาน ไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยง ด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนด สิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความ จำเป็นในการใช้งาน การไม่ได้มีการกำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่าง รัดกุมเพียงพอ การมิได้จำกัดและควบคุมให้เฉพาะ เจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์ คอมพิวเตอร์ เป็นต้น

2.2 Integrity Risk : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงาน ของระบบคอมพิวเตอร์ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการ บันทึกรหัสข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่ หน่วยงานมิได้มีการ ควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่ เกี่ยวข้องที่รอบคอบและ

รัศกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบ คอมพิวเตอร์อาจถูกแก้ไข เปลี่ยนแปลงโดยมิชอบได้หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและ ตรวจสอบอย่างเพียงพอเพื่อให้ มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความ ถูกต้องครบถ้วน นอกจากนี้การบริหาร จัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือ เปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและ รัศกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการ ประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับ ความต้องการของผู้ใช้งานได้

2.3 Availability Risk : เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ ได้ อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้โดยความเสี่ยงนี้อาจเกิด จากการ มิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยัง รวมไปถึง การมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้หาก หน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบ และรัศกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของ ระบบคอมพิวเตอร์เสียหายได้

2.4 Infrastructure Risk : เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานมิได้จัดให้มีการบริหาร จัดการ ด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ตีรวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ โดยความเสี่ยงนี้อาจเกิดจาก การแบ่งแยกอำนาจ หน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบย้อนและการตรวจสอบการปฏิบัติงาน ที่เพียงพอ รวมถึงการ มิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและ ขั้นตอนการปฏิบัติงานที่ ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการ ปฏิบัติงาน นอกจากนี้ก็อาจ เกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การ สนับสนุนการดำเนินงาน และการ มิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มี ความรอบรู้และเชี่ยวชาญในงานที่ รับผิดชอบ

นอกจากความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารของ หน่วยงานมิได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจ ดังนั้น หน่วยงาน ควร พิจารณาว่าข้อมูลใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของ ข้อมูล และจัดเตรียมข้อมูลดังกล่าวให้พร้อม เพื่อประโยชน์ในการดำเนินงานของหน่วยงาน

3. ความเสี่ยงและแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศขององค์กรสามารถแบ่งออกเป็น 4 ประเภท ดังนี้

3.1 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทาง ธรรมชาติ สิ่งแวดล้อมที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น

- วัตถุภัย อุทกภัย ไฟฟ้า น้ำท่วม
- กระแสไฟฟ้าขัดข้อง
- เพลิงไหม้
- การไม่มีระบบควบคุมการเข้า-ออก ห้องคอมพิวเตอร์แม่ข่าย (Server Room)

การบริหารจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม มีประเด็นหลัก ดังนี้

3.1.1 พิจารณาการตำแหน่งของห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารหลัก (Server Room & Network Equipment) ที่จะเป็นที่จัดเก็บและติดตั้งระบบเทคโนโลยีสารสนเทศไว้ยังเครื่อง คอมพิวเตอร์แม่ข่าย (Server Computer) และการกำหนดที่ตั้งระบบเทคโนโลยีสารสนเทศไว้ยังเครื่อง คอมพิวเตอร์การเดินสายไฟฟ้า สายวงจร สายสัญญาณของระบบต่างๆ อย่างเน้นความปลอดภัยและ หลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่น เครื่องปรับอากาศ ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย หน้าต่างระบบความร้อนถึงดับเพลิง เป็นต้น

3.1.2 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) โดยมีการจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อ พ่วงระบบสัญญาณเครือข่ายที่เชื่อมโยงไว้ในห้องคอมพิวเตอร์แม่ข่าย (Server Room) ของสำนักงาน ซึ่ง ในกรณีที่มีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำอำนาจมีความจำเป็นต้องเข้าห้องคอมพิวเตอร์แม่ข่ายในบางครั้ง จำเป็นต้องมีการควบคุมอย่างรัดกุมและรอบคอบ เช่น กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบ ควบคุมดูแลการทำงานตลอดเวลา การแจ้งทีมงานเทคโนโลยีสารสนเทศทราบก่อนทุกครั้งและต้องเซ็นชื่อ ในสมุดบันทึกเข้าออกห้องสื่อสารทุกครั้ง เป็นต้น

3.1.3 จัดห้องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วนเฉพาะ โดยแบ่งออกเป็นสัดส่วน ดังนี้ส่วน เครื่องคอมพิวเตอร์แม่ข่าย (server zone) ส่วนคอมพิวเตอร์ลูกข่าย (client zone) และส่วนของระบบ เครือข่าย (network zone) เพื่อความสะดวกในการปฏิบัติงาน และยังทำให้การควบคุมการเข้าถึงอุปกรณ์ คอมพิวเตอร์ต่างๆ มีประสิทธิภาพมากยิ่งขึ้น

3.1.4 การจัดแยกส่วนอุปกรณ์ที่จำเป็นในการเข้าถึงข้อมูลโดยเจ้าหน้าที่ของศูนย์ข้อมูล เช่น ส่วนที่ใช้เก็บรายงานต่างๆหรือข้อมูลทำงานเทคโนโลยีสารสนเทศของจังหวัดได้จัดทำสำรองข้อมูล (Backup) ไว้กรณีฉุกเฉินเมื่อข้อมูลที่จัดทำไว้เกิดการเสียหาย โดยจัดเก็บไว้โดยเจ้าหน้าที่ของงาน เทคโนโลยีสารสนเทศ กลุ่มงาน ข้อมูลสารสนเทศและการสื่อสาร

3.1.5 การป้องกันความเสียหาย โดยการวางระบบป้องกันไฟที่เหมาะสม มีระบบตรวจจับ คิวไฟ จัดให้มีถึงดับเพลิงที่พร้อมใช้งานได้ตลอดเวลากรณีฉุกเฉินเพื่อใช้ในการดับเพลิงเบื้องต้น

3.1.6 การป้องกันความเสี่ยงจากระบบป้องกันไฟฟ้าลัดวงจร ทำได้โดยมีระบบป้องกันไฟฟ้า กระชากไม่ให้คอมพิวเตอร์แม่ข่ายได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้าท้องถิ่น อีกทั้งการ ติดตั้งระบบ สายดิน (Ground) ที่ได้มาตรฐานอุปกรณ์ป้องกันไฟ จัดให้ระบบไฟฟ้าสำรองสำหรับ คอมพิวเตอร์ทั้งแม่ข่าย และลูกข่าย เพื่อให้การดำเนินงานมีความต่อเนื่องกรณีท้องถิ่นดับหรือเกิดขัดข้องไม่ สามารถใช้งานได้

3.1.7 การป้องกันความเสี่ยงจากระบบควบคุมอุณหภูมิและความชื้น ทำโดยให้มีการควบคุม สภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยการตั้งอุณหภูมิเครื่องปรับอากาศและค่า ความชื้นให้ มีระดับเหมาะสมกับลักษณะ (specification) ของระบบคอมพิวเตอร์สิ่งแวดล้อมที่เหมาะสม ที่คอมพิวเตอร์จะ ทำงานได้ดีนั้น อุณหภูมิและความชื้นจะต้องมีความชื้นจะต้องมีความเหมาะสมดังนั้นห้อง ทำงานด้าน คอมพิวเตอร์จึงควรเป็นห้องปรับอากาศที่มีประสิทธิภาพ ปราศจากฝุ่นละอองและความชื้น เพราะเครื่อง คอมพิวเตอร์และข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์อาจได้รับความเสียหายจากการได้รับ ความร้อนสูง ในส่วนของห้องคอมพิวเตอร์และข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์อาจได้รับความ เสียหายจากการได้รับความ ร้อนสูง

3.1.8 ความเสี่ยงในเรื่องของงบประมาณที่จะดำเนินการอย่างได้ประสิทธิภาพสูงสุดและ เกิดความ ต่อเนื่อง

3.1.9 ความเสี่ยงในเรื่องของประเด็นนโยบายของกระทรวงมหาดไทย ศูนย์เทคโนโลยี สารสนเทศและ การสื่อสารที่ให้น้ำหนักและความสำคัญในเรื่องระบบเทคโนโลยีสารสนเทศ ซึ่ง นโยบายและวิสัยทัศน์ของ แต่ละยุคสมัยเปลี่ยนแปลงไป อันส่งผลมายังหน่วยงานในแต่ละจังหวัด ตลอดถึงแนวทางในการดำเนินงานใน ชั้นตอนต่อไป

3.1.10 ความเสี่ยงในเรื่องของการบริหารจัดการ สามารถวางแผนบริหารความเสี่ยง และ ดำเนินการ เพื่อความเสี่ยงได้ดังนี้

- ศึกษาวิเคราะห์และจัดทำระบบข้อมูลเพื่อการบริหารราชการ ในการสนับสนุนการ ตัดสินใจผู้บริหาร ระดับสูง (Executive Information System)

- ให้บริการฝึกอบรมเพื่อพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศของบุคลากร

3.2 ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศของจังหวัดรวมถึงการวางแผนการตรวจสอบการทำงานการ มอบหมายหน้าที่และสิทธิของบุคลากร / คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่าง ละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบ เทคโนโลยีสารสนเทศ ตลอดจนบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อมล้วนแต่เป็นความเสี่ยง ความเสี่ยงด้านบุคลากรเป็นความเสี่ยงหนึ่งที่สำคัญ ดังนั้นจึงควรมีแนวทางและการวางแผนที่กำกับ ดูแลการบริหารจัดการและควบคุมความเสี่ยงบุคลากรของจังหวัดอย่างจริงจังจึงการบริหารจัดการความเสี่ยง ด้านบุคลากร มีประเด็นหลัก ดังนี้

3.2.1 กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศของจังหวัด และการบริหารจัดการด้านบุคลากร การแต่งตั้งเจ้าหน้าที่ที่มีความเหมาะสม (มีความรู้ความสามารถและประสบการณ์ด้านคอมพิวเตอร์ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีด้านการรักษาความปลอดภัยระบบฯ และสามารถความรู้ชั้น ให้แก่ผู้ใช้งานระบบฯของหน่วยงานได้อย่างมีประสิทธิภาพ) เมื่อมีการปรับและแจ้ง รายชื่อผู้รับผิดชอบ เจ้าหน้าที่ที่รักษาความปลอดภัยระบบฯ และผู้ดูแลระบบฯ) ที่มีการเปลี่ยนแปลง เช่น โยกย้ายลาออก ฯลฯ จะต้องแจ้งให้แก่ผู้บังคับบัญชาได้รับทราบ เพื่อประโยชน์ในการบริหารบุคลากร การติดต่อประสาน แจ้งเตือนภัย ฝึกอบรม และการรักษาความปลอดภัยระบบสารสนเทศ อย่างมีประสิทธิภาพ หากบุคลากรด้านเทคโนโลยีสารสนเทศไม่มีการจัดโครงสร้างและการบริหารจัดการที่ดี เพียงพอ ก็อาจทำให้เกิดความเสี่ยงด้านโครงสร้างการบริหารงานได้การกำหนดโครงสร้าง การแบ่งแยก อำนาจหน้าที่ การกำหนดนโยบายและขั้นตอนการปฏิบัติงานและกำกับดูแลควบคุมการปฏิบัติงานเป็น หลัก

3.2.2 การว่าจ้าง / จัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อจัดทำโครงการด้านระบบ เทคโนโลยีสารสนเทศภูมิศาสตร์เพราะเป็นผู้มีความรู้ความชำนาญเฉพาะทาง มีเครื่องมือและเทคโนโลยี ที่ใช้พร้อมและทันต่อการพัฒนาระบบฐานข้อมูลสารสนเทศเฉพาะด้านมากกว่าภาคราชการ โดยการ ว่าจ้างบุคลากรภายนอกนี้ก็จะมีความเสี่ยงในเรื่องของ ความรู้ความเข้าใจในระบบราชการ และผลสัมฤทธิ์ ที่เกิดจากการทำงาน อีกทั้งในแง่ของความคุ้มค่าของการใช้จ่ายงบประมาณ ดังนั้น แนวทางในการ วางแผนบริหารความเสี่ยงของการว่าจ้างบุคลากรภายนอกนี้ทำได้โดย หน่วยงานที่เป็นเจ้าของเรื่อง หรือ เป็นผู้รับผิดชอบในประเด็นต่างๆ ต้องเป็นผู้เข้ามากำกับดูแลตั้งแต่เริ่มกระบวนการ และต่อเนื่อง โดย หลักการบริหารจัดการที่ดีอีกทั้งรักษาผลประโยชน์ของทางราชการให้มากที่สุด

3.2.3 บุคลากรของภาคราชการ ขาดความรู้ความเข้าใจเรื่องของระบบเทคโนโลยีสารสนเทศ โดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรม และนวัตกรรมใหม่ ทำให้เกิดช่องว่างในการที่จะประสานงาน และรับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงในประเด็นนี้ โดยการส่ง

เจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศ รวมถึงการรับบุคลากรที่มีความรู้ ความเข้าใจด้านระบบเทคโนโลยีสารสนเทศมาปฏิบัติงานในหน่วยงานราชการมากยิ่งขึ้น

3.2.4 แผนการบริหารความเสี่ยงด้านบุคลากร คือ ต้องมีการฝึกอบรมในด้านที่เกี่ยวข้องกับ ระบบฐานข้อมูลสารสนเทศของจังหวัด สำหรับบุคลากรของส่วนราชการ ใน 2 ระดับ คือ ระดับผู้ดูแล ระบบ (Administrator) และใช้งานทั่วไป (User) ทำให้บุคลากรของหน่วยงานสามารถใช้งานระบบ สารสนเทศ ดูแลปรับปรุง และพัฒนาระบบได้เป็นการสนับสนุนบุคลากรทางคอมพิวเตอร์รวมทั้ง ผู้ใช้งานให้มีความรู้ด้านการรักษาความปลอดภัยระบบ ได้อย่างมีประสิทธิภาพ

3.3 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาด ช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเป็นความเสี่ยงที่เกิดจากทำงานผิดพลาดของอุปกรณ์ ช่องโหว่ของอุปกรณ์ตลอดจนการเคลื่อนย้ายตัวเครื่อง อุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ ไวรัสคอมพิวเตอร์ เป็นต้น การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ มีประเด็นหลัก ดังนี้

3.3.1 ความเสี่ยงในเรื่องของจัดหาอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมกับแผนงาน / โครงการและองค์กร (Planning and Organization) ซึ่งควรให้มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ ต่างๆให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการ และเหมาะสมด้วยงบประมาณ

3.3.2 ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (Support) ซึ่งการ ลดโอกาสที่จะเกิดความเสียหายในกรณีได้แก่

- 1) การบำรุงรักษาและลดความเสี่ยง
 - มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และการดูแลอย่างถูกต้องและต่อเนื่อง
 - ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว
 - การใช้แผ่นซีดีหรือ Handy drive ควรตรวจสอบไวรัสก่อนทุกครั้ง
 - ควรปิดฝุ่นหรือทำความสะอาดเครื่องคอมพิวเตอร์ให้ใหม่อยู่เสมอ เพราะเมื่อมีฝุ่น เข้าสู่เครื่องคอมพิวเตอร์มากๆ จะทำให้เครื่องคอมพิวเตอร์ร้อนจัดได้ง่าย เป็นสาเหตุของอาการเครื่องค้าง หรือรวนได้
 - โปรแกรม Windows จะมีคำสั่งในการบำรุงรักษาเครื่อง (Maintenance) ซึ่งผู้ดูแล ระบบควรใช้คำสั่งนี้เป็นประจำ

- การติดตั้งไฟร์วอลล์ (Firewall) เพื่อป้องกันเบื้องต้นไม่ให้ผู้ที่ไม่ได้รับอนุญาตจาก ระบบเครือข่าย อินเทอร์เน็ตสามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ

- การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ

- การฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงานเกี่ยวกับ การใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง และการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ เช่น การกำหนดรหัส ผู้ใช้และการใช้รหัสผ่าน

- การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ

- การสำรองข้อมูล (Backup) ข้อมูลระบบสารสนเทศ

- การบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ได้แก่ ระบบปฏิบัติการ คอมพิวเตอร์ระบบ เครือข่าย และการใช้งานและประสิทธิภาพของเครื่องคอมพิวเตอร์อุปกรณ์เทคโนโลยี สารสนเทศ

2) การรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่าย (Server)

- กำหนดขั้นตอนหรือวิธีการปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของ คอมพิวเตอร์แม่ข่าย และในกรณีที่มีพบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข และรายงานให้ผู้บังคับบัญชาทราบทันที

- ทำการทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัยและ ประสิทธิภาพการใช้งาน อย่างสม่ำเสมอ

- กำหนดบุคคลรับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ โปรแกรม คอมพิวเตอร์แม่ข่ายอย่างชัดเจน

3.4 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรม ต่างๆ ที่ได้จัดทำและพัฒนาขึ้น สำหรับโครงการด้านเทคโนโลยีสารสนเทศ รวมถึงโปรแกรมประยุกต์อื่นๆ ที่ใช้ประกอบการใช้โปรแกรมและระบบงาน ตัวอย่าง ตัวอย่างเช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไข เปลี่ยนแปลง คำสั่ง และการถูกไม่หวังดีทำลายระบบ (Hacker) เป็นต้น การบริหารจัดการความเสี่ยงด้านโปรแกรม คอมพิวเตอร์มีประเด็นหลัก ดังนี้

3.4.1 มีการพัฒนามาตรฐานและการบริหารโปรแกรมคอมพิวเตอร์

- พัฒนาและปรับปรุงมาตรฐาน Hardware Software People ware Data และ Network ให้เป็นฐานข้อมูลกลางของงานเทคโนโลยีสารสนเทศ และเป็นไปในทิศทางเดียวกัน
- สร้างกลไกการจัดการฐานข้อมูล การจัดระบบสารสนเทศเพื่อการบริหารจัดการ ของหน่วยงานให้ครบถ้วนและครอบคลุมมากยิ่งขึ้น
- พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลให้มีมาตรฐานและแบ่งสรรกรการ ให้ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้
- พัฒนาโปรแกรมให้สามารถจัดเก็บ รวบรวม ประมวลข้อมูล ศึกษาวิเคราะห์เพื่อ การนำเสนอและสนับสนุนการบริหารราชการ และพัฒนา ส่งเสริม บำรุงรักษาระบบ และการเผยแพร่ ข้อมูลข่าวสารของจังหวัดได้ในลักษณะของ Web Application เพื่อความสะดวกในการใช้งานและ แสดงผล

3.5 ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่างๆที่เกิดขึ้นกับระบบเครือข่าย ขององค์กรทั้งระบบอินทราเน็ต (Intranet) และอินเทอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจาก ปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้านกายภาพ ความเสี่ยงด้าน ระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัย คุกคามต่างๆ การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีประเด็นหลัก ดังนี้

3.5.1 ความเสียหายที่เกิดขึ้นจากระบบเครือข่าย การเฝ้าระวังและตรวจสอบระบบเครือข่าย และการจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่าย ได้มีระบบการติดตามและเฝ้าดูแลการใช้ เครือข่าย ภายในและการเข้าออก Internet ทุกวัน รวมทั้งการสร้าง Firewall เพื่อป้องกันการเข้าถึงและ การโจมตีจากภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย (Client) ในเครือข่ายระบบฐานข้อมูล ระบบ Web Server เป็นต้น

3.5.2 พัฒนาระบบงานด้านเครือข่าย โดยการพัฒนา บริหาร ควบคุม กำกับดูแลและ บำรุงรักษาระบบ เครื่องคอมพิวเตอร์และเครือข่ายสารสนเทศพื้นฐานของกระทรวงมหาดไทย ร่วมกับ หน่วยงานอื่นๆ ที่เกี่ยวข้อง การเพิ่มการรักษาและคุ้มครองความปลอดภัยข้อมูลผ่านระบบเครือข่าย

3.5.3 เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ภายในให้มีความเสถียร และมีประสิทธิภาพรองรับกับปริมาณข้อมูล และการเคลื่อนไหวของฐานข้อมูล

3.5.4 หน่วยงานภายในสำนักงาน และผู้มีความรู้ต้องร่วมวิเคราะห์ออกแบบ วางแผนการ จัดการ ระบบโครงข่ายร่วมกันอย่างสมบูรณ์การ และมีการให้คำปรึกษา แนะนำและแก้ไขปัญหาในการ พัฒนา เครือข่าย

3.5.5 มีแผนการรักษาความปลอดภัยของระบบเครือข่าย (Network Security) มี วัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ส่วนรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (Integrity risk) ข้อมูลหรือการทำงานของระบบเครือข่ายที่จะมีผลถึงระบบเครือข่ายที่มีผลถึงระบบ คอมพิวเตอร์ในส่วนที่มีได้อำนาจหน้าที่เกี่ยวข้อง การป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์ เพื่อป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสี่ยง (availability risk) แก่ข้อมูลหรือการทำงานของ ระบบคอมพิวเตอร์ โดยเนื้อหา รายละเอียดเกี่ยวกับแนวในการรักษาความปลอดภัยข้อมูลระบบ คอมพิวเตอร์เครื่องแม่ข่ายและระบบเครือข่าย

1) การบริหารจัดการข้อมูลบนเครือข่าย

- กำหนดชั้นความสำคัญในการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงการเข้าถึงข้อมูลผ่านเครือข่าย

- ในการรับส่งข้อมูลผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็น มาตรฐานสากล

- กำหนดมาตรการรักษาความปลอดภัยข้อมูล เช่น กรณีนำเครื่องคอมพิวเตอร์ส่งซ่อม เป็นต้น

2) การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

- กำหนดสิทธิการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิในการใช้ โปรแกรมระบบงานคอมพิวเตอร์ (Application System) ให้แก่ ผู้ใช้งานให้ เหมาะสมกับหน้าที่และความรับผิดชอบ

- กำหนดระยะเวลาการใช้งานของ User พร้อม Password และระงับการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าว

- กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างรอบคอบ และมีความลับ

- ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นให้มีสิทธิในการใช้งานระบบ คอมพิวเตอร์เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่างๆ ต้องมีการ อนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นรวมถึง กำหนดระยะเวลาในการใช้งาน

3) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

- กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากลโดยทั่วไปไม่ต่ำกว่า 6 ตัวอักษร

- ควรใช้อักขระพิเศษประกอบ เช่น @ ; < > เป็นต้น

- สำหรับผู้ใช้งานทั่วไปจะมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน ส่วน ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 3 เดือน

- ในการเปลี่ยนรหัสผ่านแต่ละครั้งจะไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม ครั้งสุดท้าย
- ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่ มีการลวงรู้รหัสผ่าน โดยบุคคลอื่น ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

3.5.6 การบริหารจัดการและการตรวจรหัสผ่านใหม่โดยทันที

1) กำหนดแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่าย ภายในส่วน เครือข่ายภายนอก

2) ติดตั้งระบบป้องกันการบุกรุก เช่น Firewall ระหว่างเครือข่ายในกับเครือข่ายนอก โดยการติดตั้ง ผ่านอุปกรณ์คอมพิวเตอร์ติดตั้งระบบป้องกันการบุกรุกในระบบเครือข่ายด้วยซอฟต์แวร์และ ฮาร์ดแวร์ให้แก่ ระบบ Firewall ซึ่งเป็นซอฟต์แวร์ทำหน้าที่เสมือนกับกำแพงกันไฟไม่ให้ลูกกลมขยายตัวหาก มีไหม้เกิดขึ้น Firewall จะอาศัยคอมพิวเตอร์เครื่องหนึ่งเป็นด่านเข้าออกเครือข่ายและเป็นเสมือน กำแพงกันไฟ และมี ซอฟต์แวร์ที่ดูแลระบบจะติดตั้งและกำหนดรูปแบบการอนุญาตให้เข้าใช้เครือข่าย อินเทอร์เน็ต

3) จัดทำแผนผังระบบเครือข่าย / แผนผังการเชื่อมโยงระบบเครือข่าย (Network Diagram) ซึ่งมี รายละเอียดเกี่ยวกับขอบเขตของเครือข่ายทั้งในและภายนอกและอุปกรณ์ให้เป็นปัจจุบันอยู่เสมอ

4) ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบ ไวรัส เป็นต้น

5) กำหนดบุคคลผู้รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของอุปกรณ์ เครือข่าย

3.5.7 การป้องกันไวรัสสำหรับระบบเครือข่าย

1) กำหนดมาตรการป้องกันไวรัสที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและ เครื่อง คอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น การปกป้องระบบเครือข่าย สิ่งที่สำคัญอย่างยิ่งคือ ผู้ใช้งานในระบบจะต้องคอยดูแล และป้องกัน ไม่ให้ตนเอง เป็นช่องทางผ่านของ Hacker ผู้ดูแลระบบจะต้องคอยติดตามและหากหาวิธีการป้องกัน และ แก้ไขจุดบกพร่อง ของซอฟต์แวร์ที่ใช้งาน เพราะไม่มีระบบเครือข่ายใดที่ปลอดภัยสมบูรณ์แบบ ดังนั้นต้องมี ระบบป้องกันที่ดีโดย มีวิธีการดังนี้

- ติดตั้งโปรแกรมกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม

- สร้างแผ่น Emergency Disk เพื่อใช้ในการกู้ระบบ
- อัปเดตข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัปเดต
- เปิดใช้งาน Auto Protect
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง
- การป้องกันจากการเปิดไฟล์จากบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- แผ่น CD เทปต่างๆ • สแกนหาไวรัสจากอื่นบันทึกก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif เป็นต้น
- ไม่ใช่สื่อบันทึกที่ไม่ทราบแหล่งที่มา
- การป้องกันจากการเปิด E-Mail
- อย่าเปิดไฟล์ E-Mail จากผู้ส่งที่ไม่รู้จัก และไม่ทราบที่มา
- อย่าเปิดอ่าน E-Mail ที่มีหัวเรื่องเป็นข้อความไม่ปกติ
- ลบ E-Mail ที่ไม่ทราบแหล่งที่มาทั้งหมด
- อัปเดตโปรแกรม E-Mail เสมอ
- การป้องกันจากการดาวน์โหลดจาก Internet
- ไม่เปิดไฟล์ที่แนบมากับโปรแกรมสนทนาต่างๆ
- ไม่ควรเข้า Website ที่มากับ E-Mail
- ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่มั่นใจหรือไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนจากแหล่งข้อมูลก้านความปลอดภัยเสมอ
- หลีกเลี่ยงการแชร์ไฟล์ไม่จำเป็น
- หลีกเลี่ยงการแชร์ไฟล์ประเภท Peer to Peer

3.6 ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆในระบบสารสนเทศ อันอาจจะก่อให้เกิดความเสียหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุก การโจรกรรมข้อมูลสำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ความเสี่ยงเหล่านี้ล้วนมีความจำเป็นที่จะต้องมีการบริหารจัดการ ความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความมั่นคงปลอดภัยของข้อมูลจึงเป็นเรื่องที่สำคัญ ข้อมูลสารสนเทศ เป็นส่วนสำคัญสำหรับผู้บริหาร ที่จะนำความมั่นคงปลอดภัยของข้อมูลจึงเป็นเครื่องมือสำหรับ การตัดสินใจในการวางแผน การจัดการข้อมูล (Management of Data and Communication) ดังนั้น การรักษาความ ปลอดภัยของระบบข้อมูล และ Computer จากภัยต่างๆ ทั้งจากคน จากธรรมชาติหรือ เหตุการณ์ใดๆ จึงสำคัญและจำเป็นต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยีการรักษา ความปลอดภัยด้านข้อมูลสารสนเทศ มีแนวทางหลักดังนี้

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
4. การรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์และระบบเครือข่าย (Information and Network Security)
5. การสำรองข้อมูลระบบคอมพิวเตอร์และการเตรียมพร้อมกรณีฉุกเฉิน (Backup IT Continuity Plan)
6. การบำรุงรักษาอุปกรณ์เครือข่ายและระบบคอมพิวเตอร์ การบริหารจัดการความเสี่ยงด้านข้อมูล มีประเด็นหลัก ดังนี้

3.6.1 ฐานข้อมูล มีความเสี่ยงกับการเข้าถึงข้อมูล (Access Risk)และระบบคอมพิวเตอร์ใน ส่วนที่เกี่ยวข้องหรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบ คอมพิวเตอร์ใน ส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งทางหน่วยงานไม่มีวิธีการจัดการและควบคุมความ เสี่ยง (Access Risk) ที่รอบคอบและรัดกุมอาจทำให้บุคคลไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับข้อมูลและนำ ข้อมูลไปใช้ก่อให้เกิดความเสียหายได้อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ก็อาจถูกแก้ไข เปลี่ยนแปลงได้สำนกรณีบุคคลที่มี อำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลระบบคอมพิวเตอร์ในส่วนที่ เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น

3.6.2 ฐานข้อมูล มีความเสี่ยงเกี่ยวกับความเสี่ยงไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) และ การทำงานของระบบคอมพิวเตอร์ซึ่งอาจเกิดจากถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมา จากการที่หน่วยงาน ไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจ หน้าที่เกี่ยวข้องที่รอบคอบ

และรักรุมเพียงพอ (Access Risk) ซึ่งส่งผลให้ข้อมูลและการทำงานของระบบ คอมพิวเตอร์อาจถูกแก้ไข เปลี่ยนแปลงได้หรือสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบ อย่างเพียงพอ เพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประเมินผล และการแสดงผลมีความถูกต้องครบถ้วน

3.6.3 ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล(Availability Risk) หรือ ระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการซึ่งอำนาจทำให้การปฏิบัติงานหยุดชะงักได้โดย ความเสี่ยงนี้อาจไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมถึงการที่ไม่ได้สำรองข้อมูลและระบบงานคอมพิวเตอร์และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้หากหน่วยงานไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบ คอมพิวเตอร์ที่รักรุมเพียงพอแล้ว (Access Risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถ เข้ามาทำให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์เสียหายได้

3.6.4 ฐานข้อมูล มีความเสี่ยงกับการที่หน่วยงานไม่ได้จัดให้มีการบริหารจัดการด้าน เทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี (Infrastructure Risk) รวมทั้งไม่ได้จัดให้มีระบบ คอมพิวเตอร์และบุคลากรที่เหมาะสมและเพียงพอแก่การสนับสนุนการทำงานของหน่วยงานโดยความ เสี่ยงนี้อาจเกิดจากการ แบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม รวมถึงไม่มีการจัดให้มีนโยบายเกี่ยวกับการ รักษาความปลอดภัยด้าน เทคโนโลยีสารสนเทศ ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือ เกิดจากการไม่มีแผนงานและ ขั้นตอนการปฏิบัติงานสำคัญทุกด้าน และการจัดให้มีการอบรมบุคลากรด้าน คอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรู้ความรุ้และเชี่ยวชาญในงานที่รับผิดชอบสำหรับการควบคุมการ ปฏิบัติงาน

3.6.5 ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรอง ข้อมูล (Back up) ที่สำคัญของศูนย์เทคโนโลยีสารสนเทศนั้นเพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการ ปฏิบัติในการบริหารจัดการในการเก็บข้อมูล(Back up) การกู้คืนข้อมูล (Recovery) ตลอดจนสถานีจัดเก็บ ข้อมูลที่เหมาะสมและปลอดภัย ดังนั้นการสำรองข้อมูลและการเตรียมข้อมูลให้ พร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) จึงมีวัตถุประสงค์เพื่อให้ข้อมูลและระบบ คอมพิวเตอร์สำหรับการใช้งานได้อย่าง ต่อเนื่อง มีประสิทธิภาพและในเวลาที่ต้องการ (Availability Risk) โดยที่เนื้อหาครอบคลุมเกี่ยวข้องกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์รวมทั้งการทดสอบ และการเก็บรักษา นอกจากนี้ยังมีเนื้อหา ครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

1) การกำหนดการสำรองข้อมูล (Back up)

2) การทดสอบ กำหนดทดสอบข้อมูลสำรองอย่างน้อยเดือนละ 1 ครั้ง เพื่อตรวจสอบได้ ว่าข้อมูล รวมทั้งโปรแกรมต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้

3) การเก็บรักษา ที่เจ้าหน้าที่จัดเก็บข้อมูลโดยตรง และมีการจัดเก็บข้อมูลสำรองไว้ใน สถานที่ที่ปลอดภัย และติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง

4) การกู้คืนข้อมูลสู่ระบบ มีกำหนดบุคลากรผู้ได้รับสิทธิ์กู้คืนข้อมูลที่ได้ทำการสำรองไว้ โดย Login ผ่าน Username & Password ที่กำหนดไว้

3.7 กระบวนการในการบริหารความเสี่ยงของระบบสารสนเทศ

ขั้นที่ 1 การระบุความเสี่ยงและผลกระทบที่มีผลกระทบต่อระบบข้อมูลสารสนเทศ

ขั้นที่ 2 ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยงและความรุนแรงของผลกระทบ โดย ผลกระทบจากผลการประเมินโอกาสความเสี่ยงที่จะเกิดขึ้นต่อระบบข้อมูลสารสนเทศ ผลกระทบของ ความเสี่ยงที่อาจเกิดขึ้นต่อระบบข้อมูลสารสนเทศ นั้นจะส่งผลกระทบตามมาสร้างความเสียหายต่อ ระบบข้อมูลสารสนเทศ สร้างความเสียหายต่อระบบในหลายๆด้าน ซึ่งแต่ละความเสี่ยงก็จะมี ความรุนแรง แตกต่างกันไป ทั้งนี้การควบคุม ความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุม ความเสี่ยงของแต่ละหน่วยงาน

ขั้นที่ 3 มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้ สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ใน การวางแผน จะต้องมี การกำหนดกลยุทธ์ ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมิน เอาไว้โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบของแต่ละหน่วยงานเป็นผู้ดูแลรักษาความมั่นคงปลอดภัย ของระบบและป้องกัน / แก้ไข / ควบคุมความเสี่ยงไม่ให้มีผลกระทบที่วางไว้โดยสามารถดำเนินการตาม แผนได้

ขั้นที่ 4 การติดตามข้อมูลเพื่อทราบร่องรอยของความเสี่ยงในขั้นตอนนี้เจ้าหน้าที่ ผู้รับผิดชอบจะต้องมีการรวบรวมและรายงานข้อมูลของความเสี่ยงได้ทั้งระยะยาวและข้อมูลที่เกี่ยวข้องเพื่อนำเสนอให้บังคับบัญชา ทราบและจะได้มีบันทึกไว้เป็นหลักบาน

ขั้นที่ 5 การติดตาม กำกับ และตรวจสอบ การปฏิบัติการควบคุมความเสี่ยง มีการตรวจสอบ การทำงานของเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรักษาความมั่นคงปลอดภัยของระบบโดยมีหลักฐาน ประกอบการปฏิบัติหน้าที่ตามระยะเวลาที่กำหนด

4. การประเมินความเสี่ยง (Risk assessment)

4.1 การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของกรมสามารถแยก ประเภทความเสี่ยงด้านเป็น 4 ประเภท ดังนี้

4.1.1 ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์เครื่องมือ และอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดีถูกก่อกวนจาก Hacker ถูกเจาะ ทำลายระบบ จาก Cracker เป็นต้น

4.1.2 ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดการ ความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบ สารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูล สารสนเทศได้

4.1.3 ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตาม ธรรมชาติ หรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

4.1.4 ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหาร จัดการที่ อาจส่งผลกระทบต่อการทำงานด้านสารสนเทศ

ลักษณะรายละเอียดความเสี่ยง (Description of risk) แสดงตามตาราง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง / สิ่งคุกคาม	ผลกระทบ / ผู้ที่ได้รับผลกระทบ
1. ความเสี่ยงในการเข้าถึงข้อมูลบุคคลอื่น	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าถึงระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอ้างสิทธิ์หรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล โดยไม่ได้รับอนุญาต และไม่มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือการไม่ได้ตั้งค่าการรักษาความปลอดภัยทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆ ที่ได้รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของโรงพยาบาลทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของโรงพยาบาล	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องแม่ข่ายคอมพิวเตอร์

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง / สิ่งคุกคาม	ผลกระทบ / ผู้ที่ได้รับผลกระทบ
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้อัตโนมัติ	<ul style="list-style-type: none"> - แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่ 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
4. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ใช้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูล คำสั่งเจตนาร้าย การดัดไวรัสหรือเวิร์ม	<ul style="list-style-type: none"> - แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services /DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส / เวิร์ม 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องแม่ข่ายคอมพิวเตอร์

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง / สิ่งคุกคาม	ผลกระทบ / ผู้ที่ได้รับผลกระทบ
5. ความเสี่ยงจากการขาดแคลนบุคลากร ผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบาย	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลง ทำให้การดำเนินการโครงการต่างๆ ได้รับความกระทบ	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องอาจมีประสิทธิภาพ		- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบฐานข้อมูล - ระบบสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง / สิ่งคุกคาม	ผลกระทบ / ผู้ที่ได้รับผลกระทบ
8. ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ความเสียหายจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	-ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง -ภัยธรรมชาติ	ผู้ใช้งาน -ผู้ดูแลระบบ -เครื่องคอมพิวเตอร์แม่ข่าย -อุปกรณ์เครือข่าย -ระบบฐานข้อมูล -ระบบสารสนเทศ
9. ความเสี่ยงจากสถานะการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสียหายจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือ ความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	-การชุมนุมประท้วง -การจลาจล -การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ
10. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์จัดซื้อไม่ สามารถทำงานได้ปกติ	ความเสียหายด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	-การลักทรัพย์	ผู้ใช้งาน -ผู้ดูแลระบบ -เครื่องคอมพิวเตอร์แม่ข่าย -อุปกรณ์เครือข่าย
11. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสียหายด้านการบริหารจัดการ/ความเสียหายจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือชิ้นส่วนภายในเครื่อง เช่น cpu และ ram ทำให้ไม่สามารถปฏิบัติงานหรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	-การลักทรัพย์	ผู้ใช้งาน -ผู้ดูแลระบบ -เครื่องคอมพิวเตอร์แม่ข่าย -อุปกรณ์เครือข่าย

4.2 การประมาณความเสี่ยง (Risk estimation) เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับ โอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง

5. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting) เมื่อประเมินความเสี่ยงแล้วเสร็จ จำเป็นต้องออกรายงานการประเมินเป็นเอกสารที่ผู้อื่นสามารถ อ่านได้เอกสารนี้จะเป็นสาระสำคัญในการสื่อสารให้บุคลากรทั้งองค์กรได้รับรู้รายงานประกอบด้วย รายละเอียดอย่างน้อยตามลักษณะรายละเอียดของความเสี่ยง และการออกรายงานมีวัตถุประสงค์ให้ส่วน ต่างๆได้รับรู้ดังต่อไปนี้

5.1 ฝ่ายบริหาร ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- รับรู้ภัยสำคัญของความเสี่ยงที่องค์กรเผชิญอยู่
- เข้าใจผลที่กระทบต่อผู้มีส่วนได้เสียต่างๆในกรณีที่เกิดมีเหตุ หรือเหตุการณ์และเกิดผล เสียต่อภารกิจ และผลประกอบการ
- ดำเนินการเพื่อสร้างความตระหนักในปัญหาความเสี่ยงให้เกิดการรับรู้ทั่วทั้งองค์กร
- เข้าใจผลกระทบที่อาจมีต่อความมั่นใจของผู้ที่ได้รับผลกระทบ
- ให้แน่ใจว่ากระบวนการบริหารความเสี่ยงกำลังเป็นไปอย่างได้ผล
- ออกนโยบายบริหารความเสี่ยงที่มีเนื้อหาด้านปรัชญาและความรับผิดชอบของหน่วยงาน และบุคลากรต่างๆในการบริหารความเสี่ยง

5.2 หัวหน้า ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้เช่น

- ตระหนักในความเสี่ยงอันเกี่ยวข้องกับภาระหน้าที่ของตน ผลกระทบที่อาจมีต่อ หน่วยงานอื่น หรือกิจกรรมอื่นในองค์กร ผลกระทบ มาก น้อย โอกาสที่จะเกิด มาก
- มีดัชนีชี้วัดสมรรถนะของกิจกรรมในหน่วยงานเพื่อดูว่าระบบงานของตนเองได้รับผลกระทบจากความเสียหายมากน้อยเพียงใด
- รายงานผลกระทบจากความเสี่ยงในกรณีเกิดหรือจะเกิดเหตุและเสนอแนะแนวทางการ แก้ไข
- รายงานความเสี่ยงใดๆที่เกิดขึ้นใหม่หรือความล้มเหลวใดๆ ในมาตรการการควบคุมหรือ ป้องกันอารักขาสารสนเทศที่มีอยู่

5.3 ผู้ปฏิบัติงาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้เช่น

- เข้าในบทบาทภาระหน้าที่และความรับผิดชอบในความเสี่ยงแต่ละรายการ
- เข้าใจบทบาทในการดำเนินการพัฒนาอย่างต่อเนื่องด้านการบริหารความเสี่ยง
- เข้าใจการบริหารความเสี่ยงและความตระหนักต่อความเสี่ยงในการเป็นวัฒนธรรมองค์กร ที่สำคัญอย่างหนึ่ง

6. กระบวนการบำบัดความเสี่ยง (Risk treatment) เมื่อผู้บริหารได้รับรายงานการประเมินความเสี่ยงแล้วจำเป็นต้องทำการตัดสินใจ โดยพิจารณา จากหลักเกณฑ์การยอมรับความเสี่ยงที่องค์กรมีอยู่ว่าจะยอมรับโดยไม่ทำอะไร หรือจะดำเนินการบำบัด ความเสี่ยง ซึ่งได้แก่กระบวนการดังต่อไปนี้

6.1 การยอมรับความเสี่ยง (acceptance) เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไร และ ยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ id/ password มีความเสี่ยงเพราะอาจมีการ ขโมยไปใช้ได้การ ให้มีใช้ชีวมาตร (biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า โรงพยาบาล อาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร

6.2 การเลี่ยงความเสี่ยง (avoidance) การหลีกเลี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบัน โรงพยาบาล มีการสำรองข้อมูลเพียง 1 ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจ ได้แก่การทำสำรองข้อมูล 2 ชุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่าย ผ่านโมเด็ม ถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กร อาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

6.3 การโอนย้ายความเสี่ยง (transfer) เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกัน เพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือ สัญญาการบำรุงรักษา หลังขาย (Maintenance service) เป็นต้น

6.4 การลดความเสี่ยง (reduction) ได้แก่การมีมาตรการควบคุมมากขึ้น หรือชนิดที่ เข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (biometrics) เพื่อใช้ในการพิสูจน์ตัวจริง นอกเหนือไปจากการใช้ id/ password ที่มีอยู่เดิม

7. การรายงานความเสี่ยงตกค้าง (Residual risk reporting) เมื่อมีการบำบัดความเสี่ยงแล้ว จำเป็นต้องมีการรายงานและทบทวนอยู่เสมอเพื่อดูว่ามีการ ประเมิน และการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่างๆที่ออกมาใช้ได้ผล หรือไม่เพียงไร วิธีการมาตรฐานที่ใช้กันโดยทั่วไป

คือการใช้หน่วยงานภายในหรือภายนอกทำการตรวจสอบ โดยกระบวนการ IT auditing ที่เหมาะสม เนื่องจากสิ่งแวดล้อมและกฎระเบียบมีพลวัตและการเปลี่ยนแปลงเกิดขึ้นตลอดเวลา จึงจำเป็นต้องมีการบริหารความเสี่ยงและการตรวจสอบเป็นประจำ

8. การเฝ้าสังเกต (Monitoring) กระบวนการเฝ้าสังเกตเป็นหลักประกันว่า องค์กรมีมาตรการต่างๆ ที่จำเป็นและเหมาะสมสำหรับ การบริหารความเสี่ยงต่างๆ และมาตรการเหล่านั้นมีผู้ปฏิบัติตามและบังเกิดผลจริง ดังนั้น กระบวนการ เฝ้าสังเกตพึงพิจารณาว่า

- 8.1 ได้มีการปฏิบัติตามมาตรการต่างๆและบังเกิดผล
- 8.2 กระบวนการที่กำหนดขึ้นมาสามารถปฏิบัติได้จริง
- 8.3 มีการเรียนรู้เกิดขึ้นในหน่วยงานอันเป็นผลมาจากการบริหารความเสี่ยง

บทสรุป การบริหารจัดการความเสี่ยง มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ขององค์กร และยังรวมถึงการปกป้อง “พันธกิจ” ขององค์กรให้รอดพ้นจาก ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้ อยู่ในความรับผิดชอบหลักของฝ่ายเทคนิค ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศเป็นผู้บริหาร และฝ่ายบริหารขององค์กร องค์กรจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการ สื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้ององค์กรจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อความสามารถในการดำเนินพันธกิจขององค์กรให้บรรลุผลสำเร็จ ไม่ใช่แค่เพียงการปกป้อง สินทรัพย์เทคโนโลยีสารสนเทศหรือองค์กรเพียงเท่านั้น