การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. ความหมายและความสำคัญของการจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน 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 สามารถสร้างความสมดุลของต้นทุนเชิงเศรษฐศาสตร์ และการดำเนินธุรกิจ ระหว่างมาตรการในการป้องกันและการบรรลุผลสำเร็จของพันธกิจ ด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

2.1 Access Risk : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานมิได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การมิได้มีการกำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การมิได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

2.2 **Integrity Risk :** เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

2.3 **Availability Risk :** เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิด

จากการมิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ หากหน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

2.4 Infrastructure Risk : เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานมิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินงาน และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

นอกจากความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารของหน่วยงานมิได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจ ดังนั้น หน่วยงานควรพิจารณาว่าข้อมูลใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของข้อมูล และจัดเตรียมข้อมูลดังกล่าวให้พร้อม เพื่อประโยชน์ในการดำเนินงานของหน่วยงาน

3. ความเสี่ยงและแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศขององค์กรสามารถแบ่งออกเป็น 4 ประเภท ดังนี้

3.1 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติสิ่งแวดล้อมที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น

- วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม
- กระแสไฟฟ้าขัดข้อง
- เพลิงไหม้
- การไม่มีระบบควบคุมการเข้า-ออก ห้องคอมพิวเตอร์แม่ข่าย (Server Room)

การบริหารจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม มีประเด็นหลัก ดังนี้

3.1.1 พิจารณาการตำแหน่งของห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารหลัก (Server Room & Network Equipment) ที่จะเป็นที่จัดเก็บและติดตั้งระบบเทคโนโลยีสารสนเทศไว้ยังเครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) และการกำหนดที่ตั้งระบบเทคโนโลยีสารสนเทศไว้ยังเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้า สายวงจร สายสัญญาณของระบบต่างๆ อย่างเน้นความปลอดภัยและหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่น เครื่องปรับอากาศ ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย หน้าต่างระบบความร้อนถังดับเพลิง เป็นต้น

3.1.2 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) โดยมีการจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงระบบสัญญาณเครือข่ายที่เชื่อมโยงไว้ในห้องคอมพิวเตอร์แม่ข่าย (Server Room) ของสำนักงาน ซึ่งในกรณีที่มีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำอำนาจมีความจำเป็นต้องเข้าห้องคอมพิวเตอร์แม่ข่ายในบางครั้ง จำเป็นต้องมีการควบคุมอย่างรัดกุมและรอบคอบ เช่น กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบควบคุมดูแลการทำงานตลอดเวลา การแจ้งให้งานเทคโนโลยีสารสนเทศทราบก่อนทุกครั้งและต้องเซ็นชื่อในสมุดบันทึกเข้าออกห้องสื่อสารทุกครั้ง เป็นต้น

3.1.3 จัดห้องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วนเฉพาะ โดยแบ่งออกเป็นสัดส่วน ดังนี้ ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (server zone) ส่วนคอมพิวเตอร์ลูกข่าย (client zone) และส่วนของระบบเครือข่าย (network zone) เพื่อความสะดวกในการปฏิบัติงาน และยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ต่างๆ มีประสิทธิภาพมากยิ่งขึ้น

3.1.4 การจัดแยกส่วนอุปกรณ์ที่จำเป็นในการเข้าถึงข้อมูลโดยเจ้าหน้าที่ของศูนย์ข้อมูล เช่น ส่วนที่ใช้เก็บรายงานต่างๆหรือข้อมูลที่งานเทคโนโลยีสารสนเทศของจังหวัดได้จัดทำการสำรองข้อมูล (Backup) ไว้กรณีฉุกเฉินเมื่อข้อมูลที่จัดทำไว้เกิดการเสียหาย โดยจัดเก็บไว้โดยเจ้าหน้าที่ของงานเทคโนโลยีสารสนเทศ กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร

3.1.5 การป้องกันความเสียหาย โดยการวางระบบป้องกันไฟที่เหมาะสม มีระบบตรวจจับควันไฟ จัดให้มีถังดับเพลิงที่พร้อมใช้งานได้ตลอดเวลากรณีฉุกเฉินเพื่อใช้ในการดับเพลิงเบื้องต้น

3.1.6 การป้องกันความเสี่ยงจากระบบป้องกันไฟฟ้าลัดวงจร ทำได้โดยมีระบบป้องกันไฟฟ้ากระชากไม่ให้คอมพิวเตอร์แม่ข่ายให้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้าท้องถิ่น อีกทั้งการติดตั้งระบบสายดิน (Ground) ที่ได้มาตรฐานอุปกรณ์ป้องกันไฟ จัดให้ระบบไฟฟ้าสำรองสำหรับคอมพิวเตอร์ทั้งแม่ข่ายและลูกข่าย เพื่อให้การดำเนินงานมีความต่อเนื่องกรณีท้องถิ่นดับหรือเกิดขัดข้องไม่สามารถใช้งานได้

3.1.7 การป้องกันความเสี่ยงจากระบบควบคุมอุณหภูมิและความชื้น ทำโดยให้มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยการตั้งอุณหภูมิเครื่องปรับอากาศและค่า

ความชื้นให้มีระดับเหมาะสมกับลักษณะ (specification) ของระบบคอมพิวเตอร์สิ่งแวดล้อมที่เหมาะสมที่คอมพิวเตอร์จะทำงานได้ดีนั้น อุณหภูมิและความชื้นจะต้องมีความชื้นจะต้องมีความเหมาะสมดังนั้นห้องทำงานด้านคอมพิวเตอร์จึงควรเป็นห้องปรับอากาศที่มีประสิทธิภาพ ปราศจากฝุ่นละอองและความชื้น เพราะเครื่องคอมพิวเตอร์และข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์อาจได้รับความเสียหายจากการได้รับความร้อนสูง ในส่วนของห้องคอมพิวเตอร์และข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์อาจได้รับความเสียหายจากการได้รับความร้อนสูง

3.1.8 ความเสี่ยงในเรื่องของงบประมาณที่จะดำเนินการอย่างได้ประสิทธิภาพสูงสุดและเกิดความต่อเนื่อง

3.1.9 ความเสี่ยงในเรื่องของประเด็นนโยบายของกระทรวงมหาดไทย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารที่ให้น้ำหนักและความสำคัญในเรื่องระบบเทคโนโลยีสารสนเทศ ซึ่งแนวนโยบายและวิสัยทัศน์ของแต่ละยุคสมัยเปลี่ยนแปลงไป อันส่งผลมายังหน่วยงานในแต่ละจังหวัดตลอดถึงแนวทางในการดำเนินงานในขั้นตอนต่อไป

3.1.10 ความเสี่ยงในเรื่องของการบริหารจัดการ สามารถวางแผนบริหารความเสียง และดำเนินการเพื่อความเสี่ยงได้ ดังนี้

- ศึกษาวิเคราะห์และจัดทำระบบข้อมูลเพื่อการบริหารราชการ ในการสนับสนุนการตัดสินใจของผู้บริหารระดับสูง (Executive Information System)
- ให้บริการฝึกอบรมเพื่อพัฒนาความรู้ด้านเทคโนโลยีสานสนเทศของบุคลากร

3.2 ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสานสนเทศของจังหวัดรวมถึงการวางแผนการตรวจสอบการทำงานการมอบหมายหน้าที่และสิทธิของบุคลากร / คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ตลอดจนบุคลากรภายนอกทีเกี่ยวข้องทั้งทางตรงและทางอ้อมล้วนแต่เป็นความเสี่ยง ความเสี่ยงด้านบุคลากรเป็นความเสี่ยงหนึ่งที่สำคัญ ดังนั้นจึงควรมีแนวทางและการวางแผนที่กำกับดูแลการบริหารจัดการและควบคุมความเสี่ยงบุคลากรของจังหวัดอย่างจริงจังการบริหารจัดการความเสี่ยงด้านบุคลากร มีประเด็นหลัก ดังนี้

3.2.1 กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศของจังวัด และการบริหารจัดการด้านบุคลากร การแต่งตั้งเจ้าหน้าที่ฯที่มีความเหมาะสม (มีความรู้ความสามารถและประสบการณ์ด้านคอมพิวเตอร์ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีด้านการรักษาความปลอดภัยระบบฯ และสามารถความรู้นั้น ให้แก่ผู้ใช้งานระบบฯของหน่วยงานได้อย่างมีประสิทธิภาพ) เมื่อมีการปรับและแจ้งรายชื่อผู้รับผิดชอบ เจ้าหน้าที่ที่รักษาความปลอดภัยระบบฯ และผู้ดูลแลระบบฯ) ที่มีการเปลี่ยนปลง เช่น โยกย้าย ลาออก ฯลฯ จะต้องแจ้งให้แก่ผู้บังคับบัญชาได้รับทราบ เพื่อประโยชน์ในการบริหารบุคลากร การติดต่อประสาน แจ้งเตือนภัย ฝึกอบรม และการรักษาความปลอดภัยระบบสารสนเทศ อย่างมี

ประสิทธิภาพ หากบุคลากรด้านเทคโนโลยีสารสนเทศไม่มีการจัดโครงสร้างและการบริหารจัดการที่ดีเพียงพอ ก็อาจทำให้เกิดความเสี่ยงด้านโครงสร้างการบริหารงานได้ การกำหนดโครงสร้าง การแบ่งแยกอำนาจหน้าที่ การกำหนดนโยบายและขั้นตอนการปฏิบัติงานและกำกับดูแลควบคุมการปฏิบัติงานเป็นหลัก

3.2.2 การว่าจ้าง / จัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อจัดทำโครงการด้านระบบเทคโนโลยีสารสนเทศภูมิศาสตร์ เพราะเป็นผู้มีความรู้ ความชำนาญเฉพาะทาง มีเครื่องมือและเทคโนโลยีที่ใช้พร้อมและทันต่อการพัฒนาระบบฐานข้อมูลสารสนเทศเฉพาะด้านมากกว่าภาคราชการ โดยการว่าจ้างบุคลากรภายนอกนี้ก็จะมีความเสี่ยงในเรื่องของ ความรู้ความเข้าใจในระบบราชการ และผลสัมฤทธิ์ที่เกิดจากการทำงาน อีกทั้งในแง่ของความคุ้มค่าของการใช้จ่ายงบประมาณ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงของการว่าจ้างบุคลากรภายนอกนี้ ทำได้โดย หน่วยงานที่เป็นเจ้าของเรื่อง หรือเป็นผู้รับผิดชอบในประเด็นต่างๆ ต้องเป็นผู้เข้ามากำกับดูแลตั้งแต่เริ่มกระบวนการ และต่อเนื่อง โดยหลักการบริหารจัดการที่ดี อีกทั้งรักษาผลประโยชน์ของทางราชการให้มากที่สุด

3.2.3 บุคลากรของภาคราชการ ขาดความรู้ความเข้าใจเรื่องของระบบเทคโนโลยีสารสนเทศโดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรม และนวัตกรรมใหม่ ทำให้เกิดช่องว่างในการที่จะประสานงานและรับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผกนบริหารความเสี่ยงในประเด็นนี้โดยการส่งเจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศ รวมถึงการรับบุคลากรที่มีความรู้ความเข้าใจด้านระบบเทคโนโลยีสารสนเทศมาปฏิบัติงานในหน่วยงานราชการมากยิ่งขึ้น

3.2.4 แผนการบริหารความเสี่ยงด้านบุคลากร คือ ต้องมีการฝึกอบรมในด้านที่เกี่ยวข้องกับระบบฐานข้อมูลสารสนเทศของจังหวัด สำหรับบุคลากรของส่วนราชการ ใน 2 ระดับ คือ ระดับผู้ดูแลระบบ (Administrator) และใช้งานทั่วไป (User) ทำให้บุคลากรของหน่วยงานสามารถใช้งานระบบสารสนเทศ ดูแล ปรับปรุง และพัฒนาระบบได้ เป็นการสนับสนุนบุคลากรทางคอมพิวเตอร์ รวมทั้งผู้ใช้งานให้มีความรู้ด้านการรักษาความปลอดภัยระบบ ได้อย่างมีประสิทธิภาพ

3.3 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ ไม่ว่าจะเป็นความเสี่ยงที่ที่เกิดจากทำงานผิดพลาดของอุปกรณ์ช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ ไวรัสคอมพิวเตอร์เป็นต้น

การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ มีประเด็นหลัก ดังนี้

3.3.1 ความเสี่ยงในเรื่องของจัดหาอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมกับแผนงาน / โครงการ และองค์กร (Planning and Organization) ซึ่งควรให้มีการจัดหาเครื่องคอมพิวเตอร์แลอุปกรณ์ต่างๆให้ได้ตามาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการ และเหมาะสมดับงบประมาณ

3.3.2 ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (Support) ซึ่งการลดโอกาสที่จะเกิดความเสี่ยงในกรณี ได้แก่

1) การบำรุงรักษาและลดความเสี่ยง

- มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และการดูแลอย่างถูกต้องและต่อเนื่อง
- ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว
- การใช้แผนซีดี หรือ Handy drive ควรตรวจสอบไวรัสก่อนทุกครั้ง
- ควรปัดฝุ่นหรือทำความสะอาดเครื่องคอมพิวเตอร์ให้ใหม่อยู่เสมอ เพราะเมื่อมีฝุ่นเข้าสู่เครื่องคอมพิวเตอร์มากๆ จะทำให้เครื่องคอมพิวเตอร์ร้อนจัดได้ง่าย เป็นสาเหตุของอาการเครื่องค้างหรือรวนได้
- โปรแกรม Windows จะมีคำสั่งในการบำรุงรักษาเครื่อง (Maintenance) ซึ่งผู้ดูแลระบบควรใช้คำสั่งนี้เป็นประจำ
- การติดตั้งไฟร์วอลล์ (Firewall) เพื่อป้องกันเบื้องต้นไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ
- การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ
- การฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงานเกี่ยวกับการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง และการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ เช่น การกำหนดรหัสผู้ใช้ และการใช้รหัสผ่าน
- การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ
- การสำรองข้อมูล (Backup) ข้อมูลระบบสารสนเทศ
- การบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ได้แก่ ระบบปฏิบัติการคอมพิวเตอร์ ระบบเครือข่าย และการใช้งานและประสิทธิผลของเครื่องคอมพิวเตอร์อุปกรณ์เทคโนโลยีสารสนเทศ

2) การรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่าย (Server)

- กำหนดขั้นตอนหรือวิธีการปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที
- ทำการทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ
- กำหนดบุคคลรับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนค่า Parameter ต่างๆ โปรแกรมคอมพิวเตอร์แม่ข่ายอย่างชัดเจน

3.4 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรมต่างๆ ที่ได้จัดทำแลพัฒนาขึ้นสำหรับโครงการด้านเทคโนโลยีสารสนเทศ รวมถึงโปรแกรมประยุกต์อื่นๆ ที่ใช้ประกอบการใช้โปรแกรมและระบบงาน ตัวอย่าง ตัวอย่างเช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่ง และการถูกไม่หวังดีทำลายระบบ (Hacker) เป็นต้น

การบริหารจัดการความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ มีประเด็นหลัก ดังนี้

3.4.1 มีการพัฒนามาตรฐานและการบริการโปรแกรมคอมพิวเตอร์

- พัฒนาและปรับปรุงมาตรฐาน Hardware Software People ware Data และ Network ให้เป็นฐานข้อมูลกลางของงานเทคโนโลยีสารสนเทศ และเป็นไปในทิศทางเดียวกัน

- สร้างกลไกการจัดการฐานข้อมูล การจัดระบบสารสนเทศเพื่อการบริหารจัดการของหน่วยงานให้ครบถ้วนและครอบคลุมมากยิ่งขึ้น

- พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลให้มีมาตรฐานและแบ่งสรรการให้ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้

- พัฒนาโปรแกรมให้สามารถจัดเก็บ รวบรวม ประมวลข้อมูล ศึกษาวิเคราะห์ เพื่อการนำเสนอและสนับสนุนการบริหารราชการ และพัฒนา ส่งเสริม บำรุงรักษาระบบ และการเผยแพร่ข้อมูลข่าวสารของจังหวัดได้ ในลักษณะของ Web Application เพื่อความสะดวกในการใช้งานและแสดงผล

3.5 ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่างๆที่เกิดขึ้นกับระบบเครือข่ายขององค์กรทั้งระบบอินทราเน็ต (Intranet) และอินเตอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้ายกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่างๆ การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีประเด็นหลัก ดังนี้

3.5.1 ความเสียหายที่เกิดขึ้นจากระบบเครือข่าย การเฝ้าระวังและตรวจสอบระบบเครือข่ายและการจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่าย ได้มีระบบการติดตามและเฝ้าดูแลการใช้เครือข่ายภายในและการเข้าออก Internet ทุกวัน รวมทั้งการสร้าง Firewall เพื่อป้องกันการเข้าถึงและการโจมตีจากภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย (Client) ในเครือข่ายระบบฐานข้อมูล ระบบ Web Server เป็นต้น

3.5.2 พัฒนาระบบงานด้านเครือข่าย โดยการพัฒนา บริหาร ควบคุม กำกับดูแลและบำรุงรักษาระบบเครื่องคอมพิวเตอร์และเครือข่ายสารสนเทศพื้นฐานของกระทรวงมหาดไทย ร่วมกับหน่วยงานอื่นๆ ที่เกี่ยวข้อง การเพิ่มการรักษาและคุ้มครองความปลอดภัยข้อมูลผ่านระบบเครือข่าย

3.5.3 เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ภายในให้มีความเสถียรและมีประสิทธิภาพรองรับกับปริมาณข้อมูล และการเคลื่อนไหวของฐานข้อมูล

3.5.4 หน่วยงานภายในสำนักงาน และผู้มีความรู้ต้องร่วมวิเคราะห์ ออกแบบ วางแผนการจัดการระบบโครงข่ายร่วมกันอย่างสมบูรณาการ และมีการให้คำปรึกษา แนะนำและแก้ไขปัญหาในการพัฒนาเครือข่าย

3.5.5 มีแผนการรักษาความปลอดภัยของระบบเครือข่าย (Network Security) มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (Integrity risk) ข้อมูล หรือการทำงานของระบบเครือข่ายที่จะมีผลถึงระบบเครือข่ายที่จะมีผลถึงระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง การป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสี่ยง (availability risk) แก้ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยเนื้อหารายละเอียดเกี่ยวกับแนวในการรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์เครื่องแม่ข่ายและระบบเครือข่าย

1) การบริหารจัดการข้อมูลบนเครือข่าย

- กำหนดชั้นความสำคัญในการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงการเข้าถึงข้อมูลผ่านเครือข่าย
- ในการรับส่งข้อมูลผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล
- กำหนดมาตรการรักษาความปลอดภัยข้อมูล เช่น กรณีนำเครื่องคอมพิวเตอร์ส่งซ่อม เป็นต้น

2) การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

- กำหนดสิทธิการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิในการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) ให้แก่ ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ
- กำหนดระยะเวลาการใช้งานของ User พร้อม Password และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างรอบคอบ และมีความลับ
- ในการที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นให้มีสิทธิในการใช้งานระบบคอมพิวเตอร์ เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่างๆ ต้องมีการอนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นรวมถึงกำหนดระยะเวลาในการใช้งาน

3) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

- กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากลโดยทั่วไปไม่ต่ำกว่า 6 ตัวอักษร

- ควรใช้อักขระพิเศษประกอบ เช่น @ ; < > เป็นต้น
- สำหรับผู้ใช้งานทั่วไปจะมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน ส่วนผู้ดูแลระบบควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 3 เดือน
- ในการเปลี่ยนรหัสผ่านแต่ละครั้งจะไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย
- ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่นผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

3.5.6 การบริหารจัดการและการตรวจรหัสผ่านใหม่โดยทันที

1) กำหนดแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายในส่วนเครือข่ายภายนอก

2) ติดตั้งระบบป้องกันการบุกรุก เช่น Firewall ระหว่างเครือข่ายในกับเครือข่ายนอก โดยการติดตั้งผ่านอุปกรณ์คอมพิวเตอร์ ติดตั้งระบบป้องกันการบุกรุกในระบบเครือข่ายด้วยซอฟต์แวร์และฮาร์ดแวร์ ให้แก่ ระบบ Firewall ซึ่งเป็นซอฟต์แวร์ทำหน้าที่เสมือนกับกำแพงกันไฟไม่ให้ลุกลามขยายตัวหาก มีไหม้เกิดขึ้น Firewall จะอาศัยคอมพิวเตอร์เครื่องหนึ่งเป็นด่านเข้าออกเครือข่ายและเป็นเสมือนกำแพงกันไฟ และมีซอฟต์แวร์ที่ดูแลระบบจะติดตั้งและกำหนดรูปแบบการอนุญาตให้เข้าใช้เครือข่ายอินเตอร์เน็ต

3) จัดทำแผนผังระบบเครือข่าย / แผนผังการเชื่อมโยงระบบเครือข่าย (Network Diagram) ซึ่งมีราละเอียดเกี่ยวกับขอบเขตของเครือข่ายทั้งในและภายนอกและอุปกรณ์ให้เป็นปัจจุบันอยู่เสมอ

4) ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส เป็นต้น

5) กำหนดบุคคลผู้รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของอุปกรณ์เครือข่าย

3.5.7 การป้องกันไวรัสสำหรับระบบเครือข่าย

1) กำหนดมาตรการป้องกันไวรัสที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมกต่อกับระบบเครือข่ายทุกเครื่อง เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น การปกป้องระบบเครือข่าย สิ่งที่สำคัญอย่างยิ่งคือ ผู้ใช้งานในระบบจะต้องคอยดูแล และป้องกันไม่ให้ตนเองเป็นช่องทางผ่านของ Hacker ผู้ดูแลระบบจะต้องคอยติดตามและหากหาวิธีการป้องกัน และแก้ไขจุดบกพร่องของซอฟต์แวร์ที่ใช้งาน เพราะไม่มีระบบเครือข่ายใดที่ปลอดภัยสมบูรณ์แบบ ดังนั้นต้องมีระบบป้องกันที่ดีโดยมีวิธีการดังนี้

- ติดตั้งโปรแกรมกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม
- สร้างแผ่น Emergency Disk เพื่อใช้ในการกู้ระบบ
- อะเดตข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัเดต
- เปิดใช้งาน Auto Protect
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ
- ใช่โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง

- การป้องกันจากการเปิดไฟล์จากบันทึกข้อมูลก่อนใช้งานทุกครั้ง
  - แผ่น CD เทปต่างๆ
  - สแกนหาไวรัสจากอื่นบันทึกก่อนใช้งานทุกครั้ง
  - ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif เป็นต้น
  - ไม่ใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา
- การป้องกันจากการเปิด E-Mail
  - อย่าเปิดไฟล์ E-Mail จากผู้ส่งที่ไม่รู้จัก และไม่ทราบที่มา
  - อย่าเปิดอ่าน E-Mail ที่มีหัวเรื่องเป็นข้อความไม่ปกติ
  - ลบ E-Mail ที่ไม่ทราบแหล่งที่มาทั้งทันที
  - อัพเดตโปรแกรม E-Mail สม่ำเสมอ
- การป้องกันจาการดาวน์โหลดจาก Internet
  - ไม่เปิดไฟล์ทีแนบมากับโปรแกรมสนทนาต่างๆ เช่น MSN
  - ไม่ควรเข้า Website ที่มากับ E-Mail
  - ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่มั่นใจหรือไม่เน่าเชื่อถือ
  - ติดตามข้อมูลการแจ้งเตือนจากแหล่งข้อมูลก้านความปลอดภัยเสมอ
  - หลีกเลี่ยงการแชร์ไฟล์ไม่จำเป็น
  - หลีกเลี่ยงการแชร์ไฟล์ประเภท Peer to Peer

3.6 ความเสี่ยงดด้านข้อมูล หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆในระบบสารสนเทศ อันอาจจะก่อให้เกิดความเสี่ยหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุก การโจรกรรมข้อมูลสำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ความเสี่ยงเหล่านี้ล้วนมีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความมั่นคงปลอดภัยของข้อมูลจึงเป็นเรื่องที่สำคัญ ข้อมูลสารสนเทศเป็นส่วนสำคัญสำหรับผู้บริหาร ที่จะนำความมั่นคงปลอดภัยของข้อมูลจึงเป็นเครื่องมือสำหรับการติดสินใจในการวางแผน การจัดการข้อมูล (Management of Data and Communication) ดังนั้น การรักษาความปลอดภัยของระบบข้อมูล และ Computer จากภัยต่างๆ ทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ จึงสำคัญ และจำเป็นต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี การรักษาความปลอดภัยด้านข้อมูลสารสนเทศ 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

5.6.1 ฐานข้อมูล มีความเสี่ยงกับการเข้าถึงข้อมูล (Access Risk)และระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องหรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งทางหน่วยงานไม่มีวิธีการจัดการและควบคุมความเสี่ยง (Access Risk) ที่รอบคอบและรัดกุมอาจทำให้บุคคลไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับข้อมูลและนำข้อมูลไปใช้ก่อให้เกิดความเสี่ยหายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่านกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น

3.6.2 ฐานข้อมูล มีความเสี่ยงเกี่ยงกับความเสี่ยงไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) และการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าทีเกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access Risk) ซึ่งส่งผลให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์อาจถูกแก้ไขเปลี่ยนแปลงได้ หรือสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ เพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประเมินผล และการแสดงผลมีความถูกต้องครบถ้วน

3.6.3 ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล(Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการซึ่งอำนาจทำให้การปฏิบัติงานหยุดชะงักได้โดยความเสี่ยงนี้อาจไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการที่ไม่ได้สำรองข้อมูลและระบบงานคอมพิวเตอร์และจัดให้มีแผลรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้หากหน่วยงานไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่รัดกุมเพียงพอแล้ว (Access Risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์เสียหายได้

3.6.4 ฐานข้อมูล มีความเสี่ยงกับการที่หน่วยงานไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบคบคุมภายในที่ดี (Infrastructure Risk) รวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการทำงานของหน่วยงานโดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม รวมถึงไม่มีการจัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานสำคัญทุกด้าน และการจัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรู้ความรู้และเชี่ยวชาญในงานที่รับผิดชอบสำหรับการควบคุมการปฏิบัติงาน

3.6.5 ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back up) ที่สำคัญของศูนย์เทคโนโลยีสารสนเทศ นั้นเพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูล(Back up) การกู้คืนข้อมูล (Recovery) ตลอดจนสถานีจัดเก็บข้อมูลที่เหมาะสมและปลอดภัย ดังนั้นการสำรองข้อมูลและการเตรียมข้อมูลให้พร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) จึงมีวัตถุประสงค์เพื่อให้ข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและในเวลาที่ต้องการ (Availability Risk) โดยทีเนื้อหาครอบคลุมเกี่ยวข้องกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

1) การกำหนดการสำรองข้อมูล (Back up)

2) การทดสอบ กำหนดทดสอบข้อมูลสำรองอย่างน้อยเดือนละ 1 ครั้ง เพื่อตรวจสอบได้ว่าข้อมูลรวมทั้งโปรแกรมต่างๆ ทีได้สำรองไว้ทีความถูกต้องครบถ้วนและใช้งานได้

3) การเก็บรักษา ทีเจ้าหน้าที่จัดเก็บข้อมูลโดยตรง และมีการจัดเก็บข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัย และติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง

4) การกู้คืนข้อมลสู่ระบบ มีกำหนดบุคลากรผู้ได้รับสิทธิ์กู้คืนข้อมูลที่ได้ทำการสำรองไว้โดย Login ผ่าน Username & Password ที่กำหนดไว้

3.7 กระบวนการในการบริหารความเสี่ยงของระบบสารสนเทศ

ขั้นที่ 1 การระบุความเสี่ยงและผลกระทบที่มีผลกระทบต่อระบบข้อมูลสารสนเทศ

ขั้นที่ 2 ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยงและความรุนแรงของผลกระทบ โดยผลกระทบจากผลการประเมินโอกาสความเสี่ยงที่จะเกิดขึ้นต่อระบบข้อมูลสารสนเทศ ผลกระทบของความเสี่ยงที่อาจจะเกิดขึ้นต่อระบบข้อมูลสานสนเทศ นั้นจะส่งผลกระทบตามมาสร้างความเสียหายต่อระบบข้อมูลสารสนเทศ สร้างความเสียหายต่อระบบในหลายๆด้าน ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน

ขั้นที่ 3 มีการวางแผนโดยกกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบของแต่ละหน่วยงานเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบและป้องกัน / แก้ไข / ควบคุมความเสี่ยงไม่ให้มีผลกระทบที่วางไว้ โดยสามารถดำเนินการตามแผนได้

ขั้นที่ 4 การติดตามข้อมูลเพื่อทราบร่องรอยของความเสี่ยงในขั้นตอนนี้ เจ้าหน้าที่ผู้รับผิดชอบจะต้องมีการรวบรวมและรายงานข้อมูลของความเสี่ยงได้ ทั้งระยะยาวและข้อมูลที่เกี่ยวข้องเพื่อนำเสนอให้ผู้บังคับบัญชาทราบและจะได้มีบันทึกไว้เป็นหลักบาน

ขั้นที่ 5 การติดตาม กำกับ และตรวจสอบ การปฏิบัติการควบคุมความเสี่ยง มีการตรวจสอบการทำงานของเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรักษาความมั่นคงปลอดภัยของระบบโดยมีหลักฐานประกอบการปฏิบัติหน้าที่ตามระยะเวลาที่กำหนด

4. การประเมินความเสี่ยง (Risk assessment)

4.1 การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของกรมสามารถแยกประเภทความเสี่ยงด้านเป็น 4 ประเภท ดังนี้

4.1.1 ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

4.1.2 ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

4.1.3 ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

4.1.4 ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตาราง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรม โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของกรม	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่แม่ข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
5. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบฐานข้อมูล - ระบบสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
8. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ
9. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	- ผู้ใช้งาน - ผู้ดูแลระบบ
10. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย
11. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย

4.2 การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

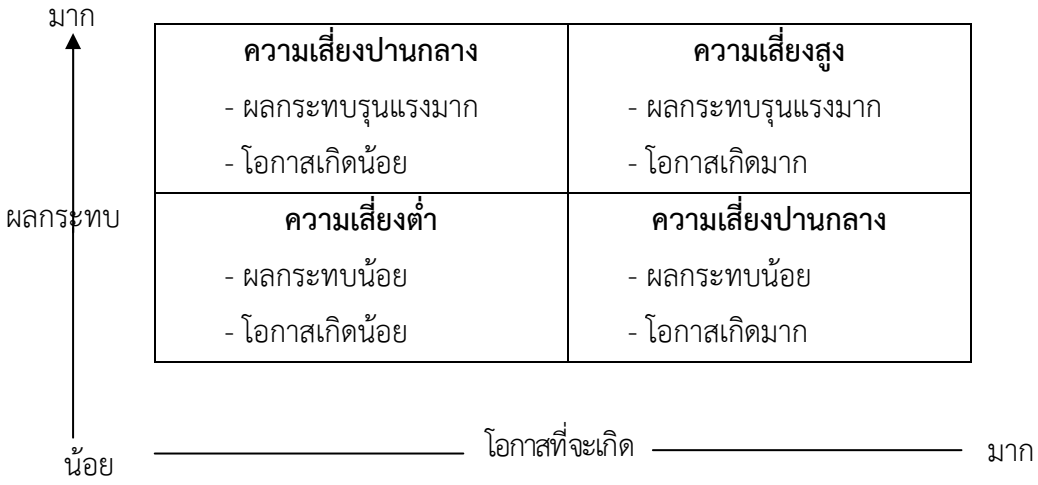
เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งกรมใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	5 ครั้ง/ปี
4	สูง	4 ครั้ง/ปี
3	ปานกลาง	3 ครั้ง/ ปี
2	น้อย	2 ครั้ง/ปี
1	น้อยมาก	ไม่เกิน 1 ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

4.3 แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง



5. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

เมื่อประเมินความเสี่ยงแล้วเสร็จ จำเป็นต้องออกรายงานการประเมินเป็นเอกสารที่ผู้อื่นสามารถอ่านได้เอกสารนี้จะเป็นสาระสำคัญในการสื่อสารให้บุคลากรทั้งองค์กรได้รับรู้ รายงานประกอบด้วยรายละเอียดอย่างน้อยตามลักษณะรายละเอียดของความเสี่ยง และการออกรายงานมีวัตถุประสงค์ให้ส่วนต่างๆได้รับรู้ดังต่อไปนี้

5.1 ฝ่ายบริหาร ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- รับรู้นัยสำคัญของความเสี่ยงที่องค์กรเผชิญอยู่
- เข้าใจผลที่กระทบต่อผู้มีส่วนได้เสียต่างๆในกรณีที่เกิดมีเหตุ หรือเหตุการณ์และเกิดผลเสียต่อภารกิจและผลประกอบการ
- ดำเนินการเพื่อสร้างความตระหนักในปัญหาความเสี่ยงให้เกิดการรับรู้ทั่วทั้งองค์กร
- เข้าใจผลกระทบที่อาจมีต่อความมั่นใจของผู้ที่ได้รับผลกระทบ
- ให้แน่ใจว่ากระบวนการบริหารความเสี่ยงกำลังเป็นไปอย่างได้ผล
- ออกนโยบายบริหารความเสี่ยงที่มีเนื้อหาด้านปรัชญาและความรับผิดชอบของหน่วยงานและบุคลากรต่างๆในการบริหารความเสี่ยง

5.2 หัวหน้างาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- ตระหนักในความเสี่ยงอันเกี่ยวข้องกับภาระหน้าที่ของตน ผลกระทบที่อาจมีต่อหน่วยงานอื่น หรือกิจกรรมอื่นในองค์กร

- มีดัชนีชี้วัดสมรรถนะของกิจกรรมในหน่วยงานเพื่อดูว่าระบบงานของตนเองได้รับผลกระทบจากความเสี่ยงมากน้อยเพียงใด
- รายงานผลกระทบจากความเสี่ยงในกรณีเกิดหรือจะเกิดเหตุและเสนอแนะแนวทางการแก้ไข
- รายงานความเสี่ยงใดๆที่เกิดใหม่หรือความล้มเหลวใดๆ ในมาตรการการควบคุมหรือป้องกันอารักขาสารสนเทศที่มีอยู่

5.3 ผู้ปฏิบัติงาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- เข้าในบทบาทภาระหน้าที่และความรับผิดชอบในความเสี่ยงแต่ละรายการ
- เข้าใจบทบาทในการดำเนินการพัฒนาอย่างต่อเนื่องด้านการบริหารความเสี่ยง
- เข้าใจการบริหารความเสี่ยงและความตระหนักต่อความเสี่ยงในการเป็นวัฒนธรรมองค์กรที่สำคัญอย่างหนึ่ง

6. กระบวนการบำบัดความเสี่ยง (Risk treatment)

เมื่อผู้บริหารได้รับรายงานการประเมินความเสี่ยงแล้วจำเป็นต้องทำการตัดสินใจ โดยพิจารณาจากหลักเกณฑ์การยอมรับความเสี่ยงที่องค์กรมีอยู่ว่าจะยอมรับโดยไม่ทำอะไร หรือจะดำเนินการบำบัดความเสี่ยง ซึ่งได้แก่กระบวนการดังต่อไปนี้

6.1 การยอมรับความเสี่ยง (acceptance) เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ id/ password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การให้มีใช้ชีวมาตร (biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า โรงพยาบาลอาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร

6.2 การเลี่ยงความเสี่ยง (avoidance) การหลีกเลี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบันโรงพยาบาล มีการสำรองข้อมูลเพียง 1 ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล 2 ชุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็ม ถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กรอาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

6.3 การโอนย้ายความเสี่ยง (transfer) เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังขาย (Maintenance service) เป็นต้น

6.4 การลดความเสี่ยง (reduction) ได้แก่การมีมาตรการควบคุมมากชนิดขึ้น หรือชนิดที่เข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (biometrics) เพื่อใช้ในการพิสูจน์ตัวจริงนอกเหนือไปจากการใช้ id/ password ที่มีอยู่เดิม

7. การรายงานความเสี่ยงตกค้าง (Residual risk reporting)

เมื่อมีการบำบัดความเสี่ยงแล้ว จำเป็นต้องมีการรายงานและทบทวนอยู่เสมอเพื่อดูว่ามีการประเมิน และการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่างๆที่ออกมาใช้ได้ผลหรือไม่เพียงไร วิธีการมาตรฐานที่ใช้กันโดยทั่วไป คือการมีหน่วยงานภายในหรือภายนอกทำการตรวจสอบโดยกระบวนการ IT auditing ที่เหมาะสม เนื่องจากสิ่งแวดล้อมและกฎระเบียบมีพลวัตรและการเปลี่ยนแปลงเกิดขึ้นตลอดเวลา จึงจำเป็นต้องมีการบริหารความเสี่ยงและการตรวจสอบเป็นประจำ

8. การเฝ้าสังเกต (Monitoring)

กระบวนการเฝ้าสังเกตเป็นหลักประกันว่า องค์กรมีมาตรการต่างๆ ที่จำเป็นและเหมาะสมสำหรับการบริหารความเสี่ยงต่างๆ และมาตรการเหล่านั้นมีผู้ปฏิบัติตามและบังเกิดผลจริง ดังนั้น กระบวนการเฝ้าสังเกตพึงพิจารณาว่า

8.1 ได้มีการปฏิบัติตามมาตรการต่างๆและบังเกิดผล

8.2 กระบวนงานที่กำหนดขึ้นมาสามารถปฏิบัติได้จริง

8.3 มีการเรียนรู้เกิดขึ้นในหน่วยงานอันเป็นผลมาจากการบริหารความเสี่ยง

บทสรุป

การบริหารจัดการความเสี่ยง มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ขององค์กร และยังรวมถึงการปกป้อง “พันธกิจ” ขององค์กรให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้อยู่ในความรับผิดชอบหลักของฝ่ายเทคนิค ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศเป็นผู้บริหารและฝ่ายบริหารขององค์กร

องค์กรจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องค์กรจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อความสามารถในการดำเนินพันธกิจขององค์กรให้บรรลุผลสำเร็จ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือองค์กรเพียงเท่านั้น