การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑. ความหมายและความสำคัญของการจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายใน สถานการณ์ที่ไม่แน่นอน ซึ่งมีโอกาสที่จะเกิดขึ้นในอนาคต และมีผลกระทบ ทั้งทางบวกและทางลบ หาก เป็นทางลบจะก่อให้เกิดความผิดพลาดความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึง ประสงค์ ทำให้การดำเนินงานขององค์กรไม่ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้และจะส่งผล กระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุของความเสี่ยง ที่จะทำให้ไม่บรรลุ วัตถุประสงค์ตามขั้นตอนการดำเนินงานที่กำหนดไว้ ทั้งปัจจัยภายในองค์กรเช่น โครงสร้างพื้นฐาน (Infrastructure) พนักงาน (Personnel) กระบวนการ(Process) เทคโนโลยี(Technology) และภายนอก องค์กร เช่น ภัยธรรมชาติ(Natural Environment) ภาวะเศรษฐกิจ(Economic) ภาวะการเมือง(Political) เทคโนโลยี(Technology) ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และ กำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และ ผลกระทบ(Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหาร จัดการ ให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์รวมทั้ง การกำหนดวิธีการในการบริหารและการควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้ ซึ่งการ จัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือการยอมรับ การลด/ควบคุม การยกเลิก และ การโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อ ลดความเสี่ยง โดยทำตามแนวทางการตอบสนองต่อความเสี่ยงที่วางไว้ ประกอบด้วยกิจกรรมการควบคุม เกิดขึ้นในทุกระดับ ทุกหน้าที่งานและทั่วทั้งองค์กร และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้

๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ค้นพบ การควบคุมแบบส่งเสริม และการควบคุม แบบแก้ไข

๒. ความเสี่ยงหลักด้านระบบเทคโนโลยีสารสนเทศ

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ กระบวนการการทำงานที่ ช่วยให้ IT Managers สามารถองค์กรดำเนินธุรกิจให้บรรลุผลสำเร็จของพันธกิจ และปกป้องระบบเทคโนโลยี สารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

๒.๑ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ (Access Risk) โดย บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูล และระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานมิได้มีวิธีการจัดการและควบคุม ความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบ คอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบ คอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบ คอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การมิได้มีการ กำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การมิได้จำกัดและ ควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

๒.๒ ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบ คอมพิวเตอร์ Integrity Risk ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงาน มิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่ รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูลรวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูก แก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ เพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่ รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

๒.๓ ความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการ Availability Risk ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิด จากการมิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวม ไปถึงการมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ หากหน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและ รัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

๒.๔ ความเสี่ยงเกี่ยวกับการที่หน่วยงานมิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยี สารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี Infrastructure Risk : รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ โดยความเสี่ยงนี้อาจเกิดจากการ แบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการ ปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการ

ปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินงาน และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และ เชี่ยวชาญในงานที่รับผิดชอบ

๓. แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศขององค์กรสามารถ แบ่งออกเป็น ๔ ประเภท ดังนี้

๓.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทาง ธรรมชาติสิ่งแวดล้อมที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบควบคุมการเข้า-ออก ห้องคอมพิวเตอร์ แม่ข่าย (Server Room)

การบริหารจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม มีประเด็นหลัก ดังนี้

- ตำแหน่งของห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารหลัก การเดินสายไฟฟ้า สายวงจร สายสัญญาณของระบบต่างๆ อย่างเน้นความปลอดภัยและหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยง รวมทั้ง มีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่นเครื่องปรับอากาศ ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์ แม่ข่าย ถังดับเพลิง เป็นต้น
- การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) ของห้องคอมพิวเตอร์แม่ข่าย (Server Room) ของสำนักงาน จำเป็นต้องมีการควบคุม เข้าได้เฉพาะ บุคคที่เกี่ยวข้องเท่านั้น ในกรณีที่มีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำอำนาจมีความจำเป็นต้องเข้าห้อง คอมพิวเตอร์แม่ข่ายในบางครั้ง จำเป็นต้องมีการควบคุมอย่างรัดกุมและรอบคอบ เช่น การแจ้งให้งาน เทคโนโลยีสารสนเทศทราบก่อนทุกครั้งและต้องเซ็นชื่อในสมุดบันทึกเข้าออกห้องสื่อสารทุกครั้ง เป็นต้น
- การป้องกันความเสียหาย โดยการวางระบบป้องกันไฟที่เหมาะสม จัดให้มีถังดับเพลิงที่ พร้อมใช้งานได้ตลอดเวลากรณีฉุกเฉินเพื่อใช้ในการดับเพลิงเบื้องต้น
- การป้องกันความเสี่ยงจากระบบป้องกันไฟฟ้าลัดวงจร ทำได้โดยมีระบบป้องกันไฟฟ้า กระชากไม่ให้คอมพิวเตอร์แม่ข่ายให้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า อุปกรณ์ป้องกันไฟ จัดให้ระบบไฟฟ้าสำรองสำหรับคอมพิวเตอร์ทั้งแม่ข่ายและลูกข่าย เพื่อให้การดำเนินงานมีความต่อเนื่องกรณี ท้องถิ่นดับหรือเกิดขัดข้องไม่สามารถใช้งานได้
- ความเสี่ยงในเรื่องของงบประมาณที่จะดำเนินการอย่างได้ประสิทธิภาพสูงสุดและเกิดความต่อเนื่อง
- ความเสี่ยงในเรื่องของประเด็นนโยบายผู้บริหาร ซึ่งแนวนโยบายและวิสัยทัศน์ของแต่ละยุคสมัยเปลี่ยนแปลงไปอันส่งผลมายังแนวทางในการดำเนินงาน

๓.๒ ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการ ดำเนินงานด้านเทคโนโลยีสารสนเทศรวมถึงการวางแผนการตรวจสอบการทำงานการมอบหมายหน้าที่และ สิทธิของบุคลากร / คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากร มีความรู้ความเข้าใจในการใช้งาน

การบริหารความเสี่ยงด้านบุคคลกร มีประเด็นหลัก ดังนี้

- กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการด้านบุคลากร การแต่งตั้งเจ้าหน้าที่ที่มีความเหมาะสม การกำหนดโครงสร้าง การแบ่งแยกอำนาจหน้าที่ การ กำหนด นโยบายและขั้นตอนการปฏิบัติงานและกำกับดูแลควบคุมการปฏิบัติงานเป็นหลัก
- การว่าจ้าง / จัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อจัดทำโครงการด้านระบบ เทคโนโลยีสารสนเทศ เพราะเป็นผู้มีความรู้ ความชำนาญเฉพาะทาง มีเครื่องมือและเทคโนโลยีที่ใช้พร้อมและ ทันต่อการพัฒนาระบบฐานข้อมูลสารสนเทศเฉพาะด้านมากกว่าภาคราชการ โดยการว่าจ้างบุคลากรภายนอกนี้ ก็จะมีความเสี่ยงในเรื่องของ ความรู้ความเข้าใจในระบบราชการ และผลสัมฤทธิ์ที่เกิดจากการทำงาน อีกทั้งใน แง่ของความคุ้มค่าของการใช้จ่ายงบประมาณ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงของการว่าจ้าง บุคลากรภายนอกนี้ทำได้โดย หน่วยงานที่เป็นเจ้าของเรื่อง หรือเป็นผู้รับผิดชอบในประเด็นต่างๆ ต้องเป็นผู้เข้า มากำกับดูแลตั้งแต่เริ่มกระบวนการ และต่อเนื่อง โดยหลักการบริหารจัดการที่ดี อีกทั้งรักษาผลประโยชน์ของ ทางราชการให้มากที่สุด
- บุคลากรของภาคราชการ ขาดความรู้ความเข้าใจเรื่องของระบบเทคโนโลยีสารสนเทศ โดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรม และนวัตกรรมใหม่ ทำให้เกิดช่องว่างในการที่จะประสานงานและ รับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงในประเด็นนี้โดยการส่ง เจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศ รวมถึงการรับบุคลากรที่มีความรู้ ความเข้าใจด้าน ระบบเทคโนโลยีสารสนเทศมาปฏิบัติงานมากยิ่งขึ้น
- แผนการบริหารความเสี่ยงด้านบุคลากร คือ ต้องมีการฝึกอบรมในด้านที่เกี่ยวข้องกับระบบ ใน ๓ ระดับ คือ ระดับผู้บริหาร(CIO) ระดับผู้ดูแลระบบ (Administrator) และใช้งานทั่วไป (User) ทำให้ บุคลากรของหน่วยงานสามารถใช้งานวางแผนงานระบบสารสนเทศ ดูแล ปรับปรุง และพัฒนาระบบได้ เป็น การสนับสนุนบุคลากรทางคอมพิวเตอร์ รวมทั้งผู้ใช้งานให้มีความรู้ด้านการรักษาความปลอดภัยระบบ ได้อย่าง มีประสิทธิภาพ

๓.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความ ผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ ไม่ว่าจะเป็นความเสี่ยงที่เกิดจากทำงานผิดพลาดของ อุปกรณ์ช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ ไวรัสคอมพิวเตอร์ เป็นต้น

การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ มีประเด็นหลัก ดังนี้

- ความเสี่ยงในเรื่องของจัดหาอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมกับแผนงาน / โครงการ และองค์กร ซึ่งควรให้มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆให้ได้ตามมาตรฐานของ อุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมตามลักษณะของโครงการ และ งบประมาณ

- ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (Support) โดยมีข้อควรปฏิบัติ ได้แก่

- มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และการดูแลอย่างถูกต้องและต่อเนื่อง

- ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว

- การใช้อุปกรณ์ต่อพ่วง เช่น Flash Drive ควรตรวจสอบไวรัสก่อนทุกครั้ง

- ควรปัดฝุ่นหรือทำความสะอาดเครื่องคอมพิวเตอร์อยู่เสมอ เพราะเมื่อมีฝุ่นเข้าสู่เครื่อง คอมพิวเตอร์มากๆ จะทำให้เครื่องคอมพิวเตอร์ร้อนจัดได้ง่าย เป็นสาเหตุของอาการเครื่องค้างหรือรวนได้

- ระบบปฏิบัติการ Windows ควรทำการ Update เป็นประจำ

- การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ

- การฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงานเกี่ยวกับการ ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง และการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ เช่น การ กำหนดรหัสผู้ใช้ และการใช้รหัสผ่าน

- การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ

- การสำรองข้อมูล (Backup) ข้อมูลระบบสารสนเทศ

- การบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ได้แก่ ระบบปฏิบัติการ คอมพิวเตอร์ ระบบเครือข่าย และการใช้งานและประสิทธิผลของเครื่องคอมพิวเตอร์อุปกรณ์เทคโนโลยี สารสนเทศ

- กำหนดขั้นตอนหรือวิธีการปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของ คอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

- ทำการทดสอบ Software เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งาน

อย่างสม่ำเสมอ

- กำหนดบุคคลรับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนค่า Parameter ต่างๆ ของ ระบบคอมพิวเตอร์แม่ข่ายอย่างชัดเจน

๓.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงาน โปรแกรมต่างๆ ที่ได้จัดทำและพัฒนาขึ้นสำหรับโครงการด้านเทคโนโลยีสารสนเทศ รวมถึงโปรแกรมประยุกต์ อื่นๆ ที่ใช้ประกอบการใช้โปรแกรมและระบบงาน ตัวอย่างเช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความ ผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่ง และการถูกไม่หวังดีทำลายระบบ (Hacker) เป็นต้น

การบริหารจัดการความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ มีประเด็นหลัก ดังนี้

- มีการพัฒนามาตรฐานและการบริการโปรแกรมคอมพิวเตอร์พัฒนาและปรับปรุงมาตรฐาน Hardware Software, Peopleware Data และNetwork ให้เป็นฐานข้อมูลกลางของงานเทคโนโลยี สารสนเทศ และเป็นไปในทิศทางเดียวกัน
- พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลให้มีมาตรฐานและแบ่งสรรการให้ ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้

๓.๕ ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่างๆ ที่เกิดขึ้นกับระบบ เครือข่ายขององค์กรทั้งระบบอินทราเน็ต (Intranet) และอินเตอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุ มาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้ายกายภาพ ความเสี่ยงด้าน ระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัย คุกคามต่าง ๆ

การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีประเด็นหลัก ดังนี้

- ความเสียหายที่เกิดขึ้นจากระบบเครือข่าย การเฝ้าระวังและตรวจสอบระบบเครือข่ายและ การจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่าย ได้มีระบบการติดตามและเฝ้าดูแลการใช้เครือข่าย ภายในและการเข้าออก Internet ทุกวัน รวมทั้งการสร้าง Firewall เพื่อป้องกันการเข้าถึงและการโจมตีจาก ภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย (Client) ในเครือข่ายระบบฐานข้อมูลระบบ Web Server เป็นต้น
- เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ภายในให้มีความเสถียรและ มีประสิทธิภาพรองรับกับปริมาณข้อมูล และการเคลื่อนไหวของฐานข้อมูล
- มีแผนการรักษาความปลอดภัยของระบบเครือข่าย (Network Security) มีวัตถุประสงค์ เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง(Integrity risk) ข้อมูล หรือการทำงานของระบบเครือข่ายที่จะมีผลถึงระบบเครือข่ายที่จะมีผลถึงระบบคอมพิวเตอร์ในส่วนที่ มิได้มีอำนาจหน้าที่เกี่ยวข้อง การป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส มิ ให้เข้าถึงหรือสร้างความเสี่ยง(availability risk) แก้ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์
- กำหนดมาตรการรักษาความปลอดภัยข้อมูล เช่น กรณีนำเครื่องคอมพิวเตอร์ส่งซ่อม
- กำหนดชั้นความสำคัญในการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการ เข้าถึงผ่านระบบงาน รวมถึงการเข้าถึงข้อมูลผ่านเครือข่ายในการรับส่งข้อมูลผ่านเครือข่ายสาธารณะต้องได้รับ การเข้ารหัสที่เป็นมาตรฐานสากล
- การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)เช่น สิทธิในการใช้ โปรแกรมระบบงานคอมพิวเตอร์ (Application System) ให้แก่ ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ
- กำหนดระยะเวลาการใช้งานของ User พร้อม Password และระงับการใช้งานทันทีเมื่อ พ้นระยะเวลาดังกล่าว
- กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างรอบคอบ และมีความลับ

- ในการที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นให้มีสิทธิในการใช้งานระบบคอมพิวเตอร์ เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่างๆ ต้องมีการอนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง โดยบันทึก เหตุผลและความจำเป็นรวมถึงกำหนดระยะเวลาในการใช้งาน
- ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

- กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากลโดยทั่วไปไม่ต่ำกว่า ๖ ตัวอักษร

- ควรใช้อักขระพิเศษประกอบ เช่น @ ; < > เป็นต้น

- สำหรับผู้ใช้งานทั่วไปจะมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน ส่วนผู้ดูแลระบบ ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๓ เดือน

- ในการเปลี่ยนรหัสผ่านแต่ละครั้งจะไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

- ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคล อื่นผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

- กำหนดแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก
- ติดตั้งระบบป้องกันการบุกรุก เช่น Firewall ระหว่างเครือข่ายในกับเครือข่ายนอกโดยการ ติดตั้งผ่านอุปกรณ์คอมพิวเตอร์ ติดตั้งระบบป้องกันการบุกรุกในระบบเครือข่ายด้วยซอฟต์แวร์และฮาร์ดแวร์ ให้แก่ และมีซอฟต์แวร์ที่ดูแลระบบจะติดตั้งและกำหนดรูปแบบการอนุญาตให้เข้าใช้เครือข่ายอินเตอร์เน็ต
- จัดทำแผนผังระบบเครือข่าย / แผนผังการเชื่อมโยงระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายทั้งในและภายนอกและอุปกรณ์ให้เป็นปัจจุบันอยู่เสมอ
- ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส เป็นต้น
- กำหนดบุคคลผู้รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของ
- อุปกรณ์เครือข่าย

- กำหนดมาตรการป้องกันไวรัสที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่อง คอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัสเป็น ต้น การ ปกป้องระบบเครือข่าย สิ่งที่สำคัญอย่างยิ่งคือ ผู้ใช้งานในระบบจะต้องคอยดูแล และป้องกันไม่ให้ตนเองเป็น ช่องทางผ่านของ Hacker ผู้ดูแลระบบจะต้องคอยติดตามและหากหาวิธีการป้องกัน และแก้ไขจุดบกพร่องของ ซอฟต์แวร์ที่ใช้งาน เพราะไม่มีระบบเครือข่ายใดที่ปลอดภัยสมบูรณ์แบบ ดังนั้นต้องมีระบบป้องกันที่ดีโดยมี วิธีการดังนี้

- ติดตั้งโปรแกรมกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม

- สร้างแผ่น Emergency Disk เพื่อใช้ในการกู้ระบบ

- อัพเดทข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัพเดท

- เปิดใช้งาน Auto Protect

- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

การป้องกันจากการเปิดไฟล์จากบันทึกข้อมูลก่อนใช้งานทุกครั้ง

- แผ่น CD เทปต่างๆ

- สแกนหาไวรัสจากอื่นบันทึกก่อนใช้งานทุกครั้ง

- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif , .exe เป็นต้น

- ไม่ใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

การป้องกันจากการเปิด E-Mail

- อย่าเปิดไฟล์ E-Mail จากผู้ส่งที่ไม่รู้จัก และไม่ทราบที่มา

- อย่าเปิดอ่าน E-Mail ที่มีหัวเรื่องเป็นข้อความไม่ปกติ

- ลบ E-Mail ที่ไม่ทราบแหล่งที่มาทั้งทันที

- อัพเดทโปรแกรม E-Mail สม่ำเสมอ

การป้องกันจาการดาวน์โหลดจาก Internet

- ไม่เปิดไฟล์ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น MSN

- ไม่ควรเข้า Website ที่มากับ E-Mail

- ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่มั่นใจหรือไม่น่าเชื่อถือ

- ติดตามข้อมูลการแจ้งเตือนจากแหล่งข้อมูลด้านความปลอดภัยเสมอ

- หลีกเลี่ยงการแชร์ไฟล์ไม่จำเป็น

- หลีกเลี่ยงการแชร์ไฟล์ประเภท Peer to Peer

๓.๖ ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบ สารสนเทศอันอาจจะก่อให้เกิดความเสี่ยหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุก การโจรกรรมข้อมูลสำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล

การบริหารจัดการความเสี่ยงด้านข้อมูล มีประเด็นหลัก ดังนี้

- ฐานข้อมูล มีความเสี่ยงกับการเข้าถึงข้อมูล (Access Risk) และระบบคอมพิวเตอร์ใน ส่วนที่เกี่ยวข้องหรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบ คอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งทางหน่วยงานไม่มีวิธีการจัดการและควบคุมความ เสี่ยง (Access Risk) ที่รอบคอบและรัดกุมอาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับข้อมูลและนำข้อมูลไปใช้ ก่อให้เกิดความเสียหายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ก็อาจถูกแก้ไขเปลี่ยนแปลงได้
- ฐานข้อมูล มีความเสี่ยงเกี่ยวกับความเสี่ยงไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) และการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่ หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ที่รอบคอบและรัดกุมเพียงพอ (Access Risk) ซึ่งส่งผลให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์อาจถูก แก้ไขเปลี่ยนแปลงได้ หรือสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ
- ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบ คอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้โดยความเสี่ยงนี้ อาจไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวม ไปถึงการที่ไม่ได้สำรองข้อมูลและระบบงานคอมพิวเตอร์และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ หากไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่รัดกุมเพียงพอแล้ว (Access Risk) ก็อาจ ส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์ เสียหายได้
- ฐานข้อมูล มีความเสี่ยงกับการที่หน่วยงานไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยี สารสนเทศที่สะท้อนระบบคบคุมภายในที่ดี (Infrastructure Risk) รวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์และ บุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการทำงานของหน่วยงาน รวมถึงไม่มีการจัดให้มีนโยบาย เกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานสำคัญทุกด้าน และการจัดให้มีการอบรมบุคลากรดานคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรู้ความรู้และเชี่ยวชาญในงานที่รับผิดชอบสำหรับการควบคุมการปฏิบัติงาน
- ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back up)ที่สำคัญของศูนย์เทคโนโลยีสารสนเทศ นั้นเพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการ ปฏิบัติในการบริหารจัดการในการเก็บข้อมูล (Back up) การกู้คืนข้อมูล (Recovery) ตลอดจนสถานที่จัดเก็บข้อมูลที่เหมาะสมและปลอดภัย ดังนั้นการสำรองข้อมูลและการเตรียมข้อมูลให้พร้อมกรณีฉุกเฉิน จึงมี วัตถุประสงค์เพื่อให้ข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและในเวลา ที่ต้องการ (Availability Risk) โดยที่เนื้อหาครอบคลุมเกี่ยวข้องกับแนวทางการสำรองข้อมูลและระบบ คอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการ ทดสอบแผนฉุกเฉิน

- การกำหนดการสำรองข้อมูล (Back up)

- การทดสอบ กำหนดทดสอบข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบได้ว่า ข้อมูลรวมทั้งโปรแกรมต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้การเก็บรักษาที่เจ้าหน้าที่จัดเก็บ ข้อมูลโดยตรง และมีการจัดเก็บข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัย และติดฉลากที่มีรายละเอียดชัดเจนไว้บน สื่อบันทึกข้อมูลสำรอง

- การกู้คืนข้อมูลสู่ระบบ มีกำหนดบุคลากรผู้ได้รับสิทธิ์กู้คืนข้อมูลที่ได้ทำการสำรองไว้โดย

Login ผ่าน Username & Password ที่กำหนดไว้

๓.๗ ระบวนการในการบริหารความเสี่ยงของระบบสารสนเทศ

ขั้นที่ ๑ การระบุความเสี่ยงและผลกระทบที่มีผลกระทบต่อระบบข้อมูลสารสนเทศ

ขั้นที่ ๒ ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยงและความรุนแรงของผลกระทบซึ่งแต่ละ ความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับ มาตรการควบคุมความเสี่ยง

ขั้นที่ ๓ มีการวางแผนโดยกำหนดมาตรการกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่

อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบของ แต่ละหน่วยงานเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบและป้องกัน / แก้ไข / ควบคุมความเสี่ยงไม่ให้มี ผลกระทบที่วางไว้

ขั้นที่ ๔ การติดตามข้อมูลเพื่อทราบร่องรอยของความเสี่ยงในขั้นตอนนี้ เจ้าหน้าที่รับผิดชอบ

จะต้องมีการรวบรวมและรายงานข้อมูลของความเสี่ยงได้ ทั้งระยะยาวและข้อมูลที่เกี่ยวข้องเพื่อนำเสนอให้ ผู้บังคับบัญชาทราบและจะได้มีบันทึกไว้เป็นหลักฐาน

ขั้นที่ ๕ การติดตาม กำกับ และตรวจสอบ การปฏิบัติการควบคุมความเสี่ยง มีการตรวจสอบ

การทำงานของเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรักษาความมั่นคงปลอดภัยของระบบโดยมีหลักฐาน ประกอบการปฏิบัติหน้าที่ตามระยะเวลาที่กำหนด

๔. การประเมินความเสี่ยง (Risk assessment)

๔.๑ การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศสามารถแยก ประเภทความเสี่ยงด้านเป็น ๔ ประเภท ดังนี้

๔.๑.๑ ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะ ทำลายระบบจาก Hacker เป็นต้น

๔.๑.๒ ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการจัด

ความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศ ได้

๔.๑.๓ ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัย

พิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้า ขัดข้องน้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔.๑.๔ ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการ

บริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

๔.๒ การประเมินความเสี่ยง (Risk Estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใดเกณฑ์การประมาณ เป็น การกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรง ของผลกระทบ และระดับความเสี่ยง ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ		
ระดับ	โอกาส	คำอธิบาย
๕	สูงมาก	๕ ครั้ง/ปี
๔	สูง	๔ ครั้ง/ปี
๓	ปานกลาง	๓ ครั้ง/ปี
๒	น้อย	๒ ครั้ง/ปี
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความ เสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลต่าง ๆ
๔	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผล ต่อความถูกต้องของข้อมูล บางส่วน
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

๔.๓ แผนภูมิความเสี่ยง (Risk Map)

ความเสี่ยงปานกลาง	**ความเสี่ยงสูง**
-ผลกระทบรุนแรงมาก -โอกาสเกิดน้อย	-ผลกระทบรุนแรงมาก -โอกาสเกิดมาก
ความเสี่ยงต่ำ	**ความเสี่ยงปานกลาง**
-ผลกระทบน้อย -โอกาสเกิดน้อย	-ผลกระทบน้อย -โอกาสเกิดมาก

๕. วิธีการจัดการความเสี่ยง (Risk treatment)

การกำหนดวิธีการจัดการความเสี่ยง เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์ การจัดการความเสี่ยงอย่างใดอย่างหนึ่งผสมผสานกันดังต่อไป

๕.๑ Take – การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับให้มีความเสี่ยง เนื่องจาก ค่าใช้จ่ายในการจัดการหรือสร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้ แต่ก็ควรมีมาตรการติดตามและ ดูแล เช่น การกำหนดระดับของผลกระทบที่ยอมรับได้ เตรียมแผนการตั้งรับ/จัดการความเสี่ยง เป็นต้น

๕.๒ Treat – การลด/ควบคุมความเสี่ยง (Risk Reduction/Control) การออกแบบระบบ ควบคุม การแก้ไขปรับปรุงการทำงาน เพื่อป้องกันหรือจำกัดผลกระทบ และโอกาสเกิดความเสียหาย เช่น ติดตั้งอุปกรณ์ความปลอดภัย ฝึกอบรมเพื่อพัฒนาทักษะวางมาตรการเชิงรุก เป็นต้น

๕.๓ Terminate – การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การหยุดหรือเปลี่ยนแปลง กิจกรรมที่เป็นความเสี่ยง เช่น งดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบการ ทำงาน ลดขอบเขตการดำเนินการ เป็นต้น

๕.๔ Transfer – การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading) การกระจายทรัพย์สินหรือกระบวนการต่าง ๆ เพื่อลดความเสี่ยงจากการสูญเสีย เช่น การประกันทรัพย์สิน เพื่อโอนความเสี่ยงไปยังบริษัทประกัน การจ้างบริษัทภายนอกให้ทำงานบางส่วนแทน การทำสำเนาเอกสารหลายๆ ชุด การ กระจายที่เก็บทรัพย์สินมีค่า เป็นต้น

๖. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

เมื่อประเมินความเสี่ยงแล้วเสร็จ จำเป็นต้องออกรายงานการประเมินเป็นเอกสารที่ผู้อื่น สามารถอ่านได้เอกสารนี้จะเป็นสาระสำคัญในการสื่อสารให้บุคลากรทั้งองค์กรได้รับรู้ รายงานประกอบด้วย รายละเอียดอย่างน้อยตามลักษณะรายละเอียดของความเสี่ยง และการออกรายงานมีวัตถุประสงค์ให้ส่วนต่างๆ ได้รับรู้ดังต่อไปนี้

๖.๑ ฝ่ายบริหาร ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- รับรู้ความเสี่ยงที่องค์กรเผชิญอยู่
- เข้าใจผลที่กระทบต่อผู้มีส่วนได้เสียต่างๆในกรณีที่เกิดมีเหตุ หรือเหตุการณ์และเกิดผล เสียต่อภารกิจและผลประกอบการ
- ดำเนินการเพื่อสร้างความตระหนักในปัญหาความเสี่ยงให้เกิดการรับรู้ทั่วทั้งองค์กร
- เข้าใจผลกระทบที่อาจมีต่อความมั่นใจของผู้ที่ได้รับผลกระทบ
- ให้แน่ใจว่ากระบวนการบริหารความเสี่ยงกำลังเป็นไปอย่างได้ผล
- ออกนโยบายบริหารความเสี่ยงและความรับผิดชอบของหน่วยงานและบุคลากรต่างๆ ในการบริหารความเสี่ยง

๖.๒ หัวหน้างาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- ตระหนักในความเสี่ยงอันเกี่ยวข้องกับภาระหน้าที่ของตน ผลกระทบที่อาจมีต่อ หน่วยงานอื่น หรือกิจกรรมอื่นในองค์กร
- มีดัชนีชี้วัดสมรรถนะของกิจกรรมในหน่วยงานเพื่อดูว่าระบบงานของตนเองได้รับ ผลกระทบจากความเสี่ยงมากน้อยเพียงใด
- รายงานผลกระทบจากความเสี่ยงในกรณีเกิดหรือจะเกิดเหตุและเสนอแนะแนวทางการแก้ไข
- รายงานความเสี่ยงใดๆที่เกิดใหม่หรือความล้มเหลวใดๆ ในมาตรการการควบคุมหรือป้องกันอารักขาสารสนเทศที่มีอยู่

๖.๓ ผู้ปฏิบัติงาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

- เข้าในบทบาทภาระหน้าที่และความรับผิดชอบในความเสี่ยงแต่ละรายการ
- เข้าใจบทบาทในการดำเนินการพัฒนาอย่างต่อเนื่องด้านการบริหารความเสี่ยง

- เข้าใจการบริหารความเสี่ยงและความตระหนักต่อความเสี่ยงในการเป็นวัฒนธรรม องค์กรที่สำคัญอย่างหนึ่ง

๗. การรายงานความเสี่ยงตกค้าง (Residual risk reporting)

เมื่อมีการบำบัดความเสี่ยงแล้ว จำเป็นต้องมีการรายงานและทบทวนอยู่เสมอเพื่อดูว่ามีการ ประเมิน และการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่างๆที่ออกมาใช้ได้ผลหรือไม่ เพียงไร วิธีการมาตรฐานที่ใช้กันโดยทั่วไป คือการมีหน่วยงานภายในหรือภายนอกทำการตรวจสอบ โดย กระบวนการ IT auditing ที่เหมาะสม เนื่องจากสิ่งแวดล้อมและกฎระเบียบ มีการเปลี่ยนแปลงเกิดขึ้น ตลอดเวลา จึงเป็นต้องมีการบริหารความเสี่ยงและการตรวจสอบเป็นประจำ

๘. บทสรุป

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นการบริหารเพื่อให้การดำเนินงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีการพัฒนาและใช้งานได้อย่างต่อเนื่อง เพื่อสนับสนุนภารกิจของ หน่วยงานภายในองค์กร ช่วยป้องกันหรือลดเหตุการณ์ที่จะทำให้เกิดความเสียหายต่อระบบเทคโนโลยี สารสนเทศและการสื่อสารให้อยู่ในระดับที่สามารถยอมรับ ควบคุม และตรวจสอบได้อย่างมีระบบ ซึ่งการ บริหารจัดการนอกจากผู้ปฏิบัติงานโดยตรงจะต้องรับทราบแล้ว ผู้บริหารควรได้รับทราบถึงความเสี่ยงในด้าน ต่างๆ เพื่อนำไปจัดการและวางแผนการบริหาร ให้องค์กรดำเนินงานได้อย่างต่อเนื่องต่อไป