



รายงานการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ของ สำนักงานนโยบายและแผนการขนส่งและจราจร
กระทรวงคมนาคม

ประจำปีงบประมาณ พ.ศ. 2569



โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร



รายงานการประเมินความเสี่ยง
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

สารบัญ

เรื่อง	หน้า
บทที่ ๑ บทนำ	๑
๑.๑ หลักการและเหตุผล	๑
๑.๒ วัตถุประสงค์	๑
๑.๓ เป้าหมาย	๑
๑.๔ ขอบเขตการดำเนินงาน	๑
๑.๕ ประโยชน์ที่คาดว่าจะได้รับ	๒
บทที่ ๒ การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ	๓
๒.๑ คำนิยาม	๓
๒.๒ คำนิยามความเสี่ยง	๓
๒.๓ หลักการบริหารจัดการความเสี่ยง	๔
๒.๔ หลักการวิเคราะห์ ประเมิน การจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Tread way Commission)	๖
๒.๕ การประเมินความเสี่ยง (Risk Assessment)	๘
๒.๖ กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)	๙
๒.๗ กิจกรรมการบริหารความเสี่ยง (Control Activities)	๙
๒.๘ ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)	๑๐
๒.๙ การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)	๑๐
๒.๑๐ ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๑
๒.๑๑ การตอบสนองความเสี่ยง	๑๒
๒.๑๒ ปัจจัยความเสี่ยงของ สนข.	๑๓
๒.๑๓ การประเมินความเสี่ยงหาย	๑๓
๒.๑๔ การติดตามและรายงาน	๑๓
๒.๑๕ ระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของ สนข.	๑๓
บทที่ ๓ การวิเคราะห์การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๕
๓.๑ ขั้นตอนการดำเนินการบริหารความเสี่ยง	๑๕
๓.๒ กระบวนการจัดทำแผนบริหารจัดการความเสี่ยง	๑๖
๓.๓ การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๖
๓.๔ การประเมินระดับความเสี่ยงและแนวทางในการบริหารจัดการความเสี่ยง	๒๙
๓.๕ การจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	๓๕
บทที่ ๔ สรุปผลและข้อเสนอแนะ	๓๖
๔.๑ วัตถุประสงค์	๓๖
๔.๒ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ	๓๖
๔.๓ ข้อเสนอแนะ	๓๗

เอกสารอ้างอิง

บทที่ ๑ บทนำ

๑.๑ หลักการและเหตุผล

สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) กระทรวงคมนาคม ตั้งขึ้นตามพระราชบัญญัติปรับปรุง กระทรวง ทบวง กรม พ.ศ. ๒๕๔๕ และพระราชกฤษฎีกาการโอนกิจการบริหารและอำนาจหน้าที่ของส่วนราชการ ให้เป็นไปตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. ๒๕๔๕ มีพันธกิจและภารกิจเกี่ยวกับการเสนอแนะนโยบาย มาตรา มาตรฐานและจัดทำแผนหลัก แผนแม่บท และยุทธศาสตร์การพัฒนา ระบบการขนส่งและจราจร ศึกษา วิจัย พัฒนางานคมนาคม รวมทั้งการส่งเสริมความปลอดภัยและสิ่งแวดล้อมในระบบคมนาคมและการขนส่งของประเทศ โดยในปัจจุบันได้นำเทคโนโลยีสารสนเทศมาใช้ เพื่อสนับสนุนการบริหารจัดการภายในหน่วยงาน การบูรณาการข้อมูลระหว่างหน่วยงาน และระบบสารสนเทศเพื่อให้บริการประชาชน รวมถึงการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้สามารถรองรับภารกิจต่าง ๆ ของหน่วยงาน และด้วยความก้าวหน้าทางเทคโนโลยีที่เพิ่มขึ้นอย่างรวดเร็ว ส่งผลให้ภัยคุกคามทางไซเบอร์เพิ่มขึ้น สำนักงานนโยบายและแผนการขนส่งและจราจรอาจเผชิญกับภัยและความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบให้การดำเนินภารกิจต้องหยุดชะงัก หรือเกิดความเสียหายแก่ข้อมูลสำคัญทางราชการ ดังนั้น เพื่อเป็นแนวทางป้องกันปัญหา และเป็นการเฝ้าระวังภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ สนข. จึงได้จัดทำแผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ขึ้น เพื่อเป็นแนวทางในการดำเนินงานของหน่วยงาน

๑.๒ วัตถุประสงค์

เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีผลต่อระบบเทคโนโลยีสารสนเทศของ สนข. ให้มั่นใจได้ว่าความเสี่ยงของระบบสารสนเทศของ สนข. ได้ถูกพิจารณา และได้มีการจัดเตรียมมาตรการในการควบคุมความเสี่ยงที่เหมาะสม เพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ สนข. ได้

๑.๓ เป้าหมาย

๑.๓.๑ ผู้บริหารและผู้ปฏิบัติงานมีความรู้ความเข้าใจในเรื่องการบริหารความเสี่ยง เพื่อนำไปใช้ดำเนินงานตามยุทธศาสตร์ และแผนการปฏิบัติงานประจำปีให้บรรลุตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๑.๓.๒ บุคลากรผู้ปฏิบัติงาน สามารถระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความเสี่ยง และจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๑.๓.๓ สามารถนำแผนบริหารความเสี่ยงไปใช้ในการบริหารงานที่รับผิดชอบ

๑.๓.๔ เพื่อพัฒนาความสามารถของบุคลากรและกระบวนการดำเนินงานภายใน สนข. อย่างต่อเนื่อง

๑.๓.๕ สร้างความรับผิดชอบต่อความเสี่ยงและการบริหารความเสี่ยงถูกกำหนดขึ้นอย่างเหมาะสมครอบคลุม

๑.๔ ขอบเขตการดำเนินงาน

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ได้แก่ ด้านโครงสร้างพื้นฐาน ด้านระบบสารสนเทศ และด้านฐานข้อมูลของ สนข.

๑.๕ ประโยชน์ที่คาดว่าจะได้รับ

- ๑.๕.๑ มีแนวปฏิบัติในการดำเนินงาน ติดตาม และประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ๑.๕.๒ สามารถกำหนดแผนงาน/โครงการ ในอนาคตที่สอดคล้องกับแนวทางการป้องกันความเสี่ยง
- ๑.๕.๓ สามารถลดความเสียหายที่อาจเกิดขึ้นกับโครงสร้างพื้นฐาน ระบบสารสนเทศ และฐานข้อมูลได้
- ๑.๕.๔ สามารถช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้น
- ๑.๕.๕ สามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้ สนข. เกิดความเสียหาย
- ๑.๕.๖ สร้างวัฒนธรรมการตระหนักถึงความเสี่ยงภายในหน่วยงาน

บทที่ ๒

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๑ คำนิยาม

เทคโนโลยีสารสนเทศ หมายถึง ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบงานสารสนเทศ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ อินเทอร์เน็ต อุปกรณ์โทรคมนาคม ระบบงานบริการอิเล็กทรอนิกส์ และระบบงานที่ใช้คอมพิวเตอร์

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) เรียกว่า “การประเมินความเสี่ยง (Risk Assessment)” เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงระดับหน่วยงาน โดยการประเมินความเสี่ยงหน่วยงานจะสามารถ :

- ระบุเหตุการณ์ “สิ่งนี้อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจากการกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ที่ไม่พึงประสงค์
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมการตระหนักถึงความเสี่ยงภายในหน่วยงาน การประเมินความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้บุคลากรมีส่วนร่วมคิดเกี่ยวกับกระบวนการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ของ สนข.

๒.๒ คำนิยามความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและที่ไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว ลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงินและการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ลักษณะของความเสี่ยง สามารถแบ่งออกได้เป็น ๓ ส่วน ดังนี้

- ๑) ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง
- ๒) เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงาน หรือนโยบาย
- ๓) ผลกระทบของความเสี่ยง คือ ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุ วัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้ว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยงการวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูงปานกลาง และต่ำ

การวิเคราะห์ความเสี่ยง หลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นตอนต่อไปคือการวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสียหายต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธีเนื่องจากการวัดความเสี่ยงเป็นตัวเลขว่ามีผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก โดยทั่วไปจะวิเคราะห์ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสียหาย และความถี่ที่จะเกิดหรือโอกาสที่จะเกิดความเสี่ยง

การบริหารความเสี่ยง หมายถึง การบริหารปัจจัยและควบคุมกิจกรรมรวมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดเหตุจากโอกาสที่จะทำให้เกิดความเสียหายจากการดำเนินงานไม่เป็นไปตามแผนเพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายของหน่วยงานเป็นสำคัญ

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนการปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อป้องกัน การควบคุมเพื่อให้ตรวจสอบการควบคุมโดยการชี้แนะและการควบคุมเพื่อการแก้ไข

ทรัพย์สิน (Asset) หมายถึง ทรัพย์สินต่าง ๆ ขององค์กรแบ่งเป็น ๕ หมวด ได้แก่ หมวดข้อมูล หมวดบุคลากร หมวดฮาร์ดแวร์ หมวดซอฟต์แวร์ และหมวดบริการ

๒.๓ หลักการบริหารจัดการความเสี่ยง

๒.๓.๑ การระบุความเสี่ยงหรือปัจจัยความเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องของโครงการหรือกิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายในและภายนอกองค์กร วิธีการระบุความเสี่ยงมีหลายวิธี เช่น

๒.๓.๑.๑ การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๒.๓.๑.๒ การทำ Checklist

๒.๓.๑.๓ การวิเคราะห์สถานการณ์จากการตั้งคำถามสมมุติ What-if

๒.๓.๑.๔ การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

ในขั้นตอนนี้ มีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปแบบของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินงานใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จและปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๒.๓.๒ การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมินและการจัดระดับความเสี่ยงประกอบด้วย ๔ ขั้นตอน คือ

๒.๓.๒.๑ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) ซึ่งต้องกำหนดเกณฑ์ อาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยง อาจกำหนดเป็นเกณฑ์ ๕ ระดับ ได้แก่ สูงมาก (รุนแรงมากที่สุด) สูง (ค่อนข้างรุนแรง) ปานกลาง น้อย และน้อยมาก ส่วนระดับของความเสี่ยงอาจกำหนดเป็น ๔ ระดับ ได้แก่ สูงมาก สูง ปานกลาง และต่ำ

๒.๓.๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยที่ระบุไว้มาประกอบโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรง หรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงจะมีความรุนแรงที่แตกต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาส ของความเสี่ยงที่จะเกิดขึ้น

ตัวอย่างเกณฑ์การประเมินผลกระทบ (ความน่าเชื่อถือ/ความพึงพอใจของผู้ใช้บริการ) ดังนี้

ตารางที่ ๒-๑ ตัวอย่างเกณฑ์การประเมินผลกระทบ

ผลกระทบ ที่จะเกิด	ความเสียหายที่เกิดขึ้น		ระดับ คะแนน
	เชิงคุณภาพ	เชิงปริมาณ	
สูงมาก	มีการสูญเสียทรัพย์สินอย่างมาก ผู้บริหารถูกลงโทษทางวินัย	มูลค่ามากกว่า สิบล้านบาท	๕
สูง	มีการสูญเสียทรัพย์สินอย่างมาก ผู้บริหารถูกตำหนิหรือถูกร้องเรียน	มูลค่าห้าล้านบาท ถึง สิบล้านบาท	๔
ปานกลาง	มีการสูญเสียทรัพย์สินมาก เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย	มูลค่าหนึ่งล้านบาท ถึง ห้าล้านบาท	๓
ต่ำ	มีการสูญเสียทรัพย์สินพอสมควร เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ	มูลค่าห้าแสนบาท ถึง หนึ่งล้านบาท	๒
ต่ำมาก	มีการสูญเสียทรัพย์สินเล็กน้อย แทบไม่มีผลกระทบเลย	มูลค่าน้อยกว่า ห้าแสนบาท	๑

ตัวอย่างเกณฑ์การประเมินโอกาสของการประเมินความเสี่ยง ดังนี้

ตารางที่ ๒-๒ ตารางตัวอย่างเกณฑ์การประเมินโอกาสของการประเมินความเสี่ยง

โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้นของความเสี่ยง	ระดับคะแนน
	เชิงปริมาณ	
สูงมาก	มากกว่า ๔ ครั้งต่อปี	๕
สูง	๔ ครั้งต่อปี	๔
ปานกลาง	๓ ครั้งต่อปี	๓
น้อย	๒ ครั้งต่อปี	๒
น้อยมาก	ไม่เกิน ๑ ครั้งต่อปี	๑

๒.๓.๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยงต้องคร่าวๆจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูง ที่จะต้องบริหารจัดการความเสี่ยงก่อน

ตารางที่ ๒-๓ ตารางแสดงระดับการประเมินความเสี่ยง

ระดับความเสี่ยง	ระดับสี	คำอธิบาย	คะแนน
สูงมาก	แดง	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้โดยทันที	๑๕ - ๒๕
สูง	ส้ม	ระดับที่ไม่สามารถยอมรับได้ โดยจำเป็นต้องติดตามความเสี่ยง อย่างใกล้ชิด เพื่อให้ความเสี่ยงลดลงและป้องกันไม่ไห้ ความเสี่ยงไปอยู่ในระดับสูงมาก	๘ - ๑๔
ปานกลาง	เขียว	ระดับที่พอยอมรับได้ แต่ต้องการมีการควบคุมเพื่อป้องกัน ไม่ไห้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	๔ - ๗
ต่ำ	ฟ้า	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง หรือไม่ต้องมีการจัดการเพิ่มเติม	๑ - ๓

การประเมินความเสี่ยง

ผลกระทบ	๕	๑๐	๑๕	๒๐	๒๕
	๔	๘	๑๒	๑๖	๒๐
	๓	๖	๙	๑๒	๑๕
	๒	๔	๖	๘	๑๐
	๑	๒	๓	๔	๕
โอกาสที่จะเกิด					

รูปที่ ๒-๑ แผนผังค่าความเสี่ยงแต่ละระดับ (Risk Matrix)

๒.๓.๒.๔ การจัดลำดับความเสี่ยงเป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้แล้ว เลือกความเสี่ยงที่มีระดับสูงมากหรือสูงมาจัดทำแผนการบริหารความเสี่ยง

๒.๔ หลักการวิเคราะห์ ประเมิน การจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยง ตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Tread way Commission) มีดังนี้

๒.๔.๑ การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

เป็นการกำหนดวัตถุประสงค์ของการดำเนินการบริหารจัดการความเสี่ยง ซึ่งจะต้องสอดคล้องกับ วิสัยทัศน์ พันธกิจ และยุทธศาสตร์การดำเนินงานขององค์กร ตั้งแต่ระดับองค์กร หน่วยงาน กิจกรรมจนถึงระดับ บุคคล เพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าประสงค์ และเพื่อเพิ่มประสิทธิภาพในการตัดสินใจ โดยคำนึงถึง ปัจจัยเสี่ยงและความเสี่ยงในด้านเทคโนโลยีสารสนเทศของ สนข. ที่น่าจะส่งผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบายโดยพิจารณาหาแนวทางในการป้องกัน หรือจัดการกับความเสี่ยงเหล่านั้นก่อนที่จะเริ่ม ปฏิบัติงาน หรือดำเนินกิจการตามแผนที่กำหนดไว้สำหรับวัตถุประสงค์ของการบริหารความเสี่ยง อาจแบ่งออก ได้เป็น ๒ ระดับ คือ

๑) วัตถุประสงค์ระดับองค์กร (Corporate Objective) เป็นวัตถุประสงค์ของการดำเนินงาน ในภาพรวม ตามแผนยุทธศาสตร์และแผนปฏิบัติราชการประจำปีขององค์กร

๒) วัตถุประสงค์ระดับกิจกรรม (Activities Objective) เป็นวัตถุประสงค์ของการดำเนินงาน ที่เฉพาะเจาะจงลงไป สำหรับแต่ละกิจกรรมที่องค์กรกำหนดเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การกำหนดวัตถุประสงค์ที่ชัดเจนช่วยให้การระบุและวิเคราะห์ความเสี่ยงที่เกิดขึ้นได้อย่างครบถ้วน ซึ่งวัตถุประสงค์ที่กำหนดขึ้นในแต่ละระดับ ควรมีการกำหนดเป้าหมายและตัวชี้วัดความสำเร็จและสามารถ วัดผลได้วัตถุประสงค์ที่ดี (SMART) ควรมีลักษณะ ดังนี้

S	: Specific	หมายถึง	มีการกำหนดเป้าหมายที่ชัดเจน
M	: Measurable	หมายถึง	สามารถวัดผลหรือประเมินผลได้
A	: Achievable	หมายถึง	สามารถปฏิบัติให้บรรลุผลได้
R	: Reasonable	หมายถึง	สมเหตุผล มีความเป็นไปได้
T	: Time Constrained	หมายถึง	มีกรอบเวลาที่ชัดเจนและเหมาะสม

๒.๔.๒ การระบุความเสี่ยงต่าง ๆ (Event Identification)

นอกจากการกำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศตามแนวทางของ COSO ออกเป็น ๘ ประเภทแล้ว การระบุความเสี่ยงยังต้องนำหลักธรรมาภิบาลมาเป็นปัจจัยในการวิเคราะห์ และระบุความเสี่ยง เพื่อให้เป็นไปตามแนวทางการบริหารกิจการบ้านเมืองที่ดี ประกอบด้วย ๑๐ ประการ ดังนี้

๑) หลักประสิทธิผล (Effectiveness) หมายถึง ผลการปฏิบัติราชการที่บรรลุวัตถุประสงค์ และเป้าหมายของแผนปฏิบัติราชการที่ได้รับงบประมาณมาดำเนินการ โดยการปฏิบัติราชการจะต้องมีทิศทาง ยุทธศาสตร์ และเป้าประสงค์ที่ชัดเจน มีกระบวนการปฏิบัติงานและระบบงานที่เป็นมาตรฐาน รวมถึงการติดตาม ประเมินผล และพัฒนาปรับปรุงอย่างต่อเนื่องและเป็นระบบ

๒) หลักประสิทธิภาพ (Efficiency) หมายถึง การบริหารราชการตามแนวทางการกำกับดูแลที่ดี มีการออกแบบกระบวนการปฏิบัติงานโดยใช้เทคนิคและเครื่องมือการบริหารจัดการที่เหมาะสม ให้องค์กรสามารถใช้ทรัพยากรทั้งด้านต้นทุน แรงงาน และระยะเวลาให้เกิดประโยชน์สูงสุดต่อการพัฒนาขีดความสามารถในการปฏิบัติราชการตามภารกิจ เพื่อตอบสนองความต้องการของประชาชน และผู้มีส่วนได้ส่วนเสียทุกกลุ่ม

๓) หลักการตอบสนอง (Responsiveness) หมายถึง การให้บริการที่สามารถดำเนินการได้ ภายในระยะเวลาที่กำหนดและสร้างความเชื่อมั่น ความไว้วางใจ รวมถึง ตอบสนองตามความคาดหวัง/ความต้องการของประชาชนผู้รับบริการ และผู้มีส่วนได้ส่วนเสียที่มีความหลากหลายและมีความแตกต่าง

๔) หลักการรับผิดชอบ (Accountability) หมายถึง การแสดงความรับผิดชอบในการปฏิบัติหน้าที่ และผลงานต่อเป้าหมายที่กำหนดไว้ โดยความรับผิดชอบนั้นควรอยู่ในระดับที่สนองต่อความคาดหวังของสาธารณะ รวมทั้งการแสดงถึงความสำนึกในการรับผิดชอบต่อปัญหาสาธารณะ

๕) หลักความโปร่งใส (Transparency) หมายถึง กระบวนการเปิดเผยอย่างตรงไปตรงมา ชี้แจงได้เมื่อมีข้อสงสัย และสามารถเข้าถึงข้อมูลข่าวสารอันไม่ต้องห้ามตามกฎหมายได้อย่างเสรีโดยประชาชนสามารถรู้ทุกขั้นตอนในการดำเนินกิจกรรม หรือกระบวนการต่าง ๆ และสามารถตรวจสอบได้

๖) หลักการมีส่วนร่วม (Participation) หมายถึง กระบวนการที่ข้าราชการ ประชาชน และผู้มีส่วนได้ส่วนเสียทุกกลุ่มมีโอกาสได้เข้าร่วมรับรู้ เรียนรู้ หาความเข้าใจ ร่วมแสดงทักษะ ร่วมเสนอปัญหา/ประเด็น ที่สำคัญที่เกี่ยวข้อง ร่วมคิดแนวทาง ร่วมการแก้ไขปัญหา ร่วมในกระบวนการตัดสินใจ และร่วมกระบวนการพัฒนาในฐานะหุ้นส่วนพัฒนา

๗) หลักการกระจายอำนาจ (Decentralization) หมายถึง การถ่ายโอนอำนาจการตัดสินใจ การมอบอำนาจและความรับผิดชอบในการตัดสินใจ และการดำเนินการให้แก่บุคลากร โดยมุ่งเน้นการสร้าง ความพึงพอใจในการให้บริการต่อผู้รับบริการและผู้มีส่วนได้ส่วนเสีย การปรับปรุงกระบวนการเพิ่มผลิตภาพ เพื่อผลการดำเนินงานที่ดีของส่วนราชการ

๘) หลักนิติธรรม (Rule of Law) หมายถึง การใช้อำนาจของกฎหมาย กฎระเบียบข้อบังคับ ในการบริหารราชการด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของผู้มีส่วนได้ส่วนเสีย

๙) หลักความเสมอภาค (Equity) หมายถึง การได้รับการปฏิบัติ และได้รับการอย่างเท่าเทียมกัน โดยไม่มีการแบ่งแยกด้านชาย/หญิง ถิ่นกำเนิด เชื้อชาติ ภาษา เพศ อายุ ความพิการ สภาพทางกาย หรือสุขภาพ สถานะบุคคล ฐานะทางเศรษฐกิจและสังคม ความเชื่อทางศาสนา การศึกษา และอื่น ๆ

๑๐) หลักมุ่งเน้นฉันทามติ (Consensus Oriented) หมายถึง การหาข้อตกลงทั่วไปภายในกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ซึ่งเป็นข้อตกลงที่เกิดจากการใช้กระบวนการ เพื่อหาข้อคิดเห็นจากกลุ่มบุคคล ที่รับประโยชน์และเสียประโยชน์ โดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง ซึ่งต้องไม่มีข้อคัดค้านที่ยุติไม่ได้ ในประเด็นที่สำคัญ โดยฉันทามติไม่จำเป็นต้องหมายความว่าเห็นพ้องโดยเอกฉันท์

๒.๕ การประเมินความเสี่ยง (Risk Assessment)

เป็นขั้นตอนในการใช้หลักเกณฑ์การให้คะแนนจากระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) มาเป็นเครื่องมือในการประเมินความเสี่ยง และกำหนดกลยุทธ์ที่ใช้จัดการกับความเสี่ยง โดย สนข. แบ่งการจัดระดับความเสี่ยง (Degree of Risk) ออกเป็น ๕ ระดับตามระดับคะแนน ได้แก่ ระดับความเสี่ยงต่ำ ระดับความเสี่ยงปานกลาง ระดับความเสี่ยงสูง และระดับความเสี่ยงสูงมาก ซึ่งการจัดทำแผนผังระดับความเสี่ยง (Risk Matrix) จะช่วยในการตัดสินใจในการวางแผนความเสี่ยงได้อย่างเหมาะสม และสามารถจัดลำดับความสำคัญในการจัดการได้ ซึ่งการประเมินความเสี่ยงด้วยวิธีการแบ่งการจัดระดับความเสี่ยงมีขั้นตอนดังนี้

๑) การประเมินโอกาสที่จะเกิดความเสียหาย (Likelihood : L) เป็นขั้นตอนการประเมินความเป็นไปได้ ความถี่ หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง แล้วจัดแบ่งระดับของโอกาสที่เกิดความเสี่ยง (Likelihood) ออกเป็น ๕ ระดับ ตามตารางที่ ๒-๔

ตารางที่ ๒-๔ ตารางแสดงโอกาสจะเกิดความเสียหาย (Likelihood)

ระดับโอกาส	คำนิยาม
๑	โอกาสเกิดขึ้นน้อยมาก (ไม่เกิน ๑ ครั้งต่อปี)
๒	โอกาสเกิดขึ้นน้อย (๒ ครั้งต่อปี)
๓	โอกาสเกิดขึ้นปานกลาง (๓ ครั้งต่อปี)
๔	โอกาสเกิดขึ้นสูง (๔ ครั้งต่อปี)
๕	โอกาสเกิดขึ้นสูงมาก (มากกว่า ๔ ครั้งต่อปี)

๒) การประเมินความรุนแรงของผลกระทบ (Impact : I) เป็นขั้นตอนการประเมินขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง ซึ่งสามารถจัดแบ่งออกเป็นระดับต่าง ๆ ได้จากผลกระทบที่แตกต่างกันซึ่งแสดงตามตารางที่ ๒-๕

ตารางที่ ๒-๕ ตารางแสดงการประเมินความรุนแรงของผลกระทบ (Impact)

ผลกระทบ	คำนิยาม
๑	<ul style="list-style-type: none"> - เกิดเหตุที่ไม่ส่งผลกระทบต่อการทำงานของระบบสารสนเทศ - กระทบต่อความน่าเชื่อถือขององค์กรหรือกระทบต่อความพึงพอใจของผู้ใช้บริการน้อยมาก (ระยะเวลาหยุดชะงักของระบบสารสนเทศ ไม่เกิน ๓๐ นาที)
๒	<ul style="list-style-type: none"> - เกิดเหตุที่กระทบต่อการทำงานของระบบสารสนเทศของหน่วยงานแต่แก้ไขได้ - กระทบต่อความน่าเชื่อถือขององค์กรหรือกระทบต่อความพึงพอใจของผู้ใช้บริการน้อย (ระยะเวลาหยุดชะงักไม่เกิน ๑ ชั่วโมง)
๓	<ul style="list-style-type: none"> - ระบบสารสนเทศมีปัญหา และมีความสูญเสียไม่มาก - กระทบต่อความน่าเชื่อถือขององค์กรหรือกระทบต่อความพึงพอใจของผู้ใช้บริการปานกลาง (ระยะเวลาหยุดชะงักไม่เกิน ๖ ชั่วโมง)
๔	<ul style="list-style-type: none"> - เกิดปัญหากับระบบสารสนเทศที่สำคัญและระบบความปลอดภัย ซึ่งส่งผลกระทบต่อความถูกต้องของข้อมูลบางส่วน - กระทบต่อความน่าเชื่อถือขององค์กรหรือกระทบต่อความพึงพอใจของผู้ใช้บริการมาก (ระยะเวลาหยุดชะงักไม่เกิน ๑๒ ชั่วโมง)
๕	<ul style="list-style-type: none"> - เกิดความสูญเสียต่อระบบสารสนเทศที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูล - กระทบต่อความน่าเชื่อถือขององค์กร หรือกระทบต่อความพึงพอใจของผู้ใช้บริการมากที่สุด (ระยะเวลาหยุดชะงักมากกว่า ๑๒ ชั่วโมง)

๓) การจัดระดับความเสี่ยง (Degree of Risk) เป็นขั้นตอนการนำผลการประเมินความเสี่ยงที่ประมวลจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) เข้าด้วยกัน (ระดับความเสี่ยง = ระดับโอกาส X ระดับผลกระทบ) แล้วจัดทำแผนผังระดับความเสี่ยง (Risk Matrix)

๒.๖ กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

เป็นการวิเคราะห์ทางเลือกกลยุทธ์ในการจัดการความเสี่ยง เพื่อช่วยในการตัดสินใจของบุคคลหรือองค์กรใด ๆ หาวิธีการที่ดีที่สุดในการตัดสินใจแก้ไขปัญหาต่าง ๆ ที่อาจเกิดขึ้นในอนาคต ทั้งนี้เพื่อลดผลกระทบ หรือความเสียหายที่อาจเกิดขึ้นให้น้อยที่สุด โดยมีค่าใช้จ่ายน้อยที่สุด ซึ่งมีวิธีการจัดการ ดังนี้

๑) การยอมรับความเสี่ยง (Take/Risk Acceptance) หมายถึง การไม่กระทำใด ๆ เพิ่มเติม กรณีนี้ใช้กับความเสี่ยงที่มีน้อย มีความน่าจะเป็นเกิดน้อย หรือเห็นว่าต้นทุนในการบริหารความเสี่ยงสูง โดยขออนุมัติหลักการรับความเสี่ยงไว้

๒) การลด (Treat/Risk Reduction) หมายถึง การลดโอกาสที่จะเกิดความเสี่ยง การป้องกันการเกิดความสูญเสีย หรือลดผลกระทบจากเหตุการณ์ที่อาจเกิดขึ้นในอนาคต โดยการจัดระบบการควบคุม การกำหนดแผนสำรองในเหตุการณ์ การวิเคราะห์ข้อมูลในอดีต ปัจจุบัน ซึ่งรวมถึงการคาดการณ์ในอนาคต ประกอบการตัดสินใจ

๓) การหลีกเลี่ยงความเสี่ยง (Terminate/Risk Avoidance) หมายถึง การหยุด หรือการเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น การงดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง หรือการปรับเปลี่ยนรูปแบบการทำงานและลดขอบเขตการดำเนินการ เป็นต้น

๔) การกระจาย (Transfer/Risk Sharing) หรือโอนความเสี่ยง (Risk Spreading) หมายถึง การลดโอกาสความน่าจะเป็นเกิดหรือลดความเสียหายโดยการแบ่งโอน การหาผู้รับผิดชอบในความเสี่ยง การจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน และการจัดประกันภัย เป็นต้น

๕) การลดความเสี่ยง (Risk Mitigate) หมายถึง การวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในหน่วยงานจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกเป็นทางการ และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

แนวทางปฏิบัติที่ดีที่สุดสำหรับการลดความเสี่ยง (Best Practices For Risk Mitigation)

- Cybersecurity Training Programs
- Updating Software
- Privileged Access Management Solutions
- Multi-factor Access Authentication
- Dynamic Data Backup

๒.๗ กิจกรรมการบริหารความเสี่ยง (Control Activities)

เป็นขั้นตอนดำเนินการกำหนดกิจกรรม หรือมาตรการในการจัดการความเสี่ยงให้หมดไป หรือควบคุมความเสี่ยงให้ลดลงในระดับที่ยอมรับได้โดยกิจกรรมที่กำหนดต้องเป็นกิจกรรมที่ยังไม่เคยปฏิบัติ หรือเป็นกิจกรรมที่กำหนดขึ้นเพิ่มเติมจากกิจกรรมเดิมที่เคยปฏิบัติอยู่แล้ว แต่กิจกรรมนั้นไม่สามารถควบคุมความเสี่ยงได้นอกจากนี้ยังต้องกำหนดระยะเวลาที่ใช้ในการดำเนินการแต่ละกิจกรรม ตลอดจนหน่วยงานผู้รับผิดชอบ ดังนั้น

กิจกรรมการบริหารความเสี่ยงต่าง ๆ ที่กำหนดขึ้นจึงมีเป้าหมายเพื่อควบคุมความเสี่ยง (Risk Control) ซึ่งสามารถแบ่งประเภทของการควบคุมความเสี่ยงออกเป็น ๔ ประเภท ดังนี้

๑) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

๒) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว

๓) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

๔) การควบคุมเพื่อแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขใหม่ไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

ทั้งนี้ การดำเนินกิจกรรมการควบคุมควรต้องคำนึงถึงความคุ้มค่าในด้านค่าใช้จ่าย ต้นทุน และผลประโยชน์ที่คาดว่าจะได้รับโดยกิจกรรมการควบคุมควรมีองค์ประกอบ ดังนี้

๑) วิธีการดำเนินงาน ซึ่งประกอบด้วยขั้นตอนและกระบวนการ

๒) การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น ซึ่งควรพิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน และพิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

๓) กำหนดระยะเวลาแล้วเสร็จของงาน

๒.๘ ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

เป็นขั้นตอนและกระบวนการโดยมีวัตถุประสงค์เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง มีการเปิดช่องทางการสื่อสาร และรับทราบข้อมูลด้านการบริหารความเสี่ยงให้กับผู้บริหาร และบุคลากรขององค์กรได้เข้าถึง โดยผ่านช่องทางต่าง ๆ เช่น ระบบอินเทอร์เน็ต หนังสือเวียน การประชุม การชี้แจงโดยผู้บริหาร สื่อประชาสัมพันธ์ หรือการฝึกอบรม เป็นต้น ซึ่งการสื่อสารที่มีประสิทธิผลนั้นต้องให้มั่นใจได้ว่า

๑) ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา

๒) ผู้บริหารสามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลง หรือความเสี่ยงที่เกิดขึ้นใหม่ได้ทัน่วงที

๓) มีการติดตามแผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กร และจัดการความเสี่ยงต่าง ๆ เพื่อให้องค์กรมีโอกาสนในการบรรลุวัตถุประสงค์ได้มากที่สุด

๒.๙ การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

การติดตาม และเฝ้าระวังความเสี่ยง โดยการกำหนดให้มีการติดตาม และประเมินผลว่าแต่ละหน่วยงาน มีการประเมินประสิทธิผลของการจัดการความเสี่ยงที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ เพื่อให้เกิดความมั่นใจว่ามาตรการในการปรับปรุงความเสี่ยงที่วางไว้มีความเพียงพอ เหมาะสม มีประสิทธิภาพประสิทธิผล และมีการปฏิบัติจริงสามารถลดหรือป้องกันความเสี่ยงที่อาจเกิดขึ้น นับเป็นขั้นตอนสุดท้ายและเป็นปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง ซึ่งควรพิจารณาประเด็นต่อไปนี้

๑) การรายงาน และสอบทานขั้นตอนตามกระบวนการบริหารความเสี่ยง เช่น การรายงานและติดตามผลระหว่างการทำงาน (On-Going Monitoring) เพื่อสังเกต ติดตาม รายงานความคืบหน้า รวมทั้งสอบทานหรือยืนยันผลระหว่างการทำงาน

- ๒) ความชัดเจนและสม่ำเสมอของการมีส่วนร่วม และความมุ่งมั่นของผู้บริหารระดับสูง
- ๓) บทบาทของผู้นำในการสนับสนุน และติดตามการบริหารความเสี่ยง
- ๔) การประยุกต์ใช้เกณฑ์การประเมินผลการดำเนินงานที่เกี่ยวกับการบริหารความเสี่ยง เช่น การประเมินผลอิสระ (Independent Evaluation) ซึ่งเป็นการประเมินผลที่เกิดขึ้นในช่วงเวลาที่แล้วแต่จะกำหนด หรือการประเมินโดยผู้ที่ไม่มีส่วนเกี่ยวข้อง หรือการประเมินการควบคุมด้วยตนเอง (Control Self Assessment : CSA) ซึ่งเป็นการจัดประชุมเชิงปฏิบัติร่วมกัน ระหว่าง ผู้บริหาร ผู้ปฏิบัติงาน ผู้มีความรู้ด้านการควบคุม และผู้อื่นที่มีส่วนเกี่ยวข้อง เป็นต้น

๒.๑๐ ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สนช. ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๘ ประเภท ดังนี้

๒.๑๐.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น ภัยจากอุทกภัย อัคคีภัย ไฟผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยของปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

๒.๑๐.๒ ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผนการตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

๒.๑๐.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ Malware Trojan หรือ Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

๒.๑๐.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัปเดตให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

๒.๑๐.๕ ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบสารสนเทศและการสื่อสารอันอาจก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้ความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่ต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับ

ผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูล และคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใด ๆ จึงมีความสำคัญ และจำเป็นที่จะต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

๒.๑๐.๖ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาลและผู้บริหารองค์กรต่าง ๆ ในด้านเทคโนโลยีสารสนเทศ ทำให้การกำหนดยุทธศาสตร์ และกลยุทธ์เปลี่ยนแปลงไป

๒.๑๐.๗ ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอต่อการใช้จ่ายงบประมาณ

๒.๑๐.๘ ความเสี่ยงด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยง เนื่องจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

๒.๑๑ การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพ ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรม ที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่เกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น โดยมีได้คิดทบทวนถึงผลที่จะได้รับนำมาซึ่งการเสียโอกาสของหน่วยงานได้

การจัดการ/การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ก็ควรจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้ วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้น การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วจะมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน หน่วยงานอาจอาจเลือกซื้อประกัน หรือทำสัญญาการบำรุงรักษาหลังการขาย

การยอมรับ (Take) เป็นการยอมรับความเสี่ยงหรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

๒.๑๒ ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของ สนข. ได้แก่

๒.๑๒.๑ ปัจจัยภายนอก ได้แก่

- (๑) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล เช่น ไฟไหม้ ภัยพิบัติ อุทกภัย
- (๒) การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- (๓) การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)
- (๔) ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง
- (๕) ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ
- (๖) การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker)

โดยไม่ได้รับอนุญาต

๒.๑๒.๒ ปัจจัยภายใน ได้แก่

- (๑) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย
- (๒) การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่าง ๆ จากผู้ใช้งานใน สนข.
- (๓) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๒.๑๓ การประเมินความเสียหาย

๒.๑๓.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒.๑๓.๒ ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วคราว ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๒.๑๔ การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

๒.๑๕ ระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของ สนข.

ระบบเครือข่ายคอมพิวเตอร์ของ สนข. ได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยห้องปฏิบัติการศูนย์ข้อมูล (Data Center) ของ สนข. ตั้งอยู่ที่ชั้น ๔ อาคาร สนข. มีเครือข่ายเชื่อมโยงไปยังส่วนกลางกระทรวงคมนาคม เพื่อการสื่อสารข้อมูลคอมพิวเตอร์ หรือการสื่อสารรูปแบบอื่นในอนาคต ระบบเครือข่ายคอมพิวเตอร์ของ สนข. มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังระบบเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ในการกรองข้อมูล (Package Filter) ที่ผ่านเข้ามาภายในระบบเครือข่ายคอมพิวเตอร์ของ สนข.

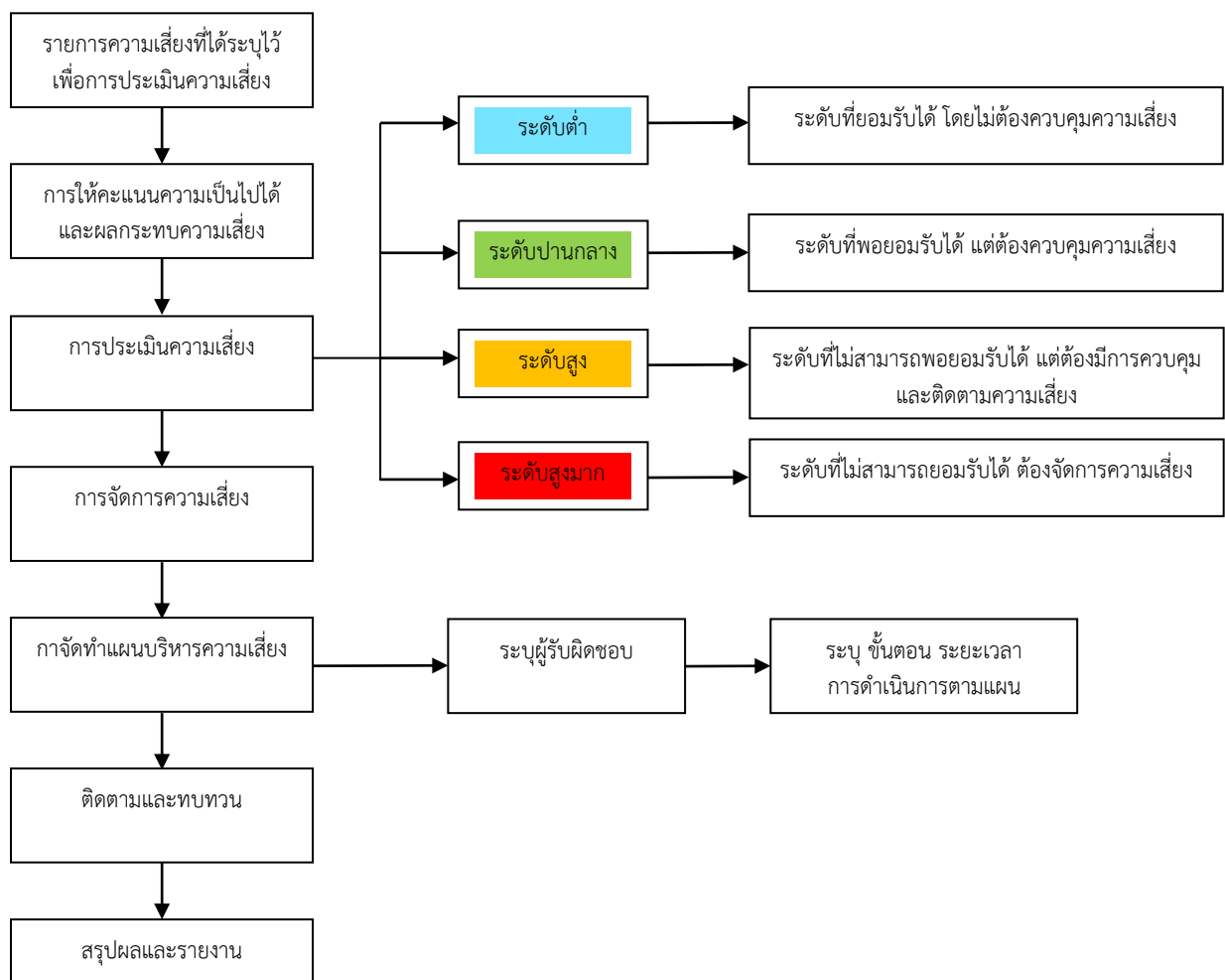
จากเครือข่ายภายนอก นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วน of เครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ที่ดูแลเครื่องแม่ข่ายทั้งหมดของ สนข. ให้บุคคลภายนอกเข้าถึงได้ รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของ สนข. เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด

บทที่ ๓

การวิเคราะห์การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สนข. ได้ตระหนักถึงความสำคัญของข้อมูลที่อยู่ภายใต้การดูแลของหน่วยงานที่อาจเกิดความเสียหายจากปัจจัยต่าง ๆ โดยศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.) ซึ่งมีหน้าที่บริหารจัดการและดูแลระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงานสารสนเทศ เล็งเห็นถึงความสำคัญในการรักษาความมั่นคงปลอดภัยให้แก่ระบบต่าง ๆ จึงได้จัดทำแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. โดยกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เริ่มต้นจากการรวบรวมข้อมูลกิจกรรมและปัจจัยความเสี่ยงที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ และจากการศึกษาข้อมูล ระดมความคิดเห็นของเจ้าหน้าที่ผู้ปฏิบัติงานด้านกิจกรรมต่าง ๆ จนเป็นกำหนดขั้นตอนได้ ดังนี้

๓.๑ ขั้นตอนการดำเนินการบริหารจัดการความเสี่ยง



รูปที่ ๓-๑ ขั้นตอนการดำเนินการบริหารจัดการความเสี่ยง

๓.๒ กระบวนการจัดทำแผนบริหารจัดการความเสี่ยง

๓.๒.๑ ศทท. ดำเนินการทบทวนแผนบริหารความเสี่ยงด้านสารสนเทศของ สนข. พร้อมทบทวนความเสี่ยงที่ สนข. เผชิญอยู่

๓.๒.๒ ศทท. ดำเนินการจัดทำ/ปรับปรุงแก้ไข (ร่าง) แผนบริหารความเสี่ยงด้านสารสนเทศของ สนข.

๓.๒.๓ ศทท. เสนอร่างแผนฯ ต่อผู้บริหารของหน่วยงานเพื่อพิจารณา (ร่าง) แผนฯ

๓.๒.๔ ปรับปรุงร่างแผนและเสนอผู้บริหารเพื่อขอความเห็นชอบ (ร่าง) แผนฯ

๓.๒.๕ ดำเนินการเผยแพร่และถือปฏิบัติตามแผนฯ

๓.๒.๖ ศทท. ดำเนินการติดตามการดำเนินงานตามแผนฯ และประเมินผลความเสี่ยง

๓.๒.๗ สรุปผลรายงานที่ได้เสนอต่อผู้บริหาร

๓.๒.๘ นำผลที่ได้จากการติดตามการดำเนินงานตามแผนฯ และประเมินผลความเสี่ยงมาทบทวนเพื่อนำไปปรับปรุงขั้นตอนการประเมินความเสี่ยงในรอบถัดไป

๓.๓ การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk Identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่ สนข. เผชิญอยู่ โดยมีการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินความเป็นไปได้และผลกระทบ ดังนี้

ระดับความเสี่ยง	ระดับสี	คำอธิบาย	คะแนน
สูงมาก	แดง	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยทันที	๑๕ - ๒๔
สูง	ส้ม	ระดับที่ไม่สามารถยอมรับได้ โดยต้องมีการควบคุมและติดตามความเสี่ยง เพื่อป้องกันไม่ให้เคลื่อนย้ายไประดับสูงมาก	๘ - ๑๔
ปานกลาง	เขียว	ระดับที่ยอมรับได้ แต่ต้องการมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	๔ - ๗
ต่ำ	ฟ้า	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยงหรือไม่ต้องการจัดการเพิ่มเติม	๑ - ๓

การประเมินความเสี่ยง

ผลกระทบ	๕	๑๐	๑๕	๒๐	๒๕
	๔	๘	๑๒	๑๖	๒๐
	๓	๖	๙	๑๒	๑๕
	๒	๔	๖	๘	๑๐
	๑	๒	๓	๔	๕

โอกาสเกิดความเสี่ยง

รูปที่ ๓-๒ แผนผังค่าความเสี่ยงแต่ละระดับ (Risk Matrix)

๓.๓.๑ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการทบทวนความเสี่ยงของ สนข. มีความเสี่ยงด้านเทคโนโลยีสารสนเทศ จำนวน ๖ ด้าน ดังนี้

ตารางที่ ๓-๑ ตารางการทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข.

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผู้ได้รับผลกระทบ/ ระบบที่ได้รับผลกระทบ
๑. ความเสี่ยงด้านกายภาพและสภาพแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์สร้างขึ้น เช่น ภัยพิบัติ แผ่นดินไหว อุทกภัย อัคคีภัย ไฟป่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบ รักษาความปลอดภัยห้องปฏิบัติการศูนย์ข้อมูล ระบบเครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ			
๐๑ ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร หรือการวางเพลิง - ภัยที่เกิดจากธรรมชาติ เช่น ไฟป่า - นำเข้าหรือมีวัตถุไวไฟ เช่น แอลกอฮอล์ ภายในห้องปฏิบัติการศูนย์ข้อมูล	- เกิดความเสียหายต่อทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูล ถูกทำลายทั้งหมด - ระบบคอมพิวเตอร์แม่ข่ายหยุดประมวลผล - การดำเนินงานหยุดชะงักทั้งระบบ	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล
๐๒ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ	แหล่งที่ให้บริการกระแสไฟฟ้าขัดข้อง หรือแรงดันไฟฟ้าขัดข้อง	- ทำให้ระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และระบบฐานข้อมูล หยุดทำงาน - เกิดความเสียหายไม่สามารถให้บริการได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล
๐๓ การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และเครือข่ายคอมพิวเตอร์ของ สนข.	ควบคุมอุณหภูมิและความชื้นที่ไม่เหมาะสม	- เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ ในห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และเครือข่ายคอมพิวเตอร์ของ สนข.	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจเกิดขึ้น	ผู้ได้รับผลกระทบ/ ระบบที่ได้รับผลกระทบ
๐๔ เกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	<ul style="list-style-type: none"> - การชุมนุมประท้วง - การจลาจล - การก่อการร้าย - เหตุภัยพิบัติ เช่น อุทกภัย แผ่นดินไหว อัคคีภัย และवादภัยฯ 	<ul style="list-style-type: none"> - เจ้าหน้าที่ไม่สามารถเข้าไปปฏิบัติงานได้ตามปกติเนื่องจากถูกปิดล้อมสถานที่ทำงาน - หน่วยงานถูกตัดกระแสไฟฟ้าทำให้ระบบงานหยุดทำงานไม่สามารถให้บริการได้ จำเป็นต้องเข้าระบบจากระยะไกล (Remote) - อุปกรณ์ฮาร์ดแวร์ ได้รับความเสียหายร้ายแรง 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล
๐๕ การถูกบุกรุกหรือเข้าถึงพื้นที่หวงห้าม	ผู้ไม่มีสิทธิ์เข้าถึงระบบคอมพิวเตอร์แม่ข่าย อุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ จนทำให้ข้อมูลถูกคัดลอก แก้ไข ลบ หรือถูกขโมยข้อมูล	<ul style="list-style-type: none"> - ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้ - อุปกรณ์ฮาร์ดแวร์ ได้รับความเสียหายร้ายแรง 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล
๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดขึ้นกับอุปกรณ์ระบบเครือข่าย เทคโนโลยีสารสนเทศต่าง ๆ เช่น ระบบเครือข่ายอินเทอร์เน็ต ไวรัสคอมพิวเตอร์ การเคลื่อนย้ายตัวเครื่อง อุปกรณ์ และการติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ภัยคุกคามทางคอมพิวเตอร์ต่าง ๆ			
๐๖ ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ไม่มีการควบคุมบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์คอมพิวเตอร์ ครุภัณฑ์เครือข่าย หรืออุปกรณ์สูญหาย	<ul style="list-style-type: none"> - ผู้ดูแลระบบ - ระบบสารสนเทศ
๐๗ ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สนข.	ไม่มีกำหนดแผนรองรับอุปกรณ์เครือข่ายและระบบแม่ข่ายของ สนข.	<ul style="list-style-type: none"> - ระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้เมื่อเกิดข้อผิดพลาด ด้านฮาร์ดแวร์หรือฮาร์ดแวร์ได้รับความเสียหายร้ายแรง 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบสารสนเทศ
๐๘ ขาดการบริหารจัดการสิทธิการใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับ ของผู้ใช้งาน	ไม่มีการควบคุมสิทธิการใช้งานของอุปกรณ์เทคโนโลยีสารสนเทศ	<ul style="list-style-type: none"> - เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งานได้ - ไม่สามารถหาผู้กระทำความผิดได้ 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบสารสนเทศ

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจเกิดขึ้น	ผู้ได้รับผลกระทบ/ ระบบที่ได้รับผลกระทบ
๐๙ ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	<ul style="list-style-type: none"> - ผู้ให้บริการอินเทอร์เน็ต (ISP) ชัดข้อง - IP Address ไม่เพียงพอสำหรับผู้ใช้งาน - ปริมาณการรับ - ส่งข้อมูล (Bandwidth) ไม่เพียงพอสำหรับการใช้งาน 	<ul style="list-style-type: none"> - ผู้ใช้งานไม่สามารถเชื่อมต่ออินเทอร์เน็ต หรือมีความล่าช้า - ไม่สามารถเข้าถึงบริการสารสนเทศได้ 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ
๑๐ ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	ความเสี่ยงด้านการบริหารจัดการหรือจากเจ้าหน้าที่ผู้ปฏิบัติงาน	<ul style="list-style-type: none"> - ไม่มีการควบคุมอุปกรณ์ที่เชื่อมต่อกับเครือข่ายของหน่วยงาน - มีจำนวนบุคลากรเพิ่มขึ้น ทำให้การจัดการไม่ครอบคลุม 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบสารสนเทศ
๑๑ ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	<ul style="list-style-type: none"> - ครุภัณฑ์อุปกรณ์ไม่ได้มาตรฐานหรือตอบสนองได้ไม่ครอบคลุมกับการทำงาน - การติดตั้งใช้งานไม่สมบูรณ์ 	<ul style="list-style-type: none"> - เกิดความเสียหายจากการใช้งานครุภัณฑ์ - ติดตั้งใช้งานได้ไม่สมบูรณ์ - การทำงานล่าช้า 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ระบบสารสนเทศ
๑๒ การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	<ul style="list-style-type: none"> - ไม่มีการกำหนดวิธีการรักษาความปลอดภัยจากการปฏิบัติงานจากระยะไกล 	<ul style="list-style-type: none"> - อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย ทำให้เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบ เนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายได้ต่อระบบ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้ 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบสารสนเทศ - ระบบฐานข้อมูล
๑๓ ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบฐานข้อมูลไม่เพียงพอ	<ul style="list-style-type: none"> - ไม่มีการวางแผนการดำเนินงาน และอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน 	<ul style="list-style-type: none"> - การให้บริการระบบสารสนเทศหยุดชะงักส่งผลกระทบต่อ การให้บริการระบบฯ ต่อประชาชนและผู้ให้บริการทั่วไป 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบสารสนเทศ
๑๔ เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับ หรือไม่สามารถให้บริการได้	<ul style="list-style-type: none"> - เสื่อมสภาพตามอายุการใช้งาน - ถูกทำลายโดยผู้บุกรุก - การตก หล่น ชน กระแทก จากการเคลื่อนย้าย หรือการติดตั้งไม่มั่นคงแน่นหนา - เกิดจากระบบไฟฟ้าขัดข้อง 	<ul style="list-style-type: none"> - เกิดความผิดพลาดในการให้บริการ ระบบสารสนเทศ ระบบข้อมูลเสียหาย/ถูกทำลาย หรือ ไม่สามารถให้บริการต่อเนื่องได้ - ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการ ได้สูญเสียข้อมูลสำคัญที่เก็บอยู่ภายในเครื่องคอมพิวเตอร์แม่ข่าย 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบเครือข่าย

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจเกิดขึ้น	ผู้ได้รับผลกระทบ/ ระบบที่ได้รับผลกระทบ
๓. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัปเดตให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น			
๐๑๕ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	<ul style="list-style-type: none"> - ถูกบุคคลที่ไม่มีสิทธิ์หรือไม่มีอำนาจเจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) - ขาดการป้องกันและตรวจจับไวรัสคอมพิวเตอร์ - ไม่ดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลและระบบฐานข้อมูล - เกิดช่วงโหว่ของซอฟต์แวร์ที่ใช้งาน - ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan) 	<ul style="list-style-type: none"> - ข้อมูลถูกเปลี่ยนแปลงหรือถูกทำลาย - ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบเครือข่าย - ระบบฐานข้อมูล
๐๑๖ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	<ul style="list-style-type: none"> - ถูกบุคคลที่ไม่มีสิทธิ์หรือไม่มีอำนาจเจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) - ขาดการป้องกันและตรวจจับไวรัสคอมพิวเตอร์ - ไม่ดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลและระบบฐานข้อมูล - เกิดช่วงโหว่ของซอฟต์แวร์ที่ใช้งาน - ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan) 	<ul style="list-style-type: none"> - การให้บริการระบบสารสนเทศหยุดชะงักส่งผลกระทบต่อ การให้บริการระบบฯ ต่อประชาชนและผู้ให้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบ เสียหาย - ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล
๐๑๗ เกิดช่องโหว่ของซอฟต์แวร์ ขาดการบำรุงรักษา หรือเกิดช่องโหว่ ของโปรแกรม	<ul style="list-style-type: none"> - ไม่มีการอัปเดตซอฟต์แวร์ ให้เป็นปัจจุบัน - ไม่มีการบำรุงรักษาโปรแกรมอย่างต่อเนื่อง 	<ul style="list-style-type: none"> - ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัย ตามที่ผู้พัฒนาระบบได้กำหนด - ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้ - เกิดข้อขัดข้องจนระบบงานไม่สามารถทำงานได้ - ไม่มีการอัปเดตเวอร์ชันใหม่อย่างสม่ำเสมอทำให้ระบบไม่ปลอดภัย 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจเกิดขึ้น	ผู้ได้รับผลกระทบ/ ระบบที่ได้รับผลกระทบ
๐๑๘ ละเมิดลิขสิทธิ์โปรแกรม อรรถประโยชน์ (Utilities Program)	- การใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์ อาจไม่ปลอดภัยจากโปรแกรมประเภทไวรัส หรือมัลแวร์	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิด ลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุกคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ
๔. ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูล ที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่ องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการ			
๐๑๙ ข้อมูลสำคัญรั่วไหล	- เครื่องคอมพิวเตอร์แม่ข่าย หรือระบบ ฐานข้อมูลถูกโจมตีจากโปรแกรมประเภทไวรัส หรือมัลแวร์ - นำเครื่องคอมพิวเตอร์เก่ากลับมาใช้ใหม่ - ถูกโจมตีหรือถูกเจาะระบบ (Hack)	- มีข้อมูลสำคัญสูญหาย หรือหลุดรั่วไปยังภายนอกหน่วยงาน - อาจถูกดำเนินคดีหรือถูกฟ้องเรียกค่าเสียหายร่วมด้วย - หน่วยงานเสื่อมเสียชื่อเสียงและความน่าเชื่อถือ	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบเครือข่าย - ระบบฐานข้อมูล
๕. ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ			
๐๒๐ การนำเข้าข้อมูลผิดพลาด ไม่ครบถ้วน หรือไม่เป็นปัจจุบัน	- การนำเข้าข้อมูลที่ไม่ถูกต้องเข้าสู่ระบบ - ระบบมีความผิดพลาด (Bug) - ไม่มีการตรวจสอบและปรับปรุงข้อมูล ก่อนนำเข้าสู่ระบบ	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถนำข้อมูลไปใช้งานได้ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบฐานข้อมูล - ระบบสารสนเทศ
๐๒๑ การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญในการ ดูแลบำรุงรักษาระบบ/พัฒนาระบบ	- ระบบเกิดปัญหา ขัดข้อง - การให้บริการติดขัด ล่าช้า - อุปกรณ์หรือระบบสารสนเทศเสียหาย - ระบบไม่สามารถบริการได้	- ระบบมีข้อผิดพลาดและไม่เป็นไปตามแผน - เสียเวลาในการแก้ไขทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด - เกิดความผิดพลาดในการใช้ระบบส่งผลทำให้การทำงาน ของระบบบกพร่อง	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบฐานข้อมูล - ระบบสารสนเทศ

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจเกิดขึ้น	ผู้ได้รับผลกระทบ/ ระบบที่ได้รับผลกระทบ
O๒๒ บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ	<ul style="list-style-type: none"> - ขาดการอบรมบุคลากรด้านไอที - หน่วยงานขาดบุคลากรด้านไอที 	<ul style="list-style-type: none"> - ไม่สามารถแก้ไขปัญหาที่เกิดขึ้นขณะปฏิบัติงาน - การปฏิบัติงานล่าช้าติดขัด - อาจเกิดความเสียหายแก่ระบบ หรือหน่วยงาน 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ
O๒๓ ผู้ใช้งาน (User) ไม่มีความรู้ ความชำนาญ และทักษะ การใช้งานระบบ	<ul style="list-style-type: none"> - ไม่มีการอบรมการใช้งานระบบแก่ผู้ใช้งาน - ระบบมีความซับซ้อน ยากต่อการใช้งาน 	<ul style="list-style-type: none"> - การใช้ระบบงานไม่เป็นไปตาม Workflow ที่กำหนด ทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขปัญหาด้วยตัวเอง ในเบื้องต้นได้ - ความล่าช้าในการปฏิบัติงานและเพิ่มปริมาณงานให้กับผู้ดูแลระบบ - ไม่มีการใช้งานทำให้ไม่มีการนำเข้าสู่ข้อมูล / ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ / ข้อมูลไม่ถูกนำไปใช้งาน 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ
O๒๔ การเชื่ออีเมลหรือหน้าเว็บไซต์ ปลอมเพื่อหลอกลวง (Mail Phishing)	<ul style="list-style-type: none"> - การเปิดไฟล์ หรือ URL ที่แนบมากับอีเมลที่น่าสงสัย - การหลงเชื่อเว็บไซต์ปลอม - ให้ข้อมูลส่วนตัวหรือลงโปรแกรมที่มาจากแหล่งที่ไม่น่าเชื่อถือ 	<ul style="list-style-type: none"> - โดนหลอกลวงเพื่อขอรหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับ - โดนหลอกเพื่อติดตั้งไวรัสลงบนคอมพิวเตอร์ หรือคอมพิวเตอร์แม่ข่าย 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล
O๒๕ การโดนดักจับข้อมูลจากการใช้ เครือข่ายเดียวกันกับบุคคลน่าสงสัย	<ul style="list-style-type: none"> - การเข้าใช้งานระบบจากระยะไกลด้วยเครือข่ายที่ไม่น่าเชื่อถือ - การให้บุคคลที่น่าสงสัยมาใช้งานเครือข่ายเดียวกัน 	<ul style="list-style-type: none"> - โดนดักเก็บข้อมูลการดำเนินการ เช่น รหัสผ่าน ข้อมูลสำคัญ และข้อมูลที่เป็นความลับ - เกิดความผิดพลาดในการให้บริการระบบสารสนเทศ และการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้ 	<ul style="list-style-type: none"> - ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบสารสนเทศ - ระบบฐานข้อมูล

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจเกิดขึ้น	ผู้ได้รับผลกระทบ/ ระบบที่ได้รับผลกระทบ
๐๒๖ ผู้ใช้งานไม่ออกจากระบบ เมื่อไม่ใช้งาน	<ul style="list-style-type: none"> - ผู้ใช้งานลืมออกจากระบบ - ผู้ใช้งานละเลยเรื่องความปลอดภัยของระบบ 	<ul style="list-style-type: none"> - เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้ 	<ul style="list-style-type: none"> - ผู้ใช้งานระบบ - ผู้ดูแลระบบ - ระบบคอมพิวเตอร์แม่ข่าย - ระบบเครือข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล
๖. ความเสี่ยงในด้านการบริหารจัดการ (Management Risk) หมายถึง ความเสี่ยงเนื่องมาจากการได้รับสนับสนุนงบประมาณไม่เพียงพอ การบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี และการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา			
๐๒๗ งบประมาณไม่เพียงพอสำหรับ ดำเนินโครงการ	<ul style="list-style-type: none"> - โคนตัด/ปรับลดงบประมาณในการดำเนินโครงการตามนโยบายการปรับลดเงินเป็นร้อยละ ทำให้โครงการที่จำเป็นต้องดำเนินการโดนตัดหรือปรับลดไปด้วย 	<ul style="list-style-type: none"> - อาจต้องลดระยะเวลา ลดคุณภาพ หรือประสิทธิภาพของงานหรือโครงการที่โดนตัดหรือปรับลดงบประมาณ - ไม่ได้ดำเนินโครงการตามเป้าที่วางไว้ - งดเงิน และงดงานไม่สอดคล้องกัน - ไม่ได้อุปกรณ์ หรือครุภัณฑ์ทดแทน ทำให้การปฏิบัติงานมีประสิทธิภาพลดลง 	<ul style="list-style-type: none"> - ผู้ใช้งานระบบ - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบคอมพิวเตอร์แม่ข่าย - ระบบสารสนเทศ
๐๒๘ ไม่สามารถดำเนินโครงการ ที่กำหนดไว้ตามแผนปฏิบัติราชการ	<ul style="list-style-type: none"> - ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนได้ 	<ul style="list-style-type: none"> - ผู้บริหารปรับลดระยะเวลาดำเนินโครงการ - ไม่สามารถดำเนินงานให้บรรลุเป้าหมายและตัวชี้วัดที่กำหนด 	<ul style="list-style-type: none"> - ผู้ใช้งานระบบ - ระบบคอมพิวเตอร์แม่ข่าย - ระบบเครือข่าย - ระบบสารสนเทศ - ระบบฐานข้อมูล
๐๒๙ กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน/ อนุมัติโครงการล่าช้า	<ul style="list-style-type: none"> - ไม่สามารถดำเนินงานได้อย่างต่อเนื่องทันที - การดำเนินการโครงการล่าช้า - การเปลี่ยนแปลงวิธีการระหว่างดำเนินการ 	<ul style="list-style-type: none"> - เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง - อนุมัติโครงการล่าช้า - ไม่สามารถหาผู้รับจ้างได้ตามแผนดำเนินการ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปีส่งผลกระทบต่อการทำงานขององค์กร 	<ul style="list-style-type: none"> - ผู้ใช้งานระบบ - ผู้ดูแลระบบ - ระบบคอมพิวเตอร์แม่ข่าย - ระบบเครือข่าย - ระบบสารสนเทศ

กิจกรรม/ความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจเกิดขึ้น	ผู้ได้รับผลกระทบ/ ระบบที่ได้รับผลกระทบ
O๓๐ ไม่สามารถปฏิบัติตามกฎหมาย และระเบียบที่เกี่ยวข้อง	<ul style="list-style-type: none"> - กฎหมาย/ระเบียบที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีผลบังคับใช้ - ไม่สามารถดำเนินการตามกฎหมาย/ระเบียบที่เกี่ยวข้องได้ทันภายในระยะเวลาที่กำหนด 	<ul style="list-style-type: none"> - การดำเนินงานไม่สามารถรองรับการปฏิบัติงานตามกฎหมาย/ระเบียบที่บังคับใช้ได้ - ไม่มีระบบสารสนเทศรองรับการดำเนินงานตามที่กฎหมายกำหนด 	<ul style="list-style-type: none"> - ผู้ใช้งานระบบ - ผู้ดูแลระบบ - ระบบสารสนเทศ
O๓๑ การเปลี่ยนแปลงนโยบาย ด้านเทคโนโลยีสารสนเทศของหน่วยงาน	<ul style="list-style-type: none"> - การปรับเปลี่ยนตำแหน่งงาน - การปรับเปลี่ยนบุคลากร - การเปลี่ยนแปลงนโยบายด้านเทคโนโลยีสารสนเทศของหน่วยงาน 	<ul style="list-style-type: none"> - การดำเนินงานล่าช้า ติดขัด 	<ul style="list-style-type: none"> - ผู้ใช้งานระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล

๓.๓.๒ การประเมินความเสี่ยงและจัดการความเสี่ยง ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

สนข. มีผลการประเมินเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ดังนี้

ตารางที่ ๓-๒ ตารางการวิเคราะห์ทบทวนโอกาสและความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข.

ที่	กิจกรรม/ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน
๑	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	๑	๕	๕
๒	ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ	๓	๓	๙
๓	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และระบบเครือข่ายคอมพิวเตอร์ของ สนข.	๒	๑	๒
๔	เกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑	๕	๕
๕	การถูกบุกรุกหรือเข้าถึงพื้นที่หวงห้าม	๑	๕	๕
๖	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยี และการสื่อสาร	๑	๔	๔
๗	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่าย และเครือข่ายคอมพิวเตอร์ สนข.	๑	๕	๕
๘	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศ ในทุก ๆ ระดับผู้ใช้งาน	๑	๓	๓
๙	ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	๑	๒	๒
๑๐	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑	๒	๒
๑๑	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	๑	๑	๑
๑๒	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑	๓	๓
๑๓	ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบฐานข้อมูลไม่เพียงพอ	๒	๒	๔
๑๔	เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับ หรือไม่สามารถให้บริการได้	๒	๓	๖
๑๕	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๓	๕	๑๕
๑๖	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๓	๕	๑๕
๑๗	เกิดช่องโหว่ของซอฟต์แวร์ขาดการบำรุงรักษา หรือเกิดช่องโหว่ของโปรแกรม	๒	๓	๖
๑๘	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	๕	๓	๑๕
๑๙	ข้อมูลสำคัญรั่วไหล	๒	๔	๘
๒๐	การนำเข้าข้อมูลผิดพลาดไม่ครบถ้วน หรือไม่ปัจจุบัน	๑	๓	๓
๒๑	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแล บำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓
๒๒	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยี ๆ ไม่เพียงพอ	๑	๒	๒
๒๓	ผู้ใช้งาน (Users) ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	๔	๒	๘
๒๔	การเชื่อมโยงอีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	๓	๒	๖
๒๕	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	๑	๒	๒
๒๖	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๕	๑	๕
๒๗	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๑	๒	๒
๒๘	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนดิจิทัลฯ	๑	๑	๑
๒๙	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน/อนุมัติโครงการล่าช้า	๑	๑	๑
๓๐	ไม่สามารถปฏิบัติตามกฎหมาย และระเบียบที่เกี่ยวข้อง	๑	๑	๑
๓๑	การเปลี่ยนแปลงนโยบายด้านเทคโนโลยีสารสนเทศของหน่วยงาน	๑	๑	๑

๓.๓.๓ การจัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ

นำผลคะแนนการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ จำนวน ๓๑ กิจกรรม มาจัดลำดับได้ดังนี้

ตารางที่ ๓-๓ ตารางการจัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข.

ลำดับที่	รหัส	กิจกรรม/ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๑	๐๑๘	ละเมิดลิขสิทธิ์โปรแกรมมอรรถประโยชน์ (Utilities Program)	๕	๓	๑๕	สูงมาก
๒	๐๑๕	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๓	๕	๑๕	สูงมาก
๓	๐๑๖	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๓	๕	๑๕	สูงมาก
๔	๐๒	ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ	๓	๓	๙	สูง
๕	๐๑๙	ข้อมูลสำคัญรั่วไหล	๒	๔	๘	สูง
๖	๐๒๓	ผู้ใช้งาน (Users) ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	๔	๒	๘	สูง
๗	๐๑๗	เกิดช่องโหว่ของซอฟต์แวร์ขาดการบำรุงรักษา หรือเกิดช่องโหว่ของโปรแกรม	๒	๓	๖	ปานกลาง
๘	๐๑๔	เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับ หรือไม่สามารถให้บริการได้	๒	๓	๖	ปานกลาง
๙	๐๒๔	การเชื่อมอีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	๓	๒	๖	ปานกลาง
๑๐	๐๑	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	๑	๕	๕	ปานกลาง
๑๑	๐๔	เกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑	๕	๕	ปานกลาง

ลำดับที่	รหัส	กิจกรรม/ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๑๒	๐๕	การถูกบุกรุกหรือเข้าถึงพื้นที่หวงห้าม	๑	๕	๕	ปานกลาง
๑๓	๐๗	ขาดแผนรองรับระบบฮาร์ดแวร์ภายใน ศูนย์ปฏิบัติการระบบแม่ข่าย และเครือข่าย คอมพิวเตอร์ สนข.	๑	๕	๕	ปานกลาง
๑๔	๐๒๖	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๕	๑	๕	ปานกลาง
๑๕	๐๖	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สิน ของอุปกรณ์ เทคโนโลยีและการสื่อสาร	๑	๔	๔	ปานกลาง
๑๖	๐๑๓	ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบฐานข้อมูลไม่เพียงพอ	๒	๒	๔	ปานกลาง
๑๗	๐๘	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์ เทคโนโลยีสารสนเทศในทุก ๆ ระดับผู้ใช้งาน	๑	๓	๓	ต่ำ
๑๘	๐๑๒	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงาน จากระยะไกลไม่ทั่วถึง	๑	๓	๓	ต่ำ
๑๙	๐๒๐	การนำเข้าข้อมูลผิดพลาดไม่ครบถ้วน หรือไม่เป็น ปัจจุบัน	๑	๓	๓	ต่ำ
๒๐	๐๒๑	การจ้างบุคคลภายนอก ที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓	ต่ำ
๒๑	๐๓	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการ ศูนย์ข้อมูล (Data Center) และระบบเครือข่าย คอมพิวเตอร์ของ สนข.	๒	๑	๒	ต่ำ
๒๒	๐๙	ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	๑	๒	๒	ต่ำ
๒๓	๐๒๒	บุคลากรด้านไอทีมีความรู้ ความเข้าใจ ด้านเทคโนโลยี ๆ ไม่เพียงพอ	๑	๒	๒	ต่ำ
๒๔	๐๒๕	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกัน กับบุคคลน่าสงสัย	๑	๒	๒	ต่ำ

ลำดับที่	รหัส	กิจกรรม/ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๒๕	๐๒๗	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๑	๒	๒	ต่ำ
๒๖	๐๑๐	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์ สื่อสารเคลื่อนที่	๑	๑	๑	ต่ำ
๒๗	๐๑๑	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ ไม่เหมาะสมกับลักษณะงาน	๑	๑	๑	ต่ำ
๒๘	๐๒๘	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผน ดิจิทัลฯ	๑	๑	๑	ต่ำ
๒๙	๐๒๙	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบ ไม่เป็นไปตามแผน/อนุมัติโครงการล่าช้า	๑	๑	๑	ต่ำ
๓๐	๐๓๐	ไม่สามารถปฏิบัติตามกฎหมายและระเบียบ ที่เกี่ยวข้อง	๑	๑	๑	ต่ำ
๓๑	๐๓๑	การเปลี่ยนแปลงนโยบายด้านเทคโนโลยีสารสนเทศ ของหน่วยงาน	๑	๑	๑	ต่ำ

จากผลการประเมินความเสี่ยงฯ พบว่า มีปัจจัยเสี่ยงทั้งสิ้น ๓๑ ปัจจัย แบ่งเป็น ปัจจัยเสี่ยงที่มีคะแนนอยู่ในระดับสูงมาก จำนวน ๓ รายการ ระดับสูง จำนวน ๓ รายการ ระดับปานกลาง จำนวน ๑๐ รายการ และระดับต่ำ จำนวน ๑๕ รายการ ทำให้ต้องมีการดำเนินการจัดการความเสี่ยง โดยความเสี่ยงที่อยู่ในระดับสูงมากเป็นระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยทันที ความเสี่ยงระดับสูง เป็นระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ต่อไป ความเสี่ยงระดับปานกลาง เป็นระดับที่สามารถยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ และความเสี่ยงระดับต่ำเป็นระดับที่สามารถยอมรับได้โดยไม่ต้องควบคุมความเสี่ยงหรือไม่ต้องมีการจัดการเพิ่มเติม

๓.๔ การประเมินระดับความเสี่ยงและแนวทางในการบริหารจัดการความเสี่ยง

ในปีงบประมาณ พ.ศ. ๒๕๖๘ ที่ผ่านมา สนข. ได้ประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ และกำหนดแนวทางในการบริหารจัดการความเสี่ยงฯ ของ สนข. ดังนี้

ตารางที่ ๓-๔ ผลการประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำหนดแนวทางในการบริหารจัดการความเสี่ยง

ลำดับที่	รหัส	ปัจจัยเสี่ยง	ค่าระดับความเสี่ยง	การตอบสนองความเสี่ยง	แนวทางการดำเนินการจัดการ/ควบคุมความเสี่ยง
๑	๐๑๘	ละเมิดลิขสิทธิ์โปรแกรมมัลแวร์ (Utilities Program)	๑๕	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none">- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติ ความมั่นคงปลอดภัยด้านสารสนเทศและการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย- กระตุ้นให้เกิดการปฏิบัติตามนโยบายหรือระเบียบฯ อย่างจริงจัง- ส่งเสริมให้ใช้โปรแกรมมัลแวร์แบบ OpenSource แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์- จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
๒	๐๑๕	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๑๕	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none">- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall- ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ- ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ- ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ- ติดตั้งโปรแกรมป้องกันไวรัส- ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ- เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
๓	๐๑๖	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๑๕	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none">- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall- ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ

ลำดับที่	รหัส	ปัจจัยเสี่ยง	ค่าระดับความเสี่ยง	การตอบสนองความเสี่ยง	แนวทางการดำเนินการจัดการ/ควบคุมความเสี่ยง
					<ul style="list-style-type: none"> - ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ทดสอบช่องโหว่ของโปรแกรม - กำหนดมาตรฐานในการพัฒนาโปรแกรมให้มีความปลอดภัย
๔	๐๒	ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ	๔	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none"> - ตรวจสอบระบบสำรองไฟฟ้า (UPS) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายให้อยู่ในสถานะพร้อมใช้งานเป็นประจำ - มีการจัดจ้างผู้เชี่ยวชาญเพื่อดำเนินการบำรุงรักษา
๕	๐๑๙	ข้อมูลสำคัญรั่วไหล	๔	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none"> - มีระบบพิสูจน์ตัวตนก่อนเข้าใช้งานระบบคอมพิวเตอร์ - ระบบเครือข่าย ระบบสารสนเทศ - มีกระบวนการทบทวนสิทธิผู้ใช้งานเป็นประจำ - มีการเก็บประวัติการเข้าใช้งานคอมพิวเตอร์ - มีกระบวนการบริหารจัดการคอมพิวเตอร์และอุปกรณ์ - มีแนวปฏิบัติในการลบหรือทำลายข้อมูลหลังจากไม่ได้ใช้งาน
๖	๐๒๓	ผู้ใช้งาน (Users) ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	๔	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none"> - อบรมการใช้งานระบบ - จัดทำคู่มือสำหรับการใช้งานระบบ - ให้มีเจ้าหน้าที่สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ และช่วยแก้ไขปัญหาให้ผู้ใช้งาน
๗	๐๑๗	เกิดช่องโหว่ของซอฟต์แวร์ขาดการบำรุงรักษา หรือเกิดช่องโหว่ของโปรแกรม	๖	การถ่ายโอนความเสี่ยง	<ul style="list-style-type: none"> - ติดตั้ง Patch ของระบบปฏิบัติการ - Update Software ระบบต่าง ๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์เป็นประจำ - มีการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่อง

ลำดับที่	รหัส	ปัจจัยเสี่ยง	ค่าระดับความเสี่ยง	การตอบสนองความเสี่ยง	แนวทางการดำเนินการจัดการ/ควบคุมความเสี่ยง
๘	๐๑๔	เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับหรือไม่สามารถให้บริการได้	๖	การถ่ายโอนความเสี่ยง	<ul style="list-style-type: none"> - มีแผนการบำรุงรักษา ตรวจสอบ และซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการจ้างผู้เชี่ยวชาญภายนอก (Outsource) ที่มีความเชี่ยวชาญเพื่อบำรุงรักษาระบบ - มีการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่อง
๙	๐๒๔	การเชื่อมโยงอีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	๖	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none"> - จัดอบรมให้ความตระหนักรู้แก่เจ้าหน้าที่ในองค์กร - มีการแจ้งข่าวสารให้เจ้าหน้าที่ในองค์กรทราบเมื่อมีการพบเจออีเมลหรือหน้าเว็บไซต์หลอกลวง
๑๐	๐๑	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	๕	การถ่ายโอนความเสี่ยง	<ul style="list-style-type: none"> - ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิงอัตโนมัติ สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งานเป็นประจำ - มีการจัดจ้างผู้เชี่ยวชาญเพื่อดำเนินการบำรุงรักษา
๑๑	๐๔	เกิดสถานการณ์ภัยพิบัติ/ ความไม่สงบทางการเมือง/ ชุมชนุมประท้วง	๕	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none"> - จัดทำ/ทบทวน แผนเตรียมความพร้อมกรณีเหตุฉุกเฉิน (IT Contingency Plan) ให้เป็นปัจจุบัน - จัดทำ/ทบทวน แผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ด้านสารสนเทศให้เป็นปัจจุบัน
๑๒	๐๕	การถูกบุกรุกหรือเข้าถึงพื้นที่หวงห้าม	๕	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none"> - มีการควบคุมทางกายภาพเพื่อควบคุมการเข้าถึงพื้นที่หวงห้าม เช่น ระบบ Access Control และระบบ CCTV
๑๓	๐๗	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่าย และเครือข่ายคอมพิวเตอร์ สนข.	๕	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none"> - มีแผนการบำรุงรักษา ตรวจสอบ และซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตามและรายงานผล - จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ
๑๔	๐๒๖	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๕	การจัดการ/ การควบคุมความเสี่ยง	<ul style="list-style-type: none"> - มีการกำหนดให้ระบบทำการออกจากระบบเมื่อผู้ใช้ไม่มีการเคลื่อนไหวตามระยะเวลาที่กำหนด - อบรมและสร้างความตระหนักรู้ถึงความสำคัญในการออกจากระบบเมื่อไม่ได้ใช้งานระบบ

ลำดับที่	รหัส	ปัจจัยเสี่ยง	ค่าระดับความเสี่ยง	การตอบสนองความเสี่ยง	แนวทางการดำเนินการจัดการ/ควบคุมความเสี่ยง
๑๕	O๖	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์ เทคโนโลยีและการสื่อสาร	๔	การจัดการ/ การควบคุมความเสี่ยง	- จัดทำทะเบียนครุภัณฑ์ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และระบบสารสนเทศสำคัญของ สนข.
๑๖	O๑๓	ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบฐานข้อมูลไม่เพียงพอ	๔	การจัดการ/ การควบคุมความเสี่ยง	- คอยตรวจสอบทรัพยากรของระบบคอมพิวเตอร์แม่ข่ายเป็นประจำ - กำหนดแนวทางการบริหารจัดการทรัพยากร เช่น ขนาดของไฟล์ในการจัดเก็บ
๑๗	O๘	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศในทุก ๆ ระดับผู้ใช้งาน	๓	การจัดการ/ การควบคุมความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับ - มีการทบทวนสิทธิ์การเข้าใช้งานเป็นประจำทุก ๖ เดือน หรือเมื่อมีการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข
๑๘	O๑๒	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๓	การจัดการ/ การควบคุมความเสี่ยง	- มีการทำ VPN สำหรับผู้ปฏิบัติงานที่มีความต้องการเข้าถึงระบบในการเข้าถึง - มีนโยบายและแนวปฏิบัติในการเข้าถึงระบบจากระยะไกล
๑๙	O๒๐	การนำเข้าข้อมูลผิดพลาดไม่ครบถ้วน หรือไม่ปัจจุบัน	๓	ยอมรับความเสี่ยง	- มีการตรวจสอบข้อมูลให้ถูกต้องก่อนนำเข้าข้อมูลสู่ระบบ - ตรวจสอบและแก้ไขข้อผิดพลาดของระบบหากพบเจอความผิดพลาด (Bug) ของโปรแกรม - มีการตรวจสอบข้อมูลที่ได้เคยนำเข้าสู่ระบบไปแล้ว โดยปรับปรุงข้อมูลให้ถูกต้องและเป็นปัจจุบัน
๒๐	O๒๑	การจ้างบุคคลภายนอก ที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๓	ยอมรับความเสี่ยง	- มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) ให้ชัดเจน และตรงตามความต้องการ - มีการติดตามงานของบุคลากรภายนอก (Outsource) และตรวจสอบการทำงานก่อนตรวจรับงาน - มีเจ้าหน้าที่ในการควบคุมดูแลการปฏิบัติงานของบุคลากรภายนอก (Outsource) - มีการติดตามเพื่อป้องกันการผิดพลาดและให้เกิดการแก้ไขปัญหาได้ทันที

ลำดับที่	รหัส	ปัจจัยเสี่ยง	ค่าระดับความเสี่ยง	การตอบสนองความเสี่ยง	แนวทางการดำเนินการจัดการ/ควบคุมความเสี่ยง
๒๑	O๓	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการ ศูนย์ข้อมูล (Data Center) และระบบเครือข่ายคอมพิวเตอร์ ของ สนข.	๒	ยอมรับความเสี่ยง	<ul style="list-style-type: none"> - ติดตั้งระบบเฝ้าระวังอุณหภูมิและความชื้น - ตรวจสอบความพร้อมใช้งานของระบบปรับอากาศ แบบควบคุมความชื้นให้อยู่ในสถานะพร้อมใช้งานเป็นประจำ - มีการจัดจ้างผู้เชี่ยวชาญเพื่อดำเนินการบำรุงรักษา
๒๒	O๙	ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	๒	ยอมรับความเสี่ยง	<ul style="list-style-type: none"> - มีระบบเครือข่ายสำรองในการให้บริการ - มีการตรวจสอบการเข้าถึงระบบเครือข่าย - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแลการใช้งาน ของผู้ใช้งานภายในหน่วยงาน - มีการบำรุงรักษาและแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก - กำหนดแบ่งช่วง IP Address สำหรับอุปกรณ์ที่เชื่อมต่อเครือข่าย - การติดตั้งสายสัญญาณให้เพียงพอต่อการใช้งาน - มีการตัดสัญญาณเมื่อไม่ได้ใช้งานระบบเป็นระยะเวลานาน (Session Timeout)
๒๓	O๒๒	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยี อย่างไม่เพียงพอ	๒	ยอมรับความเสี่ยง	<ul style="list-style-type: none"> - ส่งเสริมให้มีอบรม/การสอบมาตรฐานวิชาชีพด้านไอที - การให้บุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญ เฉพาะด้านอบรมให้แก่บุคลากรไอทีของหน่วยงาน - ส่งเสริมบุคลากรไอทีติดตามและเรียนรู้เกี่ยวกับเทคโนโลยีใหม่
๒๔	O๒๕	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกัน กับบุคคลน่าสงสัย	๒	ควบคุมความเสี่ยง	<ul style="list-style-type: none"> - มีการตรวจสอบการเข้าถึงระบบเครือข่าย - มีระบบการยืนยันตัวตนเมื่อมีการเข้าใช้งานเครือข่าย - มีการแบ่งระบบเครือข่าย - มีการติดตามและเฝ้าระวังผู้ใช้งานระบบเครือข่าย
๒๕	O๒๗	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๒	ยอมรับความเสี่ยง	<ul style="list-style-type: none"> - หน่วยงานวิเคราะห์งบประมาณ ต้องมีการดำเนินการตัด ปรับลด โดยมีการจัดทำความเสี่ยงและการ ให้น้ำหนัก ของความสำคัญของโครงการที่ใช้หมวดเงินประเภทเดียวกัน - ปรับลดโครงการตามลำดับความสำคัญ - ปรับแผนการดำเนินงานตามแผนการใช้จ่ายงบประมาณตาม งวดงานที่ได้รับ

ลำดับที่	รหัส	ปัจจัยเสี่ยง	ค่าระดับความเสี่ยง	การตอบสนองความเสี่ยง	แนวทางการดำเนินการจัดการ/ควบคุมความเสี่ยง
๒๖	O๑๐	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑	ยอมรับความเสี่ยง	- มีระบบการยืนยันตัวตนเมื่อมีการใช้งานเครือข่าย - มีการแบ่งระบบเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์แบบพกพา
๒๗	O๑๑	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	๑	ยอมรับความเสี่ยง	- ทำการตรวจสอบลักษณะของงานเพื่อจัดหาอุปกรณ์ที่เหมาะสมกับลักษณะการใช้งาน
๒๘	O๒๘	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนดิจิทัล	๑	ยอมรับความเสี่ยง	- ทบทวนการดำเนินงานโครงการให้เป็นไปตามแผน หากไม่เป็นไปตามแผนต้องปรับแผนการดำเนินโครงการ
๒๙	O๒๙	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน/อนุมัติโครงการล่าช้า	๑	ยอมรับความเสี่ยง	- จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด - รับผิดชอบและติดตามการอนุมัติให้ดำเนินโครงการให้เป็นไปตามแผน หากไม่เป็นไปตามแผนต้องเร่งดำเนินการ - กรณีพบปัญหาในการดำเนินการให้รีบแจ้งผู้บริหารเพื่อหาวิธีแก้ไขโดยเร่งด่วน - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด
๓๐	O๓๐	ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	๑	ยอมรับความเสี่ยง	- ติดตามกฎหมาย ประกาศ และระเบียบที่เกี่ยวข้อง - จัดลำดับความสำคัญและวางแผนการดำเนินงานให้สอดคล้องและเป็นไปกฎหมายและระเบียบที่เกี่ยวข้อง
๓๑	O๓๑	การเปลี่ยนแปลงนโยบายด้านเทคโนโลยีสารสนเทศของหน่วยงาน	๑	ยอมรับความเสี่ยง	- ติดตามและปรับปรุงแผนการดำเนินงานให้สอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศของหน่วยงาน

๓.๕ การจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

จากการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. มีรายการ/กิจกรรม ที่มีความเสี่ยงระดับ “สูงมาก” จำนวน ๓ กิจกรรม ซึ่งเป็นความเสี่ยงที่อยู่ในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยทันที จึงควรนำมาพิจารณาจัดทำเป็นแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ดังนี้

ตารางที่ ๓-๕ รายการความเสี่ยงที่ควรพิจารณาดำเนินการ

ประเด็นความเสี่ยง/กิจกรรม	แนวทางจัดการ/ กิจกรรมควบคุม	เป้าหมาย/ผลสำเร็จ ของการดำเนินการกิจกรรม ตามแนวทางการจัดการความเสี่ยง
๐๑๘ ละเมิดลิขสิทธิ์โปรแกรม อรรถประโยชน์ (Utilities Program)	<ul style="list-style-type: none">- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศและการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย- กระตุ้นให้เกิดการปฏิบัติตามนโยบายหรือระเบียบฯ อย่างจริงจัง- ส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ OpenSource แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์- จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	<ul style="list-style-type: none">- เจ้าหน้าที่ของ สนข. มีความเข้าใจเกี่ยวกับโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย- เจ้าหน้าที่ของ สนข. มีความตระหนักและไม่ใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์- มีการจัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
๐๑๕ ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	<ul style="list-style-type: none">- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall- ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ- ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ- ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ- ติดตั้งโปรแกรมป้องกันไวรัส- ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ- เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	<ul style="list-style-type: none">- ระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายของ สนข. มีความมั่นคงปลอดภัย
๐๑๖ ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	<ul style="list-style-type: none">- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall- ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ- ตรวจสอบ ติดตาม และเฝ้าระวัง	<ul style="list-style-type: none">- ระบบสารสนเทศและฐานข้อมูลของ สนข. มีความมั่นคงปลอดภัย

ประเด็นความเสี่ยง/กิจกรรม	แนวทางจัดการ/ กิจกรรมควบคุม	เป้าหมาย/ผลสำเร็จ ของการดำเนินการกิจกรรม ตามแนวทางการจัดการความเสี่ยง
	<p>การบุกรุกเครือข่ายอย่างสม่ำเสมอ</p> <ul style="list-style-type: none">- ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ- ติดตั้งโปรแกรมป้องกันไวรัส- ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ- เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ- ทดสอบช่องโหว่ของโปรแกรม- กำหนดมาตรฐานในการพัฒนาโปรแกรมให้มีความปลอดภัย	

บทที่ ๔

สรุปผลและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) เป็นกระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงาน เพื่อลดความเสียหายอันเนื่องมาจากความเสี่ยงที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่งให้ได้มากที่สุด เมื่อเทคโนโลยีเข้ามามีบทบาทสำคัญในการขับเคลื่อนการดำเนินการขององค์กร ส่งผลให้มีข้อมูลจำนวนมากถูกส่งผ่านระบบเครือข่ายเทคโนโลยีสารสนเทศขององค์กร ในปัจจุบันข้อมูลมีคุณค่ามหาศาลและเป็นที่ต้องการของบุคคลหรือองค์กรต่าง ๆ ข้อมูลขององค์กรจึงมีความเสี่ยงต่อการถูกทำให้เสียหาย หรือนำไปใช้ในทางที่ผิด

สนข. จึงต้องมีการจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Risk Management) ของ สนข. ขึ้นเพื่อนำผลที่ได้จากการประเมินความเสี่ยงไปใช้เป็นกรอบแนวทางในการบริหารจัดการความเสี่ยง และแก้ไขปัญหาด้านเทคโนโลยีสารสนเทศในสถานการณ์ความเสี่ยงต่าง ๆ ได้อย่างเหมาะสม รวมถึงต้องมีการจัดทำแผนการตรวจสอบความเสี่ยง เพื่อใช้เป็นแนวทางการตรวจประเมินความเสี่ยงให้มีความสอดคล้องกับการประเมินความเสี่ยง และทราบถึงความเสี่ยงที่มีอยู่หรือความเสี่ยงที่ยังต้องควบคุมความเสี่ยงต่อไป ทั้งนี้ การบริหารจัดการความเสี่ยงจะส่งผลให้ลดโอกาส/ความเสียหายที่จะเกิดขึ้นให้อยู่ในระดับที่ยอมรับได้ และควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ไม่ให้เพิ่มขึ้นไปในระดับที่ไม่สามารถยอมรับได้

๔.๑ วัตถุประสงค์

เพื่อประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข. และนำผลที่ได้จากการประเมินไปจัดทำเป็นแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. โดยมีวัตถุประสงค์ ดังนี้

๔.๑.๑ เตรียมความพร้อมเพื่อรองรับสถานการณ์ฉุกเฉิน (Contingency Event) ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและฐานข้อมูลสารสนเทศของ สนข.

๔.๑.๒ เป็นแนวทางหรือขั้นตอนปฏิบัติในการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและฐานข้อมูลสารสนเทศของ สนข. ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งานอย่างต่อเนื่อง

๔.๑.๓ มีแนวทางการบริหารจัดการความเสี่ยงอย่างเป็นระบบแบบแผนมีความต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีในกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติต่าง ๆ

๔.๒ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk Identification) จะเป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่หน่วยงานเผชิญอยู่ ซึ่งนำไปสู่การพิจารณากำหนดเป็นแผนหรือแนวทางปฏิบัติ เพื่อเร่งควบคุมความเสี่ยงที่มีผลกระทบอยู่ในระดับความเสี่ยง “สูงมาก” ทั้ง ๓ รายการ ดังนี้

ตารางที่ ๔-๑ แนวทางปฏิบัติในการจัดการรายการความเสี่ยงระดับสูงมาก

ความเสี่ยง	แนวทางปฏิบัติ
๐๑๘ ละเมิดลิขสิทธิ์โปรแกรมมัลแวร์ (Utilities Program)	<ul style="list-style-type: none"> - จัดให้มีการอบรมสร้างความตระหนักรู้ในเรื่องนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามนโยบายฯ อย่างจริงจัง - ส่งเสริมให้ใช้โปรแกรมมัลแวร์แบบ OpenSource แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - วางแนวทางจัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมายมาใช้ปฏิบัติงานภายใน สนข.
๐๑๙ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	<ul style="list-style-type: none"> - ติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายอย่างสม่ำเสมอ - ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส - ติดตั้ง/อัปเดต Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
๐๒๐ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	<ul style="list-style-type: none"> - ติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายอย่างสม่ำเสมอ - ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส - ติดตั้ง/อัปเดต Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ทดสอบช่องโหว่ของโปรแกรม - กำหนดมาตรฐานในการพัฒนาโปรแกรมให้มีความปลอดภัย

๔.๓ ข้อเสนอแนะ

เพื่อให้การบริหารจัดการความเสี่ยงฯ ของ สนข. สามารถดำเนินการไปได้อย่างเป็นระบบและได้ผลเป็นที่ประจักษ์ สนข. จึงควรมีการประเมินความเสี่ยงและจัดทำเป็นรายงานการประเมินความเสี่ยงเป็นประจำทุกปี เพื่อให้สามารถนำผลการประเมินความเสี่ยงไปทบทวนและปรับปรุงแผนบริหารความเสี่ยงให้มีความสอดคล้องกับสถานการณ์ความเสี่ยงปัจจุบัน โดยมีการเพิ่มลดรายการความเสี่ยงในส่วนรายการที่ได้ดำเนินการควบคุมความเสี่ยงแล้ว หรือรายการที่เป็นความเสี่ยงเกิดขึ้นใหม่ พร้อมทั้งมีการติดตามความเสี่ยงรายการ ที่อยู่ในระดับความเสี่ยงที่ไม่สามารถยอมรับได้จากแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. เพื่อติดตามและควบคุมให้ระดับความเสี่ยงมีความรุนแรงลดลงอยู่ในระดับที่สามารถยอมรับได้

เอกสารอ้างอิง

๑. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗
๒. แผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ผู้จัดทำร่าง

๑. นายพิสิฐ คุ้มทอง
นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. นายทรงเกียรติ ตะเภาทอง
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

ที่ปรึกษา

๑. นางสาวจิรัช ห้วยหงษ์ทอง
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. นายนฤทีร์ มัยรัตน์
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร