กรมการขนส่งทางราง
Department of Rail Transport

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กองยุทธศาสตร์และแผนงาน

514/1 Lan Luang Rd.,
Si Yaek Maha Nak,
Dusit, Bangkok 10300

https://www.drt.go.th/

Facebook/DRT.OfficialFanpage

สารบัญ

หน้า

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

กรมการขนส่งทางราง (ขร.) เป็นหน่วยงานที่มีภารกิจเกี่ยวกับการเสนอแนะนโยบาย ยุทธศาสตร์และแผนการพัฒนาด้านการขนส่งทางราง ตลอดจนการกำกับดูแลมาตรฐานและระเบียบด้านความปลอดภัยและบำรุงทาง และการประกอบกิจการ วางแผนโครงข่าย พัฒนาโครงสร้างพื้นฐานทางรางของประเทศให้มีความสมบูรณ์ครอบคลุมทั่วประเทศ โดยในปัจจุบันได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อสนับสนุนการบริหารจัดการภายในหน่วยงาน การบูรณาการข้อมูลระหว่างหน่วยงาน และอยู่ระหว่างการพัฒนาระบบสารสนเทศเพื่อรองรับการให้บริการประชาชน ตลอดจนการรวบรวมข้อมูลจากหน่วยงานภายใต้การกำกับดูแลของ ขร. รวมถึงการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้สามารถรองรับภารกิจต่าง ๆ ของหน่วยงาน และด้วยความก้าวหน้าทางเทคโนโลยีที่เพิ่มขึ้นอย่างรวดเร็ว ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนไปความเป็นดิจิทัลที่เพิ่มขึ้น กรมการขนส่งทางราง อาจเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบในทางลบต่อหน่วยงานและวัตถุประสงค์ทางธุรกิจ ดังนั้น เพื่อเป็นแนวทางป้องกันปัญหา และการเฝ้าระวังภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศภายในหน่วยงาน ขร. จึงได้จัดทำการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ – ๒๕๖๙ ขึ้น เพื่อเป็นแนวทางในการดำเนินงานของหน่วยงาน

๑.๒ วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และระบบเทคโนโลยีสารสนเทศของกรมการขนส่งทางราง ให้มั่นใจได้ว่าความเสี่ยงของระบบสารสนเทศของ ขร. ได้ถูกพิจารณาและได้มีการจัดเตรียมมาตรการในการควบคุมความเสี่ยงที่เหมาะสม เพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้นกับ ขร.ได้

๑.๓ เป้าหมาย

๑.๓.๑ ผู้บริหารและผู้ปฏิบัติงาน มีความรู้ความเข้าใจในเรื่องการบริหารความเสี่ยง เพื่อนำไปใช้ในการดำเนินงานตามยุทธศาสตร์ และแผนการปฏิบัติงานประจำปีให้บรรลุตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๑.๓.๒ ผู้บริหารและผู้ปฏิบัติงาน สามารถระบุความเสี่ยง วิเคราะความมเสี่ยง ประเมินความเสี่ยงและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๑.๓.๓ สามารถนำแผนบริหารความสี่ยงไปใช้ในการบริหารงานที่รับผิดชอบ

๑.๓.๔ เพื่อพัฒนาความสามารถของบุคลากรและกระบวนการดำเนินงานภายใน ขร. อย่างต่อเนื่อง

๑.๓.๕ ความรับผิดชอบต่อความเสี่ยงและการบริหารความเสี่ยงถูกกำหนดขึ้นอย่างเหมาะสมครอบคลุม

๑.๓.๖ การบริหารความเสี่ยงได้รับการปลูกฝังให้เป็นวัฒนธรรม ขร.

๑.๔ ขอบเขตการดำเนินงาน

ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. ได้แก่ ด้านโครงสร้างพื้นฐานด้านระบบสารสนเทศ และด้านฐานข้อมูลของ ขร.

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 องค์กรสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้ ขร. เกิดความเสียหาย

บทที่ ๒
การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑ คำนิยาม

ระบบเทคโนโลยีสารสนเทศ หมายถึง เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ อิเล็กทรอนิกส์ อินเทอร์เน็ต อุปกรณ์โทรคมนาคม และบริการทางคอมพิวเตอร์

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า"การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงระดับหน่วยงานของหน่วยงาน โดยการประเมินความเสี่ยง หน่วยงานจะสามารถ:

- ระบุเหตุการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจากการกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในหน่วยงาน การประเมินความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้พนักงานมีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยีและวิธีที่พนักงานดังกล่าวปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

๒.๒ คำนิยามความเสี่ยง

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว ลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงินและการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

การประเมินความเสี่ยง หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

การวิเคราะห์ความเสี่ยง หลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นต่อไปคือ การวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธีเนื่องจากการวัดความเสี่ยงเป็นตัวเลขว่ามีผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก โดยทั่วไปจะวิเคราะห์ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสี่ยง และความถี่ที่จะเกิดหรือโอกาสที่จะเกิดความเสี่ยง

การบริหารความเสี่ยง หมายถึง การบริหารปัจจัยและควบคุมกิจกรรมรวมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดเหตุจากโอกาสที่จะทำให้เกิดความเสียหายจากการดำเนินงานไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายของหน่วยงานเป็นสำคัญ

๒.๓ กระบวนการบริหารจัดการความเสี่ยง

๒.๓.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องของโครงการหรือกิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายในและภายนอกองค์กร

วิธีการระบุความเสี่ยงมีหลายวิธี เช่น

๒.๓.๑.๑ การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๒.๓.๑.๒ การใช้ Checklist

๒.๓.๑.๓ การวิเคราะห์สถานการณ์จากการตั้งคำถาม 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) ซึ่งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต้องกำหนดเกณฑ์ขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก (รุนแรงมากที่สุด) สูง (ค่อนข้างรุนแรง) ปานกลาง น้อย และน้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็น ๔ ระดับ (สูง ค่อนข้างสูง ค่อนข้างต่ำ และต่ำ)

๒.๓.๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยที่ระบุไว้มาประกอบโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรง หรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงจะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินผลกระทบ (ความน่าเชื่อถือ/ความพึงพอใจของผู้ใช้บริการ) ดังนี้

ผลกระทบที่จะเกิด	ความเสียหายที่เกิดขึ้น		ระดับคะแนน
	เชิงคุณภาพ	เชิงปริมาณ	
สูงมาก	มีการสูญเสียทรัพย์สินอย่างมาก ผู้บริหารถูกลงโทษทางวินัย	มากกว่า ๑,๐๐๐,๐๐๐ บาท	๕
สูง	มีการสูญเสียทรัพย์สินอย่างมาก ผู้บริหารถูกตำหนิหรือถูกร้องเรียน	มากกว่า ๒๐๐,๐๐๐ บาท ถึง ๑,๐๐๐,๐๐๐ บาท	๔
ปานกลาง	มีการสูญเสียทรัพย์สินมาก เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย	มากกว่า ๕๐,๐๐๐ บาท ถึง ๒๐๐,๐๐๐ บาท	๓
น้อย	มีการสูญเสียทรัพย์สินพอสมควร เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ	มากกว่า ๑๐,๐๐๐ บาท ถึง ๕๐,๐๐๐ บาท	๒
น้อยมาก	มีการสูญเสียทรัพย์สินเล็กน้อย แทบไม่มีผลกระทบเลย	น้อยกว่า ๑๐,๐๐๐ บาท	๑

ที่มา : แผนบริหารความเสี่ยงสถาบันสารสนเทศทรัพยากรน้ำ (องค์การมหาชน) ปีงบประมาณ พ.ศ. ๒๕๖๔

เกณฑ์การประเมินโอกาสของการประเมินความเสี่ยง ดังนี้

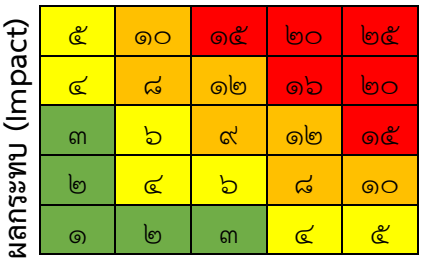
โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้นของความเสี่ยง	ระดับคะแนน
	เชิงปริมาณ	
สูงมาก	มากกว่า ๑ ครั้งต่อเดือน	๕
สูง	ระหว่าง ๑-๖ เดือนต่อครั้ง	๔
ปานกลาง	ระหว่าง ๖-๑๒ เดือนต่อครั้ง	๓
น้อย	มากกว่า ๑ ปีต่อครั้ง	๒
น้อยมาก	มากกว่า ๕ ปีต่อครั้ง	๑

๒.๓.๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงที่จะต้องบริหารจัดการความเสี่ยงก่อน

ระดับความเสี่ยง	ระดับสี	คำอธิบาย	คะแนน
สูง		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	๑๕ - ๒๕
ค่อนข้างสูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป	๘ – ๑๔
ค่อนข้างต่ำ		ระดับที่พอยอมรับได้ แต่ต้องการมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	๔ – ๗
ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม	๑ - ๓

ที่มา : แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๔

การประเมินความเสี่ยง



ที่มา : แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๔

๒.๓.๒.๔ การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้แล้ว เลือกความเสี่ยงที่มีระดับสูงหรือค่อนข้างสูงมาจัดทำแผนการบริหารความเสี่ยง

๒.๔ คำนิยามความเสี่ยง

๒.๔.๑ ความเสี่ยง (Risk)

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และ จะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว ลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงินและการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ลักษณะของความเสี่ยง สามารถแบ่งออกได้เป็น ๓ ส่วน ดังนี้

๑) ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง
๒) เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงาน หรือ นโยบาย
๓) ผลกระทบของความเสี่ยง คือ ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

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

๒.๔.๓ การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุมการยกเลิกและการโอนย้ายหรือแบ่งความเสี่ยง

๒.๔.๔ การควบคุม (Control) หมายถึง นโยบาย แนวทำงานหรือขั้นตอนการปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะและการควบคุมเพื่อการแก้ไข

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

๒.๕ หลักการวิเคราะห์ ประเมิน การจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Tread way Commission) มีดังนี้

๒.๕.๑ การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

เป็นการกำหนดวัตถุประสงค์ของการดำเนินการบริหารจัดการความเสี่ยง ซึ่งจะต้องสอดคล้องกับวิสัยทัศน์ พันธกิจ และยุทธศาสตร์การดำเนินงานขององค์กร ตั้งแต่ระดับองค์กร หน่วยงาน กิจกรรม จนถึงระดับบุคคล เพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าประสงค์ และเพื่อเพิ่มประสิทธิภาพในการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานฯ ที่น่าจะส่งผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย โดยพิจารณาหาแนวทางในการป้องกัน หรือจัดการกับความเสี่ยงเหล่านั้นก่อนที่จะเริ่มปฏิบัติงาน หรือ ดำเนินกิจการตามแผนที่กำหนดไว้ สำหรับวัตถุประสงค์ของการบริหารความเสี่ยงอาจแบ่งออกได้เป็น ๒ ระดับ คือ

๑) วัตถุประสงค์ระดับองค์กร (Corporate Objective) เป็นวัตถุประสงค์ของการดำเนินงานในภาพรวม ตามแผนยุทธศาสตร์และแผนปฏิบัติราชการประจำปีขององค์กร

๒) วัตถุประสงค์ระดับกิจกรรม (Activities Objective) เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจงลงไป สำหรับแต่ละกิจกรรมที่องค์กรกำหนดเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การกำหนดวัตถุประสงค์ที่ชัดเจนช่วยให้การระบุและวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นได้อย่างครบถ้วน ซึ่งวัตถุประสงค์ที่กำหนดขึ้นในแต่ละระดับ ควรมีการกำหนดเป้าหมายและตัวชี้วัดความสำเร็จและสามารถวัดผลได้วัตถุประสงค์ที่ดี (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

๒.๕.๒ การระบุความเสี่ยงต่าง ๆ (Event Identification)

นอกจากการกำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารตามแนวทางของ COSO ออกเป็น ๘ ประเภทแล้ว การระบุความเสี่ยงยังต้องนำหลักธรรมาภิบาลมาเป็นปัจจัยในการวิเคราะห์และระบุความเสี่ยง เพื่อให้เป็นไปตามแนวทางการบริหารกิจการบ้านเมืองที่ดี ประกอบด้วย ๑๐ ประการ ดังนี้

๑) หลักประสิทธิผล (Effectiveness) หมายถึง ผลการปฏิบัติราชการที่บรรลุวัตถุประสงค์และเป้าหมายของแผนปฏิบัติราชการที่ได้รับงบประมาณมาดำเนินการ โดยการปฏิบัติราชการจะต้องมีทิศทางยุทธศาสตร์ และเป้าประสงค์ที่ชัดเจน มีกระบวนการปฏิบัติงาน และระบบงานที่เป็นมาตรฐาน รวมถึงการติดตาม ประเมินผล และพัฒนาปรับปรุงอย่างต่อเนื่องและเป็นระบบ

๒) หลักประสิทธิภาพ (Efficiency) หมายถึง การบริหารราชการตามแนวทางการกำกับดูแลที่ดี มีการออกแบบกระบวนการปฏิบัติงาน โดยการใช้เทคนิคและเครื่องมือการบริหารจัดการที่เหมาะสม ให้องค์กรสามารถใช้ทรัพยากรทั้งด้านต้นทุน แรงงาน และระยะเวลาให้เกิดประโยชน์สูงสุดต่อการพัฒนาขีดความสามารถในการปฏิบัติราชการตามภารกิจ เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกกลุ่ม

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

๔) หลักภาระรับผิดชอบ (Accountability) หมายถึง การแสดงความรับผิดชอบในการปฏิบัติหน้าที่ และผลงานต่อเป้าหมายที่กำหนดไว้ โดยความรับผิดชอบนั้นควรอยู่ในระดับที่สนองต่อความคาดหวังของสาธารณะ รวมทั้งการแสดงถึงความสำนึกในการรับผิดชอบต่อปัญหาสาธารณะ

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

๖) หลักการมีส่วนร่วม (Participation) หมายถึง กระบวนการที่ข้าราชการ ประชาชน และผู้มีส่วนได้ส่วนเสียทุกกลุ่มมีโอกาสได้เข้าร่วมรับรู้ เรียนรู้ ทำความเข้าใจ ร่วมแสดงทักษะ ร่วมเสนอปัญหา/ประเด็นที่สำคัญที่เกี่ยวข้อง ร่วมคิดแนวทาง ร่วมการแก้ไขปัญหา ร่วมในกระบวนการตัดสินใจ และร่วมกระบวนการพัฒนาในฐานะหุ้นส่วนพัฒนา

๗) หลักการกระจายอำนาจ (Decentralization) หมายถึง การถ่ายโอนอำนาจการตัดสินใจ การมอบอำนาจและความรับผิดชอบในการตัดสินใจ และการดำเนินการให้แก่บุคลากร โดยมุ่งเน้นการสร้างความพึงพอใจในการให้บริการต่อผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย การปรับปรุงกระบวนการเพิ่มผลิตภาพเพื่อผลการดำเนินงานที่ดีของส่วนราชการ

๘) หลักนิติธรรม (Rule of Law) หมายถึง การใช้อำนาจของกฎหมาย กฎระเบียบข้อบังคับในการบริหารราชการด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของผู้มีส่วนได้ส่วนเสีย

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

๑๐) หลักมุ่งเน้นฉันทามติ (Consensus Oriented) หมายถึง การหาข้อตกลงทั่วไปภายในกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ซึ่งเป็นข้อตกลงที่เกิดจากการใช้กระบวนการ เพื่อหาข้อคิดเห็นจากกลุ่มบุคคลที่รับประโยชน์ และเสียประโยชน์ โดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง ซึ่งต้องไม่มีข้อคัดค้านที่ยุติไม่ได้ในประเด็นที่สำคัญ โดยฉันทามติไม่จำเป็นต้องหมายความว่าเป็นความเห็นพ้องโดยเอกฉันท์

๒.๖ การประเมินความเสี่ยง (Risk Assessment)

เป็นขั้นตอนในการใช้หลักเกณฑ์การให้คะแนนจากระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) มาเป็นเครื่องมือในการประเมินความเสี่ยง และกำหนดกลยุทธ์ที่ใช้จัดการกับความเสี่ยง โดยแบ่งการจัดระดับความเสี่ยง (Degree of Risk) ออกเป็น ๔ ระดับตามระดับคะแนน ได้แก่ ระดับความเสี่ยงต่ำ ระดับความเสี่ยงปานกลาง ระดับความเสี่ยงสูง และระดับความเสี่ยงสูงมาก ซึ่งการจัดทำแผนผังระดับความเสี่ยง (Risk Matrix) จะช่วยในการตัดสินใจในการวางแผนความเสี่ยงได้อย่างเหมาะสม และสามารถจัดลำดับความสำคัญในการจัดการได้ ซึ่งการประเมินความเสี่ยงด้วยวิธีการแบ่งการจัดระดับความเสี่ยงมีขั้นตอนดังนี้

๑) การประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood : L) เป็นขั้นตอนการประเมินความเป็นไปได้ความถี่ หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง แล้วจัดแบ่งระดับของโอกาสที่เกิดความเสี่ยง (Likelihood) ออกเป็น ๕ ระดับ ตามตารางที่ ๑

ระดับโอกาส	คำนิยาม
๑	นาน ๆ ครั้ง (แทบไม่เกิดขึ้นเลย)
๒	ไม่บ่อย (อาจเกิดขึ้นได้ทุก ๕ ปี)
๓	ปานกลาง (อาจเกิดขึ้นได้ทุกปี)
๔	บ่อย (อาจเกิดขึ้นได้ทุกเดือน)
๕	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

ตารางที่ ๑ โอกาสจะเกิดความเสี่ยง

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

ผลกระทบ	คำนิยาม
๑	- เกิดเหตุที่ไม่มีความสำคัญ - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการน้อยมาก (แทบไม่มีผลกระทบเลย)
๒	- เกิดเหตุที่แก้ไขได้ - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการน้อย (เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ)
๓	- ระบบ IT มีปัญหา และมีความสูญเสียไม่มาก - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)
๔	- เกิดปัญหากับระบบ IT ที่สำคัญและระบบความปลอดภัย ซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการมาก (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)
๕	- เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูล - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการมากที่สุด (ผู้บริหารถูกลงโทษทางวินัย)

ตารางที่ ๒ ผลกระทบจากความเสี่ยง

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

๒.๗ กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

เป็นการวิเคราะห์ทางเลือกกลยุทธ์ในการจัดการความเสี่ยง เพื่อช่วยในการตัดสินใจของบุคคลหรือองค์กรใด ๆ ในอันที่จะหาวิธีการที่ดีที่สุดในการตัดสินใจแก้ไขปัญหาต่าง ๆ ที่อาจเกิดขึ้นในอนาคต ทั้งนี้เพื่อลดผลกระทบหรือความเสียหายที่อาจเกิดขึ้นให้น้อยที่สุด โดยมีค่าใช้จ่ายน้อยที่สุด ซึ่งมีวิธีการจัดการ ดังนี้

๑) การยอมรับความเสี่ยง (Take/Risk Acceptance) หมายถึง การไม่กระทำใด ๆ เพิ่มเติม กรณีนี้ใช้กับความเสี่ยงที่มีน้อย มีความน่าจะเกิดน้อย หรือเห็นว่ามีต้นทุนในการบริหารความเสี่ยงสูง โดยขออนุมัติหลักการรับความเสี่ยงไว้

๒) การลด (Treat/Risk Reduction) หมายถึง การลดโอกาสที่จะเกิดความเสี่ยง การป้องกันการเกิดความสูญเสีย หรือลดผลกระทบจากเหตุการณ์ที่อาจเกิดขึ้นในอนาคต โดยการจัดระบบการควบคุม การกำหนดแผนสำรองในเหตุฉุกเฉิน การวิเคราะห์ข้อมูลในอดีต ปัจจุบัน ซึ่งรวมถึงการคาดการณ์ในอนาคตประกอบการตัดสินใจ

๓) การหลีกเลี่ยงความเสี่ยง (Terminate/Risk Avoidance) หมายถึง การหยุด หรือ การเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น การงดทำขั้นตอนที่ไม่จำเป็นและจำนำมาซึ่งความเสี่ยง หรือการปรับเปลี่ยนรูปแบบการทำงานและลดขอบเขตการดำเนินการ เป็นต้น

๔) การกระจาย (Transfer/Risk Sharing) หรือโอนความเสี่ยง (Risk Spreading) หมายถึง การลดโอกาสความน่าจะเกิดหรือลดความเสียหายโดยการแบ่งโอน การหาผู้รับผิดชอบในความเสี่ยง การจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน แลการจัดประกันภัย เป็นต้น

๕) การลดความเสี่ยง (Risk Mitigate) หมายถึง การวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง : การใช้ไฟร์วอลล์เพื่อจำกัดทราฟฟิกเครือข่ายเป็นตัวอย่างในการลดความเสี่ยงของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในหน่วยงานจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกเป็นทางการ และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

แนวทางปฏิบัติที่ดีที่สุดสำหรับการลดความเสี่ยง (Best Practices For Risk Mitigation)

- Cybersecurity training programs
- Updating Software
- Privileged access management solutions
- Multi-factor access Authentification
- Dynamic data backup

๒.๘ กิจกรรมการบริหารความเสี่ยง (Control Activities)

เป็นขั้นตอนดำเนินการกำหนดกิจกรรม หรือมาตรการในการจัดการความเสี่ยงให้หมดไป หรือควบคุมความเสี่ยงให้ลดลงในระดับที่ยอมรับได้ โดยกิจกรรมที่กำหนดต้องเป็นกิจกรรมที่ยังไม่เคยปฏิบัติ หรือเป็นกิจกรรมที่กำหนดขึ้นเพิ่มเติมจากกิจกรรมเดิมที่เคยปฏิบัติอยู่แล้ว แต่กิจกรรมนั้นไม่สามารถควบคุมความเสี่ยงได้ นอกจากนี้ยังต้องกำหนดระยะเวลาที่ใช้ในการดำเนินการแต่ละกิจกรรม 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 และผลประโยชน์ที่คาดว่าจะได้รับ โดยกิจกรรมการควบคุมควรมีองค์ประกอบ ดังนี้

๑) วิธีการดำเนินงาน ซึ่งประกอบด้วยขั้นตอนและกระบวนการ

๒) การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น ซึ่งควรพิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน และพิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

๓) กำหนดระยะเวลาแล้วเสร็จของงาน

๒.๙ ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

เป็นขั้นตอนและกระบวนการโดยมีวัตถุประสงค์เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง มีการเปิดช่องทางการสื่อสาร และรับทราบข้อมูลด้านการบริหารความเสี่ยงให้กับผู้บริหารและบุคลากรขององค์กรได้เข้าถึง โดยผ่านช่องทางต่าง ๆ เช่น ระบบอินทราเน็ต หนังสือเวียน การประชุมชี้แจงโดยผู้บริหาร หรือการฝึกอบรม เป็นต้น ซึ่งการสื่อสารที่มีประสิทธิผลนั้น ต้องให้มั่นใจได้ว่า

๑) ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา

๒) ผู้บริหารสามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่ได้ทันท่วงที

๓) มีการติดตามแผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กรและจัดากรความเสี่ยงต่าง ๆ เพื่อให้องค์กรมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด

๒.๑๐ การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

การติดตาม และเฝ้าระวังความเสี่ยง โดยการกำหนดให้มีการติดตาม และประเมินผลว่าแต่ละหน่วยงานมีการประเมินประสิทธิผลของการจัดการความเสี่ยงที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ เพื่อให้เกิดความมั่นใจว่ามาตรการในการปรับปรุงความเสี่ยงที่วางไว้มีความเพียงพอ เหมาะสม มีประสิทธิภาพประสิทธิผล และมีการปฏิบัติจริง

สามารถลดหรือป้องกันความเสี่ยงที่อาจเกิดขึ้น นับเป็นขั้นตอนสุดท้ายและเป็นปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง ซึ่งควรพิจารณาประเด็นต่อไปนี้

๑) การรายงาน และสอบทานขั้นตอนตามกระบวนการบริหารความเสี่ยง เช่น การรายงานและติดตามผลระหว่างการดำเนินงาน (On Going Monitoring) เพื่อสังเกต ติดตาม รายงานความคืบหน้า รวมทั้งสอบทานหรือยืนยันผลระหว่างการปฏิบัติงาน

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

๒.๑๑ ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กรมการขนส่งทางรางได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๘ ประเภท ดังนี้

๒.๑๑.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

๒.๑๑.๒ ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งนั้น

๒.๑๑.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan และ Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

๒.๑๑.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

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

๒.๑๑.๕ ความเสี่ยงด้านระบบข้อมูล ((Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้ความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่ต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

๒.๑๑.๖ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่าง ๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

๒.๑๑.๗ ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

๒.๑๑.๘ ความเสี่ยงด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยง เนื่องจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

๒.๑๒ การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุกาณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้น

การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่าย เมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๒.๑๓ ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของกรมการขนส่งทางราง ได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๑.๖ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่าง ๆ จากผู้ใช้ภายใน ขร.

๒.๓ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๒.๑๔ การประเมินความเสียหาย

๒.๑๔.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒.๑๔.๒ ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๒.๑๕ การติดตามและรายงานผล

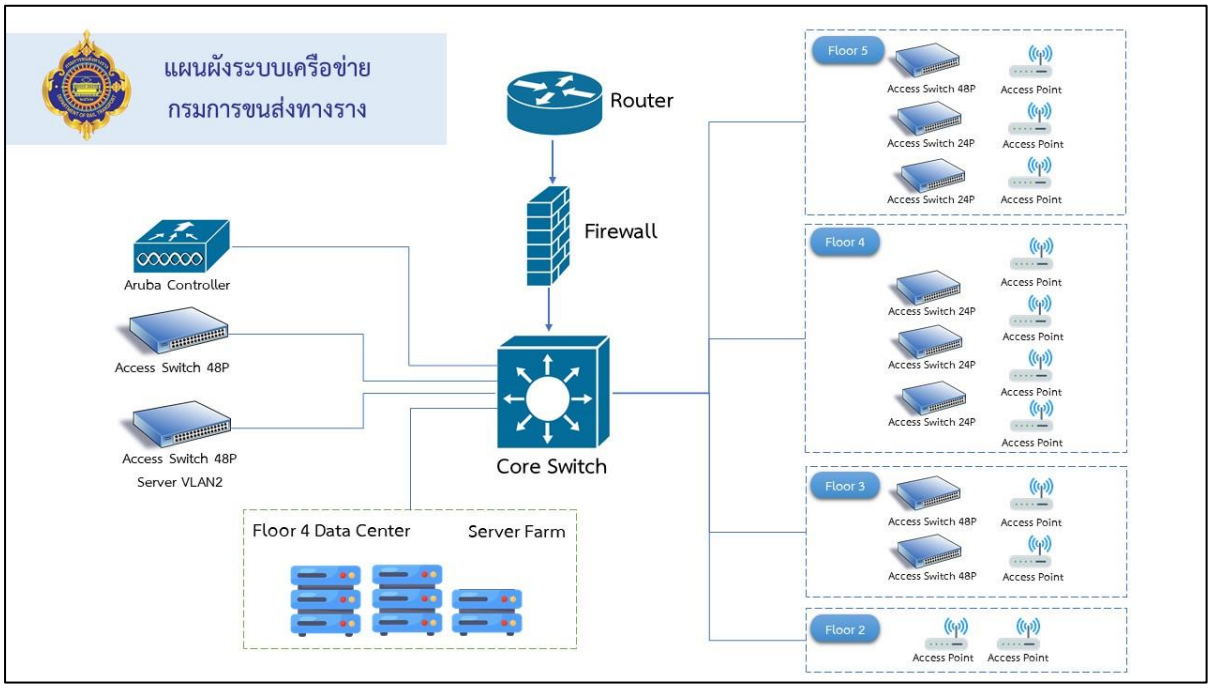
กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

๒.๑๖. ระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของ ขร.

ระบบเครือข่ายคอมพิวเตอร์ของ ขร. ได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) ของ ขร. ตั้งอยู่ที่ อาคาร ณ ถลาง ชั้น ๔ เลขที่ ๕๑๔/๑ ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กรุงเทพมหานคร และมีเครือข่ายเชื่อมโยงไปยังหน่วยงานในส่วนกลางกระทรวงคมนาคม เพื่อการสื่อสารข้อมูลคอมพิวเตอร์หรือการสื่อสารรูปแบบอื่นในอนาคต

ระบบเครือข่ายคอมพิวเตอร์ของ ขร. มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังระบบเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ในการกรองกลุ่มของข้อมูล (Package Filter) ที่ผ่านเข้ามาภายในระบบเครือข่ายคอมพิวเตอร์ส่วนกลางของ ขร. จากเครือข่ายภายนอก เช่น เครือข่ายของสำนักงานปลัดกระทรวงคมนาคม เครือข่ายอินเทอร์เน็ต เป็นต้น นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ที่ดูแลเครื่องแม่ข่ายทั้งหมดของ ขร. ให้บุคคลภายนอกเข้าถึงได้ เช่น Web Server และ Mail Server เป็นต้น รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของ ขร. เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ระบบเครือข่ายหลักของ ขร. (Core Network) ตั้งอยู่ที่กองยุทธศาสตร์และแผนงาน เป็นศูนย์กลางการเชื่อมต่อทำหน้าที่เชื่อมโยงระบบเครือข่ายภายในระดับสำนัก/กอง/กลุ่ม ในความเร็วระดับ ๑,๐๐๐ Mbps และระบบเครือข่ายภายนอก เช่น อินเทอร์เน็ตเข้าด้วยกัน เป็นต้น

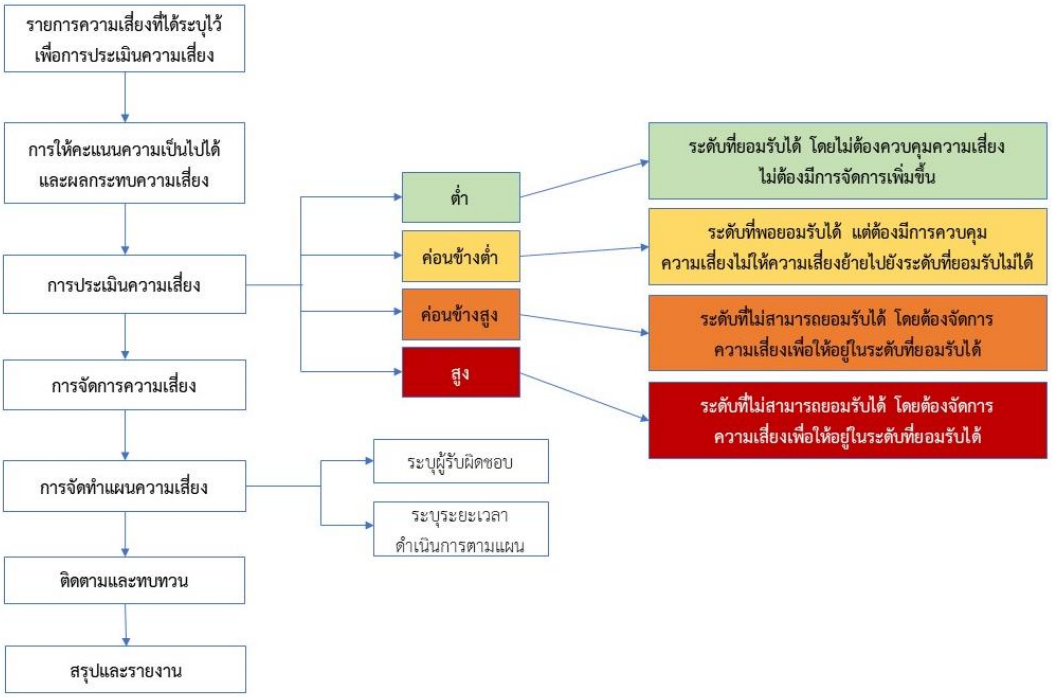
ผังระบบเครือข่ายกรมการขนส่งทางราง



บทที่ ๓
การวิเคราะห์การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

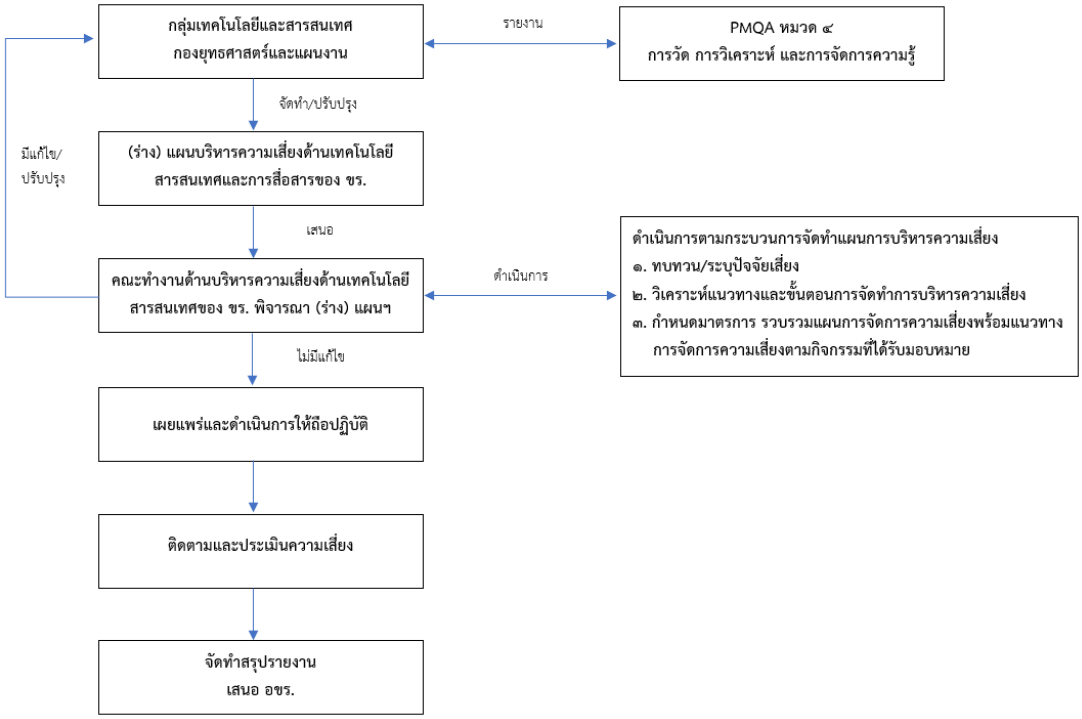
กรมการขนส่งทางราง ได้ตระหนักถึงความสำคัญของข้อมูลที่อยู่ภายใต้การดูแลของหน่วยงานที่อาจเกิดความเสียหายจากปัจจัยต่าง ๆ จึงได้มอบหมายให้กลุ่มเทคโนโลยีและสารสนเทศ (ยส.) จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของ ขร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ – ๒๕๖๘ โดยกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เริ่มต้นจากการรวบรวมข้อมูลกิจกรรมและปัจจัยเสี่ยงที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและทำการศึกษาข้อมูลระดมความคิดเห็นกับเจ้าหน้าที่ผู้ปฏิบัติงานด้านกิจกรรมต่าง ๆ ดังนี้

๓.๑ ขั้นตอนการดำเนินการบริหารจัดการความเสี่ยง



ที่มา : แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๔

๓.๒ กระบวนการจัดทำแผนบริหารจัดการความเสี่ยง



๓.๓ การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk Identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่ ขร. เผชิญอยู่ โดยมีการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินความเป็นไปได้และผลกระทบ มีดังนี้

ระดับความเสี่ยง	ระดับสี	คำอธิบาย	คะแนน
สูง		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	๑๕ - ๒๕
ค่อนข้างสูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป	๘ – ๑๔
ค่อนข้างต่ำ		ระดับที่พอยอมรับได้ แต่ต้องการมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	๔ – ๗
ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม	๑ - ๓

การประเมินความเสี่ยง

ผลกระทบ (Impact)					
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
		โอกาสเกิด		

๓.๓.๑ ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สามารถกำหนดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร จำนวน ๕ ด้าน ดังนี้

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงด้านกายภาพและสภาพแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ				
O๑ ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center)	ความเสี่ยงจากภัย หรือสถานการณ์ฉุกเฉิน	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร หรือการวางเพลิง - ภัยที่เกิดจากธรรมชาติฟ้าผ่า	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูล ถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบคอมพิวเตอร์แม่ข่ายและลูกข่ายหยุด ประมวลผลทั้งระบบ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๒ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ	ความเสี่ยงจากภัย หรือสถานการณ์ฉุกเฉิน	- แหล่งที่ให้บริการกระแสไฟฟ้า ขัดข้อง - แรงดันไฟฟ้าขัดข้อง	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่าย ไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๓ การควบคุมอุณหภูมิ/ ความชื้นภายในห้องปฏิบัติการ ศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	ความเสี่ยงด้านเทคนิค หรือความเสี่ยงจากผู้ปฏิบัติงาน	ควบคุมอุณหภูมิและความชื้น ที่ไม่เหมาะสม	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ ในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๔ ไม่มีแผนต่อเนื่องกรณีเกิด สถานการณ์ภัยพิบัติ/ความไม่สงบ ทางการเมือง/ชุมนุมประท้วง	ความเสี่ยงจากภัย หรือ สถานการณ์ฉุกเฉิน	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	- เจ้าหน้าที่ไม่สามารถเข้าไปปฏิบัติงานได้ตามปกติ เนื่องจากถูกปิดล้อมสถานที่ทำงาน - หน่วยงานถูกตัดกระแสไฟฟ้าทำให้ระบบงาน หยุดทำงานไม่สามารถให้บริการได้ เนื่องจาก ไม่สามารถเข้าระบบจากระยะไกล (Remote) ได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
๒. ความเสี่ยงด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดขึ้นกับระบบเครือข่ายเทคโนโลยีสารสนเทศต่าง ๆ เช่น ระบบเครือข่ายอินเทอร์เน็ต ไวรัสคอมพิวเตอร์ การเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ภัยคุกคามทางคอมพิวเตอร์ต่าง ๆ				
O๕ ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ไม่มีการควบคุมบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
O๖ ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ ขร.	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ไม่มีกำหนดแผนรองรับอุปกรณ์เครือข่าย และระบบแม่ข่ายของ ขร.	ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
O๗ ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งาน	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ไม่มีการควบคุมสิทธิการใช้งานอุปกรณ์เทคโนโลยีสารสนเทศ	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งานได้ - ไม่สามารถหาผู้กระทำความผิดได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
O๘ ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	ความเสี่ยงด้านเทคนิคหรือความเสี่ยงจากผู้ปฏิบัติงาน	- การขัดข้องจากทางผู้ให้บริการอินเตอร์เน็ต - IP Address ไม่เพียงพอสำหรับผู้ใช้งาน - ปริมาณการรับ-ส่งข้อมูล (Bandwidth) ไม่เพียงพอสำหรับการใช้งาน	- เสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote) ได้ - ผู้ใช้งานไม่สามารถเชื่อมต่ออินเทอร์เน็ต	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบระบบสารสนเทศ
O๙ ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่มีการควบคุมอุปกรณ์ที่เชื่อมต่อกับเครือข่ายของหน่วยงาน - จำนวนบุคลากรเพิ่มขึ้น	- ไม่สามารถระบุตัวตนผู้ใช้งานได้ - ไม่สามารถหาผู้กระทำความผิดได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
O๑๐ ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ครุภัณฑ์ อุปกรณ์ ไม่ได้มาตรฐาน การติดตั้งใช้งานไม่สมบูรณ์	- เกิดความเสียหายจากการจัดหาครุภัณฑ์อุปกรณ์ที่ไม่ได้มาตรฐาน - การติดตั้งที่ไม่ได้มาตรฐาน	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
๓. ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล หมายถึง ความเสี่ยงที่เกิดจากการทำงานของระบบสารสนเทศและการจัดเก็บฐานข้อมูลสารสนเทศ ที่อาจเกิดความเสียหายจากการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ ไม่มีการอัปเดตโปรแกรมให้ทันสมัยเพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไข เปลี่ยนแปลงคำสั่ง และการถูกผู้ไม่หวังดีทำลายระบบ (Hacker) ตลอดจนความเสี่ยงจากการถูกบุกรุกข้อมูลการสูญหายของข้อมูลความถูกต้องน่าเชื่อถือของข้อมูลและรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ				
O๑๑ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	ความเสี่ยงด้านเทคนิค หรือความเสี่ยงจากผู้ปฏิบัติงาน	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ไม่มีอำนาจ เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) - ขาดการป้องกันและตรวจจับไวรัสคอมพิวเตอร์ - ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลและระบบฐานข้อมูล - เกิดช่วงโหว่ของซอฟต์แวร์ - ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan)	- ข้อมูลถูกเปลี่ยนแปลงหรือถูกทำลาย - ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๑๒ การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	ความเสี่ยงด้านเทคนิค หรือความเสี่ยงจากผู้ปฏิบัติงาน	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ไม่มีอำนาจ เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) - ขาดการป้องกันและตรวจจับไวรัสคอมพิวเตอร์	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการระบบฯ ต่อประชาชนและผู้ใช้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
		- ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลและระบบฐานข้อมูล - เกิดช่วงโหว่ของซอฟต์แวร์ - ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan)		
O๑๓ การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	ไม่มีการกำหนดวิธีการรักษาความปลอดภัยจากการปฏิบัติงานจากระยะไกล	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายได้ต่อระบบ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย
O๑๔ พื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย (Server Storage) หรือระบบฐานข้อมูล (Database) ไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่มีการวางแผนการดำเนินโครงการและอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน - ผู้ใช้งานไม่ปรับปรุงข้อมูลให้เป็นปัจจุบัน	- ไม่มีการวางแผนการดำเนินโครงการและอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน - ผู้ใช้งานไม่ปรับปรุงข้อมูลให้เป็นปัจจุบัน	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๑๕ เกิดช่องโหว่ของซอฟต์แวร์ ขาดการบำรุงรักษา หรือเกิดช่องโหว่ของโปรแกรม	- ความเสี่ยงด้านเทคนิค - ความเสี่ยงจากการดำเนินงานหรือความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่มีการอัปเดตซอฟต์แวร์ให้เป็นปัจจุบัน - ไม่มีการบำรุงรักษาโปรแกรมอย่างต่อเนื่อง	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้ - อาจเกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้อันเกิดจากไม่มีการอัปเดตเวอร์ชั่นใหม่ ๆ อย่างสม่ำเสมอทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง/ในเวลาที่ต้องการ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
O๑๖ ละเมิดลิขสิทธิ์โปรแกรม อรรถประโยชน์ (Utilities Program)	ความเสี่ยงด้านเทคนิค หรือความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับ ในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย
๔. ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ				
O๑๗ การนำเข้าข้อมูลผิดพลาด ไม่ครบถ้วน หรือ ไม่เป็นปัจจุบัน	- ความเสี่ยงด้านการบริหาร จัดการ หรือความเสี่ยง จากเจ้าหน้าที่ผู้ปฏิบัติงาน - ความเสี่ยงด้านการบริหาร จัดการ หรือความเสี่ยง จากเจ้าหน้าที่ผู้ปฏิบัติงาน	- การนำข้อมูลที่ไม่ถูกต้องเข้าสู่ระบบ - ระบบมีความผิดพลาด - การนำข้อมูลที่ไม่ถูกต้องเข้าสู่ระบบ - ไม่มีการตรวจสอบและปรับปรุง ข้อมูลให้เป็นปัจจุบัน	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถออกรายงานได้ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้ถูกต้อง และเป็นปัจจุบัน	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๑๘ การจ้างบุคคลภายนอก ที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษา ระบบ/พัฒนาระบบ	ความเสี่ยงด้านการบริหารจัดการ หรือความเสี่ยงจากเจ้าหน้าที่ ผู้ปฏิบัติงาน	การจ้างบุคคลภายนอก ที่ขาดความรู้ความชำนาญเกี่ยวกับ ระบบที่รับผิดชอบ	ระบบมีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไขทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	- ผู้ใช้งาน - ผู้ดูแลระบบ
O๑๙ บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยี ฯ ไม่เพียงพอ	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ขาดการอบรมบุคลากรด้านไอที - หน่วยงานขาดบุคลากรด้านไอที	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่อง และอาจเกิดความเสียหายทั้งระบบได้ งบประมาณที่ใช้ในการบำรุงรักษามีปริมาณ เพิ่มขึ้นทุกปี	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง
O๒๐ ผู้ใช้งาน/Users ไม่มีความรู้ ความชำนาญ และทักษะ การใช้งานระบบ	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่มีการอบรมการใช้งานระบบ แก่ผู้ใช้งาน - ระบบมีความซับซ้อน ยากต่อการใช้งาน	- การใช้ระบบงานไม่เป็นไปตาม Workflow ที่กำหนด ทำให้เกิดข้อขัดข้อง ไม่สามารถ แก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้	- ผู้ใช้งาน - ผู้ดูแลระบบ - ผู้รับจ้าง

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
			- ความล่าช้าในการปฏิบัติงานและเพิ่มปริมาณงานให้กับผู้ดูแลระบบ - ไม่มีการใช้งานทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ/ข้อมูลไม่ถูกนำไปใช้งาน	
O๒๑ การเชื่ออีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- การเปิดไฟล์ หรือ URL ที่แนบมากับอีเมลที่น่าสงสัย - การหลงเชื่อเว็บไซต์ปลอมให้ข้อมูลส่วนตัว หรือลงโปรแกรมที่มาจากแหล่งที่ไม่น่าเชื่อถือ	- โดนหลอกลวงเพื่อขอรหัสผ่าน ข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับ - โดนหลอกเพื่อติดตั้งไวรัสลงบนคอมพิวเตอร์หรือคอมพิวเตอร์แม่ข่าย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๒๒ การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- การเข้าใช้งานระบบจากระยะไกลด้วยเครือข่ายที่ไม่น่าเชื่อถือ - การให้บุคคลที่น่าสงสัยมาใช้งานเครือข่ายเดียวกัน	- โดนดักเก็บข้อมูลการดำเนินการ เช่น รหัสผ่านข้อมูลที่เป็นความลับ - เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
O๒๓ ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	ความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ผู้ใช้งานลืมออกจากระบบ - ผู้ใช้งานละเลยเรื่องความปลอดภัยของระบบ	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
๕. ความเสี่ยงในด้านการบริหารจัดการ หมายถึง ความเสี่ยงเนื่องมาจากการได้รับสนับสนุนงบประมาณไม่เพียงพอ การบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี และการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา				
O๒๔ งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	- โดนตัด/ปรับลดโครงการตามนโยบายการปรับลดเงินเป็นร้อยละ	- ลดระยะเวลา ลดคุณภาพและประสิทธิภาพการให้บริการ	หน่วยงานซึ่งเป็นหน่วยรับงบประมาณ

กิจกรรม/ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
		- ทำให้โครงการที่จำเป็นต้องดำเนินการ โดนตัด/ปรับลดไปด้วย	- การประชุมผ่านสื่ออิเล็กทรอนิกส์ไม่สามารถรองรับผู้เข้าร่วมประชุมจำนวนมากเนื่องจากข้อจำกัดของ Package ที่ซื้อ - โครงการที่จำเป็นต้องดำเนินการ โดนตัด/ปรับลดงบประมาณ - งวดเงิน และงวดงาน ไม่สอดคล้องกัน	
O๒๕ ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนปฏิบัติราชการ ขร.	ความเสี่ยงด้านการบริหารจัดการหรือความเสี่ยงจากเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามตามแผนปฏิบัติราชการ ขร. ได้	- ผู้บริหารปรับลดระยะเวลาดำเนินโครงการ - ไม่สามารถดำเนินงานให้บรรลุเป้าหมายและตัวชี้วัดที่กำหนด	- สำนัก/กอง/กลุ่ม
O๒๖ กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า	ความเสี่ยงจากการดำเนินงานหรือความเสี่ยงเจ้าหน้าที่ผู้ปฏิบัติงาน	- ไม่สามารถดำเนินงานได้อย่างต่อเนื่องทันที - การดำเนินการโครงการล่าช้า - การเปลี่ยนแปลงวิธีการระหว่างการดำเนินการ	- เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง - อนุมัติโครงการล่าช้า - ไม่สามารถหาผู้รับจ้างได้ตามแผนดำเนินการ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปี ส่งผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน
O๒๗ ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	ความเสี่ยงจากการออกกฎหมาย/ระเบียบที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ	- กฎหมาย/ระเบียบที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีผลบังคับใช้ - ไม่สามารถดำเนินการตามกฎหมาย/ระเบียบที่เกี่ยวข้องได้ทันภายในระยะเวลาที่กฎหมายกำหนด	- การดำเนินงานไม่สามารถรองรับการปฏิบัติงานตามกฎหมาย/ระเบียบที่บังคับใช้ได้ - ไม่มีระบบสารสนเทศรองรับการดำเนินงานตามที่กฎหมายกำหนด	- สำนัก/กอง/กลุ่ม

๓.๓.๒ ผลประเมินความเสี่ยงและจัดการความเสี่ยง ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

ขร. มีการประเมินผลการควบคุมภายในระดับส่วนราชการ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ดังนี้

ลำดับ	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	คะแนน
๑	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๓	๓	๙
๒	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนปฏิบัติราชการ ขร.	๒	๔	๘
๓	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	๒	๓	๖
๔	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๒	๓	๖
๕	เกิดช่องโหว่ของซอฟต์แวร์	๒	๕	๖
๖	ผู้ใช้งาน/Users ไม่มีความรู้ ความชำนาญ และทักษะ การใช้งานระบบ	๒	๓	๖
๗	การเชื่ออีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	๓	๒	๖
๘	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า	๒	๓	๖
๙	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center)	๑	๑	๕
๑๐	ไม่มีแผนต่อเนื่องกรณีเกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑	๕	๕
๑๑	ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลของข้อมูลและระบบฐานข้อมูลครบถ้วน	๑	๕	๕
๑๒	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑	๕	๕
๑๓	ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	๑	๕	๕
๑๔	ขาดการป้องกันหรือตรวจจับไวรัส	๑	๕	๕
๑๕	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๕	๑	๕
๑๖	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๑	๔	๔
๑๗	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	๒	๒	๔
๑๘	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	๑	๓	๓
๑๙	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	๑	๓	๓
๒๐	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ ขร.	๑	๓	๓
๒๑	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งาน	๑	๓	๓
๒๒	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่าย คอมพิวเตอร์ ขร. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	๑	๓	๓
๒๓	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑	๓	๓
๒๔	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	๑	๓	๓
๒๕	พื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย(Server Storage) หรือระบบฐานข้อมูล(Database) ไม่เพียงพอ	๓	๑	๓
๒๖	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลหรือฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	๑	๓	๓

ลำดับ	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	คะแนน
๒๗	ไม่มีการกำหนดสิทธิ์การเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)	๑	๓	๓
๒๘	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	๑	๓	๓
๒๙	การนำเข้าข้อมูลผิดพลาดทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	๑	๓	๓
๓๐	การนำเข้าข้อมูลไม่ครบถ้วน และไม่เป็นปัจจุบัน	๑	๓	๓
๓๑	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแล บำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓
๓๒	ผู้บริหารไม่ให้ความสำคัญ ต่อความเสี่ยงที่อาจจะเกิดขึ้นกับระบบ เทคโนโลยีสารสนเทศและการสื่อสาร	๑	๓	๓
๓๓	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	๑	๒	๒

จากผลประเมินความเสี่ยงและจัดการความเสี่ยง ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ พบว่ามีปัจจัยเสี่ยงทั้งสิ้น ๓๓ ปัจจัย โดยแบ่งเป็น ปัจจัยเสี่ยงที่มีคะแนนอยู่ในระดับค่อนข้างสูงอยู่ ๒ รายการ ปัจจัยเสี่ยงระดับค่อนข้างต่ำ ๑๕ รายการ และปัจจัยเสี่ยงระดับต่ำ ๑๖ รายการ ต้องจัดการความเสี่ยงดังนี้ ความเสี่ยงระดับค่อนข้างสูง เป็นระดับที่ไม่สามารถยอมรับได้ต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ จึงจำเป็นต้องมีการจัดการความเสี่ยงต่อในปี ๒๕๖๖ - ๒๕๖๘ ความเสี่ยงระดับค่อนข้างต่ำเป็นระดับที่สามารถยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ และความเสี่ยงระดับต่ำเป็นระดับที่สามารถยอมรับได้โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

๓.๔ การประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘

ในปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘ ขร. ได้ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ขร. จำนวน ๒๗ กิจกรรม ดังนี้

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
๑. ความเสี่ยงด้านกายภาพและสภาพแวดล้อม	O๑	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center)	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบคอมพิวเตอร์แม่ข่ายและลูกข่ายหยุดประมวลผลทั้งระบบ	๑	๕	๕	ควบคุมความเสี่ยง	ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะ พร้อมใช้งาน และตรวจสอบระบบดับเพลิงอัตโนมัติ เป็นการจ้างบริษัทดำเนินการบำรุงรักษาเนื่องจากมีความเชี่ยวชาญเฉพาะด้าน
	O๒	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้	๒	๓	๖	ควบคุมความเสี่ยง	ติดตั้งและตรวจสอบระบบสำรองไฟฟ้า (UPS) /แบตเตอรี่สำรองไฟสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และลูกข่าย
	O๓	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) และเครือข่ายคอมพิวเตอร์ ขร.	๑	๓	๓	ควบคุมความเสี่ยง	ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้นมีการตรวจสอบสภาพแวดล้อมในห้องและระบบควบคุมอุณหภูมิ/ความชื้นผ่านระบบควบคุมอย่างสม่ำเสมอ
	O๔	ไม่มีแผนต่อเนื่องกรณีเกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	- เจ้าหน้าที่ไม่สามารถเข้าไปปฏิบัติงานได้ตามปกติเนื่องจากถูกปิดล้อมสถานที่ทำงาน - หน่วยงานถูกตัดกระแสไฟฟ้าทำให้ระบบงานหยุดทำงานไม่สามารถ	๑	๔	๔	ควบคุมความเสี่ยง	- จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan) - ปรับปรุงแผน/ใช้แผนบริหารความต่อเนื่อง Business

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
			ให้บริการได้ เนื่องจากไม่สามารถเข้าระบบจากระยะไกล (Remote) ได้					Continuity Plan (BCP) ของ ขร. ให้เป็นปัจจุบัน
๒. ความเสี่ยงด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ	O๕	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย	๑	๓	๓	ควบคุมความเสี่ยง	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์ของ ขร.
	O๖	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ ขร.	ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้ เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	๑	๓	๓	ควบคุมความเสี่ยง	- มีแผนการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตาม และสรุปผลการปฏิบัติงานทุก ๖ เดือน - จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ - ทดสอบการโจมตีตามแผนที่กำหนดจริง
	O๗	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งาน	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งานได้ - ไม่สามารถหาผู้กระทำความผิดได้	๑	๓	๓	ควบคุมความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ มีการทบทวนสิทธิ์เป็นประจำทุก ๖ เดือน โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
								- มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก ๖ เดือน
	O๘	ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	- เสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote) ได้ - ผู้ใช้งานไม่สามารถเชื่อมต่ออินเทอร์เน็ต	๓	๓	๙	ควบคุมความเสี่ยง	- ระบุข้อกำหนด/ข้อตกลงระดับการให้บริการที่ชัดเจนกับผู้ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล - มีสัญญาการบำรุงรักษาและการแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนทุกครั้งที่ขัดข้องเพื่อให้แก้ปัญหาได้ทันที - กำหนดช่วง IP Address สำหรับอุปกรณ์ที่เชื่อมต่อเครือข่ายไร้สาย - ทำการติดตั้งสายสายสัญญาณให้เพียงพอต่อการใช้งาน
	O๙	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน	๑	๓	๓	ควบคุมความเสี่ยง	- มีการยืนยันตัวตนเมื่อมีการเข้าใช้งานเครือข่าย - มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
	O๑๐	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	- เกิดความเสียหายจากการจัดหาครุภัณฑ์ อุปกรณ์ที่ไม่ได้มาตรฐาน - การติดตั้งที่ไม่ได้มาตรฐาน	๑	๓	๓	ควบคุมความเสี่ยง	- ทำการตรวจสอบลักษณะของงานเพื่อจัดหาอุปกรณ์ที่เหมาะสม - ตรวจสอบมาตรฐานของอุปกรณ์
๓. ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล	O๑๑	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	๓	๓	๙	ควบคุมความเสี่ยง	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - ติดตั้ง Patch ของระบบ ปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผลทุก ๓ เดือน

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
	O๑๒	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการระบบฯ ต่อประชาชนและผู้ใช้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	๑	๔	๔	ควบคุมความเสี่ยง	- ติดตั้งโปรแกรมป้องกันไวรัสและ Patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศทุก ๖ เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - จัดทำการสำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมออย่างน้อยเดือนละ ๑ ครั้ง
	O๑๓	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายได้ต่อระบบ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้	๑	๕	๕	ควบคุมความเสี่ยง	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง
	O๑๔	พื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย (Server Storage)	- ไม่มีการวางแผนการดำเนินโครงการและอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน	๓	๑	๓	ควบคุมความเสี่ยง	- คอยตรวจสอบพื้นที่คงเหลือของฐานข้อมูล และคอมพิวเตอร์แม่ข่าย

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
		หรือระบบฐานข้อมูล (Database) ไม่เพียงพอ	- ผู้ใช้งานระบบไม่นำข้อมูลที่ไม่ได้ใช้งานออกจากระบบ					- กำหนดขนาดพื้นที่การจัดเก็บไฟล์ของผู้ใช้งาน
	O๑๕	เกิดช่องโหว่ของซอฟต์แวร์ขาดการบำรุงรักษาหรือเกิดช่องโหว่ของโปรแกรม	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้ - อาจเกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้ อันเกิดจากไม่มีการอัปเดตเวอร์ชันใหม่ ๆ อย่างสม่ำเสมอทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง/ในเวลาที่ต้องการ	๒	๒	๔	ควบคุมความเสี่ยง	-ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่าง ๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง - ทำแผนการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่อง
	O๑๖	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	๑	๓	๓	ควบคุมความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศและการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง จัดทำและส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
๔. ความเสี่ยงด้านบุคลากร	O๑๗	การนำเข้าข้อมูลผิดพลาด ไม่ครบถ้วน หรือ ไม่เป็นปัจจุบัน	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถออกรายงานได้ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	๑	๓	๓	ควบคุมความเสี่ยง	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลของ ขร. เพื่อควบคุมคุณภาพข้อมูล ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ
	O๑๘	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	มีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไขทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	๑	๓	๓	ควบคุมความเสี่ยง	- มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน - มีการจัดทำแผนงาน ขั้นตอนการทำงานที่ชัดเจน และควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้ - มีการติดตามเพื่อป้องกันการผิดพลาดและให้เกิดการแก้ไขปัญหาได้ทันที โดยมีการประชุมทุกสัปดาห์
	๑๙	บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้เพิ่มค่าใช้จ่ายในการบำรุงรักษามากยิ่งขึ้น	๑	๒	๒	ควบคุมความเสี่ยง	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้างบุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน เพื่อจัดอบรมให้กับบุคลากร

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
								- มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรในตำแหน่งที่ว่าง
	๒๐	ผู้ใช้งาน/Users ไม่มีความรู้ความชำนาญและทักษะการใช้งานระบบ	- การใช้ระบบงานไม่เป็นไปตาม Workflow ที่กำหนด ทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้ การปฏิบัติงานติดขัด - ความล่าช้าในการปฏิบัติงานเพิ่มภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งานทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ	๒	๓	๖	ควบคุมความเสี่ยง	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีระบบ Call Center สำหรับให้คำปรึกษา เกี่ยวกับการใช้งานระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุงหรือตามความต้องการของ User
	O๒๑	การเชื่ออีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	- โดนหลอกลวงเพื่อขอรหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับ - โดนหลอกเพื่อติดตั้งไวรัสลงบนคอมพิวเตอร์หรือคอมพิวเตอร์แม่ข่าย	๓	๒	๖	ควบคุมความเสี่ยง	- จัดอบรมให้ความรู้แก่บุคลากรในองค์กร - คอยแจ้งข่าวสารให้บุคลากรในองค์กรทราบเมื่อพบอีเมล หรือหน้าเว็บไซต์ปลอม
	O๒๒	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	- โดนดักเก็บข้อมูลการดำเนินการ เช่น รหัสผ่าน ข้อมูลที่เป็นความลับ - เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้	๑	๒	๒	ควบคุมความเสี่ยง	จัดอบรมให้ความรู้แก่บุคลากรในองค์กร

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
	๐๒๓	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้	๕	๑	๕	ควบคุมความเสี่ยง	- ให้ระบบดำเนินการออกจากระบบเมื่อผู้ใช้ไม่มีการเคลื่อนไหวในระยะเวลาที่กำหนด
๕. ความเสี่ยงในด้านการบริหารจัดการ	๐๒๔	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	- ลดระยะเวลา ลดคุณภาพและประสิทธิภาพการให้บริการ - ไม่รองรับการประชุมเมื่อมีผู้ขอเข้าประชุมจำนวนมากของโปรแกรมประชุมทางไกล - โครงการที่จำเป็นต้องดำเนินการโดนตัด/ปรับลดงบประมาณ - งวดเงิน และงวดงาน ไม่สอดคล้องกัน	๓	๒	๖	ควบคุมความเสี่ยง	- หน่วยงานวิเคราะห์งบประมาณต้องมีการดำเนินการตัดปรับลดโดยมีการจัดทำความเสี่ยงและการให้น้ำหนักของความสำคัญของโครงการที่ใช้หมวดเงินประเภทเดียวกัน - ปรับลดโครงการตามลำดับความสำคัญและลดปริมาณหน่วยบริการ - ปรับแผนการดำเนินงานตามแผนการใช้จ่ายงบประมาณตามงวดงานที่ได้รับ
	๐๒๕	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนปฏิบัติราชการ ขร.	- ผู้บริหารไม่อนุมัติให้ดำเนินโครงการเนื่องจากมีความเห็นว่าเป็นระยะเวลาที่จะสิ้นสุดปีงบประมาณ - ไม่สามารถอบรมให้บรรลุเป้าหมายและตัวชี้วัดที่กำหนด - การดำเนินงานไม่สัมฤทธิผล	๑	๒	๒	ควบคุมความเสี่ยง	- บรรจุโครงการแผนปฏิบัติการให้ผู้บริหารเห็นชอบแผน - กำหนดกรอบเวลาให้ชัดเจนและอยู่ในกรอบเวลาที่สามารถดำเนินการได้ - กำหนดกลุ่มเป้าหมายที่ชัดเจน

กิจกรรม	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑) x (๒)	การตอบสนองความเสี่ยง	แนวทางการควบคุม
	O๒๖	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน	- เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง - อนุมัติโครงการล่าช้า - ไม่สามารถหาผู้รับจ้างได้ตามแผนดำเนินการ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปี ส่งผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	๒	๓	๖	ควบคุมความเสี่ยง	- จัดทำแผนปฏิบัติการและดำเนินการ ให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการอย่างจริงจัง กรณีผู้บริหารอนุมัติโครงการล่าช้า ต้องขอวาระชี้แจงเหตุผลความจำเป็นและจัดลำดับความสำคัญ/ความเร่งด่วน - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด
	O๒๗	ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	- การดำเนินงานไม่สามารถรองรับการปฏิบัติงานตามกฎหมาย/ระเบียบที่บังคับใช้ได้ - ไม่มีระบบสารสนเทศรองรับการดำเนินงานตามที่กฎหมายกำหนด	๒	๔	๘	ควบคุมความเสี่ยง	- ติดตามประกาศ/กฎหมาย/ระเบียบที่เกี่ยวข้อง - จัดลำดับความสำคัญและวางแผนการดำเนินงาน

๓.๕ แผนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘

จากการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘ สามารถนำมาจัดทำแผนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘ โดยพิจารณาจากระดับคะแนนความเสี่ยงสูง มีระยะเวลาดำเนินการระหว่างเดือนตุลาคม ๒๕๖๕ – กันยายน ๒๕๖๘ ได้ดังนี้

ประเด็นความเสี่ยง/กิจกรรม	กิจกรรมตามแนวทางการจัดการความเสี่ยง	เป้าหมาย/ผลสำเร็จของการดำเนินการกิจกรรมตามแนวทางการจัดการความเสี่ยง	ปี ๒๕๖๕	ปี ๒๕๖๖				ปี ๒๕๖๗				ปี ๒๕๖๘			ผู้รับผิดชอบ
			ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	
ด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รหัส ๐๘ ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	- ดำเนินการขอเพิ่มปริมาณการรับ-ส่งข้อมูล (Bandwidth) ของเครือข่ายให้เพียงพอสำหรับผู้ใช้งาน - ติดตั้งสายสัญญาณให้ทั่วถึง - กำหนดจำนวนการเชื่อมต่ออุปกรณ์ต่อผู้ใช้งาน	- ระบบเครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพความเสถียร - ระบบเครือข่ายสามารถรองรับการใช้งานของผู้ใช้งานทั้งองค์กร	←								→				ยส.

ประเด็นความเสี่ยง/กิจกรรม	กิจกรรมตามแนวทางการจัดการความเสี่ยง	เป้าหมาย/ผลสำเร็จของการดำเนินการกิจกรรมตามแนวทางการจัดการความเสี่ยง	ปี ๒๕๖๕	ปี ๒๕๖๖				ปี ๒๕๖๗				ปี ๒๕๖๘			ผู้รับผิดชอบ
			ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	ต.ค. - ธ.ค.	ม.ค. - มี.ค.	เม.ย. - มิ.ย.	ก.ค. - ก.ย.	
ด้านระบบสารสนเทศและฐานข้อมูล รหัส O๑๑ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ติดตั้งโปรแกรมป้องกันไวรัสบนเครื่องแม่ข่าย - ติดตามแก้ไขช่องโหว่ของซอฟต์แวร์เป็นประจำ - มีการยืนยันตัวตนและกำหนดสิทธิผู้ใช้งานก่อนการใช้งานเครือข่าย	- ระบบเครือข่ายของ ขร. มีความปลอดภัย - ผู้ใช้งานมีความมั่นใจในการใช้งานเครือข่าย	←											→	ยส.
ความเสี่ยงในด้านการบริหารจัดการ รหัส O๒๗ ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	- ติดตามประกาศ/กฎหมาย/ระเบียบที่เกี่ยวข้อง - จัดลำดับความสำคัญและวางแผนการดำเนินงาน	ขร. มีการปฏิบัติงานที่สอดคล้องตามกฎหมาย/ระเบียบที่เกี่ยวข้อง	←											→	สำนัก/กอง/กลุ่ม

บทที่ ๔
สรุปผลและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) เป็นกระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบและควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงาน เพื่อลดความเสียหายอันเนื่องมาจากความเสี่ยงที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่งให้ได้มากที่สุด เมื่อเทคโนโลยีเข้ามามีบทบาทสำคัญในการขับเคลื่อนการดำเนินการขององค์กร ส่งผลให้มีข้อมูลจำนวนมากถูกส่งผ่านระบบเครือข่ายเทคโนโลยีสารสนเทศขององค์กร ในปัจจุบันข้อมูลมีคุณค่ามหาศาลและเป็นที่ต้องการของบุคคลหรือองค์กรต่าง ๆ ข้อมูลขององค์กรจึงมีความเสี่ยงต่อการถูกทำให้เสียหาย นำไปใช้ในทางที่ผิด

ขร. จึงได้จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ขร. พ.ศ. ๒๕๖๖ - ๒๕๖๘ เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่ หรือความเสี่ยงที่ยังควบคุมความเสี่ยงต่อ เพื่อบริหารจัดการความเสี่ยง ลดโอกาส/ความเสียหายที่จะเกิดขึ้นให้อยู่ในระดับที่ยอมรับได้ และควบคุมความความเสียงที่อยู่ในระดับที่ยอมรับได้ไม่ให้เพิ่มขึ้นไปในระดับที่ไม่สามารถยอมรับได้

๔.๑ วัตถุประสงค์

แผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ ขร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘ มีวัตถุประสงค์ ดังนี้

๔.๑.๑ เตรียมความพร้อมเพื่อรองรับสถานการณ์ฉุกเฉิน (Contingency Event) ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและฐานข้อมูลสารสนเทศของ ขร.

๔.๑.๒ เป็นแนวทางหรือขั้นตอนปฏิบัติในการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและฐานข้อมูลสารสนเทศของ ขร. ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งานอย่างต่อเนื่อง

๔.๑.๓ มีแนวทางการบริหารจัดการความเสี่ยงอย่างเป็นระบบแบบแผน มีความต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีในกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติต่าง ๆ

๔.๒ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk Identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนที่มีระดับความเสี่ยงสูง ดังนี้

ความเสี่ยง	แนวทางปฏิบัติ
๑. ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	- ดำเนินการขอเพิ่มปริมาณการรับ-ส่งข้อมูล (Bandwidth) ของเครือข่ายให้เพียงพอสำหรับผู้ใช้งาน - ติดตั้งสายสัญญาณให้ทั่วถึง - กำหนดจำนวนการเชื่อมต่ออุปกรณ์ต่อผู้ใช้งาน
๒. ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ติดตามแก้ไขช่องโหว่ของซอฟต์แวร์เป็นประจำ - มีการยืนยันตัวตนและกำหนดสิทธิผู้ใช้งานก่อนการใช้งานเครือข่าย
๓. ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	- ติดตามประกาศ/กฎหมาย/ระเบียบที่เกี่ยวข้อง - จัดลำดับความสำคัญและวางแผนการดำเนินงาน

๔.๓ ข้อเสนอแนะ

เพื่อให้การบริหารความเสี่ยงขององค์กรดำเนินการอย่างเป็นระบบและได้ผล ขร. จึงได้ปรับปรุงแผนให้มีความสอดคล้องกับสถานการณ์ปัจจุบัน โดยมีการเพิ่ม/ลด รายการความเสี่ยงในรายการที่ได้ดำเนินการควบคุมความเสี่ยงแล้วหรือรายการที่เป็นความเสี่ยงเกิดขึ้นใหม่ พร้อมทั้งมีการติดตามความเสี่ยงรายการที่อยู่ในระดับความเสี่ยงที่ไม่สามารถยอมรับได้ จากแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการขนส่งทางราง ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๖๘ เพื่อติดตามและควบคุมให้ระดับความเสี่ยงมีความรุนแรงลดลงอยู่ในระดับที่สามารถยอมรับได้ โดยมีข้อเสนอแนะ ดังนี้

๑. ควรมีการติดตามรายการความเสี่ยงที่ยังอยู่ในระดับที่ไม่สามารถยอมรับได้ มาจัดการความเสี่ยงต่อโดยการทบทวนและปรับปรุงแผนความเสี่ยงด้วยวิธีที่เหมาะสม และมีความเป็นไปได้ในการปฏิบัติ

๒. ควรมีการนำข้อสังเกตตามผลการสอบทานและข้อเสนอแนะจากผู้ตรวจสอบภายใน ขร. และเปลี่ยนแปลงทั้งภายในและภายนอก ใช้เป็นแนวทางในการปรับปรุงแผนบริหารความเสี่ยงฯ ให้ครอบคลุมความเสี่ยงทางด้านต่าง ๆ

เอกสารอ้างอิง

๑. แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๔

๒. แผนบริหารความเสี่ยงสถาบันสารสนเทศทรัพยากรน้ำ (องค์การมหาชน) ปีงบประมาณ พ.ศ. ๒๕๖๔

๓. แผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

๔. แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมประมง ปี ๒๕๖๕-๒๕๗๐