บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

การบริหารจัดการความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูลการใช้งานอุปกรณ์คอมพิวเตอร์การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร ดังนั้นสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยงแล้วกำหนดแนวทางในการจัดการความเสี่ยงโดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

การพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) หมวด ๖ การปฏิบัติการ ได้กำหนดให้ส่วนราชการต้องมีแผนรองรับสถานการณ์ฉุกเฉิน หรือ Contingency plan และคู่มือความปลอดภัยทางไซเบอร์ หรือ Cyber Security ให้มีความพร้อมใช้งานอย่างต่อเนื่องในกรณีที่เกิดเหตุการณ์ฉุกเฉิน เพื่อการจัดการความมั่นคงทางข้อมูลและสารสนเทศ และตอบสนองผู้รับบริการ ผู้มีส่วนได้ส่วนเสีย และความจำเป็นทางภารกิจอย่างมีประสิทธิผล

๑.๒ วัตถุประสงค์ของการจัดทำแผนบริหารจัดการความเสี่ยง

๑.๒.๑ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลสารสนเทศของ สนข.

๑.๒.๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลสารสนเทศของ สนข. ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งานอย่างต่อเนื่อง

๑.๒.๓ เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและขั้นตอนที่ถูกต้อง สามารถที่จะแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๑.๓ เป้าหมาย

มีแผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข. ที่สามารถใช้เป็นกรอบแนวทางในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและทันเหตุการณ์

๑.๔ ขอบเขตการดำเนินงาน

เป็นการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร สนข.

๑.๕ ประโยชน์ที่คาดว่าจะได้รับ

๑.๕.๑ มีความพร้อมในการรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลสารสนเทศของ สนข.

๑.๕.๒ มีแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลสารสนเทศของ สนข. ให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๑.๖ ระยะเวลาดำเนินการ

ตารางที่ ๑-๑ ระยะเวลาดำเนินการจัดทำแผนบริหารและจัดการความเสี่ยง

ลำดับที่	กิจกรรม	ปีงบประมาณ ๒๕๖๓ ก.ย.	ปีงบประมาณ ๒๕๖๔									หน่วยงานที่รับผิดชอบ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	
๑	ศึกษา วิเคราะห์ ทบทวนแผน IT RMP ของ สนข. ปีงบประมาณ พ.ศ. ๒๕๖๓	→	→									กพค./ศทท.
๒	ประชุมเชิงปฏิบัติการ/ระดมสมองเพื่อจัดทำร่างแผน IT RMP ของ สนข. ปีงบประมาณ พ.ศ. ๒๕๖๔		→									กพค./ศทท.
๓	นำร่างแผน IT RMP ของ สนข. ปีงบประมาณ พ.ศ. ๒๕๖๔ เสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำองค์กร (DCIO) ของ สนข. เพื่อพิจารณาและให้ความเห็นชอบร่างแผนดังกล่าว			→								กพค./ศทท.
๔	เสนอ ผอ.สนข. เพื่อโปรดทราบและเพื่อโปรดพิจารณาให้ความเห็นชอบร่างแผนดังกล่าว				→							กพค./ศทท.

หมายเหตุ * IT RMP : IT Risk Management Plan

๑.๗ คณะที่ปรึกษา

๑.๗.๑ นางวิไลรัตน์ ศิริโสภณศิลป์ รองผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำองค์กรของ สนข.

๑.๗.๒ นางสาวลักษณวดี ธนามี ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร ผู้ช่วยผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำองค์กรของ สนข.

๑.๘ คณะผู้จัดทำของศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.)

๑.๘.๑ นายสมชาย ภูนาสี หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย

๑.๘.๒ นางสาวนิปริน คำแสง นักวิชาการคอมพิวเตอร์ชำนาญการ

๑.๘.๓ นายนฤทธิ์ มัยรัตน์ นักวิชาการคอมพิวเตอร์ชำนาญการ

๑.๘.๔ นายพิสิฏฐ์ ป้อมทอง นักวิชาการคอมพิวเตอร์ชำนาญการ

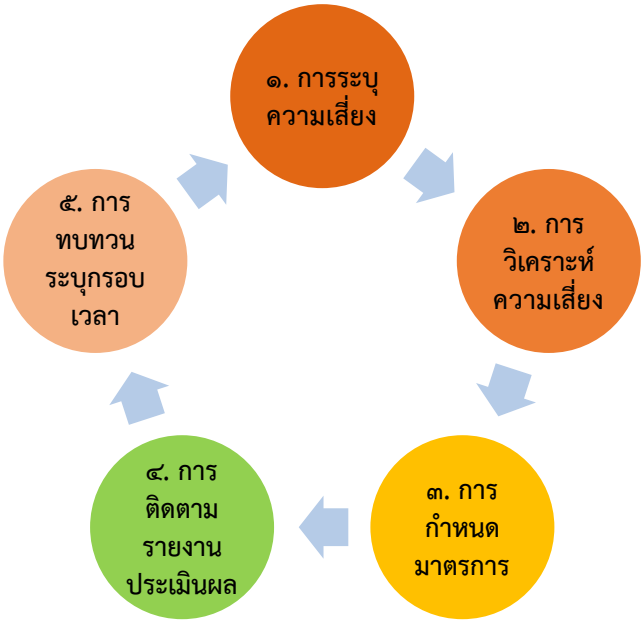
๑.๘.๔ นายชัยวัฒน์ ธรรมาสถิตนุกุล นักวิชการคอมพิวเตอร์ปฏิบัติการ

๑.๘.๖ นายทนงชัย ยศชัยพงษ์ นายช่างเขียนแบบชำนาญงาน

บทที่ ๒
การบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๒.๑ กระบวนการบริหารจัดการความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมินผล และจัดระดับความเสี่ยงที่มีผลกระทบต่อเป้าหมายของหน่วยงานหรือขององค์กร รวมทั้งการกำหนดแนวทางการดำเนินงาน หรือมาตรการควบคุม เพื่อป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนในการดำเนินการกระบวนการบริหารจัดการความเสี่ยงอย่างเหมาะสม ๕ ขั้นตอน ดังต่อไปนี้



รูปที่ ๒-๑ กระบวนการบริหารจัดการความเสี่ยง

๒.๑.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและหรือปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุเป้าหมายขององค์กร ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายในและภายนอกองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

(๑) การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

(๒) การใช้ Checklist

(๓) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

(๔) การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีต ทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๒.๑.๒ การวิเคราะห์และประเมินความเสี่ยง

เป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

(๑) **การกำหนดเกณฑ์การประเมินมาตรฐาน** ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) การกำหนดเกณฑ์ของโอกาสที่จะเกิดความเสี่ยงและระดับความรุนแรงของผลกระทบ อาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก สูง ปานกลาง น้อย และน้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (รุนแรง สูง ปานกลาง น้อย และยอมรับได้)

(๒) **การประเมินโอกาสและผลกระทบของความเสี่ยง** เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาพิจารณาโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนด ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติโอกาสที่จะเกิดความเสี่ยง และมิติผลกระทบ

ตารางที่ ๒-๑ เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง เป็นดังนี้

ระดับ	การประเมิน
๑	เกิดขึ้นน้อยมาก นานๆ ครั้ง (แทบไม่เกิดขึ้นเลย)
๒	เกิดขึ้นน้อย ไม่บ่อย (อาจเกิดขึ้นได้ทุก ๕ ปี)
๓	เกิดขึ้นปานกลาง (อาจเกิดขึ้นได้ทุกปี)
๔	เกิดขึ้นสูง หรือบ่อย (อาจเกิดขึ้นได้ทุกเดือน)
๕	เกิดขึ้นสูงมาก หรือบ่อยมาก (อาจเกิดขึ้นได้ทุกเวลา)

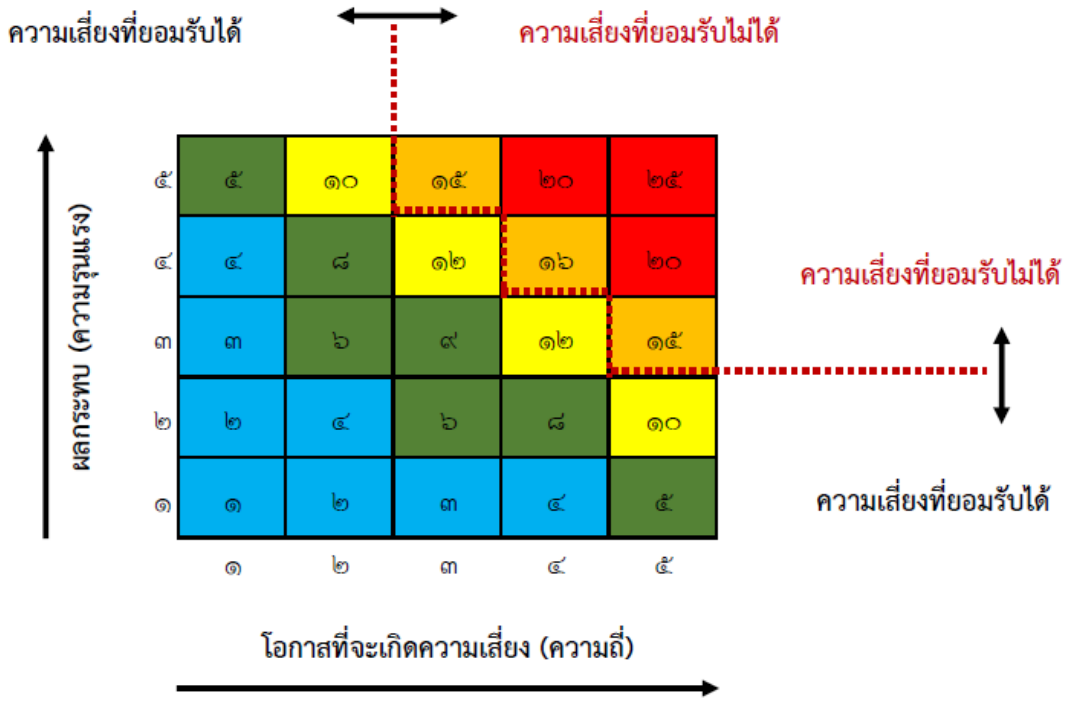
ตารางที่ ๒-๒ เกณฑ์การประเมินผลกระทบหรือความรุนแรงของความเสี่ยง เป็นดังนี้

ระดับ	การประเมิน
๑	น้อยมาก (แทบไม่มีผลกระทบเลย)
๒	น้อย (เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ)
๓	ปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)
๔	สูง (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)
๕	สูงมาก (ผู้บริหารถูกลงโทษทางวินัย)

(๓) **การวิเคราะห์ความเสี่ยง การวิเคราะห์ความเสี่ยง** เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยพิจารณาจากค่าคะแนนระหว่าง ๑-๒๕ ซึ่งคำนวณได้จากสูตร

ระดับความเสี่ยง = โอกาสที่จะเกิดความเสี่ยง (Likelihood) x ความรุนแรงของผลกระทบ (Impact)

ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน โดยใช้ตารางระดับความเสี่ยง ดังรูปที่ ๒-๓



รูปที่ ๒-๒ แผนผังประเมินความเสี่ยง

ตารางที่ ๒-๓ ช่วงคะแนนระดับความเสี่ยง (Degree of Risk)

ระดับความเสี่ยง	ช่วงคะแนน	สัญลักษณ์สี	ความหมาย
๕ (Severe)	๒๐-๒๕		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยด่วน
๔ (High)	๑๕-๑๙		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ต่อไป
๓ (Medium)	๑๐-๑๔		ระดับที่พอยอมรับได้ แต่ต้องใช้ความพยายามที่จะลดความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
๒ (Low)	๕-๙		ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้นไปในระดับที่ยอมรับไม่ได้
๑ (Accept)	๑-๔		ระดับที่ยอมรับได้โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการใด ๆ เพิ่มเติม

(๔) เป็นการจัดเรียงระดับความรุนแรงของความเสี่ยงที่มีผลต่อการบรรลุเป้าหมายขององค์กร เพื่อพิจารณากำหนดมาตรการเพื่อควบคุมความเสี่ยงให้เหมาะสม โดยพิจารณาเลือกความเสี่ยงที่มีระดับรุนแรงหรือสูง มาจัดทำแผนการบริหารจัดการความเสี่ยงก่อน

๒.๑.๓ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

เป็นกระบวนการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดระดับความรุนแรงของความเสียหายให้อยู่ในระดับที่หน่วยงานยอมรับได้ หรือไม่มีความเสี่ยงหลงเหลืออยู่อีกต่อไป โดยการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลและดำเนินการควบคุมความเสี่ยงตามแผนที่กำหนดไว้ได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

(๑) ควบคุมแบบป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุมและการเข้าถึงเอกสาร เป็นต้น

(๒) การควบคุมแบบค้นพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับและการรายงานข้อบกพร่อง เป็นต้น

(๓) การควบคุมแบบส่งเสริม (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

(๔) การควบคุมแบบแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคต

หลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่า ได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก โดยใช้ขั้นตอน ดังนี้

(๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมากหรือสูง มากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

(๒) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

(๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๒.๑.๔ การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่กำหนดไว้

เป็นกระบวนการประเมินคุณภาพการปฏิบัติงานและประเมินประสิทธิผลของมาตรการควบคุมความเสี่ยงที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ โดยการติดตามผลในระหว่างการปฏิบัติงาน (Ongoing Monitoring) และการประเมินผลเป็นรายครั้ง (Separate Evaluation) ซึ่งแยกเป็นการประเมินผลมาตรการควบคุมด้วยตนเอง (Control Self-Assessment) เช่น การประเมินโดยผู้ปฏิบัติงานภายในส่วนงานนั้น ๆ และการประเมินผลมาตรการควบคุมอย่างเป็นอิสระ (Independent Assessment) เช่น การประเมินผลโดยผู้ตรวจสอบภายนอก (External auditors) เพื่อความมั่นใจว่า

(๑) มาตรการควบคุมความเสี่ยงที่กำหนดไว้เพียงพอ เหมาะสม มีประสิทธิภาพ และมีการปฏิบัติจริง

(๒) มาตรการควบคุมความเสี่ยงดำเนินไปอย่างมีประสิทธิผล

(๓) ข้อตรวจพบจากการตรวจสอบและการสอบทานอื่น ๆ ได้รับการปรับปรุงแก้ไขอย่างเหมาะสมและทันเวลา

(๔) ความเสี่ยงได้รับการปรับปรุงแก้ไขตามมาตรการควบคุมให้มีความสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

๒.๑.๕ การทบทวนการบริหารจัดการความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการทบทวนผลภายหลังจากได้ดำเนินการตามแผนการบริหารจัดการความเสี่ยงเสร็จเรียบร้อยแล้วว่ายังมีความเสี่ยงหลงเหลืออยู่อีกหรือไม่ ถ้ายังมีอยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีมาตรการจัดการกับความเสี่ยงนั้นอย่างไร เพื่อให้มั่นใจว่ามาตรการจัดการความเสี่ยงที่กำหนดไว้นั้นมีประสิทธิภาพ ทั้งนี้ เพื่อเป็นการประเมินคุณภาพและความเหมาะสมของมาตรการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการจัดการความเสี่ยง โดยอาจมีการการทบทวนผลในระหว่างการปฏิบัติงาน หรือทบทวนผลเป็นรายครั้งตามรอบระยะเวลา

๒.๒ ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

สนข. ได้กำหนดประเภทความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารออกได้เป็น ๖ ประเภท ดังนี้

๒.๒.๑ ความเสี่ยงด้านฮาร์ดแวร์

เป็นความเสี่ยงที่เกิดขึ้นกับอุปกรณ์ต่าง ๆ เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (PC) เครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ระบบเครือข่าย และสายสัญญาณ จนทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง ทำให้การปฏิบัติงานหรือการดำเนินงานด้านสารสนเทศของสำนักงานนโยบายและแผนการขนส่งและจราจรล่าช้าหรือไม่สามารถปฏิบัติงานได้ หรือทำให้ข้อมูลที่ทำการสำรอง (Backup) ไว้ชำรุดสูญหาย

๒.๒.๒ ความเสี่ยงด้านซอฟต์แวร์

เป็นความเสี่ยงที่เกิดจากโปรแกรมระบบ แอพพลิเคชัน รวมถึงโปรแกรมประยุกต์อื่น ๆ ที่ใช้งานทำงานผิดพลาดหรือใช้งานคุณสมบัติต่าง ๆ ได้ไม่ครบถ้วนเนื่องจากเป็นโปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่ใช้งานมีช่องโหว่และไม่มีการปรับปรุง (update) ให้เป็นรุ่นหรือเวอร์ชั่นปัจจุบัน ทำให้ผู้ไม่ประสงค์ดีสามารถบุกรุก (Hacker) เข้ามาในระบบเพื่อแก้ไขข้อมูล เปลี่ยนแปลงคำสั่ง หรือทำลายระบบ

๒.๒.๓ ความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ

เป็นความเสี่ยงที่เกิดขึ้นจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ เมื่อเกิดขึ้นแล้วจะสร้างความเสียหายแก่เครื่องคอมพิวเตอร์ส่วนบุคคล (PC) เครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ระบบเครือข่าย สายสัญญาณ ซึ่งความเสียหายมีตั้งแต่ระดับเสียหายเพียงบางส่วนไปจนถึงระดับเสียหายทั้งหมด ระบบฐานข้อมูลสารสนเทศหยุดทำงานทั้งระบบ จนทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง ทำให้การปฏิบัติงานหรือการดำเนินงานด้านสารสนเทศของสำนักงานนโยบายและแผนการขนส่งและจราจรล่าช้าหรือไม่สามารถปฏิบัติงานได้

๒.๒.๔ ความเสี่ยงด้านระบบเครือข่ายและอินเตอร์เน็ต

เป็นความเสี่ยงหรือภัยต่างๆ ที่อาจเกิดขึ้นกับระบบเครือข่ายขององค์กร ทั้งระบบอินทราเน็ต (Intranet) และอินเทอร์เน็ต (Internet) ระบบเครือข่ายภายใน (Local Area Network : LAN) ที่เกิดจากความผิดพลาดในการตั้งค่าอุปกรณ์เครือข่าย การเคลื่อนย้ายตัวอุปกรณ์หรือการติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ความเสื่อมสภาพของอุปกรณ์ตามกาลเวลา ความเสียหายของอุปกรณ์ที่เกิดขึ้นกระทันหัน การถูกโจมตีจากโปรแกรมมัลแวร์ต่าง ๆ ทำให้ระบบเทคโนโลยีสารสนเทศของ สนข. ไม่สามารถให้บริการได้หรือหยุดทำงานทั้งระบบ

๒.๒.๕ ความเสี่ยงด้านความมั่นคงปลอดภัย

ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ชั่วคราว ผู้ใช้งาน (User) ไม่สามารถเข้ามาใช้งานในระบบได้ทั้งหมด ทำความเสียหายระยะยาวให้แก่อุปกรณ์คอมพิวเตอร์ และเมื่อมีกระแสไฟฟ้าขัดข้องหรือดับบ่อยครั้งจะส่งผลให้เกิดความเสียหายที่ถาวรแก่ข้อมูลไม่สามารถกู้กลับข้อมูลได้

ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำไปแสวงหาประโยชน์โดยมิชอบได้ ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิแก่บุคคลที่มีหน้าที่รับผิดชอบให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ ส่งผลให้ไม่สามารถปฏิบัติงานได้ ระบบขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ ทำให้ข้อมูลและการทำงานของระบบเสียหาย ส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้ สูญเสียค่าใช้จ่ายในการเก็บรวบรวมข้อมูล ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข

มีไวรัสแพร่กระจายรบกวนการทำงานของระบบและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ มีการส่งหรือรับข้อมูลในเครือข่ายของหน่วยงานเป็นปริมาณสูงมากผิดปกติ ซึ่งปริมาณข้อมูลในเครือข่ายที่สูงเกินไปนี้จะมีผลทำให้การใช้งานเครือข่ายเป็นไปอย่างล่าช้า ติดขัด หรืออาจไม่สามารถใช้งานได้

เกิดความสับสนในกระบวนการกู้คืนข้อมูล หรือ Set up ระบบเครือข่ายไม่เสร็จทันตามกำหนดเวลา ทำให้ระบบงานต่าง ๆ เกิดหยุดชะงัก และเสียเวลาในการกู้คืนระบบมากเกินไป

๒.๒.๖ ความเสี่ยงด้านตัวบุคคลและการใช้งาน

เป็นความเสี่ยงที่เกิดจากการขาดการตรวจสอบระบบรักษาความปลอดภัยในการเข้า - ออกห้องศูนย์ข้อมูล ทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้าถึงห้องศูนย์ข้อมูลได้ และอาจจะทำลายเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ระบบเครือข่าย ก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลสารสนเทศของ สนข. ได้ หรืออาจทำการขโมยข้อมูล คัดลอกข้อมูล แก้ไขเปลี่ยนแปลงข้อมูล หรือล่วงรู้ข้อมูลที่เป็นความลับ และอาจนำข้อมูลนี้ไปแสวงหาผลประโยชน์โดยมิชอบ หรือแก้ไขเปลี่ยนแปลงค่าการทำงานของระบบ หรือแก้ไขสิทธิ์ให้บุคคลที่ไม่มีอำนาจสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลสารสนเทศในฐานะผู้ดูแลระบบ (Administrator) ได้ หรือแก้ไขสิทธิ์ให้ผู้ดูแลระบบเข้าถึงระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลสารสนเทศในฐานะผู้ใช้งานระบบทั่วไป (User) เพื่อทำให้ไม่สามารถปฏิบัติงานได้

๒.๓ การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินตามระดับความสำคัญแล้ว ต้องมีวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้ เพื่อให้การบริหารจัดการความเสี่ยงมีประสิทธิผลสูงสุดอาจต้องเลือกวิธีการจัดการความเสี่ยงวิธีใดวิธีหนึ่งหรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่จะเกิดขึ้น (Likelihood) และความรุนแรงของผลกระทบ (Impact) ของเหตุการณ์ให้อยู่ในระดับที่องค์กรสามารถยอมรับได้ (Risk Tolerance) ซึ่งวิธีการจัดการความเสี่ยงมี ๔ ประการ (๔T) ด้วยกัน ดังนี้

๒.๓.๑ การหลีกเลี่ยง (Terminate)

เป็นวิธีการที่ง่ายที่สุดในการบริหารจัดการความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ หรือหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มค่ากับสิ่งที่จะเกิดขึ้น จึงเลือกหลีกเลี่ยงที่จะเผชิญกับกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้นโดยมิได้คิดทบทวนถึงผลที่จะได้รับ ซึ่งอาจนำมาซึ่งการเสียโอกาสของหน่วยงานได้

๒.๓.๒ การยอมรับ (Take)

เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ต้องจัดการใด ๆ เลย และยอมรับผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสที่จะเกิดและระดับความรุนแรงของความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างกิจกรรมสำหรับการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้ User/Password ที่กำหนดให้แล้วอาจจะบอก User/Password ของตนให้ผู้ใต้บังคับบัญชาทราบ และเมื่อผู้ใต้บังคับบัญชาทราบ User/Password ของหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย และหน่วยงานที่รับผิดชอบต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น แล้วจึงแก้ไขโดยการกำหนด User/Password ใหม่ ให้กับหัวหน้างาน เป็นต้น

๒.๓.๓ การควบคุม (Treat)

เป็นการปรับปรุงกระบวนการทำงาน หรือการออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีการควบคุมความสูญเสียมี ๒ วิธี คือ

(๑) การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย คือ การหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคลหรือไวรัสคอมพิวเตอร์มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ เป็นต้น

(๒) การควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดระดับความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควันเครื่องตรวจจับความร้อนหรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้องศูนย์ข้อมูล เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายในห้องศูนย์ข้อมูล ให้มีความเสียหายน้อยที่สุด หรือไม่ให้เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่ายแต่อย่างใด เป็นต้น

๒.๓.๔ การถ่ายโอน (Transfer)

การโอนย้ายหรือกระจายความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะเวลาในการรับประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขายให้ทันก่อนระยะเวลาในการรับประกันจะสิ้นสุด

๒.๔ ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลสารสนเทศของ สนข. มีดังนี้

๒.๔.๑ ปัจจัยภายนอก ได้แก่

(๑) ความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ

(๒) ความเสี่ยงด้านความมั่นคงปลอดภัย

(๓) ความเสี่ยงด้านระบบเครือข่ายและอินเตอร์เน็ต

๒.๔.๒ ปัจจัยภายใน ได้แก่

(๑) ความเสี่ยงด้านซอฟต์แวร์

(๒) ความเสี่ยงด้านฮาร์ดแวร์

(๓) ความเสี่ยงด้านระบบเครือข่ายและอินเตอร์เน็ต

(๔) ความเสี่ยงด้านความมั่นคงปลอดภัย

(๕) ความเสี่ยงด้านตัวบุคคลและการใช้งาน

๒.๕ การประเมินความเสียหาย

๒.๕.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่

(๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบ

(๒) การขโมยเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบฐานข้อมูลสารสนเทศ อุปกรณ์ระบบเครือข่ายรวมถึงข้อมูลสารสนเทศที่เก็บไว้ภายในระบบฐานข้อมูลสารสนเทศ

(๓) การชำรุดเสียหายของ Server หรืออุปกรณ์ระบบเครือข่าย จากการเคลื่อนย้าย หรือความเสียหายที่เกิดขึ้นจากภัยพิบัติต่าง ๆ

(๔) ตัวเครื่องประมวลผลหลักหรือ Server และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒.๕.๒ ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบประมวลผลทั้งระบบลงชั่วขณะ ได้แก่

(๑) การถูกเจาะเข้าระบบฐานข้อมูล

(๒) วงจรสื่อสารของระบบเครือข่ายคอมพิวเตอร์หลัก (Core Network) เสียหาย/ขัดข้อง

(๓) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/โดยตัดกระแสไฟ

๒.๖ การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

๒.๗ เทคโนโลยีสารสนเทศขององค์กร

สนข. มีภารกิจเกี่ยวกับการเสนอแนะนโยบายและจัดทำแผนหลัก แผนแม่บท และยุทธศาสตร์การพัฒนาระบบการขนส่งและจราจร ความปลอดภัยและสิ่งแวดล้อมในระบบการขนส่งของประเทศ รวมทั้งปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของสำนักงานหรือตามที่รัฐมนตรีหรือคณะรัฐมนตรีมอบหมาย และต้องมีการเผยแพร่ข้อมูลข่าวสารด้านการขนส่งและจราจรตาม พ.ร.บ. ข้อมูลข่าวสาร พ.ศ.๒๕๔๐ ข้อมูลข่าวสารภายในขององค์กร และการให้บริการระบบงานต่าง ๆ ดังต่อไปนี้

๒.๗.๑ ระบบอินเตอร์เน็ต

สำหรับให้บริการข้อมูลข่าวสารด้านการขนส่งและจราจร ข้อมูลการจัดซื้อจัดจ้าง ข้อมูลการรับสมัครงาน ข้อมูลโครงการศึกษาของ สนข. บทความวิชาการ และข้อมูลอื่น ๆ

๒.๗.๒ ระบบอินทราเน็ต

สำหรับให้บริการข้อมูลข่าวสารภายในองค์กรแก่บุคลากรของ สนข. เช่น ข่าวประชาสัมพันธ์ ประกาศ คำสั่ง หนังสือเวียน แผนยุทธศาสตร์ เอกสารเผยแพร่องค์ความรู้ขององค์กร

๒.๗.๓ ระบบงานบริหารสำนักงานอัตโนมัติ ใช้สนับสนุนการปฏิบัติงานของบุคลากรให้มีความสะดวกต่อเนื่อง รวดเร็ว มีประสิทธิภาพ และพร้อมใช้งานได้ตลอดทุกที่ทุกเวลา เช่น ระบบสารบรรณ, ระบบสร้าง-ส่ง/เวียน-ลงนามเอกสาร, ระบบบุคลากร, ระบบจองห้องประชุม จองรถยนต์ และทรัพย์สิน เป็นต้น

๒.๗.๔ ระบบเผยแพร่ข้อมูลสารสนเทศการขนส่งและจราจร (MIS) ระบบสารสนเทศเพื่อการบริหาร (EIS) และระบบภูมิสารสนเทศการขนส่งและจราจร (GIS) สำหรับการวางแผน กำหนดนโยบาย และบริหารจัดการด้านการขนส่งและจราจรในระดับประเทศ

๒.๗.๕ ระบบพิสูจน์ตัวตน (Active Directory) เพื่อใช้สำหรับตรวจสอบตัวบุคคลและสิทธิ์การเข้าถึงหรือเข้าใช้งานว่า ผู้ที่เข้าใช้งานระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตนั้นคือใคร มีสิทธิ์ในการเข้าถึงข้อมูลในระดับใด และสามารถใช้งานทรัพยากรของระบบภายในอะไรได้บ้าง

๒.๗.๖ ระบบฐานข้อมูลแอปพลิเคชันนำทาง (NAMTANG) คือแอปพลิเคชันที่พัฒนาขึ้นเพื่อให้บริการประชาชนในการวางแผนและตัดสินใจในการเลือกใช้เส้นทางและขนส่งสาธารณะทั้งทางถนน ทางราง และทางน้ำภายในเขตกรุงเทพมหานครและปริมณฑล ที่มีความถูกต้อง เหมาะสม สะดวกและรวดเร็วผ่านทางเว็บแอปพลิเคชัน

และโมบายแอปพลิเคชัน ที่ชื่อว่า **“นำทาง”** (NAMTANG) รองรับการใช้งานได้หลากหลาย ทั้งระบบปฏิบัติการ Windows, iOS และ Android

๒.๗.๗ ระบบสำรองข้อมูลสารสนเทศและกู้คืน (Backup & Recovery System) เพื่อใช้สำหรับจัดเก็บและสำรองข้อมูลสำหรับใช้ในการกู้คืนการทำงานของระบบสารสนเทศของ สนข. ให้กลับมาทำงานได้ตามปกติโดยเร็วตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของ สนข. และแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ของ สนข.

และระบบงานที่จะเกิดขึ้นในอนาคต ดังต่อไปนี้

๒.๗.๘ ระบบการเรียนและฝึกอบรมผ่านเครือข่ายอินเทอร์เน็ต (e-Learning)

การนำเทคโนโลยีสารสนเทศเหล่านี้มาใช้งานก็เพื่อเป็นการยกระดับการปฏิบัติงานและการให้บริการของ สนข. ให้สามารถตอบสนองความต้องการข้อมูลข่าวสารด้านการขนส่งและจราจรแก่หน่วยงานที่เกี่ยวข้องและประชาชนได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ดังนั้นระบบฐานระบบเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศของ สนข. จึงมีความสำคัญเป็นอย่างยิ่ง เนื่องจากเป็นส่วนที่เก็บข้อมูลดิบ (Raw Data) สำหรับใช้ในการประมวลผลเพื่อให้ได้สารสนเทศที่ตรงตามความต้องการและนำมาเผยแพร่ผ่านระบบเทคโนโลยีสารสนเทศช่องทางต่าง ๆ เช่น เว็บไซต์ โซเชียลมีเดีย เป็นต้น ซึ่งในปัจจุบันระบบฐานระบบเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศของ สนข. ต่าง ๆ ที่กล่าวมานี้ ถูกจัดเก็บไว้ภายในฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ให้บริการระบบงานนั้น ๆ เพียงแห่งเดียวโดยไม่มีการสำรองข้อมูลแยกไว้ต่างหาก ในกรณีที่ฮาร์ดดิสก์ที่ใช้จัดเก็บข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายหรือตัวเครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย ข้อมูลหรือระบบฐานข้อมูลสารสนเทศภายในฮาร์ดดิสก์ก็อาจได้รับความเสียหายจนไม่สามารถใช้งานได้ด้วย ย่อมก่อให้เกิดความเสียหายต่อ สนข. ได้

๒.๘ การรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของ สนข.

ระบบเครือข่ายคอมพิวเตอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) ได้มีการปรับปรุงและพัฒนามาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบเครือข่ายคอมพิวเตอร์ของ สนข. เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ

ระบบเครือข่ายคอมพิวเตอร์หลักของ สนข. (Core Network) ตั้งอยู่ที่ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร ทำหน้าที่เป็นศูนย์กลางในการให้บริการระบบเครือข่ายภายใน (Local Area Network) ของ สนข. ที่ความเร็วระดับ ๑,๐๐๐ Mbps นอกจากนี้ยังเชื่อมโยงกับระบบเครือข่ายอินเทอร์เน็ตของบริษัท ทีโอที จำกัด ที่ความเร็ว ๒๐๐ Mbps ระบบเครือข่ายของสำนักงานปลัดกระทรวงคมนาคม (MOTNET) ที่ความเร็วระดับ ๑๖ Mbps และระบบเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ที่ความเร็วระดับ ๒๐ Mbps เพื่อรองรับการสื่อสารข้อมูลหรือการสื่อสารรูปแบบอื่นในอนาคต ซึ่งมีอุปกรณ์ Core Switch ที่มีประสิทธิภาพสูงรองรับการทำงานได้แบบ ๒๔x๗ (ตลอดเวลา) ที่เชื่อมต่อไปยังอุปกรณ์ Distributed Switch (L๓), Access Switch (L๒) และ End Node ที่ติดตั้งอยู่ตามชั้นต่าง ๆ ซึ่งเป็นที่ตั้งของสำนัก/กอง/ศูนย์/สำนักงานโครงการ/กตส./กพร. ของ สนข.

ระบบเครือข่ายคอมพิวเตอร์ของ สนข. มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งอุปกรณ์ฮาร์ดแวร์และระบบซอฟต์แวร์ในการทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังระบบเครือข่ายคอมพิวเตอร์ของ สนข. โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ของ Fortigate ซึ่งใช้คัดกรองแพ็กเก็ตข้อมูล (Packet Filter) ที่ผ่านเข้ามาภายในระบบ

เครือข่ายคอมพิวเตอร์ของ สนข. จากเครือข่ายภายนอก เช่น เครือข่ายของสำนักงานปลัดกระทรวงคมนาคม เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ เครือข่ายอินเทอร์เน็ต และใช้ซอฟต์แวร์ระบบพิสูจน์ตัวตน (Active Directory : AD) ทำหน้าที่จัดเก็บทะเบียนผู้ใช้งานเพื่อกำหนดตัวตนและสิทธิ์การใช้งานของผู้ใช้แต่ละคนดังนี้

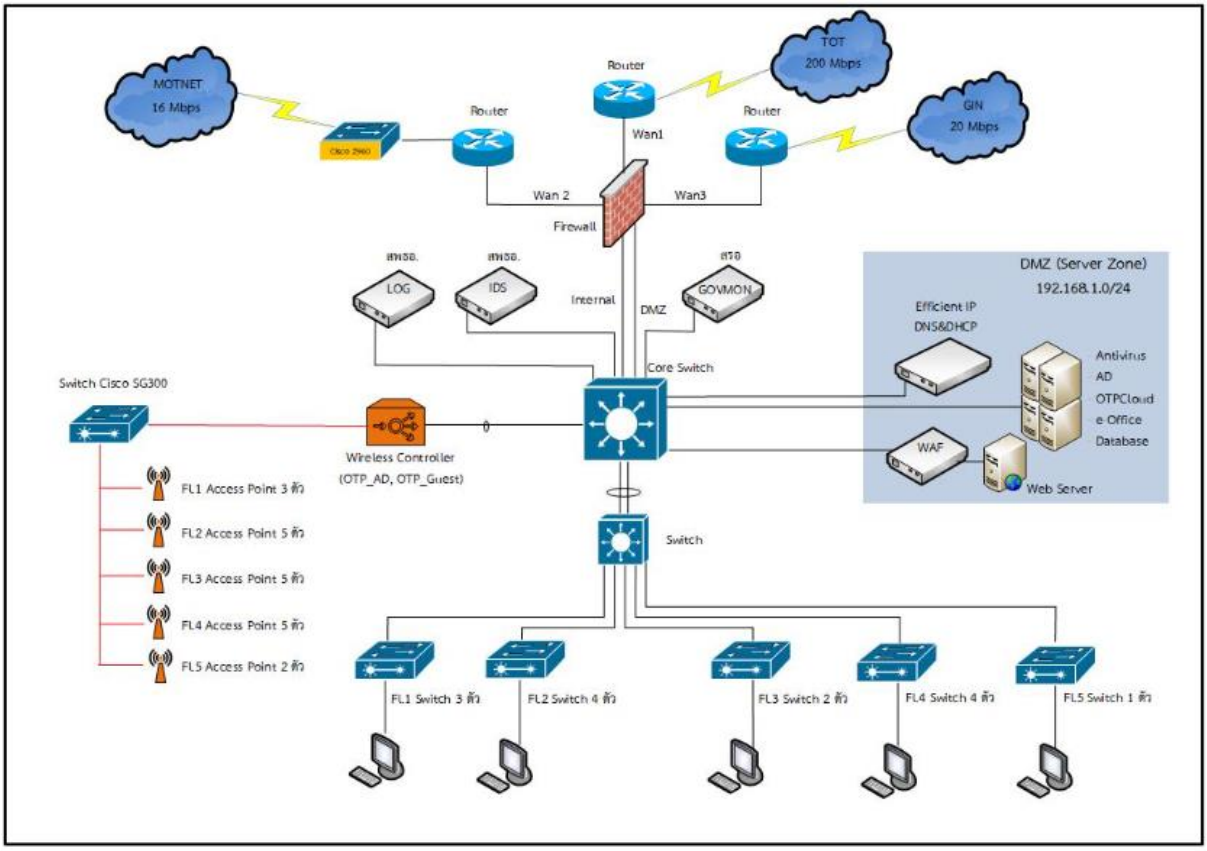
๒.๒.๑ การพิสูจน์ตัวตนในการเข้าใช้งานระบบ (Authentication)

๒.๒.๒ การตรวจสอบสิทธิในการใช้งานหรือการเข้าถึงระบบตามที่กำหนด (Authorization)

๒.๒.๓ การเก็บข้อมูลและบันทึกว่าแต่ละคนได้ดำเนินการอะไรในระบบบ้าง เพื่อเก็บไว้เป็นข้อมูลในการตรวจสอบ (Accounting)

และยังมีการกำหนด Server Zone หรือ *Demilitarized Zone* (DMZ) สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายของ สนข. ที่อนุญาตให้บุคคลภายนอกเข้าถึงได้ เช่น Web Server และ Mail Server เป็นต้น รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบและป้องกันเครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่ออยู่ภายในระบบเครือข่ายคอมพิวเตอร์ของ สนข. ให้ได้รับความปลอดภัย

สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลทั้งหมดที่อยู่ในระบบเครือข่ายคอมพิวเตอร์ของ สนข. ได้มีการกำหนดนโยบาย มาตรการ และข้อปฏิบัติในการใช้งานอย่างเข้มงวด รวมถึงมีการติดตั้งโปรแกรมป้องกันไวรัสเพื่อให้มีความมั่นคงปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ของ สนข. ทั้งหมด ดังแสดงในรูปที่ ๒-๓



รูปที่ ๒-๓ แสดงแผนภูมิระบบเครือข่ายคอมพิวเตอร์ของ สนข.

บทที่ ๓
การทบทวนและวิเคราะห์การบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข.

สนข. ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจเสียหายอันเนื่องมาจากปัจจัยเสี่ยงต่าง ๆ ได้ดำเนินการนำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ปีงบประมาณ พ.ศ. ๒๕๖๓ มาทบทวนและปรับปรุงใหม่ เพื่อให้สอดคล้องและทันต่อสถานการณ์ความเสี่ยงในปัจจุบัน โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงาน เริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยงหรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้น ๆ ในการระบุ/บ่งชี้ความเสี่ยง การประเมินโอกาสที่จะเกิดความเสี่ยงและความรุนแรงของผลกระทบ การประเมินระดับความเสี่ยง การตอบสนองและการจัดการความเสี่ยง การจัดทำแผนบริหารจัดการความเสี่ยง การติดตามและทบทวน การสรุปผลและรายงานผล ดังต่อไปนี้

๓.๑ ผลการทบทวน IT Risk Management Plan ปีงบประมาณ พ.ศ. ๒๕๖๓ ของ สนข.

ศทท. ได้ดำเนินการทบทวน IT Risk Management Plan ของ สนข. ปีงบประมาณ พ.ศ. ๒๕๖๓ สรุปได้ ดังนี้

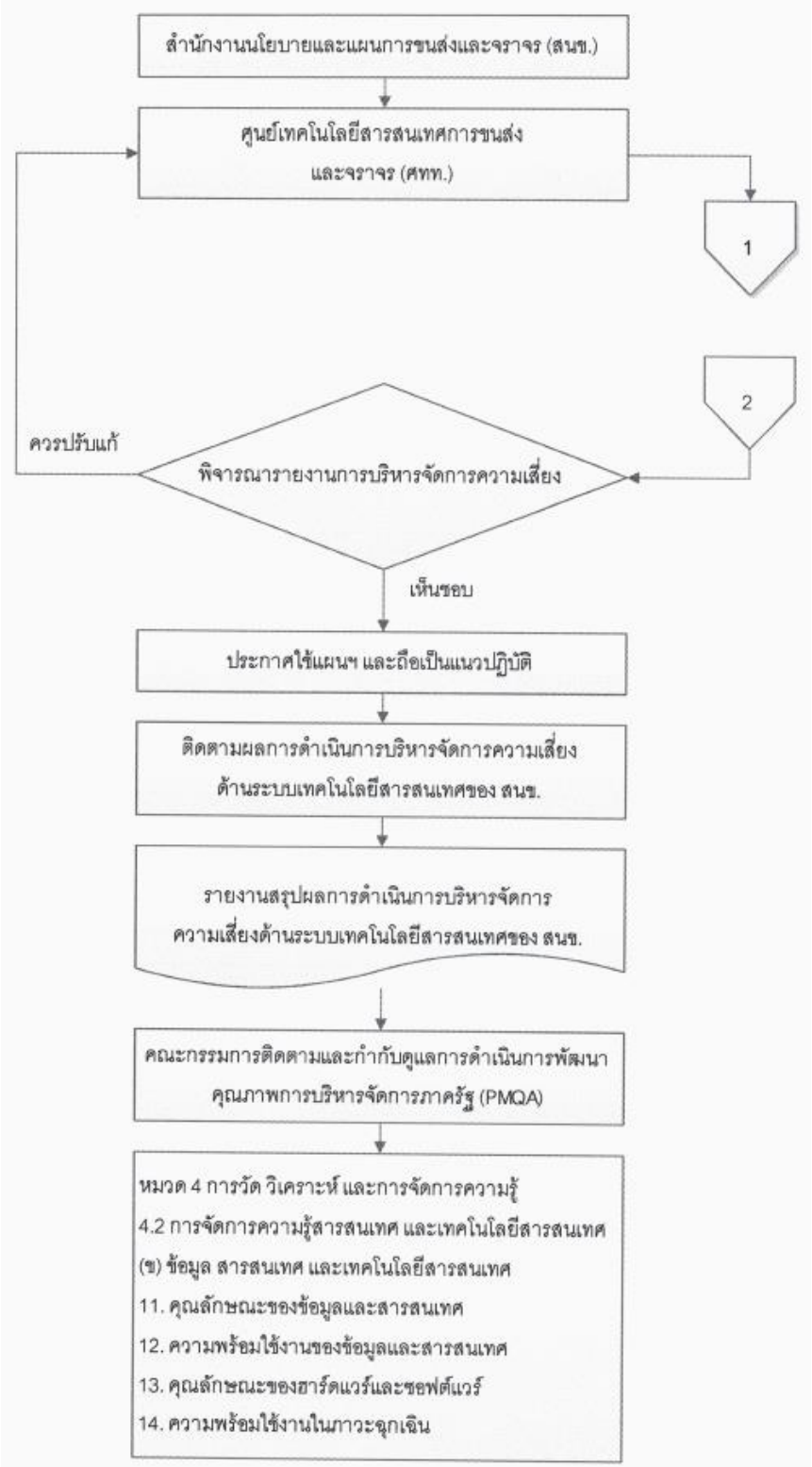
ประเภทความเสี่ยง	ความเสี่ยง	ผลการทบทวน
๑. ความเสี่ยงด้านฮาร์ดแวร์	๑. อุปกรณ์คอมพิวเตอร์ชำรุดเสียหาย	- ได้ดำเนินการตามแผน โดยมีการสำรองข้อมูลเป็นประจำทุกเดือน - ศทท. ได้ดำเนินการแก้ไขอุปกรณ์คอมพิวเตอร์ในเบื้องต้นให้สามารถใช้งานได้ รวมทั้ง จัดหาอุปกรณ์ทดแทน ในกรณีที่ไม่สามารถซ่อมแซมได้ หรือดำเนินโครงการจัดหาอุปกรณ์เพื่อทดแทน
	๒. อุปกรณ์คอมพิวเตอร์ถูกขโมย	- ได้ดำเนินการตามแผน โดยมีการตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV, Access Control เป็นประจำทุกเดือน

ประเภทความเสี่ยง	ความเสี่ยง	ผลการทบทวน
๒. ความเสี่ยงด้านซอฟต์แวร์	- ซอฟต์แวร์ระบบฐานข้อมูล/โปรแกรมหรือแอพพลิเคชันเสียหาย	ได้ดำเนินการตามแผน โดยมีการ - สำรองไฟล์ระบบแบบ Full Backup เป็นประจำทุกเดือน - สำรองไฟล์ระบบแบบ Incremental เป็นประจำทุกสัปดาห์หรือทุกวัน - จัดซื้อ/จัดหาซอฟต์แวร์หรือ License เพิ่มเติม ตามความจำเป็นและความต้องการของสำนัก/กอง/ศูนย์/สำนักงานโครงการ/กตส./กพร.
๓. ความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ	๑. ระบบไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า	- ได้ดำเนินการตามแผน โดยมีการตรวจสอบความพร้อมใช้งานของ UPS เป็นประจำทุกเดือน
	๒. การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data Room)	- ได้ดำเนินการตามแผน โดยมีการตรวจสอบความพร้อมใช้งานของระบบดับเพลิงและระบบเตือนภัยอัตโนมัติ (Automatic Warning System) เป็นประจำทุกเดือน
	๓. ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า, แผ่นดินไหว, น้ำท่วม	ได้ดำเนินการตามแผน โดยมีการ - ตรวจสอบการติดตั้ง/จัดวางอุปกรณ์ต่าง ๆ ทั้งภายนอกและภายในตู้ Rack ทั้งหมด เป็นประจำทุกเดือน - ตรวจสอบพร้อมใช้งานของระบบดับเพลิงและระบบเตือนภัยอัตโนมัติ (Automatic Warning System) เป็นประจำทุกเดือน
	๔. เครื่องปรับอากาศภายในห้องศูนย์ข้อมูลไม่ทำงาน	- ได้ดำเนินการตามแผน โดยมีการตรวจสอบความพร้อมใช้งานของเครื่องปรับอากาศเป็นประจำทุกเดือน
๔. ความเสี่ยงด้านระบบเครือข่ายและอินเตอร์เน็ต	- ระบบเครือข่ายหลักเสียหาย/ขัดข้อง ไม่สามารถใช้งานได้	ได้ดำเนินการตามแผน โดยมีการ - ตรวจสอบสถานะความพร้อมใช้งานของระบบเครือข่ายหลักเป็นประจำทุกเดือน - ตรวจสอบสถานการณ์ทำงานของอุปกรณ์เครือข่ายเป็นประจำทุกเดือน - สำรองค่าการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายแต่ละตัวไว้เป็นประจำทุกเดือน

ประเภทความเสี่ยง	ความเสี่ยง	ผลการทบทวน
๕. ความเสี่ยงด้านความมั่นคงปลอดภัย	๑. ถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี	ได้ดำเนินการตามแผน โดยมีการ - ตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall เป็นประจำทุกเดือน - ตรวจสอบสถานการณ์ทำงานของโปรแกรมป้องกันมัลแวร์ต่าง ๆ เป็นประจำทุกเดือน - ปรับปรุงโปรแกรมป้องกันมัลแวร์ต่าง ๆ ให้เป็นปัจจุบัน ซึ่งจะดำเนินการทันทีที่เจ้าของผลิตภัณฑ์แจ้งให้ทราบ
	๒. การเข้าถึงห้องศูนย์ข้อมูลโดยไม่ได้รับอนุญาต	- ได้ดำเนินการตามแผน โดยมีการตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV, Access Control เป็นประจำทุกเดือน
	๓. ระบบคอมพิวเตอร์ถูกเจาะ (Hack)	- ได้ดำเนินการตามแผน โดยมีการตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall เป็นประจำทุกเดือน
	๔. การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์	- ได้ดำเนินการตามแผน โดยมีการทดสอบการกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศจาก Backup File เป็นประจำทุก ๖ เดือน
	๕. การก่อความไม่สงบ/จราจล	ได้ดำเนินการตามแผน โดยมีการ - ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV, Access Control เป็นประจำทุก ๖ เดือน - ทดสอบการกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศจาก Backup File เป็นประจำทุก ๖ เดือน
๖. ความเสี่ยงด้านตัวบุคคลและการใช้งาน	๑. การใช้งานซอฟต์แวร์เถื่อนหรือซอฟต์แวร์ละเมิดลิขสิทธิ์	- ได้ดำเนินการตามแผน โดยมีการจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความเหมาะสมและความต้องการของสำนัก/กอง/ศูนย์/สำนักงานโครงการ/กตส./กพร.
	๒. การใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ผิดวัตถุประสงค์	ได้ดำเนินการตามแผน โดยมีการ - รายงานผลการใช้งานระบบเครือข่าย

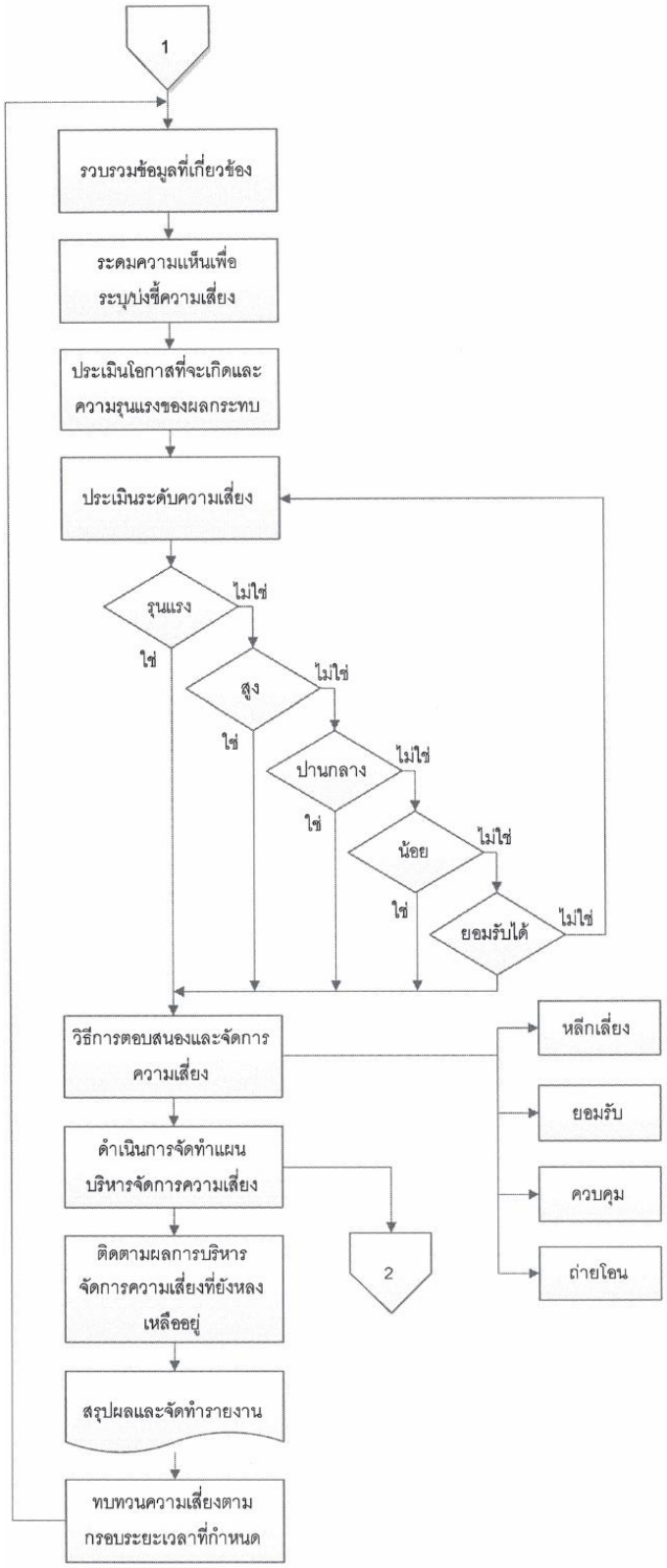
ประเภทความเสี่ยง	ความเสี่ยง	ผลการทบทวน
		และเครื่องคอมพิวเตอร์ของผู้ใช้งานทันทีที่ทราบ - ตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall เป็นประจำทุกเดือน

๓.๒ กระบวนการจัดทำแผนบริหารจัดการความเสี่ยงของ สนข.



แผนภาพที่ ๓-๑ กระบวนการจัดทำแผนบริหารจัดการความเสี่ยง

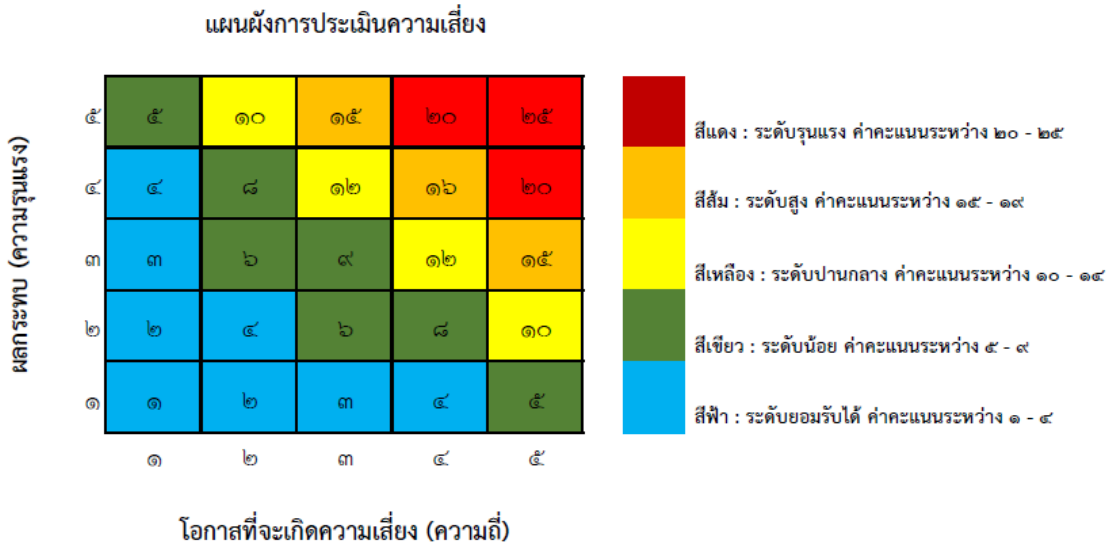
๓.๓ ขั้นตอนการดำเนินการบริหารจัดการความเสี่ยงของ สนข.



แผนภาพที่ ๓-๒ ขั้นตอนการดำเนินการบริหารจัดการความเสี่ยง

๓.๔ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข.

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่องค์กรเผชิญอยู่ ผลสรุปการกำหนดประเด็นความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ รวมทั้งการประเมินโอกาสที่จะเกิดความเสี่ยง ความรุนแรงของผลกระทบ และระดับความเสี่ยง ดังนี้



รูปที่ ๓-๑ ช่วงคะแนนการประเมินความเสี่ยง

สนข. ได้พิจารณาทบทวนแผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ของ สนข. ปีงบประมาณ พ.ศ. ๒๕๖๓ ที่ผ่านมา ซึ่งมีการจัดแบ่งความเสี่ยงออกเป็น ๖ ประเภท รวมจำนวน ๑๕ ความเสี่ยง ดังแสดงในตารางที่ ๓-๑ ซึ่งพบว่ายังครอบคลุมการทำงานของ สนข. อยู่ จึงยังคงบรรจุไว้ในแผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ของ สนข. ปีงบประมาณ พ.ศ. ๒๕๖๓ โดยสรุปรายละเอียดรายการความเสี่ยงและระดับความเสี่ยงดังแสดงในตารางที่ ๓-๑

ตารางที่ ๓-๑ รายการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข.

ลำดับที่	ความเสี่ยง	ประเภทความเสี่ยง	ระดับโอกาสที่จะเกิดขึ้น (a)	ระดับผลกระทบ (ความรุนแรง) (b)	คะแนนรวม (a x b)	
๑	ถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี	๕	๕	๕	๒๕	สูงมาก
๒	ซอฟต์แวร์ระบบฐานข้อมูล/โปรแกรมหรือแอพพลิเคชั่นเสียหาย	๒	๔	๕	๒๐	สูง
๓	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า	๓	๔	๔	๑๖	
๔	การเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต	๕	๓	๕	๑๕	

ลำดับที่	ความเสี่ยง	ประเภทความเสี่ยง	ระดับโอกาสที่จะเกิดขึ้น (a)	ระดับผลกระทบ (ความรุนแรง) (b)	คะแนนรวม (a x b)	
๕	อุปกรณ์คอมพิวเตอร์ชำรุดเสียหาย	๑	๒	๕	๑๐	ปานกลาง
๖	การใช้งานระบบซอฟต์แวร์เถื่อนหรือซอฟต์แวร์ละเมิดลิขสิทธิ์	๖	๓	๓	๙	
๗	ระบบเครือข่ายหลักเสียหาย/ขัดข้อง ไม่สามารถใช้งานได้	๔	๒	๓	๖	
๘	การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data room)	๓	๑	๕	๕	
๙	ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า แผ่นดินไหว และน้ำท่วม)	๓	๑	๕	๕	
๑๐	ระบบคอมพิวเตอร์ถูกเจาะ (Hack)	๕	๑	๕	๕	
๑๑	การใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ผิดวัตถุประสงค์	๖	๕	๑	๕	
๑๒	อุปกรณ์คอมพิวเตอร์ถูกขโมย	๑	๑	๕	๕	
๑๓	การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์	๕	๑	๔	๔	
๑๔	เครื่องปรับอากาศห้องศูนย์ข้อมูลไม่ทำงาน	๓	๑	๔	๔	
๑๕	การก่อความไม่สงบ/จลาจล	๕	๑	๓	๓	

<u>หมายเหตุ</u>

- ประเภทความเสี่ยง : ๑ หมายถึง ความเสี่ยงด้าน Hardware
  ๒ หมายถึง ความเสี่ยงด้าน Software
  ๓ หมายถึง ความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ
  ๔ หมายถึง ความเสี่ยงด้านระบบเครือข่ายและ Internet
  ๕ หมายถึง ความเสี่ยงด้านความมั่นคงปลอดภัย
  ๖ หมายถึง ความเสี่ยงด้านตัวบุคคลและการใช้งาน

• ระดับโอกาสที่จะเกิดขึ้นและระดับผลกระทบ :

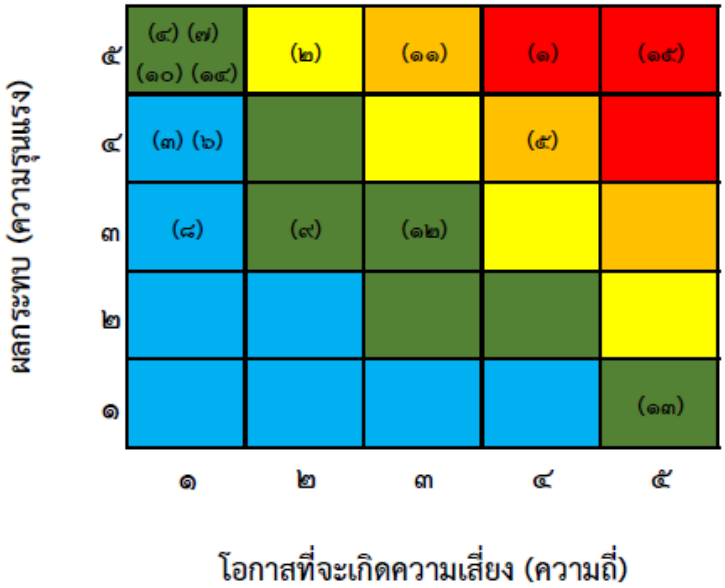
๑ หมายถึง น้อยมาก

๒ หมายถึง น้อย

๓ หมายถึง ปานกลาง

๔ หมายถึง สูง

๕ หมายถึง สูงมาก



รูปที่ ๓-๒ ระดับความเสี่ยงแต่ละรายการก่อนเริ่มดำเนินการจัดการความเสี่ยง

พร้อมทั้งดำเนินการจัดทำร่างแผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ของ สนข. ปีงบประมาณ พ.ศ. ๒๕๖๔ และกรอบระยะเวลาของกิจกรรมควบคุมความเสี่ยงแต่ละปัจจัยเสร็จเรียบร้อยแล้ว **ซึ่งระบุรายการความเสี่ยงเพื่อดำเนินการบริหารจัดการความเสี่ยงได้เป็น ๖ ประเภท รวมจำนวน ๑๕ ความเสี่ยง** พร้อมทั้งกรอบระยะเวลาของกิจกรรมควบคุมความเสี่ยงแต่ละปัจจัยเสร็จเรียบร้อยแล้ว ดังนี้

๓.๔.๑ ความเสี่ยงด้านฮาร์ดแวร์ ประกอบด้วย (๑) อุปกรณ์คอมพิวเตอร์ชำรุดเสียหาย และ (๒) อุปกรณ์คอมพิวเตอร์ถูกขโมย

๓.๔.๒ ความเสี่ยงด้านซอฟต์แวร์ ประกอบด้วย ซอฟต์แวร์ระบบฐานข้อมูล/โปรแกรมหรือแอพพลิเคชันเสียหาย

๓.๔.๓ ความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ ประกอบด้วย (๑) ระบบไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า (๒) การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data Room) (๓) ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า แผ่นดินไหว น้ำท่วม และ (๔) เครื่องปรับอากาศภายในห้องศูนย์ข้อมูลไม่ทำงาน

๓.๔.๔ ความเสี่ยงด้านระบบเครือข่ายและอินเตอร์เน็ต ประกอบด้วย ระบบเครือข่ายหลักเสียหาย/ขัดข้องไม่สามารถใช้งานได้

๓.๔.๕ ความเสี่ยงด้านความมั่นคงปลอดภัย ประกอบด้วย (๑) ถูกโปรแกรมมัลแวร์ประเภทต่างๆ โจมตี (๒) การเข้าถึงห้องศูนย์ข้อมูลโดยไม่ได้รับอนุญาต (๓) ระบบคอมพิวเตอร์ถูกเจาะ (Hack) (๔) การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์ รวมทั้ง (๕) การก่อความไม่สงบ/จราจล

๓.๔.๖ ความเสี่ยงด้านตัวบุคคลและการใช้งาน ประกอบด้วย (๑) การใช้งานซอฟต์แวร์เถื่อนหรือซอฟต์แวร์ละเมิดลิขสิทธิ์ และ (๒) การใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ผิดวัตถุประสงค์

โดยมีรายละเอียด ดังนี้

ตารางที่ ๓-๒ แผนการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
๑	ถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี	๑. ระบบสารสนเทศทำงานผิดพลาดจนไม่สามารถให้บริการได้ หรือหยุดทำงาน ๒. มีปริมาณข้อมูล (Traffic) บนระบบเครือข่ายสูงมากผิดปกติ ทำให้การให้บริการเป็นไปอย่างล่าช้าหรืออาจไม่สามารถใช้งานได้ ๓. มีอัตราการรับ - ส่งข้อมูล (Bandwidth) บนระบบเครือข่ายสูงมากผิดปกติ ทำให้การให้บริการเป็นไปอย่างล่าช้าหรืออาจไม่สามารถใช้งานได้	รุนแรง (๕x๕=๒๕)	๑. จัดทำแผนตรวจสอบสถานการณ์ทำงานของอุปกรณ์ Firewall ๒. จัดทำแผนตรวจสอบสถานการณ์ทำงานของโปรแกรมป้องกันมัลแวร์ต่าง ๆ ๓. ตรวจสอบโปรแกรมป้องกันมัลแวร์ต่าง ๆ ให้เป็นรุ่นปัจจุบัน ๔. จัดซื้อโปรแกรมป้องกันมัลแวร์ต่าง ๆ ในระดับองค์กรมาใช้งาน	๑. ตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall ตามระยะเวลาที่กำหนด ๒. ตรวจสอบสถานะการทำงานของโปรแกรมป้องกันมัลแวร์ต่าง ๆ ตามระยะเวลาที่กำหนด ๓. ปรับปรุง/อัพเดทโปรแกรมป้องกันมัลแวร์ต่าง ๆ ให้เป็นปัจจุบัน	ทุกเดือน ทุกเดือน ดำเนินการทันทีที่เจ้าของผลิตภัณฑ์แจ้งให้ทราบ	ศทท.
๒	ซอฟต์แวร์ระบบฐานข้อมูล/โปรแกรมหรือแอพพลิเคชั่นเสียหาย	๑. ไม่สามารถใช้งานระบบสารสนเทศได้ ๒. มีซอฟต์แวร์ไม่เพียงพอต่อความต้องการใช้งาน	รุนแรง (๔x๕=๒๐)	๑. จัดทำแผนการสำรองข้อมูล (Backup) ๒. สำรวจความต้องการใช้งานซอฟต์แวร์ต่าง ๆ ประจำปี	๑. ทำการสำรองไฟล์ระบบแบบ Full Backup เก็บไว้ใน External Hard Disk ๒. ทำการสำรองไฟล์ระบบแบบ Incremental หรือ Differential	ทุกเดือน ทุกสัปดาห์หรือทุกวัน	ศทท.

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
					เก็บไว้ใน External Hard Disk ๓. จัดซื้อ/จัดหาซอฟต์แวร์หรือ License เพิ่มเติม	ตามความจำเป็นและความต้องการของสำนัก/กอง/ศูนย์/สำนักงานโครงการ/กตส./กพร.	
๓	ระบบไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า	๑. ระบบเครือข่ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายหยุดทำงานชั่วคราว ๒. ผู้ใช้งานไม่สามารถใช้งานระบบสารสนเทศได้ ๓. ฮาร์ดดิสก์ (Hard Disk Drive) ชนิดจานแม่เหล็ก (Platters) เสียหายในระยะยาว ๔. ข้อมูลสารสนเทศสูญหาย	สูง (๔x๔=๑๖)	๑. จัดทำแผนตรวจสอบความพร้อมใช้งานของเครื่องสำรองไฟฟ้า (UPS) ๒. จัดหาแหล่งจ่ายไฟฟ้าสำรองเพิ่มเติม (หากมีความจำเป็น)	ตรวจสอบความพร้อมใช้งานของเครื่องสำรองไฟฟ้า (UPS)	ทุกเดือน	ศทท.
๔	การเข้าถึงห้องศูนย์ข้อมูลโดยไม่ได้รับอนุญาต	๑. บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถล่วงรู้ข้อมูลและอาจนำข้อมูลนี้ไปแสวงหาผลประโยชน์	สูง (๓x๕=๑๕)	จัดทำแผนตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง	ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV อุปกรณ์ควบคุม	ทุกเดือน	ศทท.

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
		โดยมิชอบได้ ๒. อุปกรณ์ต่าง ๆ ภายในห้องศูนย์ข้อมูล เช่น เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ฐานข้อมูล อาจถูกทำลายจนส่งผลให้เกิดความเสียหายกับทรัพย์สินของทางราชการและระบบสารสนเทศของ สนข. ไม่สามารถใช้งานได้ ๓. อุปกรณ์ต่าง ๆ ภายในห้องศูนย์ข้อมูล เช่น เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ฐานข้อมูล อาจถูกขโมย ส่งผลให้เกิดความเสียหายกับระบบสารสนเทศของ สนข. จนไม่สามารถใช้งานได้		CCTV อุปกรณ์ควบคุมการเข้า-ออก (Access Control) ตามระยะเวลาที่กำหนด และติดตั้งระบบรักษาความปลอดภัยสำหรับห้องศูนย์ข้อมูล (การ Scan นิ้ว เข้า-ออก ซึ่งอนุญาตเฉพาะเจ้าหน้าที่ที่ได้รับอนุญาต)	การเข้า-ออก (Access Control)		
๕	อุปกรณ์คอมพิวเตอร์ชำรุดเสียหาย	ข้อมูลสารสนเทศได้รับความเสียหาย หรือสูญหาย	ปานกลาง (๒x๕=๑๐)	จัดทำแผนการสำรองข้อมูล (Backup)	๑. ทำการสำรองข้อมูลระบบแบบ Full Backup เก็บไว้ใน External Hard Disk	ทุกเดือน	ศทท.

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
					๒. ทำการสำรองข้อมูลระบบแบบ Incremental หรือ Differential เก็บไว้ใน External Hard Disk	ทุกสัปดาห์หรือทุกวัน	
๖	การใช้งานซอฟต์แวร์เถื่อนหรือซอฟต์แวร์ละเมิดลิขสิทธิ์	๑. ถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้น ๆ ๒. ใช้งานซอฟต์แวร์ได้ไม่เต็มประสิทธิภาพ ๓. องค์กรเสื่อมเสียชื่อเสียงและความน่าเชื่อถือ	น้อย (๓x๓=๙)	รณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย	ดำเนินการจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามภาระงานที่จำเป็น	ตามความเหมาะสมและความต้องการของสำนัก/กอง/ศูนย์/สำนักงานโครงการ/กตส./กพร.	
๗	ระบบเครือข่ายหลักเสียหาย/ขัดข้อง ไม่สามารถใช้งานได้	๑. ไม่สามารถใช้งานระบบสารสนเทศและอินเตอร์เน็ตได้ ๒. ไม่สามารถใช้งานระบบสารสนเทศและอินเตอร์เน็ตได้ ๓. ใช้ระยะเวลาในการกู้คืนการทำงานของอุปกร์ระบบมากเกินไป	น้อย (๒x๓=๖)	๑. จัดทำแผนตรวจสอบความพร้อมใช้งาน (availability) ของระบบเครือข่ายหลัก ๒. จัดทำแผนตรวจสอบสถานการณ์ทำงานของอุปกรณ์เครือข่ายต่าง ๆภายในห้องศูนย์ข้อมูล	๑. ตรวจสอบสถานะความพร้อมใช้งานของระบบเครือข่ายหลัก ๒. ตรวจสอบสถานะการทำงานของอุปกรณ์เครือข่ายต่าง ๆ ด้วยโปรแกรมประเภท Network Monitoring	ทุกเดือน	ศทท.

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
				๓. จัดทำแผนการสำรองข้อมูล สถานะการทำงานของอุปกรณ์เครือข่าย	๓. ทำการสำรองค่าการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายแต่ละตัว ไว้ใน External Hard Disk		
๘	การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data Room)	๑. เกิดความเสียหายกับทรัพย์สินของทางราชการ ๒. ไม่สามารถใช้งานระบบสารสนเทศได้	น้อย (๑x๕=๕)	๑. จัดทำแผนตรวจสอบความพร้อมใช้งานของระบบดับเพลิงสำหรับห้องศูนย์ข้อมูล ๒. จัดทำแผนตรวจสอบความพร้อมใช้งานของระบบเตือนภัย (Warning System)	ตรวจสอบความพร้อมใช้งานของระบบดับเพลิงและระบบเตือนภัยอัตโนมัติ (Automatic Warning System)	ทุกเดือน	ศทท.
๙	ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า, แผ่นดินไหว, น้ำท่วม	๑. อุปกรณ์ต่างๆ เสียหายจากแรงสั่นสะเทือนหรือการตกหล่น ๒. อุปกรณ์ต่าง ๆ เสียหายจากความชื้น ๓. ผู้ใช้งานไม่สามารถใช้งานระบบสารสนเทศได้	น้อย (๑x๕=๕)	๑. จัดทำแผนตรวจสอบการติดตั้งอุปกรณ์ต่างๆ ภายในห้องศูนย์ข้อมูล ๒. จัดทำแผนตรวจสอบความพร้อมใช้งานของระบบเตือนภัย (Warning System)	๑. ตรวจสอบการติดตั้ง/จัดวางอุปกรณ์ต่าง ๆ ทั้งภายนอกและภายในตู้ Rack ทั้งหมด ๒. ตรวจสอบพร้อมใช้งานของระบบดับเพลิงและระบบเตือนภัยอัตโนมัติ (Automatic	ทุกเดือน	ศทท.

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
					Warning System)		
๑๐	ระบบคอมพิวเตอร์ถูกเจาะ (Hack)	๑. มีการแก้ไข เปลี่ยนแปลงค่าการทำงานของอุปกรณ์เครือข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายจนทำงานผิดพลาด หรือไม่อาจทำงานได้ ๒. มีการแก้ไข เปลี่ยนแปลง ลบทำลายค่าการทำงานอุปกรณ์เครือข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายจนกระทั่งทำงานผิดพลาดหรือไม่อาจทำงานได้ ๓. ระบบสารสนเทศขององค์กรขาดความน่าเชื่อถือ ๔. มีการแก้ไข เปลี่ยนแปลง ลบทำลาย หรือคัดลอกสำเนาข้อมูลสำคัญออกมาใช้แสวงหาผลประโยชน์ในทางมิชอบ ๕. แก้ไขสิทธิการเข้าใช้งานระบบในฐานะผู้ดูแลระบบ	น้อย (๑x๕=๕)	จัดทำแผนตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall	ตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall	ทุกเดือน	ศทท.

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
		๖. แก้ไขสิทธิผู้ดูแลระบบจนไม่สามารถเข้าใช้งานระบบได้ ๗. สูญเสียเวลาและค่าใช้จ่ายในการเก็บรวบรวมข้อมูลที่ต้องการใหม่ ๘. ข้อมูลสารสนเทศขององค์กรขาดความน่าเชื่อถือ					
๑๑	การใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ผิดวัตถุประสงค์	๑. สูญเสีย Bandwidth ในเครือข่ายโดยเปล่าประโยชน์ ๒. ใช้ในการกระทำผิดกฎหมายจนถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	น้อย (๕x๑=๕)	๑. จัดทำข้อปฏิบัติในการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ ๒. กำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port สำหรับการปฏิบัติงานเท่าที่จำเป็น	๑. รายงานผลการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่ฝ่าฝืนต่อผู้บังคับบัญชา ๒. ตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall	ทันทีที่ทราบ ทุกเดือน	ศทท.
๑๒	อุปกรณ์คอมพิวเตอร์ถูกขโมย	๑. ไม่สามารถใช้งานระบบสารสนเทศได้ ๒. สูญเสียข้อมูลที่มีความสำคัญ ๓. สูญเสียงบประมาณในการจัดซื้อ/จัดหา	น้อย (๑x๕=๕)	จัดทำแผนตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV อุปกรณ์ควบคุมการเข้า-ออก	ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV อุปกรณ์ควบคุมการเข้า-ออก (Access Control)	ทุกเดือน	ศทท.

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
		เครื่องใหม่มาทดแทน		(Access Control)			
๑๓	การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์	๑. ไม่สามารถเรียกหรือกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศกลับมาใช้งานได้ ๒. ข้อมูลสารสนเทศไม่ครบถ้วน	ยอมรับได้ (๑x๔=๔)	๑. จัดทำแผนทดสอบการกู้คืนระบบและข้อมูล ๒. จัดหาระบบคอมพิวเตอร์สำรองฉุกเฉิน (Disaster Recovery Site : DR Site) หากมีความจำเป็น	ดำเนินการทดสอบการกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศจาก Backup File	ทุก ๖ เดือน	ศทท.
๑๔	เครื่องปรับอากาศภายในห้องศูนย์ข้อมูลไม่ทำงาน	๑. อุณหภูมิภายในห้องศูนย์ข้อมูลสูงขึ้น ๒. อุปกรณ์ต่าง ๆ ทำงานผิดปกติ	ยอมรับได้ (๑x๔=๔)	เครื่องปรับอากาศที่มีอยู่สามารถทำงานได้ตลอดเวลา	ตรวจสอบความพร้อมใช้งานของเครื่องปรับอากาศทั้ง ๒ เครื่อง ให้สลับกันทำงานเครื่องละ ๖ ชม.	ทุกเดือน	ศทท.
๑๕	การก่อความไม่สงบ/จราจล	๑. บุคคลภายนอกสามารถเข้าถึงอุปกรณ์ต่าง ๆ ภายในห้องศูนย์ข้อมูลได้ ๒. อุปกรณ์ต่าง ๆ ภายในห้องศูนย์ข้อมูลถูกทำลายจนเสียหาย ๓. อุปกรณ์ต่าง ๆ ภายในห้องศูนย์ข้อมูลถูกขโมย/โจรกรรม ๔. ข้อมูลสารสนเทศที่สำคัญถูกแก้ไข เปลี่ยนแปลง ลบ ทำลายจนเสียหาย หรือ	ยอมรับได้ (๑x๓=๓)	๑. จัดทำแผนตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV อุปกรณ์ควบคุมการเข้าถึง (Access Control) และติดตั้งระบบรักษาความปลอดภัยสำหรับห้องศูนย์ข้อมูล (การ Scan นิ้ว เข้า-ออก	๑. ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV อุปกรณ์ควบคุมการเข้าถึง (Access Control) ๒. ดำเนินการทดสอบการกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศจาก Backup File	ทุก ๖ เดือน	ศทท.

ลำดับที่	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	การจัดการความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
		คัดลอกสำเนาข้อมูลมาใช้แสวงหาผลประโยชน์ในทางมิชอบ ๕. ผู้ใช้งานไม่สามารถใช้งานระบบสารสนเทศได้		ซึ่งอนุญาตเฉพาะเจ้าหน้าที่ที่ได้รับอนุญาต) ๒. จัดทำแผนทดสอบการกู้คืนระบบสารสนเทศ			

บทที่ ๔
สรุปผลและข้อเสนอแนะ

การบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management) คือ กระบวนการในการค้นหา ระบุ วิเคราะห์ ประเมิน และควบคุมความเสี่ยงที่อาจเกิดจากการดำเนินกิจกรรมหรือกระบวนการทำงานด้านเทคโนโลยีสารสนเทศของ สนข. เพื่อลดระดับความเสียหายจากความรุนแรงของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ หรือขจัดความเสี่ยงให้หมดไป

ในปัจจุบัน **"ระบบเทคโนโลยีสารสนเทศ"** ก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อนการดำเนินงานขององค์กร การดำเนินงานทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศแทบทั้งสิ้น โดยในแต่ละวันข้อมูลสารสนเทศจำนวนมหาศาลถูกส่งผ่านระบบเครือข่ายอินเทอร์เน็ตโดยใช้เทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกในการปฏิบัติงานของทุกหน่วยงานภายใน สนข. และ **"ข้อมูลสารสนเทศ"** ก็ถือว่าเป็นทรัพย์สินอันทรงคุณค่าอย่างมหาศาล หากข้อมูลสารสนเทศนี้ตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหาย และหรือถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและบุคคลภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ไขปัญหานี้จึงควรเริ่มตั้งแต่การจัดการระบบเทคโนโลยีสารสนเทศขององค์กรให้ได้มาตรฐานทางด้านความปลอดภัย ซึ่งก็คือ การบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศในองค์กรนั่นเอง

๔.๑ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข.

สนข. ได้พิจารณาทบทวนแผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ของ สนข. ปีงบประมาณ ๒๕๖๓ ที่ผ่านมา พร้อมทั้งพิจารณาค้นหาความเสี่ยงจากกิจกรรมต่าง ๆ ด้านระบบเทคโนโลยีสารสนเทศของ สนข. ที่อาจเกิดเพิ่มเติมขึ้นใหม่ โดยดำเนินการจัดประเภทความเสี่ยงและปัจจัยเสี่ยงเดิมที่ซ้ำซ้อนกันกับประเภทความเสี่ยงและปัจจัยเสี่ยงใหม่ให้อยู่ในกลุ่มเดียวกัน **ซึ่งสามารถค้นหาและระบุรายการความเสี่ยงเพื่อดำเนินการบริหารจัดการความเสี่ยงได้เป็น ๖ ประเภท รวมจำนวน ๑๕ ความเสี่ยง** ส่วนการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงแต่ละรายการโดยเรียงลำดับจากระดับความเสี่ยงรุนแรง สูง ปานกลาง น้อย และยอมรับได้ สรุปได้ ดังนี้

๔.๑.๑ ถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี อยู่ในระดับรุนแรง (๒๕ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

(๑) ตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall ตามระยะเวลาที่กำหนด

(๒) ตรวจสอบสถานะการทำงานของโปรแกรมป้องกันมัลแวร์ต่างๆ ตามระยะเวลาที่กำหนด

(๓) ปรับปรุง/อัพเดทโปรแกรมป้องกันมัลแวร์ต่าง ๆ ให้เป็นปัจจุบัน

๔.๑.๒ ซอฟต์แวร์ระบบฐานข้อมูล/โปรแกรมหรือแอพพลิเคชั่นเสียหาย อยู่ในระดับรุนแรง (๒๐ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

(๑) ทำการสำรองไฟล์ระบบแบบ Full Backup เก็บไว้ใน External Hard Disk

(๒) ทำการสำรองไฟล์ระบบแบบ Incremental หรือ Differential เก็บไว้ใน External Hard Disk

(๓) จัดซื้อ/จัดหาซอฟต์แวร์หรือ License เพิ่มเติม

(๔) จัดทำโครงการระบบสำรองข้อมูลสารสนเทศและกู้คืน (Backup & Recovery System)

๔.๑.๓ ระบบไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า อยู่ในระดับสูง (๑๖ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

- ตรวจสอบความพร้อมใช้งานของเครื่องสำรองไฟฟ้า (UPS) ตามระยะเวลาที่กำหนด

๔.๑.๔ การเข้าถึงห้องศูนย์ข้อมูลโดยไม่ได้รับอนุญาต อยู่ในระดับสูง (๑๕ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

- ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV อุปกรณ์ควบคุมการเข้า-ออก (Access Control) ตามระยะเวลาที่กำหนด

๔.๑.๕ อุปกรณ์คอมพิวเตอร์ชำรุดเสียหาย อยู่ในระดับปานกลาง (๑๐ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

(๑) ทำการสำรองข้อมูลระบบแบบ Full Backup เก็บไว้ใน External Hard Disk

(๒) ทำการสำรองข้อมูลระบบแบบ Incremental หรือ Differential เก็บไว้ใน External Hard Disk

(๓) จัดทำโครงการระบบสำรองข้อมูลสารสนเทศและกู้คืน (Backup & Recovery System)

๔.๑.๖ การใช้งานซอฟต์แวร์เถื่อนหรือซอฟต์แวร์ละเมิดลิขสิทธิ์ อยู่ในระดับน้อย (๙ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

- ดำเนินการจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามภาระงานที่จำเป็น

๔.๑.๗ ระบบเครือข่ายหลักเสียหาย/ขัดข้อง ไม่สามารถใช้งานได้ อยู่ในระดับน้อย (๖ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

(๑) ตรวจสอบสถานะความพร้อมใช้งานของระบบเครือข่ายหลักตามระยะเวลาที่กำหนด

(๒) ตรวจสอบสถานะการทำงานของอุปกรณ์เครือข่ายต่าง ๆ ภายในห้องศูนย์ข้อมูลด้วยโปรแกรมประเภท Network Monitoring ตามระยะเวลาที่กำหนด

(๓) ทำการสำรองค่าการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายแต่ละตัว ทั้งแบบอัตโนมัติ (Auto Backup) และแบบกำหนดเอง (Manual Backup) ไว้ใน External Hard Disk

(๔) จัดซื้อ/จัดหาซอฟต์แวร์กำหนดค่าเครือข่าย (Software Defined Network : SDN) มาใช้งาน

๔.๑.๘ การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data Room) อยู่ในระดับน้อย (๕ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

- ตรวจสอบพร้อมใช้งานของระบบดับเพลิงและระบบเตือนภัย (Warning System) ตามระยะเวลาที่กำหนด

๔.๑.๙ ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า, แผ่นดินไหว, น้ำท่วม อยู่ในระดับน้อย (๕ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

(๑) ตรวจสอบการติดตั้ง/จัดวางอุปกรณ์ต่าง ๆ ทั้งภายนอกและภายในตู้ Rack ทั้งหมด

(๒) ตรวจสอบพร้อมใช้งานของระบบดับเพลิงและระบบเตือนภัย (Warning System) ตามระยะเวลาที่กำหนด

๔.๑.๑๐ ระบบคอมพิวเตอร์ถูกเจาะ (Hack) อยู่ในระดับน้อย (๕ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

- ตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall ตามระยะเวลาที่กำหนด

๔.๑.๑๑ การใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ผิดวัตถุประสงค์ อยู่ในระดับน้อย (๕ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

(๑) รายงานผลการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่ฝ่าฝืนต่อผู้บังคับบัญชา

(๒) ตรวจสอบสถานะการทำงานของอุปกรณ์ Firewall ตามระยะเวลาที่กำหนด

๔.๑.๑๒ อุปกรณ์คอมพิวเตอร์ถูกขโมย อยู่ในระดับน้อย (๕ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

- ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV อุปกรณ์ควบคุมการเข้า-ออก (Access Control) ตามระยะเวลาที่กำหนด

๔.๑.๑๓ การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์ อยู่ในระดับยอมรับได้ (๔ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

- ดำเนินการทดสอบการกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศจาก Backup File

๔.๑.๑๔ เครื่องปรับอากาศภายในห้องศูนย์ข้อมูลไม่ทำงาน อยู่ในระดับยอมรับได้ (๔ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

- ตรวจสอบความพร้อมใช้งานของเครื่องปรับอากาศทั้ง ๒ เครื่อง ให้สลับกันทำงานเครื่องละ ๖ ชม.

๔.๑.๑๕ การก่อความไม่สงบ/จราจล อยู่ในระดับยอมรับได้ (๓ คะแนน) มีแนวทางการจัดการความเสี่ยง มีดังนี้

(๑) ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย เช่น กล้อง CCTV อุปกรณ์ควบคุมการเข้าถึง (Access Control) ตามระยะเวลาที่กำหนด

(๒) ดำเนินการทดสอบการกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศจาก Backup File

๔.๒ สรุป

แผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

๔.๒.๑ เตรียมความพร้อมเพื่อรองรับสถานการณ์ฉุกเฉิน (contingency event) ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและฐานข้อมูลสารสนเทศของ สนข.

๔.๒.๒ เป็นแนวทางหรือขั้นตอนปฏิบัติในการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและฐานข้อมูลสารสนเทศของ สนข.ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งานอย่างต่อเนื่อง

๔.๒.๓ มีแนวทางการบริหารจัดการความเสี่ยงอย่างเป็นระบบแบบแผน มีความต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีในกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติต่าง ๆ

๔.๓ ข้อเสนอแนะ

๔.๓.๑ การกำหนดนโยบายและการควบคุมกระบวนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศถือเป็นสิ่งสำคัญเพื่อให้มั่นใจได้ว่าองค์กรสามารถเลือกใช้มาตรการควบคุมเพื่อตอบสนองกับความเสี่ยงได้อย่างถูกต้องและมีประสิทธิภาพ ซึ่งสามารถลดระดับความเสียหายจากความรุนแรงของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้หรือขจัดความเสี่ยงให้หมดไปได้ ดังนั้น องค์กรควรมีการกำหนดผู้รับผิดชอบรับผิดชอบในการดำเนินการตามมาตรการเพื่อตอบสนองกับความเสี่ยงนั้น โดยผู้รับผิดชอบที่ได้รับมอบหมายควรมีความรับผิดชอบ ดังนี้

(๑) พิจารณาประสิทธิภาพของมาตรการควบคุมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข. ที่ได้ดำเนินการอยู่ในปัจจุบัน

(๒) พิจารณาแนวทางหรือขั้นตอนการปฏิบัติที่จำเป็นเพิ่มเติม เพื่อเพิ่มประสิทธิภาพของการบริหารจัดการความเสี่ยงนั้น

(๓) ดำเนินการกิจกรรมเพื่อบริหารจัดการความเสี่ยงให้แล้วเสร็จตามระยะเวลาที่กำหนดไว้ในแผน

(๔) พิจารณาเปรียบเทียบระดับความเสี่ยงทั้งก่อนดำเนินการและหลังจากดำเนินการตามแผนเรียบร้อยแล้ว

(๕) ติดตามและการทบทวนแผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข. อย่างต่อเนื่อง

๔.๓.๒ การติดตามและการทบทวนการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สนข. เพื่อให้มั่นใจว่าแผนการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพและมีความเหมาะสมทันกับสถานการณ์ปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็ว ดังนั้น จึงควรมีการดำเนินการติดตามและทบทวนผลการบริหารจัดการความเสี่ยงอย่างต่อเนื่องและสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงทีและถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามผลการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ