สำนักงานสาธารณสุข
จังหวัดสระแก้ว

ปีงบประมาณ
2566

RISK MANAGEMENT

แผนบริหารความเสี่ยง

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

โดยงานข้อมูลข่าวสารและเทคโนโลยีสารสนเทศ
กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข
สำนักงานสาธารณสุขจังหวัดสระแก้ว

คำนำ

แผนบริหารความเสี่ยงด้านระบบข้อมูลข่าวสารและเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขจังหวัดสระแก้ว ปีงบประมาณ 2566 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการระบุความเสี่ยง วิเคราะห์ ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วน ราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้ง ทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสม ในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้ อย่างมีประสิทธิภาพมากขึ้น งานข้อมูลข่าวสารและเทคโนโลยีสารสนเทศ หวังเป็นอย่างยิ่งว่าแผนบริหารความ เสี่ยงด้านระบบเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขจังหวัดสระแก้ว ฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความ เสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของ สำนักงานสาธารณสุขจังหวัดสระแก้ว ต่อไป

งานข้อมูลข่าวสารและเทคโนโลยีสารสนเทศ
กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข
สำนักงานสาธารณสุขจังหวัดสระแก้ว
กรกฎาคม 2565

สารบัญ

สารบัญรูป

สารบัญตาราง

บทที่ 1
บทนำ

1. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ เป็นไปอย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่จะทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศ ที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานร่วมกับระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการ ความเสี่ยงโดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

2. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

1. เพื่อเตรียมความพร้อมในการรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขจังหวัดสระแก้ว
2. เพื่อเป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
3. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ในกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศ (Database & Software) เช่น เว็บไซต์สำนักงานสาธารณสุขจังหวัดสระแก้ว ฐานข้อมูลเว็บไซต์สำนักงานสาธารณสุขจังหวัดสระแก้ว ฐานข้อมูลสุขภาพจังหวัดสระแก้ว และฐานข้อมูลการสแกนลายนิ้วมือเพื่อยืนยันตัวตนต่างด้าว เป็นต้น

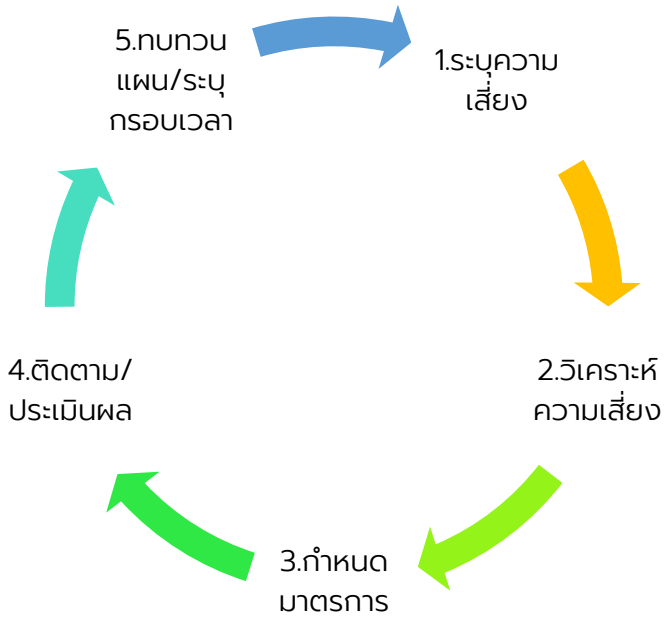
ระบบฐานข้อมูลสำหรับการบริหารงานภายใน (Back Office) ได้แก่ ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์ ฐานข้อมูลระบบสารสนเทศทรัพยากรบุคคล เป็นต้น

ระบบให้บริการเครือข่าย ได้แก่ ระบบเครือข่ายภายใน (LAN) ระบบเครือข่ายอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (WiFi) ระบบเครือข่ายกระทรวงสาธารณสุข (GIN)

อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบสารสนเทศ (Web Application Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (NoteBook) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น ระบบรักษาความปลอดภัย ได้แก่ โปรแกรมตรวจสอบและป้องกันการบุกรุกทางไซเบอร์ Firewall IPS (Intrusion Prevention System)

4. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร การบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอน ดังนี้



รูปที่ 1 แสดงกระบวนการบริหารความเสี่ยง

1. การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้อง กับระบบสารสนเทศของหน่วยงาน เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการดำเนินงานของหน่วยงานที่ต้องใช้ระบบสารสนเทศเป็นเครื่องมือในการดำเนินงาน ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

1.1 การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

1.2 การใช้ Checklist

1.3 การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

1.4 การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

1.5 การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความสูญเสียที่เกิดขึ้น ในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

2. การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และการจัด ระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

2.1 การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้ง เกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของ ความเสี่ยงอาจกำหนดเป็นเกณฑ์ 4 ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

2.2 การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยง แต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับ มาตรการควบคุมความเสี่ยงของหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

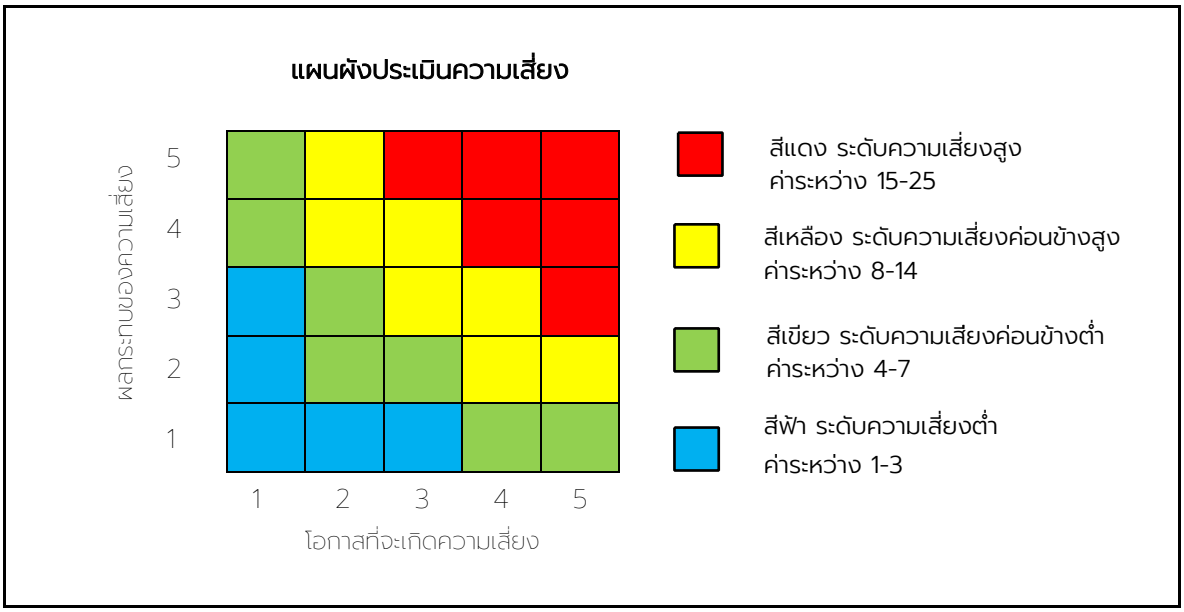
เกณฑ์การประเมินผลกระทบ เป็นดังนี้

ระดับ	การประเมิน
1	น้อยมาก
2	น้อย
3	ปานกลาง
4	สูง
5	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยงเป็นดังนี้

ระดับ	โอกาสที่จะเกิด	เชิงปริมาณ	เชิงคุณภาพ
1	น้อยมาก	ไม่เกิน 1 ครั้ง ต่อปี	มีโอกาสเกิดเกือบทุกครั้ง
2	น้อย	2 ครั้งต่อปี	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยครั้ง
3	ปานกลาง	3 ครั้งต่อปี	มีโอกาสเกิดบางครั้ง
4	สูง	4 ครั้งต่อปี	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
5	สูงมาก	มากกว่า 4 ครั้งต่อปี	มีโอกาสเกิดในกรณียกเว้น

2.3 การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และ ผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปที่ 2



รูปที่ 2 แสดงแผนผังประเมินความเสี่ยง

2.4 การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณา จากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับ “สูงมาก” หรือ “สูง” มาจัดทำแผนการบริหารความเสี่ยง เป็นลำดับแรก

3. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุม ผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยมีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยง ไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ประเภท คือ

3.1 ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้ เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

3.2 การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุม เพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

3.3 การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้น ให้เกิดความสำเร็จตามวัตถุประสงค์

3.4 การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมิน ความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ ขั้นตอนดังนี้

1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น
2) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่
3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

4. การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็น การยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้ว ให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสม โดยพิจารณาจาก

4.1. พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ใน ระดับที่ยอมรับได้
4.2. เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่
4.3. กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง
4.4. ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุ วัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วย การรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อ ผู้บริหารเพื่อทราบและสั่งการ

5. การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของ วิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็น รายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

5. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

คณะทำงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสระแก้ว ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้ เป็น 8 ประเภท ดังนี้

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษา ความ

ปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีคณะทำงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศประสิทธิภาพเพียงพอ

ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจ ในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากร ภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware and Data Communication Risk)

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

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานสาธารณสุขจังหวัดสระแก้ว อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสาร อันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็น ปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัย ของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยงเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

6. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการ ความเสี่ยงที่สามารถนำไปปฏิบัติได้ และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการ จะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับ เพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือ หลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา หรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ใน วิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หาก เราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดย มีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้น การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือ การหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

7. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบสารสนเทศของสำนักงานสาธารณสุขจังหวัดสระแก้ว ได้แก่

1. ปัจจัยภายนอก
    - 1.1 ภัยธรรมชาติ ได้แก่ ไฟไหม้ น้ำท่วม สภาพอากาศร้อนจัด
    - 1.2 การโจรกรรมอุปกรณ์สารสนเทศ
    - 1.3 ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ
    - 1.4 ระบบเครือข่าย Internet ขัดข้อง
    - 1.5 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2. ปัจจัยภายใน
    - 2.1. นโยบายด้านเทคโนโลยีสารสนเทศของหน่วยงาน
    - 2.2. งบประมาณด้านเทคโนโลยีสารสนเทศของหน่วยงาน
    - 2.3. ประสิทธิภาพของแผนงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (ความครอบคลุมปัจจัยเสี่ยง การควบคุมกำกับติดตาม การประเมินผล)
    - 2.4. การเสื่อมสภาพของอุปกรณ์สารสนเทศ
    - 2.5. การป้องกัน ตรวจสอบ และบำรุงรักษาอุปกรณ์สารสนเทศอย่างเหมาะสม
    - 2.6. การถูกไวรัสคอมพิวเตอร์ (Virus) ทำให้เกิดความเสียหายในระบบ
    - 2.7. เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

8. การประเมินความเสียหาย

8.1. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงและไม่สามารถใช้งานระบบสารสนเทศได้เป็นระยะเวลาตั้งแต่ 1 วันขึ้นไป ได้แก่ ภัยธรรมชาติ,

ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลาย เสียหายจากไวรัส หรือ Hacker

8.2. ความเสียหายที่เกิดผลเสียหายปานกลาง กระทบกับบุคลากรส่วนใหญ่หรือทั้งหมดของหน่วยงานชั่วขณะ ได้แก่ ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง, กระแสไฟฟ้าขัดข้อง, Internet ขัดข้อง, อุปกรณ์กระจายสัญญาณเครือข่าย (Switching hub) ขัดข้อง

8.3. ความเสียหายที่เกิดผลกระทบน้อย ได้แก่ ความเสียหายที่เกิดจากอุปกรณ์สารสนเทศ ที่ไม่กระทบการการใช้งานระบบสารสนเทศของบุคลากรส่วนใหญ่ในหน่วยงาน เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล, เครื่องสำรองไฟส่วนบุคคล, แป้นพิมพ์ เป็นต้น

9. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

10. ระบบรักษาความปลอดภัยบนเครือข่าย

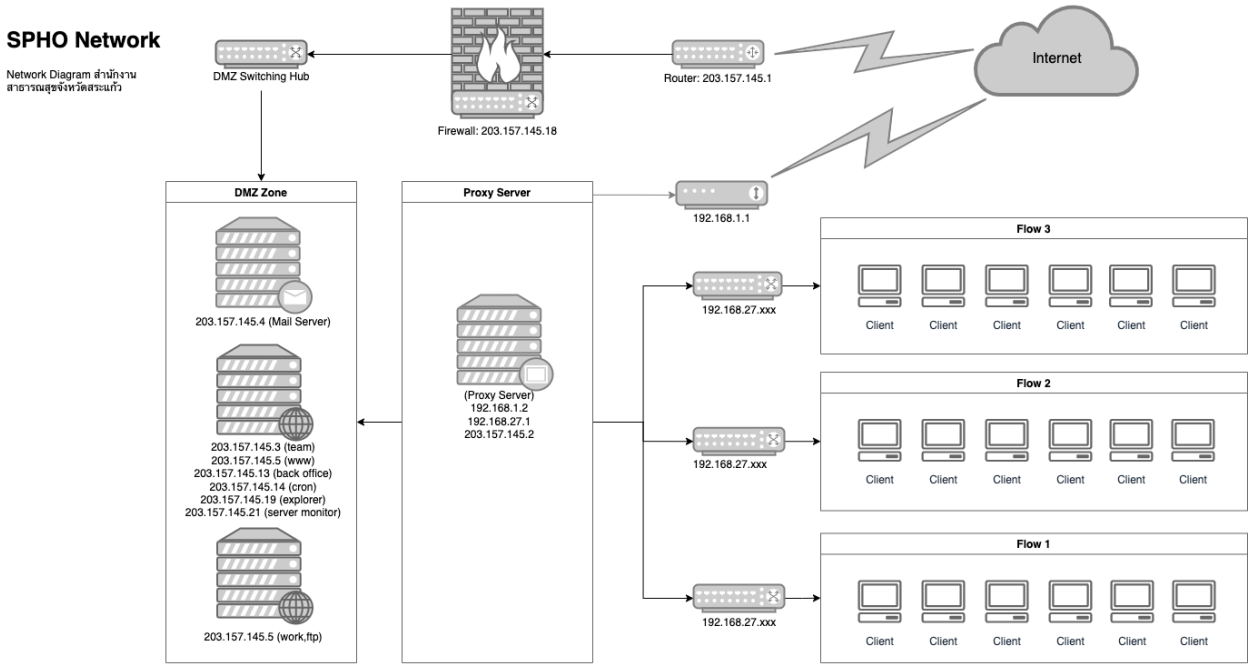
ระบบคอมพิวเตอร์และเครือข่ายของสำนักงานสาธารณสุขจังหวัดสระแก้วได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่าย สำนักงานสาธารณสุขจังหวัดสระแก้วเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ตั้งอยู่ที่อาคารสำนักงานสาธารณสุขจังหวัดสระแก้ว เลขที่ 609 หมู่ 2 ตำบลท่าเกษม อำเภอเมืองสระแก้ว จังหวัดสระแก้ว

มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์ และซอฟต์แวร์ ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนด มาตรการ (Policy) ผ่านอุปกรณ์ Firewall ของ FortiGate 110C ซึ่งใช้ในการกรอง (Filter Package) ที่ผ่าน เข้ามาภายในระบบของกระทรวงสาธารณสุขจากเครือข่ายภายนอก เช่น เครือข่ายของสำนักงานสาธารณสุขจังหวัดสระแก้ว เครือข่ายอินเทอร์เน็ต เครือข่าย GIN[1] นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของ DMZ[2] ที่ดูแลเครื่อง แม่ข่ายทั้งหมดของสำนักงานสาธารณสุขจังหวัดสระแก้ว รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่อง

คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของสำนักงานสาธารณสุขจังหวัดสระแก้ว มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของสำนักงานสาธารณสุขจังหวัดสระแก้วในส่วนกลาง กำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่ม ความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

ระบบเครือข่ายหลักของสำนักงานสาธารณสุขจังหวัดสระแก้ว (Core Network) ตั้งอยู่ที่ ห้องคอมพิวเตอร์แม่ข่ายกลาง (Data Center) งานข้อมูลข่าวสารและเทคโนโลยีสารสนเทศ กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข เป็นศูนย์กลางการเชื่อมต่อทำหน้าที่เชื่อมโยงระบบเครือข่ายภายใน ในความเร็วระดับ 1 Gbps และระบบ เครือข่ายภายนอก เช่น อินเทอร์เน็ต และ GIN เข้าด้วยกันซึ่งมี Core Switch ที่ออกแบบติดตั้งในลักษณะ ระบบเครือข่ายที่สามารถทดแทนกันได้ (Redundant Network) เพื่อแก้ปัญหาระบบเครือข่ายศูนย์กลางล่ม (Single Point of Failure) และแก้ปัญหาคอขวดในการเข้าถึงข้อมูล (Bottle neck) เพื่อรองรับภารกิจของ สำนักงานสาธารณสุขจังหวัดสระแก้ว ซึ่งลักษณะงานต้องใช้อุปกรณ์เครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพสูงสามารถรองรับการเชื่อมต่อกับระบบเครือข่ายภายในและภายนอกแบบ 24 ชั่วโมง x7 วัน เพื่อใช้ระบบงานฐานข้อมูลที่สำคัญของสำนักงานสาธารณสุขจังหวัดสระแก้ว พร้อมทั้งเชื่อมโยงไปยังอุปกรณ์ Distributed Switch (L3) และ Access Switch (L2) ไปยังอาคารต่างๆ ซึ่งเป็นที่ตั้งของหน่วยงานในสำนักงานสาธารณสุขจังหวัดสระแก้ว

1 Government Information Network (Gin)
2 โซนเครื่องคอมพิวเตอร์แม่ข่าย (Demilitarized Zone)
3 มีการแบ่งหมายเลข IP Address เป็นกลุ่มย่อย (Subnet Mask)
4 หมายเลขภายใน (Private IP Address)



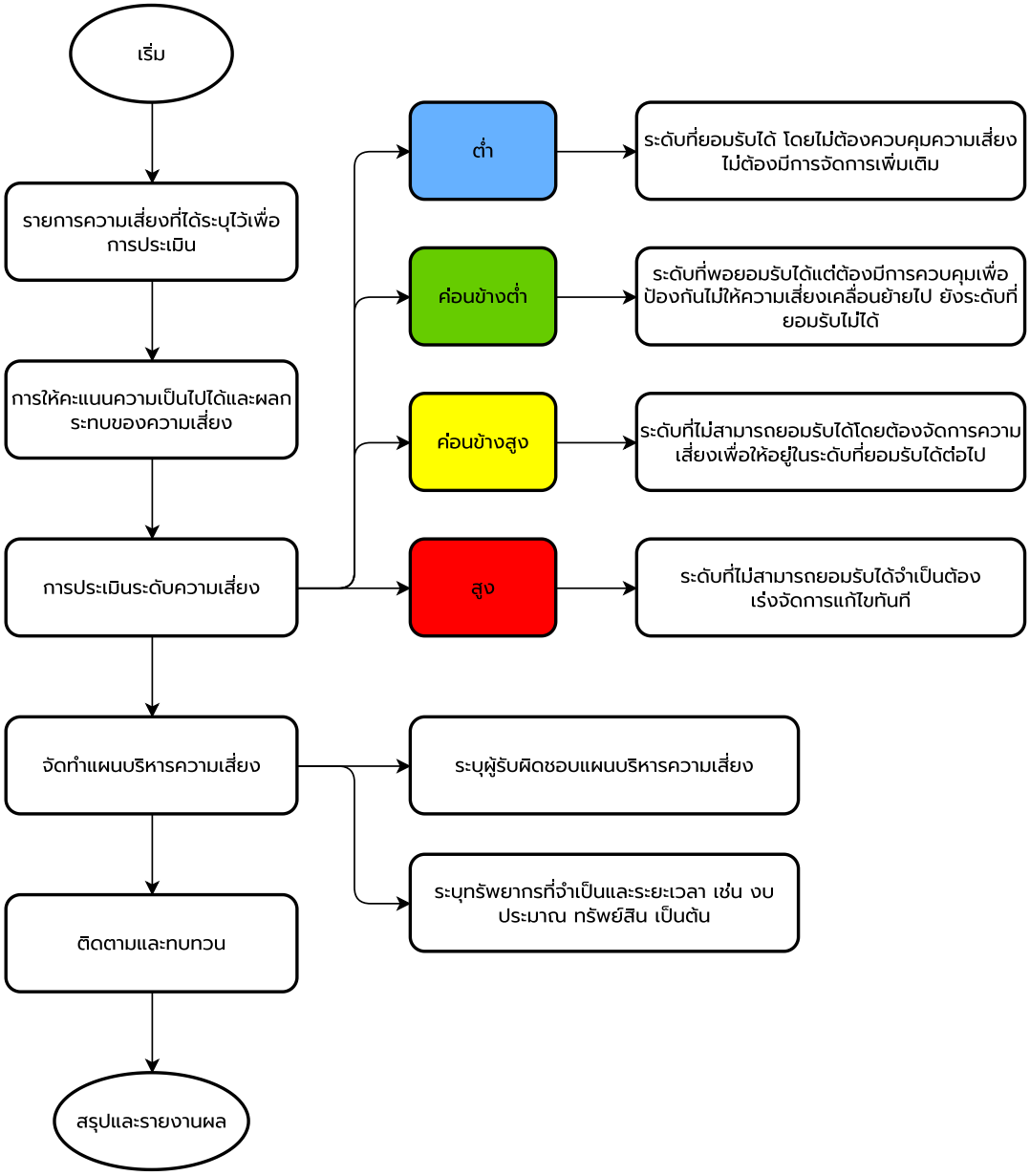
รูปที่ 3 แสดงโครงข่ายคอมพิวเตอร์สารสนเทศของสำนักงานสาธารณสุขจังหวัดสระแก้ว

บทที่ 2

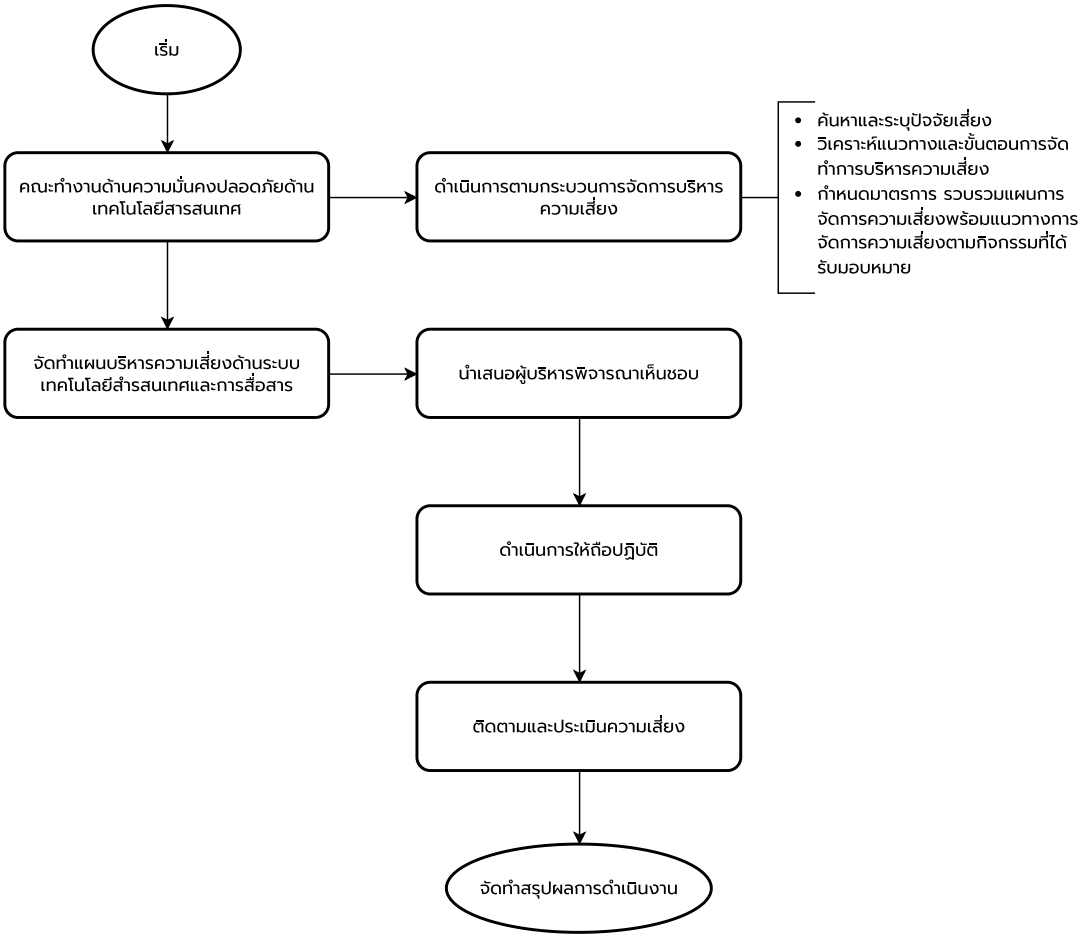
การวิเคราะห์การบริหารจัดการความเสี่ยง

สำนักงานสาธารณสุขจังหวัดสระแก้ว ได้ตระหนักถึงความสำคัญของข้อมูลและการทำงานของระบบเครือข่ายที่สนับสนุนการปฏิบัติงานของหน่วยงานที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงมอบหมายให้งานข้อมูลข่าวสารและเทคโนโลยีสารสนเทศ กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข ทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสาร พ.ศ. 2566 ให้สอดคล้องกับแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงสาธารณสุขและกฎหมายที่เกี่ยวข้อง กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตาราง การบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

1. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง

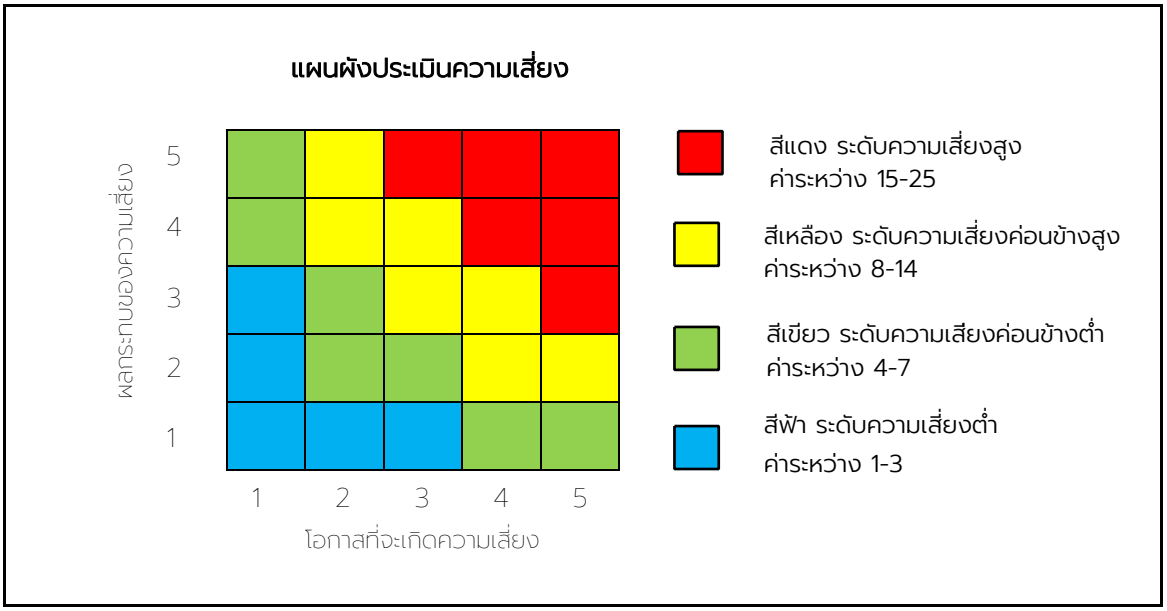


2. กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



3. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุป การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้



ตารางที่ 1 ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
1	ความชื้น อุณภูมิห้องคอมพิวเตอร์แม่ข่ายกลาง	4	4	16
2	ระบบกระแสไฟฟ้าขัดข้อง	4	4	16
3	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย	3	5	15
4	การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิด	4	4	16
5	การนำอุปกรณ์เคลื่อนที่ (Smart Phone ,Tablet , PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่าย	5	3	15
6	ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	4	4	16
7	การบุกรุกจากผู้ไม่ประสงค์ดี / ไวรัสคอมพิวเตอร์	3	4	12
8	การสูญหายของข้อมูล	2	5	10
9	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามฎหมาย	2	5	10
10	การเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	1	5	5
11	สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	1	5	5

12	แมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า / สายสัญญาน	1	4	4
13	การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	1	5	5
14	การถูกโจมตีระบบจากเครือข่ายภายใน	2	3	6
15	ข้อมูลรั่สไหลจากการเปลี่ยนมือผู้ใช้	2	3	6
16	การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	1	4	4

4. ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
			ระดับความเสี่ยงสูง				
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	1. ความเสี่ยงจากความชื้น อุณหภูมิ ห้องคอมพิวเตอร์แม่ข่ายไม่มี ระบบปรับอากาศที่ได มาตรฐาน สามารถควบคุมอุณหภูมความชื้นได้	ระบบปรับอากาศที่ไมไ ด้มาตรฐานสำหรับห้องคอมพิวเตอร์แม่ข่าย	การทำงานของเครื่องอายุและอุปกรณ์สั้นลง	สูง 4x4=16	1. ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ 2. วางแผนจัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	การยอมรับ (Take)	ศูนย์คอมฯ
	1. ความเสี่ยงไม่สามารถใช้งานเครื่อง แม่ข่าย และระบบเครือข่ายได้กรณี เกิดไฟฟ้าขัดข้อง 2. ความเสี่ยงต่อการCrash ของ เครื่องแม่ข่าย ทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ Shutdown อย่างเหมาะสม	1. ระบบกระแสไฟฟ้า ขัดข้อง 2. UPS มีอายุการใช้งานมาก ไม่มีระบบการสำรองไฟ/ไม่มระบบการแจ้ง เตือนที่รวดเร็ว	1. ระบบไม่สามารถ ทำงานได้ 2. ข้อมูล/อุปกรณ์เสียหาย 3. ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายเสียหาย ต้องมีการติดตั้งใหม่	สูง 4x4=16	1. ตรวจสอบการทำงานระบบสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ 2. วางแผนการจัดหาและติดตั้ง UPS และ เครื่องกำเนิดไฟฟ้า (Electrical Generator)	การควบคุม (Treat)	
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	1. ความเสี่ยงจากระบบคอมพิวเตอร์ แม่ข่ายหลักและอุปกรณ์เสียหาย ทำ ให้ไม่สามารถใช้ระบบงานได้เต็ม ประสิทธภาพ 2. ความเสี่ยงต่อความเสยหายของ ข้อมูลและการกู้คืนข้อมูล	- การทำงานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ขัดข้อง	1. ระบบงานไม่สามารถใช้ได้ตามปกติ 2. ข้อมูลเสียหาย	สูง 3x5=15	1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล 2. จัดหา Dr-Site 3. จัดจ้างผู้ดูแลระบบ (Out Source)	การถ่ายโอน (Transfer)	

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านบุคลากร (Human Risk)	1. ความเสี่ยงจากการถูกนำสิทธิ์การ เข้าถึงระบบเทคโนโลยีสารสนเทศของ หน่วยงานที่ไม่ได้รับอนุญาตไปใช้ ในทางที่ผิดกฎหมาย	- สิทธิ์ฐานข้อมูลผู้ใช้งานระบบเทคโนโลยี สารสนเทศไม่เป็นปัจจุบัน เนื่องจากผู้ใช้งานมีการ ลาออก โอน ย้าย สิ้นสุด การจ้างตลอดเวลา	1. หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน/ข้อมูล/อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย 2.ข้อมูลที่เป็นความลับ ถูกเผยแพร่หรือนำไปใช้ จะนำมาซึ่งการขาด ความเชื่อถือของ หน่วยงานฯ	สูง 4x4=16	หน่วยงานในสังกัด สสจ.สก ต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานภายในสำนักงานลาออก โอน ย้าย หรือสนสุดการจ้างให้หน่วยงานทำหนังสือแจ้งให้กับ ศูนย์คอมฯ/หน่วยงานผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผมีสทธิ์เข้า ใช้งานระบบเทคโนโลยีสารสนเทศให้เป็น ปัจจุบัน	การควบคุม (Treat)	หน่วยงานในสังกัด สสจ.สก/ หน่วยงาน หน่วยงานผู้ดูแล/ เจ้าของระบบ/ศูนย์คอมฯ
	2. ความเสี่ยงจากการนำอุปกรณ์ เคลื่อนที่ (Smart phone ,Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความ ระมัดระวังในการใช้งาน	อุปกรณ์ที่ใช้ไม่มีระบบ รักษาความปลอดภัยที่ ถูกต้องและเพียงพอ	1. อาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงานและอาจมีการโจมตีทำ ให้ระบบไม่สามารถ ทำงานได้	สูง 5x3=15	1. อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน 2. กำกับดูแลการปฏิบัตตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุม (Treat)	ศูนย์คอมฯ/ หน่วยงานในสังกัด สสจ.สก/ ผู้ใช้งาน
	3. ความเสี่ยงจากการที่ผู้ใช้งานขาด ความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	1. เจ้าหน้าที่หรือบุคลากรของ หน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อย่างปลอดภัย 2. การใช้ทรัพยากรของหน่วยงานทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์ หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	1. ระบบเสยหาย หยุดชะงักการทำงาน 2. สูญเสีย Bandwidth ในเครือข่ายทำให้ ต้อง จัดเพิ่ม Bandwidth ให้ มากขึ้นทุกๆ ปี 3. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	สูง 4x4=16	1. อบรม สร้างความรู้ความเข้าใจการใช้งานที่ถูกวิธี 2. กำหนด Policy ของอุปกรณ์รักษาความปลอดภัยของหน่วยงานให้มีความปลอดภัยและตรวจสอบการทำงานระบบอย่างสม่ำเสมอ และการเปิด Port เท่าที่จำเป็น 3. กำกับดูแลการปฏิบัตตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุม (Treat)	ศูนย์คอมฯ
ระดับความเสี่ยงค่อนข้างสูง							

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	1. ความเสี่ยงจากการบุกรุกจากผู้ไม่ ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker ไวรัส Malware ต่างๆเป็นต้น	การถูกโจมตี จากภายนอกผ่าน เครือข่ายอินเทอร์เน็ต	1. อาจทำให้ระบบ เครื่องแม่ข่าย หรือลูก ข่ายติดไวรัสและ แพร่กระจายสู่เครื่อง อื่นๆ ทั้งหมดใเครือข่าย 2. ระบบ/ข้อมูลอาจถูกแก้ไขหรือเปลี่ยนแปลง เช่น รูปภาพ บน Web Site ของสำนักงานฯ 3. อาจถูกโจรกรรม ข้อมูลที่เป็นความลับ	ค่อนข้างสูง 3x4=12	1. ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ 2. ติดตั้งระบบป้องกัน และเตือนภัย Spam,Virus, Malware, Trojan 3. ตรวจสอบการตั้งค่า Policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ 4. ติดตั้ง patch ของระบบปฏิบัติการสม่ำเสมอ 5. จัดเจ้าหน้าที่รับผิดชอบตรวจสอบ/เฝ้าระวัง	การควบคุม (Treat)	ศูนย์คอมฯ
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	1. ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่ สามารถดำเนินงานกู้คืนได้หากระบบ เกิดเหตุขัดข้อง	ระบบสารสนเทศที่ไม่มีการสำรองข้อมูล / ดำเนินการสำรองไม่ต่อเนื่อง	1. ระบบเกิดขัดข้อง/ข้อมูลเสียหายไม่มีข้อมูลให้ดำเนินการกู้คืน 2. ระบบเสียหายไม่สามารถใช้งานและบริการข้อมูลได้	ค่อนข้างสูง 2x5=10	1. หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบ อย่างสม่ำเสมอ 2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	การควบคุม (Treat)	ศูนย์คอมฯ/หน่วยงานเจ้าของระบบ
ความเสี่ยงด้านโปรแกรม คอมพิวเตอร์ (Software Risk)	1. การตดตั้งและใช้งานซอฟต์แวร์ที่ ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	1. หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	ค่อนข้างสูง 2x5=10	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมาย มาใช้งานตามความจำเป็น 2. สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	ยอมรับ (Accept)	ศูนย์คอมฯ/หน่วยงานในสังกัด สสจ.สก
ระดับความเสี่ยงต่ำ							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	1. ความเสี่ยงจากการเกิดไฟไหม้ น้ำ ท่วม แผ่นดินไหว อาคารถล่ม จนไม่สามารถเคลื่อนย้ายเครื่อง คอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลให้ระบบหลักไม่สามารถงานได้	- ไฟไหม้ ไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	1. เสียงบประมาณใน การจัดหาระบบทดแทน 2. ไม่สามารถใช้งาน ระบบระหว่างที่มีการ จัดหาระบบทดแทนได้	ต่ำ 1x5=5	1. จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP Plan) 2. วางแผนจัดหาและติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง 3. จัดหา Dr-Site	การควบคุม (Treat)	ศูนย์คอมฯ

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
	คอมพิวเตอร์และ เครือข่ายและข้อมูลสญหาย				4. สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด		
	2. ความเสี่ยงจากสถานการณ์ความ สงบเรียบร้อยในบ้านเมือง	- การชุมนุมประท้วง - การจลาจล/ก่อการร้าย - การสูญหายและถูกทำลายของอุปกรณ์ และข้อมูลที่เป็นส่วน สำคัญขององค์กร	การเกิดสถานการณ์ความรุนแรงหรือความ ไม่สงบเรียบร้อย จนทำ ให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	ต่ำ 1x5=5	1. จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP Plan) 2. จัดทำศูนย์สำรอง (Backup Site)	การควบคุม (Treat)	ศูนย์คอมฯ
	3. ความเสี่ยงจากแมลง หรือสัตว์กดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า/ สายสญญาณ	เสี่ยงต่อการอุปกรณ์/ ระบบไม่สามารถใช้งานได้ ปกติ	1. เสียงบประมาณใน การซ่อมแซมหรือจัดหาทดแทน 2. ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	ต่ำ 1x4=4	1. ไม่ปล่อยให้มีสายไฟฟ้าหรือ สายสญญาณไม่มีท่อห่อหุ้มจนถึงจุด ทางเข้าตู้ Rack 2. ไม่นำอาหารหรือเครื่องดื่มมาทาน หรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การควบคุม (Treat)	ศูนย์คอมฯ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	1. ความเสี่ยงจากการเชื่อมต่อระบบ เครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	1. ไม่สามารถใช้งานระบบงานของ สำนักงานฯ ผ่าน เครือข่ายอินทราเน็ตได้ 2. ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่าย อินเทอร์เน็ตได้	1.เจ้าหน้าที่และผู้บริหารงานสำนักงานฯ ไม่สามารถใช้งานระบบอินเทอร์เน็ตสำห รับปฏิบัติงานได้ 2.บุคคลภายนอกไม่สามารถเข้าใช้งานข้อมูลสารสนเทศของ หน่วยงานผ่านเครือข่าย	ต่ำ 1x5=5	1. ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการเครือข่ายอินเทอร์เน็ต 2. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ	การควบคุม (Treat)	ศูนย์คอมฯ
	2. ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่ เครื่องลูกข่ายโดย ผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้หรือใช้ได้แต่ช้ามาก	ต่ำ 2x3=6	1. กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ 2. การควบคุมด้วยระบบ Desktop Management	การควบคุม (Treat)	ศูนย์คอมฯ

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	1. ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลยนมือ ผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรืออุปกรณ์สารองข้อมูลประเภทต่างๆ	1. ข้อมูลที่อยู่ในชั้นความลับ รั่วไหลทำให้เสียหายต่อความเชื่อถือของ สสจ.สก 2. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	ต่ำ 2x3=6	1. มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk อุปกรณส์ ำรอง ข้อมูลประเภทต่างๆ ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่าง ถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้ก่อนจำหน่าย	การยอมรับ (Take)	ศูนย์คอมฯ/หน่วยงานในสังกัด สสจ.สก
	2. ความเสี่ยงจากการ โจรกรรมอุปกรณ์ คอมพิวเตอร์แม่ข่าย หรือ เครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสญหาย ของอุปกรณ์ และ ข้อมูลที่มีความสำคัญ	1. เสียงบประมาณใน การจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง 2. เสียเวลาในการกู้ ระบบ 3. เสียภาพลักษณ์ของสำนักงานฯ	ต่ำ 1x4=4	1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย 2. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน 3. ควบคุมการเข้าออกและขนย้ายเครื่องคอมพิวเตอร์เข้า-ออก อาคารตลอดเวลา 3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุก ที่ๆ มี เครื่องคอมพิวเตอร์และอุปกรณ์ ติดตั้งอยู่	การควบคุม (Treat)	ศูนย์คอมฯ/หน่วยงานในสังกัด สสจ.สก