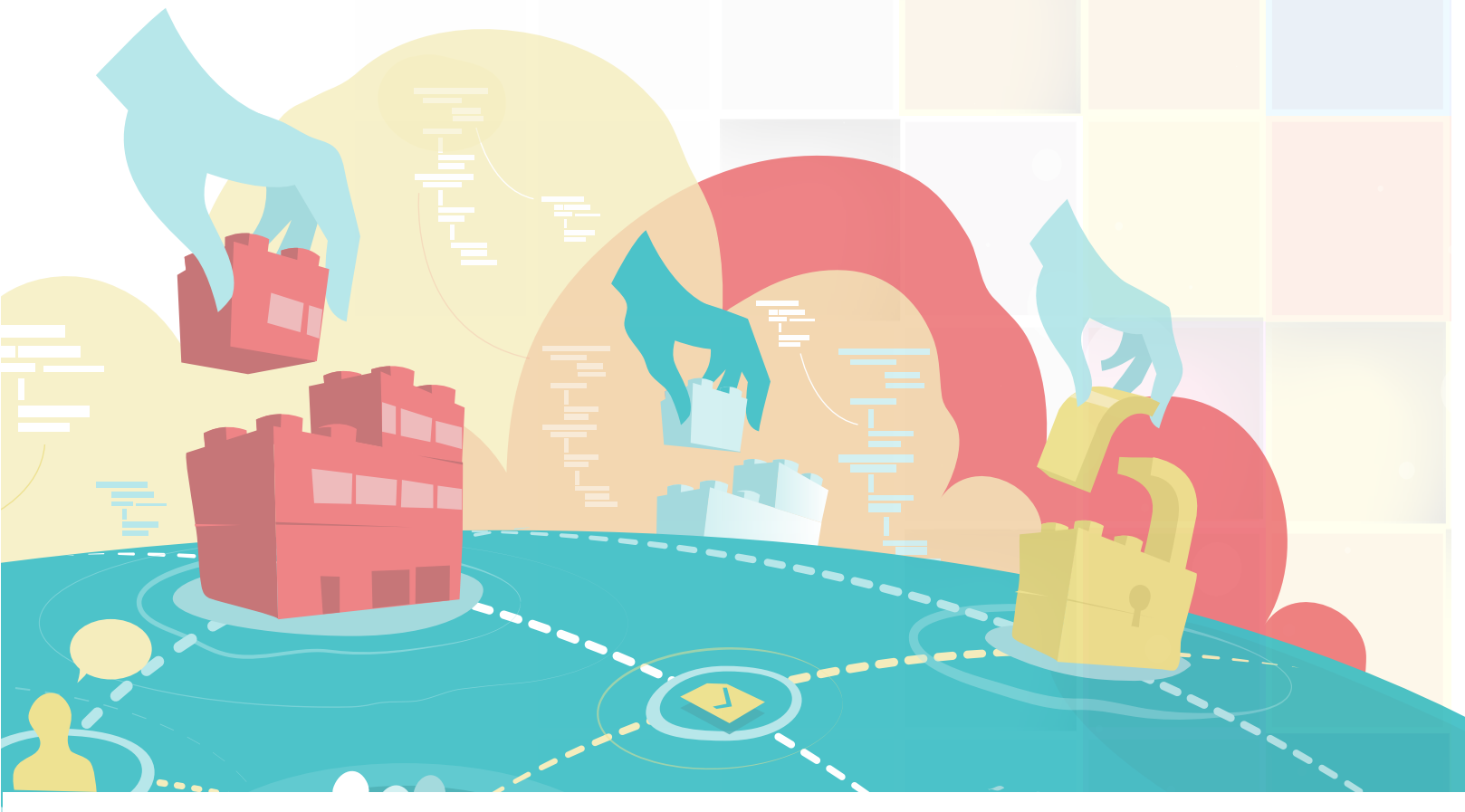
แผนบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ของ สำนักงานปลัดกระทรวงเกษตรและสหกรณ์



ประจำปีงบประมาณ ๒๕๕๙ - ๒๕๖๓

คำนำ

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (สป.กษ.) ปี ๒๕๕๙-๒๕๖๓ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สป.กษ. ฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของ สป.กษ. ต่อไป

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงเกษตรและสหณณ์
สิงหาคม ๒๕๕๙

บทที่ ๑
บทนำ

๑. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๑. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของ สป.กษ.

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น เว็บไซต์กระทรวงเกษตรและสหกรณ์และเว็บไซต์กระทรวงเกษตรและสหกรณ์ ฐานข้อมูลเว็บไซต์กระทรวงเกษตรและสหกรณ์และฐานข้อมูลเว็บไซต์สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เป็นต้น

ระบบฐานข้อมูลบริหารงานภายใน (Back Office) ได้แก่ ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban) ฐานข้อมูลระบบสารสนเทศทรัพยากรบุคคล (DPIS) ฐานข้อมูลครุภัณฑ์คอมพิวเตอร์ (ICT Asset) เป็นต้น

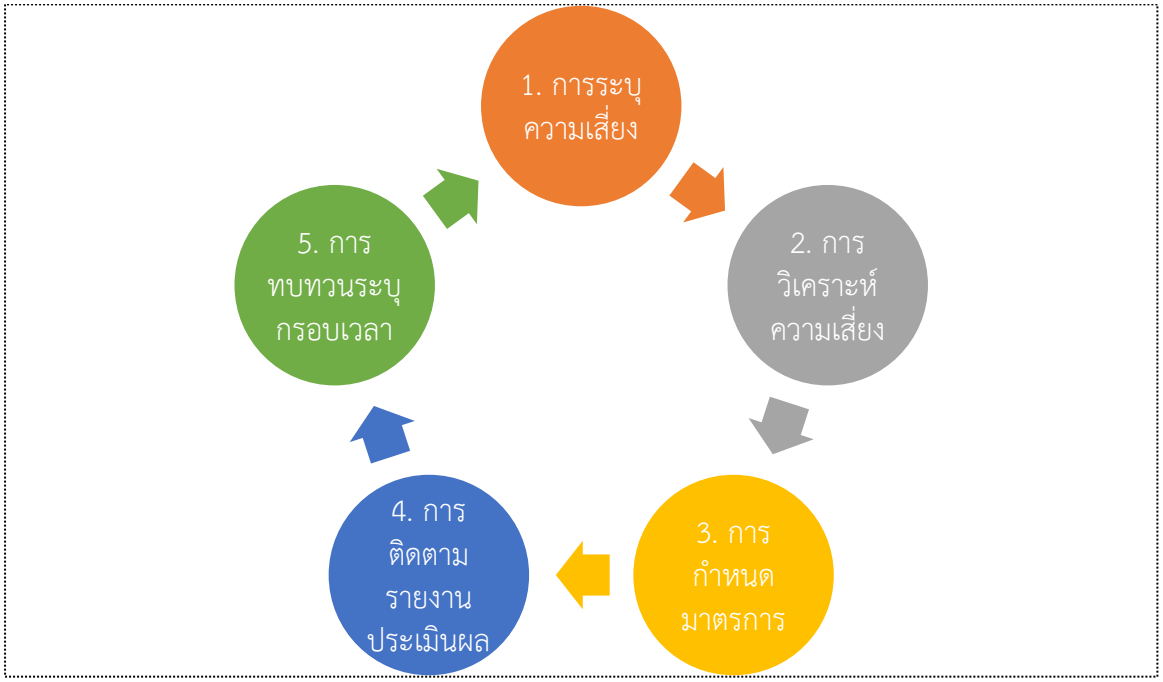
ระบบให้บริการเครือข่าย ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์สำนักงานปลัดกระทรวงเกษตรและสหกรณ์(Web Application Program) เป็นต้น

อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเน็ตเวิร์ค (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์สำนักงานปลัดกระทรวงเกษตรและสหกรณ์(Web Server) เครื่องคอมพิวเตอร์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall)

เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer)เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

๔. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้



รูปที่ ๑ แสดงกระบวนการบริหารความเสี่ยง

๑. การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

๑. การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
๒. การใช้ Checklist
๓. การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
๔. การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
๕. การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๒. การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๒.๑ การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

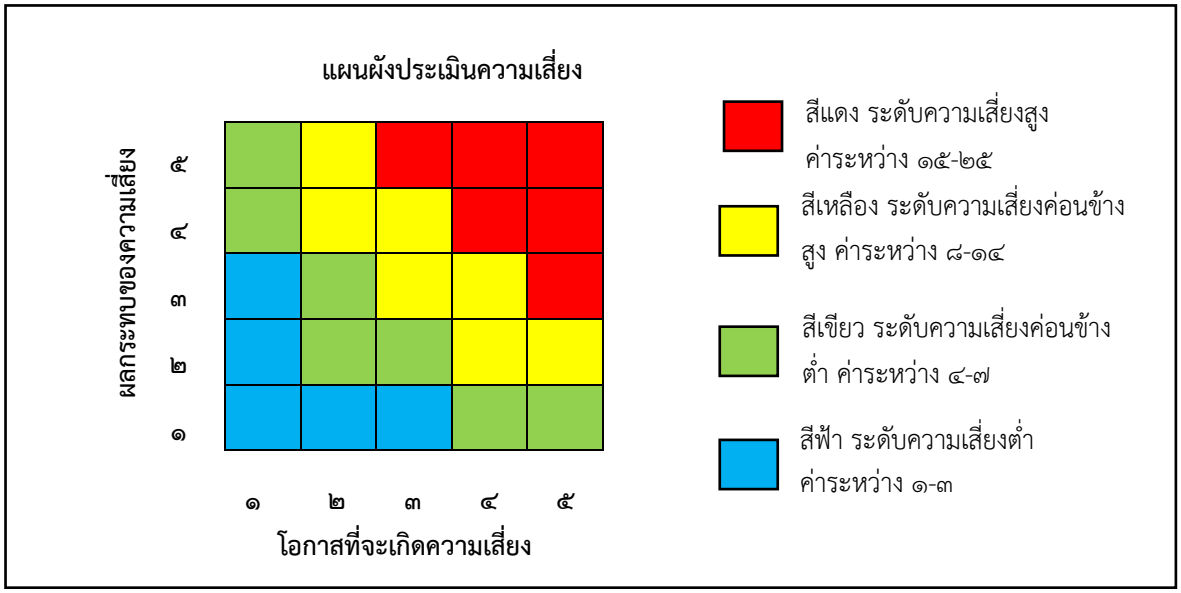
เกณฑ์การประเมินผลกระทบ เป็นดังนี้

ระดับ	การประเมิน
๑	น้อยมาก
๒	น้อย
๓	ปานกลาง
๔	สูง
๕	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยงเป็นดังนี้

ระดับ	การประเมิน
๑	เกิดขึ้นน้อยมาก
๒	เกิดขึ้นน้อย
๓	เกิดขึ้นปานกลาง
๔	เกิดขึ้นสูง
๕	เกิดขึ้นสูงมาก

๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปที่ ๒



รูปที่ ๒ แสดงแผนผังประเมินความเสี่ยง

๒.๔ การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๓. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๓.๑ ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

๓.๒ การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๓.๓ การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๓.๔ การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่

โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

๒) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๔. การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

๔.๑ พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔.๔ ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๕. การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๖. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

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

ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร
(Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ alware, 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 ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ 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 ความเสี่ยง เนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

๗. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

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

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๘. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ 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 และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

๒.๓ เจ้าหน้าที่หรือบุคลการของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๙. การประเมินความเสียหาย

๑. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒. ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๑๐. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

๑๑. ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบคอมพิวเตอร์และเครือข่ายของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่าย สำนักงานปลัดกระทรวงเกษตรและสหกรณ์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ตั้งอยู่ที่สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ถนนราชดำเนินนอก แขวงบ้านพานถม เขตพระนคร กรุงเทพฯ

ระบบคอมพิวเตอร์และเครือข่าย สำนักงานปลัดกระทรวงเกษตรและสหกรณ์มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์ และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ของ FortiGate ๖๒๐B ซึ่งใช้ในการกรอง (Filter Package) ที่ผ่านเข้ามาภายในระบบของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์จากเครือข่ายภายนอก เช่น เครือข่ายของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เครือข่ายอินเทอร์เน็ต เครือข่าย GIN[๑] นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของ DMZ[๒] ที่ดูแลเครื่องแม่ข่ายทั้งหมดของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่อง

คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ในส่วนกลาง มีการแบ่ง Subnet[๓] เพื่อให้เป็นระบบกลุ่มบรอดคาสต์โดเมน (Broadcast Domain) เดียวกัน ประกอบกับกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private[๔] เพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

ระบบเครือข่ายหลักของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (Core Network) ตั้งอยู่ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นศูนย์กลางการเชื่อมต่อทำหน้าที่เชื่อมโยงระบบเครือข่ายภายในระดับกอง/สำนักงาน ในความเร็วระดับ ๑,๐๐๐ Mbps และระบบเครือข่ายภายนอก เช่น อินเทอร์เน็ต และ GIN เข้าด้วยกันซึ่งมี Core Switch ที่ออกแบบติดตั้งในลักษณะระบบเครือข่ายที่สามารถทดแทนกันได้ (Redundant Network) เพื่อแก้ปัญหาระบบเครือข่ายศูนย์กลางล่ม (Single Point of Failure) และแก้ปัญหาคอขวดในการเข้าถึงข้อมูล (Bottleneck)เพื่อรองรับภารกิจของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ซึ่งลักษณะงานต้องใช้อุปกรณ์เครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพสูงสามารถรองรับการเชื่อมต่อกับระบบเครือข่ายภายในและภายนอกแบบ ๒๔x๗ เพื่อใช้ระบบงานฐานข้อมูลที่สำคัญของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ พร้อมทั้งเชื่อมโยงไปยังอุปกรณ์ Distributed Switch (L๓) และ Access Switch(L๒) ไปยังอาคารต่างๆ ซึ่งเป็นที่ตั้งของหน่วยงานในสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

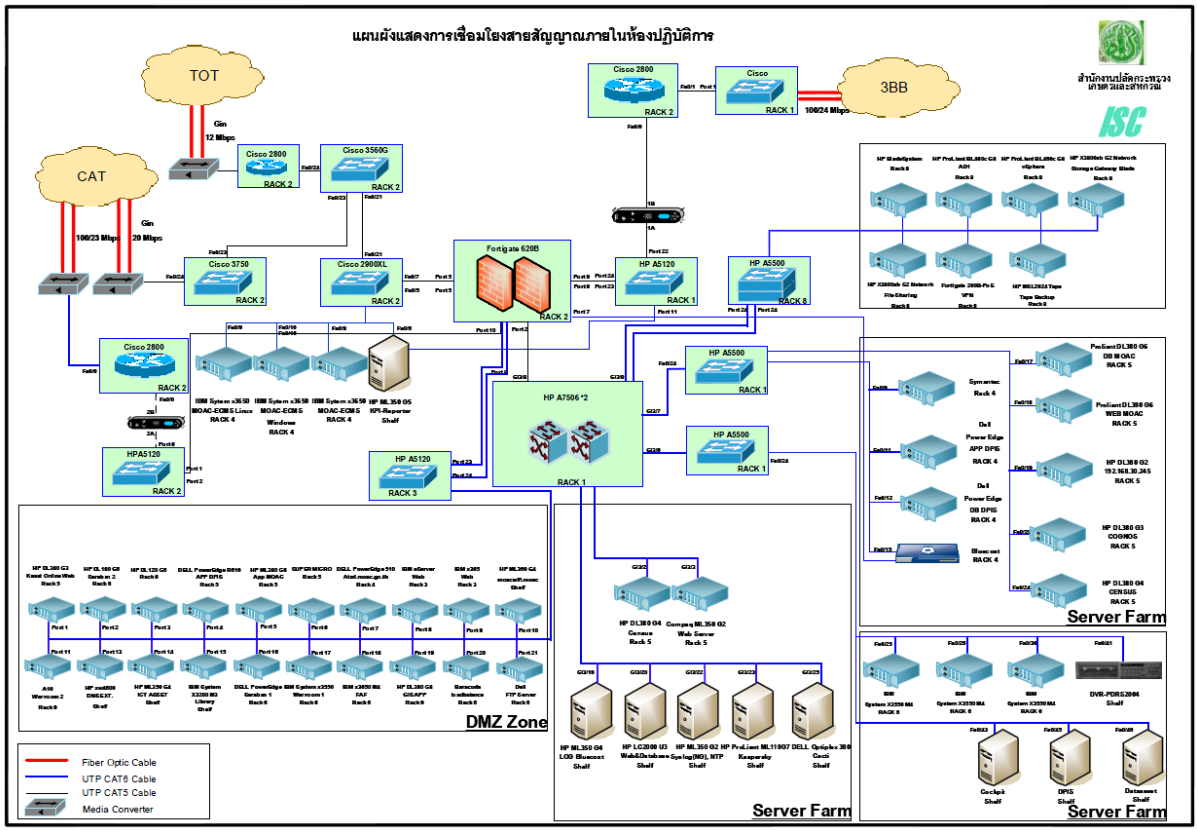
---

[๑] Government Information Network (Gin)

[๒] โซนเครื่องคอมพิวเตอร์แม่ข่าย (Demilitarized Zone)

[๓] มีการแบ่งหมายเลข IP Address เป็นกลุ่มย่อย (Subnet Mask)

[๔] หมายเลขภายใน (Private IP Address)

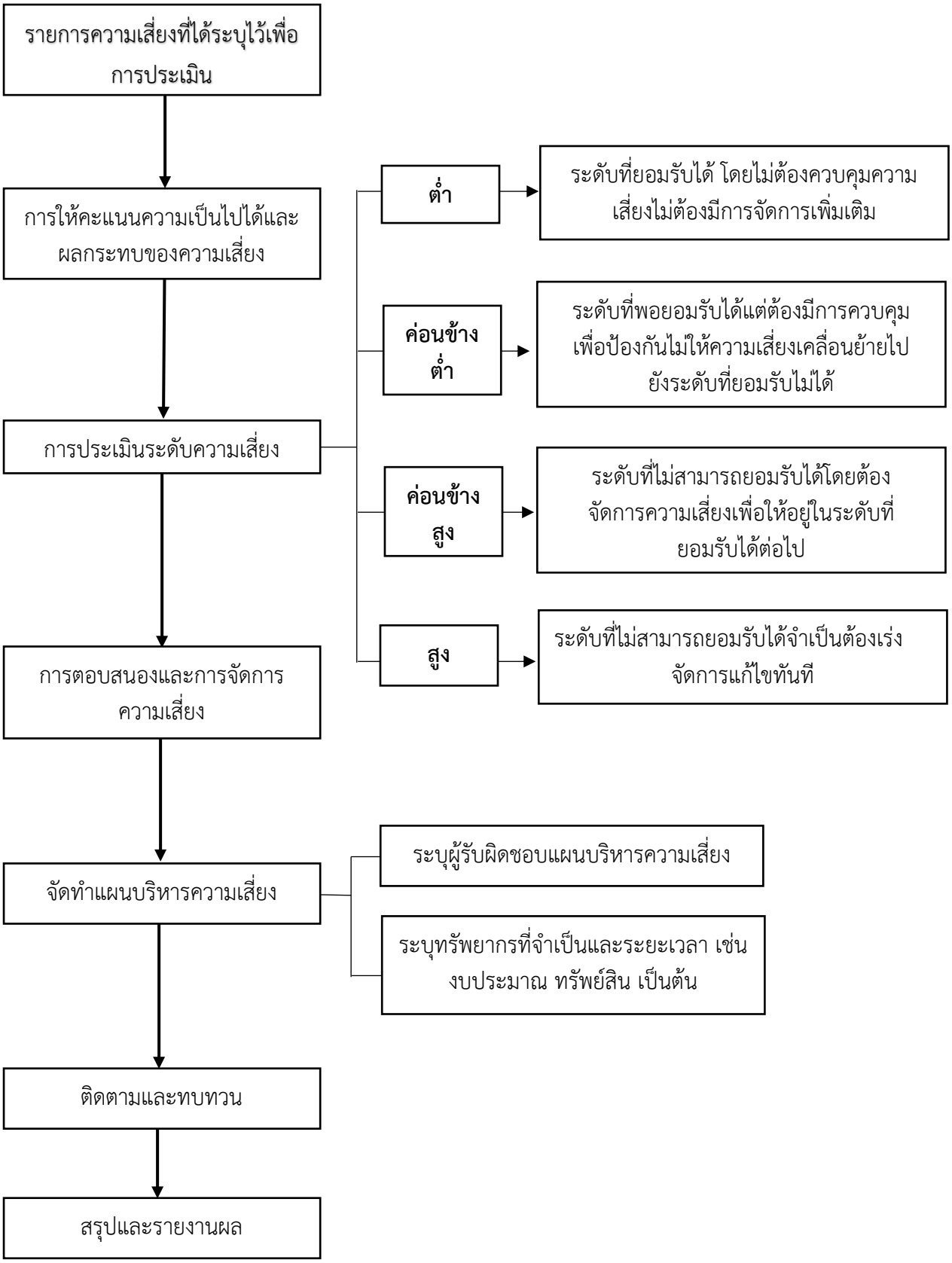


รูปที่ ๓ แสดงโครงข่ายคอมพิวเตอร์สารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

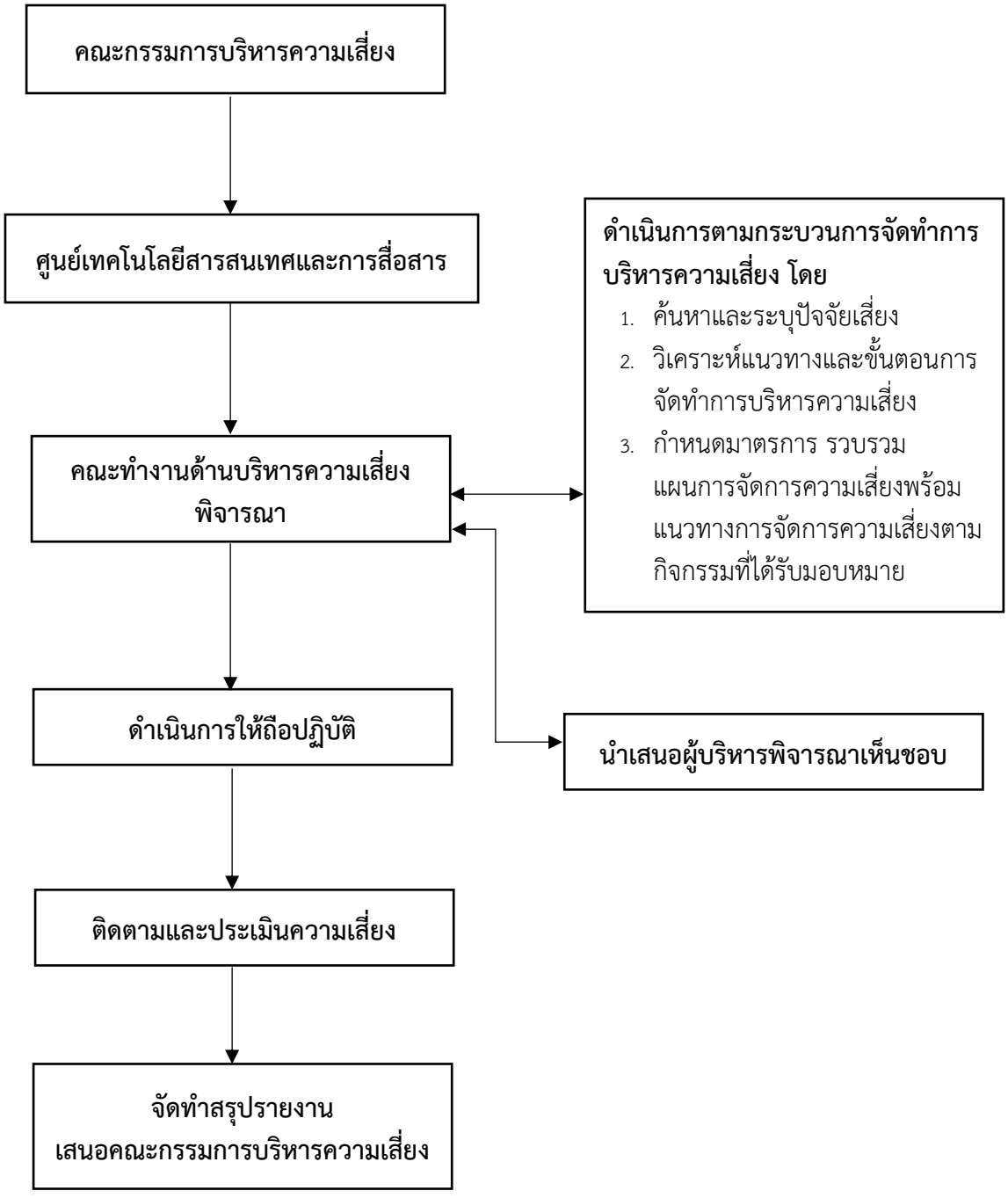
บทที่ ๒
การวิเคราะห์การบริหารจัดการความเสี่ยง

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. ๒๕๕๙-๒๕๖๓ ให้สอดคล้องกับแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของ สป.กษ. (IT๔) กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

๑ แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง

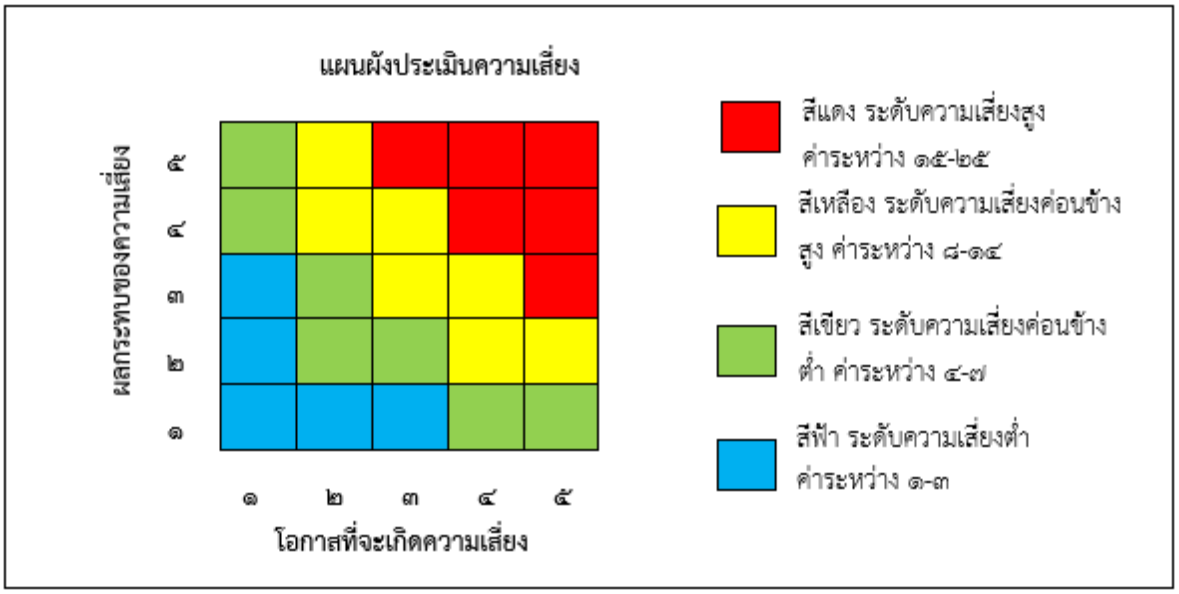


๒ กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



๓ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุป การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้



ตารางที่ ๑ ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
๑	ความเสี่ยงจากอัคคีภัย	๓	๕	๑๕
๒	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๓	๕	๑๕
๓	ความเสี่ยงจากความชื้น อุณหภูมิ	๕	๓	๑๕
๔	การไม่สำรองข้อมูล/ การสำรองข้อมูลขาดการอัพเดท	๓	๕	๑๕
๕	ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๓	๕	๑๕
๖	การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง	๓	๕	๑๕
๗	ระบบกระแสไฟฟ้าขัดข้อง	๓	๔	๑๒
๘	การเชื่อมต่อระบบอินเทอร์เน็ต/ อินทราเน็ตขัดข้อง	๓	๔	๑๒
๙	การบุกรุกโจมตีจากภายนอก	๓	๔	๑๒
๑๐	ลิขสิทธิ์ซอฟต์แวร์	๒	๕	๑๐
๑๑	ไวรัสคอมพิวเตอร์/ Malware	๒	๔	๘
๑๒	ความเสี่ยงจากการถูก Black List จาก Search Engine /Spamhaus	๒	๓	๖
๑๓	ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	๒	๓	๖
๑๔	เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	๒	๓	๖
๑๕	ความเสี่ยงจากแมลง/สัตว์กัดแทะ	๑	๕	๕

ลำดับ	ประเภทความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
๑๖	การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์	๑	๕	๕
๑๗	การโจมตี Server ของหน่วยงานไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)	๑	๕	๕
๑๘	ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต	๑	๕	๕
๑๙	วินาศภัย/การก่อการร้าย	๑	๕	๕
๒๐	การโจรกรรมฐานข้อมูล	๑	๕	๕
๒๑	ความเสี่ยงจากไฟกระชากจากปลั๊กพ่วง	๒	๒	๔
๒๒	ความเสี่ยงจากแผ่นดินไหว	๑	๔	๔
๒๓	ความเสี่ยงจากอุทกภัย	๑	๓	๓

๔ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสียงสูง							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๑. ความเสี่ยงจากการเกิดอัคคีภัย	๑. คอมพิวเตอร์และเครือข่ายถูกทำลาย ๒. ข้อมูลถูกทำลาย ๓. การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร	๑. เสียงบประมาณในการจัดหาระบบทดแทน ๒. การไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน	สูง ๓x๕=๑๕	๑. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง ๒. วางแผนจัดหาและติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง ๓. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๒. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๑. ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ ๒. เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	๑. การใช้งานระบบงานไม่สามารถใช้ได้ตามปกติ	สูง ๓x๕=๑๕	๑. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล ๒. จัดตั้งศูนย์สำรองข้อมูล (Backup Site)	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๓. ความเสี่ยงจากความชื้นอุณหภูมิ	ห้องคอมพิวเตอร์แม่ข่ายไม่มีระบบปรับอากาศที่สามารถความคุมอุณหภูมิความชื้นได้	อายุของเครื่องและอุปกรณ์สั้นลง	สูง ๕x๓=๑๕	๑. ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ ๒. จัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	การยอมรับ (Take)	ศทส.

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	๔. ความเสี่ยงจากการสำรองข้อมูล การทำงานระบบไม่มีความเสถียรภาพ หรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	๑. เสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานได้ตามปกติ ๒. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	๑. เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือ การจัดทำขึ้นมาใหม่ ๒. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้ เนื่องจากขาดความมั่นใจในข้อมูล	สูง ๓x๕=๑๕	๑. มีการบริหารจัดการในการทำการสำรองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ ๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	๕. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑. การถูกขโมยข้อมูล ๒. โปรแกรมเสียหาย ๓. การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง	๑. ลดความน่าเชื่อถือต่อ สป.กษ. หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ ๒. กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อ สป.กษ. เป็นอย่างยิ่ง	สูง ๓x๕=๑๕	๑. ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top ๑๐ Web Application Security Risks เพื่อลดความเสี่ยง ๒. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ ๓. ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่	การควบคุม (Treat)	หน่วยงานที่มีการพัฒนาระบบงานขึ้นใช้เอง
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	๖. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource) การขาดแผนบริหารความต่อเนื่อง	๑. เสี่ยงต่อการถูกขโมยข้อมูล ๒. เสี่ยงต่อการทำความเสียหายแก่โปรแกรม ๓. ไม่สามารถแก้ไขข้อบกพร่องได้เอง	๑. ลดความน่าเชื่อถือต่อ สป.กษ. หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ ๒. กรณีที่เป็นข้อมูลลับ	สูง ๓x๕=๑๕	๑. การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level ๒. การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล – ER Diagram ๓. ให้มีการส่งมอบ Source Code ในรูปแบบ DVD ในฟอร์แมตที่ไม่	การควบคุม (Treat)	ศทส. หรือ สำนัก/กองอื่นๆ ที่พัฒนาระบบงานขึ้นใช้เอง

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
		๔. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว ๕. เสียค่าใช้จ่ายสูง	อาจสร้างความเสียหายต่อสำนักงานฯ เป็นอย่างยิ่ง ๓. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลพร้อมกับการทำการบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการอัพเดทอยู่เสมอ		เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้ ๔. หากมีการพัฒนา Library ด้วยตนเอง ต้องส่ง Source Code Library ที่สามารถแก้ไขได้ ๕. มีการถ่ายทอดความรู้ เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ ๖. มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม ๗. จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงานระหว่างผู้รับจ้างกับผู้ว่าจ้าง ๘. มีแผนการบำรุงรักษาระบบงานที่ดีรวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดทเมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น		

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสียงค่อนข้างสูง							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๑. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	๑. ไม่สามารถใช้งานเครื่องแม่ข่าย และเครือข่ายได้ ๒. ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่ายทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูกทำการShutdown อย่างเหมาะสม	๑. ข้อมูลเสียหาย ๒. ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเสียหาย ต้องมีการติดตั้งใหม่	ค่อนข้างสูง ๓x๔=๑๒	๑. ตรวจสอบระบบสำรองไฟฟ้า (UPS) ๒. วางแผนการจัดหาและติดตั้งเครื่องกำเนิดไฟฟ้า (Electrical Generator) สำหรับสำนักงานปลัดทระทรวงเกษตรและสหกรณ์	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๒. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	๑. ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านเครือข่ายอินทราเน็ตได้ ๒. ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่ายอินเทอร์เน็ตได้	๑. ขัดขวางการทำงานของเจ้าหน้าที่และผู้บริหารงานสำนักงานฯ ๒. บุคคลภายนอกไม่สามารถเข้าใช้ Web Server หรือค้นหาข้อมูลที่ต้องการได้	ค่อนข้างสูง ๓x๔=๑๒	ตรวจสอบระบบเครือข่ายสื่อสารหลัก	การควบคุม (Treat)	ศทส.

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๓. ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก	เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	๑. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย ๒. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของสำนักงานฯ ๓. ถูกโจรกรรมข้อมูลที่เป็นความลับ	ค่อนข้างสูง ๓x๔=๑๒	๑. ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย ๒. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับ ๓. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	๔. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๑. การสูญหายของข้อมูล ๒. การถูกฟ้องร้องและเสื่อมเสียชื่อเสียงและความน่าเชื่อถือของสำนักงานฯ	๑. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ ๒. สป.กษ. อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ ๓. ความไม่สะดวกหากไม่ใช้งานด้วยซอฟต์แวร์ที่ไม่จำเป็นต้องมีลิขสิทธิ์ (Open Source)	ค่อนข้างสูง ๒x๕=๑๐	๑. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๒. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย	การควบคุม (Treat)	ศทส.

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๕. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	๑. โปรแกรมหรือข้อมูลถูกทำลาย ๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ ๓. การถูกขโมยข้อมูล	๑. ใช้คอมพิวเตอร์ไม่ได้ ๒. ใช้ระบบงานไม่ได้ ๓. ข้อมูลที่สำคัญสูญหาย	ค่อนข้างสูง ๒x๔=๘	๑. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย ๒. อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ	การควบคุม (Treat)	ศทส.
ความเสี่ยงค่อนข้างต่ำ							
ความเสี่ยงด้านบุคลากร (Human Risk) และความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๑. ความเสี่ยงจากการถูก Black List โดย Search Engine หรือ Spamhaus (http://www.spamhaus.org)	๑. ผู้ใช้งานที่ต้องการข้อมูลของ สป.กษ. หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ ๒. ไม่สามารถใช้งานเครือข่ายหรือ e-mail ได้	๑. ลดความน่าเชื่อถือหรือข้อมูลของ สป.กษ. ๒. สป.กษ. อาจถูกฟ้องร้องโดยผู้มีส่วนได้ส่วนเสีย	ค่อนข้างต่ำ ๒x๓=๖	๑. ติดตั้งโปรแกรม เพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ต ๒. ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server หรือ FTP Server ๓. มีการอัพเดทตัวโปรแกรมและ Signature อย่างสม่ำเสมอ และการทำการบำรุงรักษา (Maintenance) ทั้งฮาร์ดแวร์และซอฟต์แวร์ พร้อมทั้ง Update Licenses	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	๒. ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสียเช่น Hard Disk หรือ	๑. ข้อมูลที่อยู่ในชั้นความลับ รั่วไหลทำให้เสียหายต่อความเชื่อถือของ สป.กษ.	ค่อนข้างต่ำ ๒x๓=๖	มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk ม้วนเทป (Cartridge Tape) แผ่น DVD/ CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่าง	การยอมรับ (Take)	ศทส.

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
		ม้วนเทป (Cartridge Tape) แผ่น DVD/ CD	๒. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้		ถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้		
ความเสี่ยงด้านบุคลากร (Human Risk)	๓. ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/ เครือข่ายผิดวัตถุประสงค์	๑. เสี่ยงต่อการใช้งานในทางที่ผิด หรือเปล่าประโยชน์ เช่น การฟังวิทยุหรือดูโทรทัศน์ออนไลน์ เป็นต้น ๒. การใช้ Resource ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์ หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	๑. สูญเสีย Bandwidth ในเครือข่ายทำให้ ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี ๒. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	ค่อนข้างต่ำ ๒x๓=๖	๑. บริหารจัดการด้วยข้อแนะนำ Ten Ways to Protect Your Network From Insider Threats เพื่อลดความเสี่ยง ๒. กำหนด Policy ของFirewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น ๓. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่างๆ ไปใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๔. ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า/ สายสัญญาณ	เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	๑. เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน ๒. ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	ค่อนข้างต่ำ ๑x๕=๕	๑. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack ๒. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การควบคุม (Treat)	ศทส.

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๕. ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง						
	๕.๑ เครื่องแม่ข่ายสูญหาย	เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	๑. เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง ๒. เสียเวลาในการกู้ระบบ ๓. เสียภาพลักษณ์ของสำนักงานฯ	ค่อนข้างต่ำ ๑x๕=๕	๑. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย ๒. ตู้ Rack ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์จัดเก็บข้อมูล (Disk Array) และอุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจตลอดเวลา ๓. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน	การควบคุม (Treat)	ศทส.
	๕.๒ เครื่องลูกข่ายและอุปกรณ์ต่อพ่วงสูญหาย	เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	๑. เสียงบประมาณในการจัดหาอุปกรณ์ทดแทน ๒. เสียภาพลักษณ์ของ สป.กษ.	ค่อนข้างต่ำ ๑x๕=๕	๑. ควบคุมการเข้าออกอาคาร ๒. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-ออก อาคารตลอดเวลา ๓. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ๆ มี เครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	การควบคุม (Treat)	กองกลาง

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๖. ความเสี่ยงจากการโจมตีเครื่องแม่ข่ายของ สป.กษ. ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)						
	๖.๑ ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายนอก	เสี่ยงต่อการถูกโจมตีได้จากภายนอก โดยโจมตีทั้งเครื่องแม่ข่ายและ/หรือ เครือข่ายในทุกรูปแบบ ซึ่งจะมีการพัฒนาวิธีการอยู่ตลอดเวลา	ไม่สามารถใช้งานเครือข่าย ได้ หรือใช้ได้แต่ช้ามาก	ค่อนข้างต่ำ ๑x๕=๕	๑. ติดตั้งระบบป้องกัน และเตือนภัย Spam,Virus, Malware, Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้นๆ อยู่เป็นประจำเพื่อลดหรือสามารถแก้ไขได้ทันเมื่อถูกโจมตี ๒. หมั่นตรวจสอบ Policy และ Log ของ Firewall และ IPS/ IDS อย่างสม่ำเสมอ	การควบคุม (Treat)	ศทส.
	๖.๒ ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ	ไม่สามารถใช้งานเครือข่าย ได้ หรือใช้ได้แต่ช้ามาก	ค่อนข้างต่ำ ๑x๕=๕	๑. มีมาตรการ และกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่างๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายอินทราเน็ตของ สป.กษ. ๒. การควบคุมด้วยระบบ Desktop Management	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	๗. ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต	เสี่ยงต่อผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลเข้าใช้เครือข่าย อินทราเน็ต	ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ปอัน	ค่อนข้างต่ำ ๑x๕=๕	๑. ควบคุมการเข้าใช้เครือข่าย ๒. เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดย	การควบคุม (Treat)	ศทส.

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
(Hardware and Data Communication Risk)		ผ่านทาง WiFi	จะนำมาซึ่งการขาดความ เชื่อถือของสำนักงานฯ		ติดตั้งระบบยืนยันตน (Authentication)		
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๘. ความเสี่ยงจากวินาศภัย/การก่อการร้าย	การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ค่อนข้างต่ำ ๑x๕=๕	๑. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน ๒. จัดทำแผนสำรองฉุกเฉิน ๓. จัดทำศูนย์สำรอง (Backup Site)	การยอมรับ (Take)	ศทส.
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	๙. ความเสี่ยงจากการโจรกรรมฐานข้อมูล	ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ	๑. เสียชื่อเสียงและความน่าเชื่อถือที่มีต่อ สป.กษ. ๒. การสูญหายหรือถูกทำลายของข้อมูล	ค่อนข้างต่ำ ๑x๕=๕	๑. มีการบริหารจัดการด้านการป้องกันข้อมูล ๒. มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) ๓. มีการบริหารสื่อจัดเก็บข้อมูล เช่น Hard disk ๔. Disk ม้วนเทป (Cartridge Tape) แผ่น DVD/CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวรหรือได้ทำลายอุปกรณ์ หรือสื่อเก็บข้อมูลนั้นๆ ทิ้งแล้ว หากทำได้	การควบคุม (Treat)	ศทส.
ความเสี่ยงด้านบุคลากร (Human Risk)	๑๐. ความเสี่ยงจากไฟกระชากจากสายพ่วง (Extension Cord)	เสี่ยงต่อไฟไหม้ ไฟดูดไฟย้อนกลับ ทำให้อุปกรณ์เครื่องคอมพิวเตอร์เสียหายทั้งหมดได้	๑. ไม่สามารถใช้งานเครื่องคอมพิวเตอร์ได้ตามปกติ ๒. ไฟอาจลัดวงจรทำให้เครื่องเสียหาย	ค่อนข้างต่ำ ๒x๒=๔	๑. งดใช้สายพ่วง หรืองดใช้สายพ่วงที่ไม่ได้มาตรฐาน ม.อ.ก. และไม่มีสายดิน ๒. ไม่ใช้อุปกรณ์ที่ไม่มีสายดิน (ปลั๊ก ๒ ขา หรือ ๓ ขาแต่หักสายดินออก) ต่อเข้ากับสายพ่วงหรือ	การควบคุม (Treat)	ศทส.

ประเภทความเสี่ยง	ความเสียง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					เต้าไฟฟ้า (Receptacle) ๓. ต่อสายพ่วงเข้ากับอุปกรณ์ที่มีระบบ Stabilizer		
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๑๑. ความเสี่ยงจากแผ่นดินไหว	ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ค่อนข้างต่ำ ๑x๔=๔	๑. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน ๒. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไร และจะใช้เครื่องทดแทนจากที่ใด เพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง ๓. จัดทำศูนย์สำรอง (Backup Site)	การยอมรับ (Take)	ศทส.
ความเสี่ยงต่ำ							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๑. ความเสี่ยงจากการเกิดอุทกภัย	ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	การให้บริการระบบขาดความต่อเนื่อง	ค่อนข้างต่ำ ๑x๓=๓	๑. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	การยอมรับ (Take)	ศทส. และ กก.

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์
กระทรวงเกษตรและสหกรณ์

ผู้รับผิดชอบหลัก
หน่วยงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ระยะเวลาการดำเนินการ ตุลาคม ๒๕๕๙ - ตุลาคม ๒๕๖๓

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๕๙	๒๕๖๐			๒๕๖๑			๒๕๖๒			๒๕๖๓			ผลลัพธ์ความก้าวหน้า
			๑๐-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
๑. ความเสี่ยงจากการเกิดอัคคีภัย	ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	- ทุกวันที่ ๓๐ ก.ย. ของทุกปี	←			→			→			→			→	
๒. ความเสี่ยงจากการระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	- ตรวจสอบระบบคอมพิวเตอร์แม่ข่าย	- ทุก ๓ เดือน	←			→			→			→			→	
๓. ความเสี่ยงจากความชื้นอุณหภูมิ	- ตรวจสอบการทำงานอุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ	- ทุกวัน	←												→	
๔. ความเสี่ยงจากการสำรองข้อมูล การทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ - มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	- ทุกวัน - ๒ ระบบต่อปี	←			→			→			→			→	

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๕๙	๒๕๖๐			๒๕๖๑			๒๕๖๒			๒๕๖๓			ผลลัพธ์ความก้าวหน้า
			๑๐-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
๕. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่	ปีละ ๑ ครั้ง	←→			←→			←→			←→			←→	
๖. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (outsource) ขาดแผนบริหารความต่อเนื่อง	- จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงานระหว่างผู้รับจ้างกับผู้ว่าจ้าง	ปีละ ๑ ครั้ง	←→			←→			←→			←→			←→	

บทที่ ๓
สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแลตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อน การดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงานภายในสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายหรือเสียหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือการจัดการความเสี่ยงในองค์กร นั่นเอง

๑. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนสูงสุด ๖ อันดับแรก ได้ข้อสรุปดังนี้

๑. ความเสี่ยงจากการเกิดอัคคีภัย มีแนวทางปฏิบัติดังนี้

- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง
- ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง
- มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ

๒. ความเสี่ยงจากการระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย มีแนวทางปฏิบัติดังนี้

- ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักและสำรองฐานข้อมูล
- การจัดตั้งศูนย์สำรองข้อมูล (Backup Site)

๓. ความเสี่ยงจากความชื้น อุณหภูมิ มีแนวทางปฏิบัติดังนี้

- ตรวจสอบการทำงาน อุณหภูมิเครื่องปรับอากาศ ที่มีอยู่เดิมอย่างสม่ำเสมอ
- จัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาะที่เหมาะสมและสามารถทำงานสลับกันได้

๔. ความเสี่ยงจากการสำรองข้อมูล การทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดทมีแนวทางปฏิบัติดังนี้

- การบริหารจัดการในการทำการสำรองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ
- มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)

๕. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรม ประยุกต์ภายในองค์กร มีแนวทางปฏิบัติดังนี้

- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top ๑๐ Web Application Security Risks เพื่อลดความเสี่ย

- มาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ
- ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่

๖. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource) การขาดแผนบริหารความต่อเนื่อง มีแนวทางปฏิบัติดังนี้

- การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level
- การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล – ER Diagram
- ให้มีการส่งมอบ Source Code ในรูปแบบ DVD ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้
- หากมีการพัฒนา Library ด้วยตนเอง ต้องส่ง Source Code Library ที่สามารถแก้ไขได้
- มีการถ่ายทอดความรู้ เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่
- มีมาตรการในการกำหนดให้นำข้อมูลใด ออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม
- จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงานระหว่างผู้รับจ้างกับผู้ว่าจ้าง
- มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crashของโปรแกรมหรือฐานข้อมูล(Database) เกิดความเสียหาย เป็นต้น

๒. สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

๓.๒.๑ เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

๓.๒.๒ เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓.๒.๓ ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓. ข้อเสนอแนะ

๓.๓.๑ การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

๓.๓.๑.๑ พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

๓.๓.๑.๒ พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

๓.๓.๑.๓ กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

๓.๓.๒ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพ และมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ

สารบัญ

www.opsmoac.go.th
INFORMATION &
COMMUNICATION
TECHNOLOGY CENTER

INFORMATION COMMUNICATION TECHNOLOGY CENTER
3 Ratchadamnoennok Road,
Bangkok 10200.
Tel : 0-2281-5955 # 361 , 290
Email : ict_its@opsmoac.go.th