องค์การตลาดเพื่อเกษตรกร
WWW.ORTORKOR.COM

แผนบริหารความเสี่ยง
ด้านความมั่นคงปลอดภัยสารสนเทศ
องค์การตลาดเพื่อเกษตรกร
พ.ศ. 2567

กองเทคโนโลยีและสารสนเทศ

คำนำ

องค์การตลาดเพื่อเกษตรกร โดยกองเทคโนโลยีและสารสนเทศ ได้จัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ องค์การตลาดเพื่อเกษตรกร พ.ศ. ๒๕๖๗ ขึ้น ด้วยการวิเคราะห์และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อบริหารจัดการความเสี่ยงตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committees of Sponsoring Organizations of the Treadway Commission) โดยได้วิเคราะห์ความเสี่ยงให้ครอบคลุมตาม หลักธรรมภิบาล และเป็นไปตามข้อกำหนดตามเกณฑ์การพัฒนาคุณภาพการบริหารจัดการภาครัฐ (POMA) ซึ่ง สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (ISO ๒๗๐๐๑) แผนบริหารจัดการความเสี่ยงดังกล่าว จะใช้เป็นกรอบแนวทางในการปฏิบัติงานของหน่วยงานต่าง ๆ ที่เกี่ยวข้อง ตลอดจนการกำกับดูแลการใช้งานด้านความมั่นคงปลอดภัยสารสนเทศ ขององค์การตลาดเพื่อเกษตรกร เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยง ทำให้ระบบงานต่าง ๆ สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และมีความมั่นคงปลอดภัยสูงสุด

ผู้จัดทำ

กองเทคโนโลยีและสารสนเทศ

สารบัญ

บทที่ ๑

บทนำ

๑. หลักการและเหตุผล

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เป็นเครื่องมือในการป้องกันปัญหาที่อาจเกิดขึ้น อันส่งผลกระทบต่อข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร อีกทั้ง เป็นการนำเทคโนโลยีดิจิทัลมาช่วยในการสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด และลดโอกาสความเสียหายที่อาจจะเกิดขึ้นกับองค์กร โดยมีการกำหนดความเสี่ยงแต่ละด้านว่ามีปัจจัยเสี่ยงใดบ้างที่มีผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร และนำมาวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยง ตลอดจนกำหนดแนวทางการบริหารจัดการความเสี่ยง และการจัดการความเสี่ยงอย่างเหมาะสม

๒. วัตถุประสงค์

๑. เพื่อให้การจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์การตลาดเพื่อเกษตรกร มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับสถานการณ์ให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหาย

๒. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์การตลาดเพื่อเกษตรกร

๓. เพื่อให้มีการวางแผน ควบคุม และแก้ไขจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อีกทั้งเป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศขององค์การตลาดเพื่อเกษตรกรให้มีเสถียรภาพมีความพร้อมในการใช้งาน

๔. เพื่อเป็นแนวทางการดำเนินการกำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๕. เพื่อเพิ่มประสิทธิภาพการบริหารจัดการองค์กร การตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงในด้านต่าง ๆ ที่อาจมีผลกระทบกับการดำเนินงานตามวัตถุประสงค์ และนโยบายเพื่อนำมาพิจารณาและแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้นก่อนที่จะเริ่มปฏิบัติงานตลอดจนเชื่อมโยงการบริหารจัดการความเสี่ยงกับแผนงานด้านเทคโนโลยีดิจิทัล ให้ได้รับการยอมรับและมีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๓. เป้าหมาย

ข้อมูลด้านเทคโนโลยีสารสนเทศขององค์การตลาดเพื่อเกษตรกรมีความมั่นคงปลอดภัย

๔. ขอบเขตการดำเนินงาน

บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่อาจจะเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและส่งผลกระทบ หรือสร้างความเสียหายภายใต้ความรับผิดชอบของกองเทคโนโลยีและสารสนเทศองค์การตลาดเพื่อเกษตรกร

๕. ผู้รับผิดชอบ

กองเทคโนโลยีและสารสนเทศ เป็นผู้ปฏิบัติหน้าที่ตามแนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีดิจิทัลระดับองค์กรที่ดี (Digital Governance Practice) โดยได้วางมาตรการระบบรักษาความปลอดภัยที่กำหนดอำนาจและหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการวางระบบรักษาความปลอดภัย (Security) และระบบบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเตรียมพร้อมในการแก้ไขสถานการณ์ฉุกเฉินได้อย่างรวดเร็วต่อเนื่อง และมีประสิทธิภาพ

๖. ประโยชน์ที่คาดว่าจะได้รับ

๑. มีความพร้อมในการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศขององค์การตลาดเพื่อเกษตรกร

๒. มีแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูล และระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมใช้งานเกิดประโยชน์สูงสุดและลดโอกาสความเสียหายที่จะเกิดขึ้น

บทที่ ๒

นโยบายที่เกี่ยวข้องและแนวปฏิบัติ

๑. นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้องค์การตลาดเพื่อเกษตรกร มีการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพและสอดคล้องกับความเสี่ยงขององค์กร จึงควรมีนโยบายที่เกี่ยวข้องต่าง ๆ ดังนี้

๑. กำหนดให้มีนโยบายเป็นลายลักษณ์อักษรและอยู่ใต้กรอบหลักการที่สำคัญ ๓ ประการ คือ การรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ อย่างน้อยครอบคลุมนโยบายดังต่อไปนี้

- นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT security policy)
- นโยบายการกำกับดูแลและบริหารจัดการที่ดีด้านเทคโนโลยีและสารสนเทศ (IT governance policy)

๒. สอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการให้บริการหรือดำเนินธุรกิจความเสี่ยงที่เกี่ยวข้องทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศและความเสี่ยงกรณีมีการใช้บริการเชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอก รวมทั้งสอดคล้องกับแนวทางบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

๓. นโยบายดังกล่าวต้องได้รับอนุมัติจากผู้อำนวยการองค์การตลาดเพื่อเกษตรกร และได้รับการทบทวน อย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้ง ควรจัดให้มีการชี้แจง และสื่อสารนโยบายให้ผู้เกี่ยวข้อง ได้รับทราบอย่างทั่วถึงและมีการควบคุมดูแลให้มีการปฏิบัติตามนโยบายได้ อย่างถูกต้องครบถ้วน

๔. นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT security policy) ควรรวมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมอย่างน้อย

๔.๑ การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

๔.๒ การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information Security)

๔.๓ การควบคุมการเข้าถึง (Access Control)

๔.๔ การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

๔.๕ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

๔.๖ การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

๔.๗ การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System Acquisition and Development)

๔.๘ การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)

๔.๙ การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๔.๑๐ การบริหารจัดการผู้ให้บริการภายนอก (third party management)

๔.๑๑ การป้องกันโปรแกรมไม่ประสงค์ดี (Malicions Software Prevention)

๔.๑๒ การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ท (Website and Internet Security)

๕. นโยบายการกำกับดูแลและบริหารจัดการที่ดีด้านเทคโนโลยีและสารสนเทศ (IT governance policy) โดยครอบคลุมอย่างน้อย โดยต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการองค์การตลาดเพื่อเกษตรกรหรือคณะอนุกรรมการที่ได้รับมอบหมายจากคณะกรรมการองค์การตลาดเพื่อเกษตรกร โดยมีการสื่อสารไปยังผู้ที่เกี่ยวข้อง รวมทั้งมีการทบทวนและปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง และต้องทบทวนโดยทันทีเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการบริหารและจัดการความเสี่ยงด้านสารสนเทศอย่างมีนัยสำคัญ

ทั้งนี้ ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีการทบทวนหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๒. แนวทางปฏิบัติการป้องกันความเสียหาย

๒.๑. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับสูงมาก ดังนั้นสิ่งที่มักจะเกิดขึ้นและยากที่จะหลีกเลี่ยงได้ก็คือผลกระทบต่าง ๆ ที่เกิดขึ้นจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลที่สำคัญ รวมถึงการสูญเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ซึ่งประกอบด้วย

๑. <u>ไฟฟ้าตก (Say หรือ Brownout)</u> คือ สภาวะที่แรงดันไฟฟ้าลดต่ำลงจากปกติในช่วงเวลาสั้น ๆ ซึ่งเป็นปัญหาทางไฟฟ้าที่พบบ่อยที่สุด

<u>สาเหตุ</u> เกิดจากการเปิดสวิตช์อุปกรณ์บางชนิดที่ต้องการใช้กระแสไฟฟ้ามาก เช่น ลิฟต์ เครื่องปรับอากาศ และเครื่องมือเครื่องจักร เป็นต้น

<u>ผลกระทบ</u> อุปกรณ์เหล่านี้ ต้องการกระแสไฟฟ้ามากในการเริ่มการทำงานของเครื่องเมื่อเปรียบเทียบกับการทำงานในภาวะปกติ ส่งผลให้แรงดันไฟฟ้าในสายส่งการไฟฟ้าฯ ลดต่ำลง

๒. <u>ไฟฟ้าดับ (Blackout)</u> คือ สภาวะที่กระแสไฟฟ้าหยุดไหล

<u>สาเหตุ</u> เกิดจากความต้องการกระแสไฟฟ้าจากสายส่งการไฟฟ้าฯ ที่มากเกินไป เกิดไฟฟ้าลัดวงจรในสายส่ง, พายุฟ้าคะนอง แผ่นดินไหว และปัญหาที่เกิดกับสายส่งการไฟฟ้าฯ เช่น เสาไฟฟ้าล้ม หรือหม้อแปลงระเบิด ฯลฯ ซึ่งส่งผลให้ไม่สามารถจ่ายไฟจากการไฟฟ้าได้

<u>ผลกระทบ</u> การทำงานของฮาร์ดดิสก์หยุดชะงักทันที ทำให้ข้อมูลที่กำลังบันทึกสูญหาย รวมถึง อาจส่งผลให้ข้อมูลที่เก็บไว้ทั้งหมดสูญหาย บันทึกข้อมูลของตารางการจัดการแฟ้ม (FAT) สูญหายได้ ซึ่งอาจมีผลให้ข้อมูลที่เก็บไว้ทั้งหมดสูญหายได้

๓. <u>ไฟฟ้ากระชาก (Spike)</u> คือ สภาวะที่แรงดันไฟฟ้าเพิ่มสูงขึ้นอย่างกะทันหัน โดยสามารถเข้าไปยังอุปกรณ์ไฟฟ้าได้ ทั้งจากสายส่งการไฟฟ้าฯ เครือข่ายสื่อสาร และสายโทรศัพท์

<u>สาเหตุ</u> เกิดจากฟ้าผ่าในบริเวณใกล้เคียง หรืออาจเกิดจากสายส่งจากการไฟฟ้าฯ ที่หยุดการทำงาน และกลับมาทำงานใหม่อย่างกะทันหัน

<u>ผลกระทบ</u> สร้างความเสียหายหรือทำลายชิ้นส่วนอุปกรณ์อิเล็กทรอนิกส์ของอุปกรณ์ไฟฟ้าได้ รวมถึงข้อมูลเกิดการสูญหาย

๔. <u>ไฟฟ้าเกิน (Surge)</u> คือ สภาวะที่มีแรงดันไฟฟ้าไหลมามากเกินในช่วงเวลาสั้น ๆ

<u>สาเหตุ</u> เกิดจากการใช้อุปกรณ์ไฟฟ้าที่มีมอเตอร์กินไฟมาก เช่น เครื่องปรับอากาศ หรืออุปกรณ์ไฟฟ้าอื่น ๆ ที่ลักษณะใกล้เคียงกัน ฯลฯ เนื่องจากอุปกรณ์เหล่านี้เมื่อหยุดทำงานแรงดันไฟฟ้าส่วนหนึ่งที่เหลืออยู่ในมอเตอร์จะไหลกลับเข้าไปในสายส่งการไฟฟ้าฯ ทำให้เกิดแรงดันไฟฟ้าสูงเกิน

<u>ผลกระทบ</u> ทำให้ชิ้นส่วนอุปกรณ์ภายในเสื่อมสภาพเร็วกว่าปกติหรือเสียหายได้ รวมถึงหน่วยความจำของคอมพิวเตอร์สูญหายและคลาดเคลื่อน, Power supply เสียหาย และการทำงานของระบบสื่อสารผิดพลาด

๕. <u>สัญญาณรบกวน (Noise)</u> คือ สัญญาณรบกวนที่เกิดจากสนามแม่เหล็กไฟฟ้า (EMI) และสัญญาณคลื่นความถี่วิทยุ (RF) ซึ่งทั้ง ๒ สัญญาณนี้ จะไปรบกวนสัญญาณคลื่นไซน์ (Sine Wave) ของสายส่งการไฟฟ้าฯ

<u>สาเหตุ</u> เกิดขึ้นได้จากปรากฏการณ์ทางธรรมชาติ (เช่น ฟ้าผ่า), การเปิด-ปิดสวิตซ์, อุปกรณ์ไฟฟ้า เครื่องส่งวิทยุ เป็นต้น โดยสัญญาณรบกวนอาจเกิดขึ้นเป็นระยะ ๆ หรืออาจเกิดอย่างสม่ำเสมอก็ได้

<u>ผลกระทบ</u> ทำให้การประมวลผลของโปรแกรมและแฟ้มข้อมูลทำงานผิดพลาดและเกิดข้อบกพร่อง

<u>หลักปฏิบัติในการป้องกันความเสียหาย</u>

เพื่อป้องกันการมิให้เกิดความเสียหายอันเกิดจากกระแสไฟฟ้า และบุคลากรสามารถปฏิบัติตนได้ถูกต้องเมื่อเกิดปัญหาจากกระแสไฟฟ้า จึงกำหนดหลักปฏิบัติของบุคลากรในองค์กร ดังนี้

๑. เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์ ทั้งเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล

๒. เมื่อเกิดกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ ปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นๆ ภายในสำนักงานด้วย

๒.๒. ระบบป้องกันการโจรกรรม

กองเทคโนโลยีและสารสนเทศ องค์การตลาดเพื่อเกษตรกร ตั้งอยู่ เลขที่ ๑๐๑ ถนนย่านพหลโยธิน แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร ๑๐๙๐๐ (สำนักงานใหญ่) มีระบบป้องกันการโจรกรรมตามระเบียบของทางราชการเกี่ยวกับการดูแลรักษาสถานราชการ / ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ บทที่ ๕ การรักษาความปลอดภัยอันเกี่ยวกับ สถานที่ และระบบเวรยามของสำนักงาน ดังนี้

๑. ดำเนินการในส่วนที่เกี่ยวข้องตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

๒. ห้ามผู้ที่ไม่มีหน้าที่เกี่ยวข้องเข้าถึงคอมพิวเตอร์แม่ข่าย และลงทะเบียนการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายทุกครั้ง

<u>หลักปฏิบัติในการป้องกันความเสียหาย</u>

เพื่อป้องกันการโจรกรรม จึงกำหนดหลักปฏิบัติของบุคลากรในองค์กร ดังนี้

๑. ปฏิบัติตนให้เป็นไปตามระเบียบในส่วนที่เกี่ยวข้องกับการดูแลรักษาสถานที่ และระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

๒. เฝ้าระวัง และสอดส่องดูแลเพื่อป้องกันมิให้เกิดการโจรกรรมขึ้น ทั้งนี้หากพบเห็นเหตุการณ์ หรือบุคคลซึ่งคาดว่าจะนำไปสู่การโจรกรรมทรัพย์สินหรือข้อมูลสารสนเทศต่าง ๆ ให้รีบรายงานให้ผู้บังคับบัญชาตามลำดับชั้นทราบโดยด่วนที่สุด เพื่อจะได้ประสานงานกับเจ้าหน้าที่ที่เกี่ยวข้องหรือเจ้าหน้าที่ตำรวจ ในการที่จะระงับหรือจับกุมผู้ที่จะกระทำการดังกล่าวต่อไป

๓. แผนผังสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดสถานการณ์ฉุกเฉิน

เป็นไปตามแผนบริหารความต่อเนื่อง Business Continuity Plans (BCP) ขององค์การตลาดเพื่อเกษตรกร โดยมีโครงการ ดังนี้

๓.๑. คณะกรรมการบริหารความต่อเนื่องทางธุรกิจ ประกอบด้วย ผู้อำนวยการ/รองผู้อำนวยการ/ผู้อำนวยการสำนักนโยบายและแผน/หัวหน้ากองพัฒนาระบบงานและบริหารความเสี่ยง มีหน้าที่ กำหนด จัดทำ ทบทวนนโยบายฯ กำหนดกลยุทธ์ จัดทำ และทบทวนแผนฯ พิจารณาตัดสินใจประกาศใช้ และยุติการใช้แผนฯ พิจารณาให้ความเห็นชอบการวิเคราะห์ผลกระทบทางธุรกิจและการประเมินความเสี่ยงภัยคุกคาม กำกับ ควบคุม และติดตามผลการดำเนินงานของ คณะทำงานางานบริหารความต่อเนื่องทางธุรกิจระดับส่วนกลางระดับส่วนกลาง และระดับส่วนภูมิภาค ให้เป็นไปตามขั้นตอน สื่อสาร ประชาสัมพันธ์ ทบทวน ทดสอบและฝึกซ้อม ชี้แจง ให้ข้อมูลข่าวสาร ทั้งภายใน และภายนอก อ.ต.ก.

๓.๒. คณะทำงานบริหารความต่อเนื่องทางธุรกิจส่วนกลาง ประกอบด้วย รองผู้อำนวยการ (ที่ได้รับมอบหมายทางด้านบริหาร)/ผู้อำนวยการฝ่ายบริหาร/ผู้อำนวยการฝ่ายกิจการตลาด/ผู้อำนวยการฝ่ายพัฒนาธุรกิจ/ผู้อำนวยการฝ่ายธุรกิจเกษตร/ผู้อำนวยการสำนักนโยบายและแผน/ผู้อำนวยการฝ่ายการเงินและบัญชี/หัวหน้ากองพัสดุ มีหน้าที่ รักษาความปลอดภัยของชีวิตพนักงาน ทรัพย์สิน และข้อมูลสำคัญของ อ.ต.ก. ประเมินสถานการณ์ ความเสียหาย และดำเนินการตามขั้นตอนการปฏิบัติสำหรับการจัดการอุบัติการณ์ ติดตาม รวบรวมข้อมูล และประเมินสถานการณ์ความเสียหาย แนวโน้ม และระดับความรุนแรงของสถานการณ์ที่เกิดขึ้น รายงานต่อคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ ประสานงานและสนับสนุนการแก้ไขปัญหากับหน่วยงานต่างๆ ที่เกี่ยวข้อง พิจารณาและขออนุมัติงบประมาณจากคณะกรรมการบริหารความต่อเนื่องทางธุรกิจเพื่อสนับสนุน และจัดสรรทรัพยากร ให้เพียงพอ กำกับ ควบคุม และติดตามผลการดำเนินงานของส่วนงานในสังกัดให้เป็นไปตามขั้นตอนที่กำหนดไว้ รายงานผลการดำเนินงานต่อคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ แต่งตั้งทีมบริหารความต่อเนื่องทางธุรกิจของหน่วยงาน

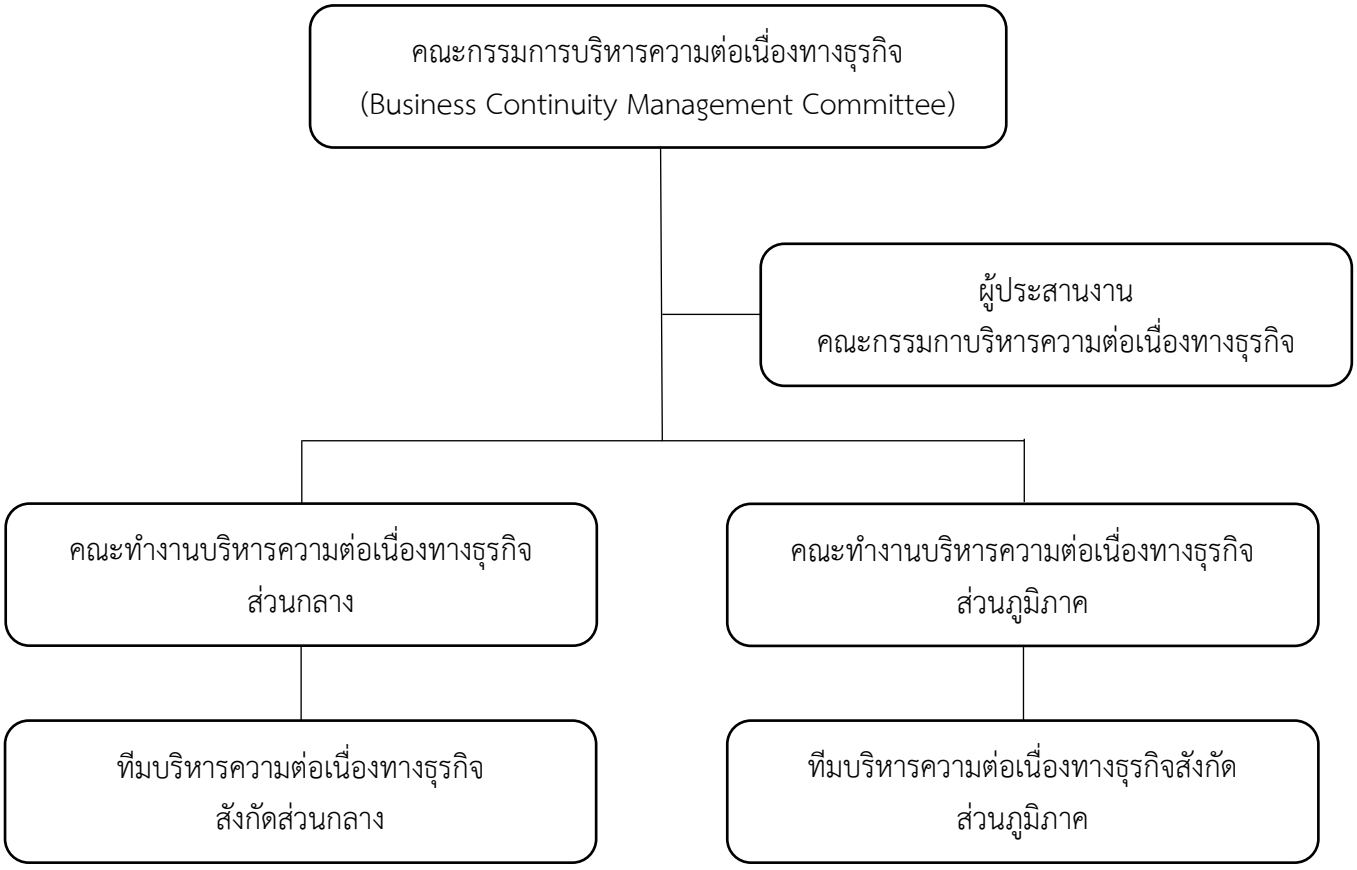
๓.๓ คณะทำงานบริหารความต่อเนื่องทางธุรกิจส่วนภูมิภาค ประกอบด้วย รองผู้อำนวยการ อ.ต.ก. (ที่ได้รับมอบหมายภูมิภาค)/ผู้อำนวยการฝ่ายกิจการภูมิภาค/ผู้จัดการ อ.ต.ก. เขต ๑/ผู้จัดการ อ.ต.ก. เขต ๒/ผู้จัดการ อ.ต.ก. เขต ๓/ผู้จัดการ อ.ต.ก. เขต ๔/หัวหน้ากลุ่มบริหารงานกิจการภูมิภาค มีหน้าที่ รักษาความปลอดภัยของชีวิตพนักงาน ทรัพย์สิน และข้อมูลสำคัญของ อ.ต.ก. ประเมินสถานการณ์ ความเสียหาย และดำเนินการตามขั้นตอนการปฏิบัติสำหรับการจัดการอุบัติการณ์ ติดตาม รวบรวมข้อมูล และประเมินสถานการณ์ความเสียหาย แนวโน้ม และระดับความรุนแรงของสถานการณ์ที่เกิดขึ้น รายงานต่อคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ ประสานงานและสนับสนุนการแก้ไขปัญหากับหน่วยงานต่างๆ ที่

เกี่ยวข้อง พิจารณาและขออนุมัติงบประมาณจากคณะกรรมการบริหารความต่อเนื่องทางธุรกิจเพื่อสนับสนุนและจัดสรรทรัพยากร ให้เพียงพอ กำกับ ควบคุม และติดตามผลการดำเนินงานของส่วนงานในสังกัดให้เป็นไปตามขั้นตอนที่กำหนดไว้ รายงานผลการดำเนินงานต่อคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ แต่งตั้งทีมบริหารความต่อเนื่องทางธุรกิจของหน่วยงาน

๓.๔ ทีมบริหารความต่อเนื่องทางธุรกิจของหน่วยงาน แต่งตั้งโดยหัวหน้าคณะทำงานบริหารความต่อเนื่องทางธุรกิจส่วนกลาง/ภูมิภาค มีหน้าที่ปฏิบัติตามขั้นตอนแนวทางของแผนบริหารความต่อเนื่องทางธุรกิจ

๓.๕ ผู้ประสานงานคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ ได้แก่ หัวหน้าสำนักงานผู้อำนวยการ มีหน้าที่ในการติดต่อและประสานงานภายในหน่วยงาน ให้การสนับสนุนในการติดต่อสื่อสารภายในหน่วยงานและดำเนินการตามขั้นตอนและแนวทางการบริหารความต่อเนื่อง

ผังโครงสร้างทีมงานแผนบริหารความต่อเนื่องทางธุรกิจ



บทที่ ๓

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๑. ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ใด ๆ ที่อาจจะเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจส่งผลกระทบหรือสร้างความเสียหาย ทั้งที่สามารถประเมินมูลค่าเป็นตัวเงินและที่ไม่สามารถประเมินมูลค่าเป็นตัวเงินได้ หรืออาจก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายและวัตถุประสงค์ตามภารกิจขององค์กร

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนทเศในการดำเนินธุรกิจ ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของ อ.ต.ก. รวมถึงความเสี่ยงที่เกิดจากภัยคุมคามทางไซเบอร์

ปัจจัยเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่จะทำให้เกิดความเสี่ยง ที่อาจทำให้ไม่บรรลุวัตถุประสงค์ ที่กำหนดไว้

เหตุการณ์เสี่ยง หมายถึง เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงานหรือนโยบาย

ผลกระทบของความเสี่ยง หมายถึง ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์ เสี่ยงที่อาจเกิดขึ้น

การบริหารความเสี่ยง หมายถึง ระบบบริหารและควบคุม รวมทั้งกระบวนการดำเนินงานต่าง ๆ เพื่อที่จะลดสาเหตุของโอกาสที่จะก่อให้เกิดความเสียหาย เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ สามารถประเมินผล ควบคุม และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าประสงค์ตามภารกิจหลัก และเป้าหมายตามแผนปฏิบัติงานขององค์กร

๒. กระบวนการบริหารความเสี่ยง

กระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร และการบริหารจัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง มีขั้นตอนการดำเนินการ ตามหลักเกณฑ์ ๕ ขั้นตอน ดังนี้

๒.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้อง เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

๒.๒ การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๑) <u>การกำหนดเกณฑ์การประเมินมาตรฐาน</u> เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยง อาจกำหนดเป็นเกณฑ์ ๕ ระดับ ได้แก่สูงมาก/รุนแรงมากที่สุด, สูง/ค่อนข้างรุนแรง, ปานกลาง, น้อย และน้อยมาก ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ ได้แก่สูงมาก, สูง, ปานกลาง และน้อย

๒) <u>การประเมินโอกาสและผลกระทบของความเสี่ยง</u> เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้ มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้น และประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนด เพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงจะมีความรุนแรงแตกต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ขึ้นอยู่กับ มาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มีผลกระทบ และมีโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง (Likelihood) ดังนี้

ระดับที่	ระดับของโอกาส	คำจำกัดความของแต่ละระดับ	
		คำอธิบาย<u>เชิงคุณภาพ</u>	**คำอธิบาย<u>เชิงปริมาณ</u>**
๕	**สูงมาก**	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้ในสภาพการณ์ส่วนใหญ่ เกิดเกือบทุกครั้ง ตัวอย่างเช่น มีโอกาสเกิดขึ้นได้มากกว่า ๘๐% ภายในระยะเวลา ๑๒ เดือนข้างหน้า	๑ เดือนต่อครั้ง หรือมากกว่า
๔	**สูง**	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้ในสภาพการณ์ส่วนใหญ่ เกิดค่อนข้างสูงหรือบ่อยๆ ตัวอย่างเช่น มีโอกาสเกิดขึ้นได้มากกว่า ๕๐% แต่ไม่เกิน ๗๙% ภายในระยะเวลา ๑๒ เดือนข้างหน้า	๑ ปีไม่เกิน ๕ ครั้ง
๓	**ปานกลาง**	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้ในบางเวลาเกิดบางครั้ง ตัวอย่างเช่น มีโอกาสเกิดขึ้นได้มากกว่า ๒๐% แต่ไม่เกิน ๔๙% ภายในระยะเวลา ๑๒ เดือนข้างหน้า	๑ ปีต่อครั้ง
๒	**ต่ำ**	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้ในบางเวลาเท่านั้น เกิดแต่นานๆครั้ง ตัวอย่างเช่น มีโอกาสเกิดขึ้นได้มากกว่า ๑๐% แต่ไม่เกิน ๑๙% ภายในระยะเวลา ๑๒ เดือนข้างหน้า	๒-๓ ปีต่อครั้ง
๑	**ต่ำมาก**	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้เมื่อเกิดสภาพการณ์ผิดปกติเท่านั้น เกิดในกรณียกเว้น ตัวอย่าง เช่น มีโอกาสเกิดขึ้นได้น้อยกว่าหรือเท่ากับ ๑๐% ภายในระยะเวลา ๑๒ เดือนข้างหน้า	๕ ปีต่อครั้ง

ทั้งนี้ ในระดับความเสี่ยงปานกลาง ต้องมีการควบคุมความเสี่ยงที่มีการติดตามผลและประเมินผลต่อความเสี่ยงที่เกิดขึ้นจริงอย่างมีประสิทธิภาพ ประสิทธิผล และมีผู้รับผิดชอบโดยตรง เช่น มีแผนปฏิบัติ คู่มือปฏิบัติ มีการมอบหมาย ที่ชัดเจน

เกณฑ์การประเมินผลกระทบ (Impact) แบ่งออกเป็น ๕ ด้าน ดังนี้

๑. ผลกระทบด้านการเงิน เป็นผลกระทบหรือความเสียหายที่เกิดจากความเสี่ยงและสามารถประเมินค่าเป็นตัวเงินได้

๒. ผลกระทบด้านชื่อเสียง ภาพลักษณ์องค์กร และความพึงพอใจของผู้ใช้บริการ

๓. ผลกระทบต่อการไม่ปฏิบัติตามกฎ ระเบียบ ข้อบังคับ

๔. ผลกระทบต่อบุคลากรสำคัญขององค์กร

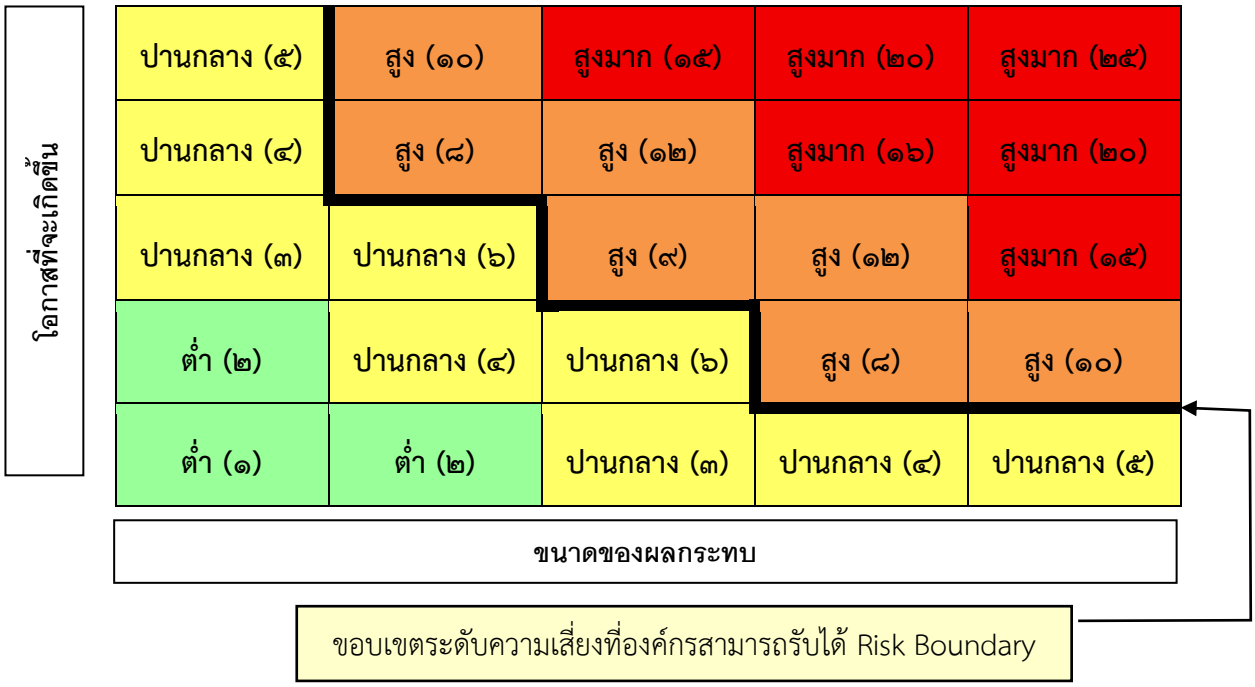
๕. ผลกระทบต่อความล่าช้าในการดำเนินงานโครงการสำคัญ

ระดับผลกระทบ	หลักเกณฑ์ในการพิจารณาระดับผลกระทบ
สูงมาก : ๕	ความสูญเสียที่มีผลกระทบอย่างรุนแรงต่อการดำรงอยู่ของกิจการหรือธุรกิจ
สูง : ๔	เหตุการณ์ที่เกิดขึ้นจำเป็นต้องอาศัยความพยายามอย่างสูงของผู้บริหารในการจัดการกับเหตุการณ์ ดังกล่าว
ปานกลาง : ๓	เหตุการณ์ที่เกิดขึ้นมีความสำคัญในระดับที่ผู้บริหารจะต้องเพิ่มการดูแลเอาใจใส่มากขึ้นจากการบริหารงานปกติ
ต่ำ : ๒	เหตุการณ์ที่เกิดขึ้นในทางตรงข้ามกับที่คาดการณ์ไว้ ซึ่งมีผลกระทบต่อกิจการในระดับที่ยอมรับได้ก็ต่อเมื่อผู้บริหารเข้าร่วมแก้ไขปัญหา
ไม่เป็นสาระสำคัญ : ๑	ผลกระทบของความเสี่ยงที่เกิดขึ้นจะถูกกลืนหายไปด้วยกิจกรรมดำเนินงานตามปกติ

<u>หมายเหตุ</u> : คู่มือการบริหารความเสี่ยงและการควบคุมภายใน องค์การตลาดเพื่อเกษตรกร

๓) <u>การวิเคราะห์ความเสี่ยง</u> เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยนำทั้งสององค์ประกอบมาพิจารณาร่วมกันให้ทราบถึงระดับความเสี่ยง (Level of Risk) ซึ่งเป็นตัวชี้วัดสำคัญของความเสี่ยงนั้น ๆ แสดงถึงระดับความสำคัญในการบริหารความเสี่ยง และพิจารณาตามตารางประเมินระดับคะแนนความเสี่ยง (Risk Assessment Matrix)

ค่าคะแนนความเสี่ยง = ระดับผลกระทบ X ระดับโอกาสที่จะเกิดความเสี่ยง



จากนั้น นำรายการความเสี่ยงแต่ละระดับความเสี่ยงที่ได้จัดเรียงไว้ (Risk Ranking) มาวิเคราะห์เปรียบเทียบกับเกณฑ์ความสามารถในการยอมรับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วยแทบสี	ความหมาย
ต่ำ (L) (สีเขียว)	๑.๐ – ๒.๙		- ระดับที่ยอมรับได้ ไม่จำเป็นต้องมีแผนดำเนินการเพิ่มเติม แต่ให้ผู้รับผิดชอบติดตามผลกระทบที่เกี่ยวเนื่องกับความเสี่ยงเป็นประจำ
ปานกลาง (M) (สีเหลือง)	๓.๐ – ๗.๙		- ระดับที่พอยอมรับได้ ไม่จำเป็นต้องมีแผนดำเนินงานเพิ่มเติม แต่มอบหมายให้ผู้รับผิดชอบ ติดตามประสิทธิภาพการควบคุมภายในกระบวนการเป็นประจำ
สูง (H) (สีส้ม)	๘.๐ – ๑๔.๙		- ระดับที่ยอมรับไม่ได้ โดยจัดทำแผนบริหารความเสี่ยงด้วยการปรับปรุงประสิทธิภาพของมาตรการหรือปรับปรุงการควบคุมภายในที่มีอยู่ในปัจจุบัน เพื่อไม่ให้เพิ่มระดับไประดับสูงมาก
สูงมาก (VH) (สีแดง)	๑๕.๐ – ๒๕.๐		- ระดับที่เกินกว่าจะยอมรับได้ จำเป็นต้องทำแผนบริหารความเสี่ยงสำหรับจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้เนื่องจากการดำเนินงานไม่เป็นไปตามเป้าหมาย

๔) <u>การจัดลำดับความเสี่ยง</u> เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้แล้ว และเลือกความเสี่ยงที่มีระดับสูงมากหรือสูง มาจัดทำแผนการบริหารความเสี่ยงก่อน

หากอยู่ในโซนที่เกินระดับคะแนน (Impact x Likelihood) ๘ หรือระดับคะแนนเกิน ๘ ในโซนสีส้มและสีแดง จะต้องทำการบริหารหรือจัดการความเสี่ยง หากมีระดับคะแนน (Impact x Likelihood) ตั้งแต่ ๗.๙ คะแนนลงมา ปัจจัยเสี่ยงนั้นก็อยู่ในระดับที่ต้องทำการเฝ้าระวัง โดยไม่ต้องมีการบริหารความเสี่ยงก็ได้

๒.๓ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยง เพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ การควบคุมแบ่งได้ เป็น ๔ ประเภท คือ

๑) ควบคุมเพื่อความป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกัน ไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุมและการเข้าถึงเอกสาร เป็นต้น

๒) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับและรายงานข้อบกพร่อง เป็นต้น

๓) การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๔) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

๒.๔ การติดตามรายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่กำหนดไว้

คือ การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงในโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ซึ่งทางเลือกในการบริหารความเสี่ยงมีหลายวิธี สามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจจะเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยงและการประเมินการควบคุมแล้ว ให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือกเพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจากประเด็นต่าง ๆ ดังนี้

๑) พิจารณาว่า ยอมรับความเสี่ยงหรือจะกำหนดกิจกรรมควบคุม เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๒) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการ ให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๓) กรณีเลือกกำหนดกิจกรรมควบคุม เพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔) ในรอบปีต่อไป ให้พิจารณาผลการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการ นำมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วย

ในการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยงว่า ยังคงมีความเสี่ยงเหลืออยู่หรือไม่ ถ้ายังมีเหลืออยู่ให้พิจารณาว่าอยู่ในในระดับความเสี่ยงสูงมากเพียงใด มีวิธีการจัดการความเสี่ยงนั้นอย่างไร และนำเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๒.๕ การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

คือ การดำเนินงานการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยงว่ามีการจัดการความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตราการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๓. การบริหารความเสี่ยงขององค์กร (Enterprise Risk Management: ERM)

การบริหารความเสี่ยงขององค์กร (Enterprise Risk Management: ERM) หรือการบริหารความเสี่ยงระดับองค์กรโดยรวม (Enterprise Wide Risk Management) คือ กระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหารและบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบ เพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่องค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้

อ.ต.ก. ได้จำแนกความเสี่ยงออกเป็น ๕ ประเภทตามหลักเกณฑ์ของกระทรวงการคลัง ดังนี้

๑. ความเสี่ยงด้านกลยุทธ์ (S : Strategic) คือ ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ และการปฏิบัติตามแผนกลยุทธ์ รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมาย กลยุทธ์ โครงสร้างองค์กร ภาวะการณ์แข่งขัน ทรัพยากร และสภาพแวดล้อม อันส่งผลกระทบต่อวิสัยทัศน์ พันธกิจ หรือเป้าหมายขององค์กร และขัดขวางการบรรลุวัตถุประสงค์ขององค์กรในด้านกลยุทธ

๒. ความเสี่ยงด้านการปฏิบัติงาน (O : Operational) คือ ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงาน อันเนื่องจากขาดการกำกับดูแลที่ดี หรือขาดการควบคุมภายในที่ดี โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากรในการปฏิบัติงาน ความปลอดภัยของทรัพย์สิน และขัดขวางการบรรลุวัตถุประสงค์ขององค์กรด้านปฏิบัติงาน

๓. ความเสี่ยงด้านการเงิน (F : Financial) คือ ความเสี่ยงที่ส่งผลกระทบต่อฐานะการเงิน เช่น สภาพคล่องทางการเงิน รายงานทางการเงิน การบริหารงบประมาณและการเงิน ที่ขัดขวางการบรรลุวัตถุประสงค์ขององค์กรด้านการเงิน

๔. ความเสี่ยงด้านการปฏิบัติตามระเบียบ / กฎหมาย (C : Compliance) คือ ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบและข้อบังคับของกฎหมาย รวมถึงข้อบังคับภายในองค์กรด้วย

๕. ความเสี่ยงด้านความน่าเชื่อถือขององค์กร (R : Reputation) คือ ความเสี่ยงที่ส่งผลกระทบต่อชื่อเสียง ความเชื่อมั่น และความน่าเชื่อถือขององค์กร

๔. ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

องค์การตลาดเพื่อเกษตรกร โดยกองเทคโนโลยีและสารสนเทศ ได้กำหนดประเภทความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามแนวทางของ COSO (Committee of Sponsoring Organization) เป็น ๘ ประเภท ดังนี้

๔.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึง การไม่มีระบบรักษาความปลอดภัยที่มีประสิทธิภาพเพียงพอ ในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย

๔.๒ ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินงานทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งานการดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

การบริหารจัดการความเสี่ยงด้านบุคลากร มีแนวทางดำเนินการ ดังนี้

๑) การกำหนดโครงสร้าง รวมถึง การมอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศ ที่มีความเหมาะสม ซึ่งมีความรู้และมีประสบการณ์เพียงพอในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีด้านการรักษาความปลอดภัยด้านข้อมูลและเครือข่ายระบบเทคโนโลยีสารสนเทศ (Data and Network Securities) และสามารถถ่ายทอดความรู้นั้น ๆ ให้แก่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ได้อย่างมีประสิทธิภาพ

๒) จัดอบรมบุคลากรเกี่ยวกับแนวทางในการวางแผนบริหารความเสี่ยง และทดสอบความรู้ทางเทคโนโลยีสารสนเทศ (Certified) อย่างต่อเนื่องและเป็นระบบ เพื่อพัฒนาคุณภาพและประสิทธิภาพของบุคคลากร

๓) ในแผนการบริหารความเสี่ยงด้านบุคลากรนั้น จำเป็นต้องมีการฝึกอบรมเจ้าหน้าที่ที่เกี่ยวข้องกับระบบฐานข้อมูล สำหรับบุคลากรใน ๒ ระดับ คือ ระดับผู้ดูแลระบบ (Administration Level) และผู้ใช้งานทั่วไป (User Level)

๔) จัดอบรมและจัดทำคู่มือในการใช้งานระบบคอมพิวเตอร์และเครือข่ายที่ถูกต้องรวมถึงข้อควรระวังในการรับส่งแฟ้มข้อมูลต่างๆ จากอุปกรณ์ที่เชื่อมโยงโดยตรงกับคอมพิวเตอร์

๔.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และภายนอก โดยผ่านทางระบบเครือข่ายหรือจากระบบคอมพิวเตอร์โดยตรง เช่น จาก Flash Drive หรือ External Hard Disk Drive เป็นต้น

๔.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดจุดอ่อนของระบบที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบหรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งอาจทำให้องค์กรถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

๖.๕ ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากการเสียหายของฐานข้อมูลต่างๆ ในระบบเทคโนโลยีสารสนเทศ เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกระบบเพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้องค์กรเกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียชื่อเสียงขององค์กร ความเสี่ยงเหล่านี้ ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศ เป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึง ประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือ เหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่ต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อข้อมูลระบบเทคโนโลยีสารสนเทศ

๔.๖ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่าง ๆ ในด้านเทคโนโลยีสารสนเทศ ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงได้

๔.๗ ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงที่ได้รับการสนับสนุนด้านงบประมาณไม่เพียงพอ

๔.๘ ความเสี่ยงในด้านการบริหารจัดการ (Management Risk) หมายถึง ความเสี่ยงอันเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีการวิเคราะห์ความคุ้มทุนของแผนงาน ไม่มีการกำหนดขั้นตอนการดำเนินงานและผลสัมฤทธิ์ของงาน และไม่มีวิธีการควบคุมติดตามประเมินผลงานเพื่อเพิ่มประสิทธิภาพ

๕. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้น เพื่อเปรียบเทียบกับผลประโยชน์ที่จะได้รับ เพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้น และลดผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) โดยมีหลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

๕.๑. การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้น ไม่คุ้มกับสิ่งที่จะเกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงาน เลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ อาจนำมาซึ่งการเสียโอกาสของหน่วยงานได้

๕.๒. การยอมรับ (Take) เป็นการยอมรับความเสี่ยงหรือความเสียหายที่อาจจะเกิดขึ้นไว้เอง โดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในเกณฑ์ที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้ User/Password ที่กำหนดให้แล้ว อาจจะบอก User/Password ของตนให้ผู้ใต้บังคับบัญชาทราบ และเมื่อผู้ใต้บังคับบัญชาทราบ User/Password ของหัวหน้างาน อาจจะเก็บไว้คนเดียว หรือนำไปบอกให้บุคคลอื่นทราบต่อในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายและหน่วยงานที่รับผิดชอบต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น แล้วจึงแก้ไขโดยการกำหนด User/Password ใหม่ ให้กับหัวหน้างาน เป็นต้น

๕.๓. การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้ วิธีการควบคุมความสูญเสียมี ๒ วิธี คือ

๑) <u>การป้องกันการเกิดความสูญเสีย</u> เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย โดยหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย เป็นการป้องกันบุคคลหรือไวรัสคอมพิวเตอร์ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ เป็นต้น

๒) <u>การควบคุมขนาดของความสูญเสีย</u> เป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้น เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ในห้องคอมพิวเตอร์แม่ข่าย เพื่อสามารถป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา เพื่อลดความสูญเสียของอุปกรณ์ให้มีความเสียหายน้อยที่สุด หรือไม่เกิดความเสียหาย หรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

๕.๔. การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น ในกรณีการรับประกันของอุปกรณ์เครือข่ายที่ซื้อมามีระยะเวลาเพียงหนึ่งปี แต่รับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกันเพิ่มระยะเวลา ๒ - ๓ ปี หรือสัญญาการบำรุงรักษาหลังการขายให้ทันก่อนระยะเวลาในการรับประกันจะสิ้นสุด

๖. ปัจจัยเสี่ยง

ปัจจัยเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ ต้องมีการระบุเหตุการณ์ที่จะเกิดขึ้นว่าเกิดขึ้นที่ไหน อย่างไร โดยระบุสาเหตุความเสี่ยงอาจที่เกิดขึ้นจริง เพื่อนำมาวิเคราะห์และกำหนดมาตรการลดความเสี่ยงที่อาจเกิดขึ้น ดังนี้

๖.๑ ปัจจัยภายนอก ได้แก่

๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่ายหลัก (Server) ระบบฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์ ได้แก่ ไฟไหม้ แผ่นดินไหว น้ำท่วม และ ภัยพิบัติอื่น ๆ

๒) การขโมยอุปกรณ์เครื่องข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓) การชำรุดเสียหายของเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากการเคลื่อนย้ายหรืออื่น ๆ

๔) การรับความเสี่ยงจากแนวนโยบายในการบริหารจัดการ อาจส่งผลกระทบต่อการดำเนินการด้านเทคโนโลยีสารสนเทศ

๕) ระบบเครือข่ายคอมพิวเตอร์หลักเสียหาย/ ขัดข้อง

๖) ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

๗) การชุมนุมประท้วงหรือความไม่สงบเรียบร้อยในบ้านเมือง

๖.๒ ปัจจัยภายใน ได้แก่

๑) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒) การถูกไวรัสคอมพิวเตอร์ (Virus Computer) ทำลายฐานข้อมูลและโปรแกรมปฏิบัติการ ต่างๆ

๓) การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลหรือระบบเครือข่ายคอมพิวเตอร์จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๖.๓ สาเหตุของปัจจัยเสี่ยง (Root Cause) หมายถึง สาเหตุที่เกี่ยวข้องกับปัจจัยเสี่ยงแยกแต่ละรายการปัจจัยเสี่ยง

๗. การประเมินความเสียหาย

๗.๑. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบ ได้แก่ ภัยธรรมชาติ เครื่องคอมพิวเตอร์แม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกไวรัสทำลายเสียหาย

๗.๒ ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ขัดข้อง หรือกระแสไฟฟ้าขัดข้อง

๘. การติดตามและรายงานผล

เพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม ดังนั้น ควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่อง และดำเนินการอย่างสม่ำเสมอ เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและแก้ไขเพื่อให้เกิดความถูกต้องและมีประสิทธิภาพ ดังนั้น จึงควรกำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบบ

๙. ระบบรักษาความปลอดภัยบนเครือข่ายหลักคอมพิวเตอร์ขององค์กร

ระบบเครือข่ายคอมพิวเตอร์ขององค์การตลาดเพื่อเกษตรกร ได้มีการพัฒนามาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบเครือข่ายขององค์กร เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยมีศูนย์คอมพิวเตอร์ตั้งอยู่ที่สำนักงานใหญ่ องค์การตลาดเพื่อเกษตรกร มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ในการกรอง (Filter Package) กลุ่มของข้อมูลจากเครือข่ายภายนอกที่ผ่านเข้ามาภายในระบบเครือข่ายคอมพิวเตอร์ส่วนกลาง นอกจากนี้ยังกำหนดมาตรการให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ที่ดูแลเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด รวมถึงการใช้โปรแกรมป้องกันไวรัส ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่อง ที่อยู่ในระบบเครือข่ายขององค์กร เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด

บทที่ ๔

การวิเคราะห์การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

การวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ต้องมีการวางระบบบริหารจัดการความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยดำเนินการ ดังนี้

๑) มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกัน หรือลดการเกิดความเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศ สำรอง และกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒) มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบสาวสนเทศ (IT Contingency Plan)

๓) มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์ เช่น ระบบ Antivirus, ระบบไฟฟ้าสำรอง เป็นต้น

๔) มีการกำหนดสิทธิ์ให้ผู้ใช้ในแต่ละระดับ (Access rights)

๑. แนวทางและขั้นตอนการบริหารความเสี่ยง

กระบวนการบริหารจัดการความเสี่ยงของหน่วยงาน เริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูลระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานในกิจกรรมนั้น ๆ ดังตารางการบริหารจัดการความเสี่ยงที่ได้จัดทำการวิเคราะห์ โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่าง ๆ ดังนี้

๑.๑ รายงานความเสี่ยงที่ได้ระบุไว้ เพื่อการประเมิน

๑.๒ ให้คะแนนความเป็นไปได้และผลกระทบของความเสี่ยง

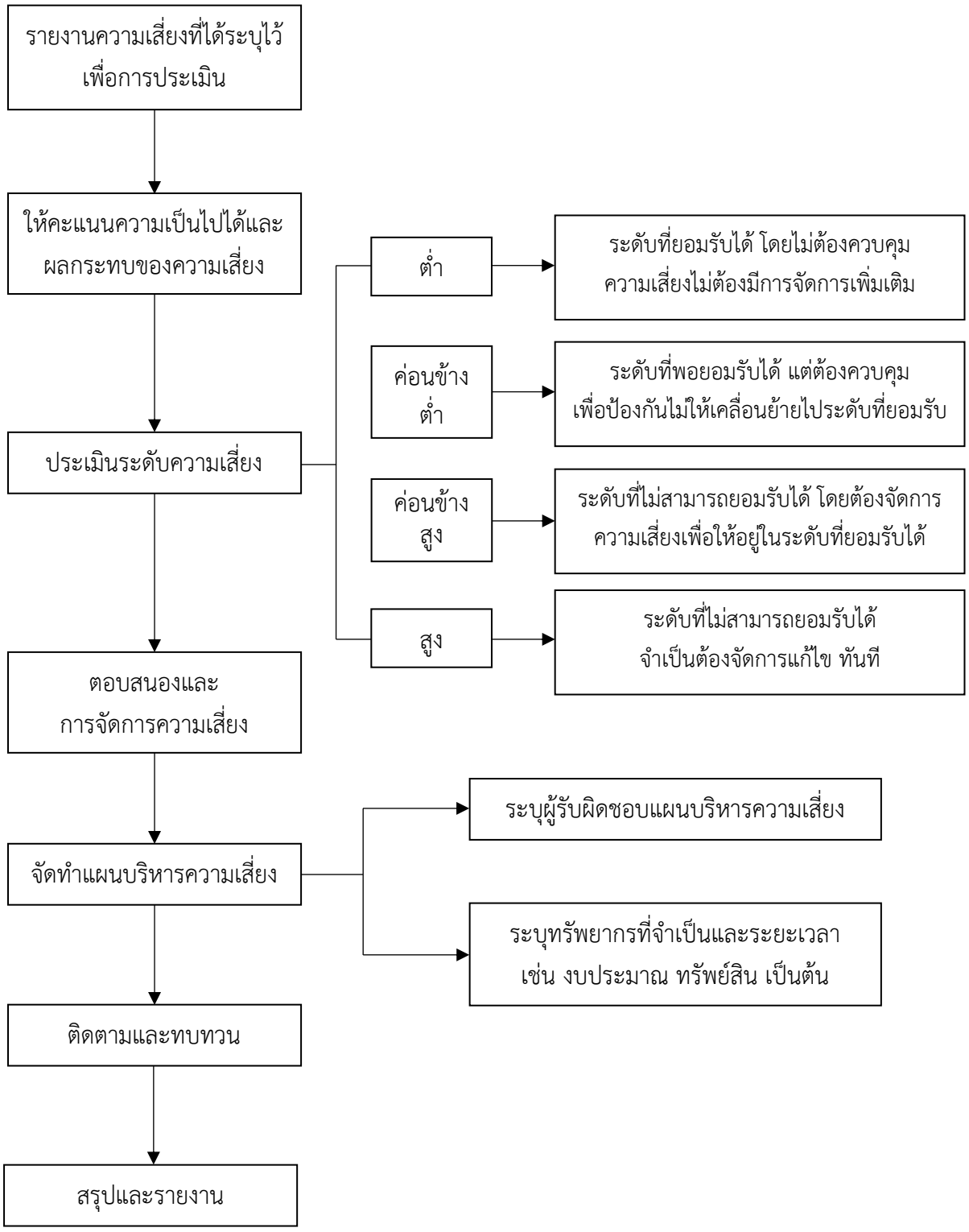
๑.๓ ประเมินระดับความเสี่ยง

๑.๔ ตอบสนองและจัดการความเสี่ยง

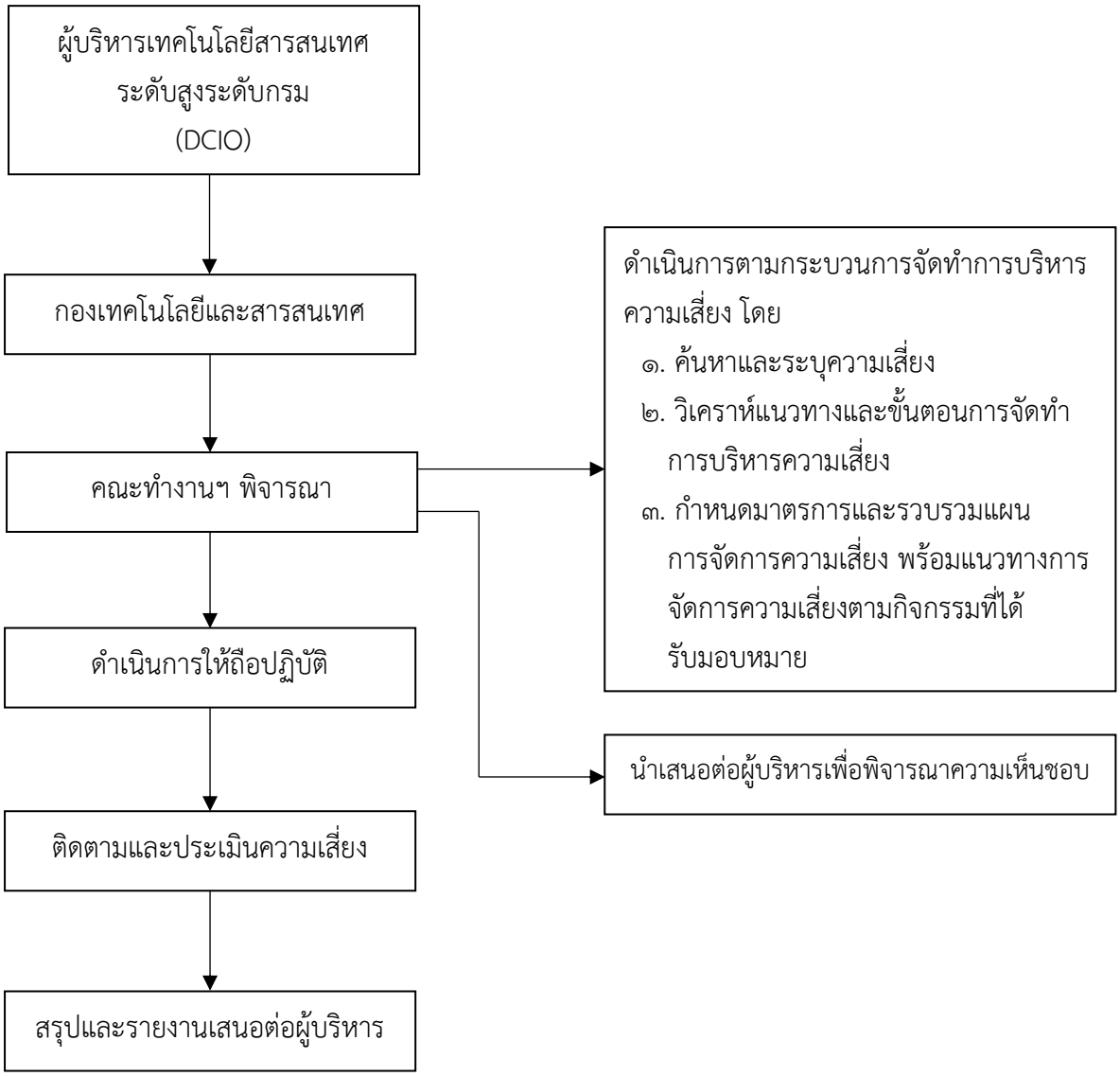
๑.๕ จัดทำแผนบริหารความเสี่ยง

๑.๖ ติดตามและทบทวน

๑.๗ สรุปและรายงานการบริหารความเสี่ยง


รายงานความเสี่ยงที่ได้ระบุไว้
เพื่อการประเมิน
ให้คะแนนความเป็นไปได้และ
ผลกระทบของความเสี่ยง
ประเมินระดับความเสี่ยง
ต่ำ
ระดับที่ยอมรับได้ โดยไม่ต้องควบคุม
ความเสี่ยงไม่ต้องมีการจัดการเพิ่มเติม
ค่อนข้าง
ต่ำ
ระดับที่พอยอมรับได้ แต่ต้องควบคุม
เพื่อป้องกันไม่ให้เคลื่อนย้ายไประดับที่ยอมรับ
ค่อนข้าง
สูง
ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการ
ความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้
สูง
ระดับที่ไม่สามารถยอมรับได้
จำเป็นต้องจัดการแก้ไข ทันที
ตอบสนองและ
การจัดการความเสี่ยง
จัดทำแผนบริหารความเสี่ยง
ระบุผู้รับผิดชอบแผนบริหารความเสี่ยง
ระบุทรัพยากรที่จำเป็นและระยะเวลา
เช่น งบประมาณ ทรัพย์สิน เป็นต้น
ติดตามและทบทวน
สรุปและรายงาน

๒. กระบวนการจัดทำการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ



๓. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดอัคคีภัย/วินาศภัย/อุทกภัย/การก่อการร้าย	อุปกรณ์เสียหาย/ถูกทำลายจากเหตุการณ์อัคคีภัย/วินาศภัย/การก่อการร้าย	O	- ไม่สามารถใช้งานข้อมูลและระบบงานได้เป็นปกติ - ข้อมูลสูญหาย - เสียงบประมาณในการจัดหาใหม่	๑ x ๕ = ๕ (ปานกลาง)	- จัดทำศูนย์สำรอง (Backup Site) - จัดทำ/ทบทวนแผนรองรับสถานการณ์ฉุกเฉิน และซักซ้อมสถานการณ์จำลองตามแผนฯ	ควบคุม	กส. (หลัก)
๒	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	ระบบกระแสไฟฟ้าขัดข้อง	- ไม่สามารถใช้งานเครื่องแม่ข่าย และเครือข่ายได้ - ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่าย อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ Shutdown อย่างเหมาะสม	O	- ข้อมูลเสียหาย - ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเสียหายต้องมีการติดตั้งใหม่	๓ x ๔ = ๑๒ (สูง)	- ตรวจสอบและจัดหาเครื่องสำรองไฟฟ้า (UPS) ที่รองรับระยะเวลาการใช้งานจนปิดระบบได้ปลอดภัย - ในจุดสำคัญที่ต้องใช้ระบบอย่างต่อเนื่องตลอดเวลาทำการ ต้องจัดหาเครื่องกำเนิดไฟฟ้า (Generator) ที่มีกำลังไฟฟ้าเพียงพอกับระยะเวลาใช้งาน	ควบคุม	กส. (หลัก)

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๓	ความเสี่ยงด้านบุคลากร	ความไม่รู้หรือไม่ชำนาญการใช้ระบบงาน	- บุคลากรตามกลุ่มเป้าหมายไม่เข้าอบรม/สัมมนา - การเปลี่ยนสายงานทำให้การใช้งานระบบไม่ต่อเนื่อง - ความไม่ตระหนักถึงการใช้ระบบอย่างไม่ถูกต้องหรือปลอดภัย	O	- บุคลากรไม่สามารถตอบสนองต่อการขับเคลื่อนการดำเนินงานได้ - ไม่ได้ปรับปรุงในระบบให้เป็นปัจจุบัน/ขาดความต่อเนื่องในการใช้งานระบบ - ถูกร้องเรียนจากบุคคลภายนอก - ติดไวรัสคอมพิวเตอร์	๓ x ๒ = ๖ (ปานกลาง)	- จัดหาหลักสูตรที่เหมาะสมกับบุคลากรแต่ละระดับ โดยจัดอบรมต่อเนื่องทุกปี โดยเฉพาะในหลักสูตรที่มีความสำคัญสูงและมีบุคลากรที่มีความรู้ในระบบนั้นๆ น้อย - จัดอบรมหรือถ่ายทอดความรู้ในหลักสูตร IT Security สำหรับพนักงานในทุกปี ๓. ติดตั้งระบบ Antivirus และตรวจสอบระบบเป็นประจำ	ควบคุม	กส. (หลัก) ทุกส่วนงาน (รอง)
๔	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	อุปกรณ์ขัดข้องหรือเสียหาย	- อุปกรณ์ชำรุดหรือเสื่อมสภาพตามอายุการใช้งาน	O	- ไม่สามารถใช้งานข้อมูลและระบบงานได้ - ข้อมูลสูญหาย - เสียงบประมาณในการจัดหาใหม่	๔ x ๓ = ๑๒ (สูง)	- เช็คความพร้อมของอุปกรณ์ระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย - ตรวจเช็คและสำรองข้อมูลระบบงานอย่างสม่ำเสมอ	ควบคุม/ถ่ายโอน	กส. (หลัก)

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
							- จัดหา Cloud Server ทดแทนเครื่องคอมพิวเตอร์แม่ข่ายที่หมดสภาพ - จัดหาอุปกรณ์ระบบ IT Security ทดแทน ในส่วนที่มีอายุใช้งานเกินกำหนด		
๕	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	ระบบคอมพิวเตอร์แม่ข่ายไม่สามารถให้บริการได้	- ต่ออายุการใช้งานระบบ Antivirus หรือระบบอื่นๆ ของ IT - การถูกบุกรุกระบบโดยผู้ไม่ประสงค์ดีจากภายนอกองค์กร - ถูกโปรแกรม Trojan โจมตีจากภายในองค์กรหรือจากผู้ใช้งานโดยไม่ตั้งใจ - ระบบงานที่ทำงานบนเครื่องคอมพิวเตอร์แม่ข่ายมีจุดอ่อนถูกเจาะระบบจากภายนอก	O	- การให้บริการระบบงานต่างๆ หยุดชะงัก ทำให้ไม่สามารถใช้ระบบงานที่ให้บริการบนเครือข่ายได้ - ข้อมูลอาจสูญหายหรือถูกทำลาย - ข้อมูลสำคัญหรือเป็นความลับในระบบฐานข้อมูลถูกขโมยหรือปลอมข้อมูล	๔ x ๓ = ๑๒ (สูง)	- ดำเนินการจัดซื้อจัดจ้างให้เป็นไปตามกรอบเวลา - ตรวจสอบการทำงานของระบบรักษาความปลอดภัยข้อมูลทางคอมพิวเตอร์ เช่น Firewall, Antivirus ให้สามารถทำงานได้เต็มประสิทธิภาพ - ตรวจเช็คและสำรองข้อมูลระบบงานอย่างสม่ำเสมอ	ควบคุม	กส. (หลัก)

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๖	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	การใช้โปรแกรมที่ไม่มีลิขสิทธิ์หรือใช้ไม่ถูกต้องตามลิขสิทธิ์	- ความไม่ตระหนักถึงผลเสียจากการใช้โปรแกรมผิดลิขสิทธิ์ของผู้ใช้งาน - หน่วยงานจำเป็นต้องใช้งานโปรแกรมโดยเร่งด่วนแต่ยังไม่ได้จัดซื้อ - ไม่มีงบประมาณเพียงพอในการจัดซื้อ	C	- ถูกฟ้องร้อง ทำให้เสื่อมเสียชื่อเสียงและค่าเสียหาย - ข้อมูลอาจสูญหายหรือถูกขโมยจากมัลแวร์ที่ติดมากับโปรแกรมที่ไม่มีลิขสิทธิ์	๒ x ๓ = ๖ (ปานกลาง)	- จัดหาโปรแกรมคอมพิวเตอร์ที่ถูกลิขสิทธิ์ ตามความจำเป็นและเหมาะสมในการใช้งาน - ให้ความรู้และรณรงค์ให้บุคลากรในองค์กรใช้โรแกรมคอมพิวเตอร์ที่มีลิขสิทธิ์หรือใช้โปรแกรม OpenSource ทดแทน	ควบคุม	กส. (หลัก) ทุกส่วนงาน (รอง)
๗	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) ขาดความต่อเนื่องในการดำเนินงาน	- ขาดงบประมาณในการจัดจ้างเพื่อดูแลระบบ - บุคลากรภายในองค์กรขาดความชำนาญในการดูแลระบบงาน	O	- การใช้ระบบเทคโนโลยีสารสนเทศไม่คุ้มค่าต่อการลงทุน	๓ x ๔ = ๑๒ (สูง)	- ต้องมีการถ่ายทอดความรู้ในการดูแลและแก้ไขปัญหาของระบบให้เจ้าหน้าที่ อ.ต.ก. ที่เกี่ยวข้อง - ต้องมีการส่งมอบเอกสารประกอบ Source Code ที่สามารถปรับปรุงแก้ไขได้ และ	ควบคุม	กส. (หลัก)

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
							หากพัฒนาระบบปรับปรุงเพิ่มเติม ต้องส่งเอกสารประกอบ Source Code ส่วนที่ปรับปรุงเพิ่มเติม		
๘	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	โปรแกรมมีข้อผิดพลาด/ไม่ตอบสนองต่อความต้องการในปัจจุบันขององค์กร	- ไม่มีงบประมาณในการดูแล/ปรับปรุง - การเปลี่ยนแปลงกระบวนการทำงานทำให้ความต้องการของผู้ใช้เปลี่ยนแปลง	S , O	- ผู้ใช้ไม่พึงพอใจในระบบงานจึงไม่ใช้งาน - การทำงานซ้ำซ้อน - ผู้บริหารไม่สามารถใช้ข้อมูลเพื่อบริหารและตัดสินใจได้	๑ x ๒ = ๒ (ต่ำ)	- จัดทำแผนงาน/โครงการในการบำรุงรักษาและปรับปรุงโปรแกรมคอมพิวเตอร์ที่มีความจำเป็นต้องปรับปรุง ทบทวนลงในแผนแม่บทฯ โดยจัดลำดับ Priority	ยอมรับ	กส. (หลัก)
๙	ความเสี่ยงด้านระบบข้อมูล	การรั่วไหลของข้อมูลในระบบคอมพิวเตอร์	- นำคอมพิวเตอร์ไปติดตั้งระบบปฏิบัติการใหม่กับบุคคลภายนอก - ผู้ดูแลระบบไม่ได้ยกเลิกสิทธิการใช้งานเนื่องจากไม่ทราบข้อมูล	O	- ข้อมูลอาจสูญหายหรือถูกทำลาย - ข้อมูลสำคัญหรือเป็นความลับในระบบฐานข้อมูลถูกขโมยหรือปลอมข้อมูล	๒ x ๓ = ๖ (ปานกลาง)	- ทบทวนและจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ และดำเนินงานตามแนวนโยบายและแนวปฏิบัติฯ โดยเคร่งครัด - ตรวจสอบการทำงานของระบบรักษาความปลอดภัยข้อมูลทางคอมพิวเตอร์ให้ทำงานเต็มประสิทธิภาพ	ควบคุม	กส. (หลัก)

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๐	ความเสี่ยงด้านระบบข้อมูล	การสำรองข้อมูลไม่อัพเดท/ขาดการสำรองข้อมูลระบบงาน	อุปกรณ์สำรองข้อมูลไม่ทำงานหรือการตั้งค่าระบบถูกรีเซ็ตโดยไม่ตั้งใจ	O	- ไม่ได้สำรองข้อมูลระบบงาน - สูญเสียข้อมูลหากเกิดปัญหาขึ้นกับระบบงาน	๓ x ๕ = ๑๕ (สูงมาก)	- ตรวจเช็คระบบสำรองข้อมูลอย่างสม่ำเสมอ พร้อมทดสอบการกู้คืนระบบ	ควบคุม	กส. (หลัก)
๑๑	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	ความชื้นอุณหภูมิในห้องคอมพิวเตอร์แม่ข่าย	ห้องคอมพิวเตอร์แม่ข่ายไม่มีระบบปรับอากาศที่สามารถความคุมอุณหภูมิความชื้นได้	O	อายุของเครื่องและอุปกรณ์สั้นลง	๔ x ๓ = ๑๒ (สูง)	- ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ - จัดหาระบบปรับอากาศชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้ - ติดตั้งตัวตรวจวัดอุณหภูมิ/ความชื้น ที่สามารถแจ้งเตือนกรณีที่มีความผิดปกติเกิดขึ้น	ยอมรับ	กส. (หลัก)
๑๒	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	- การถูกขโมยข้อมูล - โปรแกรมเสียหาย - การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Script ไว้เพื่อ	O , R	- ลดความน่าเชื่อถือหากข้อมูลถูกขโมยไปและนำไปเผยแพร่ - กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหาย	๒ x ๕ = ๑๐ (สูง)	- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top 10 Web Application Security Risks เพื่อลดความเสี่ยง	ควบคุม	กส. (หลัก) หรือ สำนัก/กอง/กลุ่ม ที่พัฒนาระบบงาน

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
			วัตถุประสงค์แอบแฝง		ต่อองค์กรเป็นอย่างยิ่ง		- มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ - ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่		ขึ้นใช้เอง (รอง)
๑๓	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง	- ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านเครือข่ายอินทราเน็ตได้ - ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่ายอินเทอร์เน็ตได้	O	- ขัดขวางการทำงานของเจ้าหน้าที่และผู้บริหารงานสำนักงานฯ - บุคคลภายนอกไม่สามารถเข้าใช้ Web Server หรือค้นหาข้อมูลที่ต้องการได้	๓ x ๕ = ๑๕ (สูงมาก)	- ตรวจสอบระบบเครือข่ายสื่อสารหลัก	ควบคุม	กส. (หลัก)
๑๔	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	การถูกบุกรุกโจมตีจากภายนอก	เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ตเนื่องจากไม่ทราบข้อมูล	O	- ทำให้ระบบเครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในครือข่าย - ถูกโจรกรรมข้อมูลที่เป็นความลับ	๓ x ๕ = ๑๕ (สูงมาก)	- ติดตั้งอุปกรณ์ป้องกันเครือข่าย - จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับ - ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย	ควบคุม	กส. (หลัก)

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๕	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	การติดไวรัสคอมพิวเตอร์หรือ Malware	- โปรแกรมหรือข้อมูลถูกทำลาย - ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ - การถูกขโมยข้อมูล	O	- ใช้คอมพิวเตอร์ไม่ได้ - ใช้ระบบงานไม่ได้ - ข้อมูลที่สำคัญสูญหาย	๒ x ๔ = ๘ (สูง)	- ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย - อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ	ควบคุม	กส. (หลัก)
๑๖	ความเสี่ยงด้านบุคลากร	การที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	- เสี่ยงต่อการใช้งานในทางที่ผิดหรือเปล่าประโยชน์ เช่น การฟังวิทยุหรือดูโทรทัศน์ ออนไลน์ เป็นต้น - การใช้ Resource ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์ หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	O	- สูญเสีย Bandwidth ในเครือข่ายทำให้ ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี - อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	๒ x ๓ = ๖ (ปานกลาง)	- กำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น - การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์หรือ Resources ต่างๆ ไปใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา	ควบคุม	กส. (หลัก) ทุกส่วนงาน (รอง)

ลำดับ	ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ประเภทความเสี่ยง (S/O/F/C/R)	ผลกระทบ	ระดับความเสี่ยง (Likelihood X Impact)	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑๗	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การที่แมลง หรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า/สายสัญญาณ	- เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	O	- เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน - ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	๑ x ๕ = ๕ (ปานกลาง)	- ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack - ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	ควบคุม	กส. (หลัก)
๑๘	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การโจรกรรมอุปกรณ์คอมพิวเตอร์ แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	- เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	O , R	- เสียงบประมาณในการจัดหาเครื่องแม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วงทดแทน - เสียเวลาในการกู้ระบบ - เสียภาพลักษณ์ของสำนักงานฯ	๑ x ๕ = ๕ (ปานกลาง)	- ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายและอาคารสำนักงานฯ - ตู้ Rack ที่ติดตั้งอุปกรณ์เครื่องแม่ข่ายและอุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจตลอดเวลา - ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ๆ มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	ควบคุม	กส. (หลัก)

๔. การจัดลำดับความสำคัญของความเสี่ยง

ในการพิจารณาเพื่อกำหนดกิจกรรมควบคุมในการบริหารความเสี่ยง จะพิจารณาจากการจัดลำดับตามความรุนแรงของความเสี่ยงที่ได้ประเมิน โดยเลือกจากความเสี่ยงที่มีระดับสูงมากหรือสูง ดังนี้

- หากอยู่ในโซนที่เกินระดับคะแนน (Impact x Likelihood) ๘ หรือระดับคะแนนเกิน ๘ ในโซนสีส้มและสีแดง จะต้องทำการบริหารหรือจัดการความเสี่ยง

- หากมีระดับคะแนน (Impact x Likelihood) ตั้งแต่ ๗.๙ คะแนนลงมา ปัจจัยเสี่ยงนั้นก็อยู่ในระดับที่ต้องทำการเฝ้าระวัง โดยไม่ต้องมีการบริหารความเสี่ยงก็ได้ แต่ต้องมีมาตรการในการควบคุมดูแลหรือเฝ้าระวังไม่ให้เกิดเหตุการณ์ความเสี่ยงขึ้น หรือลดทอนความสูญเสียลงได้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศ	ระดับ ความเสี่ยง	วิธีการจัดการ ความเสี่ยง
๑	การถูกบุกรุกโจมตีจากภายนอก	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	๑๕ (สูงมาก)	ควบคุม
๒	การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	๑๕ (สูงมาก)	ควบคุม
๓	การสำรองข้อมูลไม่อัพเดท/ขาดการสำรองข้อมูลระบบงาน	ความเสี่ยงด้านระบบข้อมูล	๑๕ (สูงมาก)	ควบคุม
๔	ระบบกระแสไฟฟ้าขัดข้อง	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	๑๒ (สูง)	ควบคุม
๕	โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) ขาดความต่อเนื่องในการดำเนินงาน	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	๑๒ (สูง)	ควบคุม
๖	อุปกรณ์ขัดข้องหรือเสียหาย	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	๑๒ (สูง)	ควบคุม
๗	ความชื้นอุณหภูมิในห้องคอมพิวเตอร์แม่ข่าย	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	๑๒ (สูง)	ควบคุม
๘	ระบบคอมพิวเตอร์แม่ข่ายไม่สามารถให้บริการได้	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	๑๒ (สูง)	ควบคุม
๙	ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	๑๐ (สูง)	ควบคุม
๑๐	การติดไวรัสคอมพิวเตอร์หรือ Malware	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	๘ (สูง)	ควบคุม
๑๑	การที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	ความเสี่ยงด้านบุคลากร	๖ (ปานกลาง)	ควบคุม

๑๒	การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ หรือใช้ไม่ถูกต้องตามลิขสิทธิ์	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	๖ (ปานกลาง)	ควบคุม
๑๓	ความไม่รู้หรือไม่ชำนาญในการใช้ระบบงาน	ความเสี่ยงด้านบุคลากร	๖ (ปานกลาง)	ควบคุม
๑๔	การรั่วไหลของข้อมูลในระบบคอมพิวเตอร์	ความเสี่ยงด้านระบบข้อมูล	๖ (ปานกลาง)	ควบคุม
๑๕	การที่แมลง หรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า/ สายสัญญาณ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	๕ (ปานกลาง)	ควบคุม
๑๖	การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	๕ (ปานกลาง)	ควบคุม
๑๗	การเกิดอัคคีภัย/ วินาศภัย/ อุทกภัย/ การก่อการร้าย	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	๕ (ปานกลาง)	ถ่ายโอน
๑๘	โปรแกรมมีข้อผิดพลาด/ไม่ตอบสนองต่อความต้องการในปัจจุบันขององค์กร	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	๒ (ต่ำ)	ยอมรับ

บทที่ ๕

สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมินดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่งเมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อน การดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้นในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกส่วนงานภายในองค์การตลาดเพื่อเกษตรกร ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายและถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือการจัดการความเสี่ยงในองค์กร นั่นเอง

๑. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนสูงสุด ๑๐ อันดับแรก ได้ข้อสรุป ดังนี้

๑) ความเสี่ยงจากการถูกบุกรุกโจมตีจากภายนอก มีแนวทางปฏิบัติดังนี้

- ติดตั้งอุปกรณ์ป้องกันการบุกรุกเครือข่าย (Firewall) เพื่อป้องกันและเตือนภัยคุกคาม
- ติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)
- จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับ
- ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย เป็นประจำ
- ดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันในทันที มิให้ความเสียหายแพร่กระจายในวงกว้าง

๒) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง มีแนวทางปฏิบัติดังนี้

- ตรวจสอบระบบเครือข่ายสื่อสารหลักทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา
- จัดให้มีระบบเครือข่ายสำรอง สำหรับใช้ในกรณีที่ระบบเครือข่ายหลักไม่สามารถใช้งานได้

๓) ความเสี่ยงการสำรองข้อมูลไม่อัพเดท/ขาดการสำรองข้อมูลระบบงาน มีแนวทางปฏิบัติดังนี้

- การบริหารจัดการในการทาการสารองข้อมูล (Backup) เป็นประจาอย่างสม่าเสมอ
- มีการทดสอบการนาข้อมูลกลับคืนสู่ระบบ (Restore)

๔) ระบบกระแสไฟฟ้าขัดข้อง มีแนวทางปฏิบัติดังนี้

- ตรวจสอบและจัดหาเครื่องสำรองไฟฟ้า (UPS) ที่รองรับระยะเวลาการใช้งานจนปิดระบบได้ปลอดภัย
- ในจุดสำคัญที่ต้องใช้ระบบอย่างต่อเนื่องตลอดเวลาทำการ ต้องจัดหาเครื่องกำเนิดไฟฟ้า (Generator) ที่มีกำลังไฟฟ้าเพียงพอกับระยะเวลาใช้งาน

๕) ความเสี่ยงจากโปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) ขาดความต่อเนื่องในการดำเนินงาน 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 Crash ของโปรแกรมหรือฐานข้อมูล(Database) เกิดความเสียหาย เป็นต้น

๖) ความเสี่ยงจากอุปกรณ์ขัดข้องหรือเสียหาย มีแนวทางปฏิบัติดังนี้

- ตรวจเช็คความพร้อมของอุปกรณ์ระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
- ตรวจเช็คและสำรองข้อมูลระบบงานอย่างสม่ำเสมอ

๗) ความเสี่ยงจากความชื้นอุณหภูมิในห้องคอมพิวเตอร์แม่ข่าย มีแนวทางปฏิบัติดังนี้

- ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ
- จัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้
- ติดตั้งตัวตรวจวัดอุณหภูมิ/ความชื้น ที่สามารถแจ้งเตือนกรณีที่มีความผิดปกติเกิดขึ้น

๘) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายไม่สามารถให้บริการได้ มีแนวทางปฏิบัติดังนี้

- ดำเนินการจัดซื้อจัดจ้างให้เป็นไปตามกรอบเวลา
- ตรวจสอบการทำงานของระบบรักษาความปลอดภัยข้อมูลทางคอมพิวเตอร์ เช่น Firewall, Antivirus ให้สามารถทำงานได้เต็มประสิทธิภาพ
- ตรวจเช็คและสำรองข้อมูลระบบงานอย่างสม่ำเสมอ

๙) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร มีแนวทางปฏิบัติดังนี้

- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top 10 Web Application Security Risks เพื่อลดความเสี่ยง
- มาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ
- ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่

๑๐) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware มีแนวทางปฏิบัติดังนี้

- ติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)
- อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ

๒. สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

๑) เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

๒) เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓) ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓. ข้อเสนอแนะ

๓.๑ การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้นโดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

๑) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

๒) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

๓) กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

๓.๒ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพ และมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ