ประกาศกรมป่าไม้

เรื่อง แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

แนวทางปฏิบัตินี้จัดทำขึ้นเพื่อกำหนดมาตรฐานและวิธีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ ให้หน่วยงานในสังกัดสามารถป้องกัน เฝ้าระวัง และลดผลกระทบจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลต่อระบบสารสนเทศ ข้อมูลสำคัญ และการดำเนินภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้เป็นไปอย่างเหมาะสม สอดคล้องกับมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งเป็นกรอบในการบริหารจัดการความมั่นคงปลอดภัยด้านไซเบอร์อย่างเป็นระบบ และอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม กรมป่าไม้จึงกำหนดแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ เพื่อให้หน่วยงานและบุคลากรในสังกัดถือปฏิบัติ กรมป่าไม้จึงประกาศไว้ ดังนี้

๑. ประกาศนี้เรียกว่า “แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้”

๒. การจัดทำแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้ มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อกำหนดแนวทางในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ให้เป็นระบบและมีมาตรฐานเดียวกัน

๒.๒ เพื่อใช้ในการระบุ วิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้นต่อระบบสารสนเทศ ทรัพย์สินสารสนเทศ และภารกิจสำคัญของหน่วยงาน

๒.๓ เพื่อกำหนดมาตรการควบคุม ป้องกัน และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ให้อยู่ในระดับที่ยอมรับได้

๒.๔ เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้สอดคล้องกับกฎหมาย มาตรฐาน รวมทั้งสร้างความเชื่อมั่นต่อผู้บริหาร บุคลากร และประชาชน

๓. เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการ ประเมิน วิเคราะห์ และควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานในสังกัด ให้เป็นไปในทิศทางเดียวกัน สอดคล้องกับกฎหมาย มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง

๔. ให้ใช้แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กรมป่าไม้ตามแนบท้ายประกาศนี้

๕. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๙

(นายนิกร ศิรโรจนานนท์)
อธิบดีกรมป่าไม้

แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

แนบท้ายประกาศกรมป่าไม้ ลงวันที่ พฤษภาคม พ.ศ. ๒๕๖๙

เรื่อง แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กรมป่าไม้

คำนำ

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งมีผลใช้บังคับ เพื่อกำหนดกรอบนโยบาย มาตรการ และกลไกในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจส่งผลกระทบต่อความมั่นคงของรัฐ การให้บริการสาธารณะ และประโยชน์สาธารณะโดยรวม ได้กำหนดให้หน่วยงานของรัฐต้องดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบและมีประสิทธิภาพ

ทั้งนี้ ตามมาตรา ๔๔ แห่งพระราชบัญญัติดังกล่าว กำหนดให้หน่วยงานของรัฐต้องจัดให้มีแนวทางหรือมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และตามมาตรา ๕๘ กำหนดให้หน่วยงานต้องดำเนินการประเมินความเสี่ยง จัดให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อย่างเหมาะสม รวมทั้งต้องมีการเฝ้าระวัง ตรวจสอบ และรายงานเหตุการณ์ที่เกี่ยวข้องต่อหน่วยงานกำกับดูแลที่เกี่ยวข้องโดยไม่ชักช้า

นอกจากนี้ ยังต้องถือปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมถึงหลักเกณฑ์ วิธีการ และมาตรฐานที่เกี่ยวข้อง เช่น กรอบแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) และแนวปฏิบัติในการจำแนกระดับความรุนแรงของภัยคุกคามทางไซเบอร์ ตลอดจนแนวทางการรายงานเหตุภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินงานมีความสอดคล้องกับข้อกำหนดทางกฎหมายและมาตรฐานสากล

ในการนี้ กรมป่าไม้จึงได้จัดทำแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ขึ้น เพื่อใช้เป็นกรอบในการระบุ วิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้นต่อระบบสารสนเทศ ทรัพย์สินสารสนเทศ และภารกิจสำคัญของหน่วยงาน รวมถึงกำหนดมาตรการควบคุมและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

แนวทางปฏิบัตินี้มุ่งหวังให้บุคลากรของกรมป่าไม้มีความเข้าใจและสามารถดำเนินการประเมินความเสี่ยงได้อย่างถูกต้อง เป็นระบบ และสอดคล้องตามกฎหมายและมาตรฐานที่เกี่ยวข้อง อันจะนำไปสู่การเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ และสนับสนุนการดำเนินภารกิจของกรมป่าไม้ให้เป็นไปอย่างมีประสิทธิภาพ โปร่งใส และเชื่อมั่นได้จากทุกภาคส่วน

พฤษภาคม ๒๕๖๙

สารบัญ

แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. บทนำ

๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ปัจจุบันเทคโนโลยีและระบบสารสนเทศ เป็นเครื่องมือสำคัญต่อการขับเคลื่อนองค์กร ให้มีความก้าวหน้าอย่างรวดเร็ว รวมทั้งการเปลี่ยนองค์กรเข้าสู่สังคมดิจิทัล (Transformation) และทำให้องค์กรต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่มากขึ้น การรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ จึงมีบทบาทที่สำคัญต่อองค์กรเป็นอย่างมาก การมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ที่มีความรัดกุมต่อระดับความเสี่ยง เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคาม ทางไซเบอร์รวมถึงการบริหารความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือเทคโนโลยีสารสนเทศ เพื่อสร้างความเชื่อมั่นต่อผู้บริหาร บุคลากรของกรมป่าไม้ และประชาชน

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) เป็นขั้นตอนที่สำคัญของการบริหารความเสี่ยง คือ การประเมินความเสี่ยงที่มีประสิทธิภาพ โดยผลที่ได้จากการประเมินความเสี่ยงเป็นข้อมูลพื้นฐานที่จะจัดลำดับความสำคัญเกี่ยวกับการรักษาความปลอดภัยไซเบอร์ โดยสิ่งที่มีความเสี่ยงสูงควรได้รับการจัดการหรือรักษาความเสี่ยงนั้นก่อน เนื่องจากองค์กรไม่สามารถจัดการได้กับทุกความเสี่ยงที่มีได้ เพราะข้อจำกัดด้านงบประมาณและทรัพยากรที่มี

ดังนั้น จึงมีความจำเป็นสำหรับหน่วยงานในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้อย่างมีประสิทธิภาพ ซึ่งเป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงระดับหน่วยงานของหน่วยงาน โดยการประเมินความเสี่ยง หน่วยงานจะสามารถ

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

๑.๒ ปัญหาโดยทั่วไป

ในขณะที่หน่วยงานต่าง ๆ ตระหนักดีว่าการประเมินความเสี่ยงเป็นส่วนสำคัญของแนวทางปฏิบัติในการประเมินความเสี่ยงของหน่วยงาน (Enterprise Risk Assessment Practice) แต่หน่วยงานหลายแห่งยังประสบปัญหากับกระบวนการในการประเมินความเสี่ยงที่เหมาะสม ช่องว่างทั่วไปบางส่วนที่สังเกต ได้แก่

๑.๒.๑ การระบุสถานการณ์ความเสี่ยงที่ไม่ดี (Poor Articulation of Risk Scenarios) สถานการณ์ความเสี่ยงที่อธิบายถึงเหตุการณ์ “สิ่งที่อาจผิดพลาดได้ (What Could Go Wrong)” มักจะคลุมเครือและเป็นเรื่องทั่วไป โดยไม่ได้ระบุเหตุการณ์ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมาที่เฉพาะเจาะจง เป็นผลให้การเข้าใจ

ขอบเขตของความเสี่ยง การเชื่อมโยงกับบริบทของหน่วยงาน หรือการระบุมาตรการเป้าหมายเพื่อจัดการกับความเสี่ยง กระทำได้ยาก

๑.๒.๒ การระบุความเสี่ยงโดยใช้วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบ (Identification of Risks Using a Compliance-Oriented Approach) หลายหน่วยงานระบุความเสี่ยงจากจุดที่ประเมินการควบคุมความมั่นคงปลอดภัย (หรือขาดไป) คล้ายกับการดำเนินการตรวจสอบการปฏิบัติตามหรือการวิเคราะห์ช่องว่างเทียบกับชุดของมาตรฐานที่กำหนดไว้ วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบเพื่อประเมินความเสี่ยงทำให้เกิดพฤติกรรม “รายการตรวจสอบ (Checklist)” ทำให้เกิดความเข้าใจผิดเกี่ยวกับความมั่นคงปลอดภัยว่าหน่วยงานจะไม่มีความเสี่ยงใด ๆ ตราบใดที่ปฏิบัติตามข้อกำหนดทั้งหมด

๑.๒.๓ การขาดการยอมรับความเสี่ยง (Absence of Risk Tolerance) หน่วยงานมักจะไม่บูรณาการแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เข้ากับโปรแกรมการจัดการความเสี่ยงของหน่วยงาน ด้วยเหตุนี้ การยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับหน่วยงานจึงมักถูกละเลย และผู้บริหารต้องเผชิญกับความยากลำบากในการตัดสินใจเลือกระดับความเสี่ยงที่เหมาะสมที่จะนำมาใช้ในขณะที่ดำเนินการตามวัตถุประสงค์ทางธุรกิจของหน่วยงาน

๑.๒.๔ การกำหนดโอกาสเสี่ยงตามเหตุการณ์ที่เกิดขึ้นในอดีตหรือที่คาดไว้ (Determining Risk Likelihood Based on Historical or Expected Occurrences) หน่วยงานต่าง ๆ มักจะใช้การวัดเวลาหรือความถี่ (เช่น เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดไว้) เพื่อประเมินโอกาสเสี่ยงของตน แนวทางนี้ อาจไม่ถูกต้องเมื่อพิจารณาจากจำนวนครั้งที่เหตุการณ์เกิดขึ้นก่อนหน้านี้ โดยเฉพาะอย่างยิ่งเมื่อไม่มีข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมา ในบริบทของความมั่นคงปลอดภัยไซเบอร์ ความน่าจะเป็นของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์นั้นไม่ขึ้นกับความถี่ของการเกิดขึ้นในอดีต

๑.๒.๕ จัดการกับความเสี่ยงด้วยการควบคุมหรือมาตรการที่ไม่เกี่ยวข้อง (Treating Risks With Irrelevant Controls/Measures) หน่วยงานอาจใช้แนวทางกว้าง ๆ ในการหามาตรการเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุ ซึ่งส่งผลให้การดำเนินการควบคุมนั้นไม่ได้ระบุถึงสาเหตุที่แท้จริงอย่างสมบูรณ์ ซึ่งมักเกิดจากความเข้าใจหรือการอธิบายสถานการณ์ความเสี่ยงที่ไม่ดีพอ

๒. วัตถุประสงค์ กลุ่มเป้าหมาย และขอบเขต

๒.๑ วัตถุประสงค์

เพื่อให้คำแนะนำแก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หน่วยงาน) เกี่ยวกับวิธีดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

๒.๒ กลุ่มเป้าหมายและขอบเขต

เพื่อใช้โดยผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ต่อไปนี้

๒.๒.๑ ผู้มีส่วนได้ส่วนเสีย (Stakeholders) เช่น หัวหน้าหน่วยธุรกิจ เจ้าของระบบ หัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ ฯลฯ ภายในหน่วยงาน

๒.๒.๒ ที่ปรึกษาภายนอกหรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของหน่วยงาน

๒.๒.๓ ขอบเขตของแนวทางฉบับนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความเสี่ยง อยู่นอกเหนือขอบเขตของแนวทางฉบับนี้

๓. สร้างบริบทความเสี่ยง

การกำหนดบริบทของความเสี่ยงเป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับการประเมินความเสี่ยง ขั้นตอนนี้ทำให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมิน ความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

๓.๑ กำหนดความเสี่ยง

เป็นการระบุรายการความเสี่ยง ที่อาจเกิดขึ้นได้ทุกกรณีและสามารถเป็นต้นเหตุของการเกิดความเสียหาย ความล้มเหลว รวมถึงการลดโอกาสที่จะบรรลุความสำเร็จตามเป้าหมายของการปฏิบัติงาน หรือกิจกรรม โดยความเสี่ยงถูกกำหนดให้เป็นผลลัพธ์ของ ๒ ปัจจัย คือ

- ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน
- ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (Likelihood, Impact)

ปัจจัยเสี่ยงแต่ละประการที่กล่าวถึงในคำจำกัดความได้อธิบายไว้ด้านล่าง

๓.๑.๑ เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง สิ่งที่เกิดจากการที่ผู้โจมตีทำอันตรายต่อองค์กร เช่น แฮคเกอร์อาจทำอันตรายโดยการแก้ไขหน้าเว็บไซต์ขององค์กร เช่น การใช้บัญชีผู้ใช้ในทางที่ผิดหรือเกินกว่าที่ได้รับอนุญาต การแก้ไขข้อมูลที่สำคัญทั้งที่ตั้งใจและที่ไม่ได้ตั้งใจ การเจาะเข้าระบบโดยไม่ได้รับอนุญาต การทำลายระบบโดยไม่ได้ตั้งใจ การรบกวนระบบสื่อสารข้อมูลทั้งภายในและภายนอก และการบุกรุกเข้าห้องควบคุมโดยไม่ได้รับอนุญาต เป็นต้น

๓.๑.๒ ช่องโหว่ (Vulnerability)

ช่องโหว่ขององค์กรแบ่งออกเป็นประเภทต่างๆ ดังนี้

๑) ช่องโหว่ทางนโยบาย เป็นช่องโหว่ที่เกิดจากการบริหารจัดการ ซึ่งส่วนใหญ่เกิดจากการขาดกฎ ระเบียบ หรือกฎหมายที่บังคับ หรือห้ามการกระทำอย่างใดอย่างหนึ่ง

๒) ช่องโหว่จากการปฏิบัติงาน เป็นช่องโหว่ที่ที่อาจเกิดขึ้นจากการดำเนินการ จัดการความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบ สารสนเทศหรือใช้ข้อมูลต่าง ๆ ของสำนักงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิด ความเสียหายต่อข้อมูลสารสนเทศได้

๓) ช่องโหว่ทางเทคนิค เป็นช่องโหว่ที่เกิดจากข้อผิดพลาดของการเขียนโปรแกรม หรือการกำหนดค่าคอนฟิกที่ไม่สมบูรณ์หรือปลอดภัย

๔) ช่องโหว่ทางกายภาพ เป็นช่องโหว่ที่เกิดจากการป้องกันและรักษาความปลอดภัยทางกายภาพ เช่น การควบคุมการเข้าออกสถานที่ การล็อกประตูหน้าต่าง เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่มีอายุการใช้งานมานาน และยังไม่มีการจัดซื้อเครื่องใหม่มาทดแทน อาจทำให้เกิดความเสียหายต่อการทำงานได้ เช่น Hard Disk เสีย จะทำให้ข้อมูลสูญหายได้ เป็นต้น

๕) ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓.๑.๓ ความน่าจะเป็น (Likelihood)

ความน่าจะเป็น หมายถึง ความน่าจะเป็นที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ สามารถใช้ประโยชน์จากช่องโหว่ที่กำหนด (หรือชุดของช่องโหว่) ความน่าจะเป็นสามารถได้รับจากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ (Reproducibility)

๓.๑.๔ ผลกระทบ (Impact)

ผลกระทบหมายถึงขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

๓.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตารางการยอมรับความเสี่ยง

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
น้อยมาก	เกิดเหตุไม่มีความสำคัญ
น้อย	เกิดเหตุเล็กน้อยที่แก้ไขได้
ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลกรมป่าไม้

๓.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในแบบฝึกหัดการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในแบบฝึกหัดการประเมินความเสี่ยง ได้แก่

๓.๑.๓ หัวหน้าหน่วยงาน (Head of Organization)

ผู้บริหารระดับสูงสุดของกรมป่าไม้ (Chief Executive Office : CEO) มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของหน่วยงาน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

๓.๒.๓ เจ้าของกระบวนการธุรกิจ (Business Owner)

สำนัก/กอง/ศูนย์/กลุ่ม ที่เป็นเจ้าของข้อมูลในระบบสารสนเทศ กรมป่าไม้ ที่รับผิดชอบในการตรวจสอบ

๓.๓.๓ ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)

สำนัก/กอง/ศูนย์/กลุ่ม / สำนักจัดการทรัพยากรป่าไม้ที่ ๑ – ๑๓ และสำนักจัดการทรัพยากรป่าไม้สาขาทุกสาขา

๓.๔.๓ ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

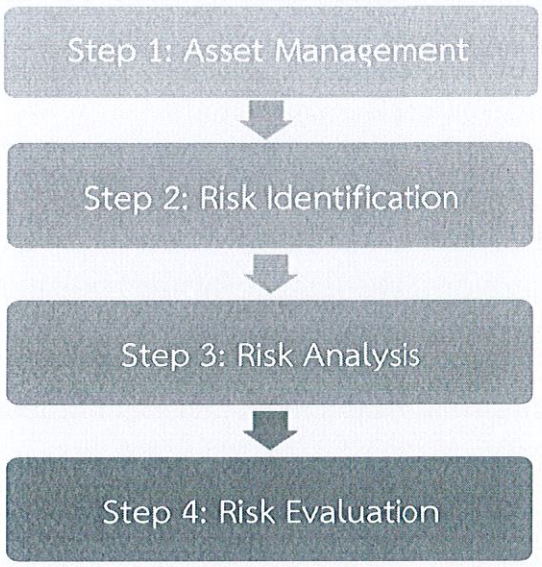
ส่วนระบบคอมพิวเตอร์และเครือข่าย และส่วนระบบสารสนเทศและภูมิสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๕.๓ ฟังก์ชั่นความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

มีขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ ๑) การจัดการทรัพย์สิน (Asset Management) ๒) การระบุความเสี่ยง (Risk Identification) ๓) การวิเคราะห์ความเสี่ยง (Risk Analysis) และ ๔) การประเมินความเสี่ยง (Risk Evaluation)



รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๔.๑ การจัดการทรัพย์สิน (Asset Management)

ทะเบียนทรัพย์สินประเภทฮาร์ดแวร์ (Network Device/Physical security)

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๑	HW-๐๐๑	อุปกรณ์ค้นหาเส้นทาง Router	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Router	ห้อง Data Center
๒	HW-๐๐๒	อุปกรณ์กระจายสัญญาณย่อย (Switch External)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	ห้อง Data Center
๓	HW-๐๐๓	อุปกรณ์ป้องกันเครือข่าย (Firewall)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Firewall	ห้อง Data Center
๔	HW-๐๐๔	อุปกรณ์กระจายสัญญาณหลัก (Core Switch)	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	ห้อง Data Center
๕	HW-๐๐๕	อุปกรณ์ควบคุมอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless Controller)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Wireless Controller	ห้อง Data Center
๖	HW-๐๐๖	อุปกรณ์แจกหมายเลข IP และ DNS	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	DNS Server	ห้อง Data Center
๗	HW-๐๐๗	อุปกรณ์บันทึกภาพแบบไอพี (Network Video Recorder)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Network Video Recorder	ห้อง Data Center
๘	HW-๐๐๘	อุปกรณ์กระจายสัญญาณย่อย (DMZ Switch)	๔	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	ห้อง Data Center
๙	HW-๐๐๙	เครื่องสแกนลายนิ้วมือ (Finger Scan)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Finger Scan	ห้อง Data Center
๑๐	HW-๐๑๐	เครื่องสำรองไฟฟ้า ขนาด ๒๐ kVA	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	UPS	ห้อง Data Center

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๑๑	HW-๐๑๑	เครื่องสำรองไฟฟ้า ขนาด ๑๕ KVA	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	UPS	ห้อง Data Center
๑๒	HW-๐๑๒	เครื่องสำรองไฟฟ้า ขนาด ๑ KVA	๑๙	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	UPS	ห้อง Data Center
๑๓	HW-๐๑๓	เครื่องปรับอากาศควบคุมอุณหภูมิและความชื้น	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Air	ห้อง Data Center
๑๔	HW-๐๑๔	เครื่องตรวจจับควันความไวสูง	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Smoke Detector	ห้อง Data Center
๑๕	HW-๐๑๕	เครื่องตรวจจับน้ำรั่วซึม	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Water Leak	ห้อง Data Center
๑๖	HW-๐๑๖	เครื่องเฝ้าดูและแจ้งเตือนอัตโนมัติ (SMS Server)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	SMS Server	ห้อง Data Center
๑๗	HW-๐๑๗	เครื่องวัดอุณหภูมิห้องปฏิบัติการคอมพิวเตอร์ (Data Center)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Room Temperature	ห้อง Data Center
๑๘	HW-๐๑๘	อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point)	๘๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Access Point	อาคารภายในกรมป่าไม้
๑๙	HW-๐๑๙	อุปกรณ์กระจายสัญญาณอาคาร (Core Switch BL)	๓	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	อาคารภายในกรมป่าไม้
๒๐	HW-๐๑๙	อุปกรณ์กระจายสัญญาณ (Access Switch)	๓๐	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	อาคารภายในกรมป่าไม้
๒๑	HW-๐๒๐	กล้องโทรทัศน์วงจรปิดแบบไอพี (IP Camera)	๑๐	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	IP Camera	อาคารเทียมคมกฤส

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๒๒	HW-๐๒๑	เครื่องกำเหนิดไฟฟ้า (Generator)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Generator	บริเวณด้านหน้า กองการอนุญาต
๒๓	HW-๐๒๒	เครื่องควบคุมการสลับสัญญาณไฟฟ้า (ATS)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	ATS	อาคารเทียมคมกฤส

ทะเบียนทรัพย์สินประเภทฮาร์ดแวร์ (Server/Storage/Backup)

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๑	SV-๐๐๑	HP ProLiant DL๓๘๐G๗	๕	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๒	SV-๐๐๒	HP ProLiant DL๓๘๐ G๙	๔	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๓	SV-๐๐๓	Storage HP MSA ๒๐๔๐	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Storage	ห้อง Data Center
๔	SV-๐๐๔	HP ProLiant BL๖๖๐c Gen๘	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๕	SV-๐๐๕	HP ProLiant BL๖๖๐๐c Gen๙	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๖	SV-๐๐๖	Storage HP	๑๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Storage	ห้อง Data Center
๗	SV-๐๐๗	HP ProLiant DL ๑๒๐ G๕	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๘	SV-๐๐๘	Acer R๗๒๐ M๒	๓	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๙	SV-๐๐๙	IBM ๕๒๐	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๑๐	SV-๐๑๒	HP BL ๖๘๐ G๕	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๑๑	SV-๐๑๑	HP BL ๔๖๐c G๖	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๑๒	SV-๐๑๒	BL ๖๘๐ G๗	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center

ทะเบียนทรัพย์สินประเภทข้อมูล (Data)

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อข้อมูล/สารสนเทศ	รายละเอียดข้อมูล/สารสนเทศ	ระดับชั้นความลับ	สื่อบันทึก/สถานที่จัดเก็บ	ผู้รับผิดชอบ	กลุ่มทรัพย์สิน
๑	INFO-๐๐๑	Source Code	โค้ดของระบบ	Confidential	Backup Server /ห้อง Data Center	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Source Code
๒	INFO-๐๐๒	Data Backup	ข้อมูลสำรองระบบสารสนเทศ	Confidential	ห้อง Data Center	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Data Backup
๓	INFO-๐๐๓	Network Log File	ข้อมูลกิจกรรมต่างๆภายในระบบ	Confidential	SAN Server และ Backup Server /ห้อง Data Center	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Network Log File
๔	INFO-๐๐๔	Network Diagram	ข้อมูลภาพโครงสร้างพื้นฐานระบบเครือข่าย	Confidential	PC Admin /ห้องศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Network Diagram

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อข้อมูล/สารสนเทศ	รายละเอียดข้อมูล/สารสนเทศ	ระดับชั้นความลับ	สื่อบันทึก/สถานที่จัดเก็บ	ผู้รับผิดชอบ	กลุ่มทรัพย์สิน
๕	INFO-๐๐๕	Network Configuration	ข้อมูล Config Network	Confidential	File Server /ห้อง Data Center	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Network Configuration

ทะเบียนทรัพย์สินระบบสารสนเทศและฐานข้อมูล (Web Application/Database)

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อระบบสารสนเทศ	ผู้รับผิดชอบ	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๑	App-๐๐๑	ระบบข้อมูลสารสนเทศทรัพยากรบุคคลระดับกรม	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๒	App-๐๐๒	ระบบบุคลากร เงินเดือน และสวัสดิการ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๓	App-๐๐๓	ระบบงานบุคคลของพนักงานราชการ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๔	App-๐๐๔	ระบบสารบรรณอิเล็กทรอนิกส์ กรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๕	App-๐๐๕	ระบบติดตามการบุกรุกทำลายป่า	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๖	App-๐๐๖	ระบบเว็บไซต์กรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๗	App-๐๐๗	ระบบอีเมล์กรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๘	App-๐๐๘	ระบบ National Single Window (NSW)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อระบบสารสนเทศ	ผู้รับผิดชอบ	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๙	App-๐๐๙	ระบบฐานข้อมูลความหลากหลายทางชีวภาพ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๐	App-๐๑๐	ระบบสวนป่าออนไลน์	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๑	App-๐๑๑	ระบบแจกจ่ายกล้าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๒	App-๐๑๒	ระบบอนุญาตอุตสาหกรรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๓	App-๐๑๓	ระบบแผนงาน งบประมาณ และติดตามประเมินผล	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๔	App-๐๑๔	ระบบฐานข้อมูลเชิงแผนที่ของกรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๕	App-๐๑๕	ระบบคอมพิวเตอร์เสมือน	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๖	App-๐๑๖	ระบบด่านป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๗	App-๐๑๗	ระบบขอตรวจพิสูจน์ไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๘	App-๐๑๘	ระบบพิทักษ์ไพร	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๙	App-๐๑๘	Mobile Application Forest๔ Thai	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Mobile App
๒๐	App-๐๒๐	ระบบภูมิสารสนเทศเพื่อการบริหารกรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App

๔.๒ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

งาน A: การระบุความเสี่ยง (Risk Identification)

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูล โดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่
๒. เว็บไซต์ และเว็บแอพพลิเคชั่น ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์ หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) - การอัพโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ขาดการอัพเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟแวร์ถูกลิขสิทธิ์
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive, Handy Drive - มีการเข้าใช้งานเครือข่ายอินเทอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม
		เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download Fileขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด
๖. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัพเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ระบบฐานข้อมูล - ระบบสารสนเทศ	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall
๗. ความเสี่ยงต่อระบบ	ความเสี่ยงด้าน	- การตั้งค่าอุปกรณ์ผิดพลาด	- ผู้ใช้งาน	- จัดหาอุปกรณ์สำรองเพื่อให้

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม
สำรองข้อมูลไม่สามารถกู้คืนระบบได้	เทคนิค	- อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ

● ทรัพย์สินสำคัญ (Crown Jewels) - ทรัพย์สินเหล่านี้มีความสำคัญต่อการบรรลุวัตถุประสงค์การดำเนินงานของกรมป่าไม้โดยรวม และมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์

ลำดับ	ชื่อระบบสารสนเทศ/อุปกรณ์	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๑	ระบบเว็บไซต์กรมป่าไม้	SAN Server /ห้อง Data Center	Web App
๒	ระบบ National Single Window (NSW)	SAN Server /ห้อง Data Center	Web App
๓	ระบบบุคลากร เงินเดือน และสวัสดิการ	SAN Server /ห้อง Data Center	Web App
๔	ระบบงานบุคคลของพนักงานราชการ	SAN Server /ห้อง Data Center	Web App
๕	ระบบภูมิสารสนเทศเพื่อการบริหารกรมป่าไม้	SAN Server /ห้อง Data Center	Web App
๖	อุปกรณ์ป้องกันเครือข่าย (Firewall)	ห้อง Data Center	Firewall
๗	อุปกรณ์กระจายสัญญาณหลัก (Core Switch)	ห้อง Data Center	Switch
๘	อุปกรณ์กระจายสัญญาณย่อย (DMZ Switch)	ห้อง Data Center	Switch
๙	อุปกรณ์ Info box อุปกรณ์แจกหมายเลข IP และ DNS	ห้อง Data Center	DNS
๑๐	อุปกรณ์ค้นหาเส้นทาง Router	ห้อง Data Center	Router

● ทรัพย์สินที่เกี่ยวข้อง (Stepping Stones) - ทรัพย์สินเหล่านี้เป็นทรัพยากรที่ผู้โจมตีต้องการควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ

ลำดับ	ชื่อระบบสารสนเทศ/อุปกรณ์	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๑	ระบบจัดเก็บบัญชีรายชื่อผู้ใช้งาน (AD)	ห้อง Data Center	Server
๒	ระบบสวนป่าออนไลน์	SAN Server /ห้อง Data Center	Web App
๓	ระบบแจกจ่ายกล้าไม้	SAN Server /ห้อง Data Center	Web App
๔	ระบบอนุญาตอุตสาหกรรมป่าไม้	SAN Server /ห้อง Data Center	Web App
๕	ระบบฐานข้อมูล	SAN Server /ห้อง Data Center	Data Base
๖	ระบบ FP	SAN Server /ห้อง Data Center	Web App

งาน B: การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)

เป็นกระบวนการจำลองเหตุภัยคุกคามที่อาจเกิดขึ้น เช่น ช่องโหว่เชิงโครงสร้าง เพื่อวิเคราะห์อย่างเป็นระบบเกี่ยวกับรูปแบบของการโจมตี เพื่อคาดการณ์รูปแบบการโจมตีที่เป็นไปได้ให้มากที่สุดและสินทรัพย์ที่ผู้โจมตีต้องการมากที่สุด โดยการสร้างแบบจำลองภัยคุกคามสามารถอธิบายถึง สินทรัพย์ที่มีมูลค่าสูงอยู่ที่ไหนในระบบ จุดที่เสี่ยงที่สุดในการถูกโจมตีคืออะไร ภัยคุกคามที่เป็นไปได้มากที่สุดคืออะไร และ มีรูปแบบการโจมตีอื่นอีกหรือไม่ที่ยังนึกไม่ถึง โดยทั่วไปแล้วมีการสร้างแบบจำลองภัยคุกคามบางรูปแบบในชีวิตประจำวันโดยไม่รู้ตัว บางคนใช้แบบจำลองภัยคุกคามในระหว่างการขับรถไปทำงานตอนเช้าเพื่อหลีกเลี่ยงอุบัติเหตุที่อาจเกิดขึ้น เป็นต้น โดยการสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้

๑. การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition) – สิ่งเหล่านี้เป็นข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคามที่แนะนำในงาน A

๒. การระบุภัยคุกคาม (Threat Identification) – หน่วยงานควรใช้แนวทางที่เป็นระบบเพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

๓. การสร้างแบบจำลองการโจมตี (Attack Modelling) – หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว หน่วยงานควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้หน่วยงานสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

งาน C: สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)

การสร้างสถานการณ์ความเสี่ยงเป็นงานสุดท้ายในการดำเนินการขั้นตอนการระบุความเสี่ยงให้เสร็จสมบูรณ์ งานนี้มีเป้าหมายเพื่อสร้างสถานการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ที่ให้มุมมองที่สมจริงและสัมพันธ์กันของความเสี่ยงตามบริบททางธุรกิจ สภาพแวดล้อมของระบบ และภัยคุกคามที่เกี่ยวข้อง

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป สถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก ๔ ประการ ต่อไปนี้:

- **ทรัพย์สิน (Asset)** - สิ่งที่มีค่าที่ได้รับการระบุในงาน A
- **เหตุการณ์ภัยคุกคาม (Threat Event)** - เหตุการณ์การโจมตีที่ระบุในงาน B
- **ช่องโหว่ (Vulnerability)** - จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง
- **ผลที่ตามมา (Consequence)** – ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

ตัวอย่างของสถานการณ์ความเสี่ยงที่สร้างมาอย่างดีแสดงไว้ด้านล่าง

Legend: Threat Event | Vulnerability | Asset | Consequence

ผู้โจมตีทำการแทรก SQL บนเว็บแอปพลิเคชันเดิมที่ไม่ได้แพตช์เพื่อดาวน์โหลดเวชระเบียนผู้ป่วยที่มีความอ่อนไหว

Attacker Performs an SQL Injection on an Unpatched Legacy Web Application to Download Sensitive Patient Medical Records.

รูปที่ ๑ เหตุการณ์ความเสี่ยง (Risk Scenario)

พนักงานภายในทำการหลอกลวงให้ชำระเงินเกินยอดเงินในบัญชีธนาคารในระบบการชำระเงินโดยไม่มีกำหนด ส่งผลให้เกิดการเบิกเกินบัญชีธนาคาร

Internal Staff Makes a Fraudulent Payment Instruction Exceeding Bank Account Balance On The Payment System With No Set Limit, Resulting in a Bank Overdraft.

รูปที่ ๒ เหตุการณ์ความเสี่ยง

พนักงานที่ไม่ได้รับอนุญาตเข้าถึงเซิร์ฟเวอร์ SCADA โดยใช้ข้อมูลรับรองการเข้าสู่ระบบเริ่มต้นและดำเนินการคำสั่งปิดระบบเพื่อรบกวนการจ่ายน้ำไปยังฝั่งตะวันออกของกรุงเทพมหานครทั้งหมด

Unauthorised Employee Accesses The SCADA Server Using Default login Credentials and Execute Shutdown Command To Disrupt The Water Supply To The Entire East Side Of Bangkok.

รูปที่ ๓ เหตุการณ์ความเสี่ยง

ผู้โจมตีส่งอีเมลฟิชชิ่งแบบเจาะจงกลุ่มเป้าหมายไปยังผู้ใช้ที่ไม่สงสัย ซึ่งเมื่อคลิกแล้ว จะทำให้บัญชีผู้ใช้ดำเนินการตรวจสอบสิทธิ์ SMB กับเซิร์ฟเวอร์ที่เป็นอันตรายและเปิดเผยข้อมูลประจำตัวที่แฮชไว้

Attacker Delivers Spear-Ohishing Email To Unsuspecting User, Which When Clicked, Triggers The User Account To Perform SMB Authentication With Malicious Server and Discloses Hashed Credentials.

รูปที่ ๔ เหตุการณ์ความเสี่ยง

๔.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

(๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น และ

(๒) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

งาน A: กำหนดโอกาส (Determine Likelihood)

เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าวเพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัตของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าจะไม่ถูกบุกรุกในอนาคตตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับ การประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้

- **ความสามารถในการค้นพบ (Discoverability)** – ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่

- **ความสามารถในการใช้ประโยชน์ (Exploitability)** – ฝ่ายตรงข้ามจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี

- **ความสามารถในการทำซ้ำ (Reproducibility)** – ฝ่ายตรงข้ามจะสามารถสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

ภาพด้านล่าง คือตารางการประเมินตัวอย่างเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำตามขั้นตอนต่อไปนี้เพื่อให้ได้รับคะแนนความเป็นไปได้ของสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(i) ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น ๓ ระดับ (เช่น ๑ – ๓)

(ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

(iii) คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสี่ยง โดยระดับ ๓ คือ “มีแนวโน้มสูง” และ ๑ คือ “เป็นไปได้ยาก”

ตารางประเมินความเสี่ยงที่อาจเกิดขึ้น

Likelihood Rating	Discoverability	Exploitability	Reproducibility
High (๓)	ช่องโหว่ของเป้าหมาย: • สามารถค้นพบได้โดยการค้นหา/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, ExploitDB) • สามารถถูกค้นพบและถูกโจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	การโจมตี: • สามารถดำเนินการได้โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย • สามารถทำได้ด้วยเครื่องมือที่หาได้ทั่วไป โดยไม่ต้องมีความรู้ด้านเทคนิค	การโจมตี: • สามารถทำซ้ำได้ตามต้องการโดยไม่มีการกำหนดค่า (Configuration) หรือเงื่อนไขของเหตุการณ์ (Event Condition) • สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่
Medium (๒)	ช่องโหว่ของเป้าหมาย: • สามารถค้นพบได้โดยการตรวจสอบการตอบสนองพฤติกรรม และการสื่อสารของเป้าหมาย (เช่น การฟัซ (Fuzzing) กับแพ็กเก็ตเครือข่าย การดักจับเครือข่าย (Network Sniffing) • สามารถถูกค้นพบและโจมตีจากภายในเครือข่ายย่อยหรือส่วนเครือข่ายเดียวกัน	การโจมตี: • สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) ของเป้าหมาย (เช่น Admin/SYSTEM/ Root) • สามารถดำเนินการได้ด้วยเครื่องมือที่เปิดเผยต่อสาธารณะ ซึ่งต้องใช้ความรู้ด้านเทคนิคในระดับกลาง	การโจมตี: • สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์ที่คาดเดาได้บางอย่าง • สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย
Low (๑)	ช่องโหว่ของเป้าหมาย: • สามารถค้นพบได้โดยการดำเนินการและโต้ตอบกับการตั้งค่าปัจจุบันหรือที่คล้ายกันของเป้าหมาย	การโจมตี: • สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin / SYSTEM / Root)	การโจมตี: • สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุ่มบางอย่าง

Likelihood Rating	Discoverability	Exploitability	Reproducibility
	• สามารถถูกค้นพบและโจมตีด้วยการเข้าถึงแบบลอจิคัลโลคัล	• สามารถดำเนินการได้ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะ ซึ่งต้องการความรู้ด้านเทคนิคขั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน	• สามารถทำซ้ำได้ในทางทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่

รายงานการประเมินความเสี่ยง

โดยวิเคราะห์จากปัจจัยความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น ให้คะแนนตามระดับ ๑ ถึง ๓ (๑ เป็น “เป็นไปได้ยาก” ๒ “ปานกลาง” และ ๓ คือ “มีแนวโน้มสูง”) แสดงดังตารางต่อไปนี้

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ความน่าจะเป็น
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๑
๒. เว็บไซต์ และเว็บแอพพลิเคชั่น ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์ หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) - การอัพโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๒
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ขาดการอัพเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟแวร์ถูกลิขสิทธิ์	๒

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ความน่าจะเป็น
			- เครื่องคอมพิวเตอร์แม่ข่าย		
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash Drive, Handy Drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์	๓
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด	๓
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัพเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ระบบฐานข้อมูล - ระบบสารสนเทศ	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	๒

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ความน่าจะเป็น
				- ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall	
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ	๑

งาน B: กำหนดผลกระทบ (Determine Impact)

โดยทั่วไป การแสดงสถานการณ์ความเสี่ยงอาจส่งผลต่อการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และ/หรือความพร้อมใช้งาน (Availability) ของทรัพย์สิน (เช่น ข้อมูล อุปกรณ์ การดำเนินงาน) การโจมตีใด ๆ ของทรัพย์สินจะแปลเป็นผลกระทบในสาม (๓) ระดับต่อไปนี้

- **ระดับชาติ (National)** – ในระดับประเทศ ผลกระทบอาจถูกมองว่าเป็นอันตรายต่อความมั่นคงและเศรษฐกิจของประเทศ

- **หน่วยงาน (Organizational)** – ในระดับหน่วยงาน ผลกระทบอาจถูกมองว่าเป็นการหยุดชะงักในการดำเนินธุรกิจ ความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน

- **บุคคล (Individual)** - ในระดับบุคคล ผลกระทบสามารถมองได้ว่าเป็นการสูญเสียชีวิต และการบาดเจ็บ

ตารางด้านล่าง คือ ตารางประเมินสำหรับการพิจารณาผลกระทบของความเสี่ยงในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” ระดับคะแนน ๒ คือ “ปานกลาง” และ ๑ คือ “เล็กน้อย”) ที่จะเกี่ยวข้องกับ

- **เกี่ยวข้องกับบริบททางธุรกิจ (Relevant to Business Context)** – เชื่อมโยงคำอธิบายกับวัตถุประสงค์ทางธุรกิจของหน่วยงานหรือวัดผลงาน

- **ไม่กำกวม (Unambiguous)** - ใช้คำอธิบายที่เป็นเลขฐานสองหรือที่มีช่วงเชิงปริมาณ (เช่น การรั่วไหลของข้อมูลที่ถูกจัดประเภทเป็น “ความลับ” หรือทำให้การบริการของลูกค้ามากกว่าร้อยละ ๕๐ หยุดชะงัก)

- **มุมมองที่หลากหลาย (Multi-perspectives)** – ระบุประเภทย่อยของผลกระทบจากแต่ละระดับจาก ๓ ระดับ (เช่น ระดับประเทศ หน่วยงาน และบุคคล)

ตารางคำอธิบายทั่วไปสำหรับการพิจารณาผลกระทบของความเสี่ยง

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or SecondaryNational Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)	มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)	มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)
ด้านการรักษาความถูกต้องครบถ้วน (Integrity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ตารางเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
การเงินหรือทรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินหนึ่งร้อยล้านบาท	เกินกว่าหนึ่งร้อยล้านบาทขึ้นไป
อันตรายต่อชีวิต ร่างกายหรืออนามัย	ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิตร่างกายหรืออนามัย	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ไม่เกินหนึ่งพันคน	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคนหรือต่อชีวิตตั้งแต่หนึ่งคน
ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับ ความเสียหายนอกจากอันตรายต่อชีวิตร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคนแต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	ไม่มีผลกระทบหรือมีผลกระทบต่อการดำเนินการตามหน้าที่ของหน่วยงานเพียงเล็กน้อย	การดำเนินการตามหน้าที่หลักของหน่วยงานด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	การดำเนินการตามหน้าที่หลักของหน่วยงานต้องหยุดชะงักไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน
ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐต้องหยุดชะงัก ไม่ต่อเนื่องและไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่แตกต่างกันในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบสูงสุดควรถือเป็นคะแนนสุดท้าย

รายงานการประเมินความเสี่ยง การกำหนดผลกระทบให้คะแนนตามระดับ ๑ ถึง ๓ (ระดับคะแนน ๑ คือ “ต่ำ” ระดับคะแนน ๒ คือ “ปานกลาง” และระดับคะแนน ๓ คือ “สูง”)

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ผลกระทบ
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๓
๒. เว็บไซต์ และเว็บแอพพลิเคชั่น ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์ หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) - การอัพโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๒

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ผลกระทบ
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ขาดการอัพเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟแวร์ถูกลิขสิทธิ์	๒
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash Drive, Handy Drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์	๓
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด	๑

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ผลกระทบ
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัพเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ระบบฐานข้อมูล - ระบบสารสนเทศ	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall	๓
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ	๓

๔.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้:

- กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)
- ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

งาน A: กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)

ดังที่กล่าวไว้ในหัวข้อที่ ๓ ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นแผนภาพโดยใช้เมทริกซ์ความเสี่ยง แสดงดังภาพด้านล่างเป็นตัวอย่างเมทริกซ์ความเสี่ยง ๓ ต่อ ๓ สำหรับกำหนดระดับความเสี่ยงสำหรับแต่ละสถานการณ์ความเสี่ยง โดยที่ระดับความเสี่ยงเป็นการคูณของ “โอกาสเป็นไปได้” และ “ผลกระทบ” ซึ่งกำหนดจากขั้นตอนการวิเคราะห์ความเสี่ยง (หัวข้อ ๔.๒)

IMPACT				
	High (๓)	M๓๑	H๓๒	H๓๓
	Medium (๒)	L๒๑	M๒๒	H๒๓
	Low (๑)	L๑๑	L๑๒	L๑๓
		Low (๑)	Medium (๒)	High (๓)
		LIKELIHOOD		

รูปที่ ๒ เมทริกซ์ความเสี่ยง ๓ คูณ ๓ สำหรับกำหนดระดับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนดโดยหน่วยงาน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

รายงานการประเมินความเสี่ยง แสดงดังตารางต่อไปนี้

ระดับความเสี่ยง = ผลกระทบ *x* โอกาสเกิด โดยระดับการประเมิน นั้น C I และ A หมายถึง *Confidentiality Availability* และ *Integrity* ตามลำดับ การตอบ *Yes* ใน *C I* หรือ *A* หมายถึง การเกิดผลกระทบต่อการรักษาความลับ *(C)* การเกิดผลกระทบต่อความสมบูรณ์ของข้อมูล *(I)* หรือการเกิดผลกระทบต่อสภาพพร้อมใช้ *(A)* ตามลำดับ และการตอบ *No* หมายถึง ไม่ได้รับผลกระทบ

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	การวิเคราะห์ความเสี่ยง					
					ระดับผลกระทบ			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง
					C	I	A			
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	Yes	Yes	Yes	๓	๑	๓
๒. เว็บไซต์ และเว็บแอพพลิเคชั่น ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มี	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https	Yes	Yes	Yes	๓	๒	๖

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	การวิเคราะห์ความเสี่ยง					
					ระดับผลกระทบ			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง
					C	I	A			
		ความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) - การอัพโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย	แม่ข่าย	- กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่						
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ขาดการอัพเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟแวร์ถูกลิขสิทธิ์	Yes	Yes	Yes	๒	๒	๔
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash Drive, Handy Drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์	Yes	Yes	Yes	๓	๓	๙

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	การวิเคราะห์ความเสี่ยง					
					ระดับผลกระทบ			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง
					C	I	A			
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด	Yes	Yes	Yes	๑	๑	๓
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัพเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ระบบฐานข้อมูล - ระบบสารสนเทศ	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall	Yes	Yes	Yes	๓	๒	๖

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	การวิเคราะห์ความเสี่ยง					
					ระดับผลกระทบ			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง
					C	I	A			
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ	Yes	Yes	Yes	๓	๑	๓

งาน B: ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

การประเมินความเสี่ยงจะไม่สมบูรณ์หากไม่มีเอกสารประกอบ ผลลัพธ์จากขั้นตอนก่อนหน้าจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยงเพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย การลงทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงที่กำหนด การลงทะเบียนความเสี่ยงเป็นเอกสารที่มีชีวิตซึ่งได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (update) เป็นประจำ เพื่อให้แน่ใจว่าฝ่ายบริหารของหน่วยงานมีภาพปัจจุบันเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานเมื่อทำการตัดสินใจโดยแจ้งความเสี่ยง ควรมีอย่างน้อยดังต่อไปนี้

- **สถานการณ์ความเสี่ยง (Risk Scenario)** – สถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สินเพื่อสร้างผลกระทบในทางลบได้อย่างไร
- **วันที่ระบุความเสี่ยง (Identification Date)** – วันที่ที่ระบุสถานการณ์ความเสี่ยง
- **มาตรการที่มีอยู่ (Existing Measures)** – มาตรการปัจจุบันที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง
- **ความเสี่ยงในปัจจุบัน (Current Risk)** – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่ (เช่น ความเสี่ยงโดยธรรมชาติ (Inherent Risk) โดยใช้มาตรการที่มีอยู่)
- **แผนจัดการความเสี่ยง (Treatment Plan)** – กิจกรรมที่วางแผนไว้ (เช่น การใช้มาตรการเพิ่มเติม) และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้ (เช่น ภายในระดับการยอมรับความเสี่ยงของหน่วยงาน)
- **สถานะความคืบหน้า (Progress Status)** – สถานะของการดำเนินการตามแผนจัดการความเสี่ยง
- **ความเสี่ยงที่คงเหลืออยู่ (Residual Risk)** – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากดำเนินการตามแผนจัดการความเสี่ยง (เช่น ความเสี่ยงปัจจุบันที่มีมาตรการเพิ่มเติม)
- **เจ้าของความเสี่ยง (Risk Owner)** – บุคคลหรือกลุ่มที่รับผิดชอบในการดูแลให้ความเสี่ยงที่เหลืออยู่อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

รายงานการประเมินความเสี่ยงมีองค์ประกอบอย่างน้อย ๘ ประการ ได้แก่ ๑) สถานการณ์ความเสี่ยง ๒) วันที่ระบุ ๓) มาตรการที่มีอยู่ ๔) ความเสี่ยงปัจจุบัน ๕) แผนจัดการความเสี่ยง ๖) สถานะความคืบหน้า ๗) ความเสี่ยงที่เหลืออยู่ และ ๘) เจ้าของความเสี่ยง ดังตารางด้านล่างนี้

สถานการณ์ความเสี่ยง	วันที่ระบุ	ความเสี่ยงปัจจุบัน	แผนจัดการความเสี่ยง	มาตรการที่มีอยู่	สถานะความคืบหน้า	ความเสี่ยงที่เหลืออยู่	เจ้าของความเสี่ยง
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยผู้ไม่ประสงค์ดี (Hacker)	เมษายน ๖๗	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูลโจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๙๐ %	- โปรแกรมระบบฐานข้อมูลเก่า ล้าสมัย - เครื่องแม่ข่ายฐานข้อมูล (Server) และเครื่องจัดเก็บข้อมูล (Storage) เก่า และไม่ได้รับการบำรุงรักษาอย่างต่อเนื่อง	ศทส
๒. เว็บไซต์ และเว็บแอพพลิเคชั่น ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	เมษายน ๖๗	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ	๑๐๐ %	- เว็บแอพพลิเคชั่นเก่าขาดการปรับปรุง Source code ให้ทันสมัยและปลอดภัย	ศทส

สถานการณ์ความเสี่ยง	วันที่ระบุ	ความเสี่ยงปัจจุบัน	แผนจัดการความเสี่ยง	มาตรการที่มีอยู่	สถานะความคืบหน้า	ความเสี่ยงที่เหลืออยู่	เจ้าของความเสี่ยง
		ประสงค์ดี (Secure Coding) - การอัพโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย		ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่			
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	เมษายน ๒๕๖๗	- ขาดการอัพเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟแวร์ถูกลิขสิทธิ์	๔๐%	ซอฟต์แวร์และระบบปฏิบัติการส่วนใหญ่ไม่สามารถอัพเดพเพื่อปิดช่องโหว่ได้	ศทส
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	เมษายน ๒๕๖๗	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash Drive, Handy Drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) - มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมป่าไม้	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอและจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์	๔๐%	มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่ยังไม่ครอบคลุมเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องลูกข่าย	ศทส

สถานการณ์ความเสี่ยง	วันที่ระบุ	ความเสี่ยงปัจจุบัน	แผนจัดการความเสี่ยง	มาตรการที่มีอยู่	สถานะความคืบหน้า	ความเสี่ยงที่เหลืออยู่	เจ้าของความเสี่ยง
		- การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัคอมพิวเตอร์	ประจำปี พ.ศ. ๒๕๖๖				
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	เมษายน ๒๕๖๗	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด	๕๐ %	ผู้ใช้งานมีสิทธิเป็น Admin ของเครื่องซึ่งทำให้สามารถติดตั้งโปรแกรม หรือ Virus, Malware จะสามารถเขียนไฟล์ หรือสร้างตัวเองลงในเครื่องได้โดยไม่ต้องขอใช้สิทธิ์	ศทส
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	เมษายน ๒๕๖๗	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัพเดตทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) - มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมป่าไม้	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความ	๙๐ %	ผู้ไม่ประสงค์ดี (Hacker) ยังสามารถใช้ช่องโหว่ ที่เกิดขึ้นในระบบเครือข่าย ระบบสารสนเทศ เพื่อเข้าแก้ไขข้อมูล ทำลายข้อมูล โดยไม่ได้รับอนุญาตยังสามารถทำงานได้ในบางระบบสารสนเทศ ซึ่งหน่วยงานควรจัดหาระบบหรือ	ศทส

สถานการณ์ความเสี่ยง	วันที่ระบุ	ความเสี่ยงปัจจุบัน	แผนจัดการความเสี่ยง	มาตรการที่มีอยู่	สถานะความคืบหน้า	ความเสี่ยงที่เหลืออยู่	เจ้าของความเสี่ยง
			ประจำปี พ.ศ. ๒๕๖๖	ปลอดภัย เช่น Firewall		อุปกรณ์ด้านการป้องกันภัยคุกคามทางไซเบอร์มาเพื่อป้องกัน	
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	เมษายน ๒๕๖๗	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัพเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) - มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมป่าไม้ ประจำปี พ.ศ. ๒๕๖๖	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ	๑๐๐%	-	ศทส

๕. ตอบสนองต่อความเสี่ยง

หลังจากประเมินความเสี่ยงที่ระบุแล้ว (เช่น ความเสี่ยงในปัจจุบัน) ขั้นตอนต่อไปคือการระบุและกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

๕.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options)

มีตัวเลือกการตอบสนองความเสี่ยง จำนวน ๔ ตัวเลือก ที่ต้องพิจารณา

(๑) ยอมรับ (Accept)

การยอมรับความเสี่ยงหมายถึงการรับความเสี่ยงตามที่เป็นอยู่โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อลดความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของหน่วยงานเท่านั้น

(๒) หลีกเลี่ยง (Avoid)

การหลีกเลี่ยงความเสี่ยงหมายถึงการยุติการกระทำหรือกิจกรรมที่ทำให้หน่วยงานมีความเสี่ยงที่ระบุ สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

ตัวอย่าง: การไม่ทำธุรกรรมการชำระเงินออนไลน์เป็นตัวอย่างของการหลีกเลี่ยงความเสี่ยงที่ผู้โจมตีจะลักลอบใช้ธุรกรรมเพื่อชำระเงินที่เป็นการฉ้อโกง

(๓) โอนย้าย (Transfer)

การโอนความเสี่ยงหมายถึงการแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือหน่วยงานอื่น เช่น โดยทั่วไปตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

ตัวอย่าง: การซื้อประกันทางไซเบอร์หรือการจ้างดำเนินการบางอย่างเป็นตัวอย่างของการแบ่งปันความเสี่ยงกับบุคคลที่สาม

(๔) การลดความเสี่ยง (Mitigate)

การลดความเสี่ยงหมายถึงการวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง: การใช้ไฟร์วอลล์เพื่อจำกัดทราฟฟิกเครือข่ายเป็นตัวอย่างในการลดความเสี่ยงของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในหน่วยงานจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกอย่างเป็นทางการ และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

๕.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุมความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตาม หน่วยงานควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่าตัวอย่างเช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบเมื่อพนักงานเข้าถึงเว็บไซต์ที่เป็นอันตราย หน่วยงานต่าง ๆ อาจต้องพิจารณาหลีกเลี่ยงความเสี่ยงโดยการทำให้เข้าถึงระบบอินเทอร์เน็ตลดลงหรือจำกัดการเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการปรับใช้ทางแก้ไขปัญหาป้องกันปลายทางที่มีราคาแพง

เมื่อหน่วยงานเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ ทั้งนี้ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยงหรือการลดผลกระทบจากความเสี่ยง

๖. การจัดการความเสี่ยง

จากนโยบายของกรมป่าไม้ ระดับความเสี่ยงที่ยอมรับได้ ≤ ๓ โดยกำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๓ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๓ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ความเสี่ยง (ภาวะคุกคาม)	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	วิธีควบคุม	แนวทางการควบคุม
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูล โดยผู้ไม่ประสงค์ดี (Hacker)	๓	มีแผนรองรับความเสี่ยง	ลด	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่
๒. เว็บไซต์ และเว็บแอพพลิเคชั่น ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	๔	มีแผนรองรับความเสี่ยง	ลด	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษ ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	๔	มีแผนรองรับความเสี่ยง	ลด	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟแวร์ถูกลิขสิทธิ์
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	๙	มีแผนรองรับความเสี่ยง	ลด	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัพเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์

ความเสี่ยง (ภาวะคุกคาม)	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	วิธีควบคุม	แนวทางการควบคุม
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	๓	มีแผนรองรับความเสี่ยง	ลด	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	๖	มีแผนรองรับความเสี่ยง	ลด	- ติดตั้งระบบตรวจสอบการบุกรุก เครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	๓	มีแผนรองรับความเสี่ยง	ลด	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่อง ระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ