แนวทางปฏิบัติ
การประเมินความเสี่ยง
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมส่งเสริมสหกรณ์
กันยายน พ.ศ. 2566

สารบัญ

๑. บทนำ (INTRODUCTION)

๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ด้วยความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็ว ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนไป และความเป็นดิจิทัลที่เพิ่มขึ้น หน่วยงานอาจเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบในทางลบต่อหน่วยงานและวัตถุประสงค์ทางธุรกิจ ดังนั้นจึงมีความจำเป็นสำหรับกรมส่งเสริมสหกรณ์ในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้อย่างมีประสิทธิภาพ

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า "การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงระดับหน่วยงานของกรมส่งเสริมสหกรณ์ โดยการประเมินความเสี่ยง กรมส่งเสริมสหกรณ์จะสามารถ :

- ระบุเหตุการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจากการกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้กรมส่งเสริมสหกรณ์สามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอเพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในหน่วยงาน การประเมินความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้บุคลากรมีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยีและวิธีที่บุคลากรดังกล่าว ปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

๑.๒ ปัญหาทั่วไปที่สังเกตได้

ในขณะที่หน่วยงาน ตระหนักดีว่าการประเมินความเสี่ยงเป็นส่วนสำคัญของแนวทางปฏิบัติในการประเมินความเสี่ยงของหน่วยงาน (Enterprise Risk assessment Practice) แต่หน่วยงานหลายแห่งก็ประสบปัญหากับกระบวนการในการประเมินความเสี่ยงที่เหมาะสม ช่องว่างทั่วไปบางส่วนที่สังเกตเห็น ได้แก่

ก. การระบุสถานการณ์ความเสี่ยงที่ไม่ดี (Poor Articulation of Risk Scenarios) สถานการณ์ความเสี่ยงที่อธิบายถึงเหตุการณ์ “สิ่งที่อาจผิดพลาดได้ (What Could Go Wrong)” มักจะคลุมเครือและเป็นเรื่องทั่วไป โดยไม่ได้ระบุเหตุการณ์ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมาที่เฉพาะเจาะจง เป็นผลให้การเข้าใจขอบเขตของความเสี่ยง การเชื่อมโยงกับบริบทของหน่วยงาน หรือการระบุมาตรการเป้าหมายเพื่อจัดการกับความเสี่ยง กระทำได้ยาก

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

ค. การขาดการยอมรับความเสี่ยง (Absence of Risk Tolerance) หน่วยงานมักจะไม่บูรณาการแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เข้ากับโปรแกรมการจัดการความเสี่ยงของหน่วยงาน ด้วยเหตุนี้ การยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับหน่วยงานจึงมักถูกละเลย และผู้บริหารต้องเผชิญกับความยากลำบากในการตัดสินใจเลือกระดับความเสี่ยงที่เหมาะสมที่จะนำมาใช้ในขณะที่ดำเนินการตามวัตถุประสงค์ทางธุรกิจของหน่วยงาน

ง. การกำหนดโอกาสเสี่ยงตามเหตุการณ์ที่เกิดขึ้นในอดีตหรือที่คาดไว้ (Determining Risk Likelihood Based on Historical or Expected Occurrences) หน่วยงานต่าง ๆ มักจะใช้การวัดเวลาหรือ

ความถี่ (เช่น เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดไว้) เพื่อประเมินโอกาสเสี่ยงของตน แนวทางนี้ อาจไม่ถูกต้องเมื่อพิจารณาจากจำนวนครั้งที่เหตุการณ์เกิดขึ้นก่อนหน้านี้ โดยเฉพาะอย่างยิ่งเมื่อไม่มีข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมา ในบริบทของความมั่นคงปลอดภัยไซเบอร์ ความน่าจะเป็นของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์นั้นไม่ขึ้นกับความถี่ของการเกิดขึ้นในอดีต

จ. จัดการกับความเสี่ยงด้วยการควบคุมหรือมาตรการที่ไม่เกี่ยวข้อง (Treating Risks With Irrelevant controls/measures) หน่วยงานอาจใช้แนวทางกว้าง ๆ ในการหามาตรการเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุ ซึ่งส่งผลให้การดำเนินการควบคุมนั้นไม่ได้ระบุถึงสาเหตุที่แท้จริงอย่างสมบูรณ์ ซึ่งมักเกิดจากความเข้าใจหรือการอธิบายสถานการณ์ความเสี่ยงที่ไม่ดีพอ

๒. วัตถุประสงค์ กลุ่มเป้าหมาย และขอบเขต (PURPOSE, AUDIENCE & SCOPE)

๒.๑ วัตถุประสงค์

- เพื่อเป็นแนวทางปฏิบัติสำหรับกรมส่งเสริมสหกรณ์ เกี่ยวกับวิธีดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม
- เพื่อให้การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมสหกรณ์ เป็นไปตามมาตรฐาน
- เพื่อสร้างความตระหนัก ความรู้และความเข้าใจต่อการประเมินความเสี่ยงด้านรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม ให้แก่บุคลากรทุกระดับ และบุคคลที่เกี่ยวข้อง

๒.๒ กลุ่มเป้าหมายและขอบเขต (Audience & Scope)

เอกสารนี้มีขึ้นเพื่อใช้โดยผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ต่อไปนี้

- ผู้มีส่วนได้ส่วนเสีย (Stakeholders) ภายในหน่วยงาน ได้แก่ หัวหน้าส่วนราชการ หน่วยงานภายในกรมส่งเสริมสหกรณ์ หน่วยงานเจ้าของข้อมูล หน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ผู้ใช้งานระบบในระดับต่าง ๆ เป็นต้น
- ที่ปรึกษาภายนอก หรือผู้ดูแลและบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม หรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของหน่วยงาน
- ขอบเขตของแนวทางฉบับนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความเสี่ยง อยู่นอกเหนือขอบเขตของแนวทางฉบับนี้

๓. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT)

การกำหนดบริบทของความเสี่ยงเป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับการประเมินความเสี่ยง ขั้นตอนนี้ทำให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมินความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

๓.๑ กำหนดความเสี่ยง (Define Risk)

มีคำจำกัดความมากมายเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนั้น ก่อนที่จะกำหนดรายละเอียดเพิ่มเติมเกี่ยวกับการประเมินความเสี่ยง สิ่งสำคัญคือต้องกำหนดคำนิยามทั่วไป

ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับวัตถุประสงค์ของแนวทางฉบับนี้ ความเสี่ยงถูกกำหนดให้เป็นผลลัพธ์ของ ๒ ปัจจัย คือ:

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

Risk = Function (Likelihood, Impact)

ปัจจัยเสี่ยงแต่ละประการที่กล่าวถึงในคำจำกัดความได้อธิบายไว้ด้านล่าง

เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor)[๑] ใช้เวกเตอร์ภัยคุกคาม (การกระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย (เรียกว่า เวกเตอร์การโจมตี (Threat Vector)[๒]) กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP) ที่ใช้โดยผู้คุกคาม

ช่องโหว่ (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สิน หรือการควบคุมภายในของกระบวนการ

ความน่าจะเป็น (Likelihood)

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

ผลกระทบ (Impact)

ผลกระทบหมายถึงขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

๓.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance)[๓] หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด

---

[๑] ผู้คุกคามหมายถึงบุคคลหรือองค์กรที่รับผิดชอบต่อเหตุการณ์ที่อาจก่อให้เกิดอันตราย

[๒] เวกเตอร์ภัยคุกคามหมายถึงเส้นทางหรือเส้นทางที่ผู้คุกคามใช้เพื่อโจมตีเป้าหมาย

[๓] แหล่งข้อมูล เช่น ISACA นิยามการยอมรับความเสี่ยง (risk tolerance) ว่าเป็น “ระดับความแปรผันที่ยอมรับได้ (acceptable level) ซึ่งผู้บริหารเต็มใจที่จะยอมให้กับความเสี่ยงใด ๆ โดยเฉพาะเมื่อองค์กรดำเนินการตามวัตถุประสงค์” และใช้คำว่าความเสี่ยงที่ยอมรับได้ (risk appetite) เพื่ออ้างถึง "ปริมาณความเสี่ยงบนระดับกว้างที่กิจการยินดีรับตามพันธกิจ”

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ:

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตารางการยอมรับความเสี่ยง

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
High	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันที ทางเลือกที่เป็นไปได้ คือ กลยุทธ์การลดระดับความเสี่ยงหรือการถ่ายโอนจำเป็นต้องดำเนินการทันที
Medium	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้ กลยุทธ์การรักษาที่มุ่งลดระดับความเสี่ยงควรได้รับการพัฒนาและดำเนินการใน ๓ - ๖ เดือนข้างหน้า
Low	ความเสี่ยงระดับนี้สามารถยอมรับได้หากไม่มีกลยุทธ์การจัดการความเสี่ยงที่สามารถดำเนินการได้ง่ายและประหยัด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม

๓.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

บทบาทและหน้าที่ความรับผิดชอบของผู้มีส่วนได้ส่วนเสีย ของกรมส่งเสริมสหกรณ์ ประกอบด้วย

หัวหน้าหน่วยงาน (Head of Organization)

ผู้บริหารระดับสูงสุด (Highest-level Senior Official) ภายในหน่วยงานที่มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของหน่วยงาน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

เจ้าของกระบวนการธุรกิจ (Business Owner)

ผู้บริหารของหน่วยงานภายใน ระดับกอง/สำนัก หรือของหน่วยธุรกิจ (Business Unit) ที่รับผิดชอบในการตรวจสอบให้แน่ใจว่ากระบวนการทำงานที่ดำเนินการอยู่บรรลุเป้าหมายทางธุรกิจ หรือแบ่งปันข้อกังวลเกี่ยวกับผลกระทบที่มีต่อการทำงานในกรณีที่ระบบมีการหยุดชะงัก

ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)

กลุ่มพัฒนาระบบบริหาร หรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งหน่วยงาน ทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและการดำเนินงานขององค์กร หรือกิจกรรมขององค์กร ในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุนการทำงานของระบบที่สนับสนุนกิจกรรมทางธุรกิจ และดำเนินงานจัดทำทรัพย์สินของระบบและอุปกรณ์ทาง

เอกสารแนวทางฉบับนี้ไม่ได้แยกความแตกต่างระหว่างการยอมรับความเสี่ยง (risk tolerance) และความเสี่ยงที่ยอมรับได้ (risk appetite) เนื่องจากพิจารณาว่าทั้งสองอย่างนี้มีความหมายกว้างๆ เหมือนกัน (เช่น ความเสี่ยงที่องค์กรยินดียอมรับ)

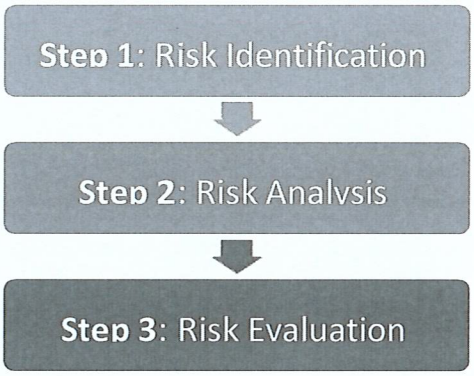
เทคโนโลยีและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

ฟังก์ชั่นความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการดำเนินการและการบำรุงรักษาการควบคุม ความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมทางธุรกิจ โดยบุคคลดังกล่าวควรระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ กำหนดแนวคิดเกี่ยวกับสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสมเพื่อจัดการกับภัยคุกคามหรือการโจมตีที่ระบุ

๔. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

การประเมินความเสี่ยงนั้นเกี่ยวกับการระบุความเสี่ยงที่เฉพาะเจาะจงกับสภาพแวดล้อม และการกำหนดระดับของความเสี่ยงที่ระบุ ขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง (**Risk Identification**) การวิเคราะห์ความเสี่ยง (**Risk Analysis**) และการประเมินความเสี่ยง (**Risk Evaluation**)



รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๔.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

(๑) ระบุทรัพย์สิน (Identify Assets)

คือการระบุและสร้างทะเบียนทรัพย์สินทางกายภาพและทางตรรกะทั้งหมดที่ประกอบกันเป็นระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยง เมื่อระบุทรัพย์สิน สิ่งสำคัญคือต้องจดบันทึกทรัพย์สินเหล่านั้น ซึ่งทรัพย์สิน ได้แก่

- ทรัพย์สินสำคัญ (Crown Jewels) - ทรัพย์สินเหล่านี้มีความสำคัญต่อการบรรลุวัตถุประสงค์ทางธุรกิจโดยรวม และมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์
- ทรัพย์สินที่เกี่ยวข้อง (Stepping Stones) - ทรัพย์สินเหล่านี้เป็นทรัพยากรที่ผู้โจมตีต้องการควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ

(๒) การระบุภัยคุกคาม (Threat Identification) – หน่วยงานควรใช้แนวทางที่เป็นระบบเพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

(๓) การระบุหรือการสร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios) เป็นการดำเนินการขั้นตอนการระบุความเสี่ยงให้เสร็จสมบูรณ์ งานนี้มีเป้าหมายเพื่อสร้างสถานการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ที่ให้มุมมองที่สมจริงและสัมพันธ์กันของความเสี่ยงตามบริบททางธุรกิจ

สภาพแวดล้อมของระบบ และภัยคุกคามที่เกี่ยวข้อง สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป ซึ่งจากการระบุหรือการสร้างสถานการณ์ความเสี่ยง หน่วยงานจะสามารถทราบสิ่งสำคัญอีก ๒ ประเด็น ได้แก่

- ช่องโหว่ (Vulnerability) - จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง

- ผลที่ตามมา (Consequence) – ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

๔.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

(๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น

(๒) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจาก การเกิดสถานการณ์ความเสี่ยง ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับการประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้

- ความสามารถในการค้นพบ (Discoverability) – ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่

- ความสามารถในการใช้ประโยชน์ (Exploitability) – ฝ่ายตรงข้ามจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี

- ความสามารถในการทำซ้ำ (Reproducibility) – ฝ่ายตรงข้ามจะสามารถสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

หน่วยงานจะใช้ ตารางการประเมินตัวอย่างเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น ซึ่งสามารถทำตามขั้นตอนต่อไปนี้เพื่อให้ได้รับคะแนนความเป็นไปได้ของสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

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

(ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

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

Likelihood Rating	ความสามารถในการค้นพบ	ความสามารถในการใช้ประโยชน์	ความสามารถในการทำซ้ำ
High (๓)	ช่องโหว่ของเป้าหมาย: • สามารถค้นพบได้โดยการค้นหา/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, ExploitDB) • สามารถถูกค้นพบและถูกโจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	การโจมตี: • สามารถดำเนินการได้โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย • สามารถทำได้ด้วยเครื่องมือที่หาได้ทั่วไปโดยไม่ต้องมีความรู้ด้านเทคนิค	การโจมตี: • สามารถทำซ้ำได้ตามต้องการโดยไม่มีการกำหนดค่า (Configuration) หรือเงื่อนไขของเหตุการณ์ (Event Condition) • สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่
Medium (๒)	ช่องโหว่ของเป้าหมาย: • สามารถค้นพบได้โดยการตรวจสอบการตอบสนอง พฤติกรรม 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 • สามารถถูกค้นพบและโจมตีด้วยการเข้าถึงแบบลอจิคัลโลคัล	การโจมตี: • สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin / SYSTEM / Root) • สามารถดำเนินการได้ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะซึ่งต้องการความรู้ด้านเทคนิคขั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน	การโจมตี: • สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุ่มบางอย่าง • สามารถทำซ้ำได้ในทางทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่

ตัวอย่างตารางประเมินความเสี่ยงที่อาจเกิดขึ้น

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 ผลกระทบสามารถมองได้ว่าเป็นการสูญเสียชีวิตและการบาดเจ็บ

ตารางด้านล่าง คือ ตัวอย่างตารางประเมินสำหรับการพิจารณาผลกระทบของความเสี่ยงในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” และ ๑ คือ “เล็กน้อย”) คำอธิบายที่ระบุในตารางตัวอย่างด้านล่างเป็นข้อมูลทั่วไป เมื่อใช้ตารางผลกระทบที่คล้ายกัน หน่วยงานควรตรวจสอบและปรับแต่งคำอธิบายสำหรับการจัดอันดับผลกระทบแต่ละรายการเพื่อให้แน่ใจว่า

- 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 Secondary National 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)

ตารางตัวอย่างเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
การเงินหรือรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินหนึ่งร้อยล้านบาท	เกินกว่าหนึ่งร้อยล้านบาทขึ้นไป
อันตรายต่อชีวิต ร่างกายหรืออนามัย	ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ไม่เกินหนึ่งพันคน	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคนหรือต่อชีวิตตั้งแต่หนึ่งคน

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับ ความเสียหายนอกจากอันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	ไม่มีผลกระทบหรือมีผลกระทบต่อการดำเนินการตามหน้าที่ของหน่วยงานเพียงเล็กน้อย	การดำเนินการตามหน้าที่หลักของหน่วยงานด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	การดำเนินการตามหน้าที่หลักของหน่วยงานต้องหยุดชะงักไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน
ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐต้องหยุดชะงัก ไม่ต่อเนื่องและไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่แตกต่างกันในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบสูงสุดควรถือเป็นคะแนนสุดท้าย

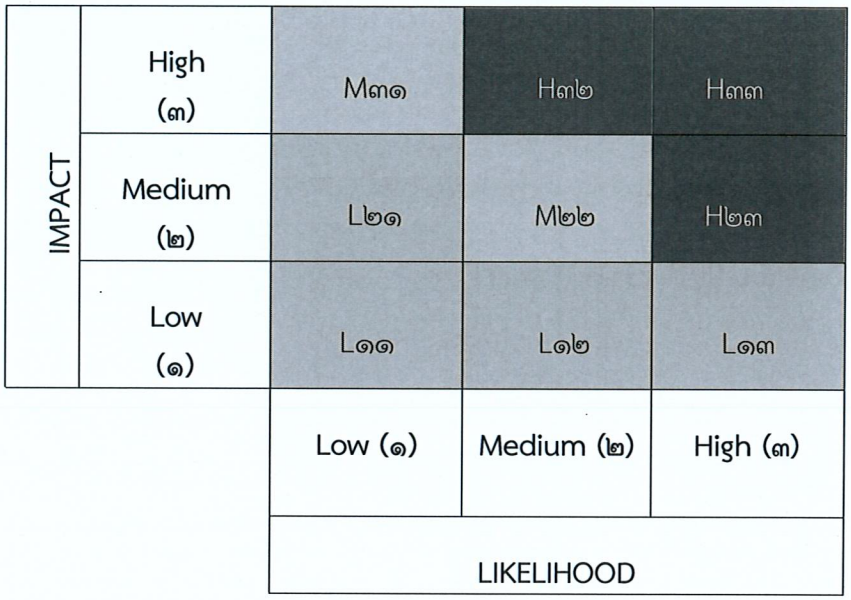
๔.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้:

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

กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)

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



รูปที่ ๒ เมทริกซ์ความเสี่ยง ๓ คูณ ๓ สำหรับกำหนดระดับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนดโดยหน่วยงาน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

การทำเอกสารเกี่ยวกับความเสี่ยง (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

ในรายงานการประเมินความเสี่ยงหน่วยงาน ทะเบียนความเสี่ยงต้องมีองค์ประกอบอย่างน้อย ๘ ประการ ได้แก่ สถานการณ์ความเสี่ยง วันที่ระบุ มาตรการที่มีอยู่ ความเสี่ยงปัจจุบัน แผนจัดการความเสี่ยง สถานะความคืบหน้า ความเสี่ยงที่เหลืออยู่ เจ้าของความเสี่ยง

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

๕.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

กรมส่งเสริมสหกรณ์จะพิจารณาการตอบสนองความเสี่ยงที่เหมาะสม เช่นการหลีกเลี่ยงหรือถ่ายโอนความเสี่ยงเป็นทางเลือกที่เป็นไปได้ มีความคุ้มค่า ซึ่งหน่วยงานจะทำการตรวจสอบให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ ซึ่งสามารถลดความเสี่ยง หรือการลดผลกระทบจากความเสี่ยง

เอกสารอ้างอิง

๑. GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE, Cyber Security Agency of Singapore, FEBRUARY ๒๐๒๑
Link: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf

๒. NIST SP ๘๐๐-๓๐ Rev. ๑ Guide for Conducting Risk Assessments, NIST, September ๒๐๑๒
Link: https://csrc.nist.gov/publications/detail/sp/๘๐๐-๓๐/rev-๑/final

๓. ISO ๓๑๐๐๐:๒๐๑๘(en) Risk management — Guidelines, ISO, FEBRUARY ๒๐๑๘
Link: https://www.iso.org/obp/ui/#iso:std:iso:๓๑๐๐๐:ed-๒:v๑:en

๔. ISO/IEC ๒๗๐๐๕:๒๐๑๘ Information technology — Security techniques — Information security risk management, ISO/IEC, July ๒๐๑๘
Link: https://www.iso.org/standard/๗๕๒๘๑.html

๕. ตัวอย่างแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ