



แนวปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

สารบัญ

๑. บทนำ (INTRODUCTION).....	๑
๒. วัตถุประสงค์ (PURPOSE).....	๑
๓. กลุ่มเป้าหมาย (AUDIENCE).....	๑
๔. ขอบเขต (SCOPE).....	๒
๕. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT)	๒
๕.๑ นิยามความเสี่ยงทางไซเบอร์.....	๒
๕.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance).....	๔
๕.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities).....	๕
๖. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)	๖
๖.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)	๖
๖.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)	๗
๖.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation).....	๑๓
๗. ตอบสนองต่อความเสี่ยง	๑๕
๗.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options).....	๑๕
๗.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions).....	๑๖
เอกสารอ้างอิง	๑๘

๑. บทนำ (INTRODUCTION)

จากความก้าวหน้าทางเทคโนโลยีบนโลกออนไลน์ มีส่วนสำคัญต่อการดำเนินชีวิตและการสะดวกสบายต่อการใช้ชีวิตประจำวัน ของผู้คนในปัจจุบัน ซึ่งความสามารถในการพัฒนาทางเทคโนโลยีที่รวดเร็วนี้อาจทำให้เกิดความเสี่ยงต่อการนำไปใช้ในทางที่ผิดและเสี่ยงที่จะเกิดภัยคุกคามต่อชีวิตเพิ่มขึ้น กล่าวคือ ภัยที่เกิดจากมิจฉาชีพหรือผู้ไม่ประสงค์ดี ใช้อินเทอร์เน็ตในการก่ออาชญากรรมและแสวงผลประโยชน์ในรูปแบบต่าง ๆ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงของมหาวิทยาลัย โดยการประเมินความเสี่ยงทำให้สามารถ

- ระบุเหตุการณ์ความเสี่ยงที่เป็นภัยคุกคาม และอาจนำไปสู่กระทบต่อมหาวิทยาลัยในด้านต่างๆ
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมองค์กรเพื่อให้บุคลากรมีส่วนร่วมในการจัดการเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๒. วัตถุประสงค์ (PURPOSE)

เพื่อให้มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ มีกรอบการดำเนินงานเกี่ยวกับวิธีดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

๓. กลุ่มเป้าหมาย (AUDIENCE)

กลุ่มเป้าหมายของเอกสารนี้:

- ก. ผู้ประเมินความเสี่ยง
- ข. หน่วยงานทางโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- ค. ผู้มีส่วนได้ส่วนเสีย ผู้ใช้งานระบบเครือข่าย ระบบสารสนเทศของมหาวิทยาลัย พนักงานของมหาวิทยาลัย นักเรียน นักศึกษา

๔. ขอบเขต (SCOPE)

เอกสารฉบับนี้เป็นกรอบแนวทางการดำเนินงาน เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิและการจัดการเท่านั้น แต่ไม่รวมถึงการติดตามและการรายงานความเสี่ยง

๕. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT)

เป็นการสร้างข้อกำหนดที่สำคัญสำหรับการประเมินความเสี่ยง เพื่อให้กลุ่มเป้าหมาย ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมินความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

๕.๑ นิยามความเสี่ยงทางไซเบอร์

คือแนวโน้มที่จะได้รับผลกระทบจากการหยุดชะงักต่อข้อมูลที่ละเอียดอ่อน การเงิน หรือการดำเนินธุรกิจออนไลน์ รวมถึงการให้บริการบางอย่างที่มีความเกี่ยวข้องต่อการดำเนินงานและการให้บริการประชาชน โดยทั่วไปความเสี่ยงทางไซเบอร์มีความเกี่ยวข้องกับเหตุการณ์ที่อาจส่งผลให้เกิดการละเมิดข้อมูล การขโมยข้อมูล หรือการทำลายข้อมูลเพื่อให้ไม่สามารถให้บริการได้

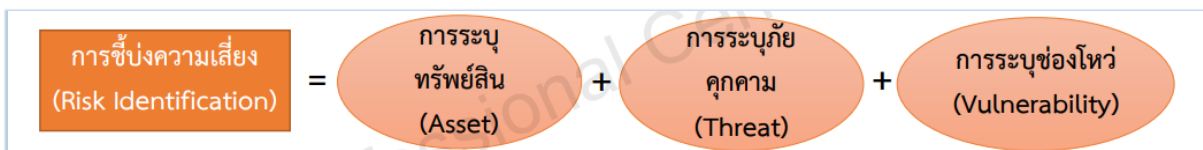
การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ช่วยให้ธุรกิจและองค์กรเข้าใจ ควบคุม และลดความเสี่ยงทางไซเบอร์ทุกรูปแบบ ที่เป็นองค์ประกอบสำคัญของการบริหารความเสี่ยงและลดความเสี่ยง หากไม่มีการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อาจส่งผลกระทบต่อข้อมูลและทรัพยากรสำคัญใน การดำเนินการอยู่ของธุรกิจและองค์กรได้ การใช้มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีวิธีการคำนวณตาม OWASP Risk Assessment

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

$$\text{Risk} = \text{Function (Likelihood, Impact)}$$

- การบ่งชี้ความเสี่ยง

เป็นการระบุปัจจัยที่มีผลกระทบในเชิงลบต่อเป้าหมายขององค์กรหรือการปฏิบัติงานทั้งในระดับองค์กรและกิจกรรม เช่น ทรัพย์สิน ภัยคุกคาม ช่องโหว่ด้านความมั่นคง



ภาพการบ่งชี้ความเสี่ยงตามแนวทางของมาตรฐานสากล ISO/IEC ๒๗๐๐๕

- สินทรัพย์สารสนเทศ

หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ ระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ เป็นต้น มีวัตถุประสงค์เพื่อบริหารกิจกรรมของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ให้บรรลุพันธกิจของมหาวิทยาลัย

- เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP) ที่ใช้

- **Ransomware (แรนซัมแวร์)** ซึ่งเป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูลไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความนิยมเชื่อถือในอุตสาหกรรมและองค์กรต่าง ๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์ได้มีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware
- **Phishing (ฟิชซิง)** คือการโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่าง ๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่นการส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่กรุณาคลิกลิงก์ด้านล่างนี้เพื่อ ยกเลิกการทำรายการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียงแคกรอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีแล้วผู้ไม่หวังดีนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่น ๆ ของเป้าหมาย เช่นข้อมูลการเงิน ข้อมูลรหัสระบบต่าง ๆ ที่เป็นข้อมูลส่วนบุคคล
- **Malware (มัลแวร์)** หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น

- **Virus (ไวรัส)** เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศเป็นอย่างยิ่งโดยมุ่งเน้นในการโจมตี ขัดขวางเพื่อไม่ให้ระบบสามารถใช้งานได้
- **Worms (เวิร์ม)** เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอกโดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงาน และขยายตัวส่งต่อภายในระบบเครือข่ายจนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้
- **Trojan (โทรจัน)** เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับเปลี่ยนแปลงแก้ไขข้อมูลซึ่งอาจส่งผลกระทบต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศหรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้
- **Spyware (สปายแวร์)** ซอฟต์แวร์ประสงค์ร้ายที่ทำงานอย่างลับๆ บนคอมพิวเตอร์และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล
- **Adware (แอดแวร์)** คือซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหาเกี่ยวกับระบบสารสนเทศได้ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัยได้
- **Data leaks (ข้อมูลรั่วไหล)** ข้อมูลรั่วไหลเกิดขึ้นเมื่อมีข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาชญากรที่ผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสียหายที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้

- ช่องโหว่ (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สินหรือการควบคุมภายในของกระบวนการ

๕.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ:

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

- ตารางการยอมรับความเสี่ยง

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

๕.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในแบบฝึกหัดการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในแบบฝึกหัดการประเมินความเสี่ยง ได้แก่

ผู้บริหาร (Head of Organization)

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

ฟังก์ชันการบริหารความเสี่ยง (Risk Management Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งหน่วยงาน ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและธุรกิจในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

ฟังก์ชันเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุนการทำงานของระบบที่สนับสนุนกิจกรรมทางธุรกิจ พวกเขาควรรู้จักทรัพย์สินของระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

ฟังก์ชันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการดำเนินการและการบำรุงรักษาการควบคุมความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมทางธุรกิจ โดยบุคคลดังกล่าวควรระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ กำหนดแนวคิดเกี่ยวกับสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสมเพื่อจัดการกับภัยคุกคามหรือการโจมตีที่ระบุ

๖. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

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



รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๖.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

- ระบุทรัพย์สิน (Identify Assets)
- การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)

การสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้

๑.การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition)

- ข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคาม

๒.การระบุภัยคุกคาม (Threat Identification)

- เพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

๓. การสร้างแบบจำลองการโจมตี (Attack Modelling)

- หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว หน่วยงานควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้หน่วยงานสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

- **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 ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมากการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง
- **ผลที่ตามมา (Consequence)** - ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

๖.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

- (๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น; และ
- (๒) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

- **กำหนดโอกาส (Determine Likelihood)**

เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าวเพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัตของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าไม่ถูกบุกรุกในอนาคต

ตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสียด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับการประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสียด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้¹

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

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

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

ภาพด้านล่าง คือตารางการประเมินตัวอย่างเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสียด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำตามขั้นตอนต่อไปเพื่อให้ได้รับคะแนนความเป็นไปได้ของสถานการณ์ความเสียด้านความมั่นคงปลอดภัยไซเบอร์

- (i) ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น ๓ ระดับ (เช่น ๑ – ๓)
- (ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มทีใกล้เคียงที่สุด
- (iii) คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสียด้านความมั่นคงปลอดภัยไซเบอร์ โดยระดับ ๓ คือ “มีแนวโน้มสูง” และ ๑ คือ “เป็นไปได้ยาก”

Likelihood Rating	Discoverability	Exploitability	Reproducibility
High (๓)	<p>ช่องโหว่ของเป้าหมาย:</p> <ul style="list-style-type: none"> สามารถค้นพบได้โดยการค้นหา/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, Exploit DB) สามารถถูกค้นพบและถูก 	<p>การโจมตี:</p> <ul style="list-style-type: none"> สามารถดำเนินการได้โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย สามารถทำได้ด้วย 	<p>การโจมตี:</p> <ul style="list-style-type: none"> สามารถทำซ้ำได้ตามต้องการโดยไม่มีข้อกำหนดค่า (Configuration)² หรือเงื่อนไขของเหตุการณ์

Likelihood Rating	Discoverability	Exploitability	Reproducibility
	โจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	เครื่องมือที่ทำได้ทั่วไป โดยไม่ต้องมีความรู้ด้านเทคนิค	(Event Condition) ³ <ul style="list-style-type: none"> สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่
Medium (๒)	ช่องโหว่ของเป้าหมาย: <ul style="list-style-type: none"> สามารถค้นพบได้โดยการตรวจสอบการตอบสนอง พฤติกรรม และการสื่อสารของเป้าหมาย (เช่น การฟิช (Fuzzing) กับแพ็กเก็ตเครือข่าย การดักจับเครือข่าย (Network Sniffing)) สามารถถูกค้นพบและโจมตีจากภายในเครือข่ายย่อยหรือส่วนเครือข่ายเดียวกัน 	การโจมตี: <ul style="list-style-type: none"> สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) ของเป้าหมาย (เช่น Admin/SYSTEM/Root) สามารถดำเนินการได้ด้วยเครื่องมือที่เปิดเผยแพร่ต่อสาธารณะ ซึ่งต้องใช้ความรู้ด้านเทคนิคในระดับกลาง 	การโจมตี: <ul style="list-style-type: none"> สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์ที่คาดเดาได้บางอย่าง สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย
Low (๑)	ช่องโหว่ของเป้าหมาย: <ul style="list-style-type: none"> สามารถค้นพบได้โดยการดำเนินการและโต้ตอบกับการตั้งค่าปัจจุบันหรือที่คล้ายกันของเป้าหมาย สามารถถูกค้นพบและ 	การโจมตี: <ul style="list-style-type: none"> สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin / SYSTEM / Root) สามารถดำเนินการได้ 	การโจมตี: <ul style="list-style-type: none"> สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุ่มบางอย่าง สามารถทำซ้ำได้ในทาง

Likelihood Rating	Discoverability	Exploitability	Reproducibility
	โจมตีด้วยการเข้าถึงแบบลอจิกัลโลคัล	ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะ ซึ่งต้องการความรู้ด้านเทคนิคขั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน	ทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่

ตัวอย่างตารางประเมินความเสี่ยงที่อาจเกิดขึ้น

- 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 (Organisational) - 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) - ระบุประเภทย่อยของผลกระทบจากแต่ละระดับ จาก ๓ ระดับ (เช่น ระดับประเทศ หน่วยงาน และบุคคล)
ตารางคำอธิบายทั่วไปสำหรับการพิจารณาผลกระทบของความเสี่ยง

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบ <u>น้อยหรือ</u> อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)	มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)	มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)
ด้านการรักษาความถูกต้องครบถ้วน(Integrity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบ <u>น้อยหรือ</u> อย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบต่อชน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบต่ออย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบต่ออย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ตารางตัวอย่างเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
การเงินหรือทรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินหนึ่งร้อยล้านบาท	เกินกว่าหนึ่งร้อยล้านบาทขึ้นไป
อันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยไม่เกินหนึ่งพันคน	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคนหรือต่อชีวิตตั้งแต่หนึ่งคน
ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายนอกจากอันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	ไม่มีผลกระทบ หรือมีผลกระทบต่อ	การดำเนินการตามหน้าที่หลักของหน่วยงานด้วยประสิทธิภาพพลงมาก	การดำเนินการตามหน้าที่หลักของหน่วยงานต้องหยุดชะงักไม่ต่อเนื่อง และไม่สามารถกู้คืน

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
	การดำเนินการตามหน้าที่ของหน่วยงานเพียงเล็กน้อย	แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	ระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน
ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้วยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐต้องหยุดชะงัก ไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่แตกต่างกันในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบสูงสุดควรถือเป็นคะแนนสุดท้าย

๖.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้:

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

- **กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)**

ดังที่กล่าวไว้ในหัวข้อที่ ๓ ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นแผนภาพโดยใช้เมทริกซ์

ความเสี่ยง แสดงดังภาพด้านล่างเป็นตัวอย่างเมทริกซ์ความเสี่ยง ๓ ต่อ ๓ สำหรับกำหนดระดับความเสี่ยง สำหรับแต่ละสถานการณ์ความเสี่ยง 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 ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนด โดยหน่วยงาน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

- **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)⁴ 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

๗. ตอบสนองต่อความเสี่ยง

หลังจากประเมินความเสี่ยงที่ระบุแล้ว (เช่น ความเสี่ยงในปัจจุบัน) ขั้นตอนต่อไปคือการระบุและกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

๗.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options)

มีตัวเลือกการตอบสนองความเสี่ยง จำนวน ๔ ตัวเลือก ที่ต้องพิจารณา

(๑) ยอมรับ (Accept)

การยอมรับความเสี่ยงหมายถึงการรับความเสี่ยงตามที่เป็นอยู่โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อลดความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของหน่วยงานเท่านั้น

(๒) หลีกเลี่ยง (Avoid)

ความเสี่ยงโดยธรรมชาติ (Inherent risk) หมายถึง ระดับความเสี่ยงที่มีอยู่โดยพิจารณาถึงมาตรการควบคุมในปัจจุบัน แต่ไม่คำนึงถึงมาตรการใด ๆ ที่จะดำเนินการเพิ่มเติม

การหลีกเลี่ยงความเสี่ยงหมายถึงการยุติการกระทำหรือกิจกรรมที่ทำให้หน่วยงานมีความเสี่ยงที่ระบุ
สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

ตัวอย่าง: การไม่ทำธุรกรรมการชำระเงินออนไลน์เป็นตัวอย่างของการหลีกเลี่ยงความเสี่ยง
ที่ผู้โจมตีจะลักลอบใช้ธุรกรรมเพื่อชำระเงินที่เป็นการฉ้อโกง

(๓) โอนย้าย (Transfer)

การโอนความเสี่ยงหมายถึงการแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือหน่วยงานอื่น เช่น
โดยทั่วไปตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

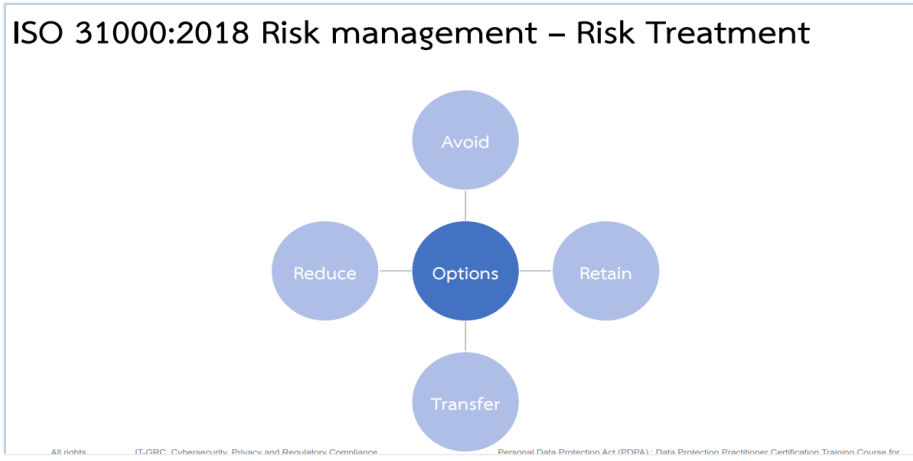
ตัวอย่าง: การซื้อประกันทางไซเบอร์หรือการจ้างดำเนินการบางอย่างเป็นตัวอย่างของการแบ่งปัน
ความเสี่ยงกับบุคคลที่สาม

(๔) การลดความเสี่ยง (Mitigate)

การลดความเสี่ยงหมายถึงการวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้
โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง: การใช้ไฟร์วอลล์เพื่อจำกัดกราฟฟิกเครือข่ายเป็นตัวอย่างในการลดความเสี่ยง
ของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และ
ความรับผิดชอบที่เหมาะสม) ภายในหน่วยงานจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกอย่างเป็นทางการ
และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่



๗.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุม
ความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตาม หน่วยงาน
ควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่า

ตัวอย่างเช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบเมื่อพนักงานเข้าถึงเว็บไซต์ที่เป็นอันตราย
หน่วยงานต่าง ๆ อาจต้องพิจารณาหลีกเลี่ยงความเสี่ยงโดยการทำให้เข้าถึงระบบอินเทอร์เน็ตลดลงหรือจำกัด
การเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการปรับใช้ทางแก้ไขปัญหาป้องกันปลายทางที่มีราคา
แพง

เมื่อหน่วยงานเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบ
ให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ
 ทั้งนี้ ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยง
หรือการลดผลกระทบจากความเสียหาย

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/defaultsource/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 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ