NSM

องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ

คู่มือ
การบริหารความเสี่ยง
ด้านความมั่นคงปลอดภัยสารสนเทศ
(IT Risk Management)
องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ

คู่มือการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
(IT Security Risk Management Guideline)

สารบัญ

1. คำนำ

ปัจจุบัน เทคโนโลยีสารสนเทศมีบทบาทอย่างมากในการขับเคลื่อนธุรกิจ และยังเป็นโครงสร้างพื้นฐานที่สำคัญในการเสริมสร้างประสิทธิภาพในกระบวนการดำเนินงานให้รองรับกลยุทธ์ทางธุรกิจ ด้วยการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีและความเสี่ยงในการเผชิญภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเพิ่มขึ้นและมีวิวัฒนาการที่ซับซ้อนมากขึ้น องค์กรพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (อพวช.) หรือต่อไปนี้เรียกว่า “อพวช.” ที่มีการประยุกต์ใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ จำเป็นต้องมีการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบและต่อเนื่อง เพื่อเตรียมความพร้อมในการรับมือกับความเสี่ยงต่าง ๆ ที่อาจส่งผลกระทบต่อ อพวช. ทั้งทางด้านการเงิน ด้านชื่อเสียงภาพลักษณ์ ด้านกฎหมาย กฎเกณฑ์ ด้านการปฏิบัติการ รวมถึงความเชื่อมั่นของลูกค้าและผู้มีส่วนได้ส่วนเสียที่มีต่อองค์กร การบริหารความเสี่ยงจึงเป็นกระบวนการที่สำคัญ ช่วยผลักดันการดำเนินธุรกิจของ อพวช. ให้บรรลุเป้าประสงค์ วิสัยทัศน์ และพันธกิจขององค์กร

2. วัตถุประสงค์

คู่มือการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของ อพวช. และเพื่อให้ อพวช. มีการกำกับดูแลและบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศ ทั้งบุคลากร กระบวนการ และการนำเทคโนโลยีสารสนเทศมาใช้ภายใต้การบริหารความเสี่ยงอย่างเหมาะสมและเพียงพอ สามารถดำเนินการวางแผน วิเคราะห์ ประเมิน และจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างมีประสิทธิภาพและประสิทธิผล สามารถควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

3. ขอบเขต

คู่มือการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศฉบับนี้ อ้างอิงจากมาตรฐาน ISO/IEC 27005:2022 (Information Security, Cybersecurity and Privacy protection - Guidance on Managing Information Security Risks) ซึ่งครอบคลุมถึงกระบวนการที่ใช้ในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของ อพวช.

4. คำนิยาม

คำ	ความหมาย
ความเสี่ยง (Risk)	เหตุการณ์ที่เกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนซึ่งส่งผลกระทบต่อการดำเนินงานให้ไม่เป็นไปตามวัตถุประสงค์และเป้าหมายทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคล โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

คำ	ความหมาย
ปัจจัยเสี่ยง (Risk Factor)	สิ่งที่เป็นต้นเหตุหรือแหล่งที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้ โดยในแต่ละปัจจัยจะมีการกำหนดสาเหตุที่แท้จริงที่ส่งผลให้เกิดความเสี่ยงต่าง ๆ เพื่อให้องค์กรสามารถวิเคราะห์และกำหนดมาตรการจัดการเพื่อลดความเสี่ยงได้อย่างถูกต้อง
การบริหารความเสี่ยง (Risk Management)	วิธีการบริหารจัดการที่เป็นไปเพื่อการคาดการณ์ และลดผลเสียของความไม่แน่นอนที่จะเกิดขึ้นกับองค์กร เป็นกลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตามและสื่อสารความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยป้องกันหรือบรรเทาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
การประเมินความเสี่ยง (Risk Assessment)	กระบวนการในการระบุระดับความรุนแรงและการจัดลำดับความสำคัญของความเสี่ยง โดยประเมินจากผลกระทบ (Impact) และโอกาสที่จะเกิดขึ้น (Likelihood) ของเหตุการณ์ความเสี่ยง
การระบุความเสี่ยง (Risk Identification)	การระบุและจำแนกปัจจัยเสี่ยงที่อาจทำให้การดำเนินงานขององค์กรไม่เป็นไปตามเป้าประสงค์
การวิเคราะห์ความเสี่ยง (Risk Analysis)	การรวบรวมและวิเคราะห์ข้อมูลเกี่ยวกับความเสี่ยงที่ต้องเผชิญ ซึ่งจะช่วยให้องค์กรตัดสินใจกำหนดแนวทางในการบริหารความเสี่ยงได้อย่างเหมาะสม
การประเมินค่าความเสี่ยง (Risk Evaluation)	การประเมินค่าผลกระทบ (Impact) และโอกาสที่จะเกิดขึ้น (Likelihood) ของเหตุการณ์ความเสี่ยง เพื่อระบุระดับความเสี่ยง (Risk Level) ของแต่ละเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
การจัดการความเสี่ยง (Risk Treatment)	แนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)
แผนการจัดการความเสี่ยง (Risk Treatment Plan)	แผนการจัดการเพื่อบรรเทาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้มาตรการควบคุมให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลงหรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลง
ระดับความเสี่ยง (Risk Level)	สถานะของความเสี่ยงที่ได้จากการประเมินผลกระทบ (Impact) และโอกาสที่จะเกิดขึ้น (Likelihood) ของเหตุการณ์ความเสี่ยง
ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)	สถานะของความเสี่ยงที่องค์กรยอมรับได้ เพื่อช่วยให้องค์กรมั่นใจได้ว่าได้มีการดำเนินการบริหารความเสี่ยงอยู่ภายในระดับที่ยอมรับได้

คำ	ความหมาย
การควบคุม (Control)	การกำหนดและบังคับใช้นโยบาย กระบวนการ ขั้นตอนปฏิบัติ หรือกลไกต่าง ๆ เพื่อบรรเทาความเสี่ยงโดยการป้องกัน (Prevention) ตรวจจับ (Detection) และ/หรือ แก้ไข (Correction)
ความเสี่ยงสืบเนื่อง (Inherent Risk)	ระดับความเสี่ยงก่อนที่จะมีการควบคุมหรือการจัดการเพื่อลดผลกระทบหรือโอกาสเกิดของเหตุการณ์ความเสี่ยง
ความเสี่ยงที่เหลืออยู่ (Residual Risk)	ระดับความเสี่ยงที่เหลืออยู่หลังจากมีการควบคุมหรือการจัดการเพื่อลดผลกระทบหรือโอกาสเกิดของเหตุการณ์ความเสี่ยง
โอกาสที่จะเกิด (Likelihood)	ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงขึ้น
ผลกระทบ (Impact)	ความรุนแรงของความเสียหาย หรือผลที่เกิดขึ้นตามมา สืบเนื่องจากเหตุการณ์ความเสี่ยง
ภัยคุกคาม (Threat)	สิ่งที่ก่อให้เกิดเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจส่งผลอันตรายต่อทรัพย์สินหรือองค์กร
ช่องโหว่ (Vulnerability)	ช่องโหว่หรือจุดอ่อนของทรัพย์สินหรือการควบคุม ที่ภัยคุกคามสามารถฉวยโอกาสหาผลประโยชน์ได้
เจ้าของความเสี่ยง (Risk Owner)	บุคคล กลุ่มบุคคล หรือหน่วยงานที่มีความรับผิดชอบโดยตรงต่อการควบคุมหรือบรรเทาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
สารสนเทศ (Information)	ข้อมูลซึ่งเป็นทรัพย์สินที่สำคัญขององค์กร โดยข้อมูลแบ่งออกเป็น 2 ประเภท คือ 1. ข้อมูลที่อยู่ในรูปแบบตีพิมพ์ (Hard Copy) 2. ข้อมูลที่อยู่ในรูปแบบอิเล็คทรอนิกส์ (Soft Copy)
การรักษาความลับ (Confidentiality)	คุณสมบัติที่สารสนเทศจะต้องไม่ถูกเปิดเผยแก่ผู้ที่ไม่ได้รับอนุญาต
ความถูกต้องครบถ้วน (Integrity)	คุณสมบัติของความถูกต้องครบถ้วนสมบูรณ์ของสารสนเทศ โดยสารสนเทศต้องไม่ถูกเปลี่ยนแปลงแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต
สภาพพร้อมใช้งาน (Availability)	คุณสมบัติของการเข้าถึงและใช้งานสารสนเทศได้ตามความต้องการของผู้ที่ได้รับอนุญาต

5. บทบาทหน้าที่ความรับผิดชอบ

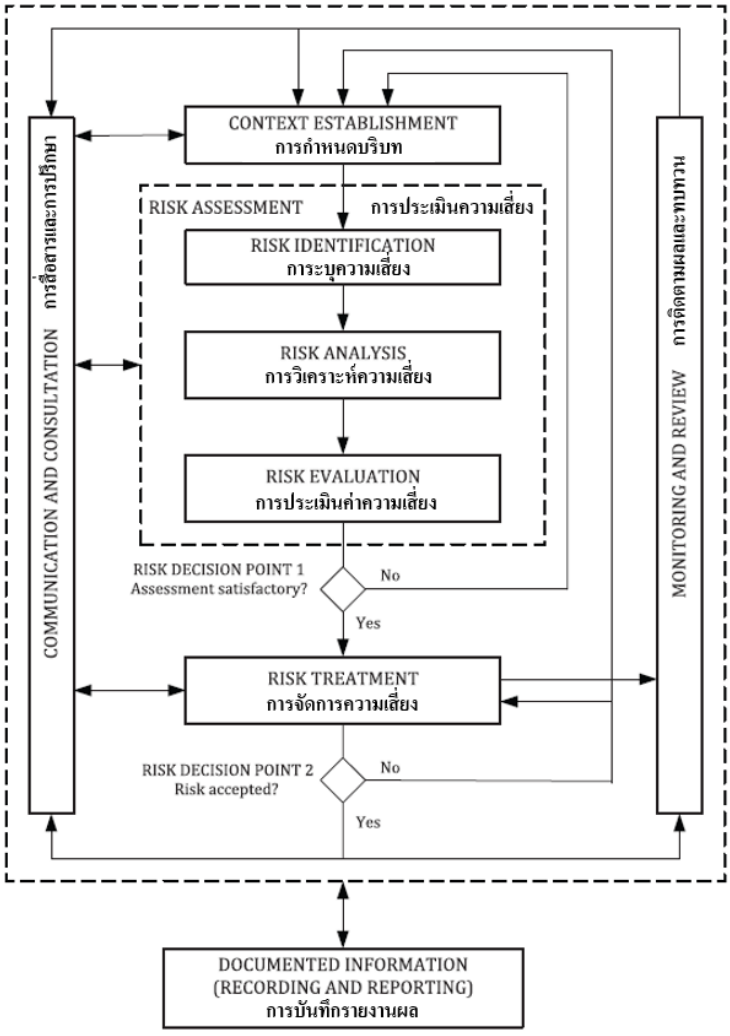
เพื่อให้มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้าน ความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม บทบาทหน้าที่ความรับผิดชอบของคณะทำงานที่ทำหน้าที่กำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีดังนี้

บทบาท	หน้าที่ความรับผิดชอบ
คณะกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Steering Committee)	ดูแลให้มีการกำหนดกลยุทธ์นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์ของ อพวช. รวมทั้งกำกับดูแลและติดตามการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ดูแลให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ โดยมีการเชื่อมโยงกับความเสี่ยงในภาพรวมของ อพวช. (Enterprise Risk Management)
คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ	ตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
คณะทำงานบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	ขับเคลื่อนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้ดำเนินการอย่างถูกต้องและดำรงรักษาไว้ซึ่งระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 รวมทั้งติดตามผลดำเนินการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง โดยต้องมีการทบทวนอย่างสม่ำเสมอ รวมทั้งประเมินและจัดทำแผนจัดการความเสี่ยง และนำเสนอต่อคณะกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศเพื่อพิจารณาอนุมัติ
เจ้าของความเสี่ยง (Risk Owner)	ร่วมจัดทำแผนจัดการความเสี่ยงในส่วนที่ตนรับผิดชอบ ซึ่งอาจต้องประสานงานกับหน่วยงานหรือบุคคลที่เกี่ยวข้องกับปัจจัยเสี่ยงนั้น ๆ เพื่อควบคุมหรือบรรเทาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

6. กระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อ้างอิงจากมาตรฐาน ISO/IEC 27005-2022 (Information Security, Cybersecurity and Privacy protection – Guidance on Managing Information Security Risks) สามารถสรุปได้เป็นขั้นตอนดังรูปที่ 1

รูปที่ 1 : กระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ



ดังที่แสดงในรูปที่ 1 กระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ มีองค์ประกอบที่สำคัญ ประกอบด้วย การกำหนดบริบทขององค์กร การประเมินความเสี่ยง การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินค่าความเสี่ยง การจัดการความเสี่ยง การสื่อสารและการปรึกษา การติดตามผลและทบทวน และการบันทึกรายงานผล

กิจกรรมการประเมินความเสี่ยง (Risk Assessment) และการจัดการความเสี่ยง (Risk Treatment) ในกระบวนการบริหารความเสี่ยงด้านความมั่นคงความปลอดภัยสารสนเทศสามารถดำเนินการซ้ำได้ตามความเหมาะสม เพื่อให้การประเมินความเสี่ยงมีข้อมูลที่เพียงพอสำหรับการกำหนดวิธีการจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กรเป็นสำคัญ

6.1 การกำหนดบริบท (Context Establishment)

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เริ่มต้นด้วยการทำความเข้าใจองค์กรและบริบทขององค์กร ตลอดจนการทำความเข้าใจความต้องการและความคาดหวังของผู้มีส่วนได้เสีย โดยการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจะเน้นการบริหารความเสี่ยงเพื่อดำรงรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมถึงการกำหนดเกณฑ์เพื่อใช้เป็นพื้นฐานในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์หรือเป้าหมายที่กำหนดไว้ในระดับความเสี่ยงที่ยอมรับได้ ซึ่งขึ้นอยู่กับขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) รวมถึงนโยบายการบริหารความเสี่ยง และผู้มีส่วนได้ส่วนเสียขององค์กร

6.2 การประเมินความเสี่ยง (Risk Assessment)

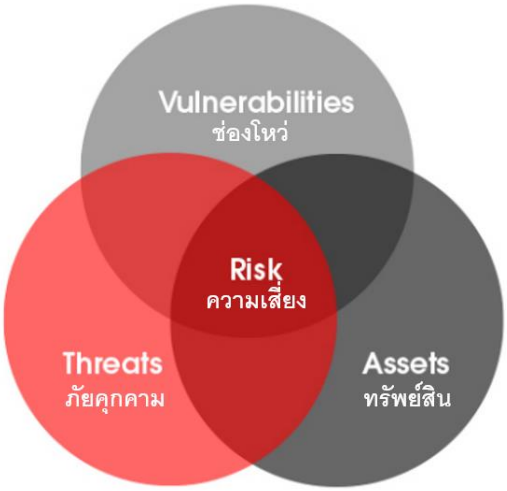
กระบวนการประเมินความเสี่ยง (Risk Assessment Process) ประกอบด้วยขั้นตอนที่สำคัญ 3 ขั้นตอน ได้แก่ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินค่าความเสี่ยง (Risk Evaluation) โดยการประเมินความเสี่ยง (Risk Assessment) ช่วยให้องค์กรสามารถจัดลำดับความสำคัญของความเสี่ยงโดยพิจารณาจากผลกระทบและโอกาสที่จะเกิดเหตุการณ์ซึ่งนำไปสู่ความเสียหาย ทำให้องค์กรไม่สามารถดำเนินงานได้ตามเป้าหมายที่กำหนดไว้ และเพื่อที่จะกำหนดวิธีการจัดการกับความเสี่ยงในขั้นตอนถัดไป

6.2.1 การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยง คือ การพิจารณาเหตุการณ์ที่นำไปสู่ความเสียหาย ในการระบุความเสี่ยงนั้นต้องพิจารณาปัจจัยทั้งจากภายในและภายนอกองค์กร ซึ่งเป็นปัจจัยที่มีผลกระทบต่อเป้าหมายและผลการปฏิบัติงานขององค์กร โดยปัจจัยภายนอกเป็นสภาพแวดล้อมภายนอก อพวช. ที่ไม่สามารถควบคุมได้ เช่น ภัยธรรมชาติ ภัยคุกคามทางไซเบอร์ กฎหมาย และคู่สัญญา ส่วนปัจจัยภายในเป็นสภาพแวดล้อมภายใน อพวช. ซึ่งสามารถควบคุมหรือเปลี่ยนแปลงได้ เช่น โครงสร้างองค์กร ระบบการบริหาร นโยบาย กระบวนการทำงาน บุคลากร และเทคโนโลยีที่นำมาใช้

ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศมีองค์ประกอบที่สำคัญ 3 องค์ประกอบ ได้แก่ ทรัพย์สิน (Asset), ช่องโหว่ (Vulnerability) และภัยคุกคาม (Threat) ดังที่แสดงในรูปที่ 2

รูปที่ 2 : องค์ประกอบของความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ



จากรูปที่ 2 สามารถสรุปได้ว่าความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจะเกิดขึ้นได้เมื่อมีการรวมทรัพย์สิน (Asset), ช่องโหว่ (Vulnerability) และภัยคุกคาม (Threat) เข้าด้วยกันจึงจะกลายเป็นความเสี่ยง (Risk) หากไม่มีทรัพย์สิน (Asset) ก็จะไม่มีช่องโหว่ (Vulnerability) หากไม่มีช่องโหว่ (Vulnerability) ก็จะไม่มีภัยคุกคาม (Threat) ที่ใช้ประโยชน์จากช่องโหว่นั้น ก็จะส่งผลให้ไม่มีความเสี่ยง (Risk) เช่นกัน

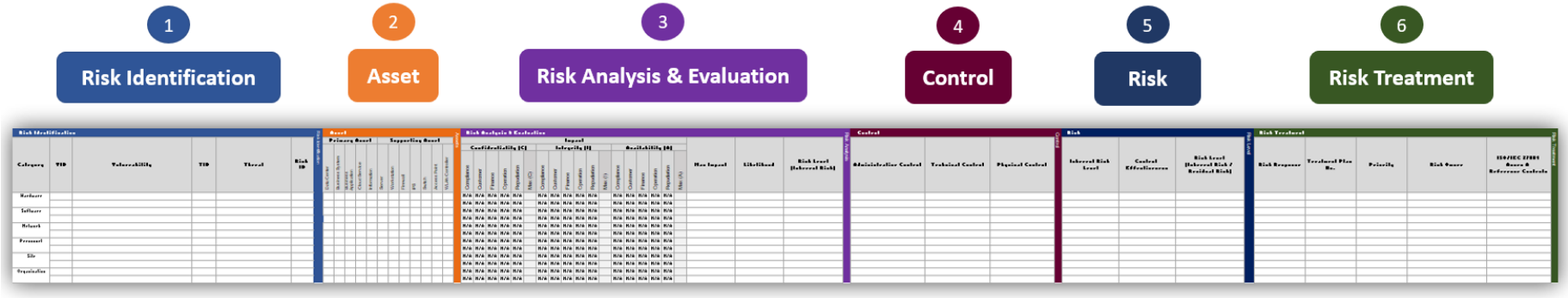
องค์กรจำเป็นต้องรวบรวมรายการทรัพย์สิน (Asset) ที่สำคัญขององค์กรสำหรับการประเมินความเสี่ยง โดยทรัพย์สิน (Asset) สามารถแบ่งเป็น 2 ประเภท ได้แก่

1) **ทรัพย์สินหลัก (Primary Asset)** คือสินทรัพย์ที่เป็นข้อมูลหรือกระบวนการทางธุรกิจขององค์กร โดยทรัพย์สินหลักของ อพวช. ได้แก่ ข้อมูล (Information), ศูนย์ข้อมูล (Data Center), ระบบธุรกิจ (Business System), แอปพลิเคชันทางธุรกิจ (Business Application), และระบบบริการคลาวด์ (Cloud Service)

2) **ทรัพย์สินสนันสนุน (Supporting Asset)** คือสินทรัพย์ที่ช่วยสนับสนุนบริการหรือกระบวนการทางธุรกิจขององค์กร โดยทรัพย์สินสนันสนุนของ อพวช. ได้แก่ เครื่องแม่ข่าย (Server), เวิร์กสเตชัน (Workstation), อุปกรณ์ไฟร์วอลล์ (Firewall), อุปกรณ์ป้องกันการบุกรุก (Intrusion prevention system: IPS), อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และอุปกรณ์ควบคุมการทำงานของอุปกรณ์ไร้สาย (WLAN Controller)

รูปที่ 3 เป็นแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Risk Assessment Form) ของ อพวช. ใช้สำหรับประเมินความเสี่ยงและกำหนดวิธีการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Risk Assessment Form) แบ่งออกเป็น 6 ส่วน ได้แก่ การระบุความเสี่ยง (Risk Identification), ทรัพย์สิน (Asset), การวิเคราะห์ความเสี่ยงและการประเมินค่าความเสี่ยง (Risk Analysis & Evaluation), การควบคุม (Control), ความเสี่ยง (Risk) และการจัดการความเสี่ยง (Risk Treatment)

รูปที่ 3 : แบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Risk Assessment Form)



การระบุความความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วยส่วนที่ 1 และ 2 ของแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Risk Assessment Form) โดยการระบุความเสี่ยง (Risk Identification) ในส่วนที่ 1 เป็นการระบุปัจจัยเสี่ยงซึ่งประกอบด้วย ประเภทของความเสี่ยง (Category), ช่องโหว่ (Vulnerability) และภัยคุกคาม (Threat) และส่วนที่ 2 ของแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Risk Assessment Form) คือ ทรัพย์สิน (Asset) ที่มีความเสี่ยงจากช่องโหว่และภัยคุกคามที่ระบุไว้ในส่วนที่ 1 โดยทรัพย์สิน (Asset) ประกอบด้วย ทรัพย์สินหลัก (Primary Asset) และทรัพย์สินสนันสนุน (Supporting Asset)

การระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ต้องคำนึงถึงองค์ประกอบต่าง ๆ ทั้งที่เคยเกิดขึ้นในอดีต เช่น เหตุการณ์ละเมิดด้านความมั่นคงปลอดภัยสารสนเทศและแหล่งที่มาของเหตุภัยคุกคามนั้น ๆ รวมถึงสิ่งที่จะเกิดขึ้นในอนาคต เช่น ช่องโหว่ (Vulnerability), ภัยคุกคาม (Threat), เหตุการณ์ความเสี่ยง (Risk Scenario) ต่าง ๆ, ผลที่จะตามมา (Consequence) ของเหตุการณ์ความเสี่ยงนั้น ๆ และทรัพย์สิน (Asset) ที่จะได้รับผลกระทบจากเหตุการณ์ความเสี่ยง โดยมาตรฐาน ISO/IEC 27005-2022 ได้แบ่งความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ออกเป็น 6 ประเภท ได้แก่

1) ฮาร์ดแวร์ (Hardware)
2) ซอฟต์แวร์ (Software)
3) ระบบเครือข่าย (Network)
4) บุคลากร (Personnel)
5) สถานที่ (Site)
6) องค์กร (Organization)

รูปที่ 4 แสดงตัวอย่างการระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยรายละเอียดของตัวอย่างรหัสความเสี่ยง (Risk ID): RID-001 มีดังนี้

- **ประเภทของความเสี่ยง (Category) :** ฮาร์ดแวร์ (Hardware)
- **รหัสช่องโหว่ (Vulnerability ID – VID) :** VH08
- **ช่องโหว่ (Vulnerability) :** ไม่มีการป้องกันอุปกรณ์บันทึกข้อมูล
- **รหัสภัยคุกคาม (Threat ID – TID) :** TH18
- **ภัยคุกคาม (Threat) :** ใช้งานอุปกรณ์โดยไม่ได้รับอนุญาต
- **รหัสความเสี่ยง (Risk ID) :** RID-001
- **ทรัพย์สินหลักที่มีความเสี่ยง (Primary Asset) :** Business System และ Information
- **ทรัพย์สินสนับสนุนที่มีความเสี่ยง (Supporting Asset) :** Server และ Workstation

รูปที่ 4 : ตัวอย่างการระบุความเสี่ยง (Risk Identification)

1 2

Risk Identification						Risk Identification	Asset												
							Primary Asset					Supporting Asset							Assets
Category	VID	Vulnerability	TID	Threat	Risk ID		Data Center	Business System	Business Application	Cloud Service	Information	Server	Workstation	Firewall	IPS	Switch	Access Point	WLAN Controller	
Hardware	VH08	ไม่มีการป้องกันอุปกรณ์บันทึกข้อมูล	TH18	ใช้งานอุปกรณ์โดยไม่ได้รับอนุญาต	RID-001			x			x	x	x						
			TH28	ข้อมูลถูกขโมย	RID-002			x			x	x	x						
Software	VS19	การควบคุมการเปลี่ยนแปลง (Change Control) ไม่มีประสิทธิภาพ	TT01	ทำให้อุปกรณ์หรือระบบขัดข้อง	RID-003			x	x										
Network																			
Personnel																			
Site																			
Organization																			

6.2.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ คือ การประเมินความเป็นไปได้ของผลกระทบที่อาจเกิดขึ้นจากปัจจัยเสี่ยง โดยความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจะจำแนกความเสี่ยงเป็น 3 มิติ ได้แก่

1) การสูญเสียการเป็นความลับของข้อมูล (Confidentiality: C)
2) การสูญเสียความถูกต้องครบถ้วนของข้อมูล (Integrity: I)
3) การสูญเสียการเข้าถึงข้อมูล (Availability: A)

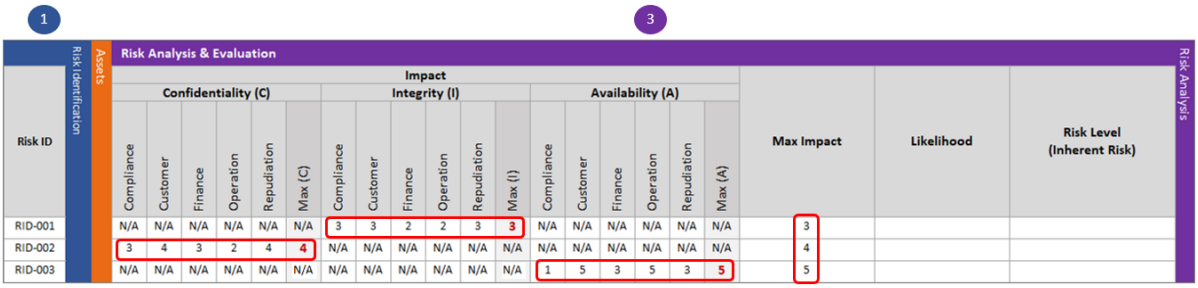
โดย อพวช. ได้กำหนดความเสี่ยงของผลกระทบไว้ 5 ด้าน ดังนี้

1) ด้านการเงิน (Finance)
2) ด้านลูกค้า (Customer)
3) ด้านปฏิบัติการ (Operation)
4) ด้านภาพลักษณ์ (Reputation)
5) ด้านกฎหมาย กฎเกณฑ์ (Compliance)

ในการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ให้พิจารณาปัจจัยเสี่ยงที่ระบุไว้ในส่วนที่ 1 และ 2 ของแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ดังที่แสดงในตัวอย่างการระบุความเสี่ยง (รูปที่ 4 หน้าที่ 12) ตามด้วยการประเมินผลกระทบความรุนแรงของแต่ละปัจจัยเสี่ยงโดยพิจารณากำหนดระดับความรุนแรงของผลกระทบทั้ง 5 ด้าน (Finance, Customer, Operation, Reputation และ Compliance) สำหรับมิติที่มีความเสี่ยงมากที่สุด (C, I หรือ A) และใส่ระดับผลกระทบที่สูงที่สุดของด้านที่มีความเสี่ยงมากที่สุดในช่อง “Max” ในแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

รูปที่ 5 เป็นตัวอย่างการวิเคราะห์ความเสี่ยง สืบเนื่องจากตัวอย่างในรูปที่ 4 โดยการประเมินค่าระดับผลกระทบ (Impact) ให้ใช้ *“เกณฑ์การประเมินผลกระทบ (Impact Criteria)”* (ตารางที่ 1, หน้าที่ 15) ซึ่งจะอธิบายในหัวข้อถัดไป

รูปที่ 5 : ตัวอย่างการวิเคราะห์ความเสี่ยง (Risk Analysis)



			Risk Analysis & Evaluation																				
			Impact																				
			Confidentiality (C)						Integrity (I)						Availability (A)								
Risk ID	Risk Identification	Assets	Compliance	Customer	Finance	Operation	Repudiation	Max (C)	Compliance	Customer	Finance	Operation	Repudiation	Max (I)	Compliance	Customer	Finance	Operation	Repudiation	Max (A)	Max Impact	Likelihood	Risk Level (Inherent Risk)
RID-001			N/A	N/A	N/A	N/A	N/A	N/A	3	3	2	2	3	3	N/A	N/A	N/A	N/A	N/A	N/A	3		
RID-002			3	4	3	2	4	4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	4		
RID-003			N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1	5	3	5	3	5	5		

6.2.3 การประเมินค่าความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยง คือ การประเมินความรุนแรงของผลกระทบ (Impact) โอกาสที่จะเกิด (Likelihood) ของเหตุการณ์ความเสี่ยง และค่าระดับความเสี่ยง (Risk Level) เพื่อประเมินความเสียหายของเหตุการณ์ความเสี่ยง จัดลำดับความสำคัญของความเสี่ยง และดำเนินการจัดการความเสี่ยงตามลำดับความสำคัญ โดยการประเมินความเสี่ยงควรพิจารณาถึงความไม่แน่นอนของเหตุการณ์หรือเงื่อนไขต่าง ๆ ใน 2 ปัจจัย ได้แก่

1) โอกาสที่จะเกิดความเสี่ยง (Likelihood)

การประเมินโอกาสเกิดของความเสี่ยง เป็นการหาข้อมูลเพื่อนำมาสนับสนุนการประมาณการที่ถูกต้อง ซึ่งอาจเป็นความถี่ของเหตุการณ์ที่เกิดขึ้นในอดีตหรือการคาดการณ์โอกาสที่จะเกิดขึ้นในอนาคต ในกรณีที่สามารถหาข้อมูลที่เกี่ยวกับเหตุการณ์ที่เกิดขึ้นในอดีต องค์กรต้องมั่นใจว่าฐานข้อมูลดังกล่าวสามารถบ่งชี้ถึงความเป็นไปได้ของเหตุการณ์ในอนาคตได้

2) ผลกระทบของความเสี่ยง (Impact)

การประเมินความเสี่ยงควรพิจารณาถึงผลกระทบทั้งทางด้านการเงินและที่ไม่ใช่ทางด้านการเงิน ตัวอย่างการวัดผลกระทบที่ไม่ใช่ทางด้านการเงิน ได้แก่ ความพึงพอใจของผู้มีส่วนได้ส่วนเสีย มุมมองของสาธารณชน สภาพแวดล้อมสังคม และผลสำเร็จของการดำเนินงาน เป็นต้น

การนำเอาองค์ประกอบของโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) มาพิจารณาร่วมกันจะทำให้ทราบถึงค่าระดับความเสี่ยง (Risk Level) ซึ่งเป็นตัวชี้วัดความสำคัญของความเสี่ยง และแสดงถึงลำดับความสำคัญในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

รูปที่ 6 แสดงถึงความสัมพันธ์ระหว่างความเสี่ยง (Risk), ผลกระทบ (Impact) และโอกาสที่จะเกิดความเสี่ยง (Likelihood)

รูปที่ 6 : ความสัมพันธ์ระหว่างความเสี่ยง ผลกระทบ และโอกาสที่จะเกิดความเสี่ยง

ความเสี่ยง (Risk) = ผลกระทบ (Impact) x โอกาสที่จะเกิด (Likelihood)

โดย *“เกณฑ์การประเมินผลกระทบ (Impact Criteria)”*, *“เกณฑ์การประเมินโอกาสที่จะเกิด (Likelihood Criteria)”* และ *“เกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria)”* ของ อพวช. มีดังนี้

ตารางที่ 1 : เกณฑ์การประเมินผลกระทบ (Impact Criteria)

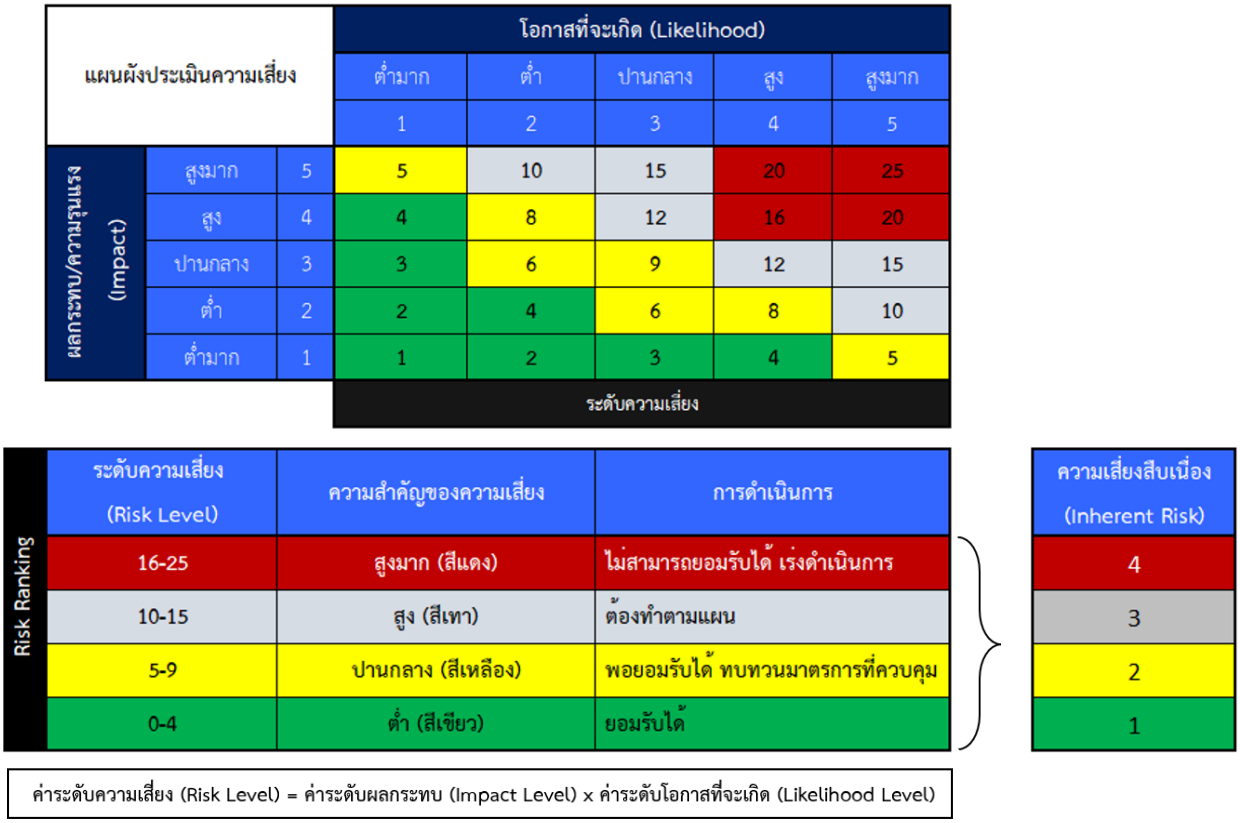
ผลกระทบ	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
1. ด้านการเงิน (Finance)					
1.1. กระทบต่อประมาณการรายได้	สูญเสียเงินหรือทรัพย์สินน้อยกว่า 1 ล้านบาท	สูญเสียเงินหรือทรัพย์สินมากกว่า 1 ล้านบาท แต่ไม่เกิน 5 ล้านบาท	สูญเสียเงินหรือทรัพย์สินมากกว่า 5 ล้านบาท แต่ไม่เกิน 10 ล้านบาท	สูญเสียเงินหรือทรัพย์สินมากกว่า 10 ล้านบาท แต่ไม่เกิน 20 ล้านบาท	สูญเสียเงินหรือทรัพย์สินมากกว่า 20 ล้านบาท แต่ไม่เกิน 30 ล้านบาท
1.2. ค่าใช้จ่าย	น้อยกว่า 1 หมื่นบาท	1 หมื่นบาท - 1 แสนบาท	1 แสนบาท - 5 แสนบาท	5 แสนบาท - 1 ล้านบาท	มากกว่า 1 ล้านบาท
2. ด้านลูกค้า (Customer)	มีผลกระทบต่อการให้บริการลูกค้า หรือไม่สามารถให้บริการต่าง ๆ ได้ ไม่เกิน 10 ราย	มีผลกระทบต่อการให้บริการลูกค้าน้อย หรือ ไม่สามารถให้บริการต่าง ๆ ได้ มากกว่า 10-30 ราย	มีผลกระทบต่อการให้บริการลูกค้าปานกลาง หรือไม่สามารถให้บริการต่าง ๆ ได้มากกว่า 30-50 ราย	มีผลกระทบต่อการให้บริการลูกค้ามาก หรือ ไม่สามารถให้บริการต่าง ๆ ได้มากกว่า 50-100 ราย	มีผลกระทบต่อการให้บริการลูกค้าสูงมาก หรือ ไม่สามารถให้บริการต่างๆ ได้มากกว่า 100 ราย
3. ด้านปฏิบัติการ (Operation)	ระบบฐานข้อมูลหยุดชะงักแต่สามารถแก้ไขให้ใช้งานได้ภายในระยะเวลา 1 ชั่วโมง	ระบบฐานข้อมูลหยุดชะงักแต่สามารถแก้ไขให้ใช้งานได้ภายในระยะเวลา 4 ชั่วโมง	ระบบฐานข้อมูลหยุดชะงักแต่สามารถแก้ไขให้ใช้งานได้ภายในระยะเวลา 12 ชั่วโมง	ระบบฐานข้อมูลหยุดชะงักแต่สามารถแก้ไขให้ใช้งานได้ภายในระยะเวลา 24 ชั่วโมง	ระบบฐานข้อมูลหยุดชะงักไม่สามารถให้ใช้งานได้ เกินระยะเวลา 24 ชั่วโมง
4. ด้านภาพลักษณ์ (Reputation)	มีการเผยแพร่ข่าวในวงจำกัดภายใน และไม่ส่งผลกระทบต่อชื่อเสียงของ อพวช.	• มีการเผยแพร่ข่าวในทางลบทางสื่อต่าง ๆ เช่น สื่อออนไลน์ หรือสิ่งพิมพ์ และ • มีผลกระทบต่อชื่อเสียงของ อพวช. บ้างเล็กน้อย ไม่เกิน 1 วัน	• มีการเผยแพร่ข่าวในทางลบทางสื่อต่าง ๆ เช่น สื่อออนไลน์ หรือสิ่งพิมพ์ และ • มีผลกระทบต่อชื่อเสียงของ อพวช. บ้างเล็กน้อย 1-7 วัน	• มีการเผยแพร่ข่าวในทางลบทางสื่อต่าง ๆ เช่น สื่อออนไลน์ หรือสิ่งพิมพ์ และ • มีผลกระทบต่อชื่อเสียงของ อพวช. อย่างต่อเนื่อง 7-30 วัน	• มีการเผยแพร่ข่าวในทางลบทางสื่อต่าง ๆ เช่น สื่อออนไลน์ หรือสิ่งพิมพ์ และ • มีผลกระทบต่อชื่อเสียงของ อพวช. อย่างต่อเนื่อง มากกว่า 30 วัน

ผลกระทบ	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
5. ด้านกฎหมาย กฎเกณฑ์ (Compliance)	ไม่มีการตักเตือนจากหน่วยงานราชการหรือหน่วยงานกำกับดูแล	ได้รับหนังสือให้ข้อเสนอแนะ/คำแนะนำจากหน่วยงานราชการหรือหน่วยงานกำกับดูแล	ได้รับหนังสือตักเตือนจากหน่วยงานราชการหรือหน่วยงานกำกับดูแล โดยจะต้องทำหนังสือชี้แจงเหตุผลและแนวทางการแก้ไขต่อหน่วยงานดังกล่าว	• ได้รับหนังสือตักเตือนจากหน่วยงานราชการหรือหน่วยงานกำกับดูแล โดยจะต้องเข้าชี้แจงเหตุผลและแนวทางแก้ไขต่อหน่วยงานดังกล่าว หรือ • มีการกระทำที่เข้าข่ายให้ อพวช. ต้องจ่ายค่าปรับหรือชดใช้ค่าเสียหาย	• มีการกระทำที่เข้าข่ายความผิดทางอาญา/ทางปกครองหรือจะถูกคำสั่งตามกฎหมายให้หยุดดำเนินธุรกิจ หรือ • เพิกถอนใบอนุญาตประกอบวิชาชีพ/ใบอนุญาตประกอบธุรกิจ หรือ • เพิกถอนการจดทะเบียนของ อพวช.

ตารางที่ 2 : เกณฑ์การประเมินโอกาสที่จะเกิด (Likelihood Criteria)

โอกาสเกิด	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
เชิงคุณภาพ	มีโอกาสเกิดน้อยมาก หรือในกรณีที่ไม่สามารถประเมินได้	มีโอกาสเกิดแต่นาน ๆ ครั้ง	มีโอกาสเกิดบางครั้ง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อย ๆ	มีโอกาสในการเกิดเกือบทุกครั้ง
เชิงปริมาณ	มากกว่า 4 ปี	ภายใน 3-4 ปี	ภายใน 2 ปี	ภายใน 1 ปี	ทุกเดือน
	น้อยกว่า 49%	น้อย 50-59%	ปานกลาง 60-69%	สูง 70-79%	มากกว่า 80%

รูปที่ 7 : เกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria)



แผนผังประเมินความเสี่ยง			โอกาสที่จะเกิด (Likelihood)				
			ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก
			1	2	3	4	5
ผลกระทบ (Impact)	สูงมาก	5	5	10	15	20	25
	สูง	4	4	8	12	16	20
	ปานกลาง	3	3	6	9	12	15
	ต่ำ	2	2	4	6	8	10
	ต่ำมาก	1	1	2	3	4	5
			ระดับความเสี่ยง				

Risk Ranking	ระดับความเสี่ยง (Risk Level)	ความสำคัญของความเสี่ยง	การดำเนินการ	ความเสี่ยงสืบเนื่อง (Inherent Risk)
	16-25	สูงมาก (สีแดง)	ไม่สามารถยอมรับได้ เร่งดำเนินการ	4
	10-15	สูง (สีเทา)	ต้องทำตามแผน	3
	5-9	ปานกลาง (สีเหลือง)	พอยอมรับได้ ทบทวนมาตรการที่ควบคุม	2
	0-4	ต่ำ (สีเขียว)	ยอมรับได้	1

ค่าระดับความเสี่ยง (Risk Level) = ค่าระดับผลกระทบ (Impact Level) x ค่าระดับโอกาสที่จะเกิด (Likelihood Level)

เกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria) ได้จัดลำดับความรุนแรงของแต่ละระดับความเสี่ยง (Risk Ranking) เป็นช่วงระดับความเสี่ยงและใช้สัญลักษณ์สี ได้แก่ สีแดง สีเทา สีเหลือง และสีเขียว เพื่อนำมาวิเคราะห์เปรียบเทียบกับเกณฑ์ความสามารถในการยอมรับความเสี่ยง (Risk Acceptance Criteria) โดยเกณฑ์ความสามารถในการยอมรับความเสี่ยง (Risk Acceptance Criteria) ของ อพวช. เป็นดังนี้

ตารางที่ 3 : เกณฑ์ความสามารถในการยอมรับความเสี่ยง (Risk Acceptance Criteria)

ระดับความเสี่ยง	ช่วงระดับคะแนน	ความสามารถในการยอมรับความเสี่ยง
สูงมาก (Very High) (สีแดง)	16-25	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
สูง (High) (สีเทา)	10-15	ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
ปานกลาง (Medium) (สีเหลือง)	5-9	ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
ต่ำ (Low) (สีเขียว)	1-4	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง และไม่จำเป็นต้องมีการจัดการเพิ่มเติม

- **ความเสี่ยงที่อยู่ในโซนสีแดง** (โอกาส x ผลกระทบ ช่วงระดับคะแนนความเสี่ยงที่อยู่ระหว่าง 16-25 คะแนน) เป็นความเสี่ยงที่อยู่ในระดับที่ไม่สามารถยอมรับได้ จะต้องมีการกำหนดมาตรการในการจัดการความเสี่ยงเพิ่มเติมโดยทันที โดยใช้กลยุทธ์การลด/ควบคุมความเสี่ยง (Mitigation) กระจาย/โอนความเสี่ยง (Transfer) หรือหลีกเลี่ยงความเสี่ยง (Avoidance) พร้อมกำหนดผู้รับผิดชอบและกรอบระยะเวลาที่ชัดเจน
- **ความเสี่ยงที่อยู่ในโซนสีเทา** (โอกาส x ผลกระทบ ช่วงระดับคะแนนความเสี่ยงที่อยู่ระหว่าง 10-15 คะแนน) เป็นความเสี่ยงที่อยู่ในระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์การลด/ควบคุมความเสี่ยง (Mitigation) หรือกระจาย/โอนความเสี่ยง (Transfer) พร้อมกำหนดผู้รับผิดชอบและกรอบระยะเวลาที่ชัดเจน โดยลำดับความสำคัญในการดำเนินงานให้น้อยกว่าโซนสีแดง
- **ความเสี่ยงที่อยู่ในโซนสีเหลือง** (โอกาส X ผลกระทบ ช่วงระดับคะแนนความเสี่ยงที่อยู่ระหว่าง 5-9 คะแนน) เป็นความเสี่ยงที่อยู่ในระดับพอยอมรับได้ (Acceptance) แต่ต้องมีการควบคุม โดยกำหนดผู้รับผิดชอบและกรอบระยะเวลาที่ชัดเจน ทั้งนี้ต้องมีการปฏิบัติตามรับการควบคุมภายในอย่างเคร่งครัด เพื่อไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่รับไม่ได้
- **ความเสี่ยงที่อยู่ในโซนสีเขียว** (โอกาส X ผลกระทบ ช่วงระดับคะแนนความเสี่ยงที่อยู่ระหว่าง 1-4 คะแนน) เป็นความเสี่ยงที่อยู่ในระดับที่ยอมรับได้ (Acceptance) ไม่จำเป็นต้องมีมาตรการจัดการเพิ่มเติมใด ๆ กับความเสี่ยงที่เกิดขึ้น ในทางกลับกันอาจมีการทบทวนระบบควบคุมภายในใหม่เพื่อผ่อนคลายการควบคุมได้ระดับหนึ่ง

รูปที่ 8 เป็นตัวอย่างการประเมินค่าความเสี่ยง สืบเนื่องจากตัวอย่างในรูปที่ 5 (หน้าที่ 13) โดยระดับผลกระทบในช่อง “Max Impact” ได้แก่ ค่าระดับผลกระทบของความเสี่ยงในด้าน (Finance, Customer, Operation, Reputation หรือ Compliance) ที่มีผลกระทบสูงสุด ของมิติ (C, I หรือ A) ที่มีความเสี่ยงมากที่สุด โดยค่าระดับความเสี่ยง (Risk Level) ที่ได้จากการประเมินผลกระทบที่สูงที่สุด (Max Impact) และโอกาสที่จะเกิดความเสี่ยง (Likelihood) ในส่วนที่ 3 ของแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เป็นค่าระดับของความเสี่ยงสืบเนื่อง (Inherent Risk) ซึ่งเป็นค่าระดับความเสี่ยงก่อนที่จะมีการควบคุมหรือการจัดการความเสี่ยง

รูปที่ 8 : ตัวอย่างการประเมินค่าความเสี่ยง (Risk Evaluation)

1 3

Risk Identification	Assets	Risk Analysis & Evaluation																			Risk Analysis
		Impact																			
		Confidentiality (C)						Integrity (I)						Availability (A)							
Risk ID		Compliance	Customer	Finance	Operation	Repudiation	Max (C)	Compliance	Customer	Finance	Operation	Repudiation	Max (I)	Compliance	Customer	Finance	Operation	Repudiation	Max (A)	Max Impact	Likelihood	Risk Level (Inherent Risk)
RID-001		N/A	N/A	N/A	N/A	N/A	N/A	3	3	2	2	3	3	N/A	N/A	N/A	N/A	N/A	N/A	3	3	9
RID-002		3	4	3	2	4	4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	4	3	12
RID-003		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1	5	3	5	3	5	5	4	20

ดังที่แสดงในตัวอย่างด้านบน ค่าระดับความเสี่ยงของ RID-001 คือ 9 ซึ่งอยู่ในโซนสีเหลือง เป็นระดับที่พอยอมรับได้แต่ต้องมีการควบคุมเพื่อลดความเสี่ยง ส่วนค่าระดับความเสี่ยงของ RID-002 คือ 12 ซึ่งอยู่ในโซนสีเทา เป็นระดับที่ไม่สามารถยอมรับได้และต้องได้รับการควบคุมเพื่อลดความเสี่ยง และค่าระดับความเสี่ยงของ RID-003 คือ 20 ซึ่งอยู่ในโซนสีแดง เป็นระดับที่ไม่สามารถยอมรับได้ ต้องได้รับการควบคุมเพื่อลดความเสี่ยงหรือหลีกเลี่ยงความเสี่ยง

ขั้นตอนถัดไปของการประเมินความเสี่ยง ได้แก่ การประเมินมาตรการควบคุมพร้อมทั้งประสิทธิผลของการควบคุมที่องค์กรมี โดยการควบคุมสามารถแบ่งออกเป็น 3 หมวดหมู่ คือ

1) **การควบคุมด้านบริหารจัดการ (Administrative Control)** หมายถึง การควบคุมด้วยนโยบาย ระเบียบ ขั้นตอน วิธีการปฏิบัติงาน และแนวทางการดำเนินการเพื่อการบริหารจัดการ ปรับใช้ และบำรุงรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ
2) **การควบคุมด้านเทคนิค (Technical Control)** หมายถึง การควบคุมด้วยเทคนิคหรือเครื่องมือเทคโนโลยี เพื่อปกป้องทรัพย์สิน (Asset) ที่สำคัญขององค์กร
3) **การควบคุมทางกายภาพ (Physical Control)** หมายถึง การควบคุมทางกายภาพที่จะปกป้องทรัพย์สิน (Asset) ที่สำคัญขององค์กรจากการถูกบุกรุก ถูกทำลาย หรือภัยธรรมชาติ

ซึ่งการควบคุม (Control) ดังกล่าวข้างต้น เป็นวิธีการจัดการความเสี่ยง ช่วยให้ค่าระดับความเสี่ยง (Risk Level) ลดลง โดยค่าระดับความเสี่ยงที่ลดลงขึ้นอยู่กับประสิทธิผลของมาตรการควบคุมที่เลือกใช้

รูปที่ 9 แสดงถึงความสัมพันธ์ระหว่างความเสี่ยงที่เหลืออยู่ (Residual Risk), ความเสี่ยงสืบเนื่อง (Inherent Risk) และประสิทธิผลของการควบคุม (Control Effectiveness)

รูปที่ 9 : ความสัมพันธ์ระหว่างความเสี่ยงที่เหลืออยู่ ความเสี่ยงสืบเนื่อง และประสิทธิผลของการควบคุม

ความเสี่ยงที่เหลืออยู่ (Residual Risk) = ความเสี่ยงสืบเนื่อง (Inherent Risk) x ประสิทธิผลของการควบคุม (Control Effectiveness)

การประเมินค่าระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) สามารถประเมินได้จาก *“เกณฑ์การประเมินประสิทธิผลของการควบคุม (Control Effectiveness Criteria)”*, *“เกณฑ์ค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk Mapping)”* และ *“เกณฑ์การประเมินความเสี่ยงที่เหลืออยู่ (Residual Risk Criteria)”* ดังนี้

ตารางที่ 4 : เกณฑ์การประเมินประสิทธิผลของการควบคุม (Control Effectiveness Criteria)

ระดับประสิทธิผลของการควบคุม		รายละเอียดการควบคุม
สูง (High)	1	มีมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศครบถ้วน สอดคล้องกับมาตรการควบคุม (Control) ใน Annex A ของมาตรฐาน ISO/IEC 27001
ปานกลาง (Medium)	2	มีมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับมาตรการควบคุม (Control) ใน Annex A ของมาตรฐาน ISO/IEC 27001 บางส่วนที่พอยอมรับได้ จำเป็นต้องทบทวนมาตรการควบคุม
ต่ำ (Low)	3	มาตรการควบคุม (Control) ที่มีอยู่ไม่เพียงพอ จำเป็นต้องทำแผนเพื่อบรรเทาความเสี่ยง เพิ่มมาตรการควบคุมให้ครอบคลุมทั้ง Administrative, Technical และ/หรือ Physical Controls

ตารางที่ 5 : เกณฑ์ค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk Mapping)

ระดับความเสี่ยง (Risk Level)	ค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk Level)
สูงมาก (สีแดง) 16-25	4
สูง (สีเทา) 10-15	3
ปานกลาง (สีเหลือง) 5-9	2
ต่ำ (สีเขียว) 1-4	1

รูปที่ 10 : เกณฑ์การประเมินความเสี่ยงที่เหลืออยู่ (Residual Risk)

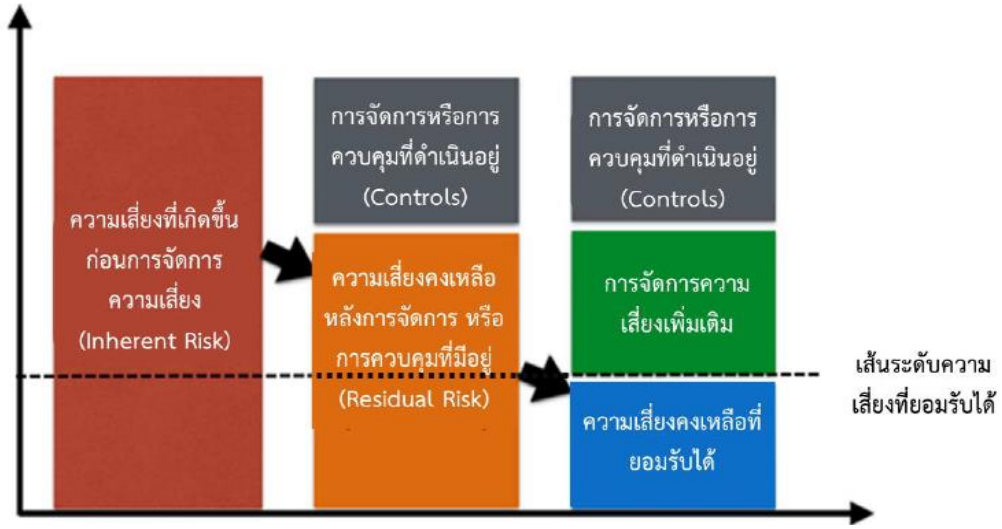
แผนผังประเมินความเสี่ยงที่เหลืออยู่หลังการควบคุม			ระดับประสิทธิผลของการควบคุม (Control Effectiveness)		
			Low	Medium	High
			3	2	1
ความเสี่ยงสืบเนื่อง (Inherent Risk)	Very High	4	**12**	**8**	**4**
	High	3	**9**	**6**	**3**
	Medium	2	**6**	**4**	**2**
	Low	1	**3**	**2**	**1**
			ระดับความเสี่ยงที่เหลืออยู่ (Residual Risk)		

ค่าระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) = ค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk) x ค่าระดับประสิทธิผลของการควบคุม (Control Effectiveness)

<u>หมายเหตุ</u> *"เกณฑ์การประเมินประสิทธิผลของการควบคุม (Control Effectiveness Criteria)", "เกณฑ์ค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk Mapping)"* และ *"เกณฑ์การประเมินความเสี่ยงที่เหลืออยู่ (Residual Risk Criteria)"* ใช้สำหรับความเสี่ยงที่มีการควบคุม (Control) เท่านั้น เมื่อมีการควบคุม (Control) จึงจะสามารถประเมินค่าระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) ได้

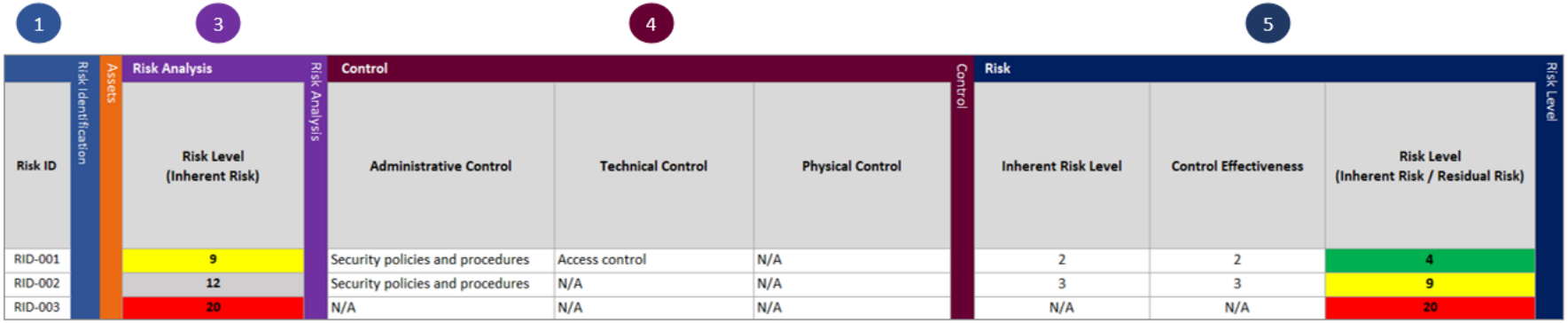
รูปที่ 11 แสดงความสัมพันธ์ของความเสี่ยงสืบเนื่อง (Inherent Risk) และความเสี่ยงที่เหลืออยู่ (Residual Risk) หลังการควบคุม (Control)

รูปที่ 11 : ความเสี่ยงก่อนและหลังการจัดการความเสี่ยง



รูปที่ 12 เป็นตัวอย่างการระบุมาตรการควบคุม (Control) ที่องค์กรมีอยู่ และระดับความเสี่ยง (Risk Level) ก่อนและหลังการควบคุม ซึ่งอยู่ในส่วนที่ 4 และ 5 ของแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

รูปที่ 12 : ตัวอย่างการระบุมาตรการควบคุม (Control) และค่าระดับความเสี่ยง (Risk Level)



ค่าระดับความเสี่ยง (Risk Level) ที่ระบุในส่วนที่ 5 ของแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อาจเป็นค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk) หรือค่าระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) ขึ้นอยู่กับความเสี่ยงนั้นว่ามีการควบคุม (Control) หรือไม่ หากความเสี่ยงไม่มีการควบคุม ค่าระดับความเสี่ยง (Risk Level) ในส่วนที่ 5 จะยังคงเป็นค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk) ดังเช่นตัวอย่างสุดท้ายในรูปที่ 12 โดยค่าระดับความเสี่ยง (Risk Level) ของ Risk ID: RID-003 มีค่าเป็น 20 ทั้งในส่วนที่ 3 และ 5 ของแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ในกรณีที่ความเสี่ยงมีการควบคุมทางด้านบริหารจัดการ (Administrative Control), ทางด้านเทคนิค (Technical Control) และ/หรือ ทางด้านกายภาพ (Physical Control) ให้พิจารณาประสิทธิผลของการควบคุมตาม *“เกณฑ์การประเมินประสิทธิผลของการควบคุม (Control Effectiveness Criteria)”* (ตารางที่ 4 หน้าที่ 20) ตามด้วยการปรับค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk Level) ตาม *“เกณฑ์ค่าระดับความเสี่ยงสืบเนื่อง (Inherent Risk Mapping)”* (ตารางที่ 5 หน้าที่ 20) และประเมินความเสี่ยงที่เหลืออยู่ (Residual Risk) ตาม *“เกณฑ์การประเมินความเสี่ยงที่เหลืออยู่ (Residual Risk)”* (รูปที่ 10 หน้าที่ 21)

หลังจากได้ค่าระดับความเสี่ยง (Risk Level) แล้ว ให้นำผลการประเมินเปรียบเทียบกับ *“เกณฑ์ความสามารถในการยอมรับความเสี่ยง”* (ตารางที่ 3 หน้าที่ 17) เพื่อกำหนดวิธีการจัดการความเสี่ยงต่อไป

6.3 การจัดการความเสี่ยง (Risk Treatment)

เมื่อความเสี่ยงได้รับการบ่งชี้และค่าระดับความเสี่ยง (Risk Level) ของแต่ละเหตุการณ์ความเสี่ยงได้ถูกประเมินและเปรียบเทียบกับ *"เกณฑ์ความสามารถในการยอมรับความเสี่ยง (Risk Acceptance Criteria)"* (ตารางที่ 3 หน้าที่ 17) แล้ว ให้ดำเนินการตอบโต้ต่อเหตุการณ์ความเสี่ยงตาม *"เกณฑ์การรับมือกับความเสี่ยง"* ดังที่แสดงในตารางที่ 6 เพื่อจัดลำดับความสำคัญของความเสี่ยงและกำหนดวิธีการดำเนินการต่าง ๆ กับความเสี่ยงแต่ละรายการตามความเหมาะสม เพื่อให้ความเสี่ยงเหล่านั้นอยู่ในระดับที่องค์กรยอมรับได้

ตารางที่ 6 : เกณฑ์การรับมือกับความเสี่ยง

ระดับความเสี่ยง (Risk Level)	การตอบโต้ความเสี่ยง (Risk Response)	ลำดับความสำคัญ (Priority)
16-25	หลีกเลี่ยงความเสี่ยง (Avoidance) ลดความเสี่ยง (Mitigation) โอนความเสี่ยง (Transfer)	สูง (High)
10-15	ลดความเสี่ยง (Mitigation) โอนความเสี่ยง (Transfer)	ปานกลาง (Medium)
5-9	ยอมรับความเสี่ยง (Acceptance) ***ต้องมีการควบคุม*	ต่ำ (Low)
0-4	ยอมรับความเสี่ยง (Acceptance)	N/A

หลังจากการพิจารณาผลการประเมินค่าระดับความเสี่ยง (Risk Level) เลือกวิธีการตอบโต้ความเสี่ยง (Risk Response) และจัดลำดับความสำคัญของความเสี่ยง (Priority) เรียบร้อยแล้ว ให้ดำเนินการจัดทำแผนการจัดการความเสี่ยง (Risk Treatment Plan) โดยกำหนดกลยุทธ์และมาตรการเพื่อควบคุมผลกระทบและโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงที่ได้ประเมินไว้ และพิจารณากำหนดกิจกรรมการควบคุมความเสี่ยงที่เหมาะสมสำหรับแต่ละรายการความเสี่ยง พร้อมทั้งนำเสนอต่อผู้บริหาร แจ้งเหตุผลการเลือกวิธีดำเนินการจัดการความเสี่ยงให้ผู้บริหารทราบเพื่อการตัดสินใจในการยอมรับความเสี่ยง และเพื่อให้อนุมัติแผนการจัดการความเสี่ยง (Risk Treatment Plan) ในลำดับถัดไป โดยเจ้าของความเสี่ยง (Risk Owner) จะเป็นผู้รับผิดชอบต่อการจัดการความเสี่ยงที่อยู่ในความรับผิดชอบของตนให้เป็นไปตามแผนการจัดการความเสี่ยงที่กำหนดไว้

รูปที่ 13 เป็นตัวอย่างการจัดการความเสี่ยง (Risk Treatment) สืบเนื่องจากตัวอย่างในรูปที่ 12 (หน้าที่ 22) โดยการจัดการความเสี่ยง (Risk Treatment) ซึ่งอยู่ในส่วนที่ 6 ของแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย

- การตอบโต้ความเสี่ยง (Risk Response)
- หมายเลขแผนการจัดการความเสี่ยง (Treatment Plan No.)
- ลำดับความสำคัญ (Priority)
- เจ้าของความเสี่ยง (Risk Owner)
- มาตรการควบคุมใน ISO/IEC 27001, Annex A ที่เลือกใช้ (ISO/IEC 27001 Annex A Reference Controls)

รูปที่ 13 : ตัวอย่างการจัดการความเสี่ยง (Risk Treatment)

1 5 6

	Risk Identification	Assets	Risk Analysis	Control	Risk			Risk Level	Risk Treatment					Risk Treatment
Risk ID					Inherent Risk Level	Control Effectiveness	Risk Level (Inherent Risk / Residual Risk)		Risk Response	Treatment Plan No.	Priority	Risk Owner	ISO/IEC 27001 Annex A Reference Controls	
RID-001					2	2	4		Acceptance	N/A	N/A	IT Department	N/A	
RID-002					3	3	9		Mitigation	RTP-100	Low	IT Department	A.9.2.2, A.9.4.1, A.9.4.2	
RID-003					N/A	N/A	20		Mitigation	RTP-101	High	IT Department	A.12.1.2, A.14.2.2, A.14.2.3	

การตัดสินใจเลือกมาตรการควบคุมเพื่อลดความเสี่ยง อาจพิจารณาถึงความเป็นไปได้และค่าใช้จ่ายของแต่ละทางเลือกเพื่อการควบคุมที่เหมาะสม โดยพิจารณาจากประเด็นต่าง ๆ ดังนี้

1) พิจารณาระดับความเสี่ยง (Risk Level) และกำหนดวิธีการตอบโต้ความเสี่ยง (Risk Response) เพื่อให้มั่นใจว่าความเสี่ยงอยู่ในระดับที่ยอมรับได้
2) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการความเสี่ยงกับผลประโยชน์หรือความคุ้มค่าที่จะได้รับจากการจัดการความเสี่ยงดังกล่าว
3) ในกรณีที่เลือกกำหนดกิจกรรมการควบคุมเพื่อลดความเสี่ยง ให้กำหนดวิธีควบคุม (Control) ในแผนการจัดการความเสี่ยง (Risk Treatment Plan) และอ้างอิงหมายเลขแผนการจัดการความเสี่ยง (Treatment Plan No.) ในแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมทั้งระบุเจ้าของความเสี่ยง (Risk Owner) และมาตรการควบคุมที่เลือกใช้ใน ISO/IEC 27001, Annex A

6.4 การสื่อสารและการปรึกษา (Communication & Consultation)

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ต้องมีการสื่อสารอย่างเหมาะสมทั้งในรูปแบบและกรอบเวลาเพื่อช่วยให้บุคลากรที่เกี่ยวข้องสามารถดำเนินงานตามความรับผิดชอบของตนได้ โดยการสื่อสารอย่างมีประสิทธิผลต้องประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงการแลกเปลี่ยนข้อมูลกับบุคคลภายนอกองค์กร เช่น เจ้าหน้าที่ของหน่วยงานอื่น ๆ หน่วยงานกำกับดูแลด้านกฎหมาย ผู้ให้บริการ หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ เป็นต้น

6.5 การติดตามผลและทบทวน (Monitoring and Review)

เมื่อสภาพแวดล้อมหรือเป้าหมายการดำเนินงานขององค์กรมีการเปลี่ยนแปลง วิธีการจัดการความเสี่ยงที่กำหนดไว้อาจจะไม่เหมาะสม กิจกรรมควบคุมความเสี่ยงอาจมีประสิทธิภาพน้อยลง ดังนั้น อพวช. จึงต้องมีการติดตามตรวจสอบว่าการบริหารความเสี่ยงในแต่ละขั้นตอนยังคงมีประสิทธิภาพ โดยศึกษาและวิเคราะห์ปัจจัยเสี่ยง เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้นกับ อพวช. และองค์กรอื่น

การตรวจสอบและทบทวนเป็นการกำกับติดตามเพื่อให้มั่นใจว่าการบริหารความเสี่ยงขององค์กรจะดำเนินไปในแนวทางที่นำไปสู่ความสำเร็จตามวัตถุประสงค์ขององค์กร โดยการติดตามการบริหารความเสี่ยงสามารถทำได้ 2 ลักษณะ คือ

1) การติดตามผลอย่างต่อเนื่อง
2) การติดตามผลเป็นรายครั้ง

การติดตามผลการดำเนินงาน มาตรการควบคุม หรือแนวทางที่ใช้ปฏิบัติในการบรรเทาความเสี่ยง หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ให้จัดทำแผนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมรายงานผลการวิเคราะห์ ผลการประเมิน รวมถึงวิธีการจัดการความเสี่ยง และนำเสนอต่อผู้บริหารเพื่อทราบ

ประเด็นสำคัญของการติดตามผลและทบทวน ได้แก่

- การติดตามผลและทบทวนเพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงมีความเหมาะสม มีคุณภาพ และมีประสิทธิภาพ
- ความเสี่ยงทั้งหมดที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรได้รับการรายงานต่อผู้บริหารที่รับผิดชอบ

6.6 การบันทึกรายงานผล (Recording & Reporting)

ส่วนงานหลักที่รับผิดชอบในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่ในการรายงานผลการบริหารความเสี่ยงต่อคณะทำงานบริหารความเสี่ยงองค์กร โดยข้อมูลที่เกี่ยวข้องกับการบริหารความเสี่ยงจะต้องถูกระบุ บันทึก และจัดเก็บอย่างเป็นระบบ เพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ บันทึกรายงานผลควรครอบคลุมอย่างน้อย ดังนี้

- รายงานผลการประเมินและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- แผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- สถานะและผลลัพธ์การดำเนินงานตามแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

7. เอกสารสำหรับบันทึก

ลำดับที่	รหัสเอกสาร	ชื่อเอกสาร
1		แบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Risk Assessment Form)
2		แผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Risk Treatment Form)

8. เอกสารที่เกี่ยวข้อง

ลำดับที่	รหัสเอกสาร	ชื่อเอกสาร
1		แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Implementation Guideline) ประจำปี 2566
2		แผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ ฉบับปรับปรุงปี 2566
3		มาตรฐาน ISO/IEC 27005-2022 (Information Security, Cybersecurity and Privacy protection –Guidance on Managing Information Security Risks)