แนวทางการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

(IT Risk Management Practice)

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

พฤศจิกายน 2562

สารบัญ

1. บทนำ

ในปัจจุบันความก้าวหน้าของเทคโนโลยีสารสนเทศมีบทบาทอย่างมากในการขับเคลื่อนธุรกิจในตลาดทุนไทย ในขณะเดียวกันความซับซ้อนและขยายตัวทางด้านเทคโนโลยีสารสนเทศนี้ทำให้ผู้ประกอบธุรกิจเผชิญความเสี่ยงต่าง ๆ ในหลายมิติมากขึ้น ได้แก่ ความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ซึ่งหมายถึง ความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจ และความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ ทั้งนี้ ความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเดิมถือเป็นส่วนหนึ่งของความเสี่ยงด้านปฏิบัติการ แต่ในปัจจุบันความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงที่มีความสำคัญมากขึ้นสืบเนื่องจากโครงการการลงทุนทางด้านเทคโนโลยีสารสนเทศที่นับวันจะยิ่งมีจำนวนมากขึ้น รวมทั้งภัยคุกคามทางด้านเทคโนโลยีสารสนเทศ หรือทางด้านไซเบอร์ที่ได้ส่งผลกระทบต่อการดำเนินธุรกิจ ชื่อเสียง และความเชื่อมั่นในการใช้บริการและผลิตภัณฑ์ต่าง ๆ ในตลาดทุน

แนวทางการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน”) ในการส่งเสริมให้ผู้ประกอบธุรกิจยกระดับการให้ความสำคัญด้านการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตั้งแต่การวางกรอบนโยบายที่ชัดเจน การระบุความเสี่ยง การประเมินความเสี่ยง รวมถึงการบริหารและจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่องค์กรยอมรับได้ ทั้งนี้ เพื่อสร้างความมั่นใจในการใช้บริการและผลิตภัณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของตลาดทุนในภาพรวม รวมทั้งยังช่วยเสริมสร้างความเชื่อมั่นต่อมาตรฐานการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจ ให้เป็นที่ยอมรับในระดับสากล

1.1 <u>วัตถุประสงค์</u>

แนวทางปฏิบัติเกี่ยวกับการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศได้จัดทำขึ้นเพื่อเป็นแนวทางในการวางกรอบและกระบวนการการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจในการปฏิบัติตามหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศ ซึ่งการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศถือเป็นส่วนสำคัญในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ โดยมุ่งเน้นให้ผู้ประกอบธุรกิจมีการกำหนดนโยบาย กระบวนการ และบทบาทหน้าที่อย่างเหมาะสมในการบริหารและจัดการความเสี่ยง โดยพิจารณาถึงลักษณะความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ 3 ประการ ได้แก่

- ความเสี่ยงอันเนื่องมาจากการพลาดโอกาสในการใช้เทคโนโลยีสารสนเทศให้เกิดประสิทธิภาพ และประสิทธิผลต่อการดำเนินงาน หรือสร้างนวัตกรรมให้แก่องค์กร รวมถึงความเสี่ยงอันเนื่องมาจากเทคโนโลยีสารสนเทศที่ไม่ตอบสนองต่อการดำเนินธุรกิจ ซึ่งส่งผลโดยตรงต่อศักยภาพในการแข่งขันของผู้ประกอบธุรกิจ (IT Benefits/Value Enhancement Risk)
- ความเสี่ยงอันเนื่องมาจากการไม่สามารถนำเทคโนโลยีสารสนเทศมาใช้ในการพัฒนาบริการหรือผลิตภัณฑ์ใหม่ โดยรวมถึงความเสี่ยงที่ไม่สามารถจัดการโครงการได้อย่างมีประสิทธิภาพ หรือตามเป้าหมายที่กำหนด (IT Programme and Project Delivery Risk)
- ความเสี่ยงอันเนื่องมาจากการปฏิบัติงานประจำวันทางด้านเทคโนโลยีสารสนเทศ เช่น ความเสี่ยงสืบเนื่องมาจากการควบคุมที่ไม่เพียงพอ หรือมีการดำเนินงานที่อาจขัดต่อกฎหมายและระเบียบข้อบังคับต่าง ๆ (IT Operations and Services Delivery Risk)

โดยเมื่อผู้ประกอบธุรกิจมีการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่เพียงพอเหมาะสมแล้ว ย่อมส่งผลต่อองค์กรในการสร้างความมั่นใจในการปรับใช้หรือพัฒนาเทคโนโลยีสารสนเทศ ในบริการหรือผลิตภัณฑ์ใหม่ รวมทั้งเสริมสร้างหรือพัฒนากระบวนการการดำเนินธุรกิจในปัจจุบัน นอกจากนี้ ยังเป็นการสร้างข้อได้เปรียบทางด้านธุรกิจที่ยั่งยืน เนื่องจาก

- ผู้ประกอบธุรกิจสามารถระบุความเสี่ยงทางด้านเทคโนโลยีสารสนเทศได้อย่างชัดเจนมากขึ้น รวมถึงสามารถวัดระดับของความเสี่ยงที่ระบุไว้
- ผู้ประกอบธุรกิจสามารถเข้าใจถึงผลกระทบของความเสี่ยงทางด้านเทคโนโลยีสารสนเทศต่อองค์กร
- ผู้ประกอบธุรกิจสามารถประเมินประโยชน์และโอกาสเกิดของความเสี่ยงในการลงทุนทางด้านเทคโนโลยีสารสนเทศ
- ผู้ประกอบธุรกิจที่มีกระบวนการบริหารและจัดการความเสี่ยงที่มีประสิทธิผลส่งผลต่อความมีประสิทธิภาพและประสิทธิผลของกระบวนการทางธุรกิจ
- ผู้ประกอบธุรกิจมีการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศในแนวทางเดียวกับการบริหารและจัดการความเสี่ยงขององค์กร ช่วยให้การสื่อสารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศไปยังผู้มีส่วนได้เสียทั้งภายในและภายนอกเป็นไปในรูปแบบเดียวกัน รวมทั้งก่อให้เกิดความตระหนักถึงความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น
- ผู้ที่มีหน้าที่รับผิดชอบในแต่ละความเสี่ยงรับทราบบทบาทหน้าที่และกิจกรรมที่เกี่ยวข้องเพื่อนำไปปฏิบัติอย่างเหมาะสม

1.2 <u>การจัดทำแนวทางการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศของ ก.ล.ต.</u>

สำนักงานได้จัดทำแนวทางการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศโดยอ้างอิงกรอบของ COBIT[1] ซึ่งเป็นกรอบการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่เป็นที่ยอมรับในระดับสากล ซึ่งสามารถเทียบเคียงกับประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ สธ. 37/2559 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ข้อ 5 (1)

[1] ผู้ประกอบธุรกิจสามารถอ้างอิงข้อมูลเกี่ยวกับแนวทางและกรอบการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศตามกรอบของ COBIT จาก Information System Audit and Control Association (www.isaca.org) และ NIST- National Institute of Standard and Technology: Guide for Conducting Risk Assessment, (https://www.nist.gov) นอกจากนี้ ผู้ประกอบธุรกิจยังสามารถอ้างอิงแนวทางและกรอบการกำกับดูแลและกรอบการบริหารและจัดการความเสี่ยงอื่น ๆ เพิ่มเติม เช่น ISO/IEC 31000:2009 Risk Management Principle and guideline (www.Iso.org) และ The Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management (www.coso.org)

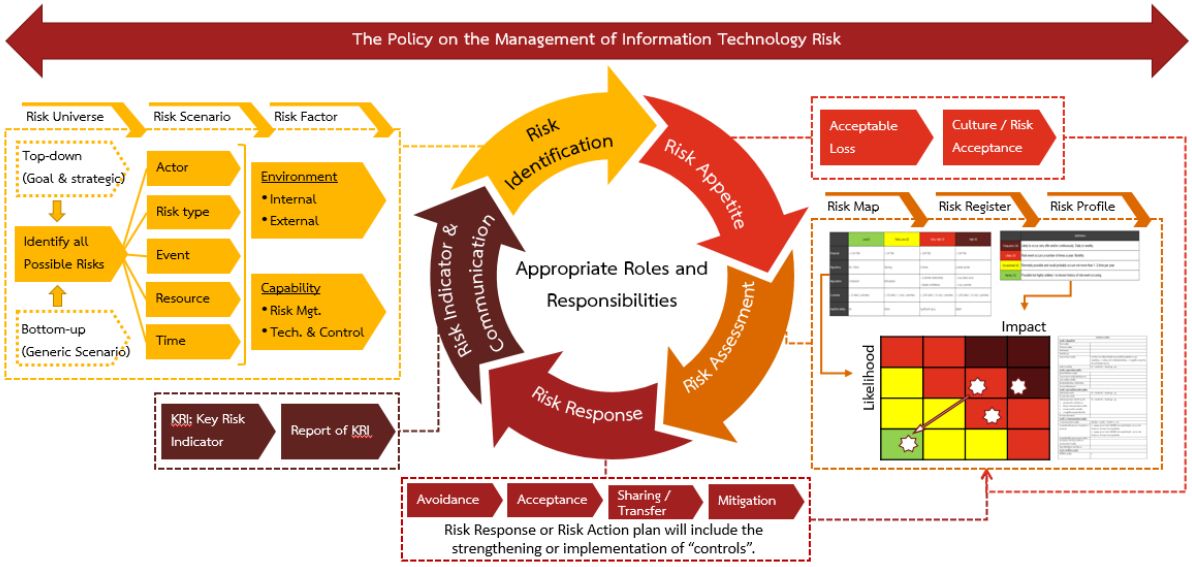
1.3 บทนิยาม

ผู้ประกอบธุรกิจ	หมายถึง	บริษัทและหน่วยงานภายใต้การกำกับดูแลของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ หรือธุรกิจสัญญาซื้อขายล่วงหน้าตามที่ระบุไว้ในหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศ
ทรัพย์สินสารสนเทศ	หมายถึง	1. ทรัพย์สินสารสนเทศประเภทระบบ ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2. ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ซึ่งได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และ อุปกรณ์อื่นใด 3. ทรัพย์สินสารสนเทศประเภทข้อมูล ซึ่งได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
ทรัพยากรสารสนเทศ	หมายถึง	ทรัพยากรสารสนเทศ ประกอบด้วย ทรัพย์สินสารสนเทศ (ระบบ อุปกรณ์ และข้อมูล) บุคลากรทางด้านเทคโนโลยีสารสนเทศ ความรู้ความสามารถทางด้านเทคโนโลยีสารสนเทศ งบประมาณ
ผู้รับผิดชอบ	หมายถึง	Accountable person หรือ ผู้ที่มีหน้าที่รับผิดชอบในผลสำเร็จหรือผลลัพธ์ของการดำเนินงานตามขอบเขตงานที่กำหนด โดยผู้รับผิดชอบมีหน้าที่ในการวางกรอบหรือ แนวทางการดำเนินงาน อนุมัติและบังคับใช้ รวมถึงติดตามผลการดำเนินงานตามกรอบที่ได้วางไว้
ผู้ทำหน้าที่	หมายถึง	Responsible person หรือผู้ที่มีหน้าที่ในการดำเนินงานตามกรอบการปฏิบัติงานที่กำหนดโดยผู้รับผิดชอบ

2. แนวทางปฏิบัติในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

เพื่อให้ผู้ประกอบธุรกิจสามารถบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิผล ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ซึ่งได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจ รวมทั้งสื่อสารทำความเข้าใจไปยังผู้ที่เกี่ยวข้อง และดำเนินการทบทวนหรือปรับปรุงนโยบายดังกล่าวอย่างสม่ำเสมอ โดยควรมีการกำหนดขั้นตอนและวิธีปฏิบัติงานสำหรับการบริหารและจัดการความเสี่ยงที่สอดคล้องกับนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่วางไว้ โดยกระบวนในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศนั้น เป็นกระบวนการที่ควรมีการดำเนินการอย่างต่อเนื่อง ประกอบด้วยกระบวนการดังสรุปในภาพประกอบที่ 1 ด้านล่าง

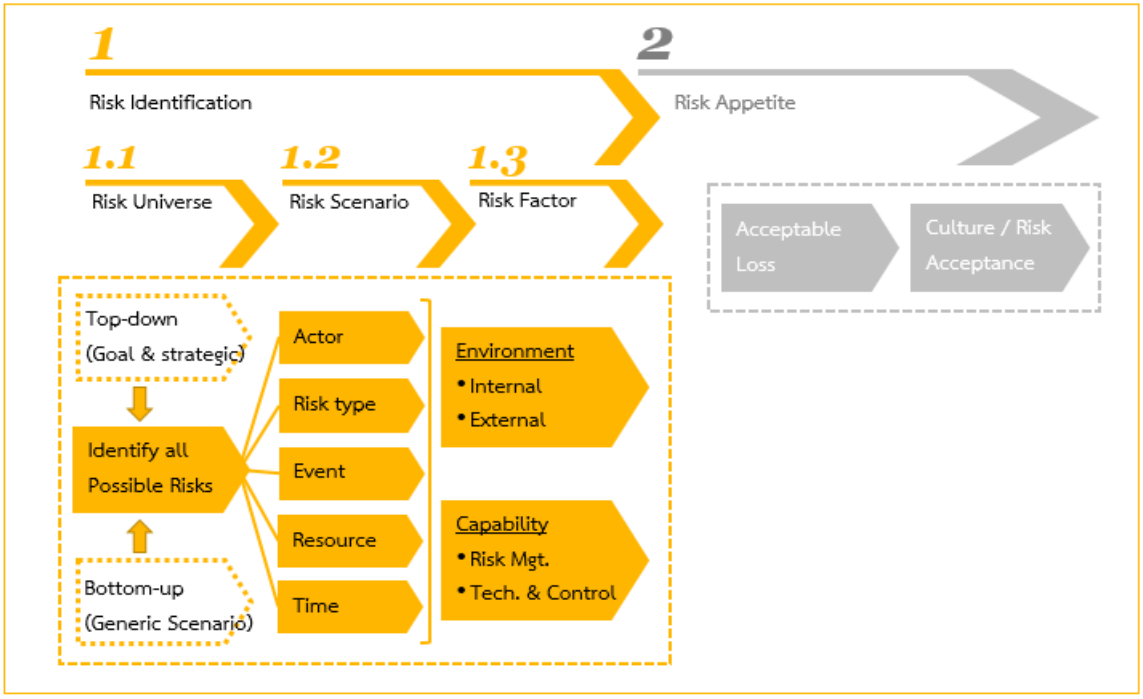
ภาพประกอบที่ 1 – กรอบการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ



2.1 <u>การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related Risk Identification)</u>

การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT related Risk) อาจประกอบด้วย 3 ขั้นตอนย่อย กล่าวคือ (1) การระบุความเสี่ยงที่เป็นไปได้ทั้งหมด (Risk Universe) เพื่อเป็นการกำหนดขอบเขตการบริหารและจัดการความเสี่ยงรวมถึงรวบรวมข้อมูลความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องทั้งหมด (2) การกำหนดเหตุการณ์ความเสี่ยง (Risk Scenario) โดยการนำความเสี่ยงที่ระบุไว้ในความเสี่ยงที่เป็นไปได้ทั้งหมดมาจัดทำเหตุการณ์ความเสี่ยง โดยระบุรายละเอียดสำคัญเพื่อการบริหารจัดการ เช่น ผู้กระทำให้เกิดความเสี่ยง ประเภท สินทรัพย์ หรือทรัพยากรที่เกี่ยวข้อง และ ช่วงเวลา (3) ระบุปัจจัยความสี่ยง (Risk Factors) ซึ่งเป็นการระบุปัจจัยหรือสาเหตุที่ก่อให้เกิดความเสี่ยง โดยปัจจัยความเสี่ยงถูกกำหนดขึ้นเพื่อประกอบการพิจารณาความสำคัญของเหตุการณ์ความเสี่ยง

ภาพประกอบที่ 2 – การระบุความเสี่ยง



2.1.1 ความเสี่ยงที่เป็นไปได้ทั้งหมด (Risk Universe)

การบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศควรเริ่มต้นจากการระบุความเสี่ยงที่เป็นไปได้ทั้งหมด (Risk Universe) ของผู้ประกอบธุรกิจ ซึ่งจะช่วยในการกำหนดขอบเขตในการบริหารและจัดการความเสี่ยง และเป็นเครื่องมือช่วยในการบริหารจัดการความครบถ้วนของความเสี่ยงที่ต้องมีการบริหารจัดการ ตลอดจนเป็นเครื่องมือที่ให้ผู้บริหารความเสี่ยงเห็นภาพรวมของความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งหมด โดยความเสี่ยงที่เป็นไปได้ทั้งหมดอาจเริ่มพิจารณาจากวัตถุประสงค์ แผนกลยุทธ์ กระบวนการทางธุรกิจ ระบบสารสนเทศที่สนับสนุนกิจกรรมทางธุรกิจ และโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศที่สนับสนุนวัตถุประสงค์และกระบวนการดังกล่าว โดยความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่เป็นไปได้ทั้งหมดควรพิจารณาครอบคลุมถึง

- กระบวนการที่เกี่ยวข้อง ทั้งกระบวนการทางด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจ
- ขอบเขตของหน่วยงานที่เกี่ยวข้อง ซึ่งอาจรวมถึงหน่วยงานภายในและภายนอกองค์กร เช่น สาขา บริษัทที่เกี่ยวข้อง ลูกค้า ผู้ให้บริการ
- กิจกรรมทางด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่มีการดำเนินการทั้งภายในและภายนอกองค์กร ซึ่งอาจรวมถึงการปรับปรุงเปลี่ยนแปลงระบบงาน การลงทุนและโครงการทางด้านเทคโนโลยีสารสนเทศ หรือการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ
- กิจกรรมและความเสี่ยงที่เกิดขึ้นใหม่ อาทิ ภัยคุกคามและความเสี่ยงทางด้านไซเบอร์
- ความหลากหลายของสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศ โดยเฉพาะในองค์กรที่มีสถานที่ปฏิบัติการในหลายพื้นที่ หรือมีการให้บริการระบบเทคโนโลยีสารสนเทศจำนวนมาก โดยควรมีการรวบรวมความเสี่ยงเพื่อพิจารณาจัดระดับความสำคัญ รวมทั้งพิจารณาความเสี่ยงที่อาจซ้ำซ้อนหรือขาดหายไป

ความเสี่ยงที่เป็นไปได้ทั้งหมดควรได้รับการพิจารณาปรับปรุงให้เป็นปัจจุบันอยู่เสมอตามสภาพแวดล้อมทั้งภายในและภายนอกที่เปลี่ยนแปลงไป

2.1.2 เหตุการณ์ความเสี่ยง (Risk Scenario)

เหตุการณ์ความเสี่ยง คือ เหตุการณ์ที่อาจเกิดขึ้น ซึ่งเมื่อเกิดขึ้นแล้วจะมีผลให้เกิดความไม่แน่นอนอันอาจส่งผลต่อการบรรลุวัตถุประสงค์ของผู้ประกอบธุรกิจทั้งในด้านบวกและด้านลบ โดยเหตุการณ์ความเสี่ยงทางเทคโนโลยีสารสนเทศควรระบุครอบคลุมองค์ประกอบเหล่านี้

1) ผู้กระทำให้เกิดความเสี่ยง หรือผู้กระทำให้เกิดเหตุการณ์ความเสี่ยง (Actor) หมายถึง บุคคล กลุ่มบุคคล หรือองค์กรที่มีส่วนรวมในการก่อให้เกิดภัยคุกคาม โดยภัยคุกคามนั้นอาจก่อให้เกิดช่องโหว่ทางด้านเทคโนโลยีสารสนเทศ เช่น พนักงาน ลูกจ้าง หุ้นส่วน ผู้ให้บริการภายนอก คู่แข่ง คู่ค้า หน่วยงานกำกับดูแล
2) ประเภทของภัยคุกคาม หรือประเภทของความเสี่ยง (Threat type or Risk type) หมายถึง ลักษณะที่มาของความเสี่ยงหรือภัยคุกคาม อาทิ ความเสี่ยงหรือภัยคุกคามจากการปฏิบัติงานในกระบวนการทำงาน ความเสี่ยงหรือภัยคุกคามจากบุคลากรภายใน บุคคลภายนอก หรือผู้ไม่ประสงค์ดี ความเสี่ยงด้านโปรแกรม ข้อมูล เป็นต้น โดยรวมถึงความเสี่ยงที่เกิดขึ้นตามธรรมชาติ เช่น ข้อผิดพลาด หรืออุบัติเหตุต่าง ๆ
3) เหตุการณ์ที่อาจเกิดขึ้น (Event) ตัวอย่างเช่น มีการรั่วไหลของข้อมูลสำคัญ มีการหยุดชะงักของระบบสารสนเทศ มีการขโมยหรือสูญหายของทรัพยากรสารสนเทศ การละเมิดกฎระเบียบข้อบังคับต่างๆ รวมทั้ง การใช้ทรัพยากรสารสนเทศอย่างไม่เหมาะสม
4) สินทรัพย์หรือทรัพยากรที่เกี่ยวข้อง (Asset/Resource) หมายถึง สินทรัพย์หรือทรัพยากรที่ได้รับผลกระทบจากความเสี่ยงที่ระบุไว้ โดยการระบุสินทรัพย์ที่เกี่ยวข้องนั้นสามารถช่วยให้เชื่อมโยงไปยังผลกระทบทางธุรกิจที่เกี่ยวข้อง สินทรัพย์หรือทรัพยากรในที่นี้ อาจประกอบด้วย บุคลากร ความสามารถของบุคลากร โครงสร้างองค์กร กระบวนการทางด้านเทคโนโลยีสารสนเทศ อุปกรณ์ และอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศ นอกจากนี้ ยังรวมถึงส่วนประกอบอื่น ๆ ในระบบสารสนเทศ เช่น ข้อมูล โปรแกรม และ ระบบงานต่าง ๆ
5) ช่วงเวลา หรือระยะเวลาที่เกิดเหตุการณ์ (Time) อันได้แก่ ความยาวของระยะเวลาของเหตุการณ์ความเสี่ยง ช่วงเวลาที่เหตุการณ์ความเสี่ยงอาจเกิดขึ้น โดยอาจรวมถึงระยะเวลาในการตรวจพบเหตุการณ์ความเสี่ยง หรือระยะเวลาที่ผลกระทบจากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้น

โดยรายละเอียดแนวทางการกำหนดเหตุการณ์ความเสี่ยงแสดงในภาคผนวก 1

2.1.3 ปัจจัยความเสี่ยง (Risk Factors)

ปัจจัยความเสี่ยง คือ ปัจจัยที่มีผลกระทบต่อความถี่และผลกระทบของเหตุการณ์ความเสี่ยง (Risk Scenario) ซึ่งอาจมีลักษณะที่แตกต่างกัน โดยสามารถจัดประเภทได้ 2 กลุ่ม ได้แก่

1) สภาพแวดล้อมการดำเนินงานขององค์กร คือ สภาพแวดล้อมหรือเหตุการณ์ของแต่ละองค์กรที่สามารถเพิ่มโอกาสเกิดหรือผลกระทบจากเหตุการณ์ความเสี่ยงที่ได้กำหนดไว้ โดยสามารถแบ่งเป็น 2 ส่วนหลัก ได้แก่
    - สภาพแวดล้อมภายนอก เช่น ปัจจัยทางด้านประเภทธุรกิจ การตลาดหรือเศรษฐกิจขององค์กร ปัจจัยทางด้านการแข่งขัน ปัจจัยทางด้านภูมิศาสตร์และรัฐศาสตร์ ปัจจัยทางด้านกฎระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม ปัจจัยทางด้านการใช้ระบบสารสนเทศขององค์กร และปัจจัยทางด้านภัยคุกคามที่เกี่ยวข้อง
    - สภาพแวดล้อมภายใน เช่น เป้าหมายและวัตถุประสงค์ขององค์กร กลยุทธ์ทางด้านเทคโนโลยีสารสนเทศ ความซับซ้อนของระบบสารสนเทศ ขนาดและโครงสร้างขององค์กร การเปลี่ยนแปลงในองค์กร โครงสร้างการปฏิบัติงานและกระบวนการต่าง ๆ ภายในองค์กร วัฒนธรรมองค์กร รวมถึงสถานะทางการเงินขององค์กร

2) ความสามารถในการบริหารจัดการทางด้านเทคโนโลยีสารสนเทศขององค์กร โดยสามารถแบ่งออกเป็น 2 ส่วน ได้แก่

- ความสามารถในการบริหารและจัดการความเสี่ยง เนื่องจากความเสี่ยงทางด้านเทคโนโลยีสารสนเทศอาจถือเป็นส่วนหนึ่งของความเสี่ยงด้านปฏิบัติการ (operational risk) ดังนั้น ความสามารถในการบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศจึงเกี่ยวเนื่องกับความสามารถในการบริหารและจัดการความเสี่ยงโดยรวมของแต่ละองค์กร ซึ่งรวมถึงกรอบวิธีการบริหารและจัดการความเสี่ยงที่ใช้ หรือการวัดผลการประเมินความเสี่ยง ซึ่งส่งผลต่อความสามารถในการระบุ และ ประเมินผลกระทบจากความเสี่ยงที่เกิดขึ้น
- ความสามารถทางด้านเทคโนโลยีสารสนเทศ และการควบคุมทางด้านเทคโนโลยีสารสนเทศ ซึ่งส่งผลในทางบวกต่อโอกาสเกิดของเหตุการณ์ความเสี่ยง และการจำกัดผลกระทบจากเหตุการณ์ความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

เนื่องจากปัจจัยความเสี่ยงมีอิทธิพลต่อความถี่และผลกระทบของเหตุการณ์ความเสี่ยง ดังนั้นจึงควรนำมาพิจารณาประกอบในการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

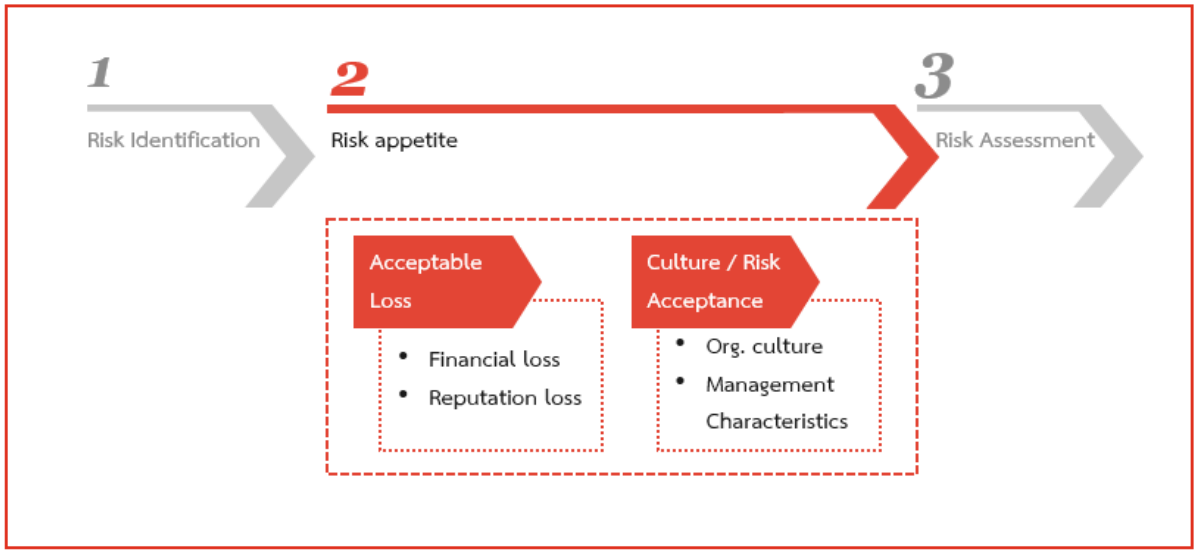
2.2 ความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite)

ความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite) คือ ปริมาณความเสี่ยงที่องค์กรสามารถยอมรับเมื่อมีความเสี่ยงเกิดขึ้น โดยการพิจารณาระดับของปริมาณความเสี่ยงที่องค์กรยอมรับได้ ประกอบด้วย

- ระดับความสูญเสียที่องค์กรสามารถยอมรับได้ ไม่ว่าจะเป็นความสูญเสียทางด้านการเงินหรือชื่อเสียง
- วัฒนธรรมขององค์กร หรือระดับการยอมรับความเสี่ยงของผู้บริหาร ซึ่งอาจหมายรวมถึงลักษณะการบริหารด้วยความระมัดระวังและความกล้าได้กล้าเสียของผู้บริหาร หรือปริมาณการสูญเสียที่องค์กรสามารถยอมรับเพื่อสร้างผลตอบแทนในอนาคต

ทั้งนี้ ความเสี่ยงที่สามารถยอมรับได้ควรได้รับการพิจารณาอนุมัติจากคณะกรรมการของผู้ประกอบธุรกิจ รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ

ภาพประกอบที่ 3 – การกำหนดระดับความเสี่ยงที่ยอมรับได้

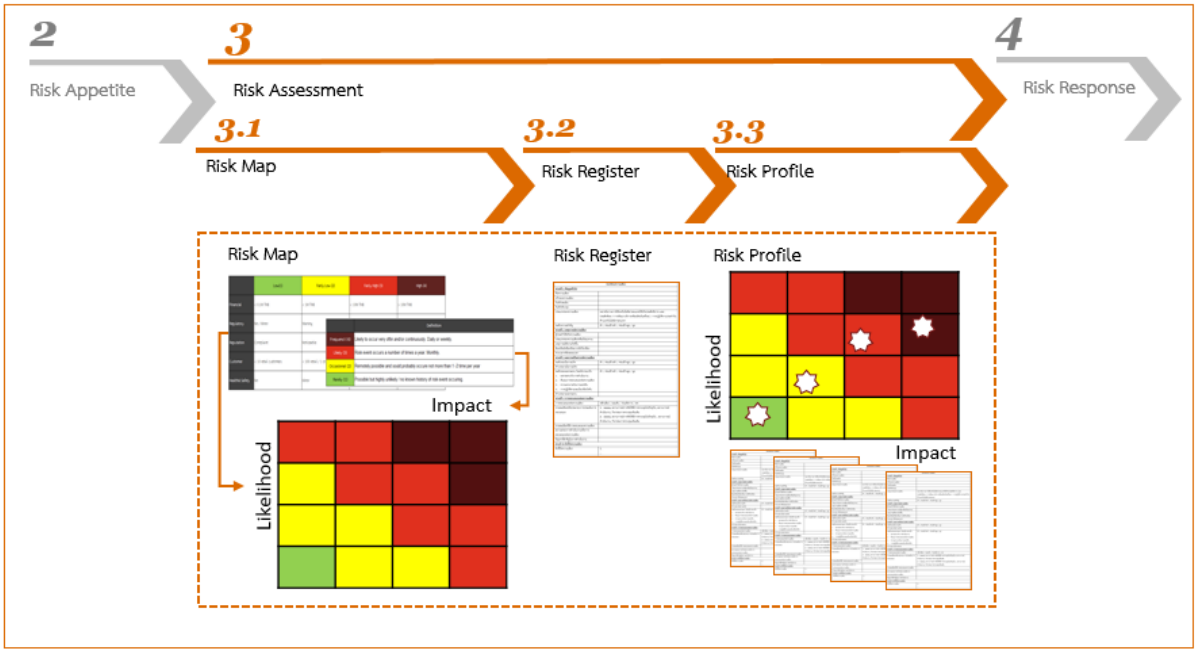


2.3 <u>การประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (IT Risk Assessment)</u>

จากเหตุการณ์ความเสี่ยงที่ระบุไว้ ผู้ประกอบธุรกิจควรมีกระบวนการในการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเพื่อประเมินระดับความสำคัญ โดยผู้ประกอบธุรกิจควรดำเนินการโดยมีขั้นตอนดังนี้

- ประเมินโอกาสเกิดและผลกระทบที่อาจเกิดขึ้นทั้งในด้านบวกและด้านลบของแต่ละเหตุการณ์ความเสี่ยง ทั้งนี้ ผลการประเมินอาจนำเสนอในรูปแบบของแผนภาพความเสี่ยง (Risk Map) ที่สามารถนำเสนอระดับของโอกาสเกิดและผลกระทบ (Risk Scale) ของแต่ละเหตุการณ์ความเสี่ยงได้ จากนั้นจึงจัดทำทะเบียนความเสี่ยง (Risk Register) ซึ่งบรรยายข้อมูลรายละเอียดของความเสี่ยงที่ระบุไว้
- จากนั้นจึงจัดทำโครงร่างของความเสี่ยง (Risk Profile) ซึ่งเป็นการรวบรวมความเสี่ยงทั้งหมด รวมทั้งแสดงสถานะของความเสี่ยงในปัจจุบัน ทั้งนี้ การประเมินความเสี่ยงเพื่อจัดทำโครงร่างของความเสี่ยงควรพิจารณาให้ครอบคลุมทุกปัจจัยความเสี่ยงที่เกี่ยวข้อง รวมทั้งกำหนดตัวควบคุมและความเสี่ยงที่ยังเหลืออยู่ภายหลังการควบคุมด้วย
- เปรียบเทียบความเสี่ยงที่ยังเหลืออยู่ภายหลังการควบคุมกับความเสี่ยงที่องค์กรยอมรับได้ โดยถ้าความเสี่ยงอยู่ในระดับที่เกินกว่าที่องค์กรยอมรับได้ ควรมีการกำหนดวิธีการปฏิบัติเพื่อจัดการกับความเสี่ยงนั้น
- วิเคราะห์ต้นทุนและประโยชน์ที่จะได้รับจากการจัดการความเสี่ยงในแต่ละรูปแบบ
- ระบุความต้องการในภาพรวมของโครงการหรือระบบงานเพื่อระบุความสี่ยงและความคาดหวังจากการควบคุมหลักที่ใช้ในการลดความเสี่ยงที่ตอบสนองต่อความต้องการของโครงการหรือระบบงานนั้น ๆ
- ประเมินผลการวิเคราะห์ความเสี่ยงก่อนการตัดสินใจดำเนินการบริหารและจัดการความเสี่ยง เพื่อให้มั่นใจว่าการวิเคราะห์สอดคล้องกับความต้องการขององค์กรและการประเมินความเสี่ยงเป็นไปอย่างเหมาะสมและสมเหตุสมผล

ภาพประกอบที่ 4 – การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ



2.3.1 แผนภาพความเสี่ยง (Risk Map)

เพื่อประเมินระดับความสำคัญของความเสี่ยงที่ระบุไว้ และเพื่อให้ผู้ที่เกี่ยวข้องในการบริหารและจัดการความเสี่ยงสามารถใช้เพื่อการจัดกลุ่มความเสี่ยงและบริหารจัดการได้อย่างมีประสิทธิผล การประเมินความเสี่ยงควรพิจารณาถึง 2 ส่วนประกอบหลัก คือ โอกาสเกิดและผลกระทบ ซึ่งเทคนิคในการนำเสนอความเสี่ยงที่เป็นที่นิยม คือ การใช้แผนภาพความเสี่ยง โดยในการจัดทำแผนภาพความเสี่ยงอาจพิจารณาให้ครอบคลุมถึง

- พิจารณาเหตุการณ์ความเสี่ยงที่เกี่ยวข้องทั้งหมดเพื่อให้มั่นใจว่าแผนภาพความเสี่ยงได้แสดงความเสี่ยงทางด้านเทคโนโลยีสารสนเทศอย่างครบถ้วน
- แยกส่วนการพิจารณาผลกระทบและโอกาสเกิดออกจากกัน เนื่องจากทั้งโอกาสเกิดและผลกระทบอาจต้องการกิจกรรมและวิธีการบริหารจัดการที่แตกต่างกัน
- การกำหนดระดับตัวเลขความสำคัญของโอกาสเกิดหรือผลกระทบนั้นเป็นเพียงตัวเลขที่กำหนดขึ้นเพื่อให้เห็นขอบเขตข้อมูลเพื่อการเปรียบเทียบระดับของความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่มีการระบุ ทั้งนี้เพื่อให้ผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการความเสี่ยงสามารถเห็นภาพรวมเชิงเปรียบเทียบของความเสี่ยงทางด้านเทคโนโลยีสารสนเทศภายในองค์กร และเพื่อให้ผู้บริหารความเสี่ยงสามารถกำหนดความเสี่ยงสำคัญเพื่อการบริหารจัดการและการตอบสนองต่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิผลเท่านั้น ทั้งนี้ ระดับตัวเลขความสำคัญไม่ได้สื่อความหมายของความเสี่ยงที่เกิดขึ้น รวมทั้งไม่สามารถนำไปใช้เพื่อการคำนวณอื่น ๆ ได้

ในการจัดทำแผนภาพความเสี่ยง อาจมีการกำหนดช่วงของระดับของโอกาสเกิดหรือผลกระทบได้ในหลายระดับ เช่น ในองค์กรที่ยังไม่มีประสบการณ์หรือมีความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ไม่ซับซ้อน อาจใช้ระดับความสำคัญของโอกาสเกิดหรือผลกระทบ เพียง 3 ระดับ หรือเมื่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศมีความซับซ้อนมากขึ้นและมีความต้องการจำแนกระดับความเสี่ยงในรายละเอียดเพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง ผู้ประกอบธุรกิจอาจพิจารณาเพิ่มระดับของโอกาสเกิดหรือผลกระทบจาก 3 เป็น 4 หรือ 5 ระดับ เพื่อให้สามารถจัดกลุ่มได้ละเอียดมากขึ้น รวมทั้งควรมีการพิจารณาเปรียบเทียบระดับความเสี่ยงในปัจจุบันกับระดับความเสี่ยงที่สามารถยอมรับได้ และความเสี่ยงที่ต้องการการบริหารจัดการเพิ่มเติม

2.3.2 ทะเบียนความเสี่ยง (Risk Register)

จัดขึ้นเพื่อเป็นการบรรยายรายละเอียดและส่วนประกอบที่เกี่ยวข้องของแต่ละความเสี่ยงที่ได้ระบุไว้ หลังจากจัดทำแผนภาพความเสี่ยงแล้ว โดยรายละเอียดของทะเบียนความเสี่ยงอาจประกอบด้วย เจ้าของความเสี่ยง รายละเอียดเหตุการณ์ความเสี่ยง ผลจากการวิเคราะห์ความเสี่ยง รายละเอียดการควบคุม หรือกิจกรรม เพื่อตอบสนองหรือการบริหารและจัดการความเสี่ยง รวมถึงสถานะการดำเนินงานในปัจจุบัน โดยสามารถอ้างอิงตัวอย่าง แผนภาพความเสี่ยงและทะเบียนความเสี่ยงในภาคผนวก 2

2.3.3 โครงร่างของความเสี่ยง (Risk Profile)

เมื่อองค์กรมีการจัดทำแผนภาพความเสี่ยงและทะเบียนความเสี่ยงแล้ว เพื่อเป็นการรวบรวมแผนภาพความเสี่ยงและทะเบียนความเสี่ยงที่ระบุขึ้น รวมทั้งแสดงให้เห็นถึงสถานะปัจจุบันของความเสี่ยงขององค์กร องค์กรควรจัดทำโครงร่างของความเสี่ยง ซึ่งโครงร่างของความเสี่ยงนี้สามารถใช้เพื่อประโยชน์ในการรายงานผลความเสี่ยง เนื่องจากโครงร่างของความเสี่ยง

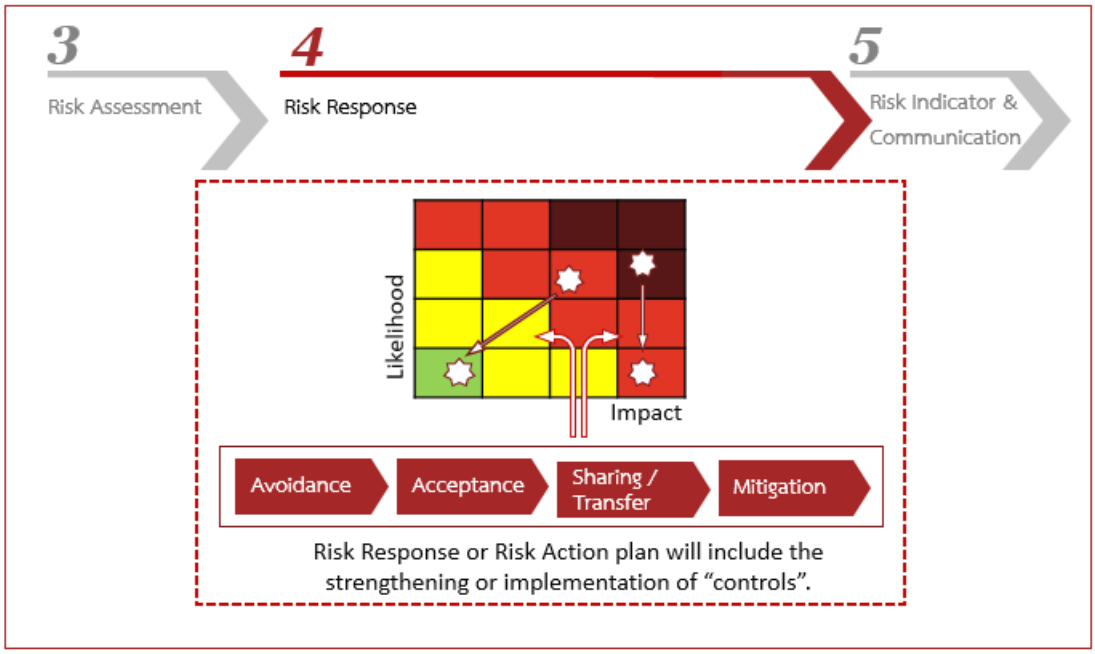
จัดทำโดยอาศัยข้อมูลของแผนภาพความเสี่ยง ทะเบียนความเสี่ยง ผลการวิเคราะห์ความเสี่ยง และตัวชี้วัดผลการปฏิบัติงานขององค์กร ทั้งนี้ ในกระบวนการในการจัดทำโครงร่างของความเสี่ยงทางด้านเทคโนโลยีสารสนเทศควรเป็นกระบวนการเดียวกันกับกระบวนการจัดทำโครงร่างของความเสี่ยงของกระบวนการทางธุรกิจขององค์กร และควรมีการปรับปรุงเพื่อให้ความเสี่ยงเป็นปัจจุบันอยู่เสมอ ทั้งนี้ ความถี่ในการปรับปรุงควรดำเนินการอย่างน้อยปีละ 1 ครั้ง โดยขึ้นอยู่กับสภาพแวดล้อมทั้งภายในและภายนอกขององค์กร โดยในโครงร่างของความเสี่ยงควรประกอบด้วยข้อมูลอย่างน้อย ดังนี้

- ปัจจัยเสี่ยง โดยพิจารณาในมุมของสภาพแวดล้อมการดำเนินงานขององค์กร และความสามารถในการบริหารจัดการทางด้านเทคโนโลยีสารสนเทศขององค์กร
- ผลการประเมินความเสี่ยง การวิเคราะห์ความเสี่ยง และแผนภาพความเสี่ยงในระดับองค์กร รวมทั้งทะเบียนความเสี่ยง
- ข้อมูลเกี่ยวกับผลเสียหายที่เคยเกิดขึ้นในอดีต เพื่อแสดงถึงความเสี่ยงที่เคยเกิดขึ้น
- ตัวชี้วัดผลการปฏิบัติงานขององค์กร เพื่อแสดงถึงระดับโอกาสเกิดที่ความเสี่ยงอาจส่งผลกระทบที่สำคัญต่อองค์กร
- ผลการตรวจสอบโดยผู้ตรวจสอบครั้งล่าสุดในส่วนที่เกี่ยวของกับความเสี่ยง โดยผลการตรวจสอบอาจสามารถใช้ในการพิจารณาเพิ่มเติมในส่วนของความสามารถในการบริหารจัดการทางด้านเทคโนโลยีสารสนเทศขององค์กร

2.4 <u>การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (Risk Response)</u>

เพื่อการวางแผนการจัดการความเสี่ยงที่เหมาะสมและตอบสนองต่อเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น องค์กรสามารถพิจารณาวิธีการในการรับมือกับความเสี่ยงใน 4 รูปแบบ ประกอบด้วย การหลีกเลี่ยงความเสี่ยง การยอมรับความเสี่ยง การร่วมจัดการหรือการถ่ายโอนความเสี่ยง และการลดความเสี่ยง ดังแสดงในภาพประกอบที่ 5

ภาพประกอบที่ 5 – แนวทางการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ



2.4.1 การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)

การหลีกเลี่ยงความเสี่ยง คือ การหลีกเลี่ยงกิจกรรมหรือสาเหตุที่อาจก่อให้เกิดความเสี่ยง ซึ่งโดยส่วนมากจะใช้วิธีการนี้ในกรณีที่ไม่มีการจัดการความเสี่ยงที่เหมาะสมในรูปแบบอื่นอีกแล้ว รวมทั้งผลกระทบจากความเสี่ยงนั้นอาจสูงเกินกว่าระดับที่องค์กรยอมรับได้

2.4.2 การยอมรับความเสี่ยง (Risk Acceptance)

การยอมรับความเสี่ยง คือ การที่บริษัทไม่มีการกำหนดกิจกรรมใด ๆ เพื่อตอบสนองต่อความเสี่ยงที่อาจเกิดขึ้น โดยผู้บริหารยอมรับผลที่อาจเกิดขึ้นจากความเสี่ยงนั้น ๆ ซึ่งโดยส่วนมากจะใช้วิธีการนี้ในกรณีที่ผลกระทบจากความเสี่ยงต่ำกว่าต้นทุนในกิจกรรมที่ใช้บริหารและจัดการความเสี่ยงนั้น ข้อควรระวังในการวางแผนการจัดการความเสี่ยงแบบการยอมรับความเสี่ยง คือ การกำหนดผู้ที่สามารถตัดสินใจยอมรับความเสี่ยงนั้น เนื่องจากความเสี่ยงทางด้านเทคโนโลยีสารสนเทศมีผลกระทบต่อการดำเนินงานทางธุรกิจในภาพรวม ดังนั้น องค์กรอาจต้องมีกระบวนการที่ชัดเจนในการระบุระดับของความเสี่ยงที่ยอมรับได้ รวมทั้งผู้ที่สามารถตัดสินใจยอมรับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศในกรณีต่าง ๆ

2.4.3 การร่วมจัดการความเสี่ยง/ถ่ายโอนความเสี่ยง (Risk Sharing/Transfer)

การร่วมจัดการความเสี่ยง คือ การลดความถี่ในการเกิดหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น โดยกระจายหรือโอนไปยังบุคคลอื่น เช่น การทำประกันหรือการใช้งานผู้ให้บริการภายนอกในราคาคงที่ (fixed price) โดยเป็นการถ่ายโอนความเสียหายนอกเหนือจากวงเงินหรือขอบเขตที่กำหนดไปยังบริษัทประกันหรือผู้ให้บริการภายนอก ทั้งนี้ การร่วมจัดการความเสี่ยงนั้นไม่สามารถถ่ายโอนความรับผิดชอบจากความเสี่ยง ซึ่งผู้ประกอบธุรกิจยังคงเป็นผู้มีหน้าที่รับผิดชอบในความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นได้

2.4.4 *การลดความเสี่ยง (Risk Mitigation)*

การลดความเสี่ยง สามารถทำได้โดยการจัดให้มีกิจกรรมการควบคุมเพื่อลดความถี่ในการเกิดหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น โดยอาจทำได้ใน 2 รูปแบบคือ แบบที่ 1 กำหนดให้มีการบริหารและจัดการความเสี่ยงอย่างรัดกุม และแบบที่ 2 มีกิจกรรมการควบคุมเพื่อลดโอกาสเกิดหรือผลกระทบจากความเสี่ยงนั้น ๆ นอกจากนี้ ยังอาจรวมถึงกิจกรรมอื่น ๆ ในการลดความเสี่ยง เช่น การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศที่เหมาะสมและการปรับใช้มาตรฐานต่าง ๆ ในการบริหารจัดการทางด้านเทคโนโลยีสารสนเทศ

โดยปัจจัยในการเลือกวิธีการบริหารจัดการความเสี่ยงที่เหมาะสม อาจประกอบด้วย

- ระดับความสำคัญของโอกาสเกิดและผลกระทบจากความเสี่ยง ซึ่งแสดงในแผนภาพความเสี่ยง
- ประสิทธิผลของการจัดการความเสี่ยง คือ การเปรียบเทียบประโยชน์ที่จะได้รับจากกิจกรรมเพื่อจัดการความเสี่ยงในแบบต่าง ๆ กับต้นทุนที่ต้องใช้เพื่อจัดให้มีกิจกรรมเพื่อจัดการความเสี่ยงนั้น ๆ
- ความสามารถของผู้ประกอบธุรกิจในการดำเนินกิจกรรมเพื่อจัดการกับความเสี่ยง อาทิ ผู้ประกอบธุรกิจที่มีความเชี่ยวชาญในการบริหารและจัดการความเสี่ยงย่อมสามารถดำเนินกิจกรรมเพื่อจัดการความเสี่ยงที่ซับซ้อนได้มีประสิทธิภาพกว่าผู้ประกอบธุรกิจที่ยังไม่มีประสบการณ์ในการบริหารและจัดการความเสี่ยง
- ประสิทธิผลของกิจกรรม หรือการควบคุมเพื่อจัดการความเสี่ยง หรือความสามารถของกิจกรรมหรือการควบคุมในการลดโอกาสเกิด หรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น

ทั้งนี้ ผู้ประกอบธุรกิจควรพิจารณาจัดระดับความสำคัญของรายการกิจกรรมเพื่อจัดการความเสี่ยง และเรียงลำดับในการจัดการความเสี่ยงตามระดับความสำคัญ เนื่องจากรายการกิจกรรมเพื่อจัดการความเสี่ยงทั้งหมดอาจใช้ทรัพยากรมากกว่าทรัพยากรที่องค์กรมีอยู่ โดยผู้ประกอบธุรกิจอาจแยกเป็น 3 ระดับความสำคัญ ได้แก่

1) ความสำคัญสูง ซึ่งเป็นกิจกรรมที่มีประสิทธิภาพและประสิทธิผลสูงในการลดความเสี่ยง หรือเป็นกิจกรรมที่จัดการต่อความเสี่ยงที่มีความสำคัญ
2) ความสำคัญปานกลาง ซึ่งเป็นกิจกรรมที่จัดการต่อความเสี่ยงที่สำคัญแต่อาจต้องใช้ทรัพยากรมากหรือดำเนินการได้ยาก หรือเป็นกิจกรรมที่มีประสิทธิภาพและประสิทธิผลที่จัดการกับความเสี่ยงในระดับที่รองลงมา ความสำคัญในระดับนี้จึงควรได้รับการพิจารณาความเหมาะสมจากผู้บริหารอีกครั้ง
3) ความสำคัญต่ำ ซึ่งเป็นกิจกรรมที่จัดการต่อความเสี่ยงที่สำคัญน้อย หรือเป็นกิจกรรมที่อาจไม่คุ้มค่าในการดำเนินการ

ในการพิจารณาทางเลือกในการจัดการความเสี่ยงที่เหมาะสม ผู้ประกอบธุรกิจควรมีกระบวนการดังต่อไปนี้

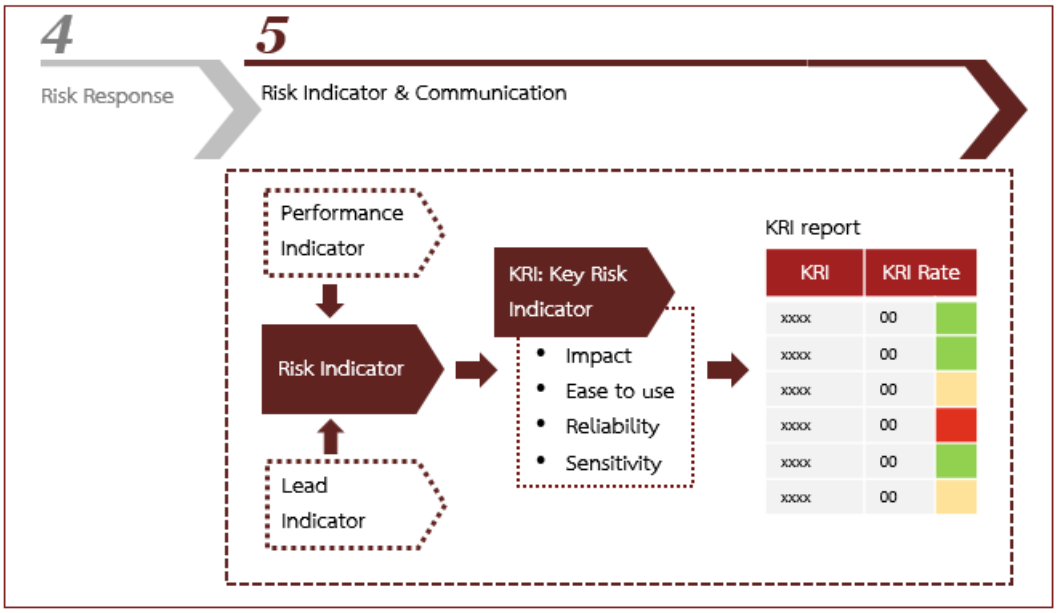
- รวบรวมกิจกรรมการควบคุมและทรัพยากรที่ใช้ในการบริหารและจัดการความเสี่ยง เพื่อให้ความเสี่ยงที่หลงเหลืออยู่ อยู่ภายใต้ความเสี่ยงที่องค์กรยอมรับได้ รวมทั้งจำแนกประเภทของกิจกรรมการควบคุมเพื่อให้สามารถเชื่อมโยงกับภาพรวมของความเสี่ยงขององค์กร
- พิจารณาการติดตามความเสี่ยงของแต่ละส่วนงาน รวมถึงความรับผิดชอบเป็นเจ้าของความเสี่ยงของแต่ละส่วนงานเพื่อให้ความเสี่ยงในความรับผิดชอบของส่วนงานอยู่ในระดับที่ยอมรับได้
- ประเมินความเหมาะสมระหว่างการออกแบบการควบคุมหรือกิจกรรมเพื่อลดความเสี่ยง และกระบวนการที่สร้างโอกาสในการดำเนินธุรกิจการตามกลยุทธ์ขององค์กร โดยพิจารณาถึงต้นทุน ผลที่ได้รับ ผลกระทบกับรายการความเสี่ยง และกฎระเบียบข้อบังคับต่าง ๆ
- จัดเตรียม ปรับปรุง และทดสอบ แผนงานที่ใช้ในการจัดการความเสี่ยงที่มีความสำคัญ หรือความเสี่ยงที่มีผลกระทบต่อการดำเนินธุรกิจ เพื่อให้มั่นใจในประสิทธิภาพและประสิทธิผลของแผนงาน รวมถึงขั้นตอนและการรายงานภายในองค์กรอย่างทั่วถึง
- แยกกลุ่มเหตุการณ์ความเสี่ยงและเปรียบเทียบผลกระทบที่อาจเกิดขึ้นกับความเสี่ยงที่ยอมรับได้ รวมทั้งมีการสื่อสารผลกระทบทางด้านธุรกิจไปยังผู้มีอำนาจตัดสินใจ ซึ่งถือเป็นส่วนหนึ่งของกระบวนการรายงานผลและปรับปรุงโครงร่างของความเสี่ยง
- ประเมินผลความสูญเสียหรือผลกระทบจากเหตุการณ์ที่เคยเกิดขึ้นในอดีตเพื่อหาสาเหตุที่แท้จริง จากนั้นมีการสื่อสารสาเหตุ การดำเนินงานเพื่อตอบต่อความเสี่ยงเพิ่มเติม และการปรับปรุงกระบวนการไปยังผู้มีอำนาจตัดสินใจ ทั้งนี้ เพื่อให้มั่นใจว่า สาเหตุ การตอบสนองต่อความเสี่ยง และการปรับปรุงกระบวนการได้บรรจุอยู่ในกระบวนการบริหารและจัดการความเสี่ยงอย่างเหมาะสม

2.5 <u>การกำหนดตัวชี้วัดความเสี่ยง (IT risk indicator) การติดตาม และรายงานผลการบริหารและจัดการความเสี่ยง (IT risk monitoring / reporting)</u>

จากโครงร่างของความเสี่ยงที่จัดทำขึ้น ผู้ประกอบธุรกิจควรกำหนดตัวชี้วัดความเสี่ยง (risk indicator) เพื่อสามารถชี้วัดและติดตามแนวโน้มของความเสี่ยงที่อาจเกิดขึ้น โดยการคัดเลือกตัวชี้วัดที่เหมาะสม ควรมีสัดส่วนระหว่างตัวชี้วัด

ผลการดำเนินงาน (performance indicator) ซึ่งเป็นตัวที่วัดเหตุการณ์ที่เกิดขึ้นแล้ว และตัวชี้วัดนำ (lead indicator) ซึ่งเป็นตัวชี้วัดความสามารถขององค์กรในการป้องกันไม่ให้เหตุการณ์ความเสี่ยงเกิดขึ้น รวมถึงบ่งชี้แนวโน้มเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้นในอนาคต นอกจากนี้ ตัวชี้วัดที่กำหนดควรเป็นตัวชี้วัดที่สามารถเชื่อมโยงถึงสาเหตุที่แท้จริงของเหตุการณ์ความเสี่ยงนั้น ๆ

ภาพประกอบที่ 6 – การกำหนดตัวชี้วัดความเสี่ยง การติดตาม และรายงานผลการบริหารและจัดการความเสี่ยง



ทั้งนี้ ผู้ประกอบธุรกิจควรมีการพัฒนาตารางเพื่อเปรียบเทียบตัวชี้วัดความเสี่ยง และจัดทำตัวชี้วัดความเสี่ยงหลัก (Key risk Indicator) โดยตัวชี้วัดความเสี่ยงหลักอาจคัดเลือกมาจาก (1) ผลกระทบจากความเสี่ยงของตัวชี้วัดความเสี่ยงนั้น (2) ความยากง่ายในการใช้งานตัวชี้วัดความเสี่ยง โดยในตัวชี้วัดที่สามารถบ่งชี้ความเสี่ยงได้เหมือนกัน ตัวชี้วัดที่สามารถจัดทำ บ่งชี้ และรายงานได้ง่ายกว่าควรถูกกำหนดเป็นตัวชี้วัดความเสี่ยงหลัก (3) ความน่าเชื่อถือ โดยอาจเลือกตัวชี้วัดที่มีความเชื่อมโยงกับความเสี่ยงสูง หรือมีความแม่นยำในการคาดการณ์ความเสี่ยงมากกว่า (4) การตอบสนองต่อการเปลี่ยนแปลงของความเสี่ยง โดยอาจเลือกตัวชี้วัดที่สามารถสะท้อนการเปลี่ยนแปลงของความเสี่ยงเมื่อความเสี่ยงมีการเปลี่ยนแปลงเกิดขึ้น โดยท้ายที่สุดนั้น ตัวชี้วัดความเสี่ยงหลักทั้งหมดควรชี้วัดความเสี่ยง สาเหตุที่แท้จริง และผลกระทบอย่างเหมาะสม โดยสามารถอ้างอิงตัวอย่างของตัวชี้วัดความเสี่ยงหลักได้ ในภาคผนวก 3

การรายงานผลการบริหารและจัดการความเสี่ยง (reporting) ผู้ประกอบธุรกิจควรมีกระบวนการดังต่อไปนี้

- รายงานผลการประเมินความเสี่ยงที่มีผลต่อผู้ที่มีส่วนได้เสียที่เกี่ยวข้องทั้งหมดในรูปแบบที่สามารถนำไปประกอบการตัดสินใจได้ เช่น ความเป็นไปได้ของผลประโยชน์ หรือการสูญเสียที่อาจเกิด เปรียบเทียบกับระดับความมั่นใจที่ผู้บริหารพิจารณาระหว่างความเสี่ยงและประโยชน์ที่อาจได้รับ
- นำเสนอข้อมูลที่เกี่ยวข้องกับผู้มีหน้าที่ตัดสินใจ โดยข้อมูลอาจรวมถึงเหตุการณ์ที่แย่หรือดีที่สุดที่อาจเกิดขึ้น การทำความเข้าใจผลกระทบ รวมทั้งพิจารณาถึงภาพลักษณ์ ชื่อเสียง กฎหมาย และ กฎระเบียบข้อบังคับต่าง ๆ

- รายงานรายการความเสี่ยงในปัจจุบันให้กับผู้มีส่วนได้ส่วนเสีย รวมถึงรายงานผลการบริหารและจัดการความเสี่ยง ประสิทธิผลของการควบคุม ข้อตรวจพบ หรือข้อปรับปรุง รวมทั้งผลกระทบกับรายการความเสี่ยง
- สอบทานวัตถุประสงค์จากการตรวจสอบโดยผู้ตรวจสอบอิสระ ผู้ตรวจสอบภายใน และ การตรวจสอบเพื่อวัดคุณภาพ โดยเชื่อมโยงกับรายการความเสี่ยงและพิจารณาถึงความเสี่ยงเพิ่มเติม
- ควรมีการสื่อสารเป็นประจำกับผู้ที่เกี่ยวข้องในเรื่องของความเสี่ยงและโอกาสทางด้านเทคโนโลยีสารสนเทศเพื่อการพิจารณาถึงการพัฒนาหรือผลกำไรที่เพิ่มขึ้นจากการยอมรับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่เพิ่มขึ้น

3. การกำหนดหน้าที่และความรับผิดชอบ และผู้ทำหน้าที่ในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

คณะกรรมการของผู้ประกอบธุรกิจ (Board of Director) ควรเป็นผู้รับผิดชอบ (Accountable person) ในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยมีหน้าที่ในการให้แนวทางและอนุมัติเห็นชอบในนโยบายการบริหารและจัดการความเสี่ยงขององค์กร ซึ่งรวมถึงความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งติดตามผลการดำเนินงานตามนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าผู้ประกอบธุรกิจมีการระบุความเสี่ยงทางด้านเทคโนโลยีสารสนเทศอย่างครบถ้วน มีการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และบริหารจัดการเพื่อให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศอยู่ในระดับที่ยอมรับได้

ทั้งนี้ ผู้ประกอบธุรกิจควรมีการมอบหมายบทบาทหน้าที่ที่เกี่ยวข้องในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเป็นทางการ โดยคำนึงถึงหลักการถ่วงดุล (Check and Balance) และการแบ่งแยกหน้าที่ความรับผิดชอบที่เหมาะสม (Segregation of duties) เป็น 3 ระดับ ได้แก่ ผู้ปฏิบัติงาน (First line of defence) ผู้ที่ทำหน้าที่บริหารความเสี่ยง (Second line of defence) และผู้ตรวจสอบ (Third line of defence) โดยบทบาทหน้าที่ของผู้ที่เกี่ยวข้องอาจมีดังต่อไปนี้

3.1 <u>ระดับที่ 1: หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (First line of defence)</u>

หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เป็นผู้ทำหน้าที่ (Responsible person) ในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ตั้งแต่การเก็บรวบรวมข้อมูล การวิเคราะห์และประเมินความเสี่ยง การจัดทำและปรับปรุงรายการความเสี่ยง จัดทำรายการกิจกรรมการบริหารและจัดการความเสี่ยง รวมถึงกำหนดกิจกรรมเพื่อตอบสนองต่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

โดยหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศนี้ยังอาจรวมถึง หน่วยงานที่ใช้งานระบบเทคโนโลยีสารสนเทศ (user) ซึ่งทำหน้าที่ในการร่วมบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่เกี่ยวเนื่องกับการใช้งานระบบเทคโนโลยีสารสนเทศ

3.2 <u>ระดับที่ 2: หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง (Second line of defence)</u>

หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง เป็นผู้ทำหน้าที่ (Responsible person) ในการกำหนดกรอบและกระบวนการการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งสนับสนุนให้มีการดำเนินงานดังกล่าว โดยหน่วยงาน

ที่ทำหน้าที่บริหารความเสี่ยงนี้จะเป็นผู้รับผิดชอบ (Accountable person) ในผลการบริหารและจัดการความเสี่ยงทุกรูปแบบทั่วทั้งองค์กร รวมถึงรับผิดชอบให้มีการจัดทำและปรับปรุงความเสี่ยงและกิจกรรมการบริหารความเสี่ยง

โดยรวมถึงหน่วยงานกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ (Compliance) ซึ่งเป็นผู้ให้คำปรึกษา และสอบทานการดำเนินงานตามกฎหมายและระเบียบข้อบังคับต่าง ๆ

3.3 <u>ระดับที่ 3: หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (Third line of defence)</u>

หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศทั้งหน่วยงานตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่เป็นอิสระจากหน่วยงานที่ปฏิบัติหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้ทำหน้าที่ (Responsible person) ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยง เพื่อให้มั่นใจว่ามีการปฏิบัติตามกรอบและกระบวนการการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

ภาคผนวก 1 แนวทางการกำหนดเหตุการณ์ความเสี่ยง

แนวทางการกำหนดเหตุการณ์ความเสี่ยงอาจประกอบด้วย 2 แนวทาง ซึ่งทั้ง 2 แนวทางควรมีการนำมาพิจารณาร่วมกัน ดังนี้

1. วิธีการแบบบนลงล่าง (Top-down Approach) – โดยเริ่มวิเคราะห์จากวัตถุประสงค์โดยรวมขององค์กร แผนกลยุทธ์ทางธุรกิจขององค์กร แผนกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศ และระบุถึงเหตุการณ์ทางด้านเทคโนโลยีสารสนเทศที่อาจส่งผลกระทบในทางลบต่อวัตถุประสงค์และแผนกลยุทธ์นั้น ทั้งนี้ เพื่อให้มั่นใจว่าเหตุการณ์ความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่กำหนดมีความเชื่อมโยงกับความเสี่ยงขององค์กร
2. วิธีการแบบล่างขึ้นบน (Bottom-up Approach) – วิเคราะห์จากรายการเหตุการณ์ความเสี่ยงทั่วไปทางด้านเทคโนโลยีสารสนเทศ และมาประยุกต์ให้เข้ากับเหตุการณ์ขององค์กรผู้ประกอบธุรกิจ ทั้งนี้ เพื่อให้มั่นใจว่าเหตุการณ์ความเสี่ยงที่นำมาพิจารณานั้นมีความครอบคลุมถึงเหตุการณ์ความเสี่ยงทั่วไปทางด้านเทคโนโลยีสารสนเทศ ตัวอย่างประเภทของเหตุการณ์ความเสี่ยงทั่วไปแสดงในตารางด้านล่าง

ประเภทของเหตุการณ์	ตัวอย่างเหตุการณ์ความเสี่ยง
1. รายการการลงทุนและการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ	● การเลือกใช้ระบบงาน หรือเลือกพัฒนาระบบงานที่ไม่เป็นไปตามกลยุทธ์ หรือระดับความสำคัญขององค์กร ● มีการเลือกใช้เทคโนโลยีสารสนเทศที่ซ้ำซ้อนกัน ● การเลือกเทคโนโลยีสารสนเทศใหม่ที่ไม่สามารถใช้งานกับเทคโนโลยีสารสนเทศในปัจจุบันหรือไม่สามารถใช้งานได้ในระยะยาว ● การจัดสรรทรัพยากรสารสนเทศโดยไม่ตรงตามลำดับความสำคัญทางธุรกิจ
2. การบริหารจัดการระบบงาน หรือโครงการทางด้านเทคโนโลยีสารสนเทศ	● โครงการทางด้านเทคโนโลยีสารสนเทศไม่ประสบความสำเร็จ ล่าช้า ต้องหยุดชะงัก ● โครงการทางด้านเทคโนโลยีสารสนเทศใช้งบประมาณและทรัพยากรเกินกว่าที่กำหนด ● โครงการทางด้านเทคโนโลยีสารสนเทศไม่ได้รับการสนับสนุนหรือมีส่วนร่วมโดยผู้ที่มีส่วนได้เสียอย่างเหมาะสม
3. การตัดสินใจลงทุนทางด้านเทคโนโลยีสารสนเทศ	● ผู้บริหารที่เกี่ยวข้องไม่มีส่วนร่วมในการตัดสินใจ ● มีการตัดสินใจเลือกลงทุนในเทคโนโลยีที่ไม่เหมาะสมในแง่ของต้นทุน ความสามารถในการทำงาน และการใช้งานร่วมกับระบบงานในปัจจุบันขององค์กร
4. ความรู้ความสามารถทางด้านเทคโนโลยีสารสนเทศ	● พนักงานขาดความรู้ความสามารถในเทคโนโลยีสารสนเทศที่บริษัทเลือกใช้ ● พนักงานขาดความเข้าใจในการดำเนินธุรกิจและความต้องการทางธุรกิจขององค์กร ● ไม่สามารถจัดหาบุคลากรทางด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอ ● กระบวนการจัดหาพนักงานไม่เหมาะสม เช่น ขาดการตรวจสอบประวัติ ● การอบรมและถ่ายทอดความรู้ทางด้านเทคโนโลยีสารสนเทศไม่เพียงพอ ● การดำเนินงานพึ่งพาบุคคลากรมากเกินไป

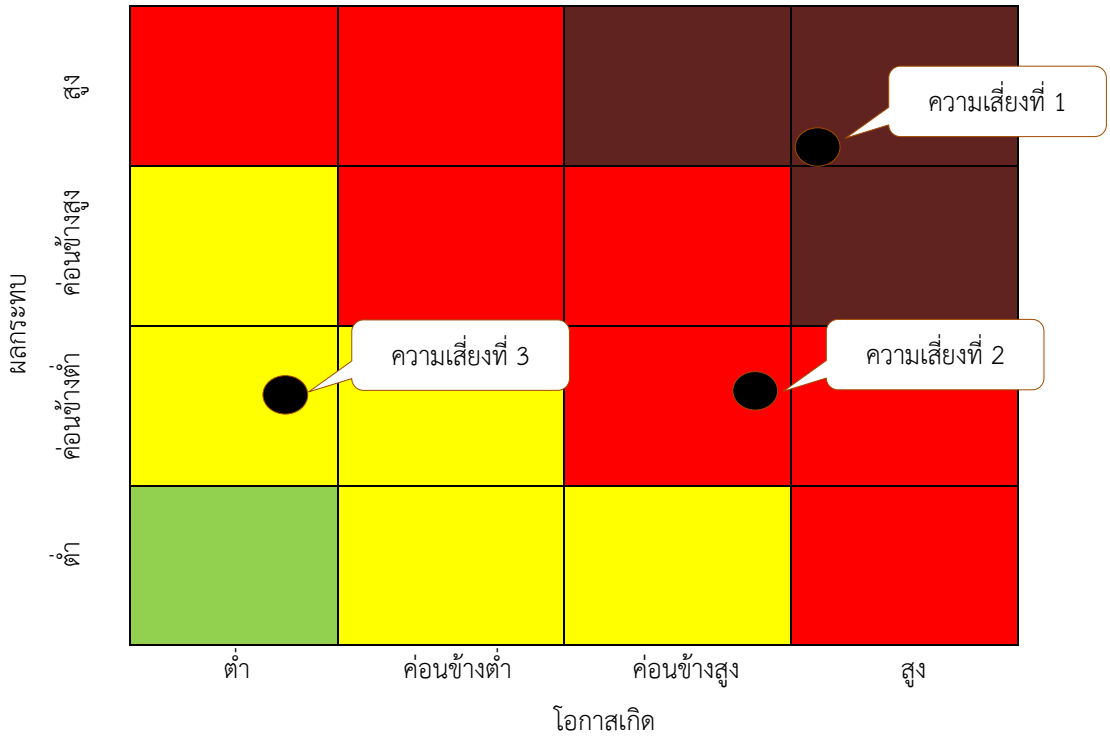
ประเภทของเหตุการณ์	ตัวอย่างเหตุการณ์ความเสี่ยง
5. ความผิดพลาดในการปฏิบัติงานของเจ้าหน้าที่สารสนเทศ (ทั้งความผิดพลาดทั้งที่ตั้งใจและไม่ตั้งใจ)	● ข้อผิดพลาดจากการปฏิบัติงานประจำวัน ● ข้อผิดพลาดจากการบันทึกข้อมูลผิดพลาด หรือการตั้งค่าในระบบ ● อุบัติเหตุต่าง ๆ ที่ทำให้สินทรัพย์สารสนเทศเสียหาย ● การใช้สิทธิการเข้าถึงระบบอย่างไม่เหมาะสม ● การโจรกรรมทรัพย์สินสารสนเทศ ● การจงใจทำลายสร้างความเสียหายแก่ทรัพย์สินสารสนเทศ
6. ข้อมูลสารสนเทศ (การเข้าถึงข้อมูล การรั่วไหลของข้อมูล หรือการสูญหายของข้อมูล)	● การไม่สามารถเข้าถึงข้อมูลที่จำเป็น ● การรั่วไหล หรือการสูญหายของข้อมูลเนื่องจากอุปกรณ์เครื่องมือทางด้านเทคโนโลยีสารสนเทศ ระบบงาน และระบบฐานข้อมูลต่าง ๆ สูญหายหรือถูกทำลาย ● มีความผิดพลาดในการสำรองข้อมูล ● ข้อมูลถูกปรับเปลี่ยน ● มีการเปิดเผยข้อมูลสำคัญอย่างไม่เหมาะสม ทั้งโดยตั้งใจและไม่ตั้งใจ ● การขาดการบริหารจัดการข้อมูลที่เหมาะสมทำให้ไม่สามารถนำข้อมูลที่เก็บไว้มาใช้งานได้ ● ลิขสิทธิ์ หรือทรัพย์สินทางปัญญารั่วไหลเนื่องจากพนักงานลาออก
7. การออกแบบโครงสร้างของระบบงานทางด้านเทคโนโลยีสารสนเทศ	● การออกแบบโครงสร้างเทคโนโลยีสารสนเทศมีความซับซ้อน ไม่ยืดหยุ่น ไม่รองรับการขยายตัวในอนาคต ส่งผลต่อการพลาดโอกาสทางธุรกิจ ● การออกแบบโครงสร้างเทคโนโลยีสารสนเทศไม่สนับสนุนการทำงานในเชิงธุรกิจ ● การออกแบบโครงสร้างเทคโนโลยีสารสนเทศไม่ตอบสนองต่อการปรับใช้กับอุปกรณ์สารสนเทศ หรือระบบงานใหม่ ๆ
8. สาธารณูปโภคทางด้านเทคโนโลยีสารสนเทศ (เครื่องคอมพิวเตอร์ ระบบปฏิบัติการ และเทคโนโลยีต่าง ๆ ที่ช่วยในการดำเนินงาน)	● การใช้ระบบงานสาธารณูปโภคทางด้านเทคโนโลยีสารสนเทศใหม่ ๆ ยังไม่เสถียร ● ระบบงานสาธารณูปโภคทางด้านเทคโนโลยีสารสนเทศไม่รองรับการใช้งานในปริมาณมาก ● ระบบสาธารณูปโภคพื้นฐานเช่น ไฟฟ้า โทรศัพท์ ไม่สามารถใช้งานได้ ● เทคโนโลยีมีความล้าสมัย
9. ระบบงานสารสนเทศ (Software)	● ระบบงานไม่สามารถทำงานได้ตามที่ต้องการ ● ผู้ใช้งานไม่สามารถใช้งานระบบงานใหม่ได้ ● การแก้ไข หรือปรับแต่งโปรแกรมที่ไม่เหมาะสมที่อาจก่อให้เกิดการทุจริตหรือการทำงานของโปรแกรมผิดพลาด ● ปัญหาการใช้งานโปรแกรม โปรแกรมเก่าที่ไม่มีการสนับสนุนโดยผู้ผลิต ● การไม่สามารถกลับไปใช้งานโปรแกรมชุดเก่าในกรณีที่โปรแกรมชุดใหม่มีปัญหา

ประเภทของเหตุการณ์	ตัวอย่างเหตุการณ์ความเสี่ยง
10. ความรับผิดชอบของหน่วยงานธุรกิจ	● หน่วยงานทางธุรกิจไม่มีส่วนร่วมรับผิดชอบในการพัฒนาหรือจัดหาโปรแกรมใหม่ ● มีการใช้โปรแกรมหรือการคำนวณภายนอกระบบงานหลักเป็นจำนวนมาก ซึ่งอาจส่งผลต่อความปลอดภัยและความถูกต้องของข้อมูล รวมทั้งการใช้ทรัพยากรทางด้านเทคโนโลยีสารสนเทศอย่างไม่คุ้มค่า ● มีการจัดซื้อทางด้านเทคโนโลยีสารสนเทศที่ไม่ได้ผ่านกระบวนการการจัดซื้อที่เหมาะสม ● การให้ความต้องการในการใช้ระบบงานไม่เพียงพอ ส่งผลต่อการบริการทางด้านเทคโนโลยีสารสนเทศที่ไม่มีประสิทธิภาพ
11. การบริหารจัดการผู้ให้บริการภายนอก	● ไม่มีการสอบประวัติและความเหมาะสมของผู้ให้บริการภายนอก ● เงื่อนไขการให้บริการ หรือเงื่อนไขในสัญญากับผู้ให้บริการภายนอกไม่เหมาะสม ● การให้บริการของผู้ให้บริการภายนอกไม่ตรงตามมาตรฐานการให้บริการขององค์กร ● ผู้ให้บริการภายนอกไม่สามารถสนับสนุนการดำเนินงานในระยะยาวขององค์กรได้ ● มีการใช้งานโปรแกรมที่ไม่ได้มาตรฐานหรือลิขสิทธิ์ไม่ถูกต้องโดยผู้ให้บริการภายนอก ● ไม่สามารถเปลี่ยนผู้ให้บริการภายนอกได้ เนื่องจากมีการพึ่งพิงผู้ให้บริการภายนอกมากเกินไป ● มีการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ เพื่อการประมวลผลความต้องการของผู้ใช้งาน (cloud computing) โดยไม่ได้รับคำปรึกษาจากหน่วยงานเทคโนโลยีสารสนเทศ ทำให้ไม่สามารถใช้งานร่วมกับระบบสารสนเทศอื่น ๆ ขององค์กรได้
12. การปฏิบัติตามกฎระเบียบข้อบังคับ	● ไม่สามารถปฏิบัติตามกฎระเบียบข้อบังคับต่าง ๆ ● ไม่ตระหนักถึงกฎระเบียบข้อบังคับที่อาจเกิดขึ้น และผลกระทบต่อการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ ● ผู้ออกกฎไม่อนุญาตให้ดำเนินงาน เนื่องจากมีการควบคุมที่ไม่เพียงพอ
13. สภาพทางด้านภูมิรัฐศาสตร์	● ไม่สามารถเข้าถึงระบบสารสนเทศเนื่องจากสภาวการณ์ผิดปกติในสถานที่ต่าง ๆ ● นโยบายของรัฐ หรือ การแทรกแซงจากหน่วยงานราชการที่ทำให้ไม่สามารถให้บริการเทคโนโลยีสารสนเทศได้ ● ระบบสาธารณูปโภคถูกทำลายจากเหตุการณ์ทางการเมือง
14. การโจรกรรม และทำลายสาธารณูปโภคทางด้านเทคโนโลยีสารสนเทศ	● การโจรกรรมอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศทำให้ข้อมูลสำคัญสูญหาย ● ศูนย์คอมพิวเตอร์ถูกทำลาย ● อุปกรณ์สารสนเทศส่วนบุคคลได้รับความเสียหาย

ประเภทของเหตุการณ์	ตัวอย่างเหตุการณ์ความเสี่ยง
15. ชุดคำสั่งที่ไม่ประสงค์ดีต่อระบบสารสนเทศ	● มีการติดตั้งชุดคำสั่งที่ไม่ประสงค์ดีในเครื่องแม่ข่าย ● มีการติดตั้งชุดคำสั่งที่ไม่ประสงค์ดีในเครื่องคอมพิวเตอร์ในระบบงานบ่อยครั้ง ● พนักงานติดตั้งชุดคำสั่งที่ไม่ประสงค์ดีในระบบงานเพื่อก่อให้เกิดความเสียหายในอนาคต ● ข้อมูลสำคัญของบริษัทรั่วไหลเนื่องจากมีการปลอมแปลงเป็นผู้ใช้งานภายในองค์กร (phishing attack)
16. การบุกรุกโจมตีในระบบงานและระบบเครือข่าย	● พบการพยายามเข้าถึงระบบสารสนเทศโดยผู้ไม่มีสิทธิ ● การให้บริการทางด้านเทคโนโลยีสารสนเทศหยุดชะงักเนื่องจากการโจมตีระบบสารสนเทศ ● การเปลี่ยนแปลงข้อมูลในเว็บไซต์ของบริษัท ● พบการแพร่ของไวรัสคอมพิวเตอร์ ● การพยายามบุกรุกโจมตีระบบ (hacking)
17. กิจกรรมที่ไม่คาดฝันในอุตสาหกรรมต่างๆ (เช่นการประท้วง)	● เกิดการประท้วงในบริษัททำให้ไม่สามารถเข้าถึงอุปกรณ์สารสนเทศได้ ● พนักงานไม่สามารถมาทำงานเนื่องจากระบบขนส่ง หรือสาธารณูปโภคอื่น ๆ หยุดดำเนินการเนื่องจากการประท้วง ● ผู้ให้บริการภายนอกไม่สามารถดำเนินงานได้เนื่องจากการประท้วง ● ไม่สามารถเบิกจ่ายเงินเนื่องจากมีการประท้วงในธุรกิจธนาคาร
18. ผลกระทบต่อสิ่งแวดล้อม	● อุปกรณ์ทางด้านเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่เกี่ยวข้องไม่เป็นมิตรต่อสิ่งแวดล้อม
19. ภัยธรรมชาติ	● เหตุการณ์ภัยธรรมชาติ เช่น แผ่นดินไหว น้ำท่วม พายุ
20. นวัตกรรม	● นวัตกรรม และแนวโน้มทางด้านสารสนเทศไม่ได้รับการพิจารณา ● ไม่สามารถปรับใช้เทคโนโลยีใหม่ ๆ ได้ทันเวลา ● เทคโนโลยีใหม่ ๆ ที่สำคัญไม่ได้รับการพิจารณานำมาใช้งาน

ภาคผนวก 2 ตัวอย่าง แผนภาพความเสี่ยง และทะเบียนความเสี่ยง

ตัวอย่างแผนภาพความเสี่ยง



หมายเหตุ: จำนวนระดับความสำคัญของโอกาสเกิด หรือผลกระทบ รวมทั้งการแบ่งระดับความสำคัญของความเสี่ยงสามารถเปลี่ยนแปลงได้ตามกระบวนการและวิธีการประเมินความเสี่ยงของแต่ละองค์กร หรือตามความเหมาะสมตามสภาพแวดล้อม และความสามารถขององค์กร โดยพื้นที่สีเขียวอาจกำหนดให้เป็นพื้นที่ของระดับความเสี่ยงต่ำ พื้นที่สีเหลืองอาจเป็นความเสี่ยงที่ค่อนข้างต่ำซึ่งสามารถยอมรับได้ พื้นที่สีแดงเป็นความเสี่ยงค่อนข้างสูงที่เกินจากความเสี่ยงที่สามารถยอมรับได้ จึงต้องการการบริหารจัดการเพิ่มเติม และส่วนสีแดงเข้มคือความเสี่ยงที่สำคัญมากต้องการการบริหารจัดการอย่างเร่งด่วน

ตัวอย่างทะเบียนความเสี่ยง

ทะเบียนความเสี่ยง	
ส่วนที่ 1 ข้อมูลทั่วไป	
ชื่อความเสี่ยง	
เจ้าของความเสี่ยง	
วันที่ประเมิน	
วันที่ปรับปรุง	
ประเภทของความเสี่ยง	พลาดโอกาสการใช้เทคโนโลยีสารสนเทศให้เกิดประสิทธิภาพ และ ประสิทธิผล / การพัฒนาบริการหรือผลิตภัณฑ์ใหม่ / การปฏิบัติงานประจำวันด้านเทคโนโลยีสารสนเทศ
ระดับความสำคัญ	ต่ำ / ค่อนข้างต่ำ / ค่อนข้างสูง / สูง
ส่วนที่ 2 เหตุการณ์ความเสี่ยง	
ผู้กระทำให้เกิดความเสี่ยง	
ประเภทของความเสี่ยงหรือภัยคุกคาม	
เหตุการณ์ที่อาจเกิดขึ้น	
สินทรัพย์หรือทรัพยากรที่เกี่ยวข้อง	
ช่วงเวลาหรือระยะเวลา	
ส่วนที่ 3 ผลการวิเคราะห์ความเสี่ยง	
ระดับของโอกาสเกิด	ต่ำ / ค่อนข้างต่ำ / ค่อนข้างสูง / สูง
คำบรรยายโอกาสเกิด	
ระดับของผลกระทบ โดยพิจารณาถึง 1. ผลกระทบกับการดำเนินงาน 2. ต้นทุนการตอบสนองต่อความเสี่ยง 3. ความสามารถในการแข่งขัน 4. การปฏิบัติตามระเบียบข้อบังคับ	ต่ำ / ค่อนข้างต่ำ / ค่อนข้างสูง / สูง
คำบรรยายผลกระทบ	
ส่วนที่ 4 การตอบสนองต่อความเสี่ยง	
การตอบสนองต่อความเสี่ยง	หลีกเลี่ยง / ยอมรับ / ร่วมจัดการ / ลด
รายละเอียดเพื่อประกอบการประเมินการตอบสนอง	**1. xxxxx,** สถานการณ์การจัดให้มีการควบคุมในปัจจุบัน สถานการณ์ดำเนินงาน กิจกรรมการควบคุมเพิ่มเติม **2. xxxxx,** สถานการณ์การจัดให้มีการควบคุมในปัจจุบัน สถานการณ์ดำเนินงาน กิจกรรมการควบคุมเพิ่มเติม
รายละเอียดวิธีการตอบสนองความเสี่ยง	
สถานะของการดำเนินงานเพื่อการตอบสนองต่อความเสี่ยง	
ปัญหาที่สำคัญในการดำเนินงาน	
ส่วนที่ 5 ตัวชี้วัดความเสี่ยง	
ตัวชี้วัดความเสี่ยง	**1.** **...**

ภาคผนวก 3 **ตัวอย่างของตัวชี้วัดความเสี่ยงหลัก**

เหตุการณ์ความเสี่ยง	**มุมมอง**		
	CIO (Chief Information Officer)	**CRO (Chief Risk Officer)**	**CEO (Chief Executive Officer) / Board of Directors**
การตัดสินใจในโครงการทางด้านเทคโนโลยีสารสนเทศ	● ร้อยละของโครงการที่ดำเนินการได้ในเวลาและงบประมาณที่กำหนด ● จำนวน และประเภทโครงการที่มีการดำเนินการนอกเหนือจากแผนงานสารสนเทศ	● ร้อยละของโครงการที่ผ่านการตรวจสอบคุณภาพ ● ร้อยละของโครงการที่มีการกำหนดประโยชน์ที่ได้รับจากเทคโนโลยีสารสนเทศที่ชัดเจน	● ร้อยละของโครงการที่ได้ประโยชน์ทางธุรกิจตรงตามหรือมากกว่าที่กำหนด ● ร้อยละของโครงการที่ใช้เงินทุนตามแผนงานหรือกลยุทธ์ทางธุรกิจที่กำหนด
ความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ	● ร้อยละของผู้ใช้งานที่ไม่ทำตามนโยบายรหัสผ่านของบริษัท	● ร้อยละของการเข้าใช้งานระบบสารสนเทศที่น่าสงสัย หรือไม่ตรงตามระดับการเข้าถึงที่กำหนด	● จำนวนเหตุการณ์ หรือปัญหาทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ พร้อมทั้งผลกระทบทางธุรกิจ
ความรู้ความสามารถของพนักงานสารสนเทศ	● ร้อยละของพนักงานสารสนเทศที่เข้าอบรมตามแผนการอบรม ● จำนวนระดับการให้บริการที่ลดลงเนื่องจากปัญหาในการปฏิบัติงานประจำวันทางด้านเทคโนโลยีสารสนเทศ	● จำนวนปัญหาที่พบอันเนื่องมาจากผู้ใช้งานมีความรู้ไม่เพียงพอหรือคู่มือและการอบรมไม่เพียงพอ	● ค่าปรับจากการไม่ปฏิบัติตามกฎระเบียบต่าง ๆ ● จำนวนกรณีที่พนักงานไม่ปฏิบัติตามกฎระเบียบต่าง ๆ ซึ่งส่งผลต่อภาพลักษณ์ และชื่อเสียงของบริษัท