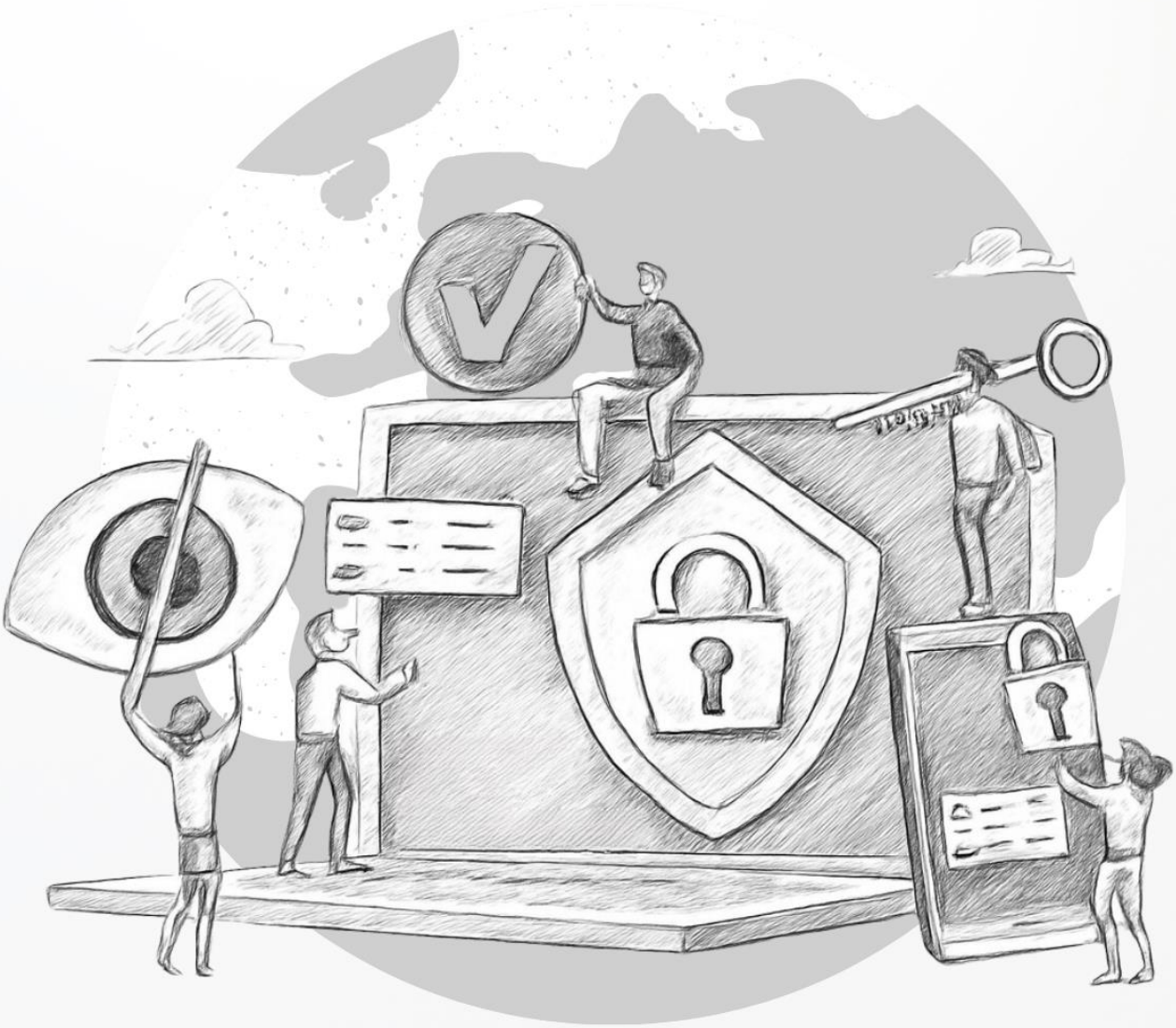
กรอบการกำกับดูแลบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ธันวาคม 2568

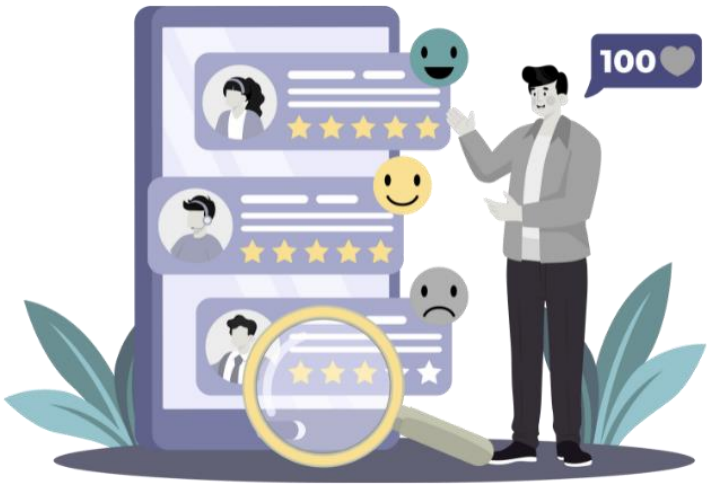
สารบัญ

1. บทนำ

ในยุคที่องค์กรภาคตลาดทุนต้องพึ่งพาบุคคลภายนอกในการดำเนินงานด้านเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นการใช้บริการคลาวด์ การเชื่อมต่อระบบกับพันธมิตร หรือการให้สิทธิ์เข้าถึงข้อมูลสำคัญ ความเสี่ยงจากบุคคลภายนอกจึงกลายเป็นประเด็นสำคัญที่ต้องได้รับการบริหารจัดการอย่างเป็นระบบและสอดคล้องกับมาตรฐานสากล เพื่อรักษาความมั่นคงปลอดภัยของระบบบริการ ความน่าเชื่อถือขององค์กร และความเป็นส่วนตัวของผู้ใช้บริการ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน”) ได้เล็งเห็นถึงความสำคัญและความจำเป็นในการกำหนดแนวทางที่ครอบคลุม และสอดคล้องกับมาตรฐานสากล จึงได้จัดทำกรอบการกำกับดูแลบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ (“กรอบการกำกับดูแล”) ฉบับนี้ขึ้น เพื่อเป็นกรอบการบริหารจัดการความเสี่ยงจากบุคคลภายนอก โดยเฉพาะในบริบทของผู้ประกอบธุรกิจที่ใช้บริการงานด้าน IT จากบุคคลภายนอก หรือมีการเชื่อมต่อระบบ IT กับบุคคลภายนอก หรืออนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ

กรอบการกำกับดูแลนี้ครอบคลุมบุคคลภายนอกใน 3 ลักษณะ ได้แก่ (1) ผู้ให้บริการงานด้านเทคโนโลยีสารสนเทศ (เช่น Cloud Computing) (2) ผู้ที่มีการเชื่อมต่อระบบ IT ของผู้ประกอบธุรกิจ และ (3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ ทั้งนี้ ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบธุรกิจ



2. กรอบการกำกับดูแลบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ

หลักการสำคัญ

หลักการสำคัญในการบริหารจัดการความเสี่ยงจากบุคคลภายนอกประกอบด้วยหลายมิติที่เชื่อมโยงกันอย่างเป็นระบบ ประการแรก คือ การกำกับดูแลที่เข้มแข็ง (Strong Governance) ซึ่งต้องมีการกำหนดบทบาทหน้าที่ของผู้บริหารระดับสูง คณะกรรมการ และหน่วยงานที่เกี่ยวข้องอย่างชัดเจน รวมถึงการจัดโครงสร้างองค์กรตามแนวคิด “Three Lines of Defense” ของ International Organization for Standardization (ISO) ซึ่งแบ่งความรับผิดชอบออกเป็น 3 ระดับ ได้แก่ หน่วยงานปฏิบัติการ หน่วยงานกำกับดูแล และหน่วยงานตรวจสอบอิสระ เพื่อให้เกิดการควบคุมภายในที่มีประสิทธิภาพ

ประการที่สอง คือ การใช้แนวทางตามระดับความเสี่ยง (Risk-Based and Tiered Approach) โดยองค์กรต้องจัดระดับความเสี่ยงของบุคคลภายนอก เช่น Tier 1–3 ตามเกณฑ์ที่ชัดเจน เช่น ปริมาณข้อมูลที่เกี่ยวข้อง ความสำคัญต่อกระบวนการธุรกิจ และผลกระทบเชิงกฎระเบียบ เพื่อให้สามารถจัดสรรทรัพยากรในการติดตามตรวจสอบได้อย่างเหมาะสม ปรับใช้มาตรการตามระดับความเสี่ยง โดยอาจใช้หลัก “ตามสัดส่วนความเสี่ยง (proportionality)” เพื่อให้การกำกับดูแลเหมาะสมและไม่สร้างภาระเกินจำเป็น

ประการที่สาม คือ การบริหารตามวงจรชีวิต (Lifecycle Approach) ซึ่งครอบคลุมตั้งแต่การวางแผน การคัดเลือก การทำสัญญา การติดตามผล ไปจนถึงการยุติความสัมพันธ์กับบุคคลภายนอก โดยต้องมีการประเมินความเสี่ยงในแต่ละขั้นตอนอย่างเหมาะสมตามระดับความสำคัญของบริการ เน้นให้มีขั้นตอนชัดเจน เช่น การตรวจสอบก่อนว่าจ้าง (due diligence) การกำหนดสิทธิการตรวจสอบ และแผนการออกจากสัญญา โดยอาจกำหนดให้มีการประเมินตนเอง และแผนความต่อเนื่องเพิ่มเติม เพื่อให้มั่นใจว่าบริการสำคัญไม่สะดุด

ประการที่สี่ คือ การเสริมความยืดหยุ่นในการดำเนินงาน (Operational Resilience) ซึ่งรวมถึงการเตรียมแผนรองรับเหตุการณ์ฉุกเฉิน การทดสอบแผนอย่างสม่ำเสมอ และการจัดทำ Exit Plan ที่สามารถนำไปใช้ได้จริงเมื่อเกิดเหตุไม่คาดคิด โดยเน้นการทดสอบความสามารถในการฟื้นตัวกลับมาให้บริการได้ตามปกติ และการเตรียมแผนสำรอง อาจกำหนดเป้าหมายความต่อเนื่องของบริการสำคัญ และการรายงานการเตรียมความพร้อม เพื่อสร้างความมั่นใจให้ผู้ใช้บริการ

ประการสุดท้าย คือ หลักความรับผิดชอบ (Accountability) ซึ่งยังคงอยู่ที่องค์กร แม้จะมีการว่าจ้างหรือใช้บริการจากบุคคลภายนอกก็ตาม **องค์กรต้องเป็นผู้กำกับดูแลและรับผิดชอบต่อผลกระทบที่อาจเกิดขึ้นจากการใช้บริการ**เหล่านั้น ดังนั้น ผู้บริหารต้องมั่นใจว่ามีการกำหนดบทบาทและหน้าที่ชัดเจน มีสิทธิในการตรวจสอบและควบคุมตามสัญญามาตรฐาน ซึ่งแนวทางในระดับสากล (ISO 27036 & European Banking Authority (EBA)) ระบุว่า “ความรับผิดชอบของคณะกรรมการและผู้บริหารไม่สามารถโอนไปให้บุคคลภายนอกได้”

นอกจากนี้ ยังต้องพิจารณาหลักกฎหมายเกี่ยวกับตัวกลางและตัวแทน (Intermediary and Agent Liability) ซึ่งมีผลต่อการกำหนดขอบเขตความรับผิดชอบในสัญญาและการบริหารความเสี่ยงร่วมกัน โดยเฉพาะในกรณีที่บุคคลภายนอกมีบทบาทในการจัดการข้อมูลส่วนบุคคลหรือให้บริการที่มีผลกระทบต่อผู้ใช้บริการโดยตรง

การนำกรอบการกำกับดูแลนี้ไปใช้ควรพิจารณาให้เหมาะสมกับลักษณะบริการ ระดับความเสี่ยง และบริบทขององค์กร โดยสามารถปรับใช้ร่วมกับนโยบายอื่น ๆ ที่เกี่ยวข้อง เช่น นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ นโยบายการคุ้มครองข้อมูลส่วนบุคคล และการบริหารความต่อเนื่องทางธุรกิจ เพื่อให้เกิดการบูรณาการที่ครอบคลุมและยั่งยืน

2.1 การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (risk governance)

2.1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

บทบาทของคณะกรรมการและผู้บริหารระดับสูงมีความสำคัญอย่างยิ่งในการกำหนดทิศทางและกรอบการบริหารความเสี่ยงจากบุคคลภายนอก (Third-Party Risk Management: TPRM) โดยต้องกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) อนุมัตินโยบาย Third-Party Risk Management ขอบเขตการใช้บริการจากบุคคลภายนอก รวมถึงทบทวนนโยบายและผลการบริหารความเสี่ยงอย่างสม่ำเสมอ และตรวจสอบให้แน่ใจว่ามีการจัดสรรทรัพยากรเพียงพอสำหรับการบริหารความเสี่ยง เพื่อให้มั่นใจว่าความเสี่ยงจากบุคคลภายนอกถูกบูรณาการอยู่ในกลยุทธ์และระดับความเสี่ยงที่องค์กรยอมรับ (Risk Appetite) นอกจากนี้ ยังต้องมี oversight ต่อบริการที่มีความสำคัญต่อธุรกิจ (critical/important functions) รวมถึงรับรองการปฏิบัติตามกฎหมายและข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

การพัฒนาความรู้และความสามารถของบุคลากรเป็นอีกหนึ่งองค์ประกอบสำคัญ องค์กรควรจัดฝึกอบรมเกี่ยวกับการบริหารความเสี่ยงจากบุคคลภายนอก ความมั่นคงไซเบอร์ และการปฏิบัติตามข้อกำหนด เพื่อสร้างวัฒนธรรมความตระหนักด้านความเสี่ยงในทุกระดับขององค์กร โดยเริ่มจากการกำหนดทักษะขั้นต่ำสำหรับผู้รับผิดชอบ TPRM และจัดให้มีการฝึกอบรมในด้านสำคัญ เช่น IT Security, Cloud, Business Continuity Management (BCM) และ Vendor Governance นอกจากนี้ควรสนับสนุนให้บุคลากรมีความเข้าใจข้อกำหนดด้านกฎระเบียบ เช่น Cloud Guideline และ Outsourcing Rules เพื่อให้การดำเนินงานสอดคล้องกับมาตรฐานและข้อบังคับที่เกี่ยวข้อง

กลไกการรายงานความเสี่ยงต้องมีความชัดเจนและโปร่งใส โดยควรจัดทำรายงานสถานะความเสี่ยงและ Risk Dashboard เพื่อนำเสนอข้อมูลต่อคณะกรรมการอย่างสม่ำเสมอ รวมถึงแจ้งเหตุการณ์สำคัญต่อหน่วยงานกำกับดูแล เช่น ก.ล.ต. ตามข้อกำหนดของกฎหมายและมาตรฐานสากล เพื่อเสริมความโปร่งใสและความรัดกุม ควรใช้หลักการ Four Eyes ในจุดสำคัญ โดยเฉพาะการอนุมัติหรือการตรวจสอบรายงานความเสี่ยงที่มีนัยสำคัญ ซึ่งต้องได้รับการตรวจสอบจากสองฝ่าย เช่น คณะกรรมการและผู้บริหารระดับสูงร่วมกันเพื่อป้องกันความผิดพลาด และลดความเสี่ยงจากการตัดสินใจฝ่ายเดียว

สุดท้าย การบริหารจัดการความเสี่ยงจากบุคคลภายนอกต้องบูรณาการกับนโยบายหลักขององค์กร ได้แก่ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy) เพื่อควบคุมการเข้าถึงและรักษาความลับของข้อมูล นโยบายการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance) เพื่อป้องกันการละเมิดข้อมูล และแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อเตรียมพร้อมรับมือเหตุการณ์หยุดชะงักที่เกี่ยวข้องกับบุคคลภายนอก

มีข้อกำหนดเพิ่มเติมที่ต้องเน้น ได้แก่

1. การรายงานด้านการกำกับดูแล (Governance Reporting)

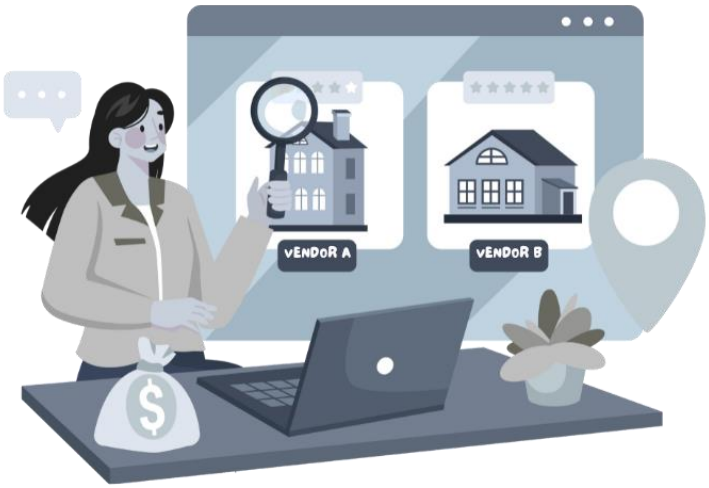
ต้องมีระบบรายงานที่สม่ำเสมอ เช่น dashboard, KRI และ heat map ทะเบียนความเสี่ยง เพื่อให้คณะกรรมการรับทราบสถานะความเสี่ยงและแนวโน้ม[1] [2]

2. การอนุมัติเกณฑ์ความสำคัญและความทนทานต่อผลกระทบ (Criticality & Tolerance Approval)

คณะกรรมการต้องอนุมัติหลักเกณฑ์ในการจำแนกบริการที่มีความสำคัญต่อธุรกิจ รวมถึงระดับที่ยอมรับได้ต่อผลกระทบ เพื่อให้แน่ใจว่าการบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ[1] [3]

3. สิทธิในการตรวจสอบตามสัญญา (Contractual Audit Rights)

ต้องระบุสิทธิในการตรวจสอบอย่างชัดเจนในสัญญา ครอบคลุมทั้งการตรวจสอบโดยตรง (Direct Audit – Onsite), การตรวจสอบทางอ้อม (Indirect Audit – ผ่านรายงาน SOC 2 Type II หรือ ISO 27001) และการตรวจสอบผู้รับเหมาช่วง (Subcontractors)[1] [3]



[1] Digital Operational Resilience Act – DORA (2022)

[2] NIST. SP 800-161 Revision 1: Cybersecurity Supply Chain Risk Management (2022)

[3] European Banking Authority. Guidelines on Outsourcing Arrangements (2021)

2.1.2 นโยบายและมาตรฐานการบริหารความเสี่ยงจากบุคคลภายนอก

องค์กรต้องมีนโยบายและมาตรฐานที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อกำหนดกรอบการบริหารความเสี่ยงจากบุคคลภายนอก โดยครอบคลุมตั้งแต่การนิยามและการจำแนกระดับบริการ ขอบเขตของ TPRM และตลอดวงจรชีวิต (lifecycle) ที่เริ่มตั้งแต่การประเมินความเสี่ยง การคัดเลือก การทำสัญญา การติดตาม (Monitoring) ไปจนถึงการยุติความสัมพันธ์ (Exit) นโยบายต้องระบุข้อกำหนดควบคุมขั้นต่ำ เช่น การควบคุมการเข้าถึง (Access Control), การเข้ารหัสข้อมูล (Encryption) และการจัดการความต่อเนื่องทางธุรกิจ

นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกควรสอดคล้องกับนโยบายอื่นที่เกี่ยวข้องของผู้ให้บริการและผู้ประกอบธุรกิจ เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกควรได้รับอนุมัติจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและควบคุมดูแลให้ปฏิบัติตามนโยบาย

ทั้งนี้ นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกควรครอบคลุมในเรื่อง

(1) โครงสร้างการกำกับดูแล บทบาทหน้าที่ของผู้เกี่ยวข้องในการกำกับดูแลและบริหารจัดการความเสี่ยงจากบุคคลภายนอก

(2) หลักเกณฑ์การจัดระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(3) การบริหารจัดการความเสี่ยงที่ครอบคลุมวงจรการบริหารจัดการบุคคลภายนอก (third party management life cycle) และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตามหลัก CIA

(4) หลักเกณฑ์การขออนุมัติความเห็นชอบ และการรายงานต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

(5) การตรวจสอบการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(6) การเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญ เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจสามารถดำเนินธุรกิจ ได้อย่างต่อเนื่อง ซึ่งรวมถึงการมีข้อมูลพร้อมใช้สำหรับการดำเนินธุรกิจและการให้บริการแก่สมาชิก ผู้ใช้บริการหรือลูกค้า

(7) การคุ้มครองผู้ใช้บริการของระบบหรือลูกค้าของผู้ให้บริการและผู้ประกอบธุรกิจ

ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีมาตรฐานและระเบียบวิธีปฏิบัติเพื่อสนับสนุนการดำเนินการตามนโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ให้สอดคล้องตามขอบเขตระดับความเสี่ยงและความมีนัยสำคัญ รวมถึงมาตรฐานสากลที่ยอมรับโดยทั่วไป

มีข้อกำหนดเพิ่มเติมที่ต้องเน้น ได้แก่

1. นโยบาย TPRM ครอบคลุมทั้งองค์กรและกลุ่มบริษัท (Enterprise/Group-wide Policy)

หากองค์กรมีการใช้บริการจากบริษัทในเครือหรือจากบริษัทแม่ จำเป็นต้องระมัดระวัง Blind Trust ซึ่งอาจเป็นความเสี่ยงที่ว่า ผู้ให้บริการภายนอกที่มาจากบริษัทในเครือนั้น อาจมีช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์และอาจขาดการซ้อมแผน BCP/DRP อย่างเป็นประจำ และบริษัทละเลยการตรวจสอบจากความเชื่อมั่น ซึ่งอาจส่งผลให้เกิดความเสี่ยงด้านกระจุกตัวและ single point of failure ส่งผลกระทบในวงกว้างได้ (concentration risk)

2. ข้อกำหนดด้านการรายงาน (Reporting Requirements)

นโยบายต้องระบุรูปแบบการรายงาน เช่น Key Risk Indicators (KRIs) ความถี่ในการรายงาน และระยะเวลาที่ใช้ในการรายงานเหตุการณ์ (event reporting timeline) เพื่อสร้างความโปร่งใสและความพร้อมในการตอบสนอง

3. การกำกับดูแลความเสี่ยงด้านการกระจุกตัวและเชิงระบบ (Concentration & Systemic Risk Governance)

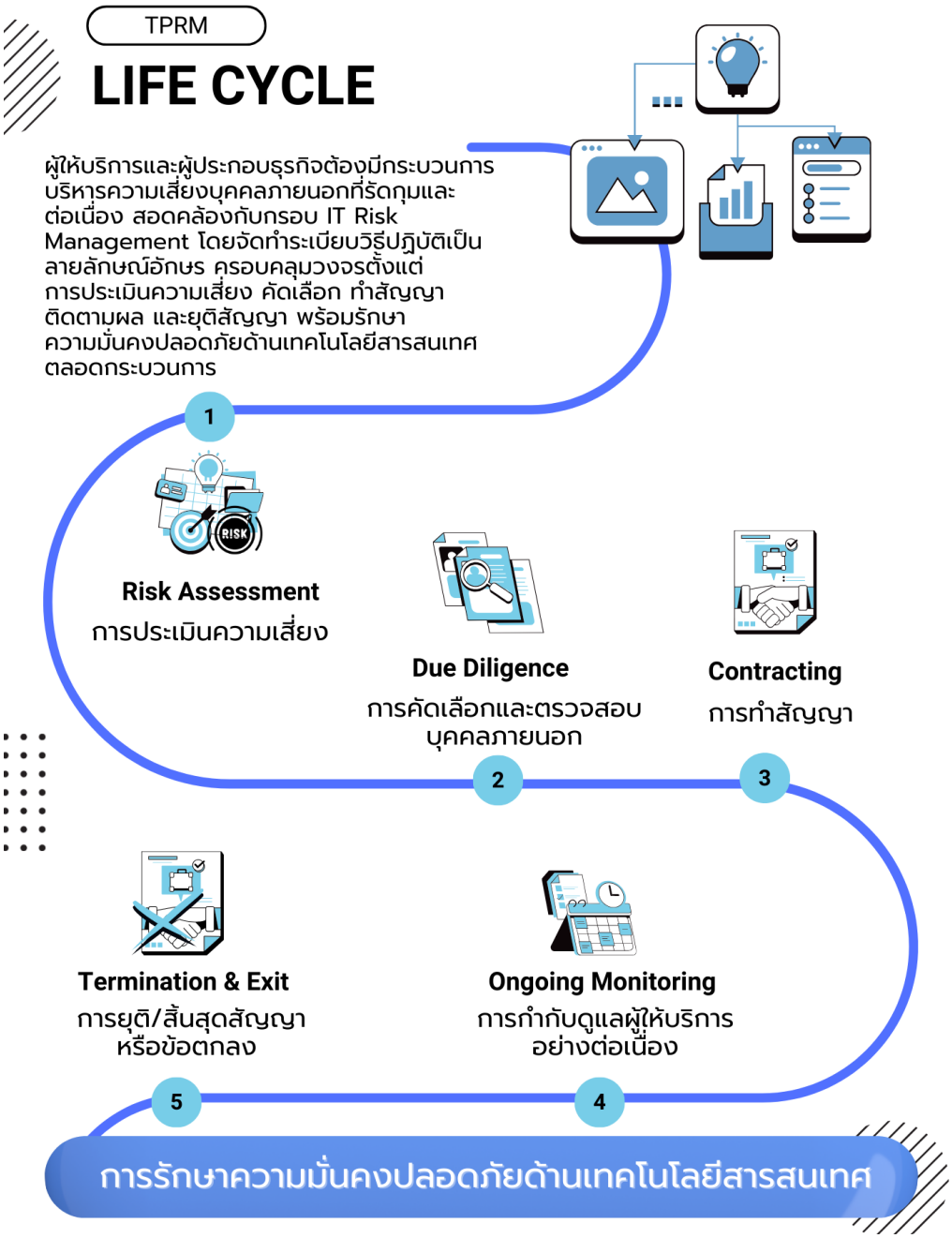
ต้องมีกระบวนการตรวจสอบความเสี่ยงจากการพึ่งพาผู้ให้บริการรายใหญ่ เช่น การตรวจสอบความเสี่ยงจากการใช้ Cloud Provider รายเดียว การประเมินความเชื่อมโยงในห่วงโซ่อุปทาน และการบริหารจัดการความเสี่ยงเชิงระบบ [4] [5]

[4] Digital Operational Resilience Act – DORA (2022)

[5] NIST. SP 800-161 Revision 1: Cybersecurity Supply Chain Risk Management (2022)

2.2 การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

2.2.1 การบริหารจัดการความเสี่ยงจากบุคคลภายนอกตลอดวงจรชีวิต



การบริหารความเสี่ยงจากบุคคลภายนอกต้องดำเนินการอย่างต่อเนื่องตลอดวงจรชีวิต ไม่ใช่เพียงแค่ก่อนการทำสัญญา โดยเริ่มจาก **การประเมินความเสี่ยง** (Risk Assessment) เพื่อระบุระดับความสำคัญของบริการและผลกระทบที่อาจเกิดขึ้นต่อธุรกิจ จากนั้นเข้าสู่ขั้นตอน **การตรวจสอบก่อนการคัดเลือก** (Due Diligence) ซึ่งเป็นการประเมินความน่าเชื่อถือของคู่ค้าในหลายมิติ เช่น สถานะทางการเงิน ความมั่นคงปลอดภัยทางไซเบอร์ ชื่อเสียง และการปฏิบัติตามกฎหมาย เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นในอนาคต

เมื่อผ่านการคัดเลือกแล้ว ขั้นตอน **การทำสัญญา (Contracting)** มีความสำคัญอย่างยิ่ง โดยต้องกำหนดเงื่อนไขที่ชัดเจน เช่น ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) สิทธิในการตรวจสอบ (Right to Audit) เงื่อนไขการออกจากสัญญา (Exit Plan) และข้อกำหนดด้านการคุ้มครองข้อมูล และการรักษาความลับ (non-disclosure agreement) เพื่อสร้างความมั่นใจว่าความเสี่ยงได้รับการควบคุมอย่างเหมาะสม

หลังจากเริ่มความสัมพันธ์ องค์กรต้องดำเนินการ **ติดตามต่อเนื่อง (Ongoing Monitoring)** โดยใช้ตัวชี้วัดประสิทธิภาพ (KPI) และการตรวจสอบตามรอบระยะเวลา รวมถึงการทบทวนความเสี่ยงเป็นประจำ เพื่อให้มั่นใจว่าบุคคลภายนอกยังคงปฏิบัติตามมาตรฐานที่กำหนด และสามารถตอบสนองต่อเหตุการณ์ผิดปกติได้ทันเวลา

ในกรณีที่ต้อง **ยุติและออกจากสัญญา (Termination & Exit)** องค์กรต้องมีแผนการออกจากสัญญาที่ครอบคลุมการส่งคืนหรือลบข้อมูล การถ่ายโอนงานอย่างปลอดภัย และการลดผลกระทบต่อธุรกิจ เพื่อให้การเปลี่ยนแปลงเกิดขึ้นอย่างราบรื่นและไม่กระทบต่อความต่อเนื่องของบริการ นอกจากนี้ การบันทึกหลักฐานและการตรวจสอบย้อนกลับเป็นสิ่งจำเป็น เพื่อรองรับการตรวจสอบจากหน่วยงานกำกับดูแลและพิสูจน์การปฏิบัติตามข้อกำหนด กระบวนการทั้งหมดนี้ต้องบูรณาการกับนโยบายหลักขององค์กร เช่น IT Security, PDPA และ Business Continuity เพื่อสร้างความมั่นคงและความยืดหยุ่นในระยะยาว

(1) ระยะที่ 1: การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นจุดเริ่มต้นสำคัญที่กำหนดระดับการกำกับดูแลที่เหมาะสมกับผู้ให้บริการแต่ละราย โดยต้องพิจารณาทั้งมิติกลยุทธ์และการดำเนินงาน กิจกรรมหลักประกอบด้วยการประเมินความจำเป็นในการใช้บริการภายนอก วิเคราะห์ผลกระทบต่อธุรกิจ และจำแนกระดับความสำคัญของบริการตามเกณฑ์สากล เช่น DORA/EBA (critical, important, non-critical) นอกจากนี้ต้องประเมินประเภทความเสี่ยงที่เกี่ยวข้อง ได้แก่ **Cyber**, **Operational**, **Compliance**, **Data Privacy**, **Financial, Sovereign** และ **Reputation Risk** พร้อมระบุข้อมูลหรือระบบที่เกี่ยวข้อง รวมถึงความอ่อนไหวของข้อมูลที่ผู้ให้บริการสามารถเข้าถึง

ผู้ประกอบธุรกิจควรประเมินความเสี่ยงและผลกระทบก่อน (1) การใช้บริการงานด้าน IT จากบุคคลภายนอก (2) การเชื่อมต่อระบบ IT กับบุคคลภายนอก และ (3) การอนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ โดยควรคำนึงถึงความเสี่ยงดังต่อไปนี้

(1) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น

(2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่รัดกุมเพียงพอ เช่น การไม่สามารถตรวจสอบการดำเนินงานของบุคคลภายนอกได้ด้วยตนเอง เป็นต้น

(3) ความเสี่ยงจากการกระจุกตัว (concentration risk) เช่น ผู้ประกอบธุรกิจและบริษัทในกลุ่มธุรกิจเดียวกันใช้บริการจากบุคคลภายนอกเพียงรายเดียว เป็นต้น

(4) ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก (third party/vendor locked-in) ซึ่งทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

(5) ความเสี่ยงด้าน IT และภัยทางไซเบอร์ เช่น ระบบที่ให้บริการโดยบุคคลภายนอกเกิดขัดข้อง ระบบของบุคคลภายนอกมีช่องโหว่ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล เป็นต้น

(6) ความเสี่ยงกรณีบุคคลภายนอกให้ผู้อื่นดำเนินการแทน (sub-contracting) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น

นอกจากนี้ อาจมีความเสี่ยงด้านอื่น ๆ ที่ควรพิจารณาเพิ่มเติม เช่น

- ความเสี่ยงด้านการดำเนินงาน (Operational Risk) - ความเสี่ยงที่เกิดจากความบกพร่องของกระบวนการภายในของบุคคลภายนอก เช่น การจัดการบุคลากรที่ไม่เพียงพอ การหยุดงาน การส่งมอบบริการที่ไม่ได้มาตรฐาน หรือการขาดแผนสำรอง (BCP/DR) ที่มีประสิทธิภาพ
- ความเสี่ยงด้านการเงิน (Financial Risk) - ความเสี่ยงที่เกิดจากฐานะทางการเงินของบุคคลภายนอกไม่มั่นคง เช่น การล้มละลาย การขาดสภาพคล่อง ซึ่งจะส่งผลกระทบต่อความต่อเนื่องของการให้บริการอย่างรุนแรง
- ความเสี่ยงด้านชื่อเสียง (Reputational Risk) - ความเสี่ยงที่บุคคลภายนอกดำเนินการโดยขาดจริยธรรม หรือมีข่าวเสียหาย (นอกเหนือจากเหตุข้อมูลรั่วไหล) ซึ่งส่งผลกระทบโดยตรงต่อภาพลักษณ์และความเชื่อมั่นของบริษัท

ทั้งนี้ ผู้ประกอบธุรกิจอาจจัดให้มีการกำหนดระดับความมีนัยสำคัญของบุคคลภายนอกแต่ละราย ในลักษณะใช้วิธีการประเมินความเสี่ยง การคำนวณระดับความเสี่ยง (Likelihood x Impact) และเกณฑ์การยอมรับความเสี่ยง (Risk Acceptance Criteria) **ตามที่กำหนดไว้ใน แนวปฏิบัติในการจัดให้มีระบบสารสนเทศ ฉบับปัจจุบัน** *(สามารถศึกษาและปรับใช้เทมเพลตตัวอย่างในไฟล์ ภาคผนวก – เครื่องมือประเมินความเสี่ยงบุคคลภายนอก ชีท a. Risk_Assessment_Template)*

ข้อเสนอแนะเพิ่มเติม

การพิจารณาความเสี่ยงของผู้ให้บริการที่มีการเก็บรักษาหรือเข้าถึงข้อมูล

ระบุข้อมูลที่ผู้ให้บริการจะเข้าถึง เช่น PII, PDPA, account-level credentials[6] และหากเป็นบริษัทในเครือ ควรตรวจสอบว่ามี data segregation หรือไม่ หากใช้งานโครงสร้างพื้นฐานเดียวกัน (common infra) ทำให้มีความเสี่ยงสูงขึ้น

[6] ISO/IEC 27036 Series: Supplier Security Management (2021–2023)

(2) ระยะที่ 2: การคัดเลือกและตรวจสอบบุคคลภายนอก (Due Diligence & Third-Party Selection)

หลังจากการประเมินความเสี่ยง องค์กรต้องดำเนินการคัดเลือกและตรวจสอบบุคคลภายนอกอย่างรอบคอบ เพื่อให้มั่นใจว่าผู้ให้บริการมีความสามารถและความน่าเชื่อถือเพียงพอ กิจกรรมหลักประกอบด้วยการวิเคราะห์ความสามารถทางการเงิน ประวัติการให้บริการ ความมั่นคงปลอดภัย และการปฏิบัติตามข้อกำหนด (Compliance) รวมถึงตรวจสอบการปฏิบัติตามมาตรฐานสากล เช่น ISO 27001, SOC 2 และ CSA STAR หากมี นอกจากนี้ต้องตรวจสอบ Governance Model, Incident Management, ความพร้อมด้าน BCM/DR และประเมินการใช้ Subcontractors เพื่อระบุความเสี่ยงในห่วงโซ่อุปทาน

1. ผู้ประกอบธุรกิจควรกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอกอย่างชัดเจน และเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกจะสามารถให้บริการได้ตรงตามความต้องการของผู้ประกอบธุรกิจ

ทั้งนี้ การตัดสินใจในการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่มีความเสี่ยงหรือมีนัยสำคัญ ควรได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

2. ผู้ประกอบธุรกิจควรประเมินศักยภาพบุคคลภายนอก (due diligence) ให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยคำนึงถึงเรื่องดังต่อไปนี้

(1) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา

(2) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน

(3) การรักษาความมั่นคงปลอดภัยด้าน IT

(4) การบริหารจัดการความต่อเนื่องทางธุรกิจและความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ

(5) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง หรือการตรวจสอบประวัติด้านการกระทำความผิด เป็นต้น

(6) การปฏิบัติตามมาตรฐานสากลด้าน IT เช่น การตรวจสอบเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO/IEC 27001 เป็นต้น โดยการรับรองการปฏิบัติตามมาตรฐานสากล ผู้ประกอบธุรกิจควรพิจารณาว่า บุคคลภายนอกได้รับการรับรองในส่วนระบบที่สำคัญ ระบบที่ผู้ประกอบธุรกิจใช้บริการ เชื่อมต่อหรือเข้าถึงข้อมูล หรือได้รับการรับรองครอบคลุมทั้งองค์กร

(7) การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบหรือข้อมูลไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

(8) กรณีที่บุคคลภายนอกมอบหมายการปฏิบัติงานที่สำคัญให้กับบุคคลอื่นต่อ (sub-contracting to another supplier) ผู้ประกอบธุรกิจควรพิจารณารายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศของบุคคลดังกล่าวด้วย

(9) ผู้ประกอบธุรกิจควรจัดให้มีการประเมินด้านคุณภาพและความน่าเชื่อถือของบุคคลภายนอก โดยพิจารณาจากประสบการณ์ คุณภาพของบริการและผลงานที่ส่งมอบ ตลอดจนมาตรฐานด้านความปลอดภัย IT ที่เกี่ยวข้องกับสินค้าและบริการ และจัดทำเป็นรายชื่อบุคคลภายนอกที่เชื่อถือได้ (trusted third-party/trusted vendor) เพื่อใช้เป็นส่วนหนึ่งของเกณฑ์การคัดเลือกผู้ให้บริการในอนาคต *(สามารถศึกษาและปรับใช้เทมเพลตตัวอย่างในไฟล์ ภาคผนวก - เครื่องมือประเมินความเสี่ยงบุคคลภายนอก ชีท b. Due_Diligence_Template)*

ข้อเสนอแนะเพิ่มเติม

1. การตรวจสอบการควบคุมทางเทคนิค (Technical Controls Validation)

องค์กรต้องตรวจสอบว่ามีการใช้งานมาตรการควบคุมทางเทคนิคที่สำคัญจริง ไม่ใช่เพียงระบุในนโยบาย เช่น การใช้ Multi-Factor Authentication (MFA) ที่มีการตั้งค่า ระยะเวลา OTP (One-Time Password) ให้เหมาะสมตามมาตรฐาน (เช่น 30–60 วินาทีตาม NIST SP 800-63B) เพื่อป้องกันการโจมตีแบบ brute-force และ replay attack การเข้ารหัสข้อมูลทั้งขณะพักและขณะส่งผ่าน (Encryption at Rest & In Transit) ระบบบริหารสิทธิ์ผู้ใช้งาน (Identity & Access Management: IAM) และการบันทึกเหตุการณ์ (Logging & Monitoring) การตรวจสอบต้องทำในระดับการตั้งค่าจริง (implementation review) โดยขอหลักฐาน เช่น configuration screen หรือผลการทดสอบ ไม่ใช่อาศัยความไว้วางใจในนโยบายของกลุ่มบริษัท อ้างอิงมาตรฐานสากล เช่น ISO 27002/27017/27018, NIST SP 800-63B, และ OWASP ASVS เพื่อยืนยันความครบถ้วนของการควบคุม

2. การทดสอบเจาะระบบและการประเมินช่องโหว่ (Pen Test & Vulnerability Assessment Review)

องค์กรต้องตรวจสอบว่าผู้ให้บริการมีการทำ Penetration Test อย่างน้อยปีละครั้ง พร้อมรายงานผลการประเมินช่องโหว่ (Vulnerability Assessment) และแผนการแก้ไข (Remediation Plan) ที่ดำเนินการเสร็จสิ้นตาม SLA หากการควบคุมถูกจัดการแบบรวมศูนย์โดยบริษัทแม่ ต้องตรวจสอบว่าระบบขององค์กรอยู่ในสภาพแวดล้อมที่แยกจากระบบอื่นหรือเป็นแบบ shared environment เพื่อประเมินความเสี่ยงที่แท้จริง การตรวจสอบนี้ควรอ้างอิงมาตรฐาน NIST 800-53 และ ISO 27036-3 เพื่อให้แน่ใจว่ากระบวนการทดสอบและการแก้ไขช่องโหว่เป็นไปตามแนวทางสากล

3. การตรวจสอบเส้นทางข้อมูล (Data Flow Validation)

องค์กรต้องมีความเข้าใจที่ชัดเจนเกี่ยวกับการไหลของข้อมูล (Data Flow) โดยตรวจสอบแผนผังการไหลของข้อมูล (Data Flow Diagram) เพื่อระบุว่าข้อมูลถูกจัดเก็บที่ใดอยู่ในภูมิภาคใด และมีการใช้ผู้ให้บริการต่อเนื่อง (Subprocessor) หรือไม่ ข้อมูลเหล่านี้สำคัญต่อการประเมินความเสี่ยงด้านกฎหมายและการปฏิบัติตามข้อกำหนด เช่น PDPA และข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล แม้เป็นบริษัทในเครือ ต้องระบุ data locality อย่างชัดเจน เช่น เซิร์ฟเวอร์อยู่ต่างประเทศ เพื่อให้มั่นใจว่าการจัดการข้อมูลสอดคล้องกับข้อกำหนด

4. วิธีการตรวจสอบทางเลือกสำหรับ Cloud (Alternative Assurance for Cloud)

ในกรณีที่ไม่สามารถตรวจสอบแบบ Onsite ได้ ต้องใช้รายงานการรับรองจากบุคคลที่สาม เช่น SOC 2, CSA STAR หรือมาตรฐาน ISO 27017/27018 เพื่อสร้างความมั่นใจในความปลอดภัยของบริการ Cloud

(3) ระยะที่ 3: การทำสัญญา (Contracting & Agreement Management)

การทำสัญญาเป็นขั้นตอนสำคัญที่ต้องกำหนดกลไกควบคุมและความชัดเจนในเงื่อนไข เพื่อสร้างความมั่นใจว่าผู้ให้บริการปฏิบัติตามมาตรฐานที่องค์กรกำหนด กิจกรรมหลักประกอบด้วยการจัดทำสัญญาที่ระบุ SLA/KPI อย่างชัดเจน กำหนดสิทธิในการตรวจสอบ (Right to Audit) และข้อกำหนดด้านความปลอดภัยข้อมูล เช่น Data Residency, Encryption, Access Control รวมถึงระบุรูปแบบการรายงานและระยะเวลาแจ้งเหตุการณ์ (Incident Notification Timeline)

ผู้ประกอบธุรกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและบุคคลภายนอก เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบ

ในการรักษาความมั่นคงปลอดภัยของระบบ IT ในระดับที่เหมาะสม โดยมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้

(1) ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก

(2) บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอกและผู้ประกอบธุรกิจ

(3) มาตรฐานขั้นต่ำในการปฏิบัติงานของบุคคลภายนอก เช่น การรักษาความปลอดภัยของระบบ IT การรักษาความลับของข้อมูล และการไม่นำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ เป็นต้น

(4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement : SLA) สำหรับการใช้บริการจากบุคคลภายนอก และความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการที่ไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น

(5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือปัญหาที่สำคัญ และการรายงานเหตุการณ์ผิดปกติอย่างทันการณ์

(6) รายชื่อ และช่องทางการติดต่อในกรณีเกิดปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบ IT

(7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก

(8) เงื่อนไขหรือสิทธิของผู้ประกอบธุรกิจในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลงกับบุคคลภายนอก เช่น กรณีที่บุคคลภายนอกมีการละเมิดสัญญาหรือข้อตกลง เป็นต้น

(9) การจัดให้มีทรัพยากร เช่น บุคลากร ระบบงาน และเทคโนโลยี เป็นต้น ที่สอดรับกับแผนฉุกเฉินด้าน IT ของผู้ประกอบธุรกิจ (Recovery Point Objective (RPO) Maximum Tolerable Downtime (MTD) และ Recovery Time Objective (RTO))

หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ

ผู้ประกอบธุรกิจควรกำหนดสิทธิให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานด้าน IT และการควบคุมภายในของบุคคลภายนอกที่ให้บริการงานด้าน IT รายที่มีนัยสำคัญ โดยระบุไว้เป็นส่วนหนึ่งของข้อตกลงหรือสัญญาการให้บริการ

ในกรณีที่ไม่สามารถระบุสิทธิดังกล่าวได้ ผู้ประกอบธุรกิจควรพิจารณาเลือกใช้บุคคลภายนอกที่มีการดำเนินการตรวจสอบด้าน IT โดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น ผลการตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 Type 2 Report) หรือ PCI-DSS Attestation of Compliance (AOC) เป็นต้น นอกจากนี้ ผู้ประกอบธุรกิจควรพิจารณารายละเอียดของผลการตรวจสอบที่จัดทำโดยผู้ตรวจสอบภายนอกอย่างเหมาะสม

นอกจากนี้ ควรมี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้า และควรมีรายละเอียดครอบคลุม ขอบเขตความรับผิดชอบ การรายงานผู้ประกอบธุรกิจเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา

ทั้งนี้ non-disclosure agreement อาจกำหนดไว้เป็นส่วนหนึ่งของสัญญาหรือข้อตกลงกับบุคคลภายนอกได้ *(สามารถศึกษาและปรับใช้เทมเพลตตัวอย่างในไฟล์ ภาคผนวก - เครื่องมือประเมินความเสี่ยงบุคคลภายนอก ชีท c. Contract Agreement Checklist)*

ข้อเสนอแนะเพิ่มเติม

1. การกำกับดูแลในสัญญา (Contractual Governance)

สัญญาต้องครอบคลุมสิทธิในการตรวจสอบทั้งแบบ Onsite และ Offsite (ผ่านรายงาน SOC 2 หรือ ISO 27001) เงื่อนไขการใช้ Sub-outsourcing (การอนุมัติ การแจ้ง และข้อจำกัด) การเก็บรักษาและการคืน/ลบข้อมูลหลังสิ้นสุดสัญญา รวมถึงข้อกำหนดด้าน Change Management และการอัปเดตเทคโนโลยี[7] [8]

2. การคุ้มครองข้อมูลของลูกค้าและข้อมูลสำคัญขององค์กรตามหลักการ CIA (Confidentiality, Integrity, Availability) และข้อกำหนด PDPA

เพื่อสร้างความมั่นใจว่าข้อมูลได้รับการปกป้องอย่างเหมาะสม มาตรการรักษาความปลอดภัยต้องครอบคลุมทั้งข้อมูลที่จัดเก็บ (Data at Rest) ข้อมูลที่ส่งผ่านเครือข่าย (Data in Transit) และข้อมูลที่อยู่บนอุปกรณ์ปลายทาง (Data at Endpoint) โดยใช้เทคโนโลยีและกระบวนการที่สอดคล้องกับมาตรฐานสากล เช่น **ISO/IEC 27001** และ **NIST Cybersecurity Framework** ซึ่งแนะนำการเข้ารหัสข้อมูล การจัดการกุญแจ และการควบคุมการเข้าถึงอย่างเข้มงวด

3. ข้อกำหนด Exit & Transition Plan

ต้องระบุแผนการยุติและการโอนย้ายบริการ (Exit & Transition Plan) ตั้งแต่เริ่มทำสัญญา ไม่ใช่รอจนถึงปลายทาง เพื่อให้มั่นใจว่าการยุติความสัมพันธ์กับผู้ให้บริการสามารถทำได้อย่างปลอดภัยและต่อเนื่อง[7] [9]

(4) ระยะที่ 4: การกำกับดูแลผู้ให้บริการอย่างต่อเนื่อง (Ongoing Monitoring)

หลังจากทำสัญญาแล้ว องค์กรต้องติดตามและประเมินผลการปฏิบัติงานของผู้ให้บริการอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีการปฏิบัติตามเงื่อนไขและมาตรฐานที่กำหนด กิจกรรมหลักประกอบด้วย การตรวจสอบผลการดำเนินงานเทียบกับ SLA/KPI ติดตามรายงานด้านความมั่นคงปลอดภัย เหตุการณ์ผิดปกติ และการหยุดชะงัก รวมถึงการตรวจทานหลักฐาน เช่น Certification, Penetration Test Report และ Vulnerability Report พร้อมทั้งจัดประชุมทบทวนสถานะกับผู้ให้บริการเป็นระยะ

ผู้ประกอบธุรกิจควรกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้

[7] Digital Operational Resilience Act – DORA (2022)

[8] ISO/IEC 27036 Series: Supplier Security Management (2021–2023)

[9] European Banking Authority. Guidelines on Outsourcing Arrangements (2021)

(1) กำหนดผู้รับผิดชอบในการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(2) จัดให้มีทะเบียนบุคคลภายนอก เพื่อให้สามารถใช้ในการบริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของบุคคลภายนอกได้อย่างครบถ้วนต่อเนื่อง โดยมีรายละเอียดครอบคลุม

(ก) ชื่อบุคคลภายนอก

(ข) รายละเอียดของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(ค) ระดับความเสี่ยงและระดับความมีนัยสำคัญ

(ง) วันเริ่มต้นและสิ้นสุดสัญญาหรือข้อตกลง

(3) จัดให้มีมาตรการควบคุมและติดตามสิทธิการเข้าถึงข้อมูลสารสนเทศของบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้สิทธิดังกล่าวเป็นไปตามหลักความจำเป็นต้องรู้ (need-to-know basis)

(4) กำหนดให้บุคคลภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องให้ผู้ประกอบธุรกิจได้รับทราบอย่างทันการณ์

(5) ประเมินผลการปฏิบัติงานหรือผลการให้บริการของบุคคลภายนอก ทั้งในด้านประสิทธิภาพของบริการ การรักษาความมั่นคงปลอดภัยด้าน IT และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่ผู้ประกอบธุรกิจกำหนด

(6) ทบทวนคุณสมบัติบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบุคคลภายนอกยังคงมีคุณสมบัติที่เหมาะสม

ข้อเสนอแนะเพิ่มเติม

1. การรวมข้อมูลการติดตามในระดับกลุ่ม (Group-Wide Monitoring Consolidation)

หากผู้ให้บริการรายเดียวรองรับหลายบริษัทในกลุ่ม ต้องรวบรวมข้อมูลการติดตามไว้ที่ศูนย์กลางเพื่อวิเคราะห์ความเสี่ยงรวมและสร้างมุมมองภาพรวมของกลุ่ม และใช้หลักการตรวจสอบแบบ Four Eyes ในจุดสำคัญ เช่น การอนุมัติรายงานหรือการตัดสินใจแก้ไขเหตุการณ์ เพื่อให้มีการตรวจสอบจากสองฝ่ายและลดความเสี่ยงจากการตัดสินใจฝ่ายเดียว

2. การติดตามความเสี่ยงจากการกระจุกตัว (Concentration Risk Monitoring)

ต้องมีการติดตามความเสี่ยงจากการพึ่งพาผู้ให้บริการรายใหญ่หรือน้อยรายอย่างเป็นระยะ เพื่อป้องกันความเสี่ยงเชิงระบบที่อาจเกิดขึ้น

3. การสร้างความเชื่อมั่นจากการติดตามอย่างต่อเนื่อง (Continuous Assurance)

การตรวจสอบต้องไม่จำกัดเฉพาะการตรวจสอบรายปี แต่ต้องมีการติดตามและตรวจสอบอย่างต่อเนื่อง (Continuous Monitoring) เพื่อให้สามารถตอบสนองต่อความเสี่ยงที่เปลี่ยนแปลงได้ทันเวลา

(5) ระยะที่ 5: การยุติ/สิ้นสุดสัญญาหรือข้อตกลง (Termination & Exit Strategy)

การยุติความสัมพันธ์กับผู้ให้บริการต้องดำเนินการอย่างเป็นระบบเพื่อป้องกันความเสี่ยงและรักษาความต่อเนื่องของธุรกิจ กิจกรรมหลักประกอบด้วยการจัดทำเอกสารและแผนการยุติการให้บริการ การโอนย้ายข้อมูล ระบบ หรือบริการกลับเข้าสู่องค์กรหรือไปยังผู้ให้บริการรายใหม่ การยืนยันการทำลายข้อมูลอย่างถูกต้อง และปิดบัญชีการเข้าถึงทั้งหมดเพื่อป้องกันการละเมิดหลังการยุติ

1. จัดให้มีมาตรฐานหรือระเบียบปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง เพื่อเป็นกรอบแนวทางการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง โดยคำนึงถึงความต่อเนื่องในการให้บริการและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้งนี้ มาตรฐานหรือระเบียบปฏิบัติดังกล่าวควรครอบคลุมบทบาทหน้าที่คณะกรรมการและหน่วยงานที่เกี่ยวข้องกระบวนการและการควบคุมภายใน เช่น การสำรองข้อมูลก่อนการยกเลิก การลบหรือส่งคืนทรัพย์สินสำคัญจากผู้ให้บริการไปยังผู้ประกอบธุรกิจ (ตัวอย่างเช่น ข้อมูล กุญแจการเข้ารหัสข้อมูล และบัญชีผู้ใช้งาน) เป็นต้น

2. การพิจารณายกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง ผู้ให้บริการและผู้ประกอบธุรกิจควรประเมินผลกระทบและความเสี่ยงที่อาจเกิดขึ้นจากการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง และดำเนินการตามมาตรฐานหรือระเบียบปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง และกำหนดกลยุทธ์และแผนงานการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง (exit strategy and exit plan) ที่ชัดเจน เช่น ต้องกำหนด Exit Triggers (เหตุการณ์ที่ต้องยุติทันที) Fallback Service หรือผู้ให้บริการสำรอง Dual Vendor Model สำหรับบริการสำคัญ และดำเนินการทดสอบแผน Exit เป็นระยะ เพื่อให้มั่นใจว่าการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลงเป็นไปอย่างมีประสิทธิภาพและได้เตรียมความพร้อมต่อผลกระทบที่อาจเกิดขึ้น เช่น การหยุดให้บริการของระบบที่ส่งผลกระทบกับสมาชิกผู้ใช้บริการของระบบหรือลูกค้า การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

ข้อเสนอแนะเพิ่มเติม

การประเมินความเสี่ยงหลังการยุติ (Post-Exit Risk Assessment)

ต้องประเมินผลกระทบและความเสี่ยงที่ยังคงเหลืออยู่หลังการยุติสัญญา เพื่อให้มั่นใจว่าการออกจากความสัมพันธ์ไม่สร้างช่องโหว่ด้านความปลอดภัยหรือความต่อเนื่องของธุรกิจ

2.2.2 การรักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และการเตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT

1. ผู้ประกอบธุรกิจควรมีแนวทางการดูแลให้มั่นใจว่าการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีการรักษาความมั่นคงปลอดภัยด้าน IT ตามกรอบหลักการที่สำคัญ 3 ประการ คือ การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบและข้อมูล และสอดคล้องกับนโยบายและการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ หรือมาตรฐานสากลที่เกี่ยวข้อง เช่น ISO/IEC 27001 เป็นต้น โดยพิจารณาให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก

2. ผู้ประกอบธุรกิจควรจัดให้มีแผนรองรับในกรณีที่บุคคลภายนอกเกิดเหตุการณ์ผิดปกติด้าน IT (incident response plan) ซึ่งมีผลกระทบกับการดำเนินการของผู้ประกอบธุรกิจ โดยครอบคลุมเหตุการณ์ที่เกี่ยวข้องกับเหตุการณ์ความปลอดภัยทางไซเบอร์ และเหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล

ทั้งนี้ กระบวนการบันทึกและรายงานเหตุการณ์ผิดปกติ (Incident Management) ต้องสอดคล้องกับมาตรฐาน และต้องมีการแจ้งเหตุการณ์สำคัญต่อผู้บริหารและหน่วยงานกำกับดูแลตาม SLA ที่กำหนด โดยใช้หลักการ **Four Eyes** ในการอนุมัติหรือการตรวจสอบเหตุการณ์ที่มีความเสี่ยงสูง เพื่อให้มีการตรวจสอบจากสองฝ่าย เช่น ฝ่ายความมั่นคงปลอดภัยไซเบอร์และฝ่ายบริหารความเสี่ยงร่วมกันดำเนินการแก้ไข การดำเนินการทั้งหมดนี้ต้องบูรณาการกับนโยบายความมั่นคงสารสนเทศขององค์กรและข้อกำหนดทางกฎหมาย เพื่อสร้างความเชื่อมั่นและลดความเสี่ยงจากการละเมิดข้อมูลในทุกขั้นตอนของการใช้บริการบุคคลภายนอก

นอกจากนี้ การจัดทำบทเรียนจากเหตุการณ์จริง (Lessons Learned) เป็นอีกหนึ่งองค์ประกอบสำคัญที่ช่วยให้องค์กรสามารถเรียนรู้จากความผิดพลาดหรือความสำเร็จที่ผ่านมา รวมถึงความผิดพลาดที่เกิดในอุตสาหกรรมข้างเคียง ถึงแม้ไม่ได้เกิดกับองค์กรของตนเอง เพื่อนำมาปรับปรุงกระบวนการและลดโอกาสเกิดเหตุซ้ำ การพัฒนาเครื่องมือและระบบอัตโนมัติในการบริหาร Third Party เช่น ระบบติดตามความเสี่ยงแบบเรียลไทม์ หรือแพลตฟอร์มที่ช่วยประเมินและจัดระดับความเสี่ยง จะช่วยเพิ่มประสิทธิภาพและความแม่นยำในการบริหารจัดการ

องค์กรต้องสร้างวัฒนธรรม “Resilience by Design” ซึ่งหมายถึงการออกแบบกระบวนการและระบบงานให้มีความยืดหยุ่นตั้งแต่ต้น เพื่อให้สามารถรับมือกับความเปลี่ยนแปลงและเหตุการณ์ไม่คาดคิดได้อย่างมีประสิทธิภาพ ต้องอาศัยการสนับสนุนจากผู้บริหาร การสื่อสารที่ชัดเจน และการมีส่วนร่วมของบุคลากรทุกระดับ เพื่อให้การปรับปรุงและพัฒนาอย่างต่อเนื่องกลายเป็นส่วนหนึ่งของ DNA ขององค์กร

เอกสารอ้างอิง

European Parliament and Council. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (Digital Operational Resilience Act – DORA). Official Journal of the European Union.

European Banking Authority (EBA). (2019). Guidelines on Outsourcing Arrangements (EBA/GL/2019/02). EBA.

Monetary Authority of Singapore (MAS). (2021). Technology Risk Management (TRM) Guidelines. MAS.

FFIEC. (2023). Interagency Guidance on Third-Party Relationships: Risk Management. Office of the Comptroller of the Currency (OCC) et al.

National Institute of Standards and Technology (NIST). (2022). Special Publication 800 161 Revision 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST.

National Institute of Standards and Technology (NIST). (2008). SP 800-115: Technical Guide to Information Security Testing and Assessment.

International Organization for Standardization (ISO). (2023). ISO/IEC 27036-3: Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security.

International Organization for Standardization (ISO). (2015). ISO/IEC/IEEE 15288: Systems and software engineering — System life cycle processes.

International Organization for Standardization (ISO). (2016). ISO/IEC 27035: Information security incident management.

International Organization for Standardization (ISO). (2019). ISO 22301: Security and resilience — Business continuity management systems — Requirements.

International Organization for Standardization / IEC. (2021). ISO/IEC 27036 Series: Cybersecurity — Supplier relationships. ISO/IEC.

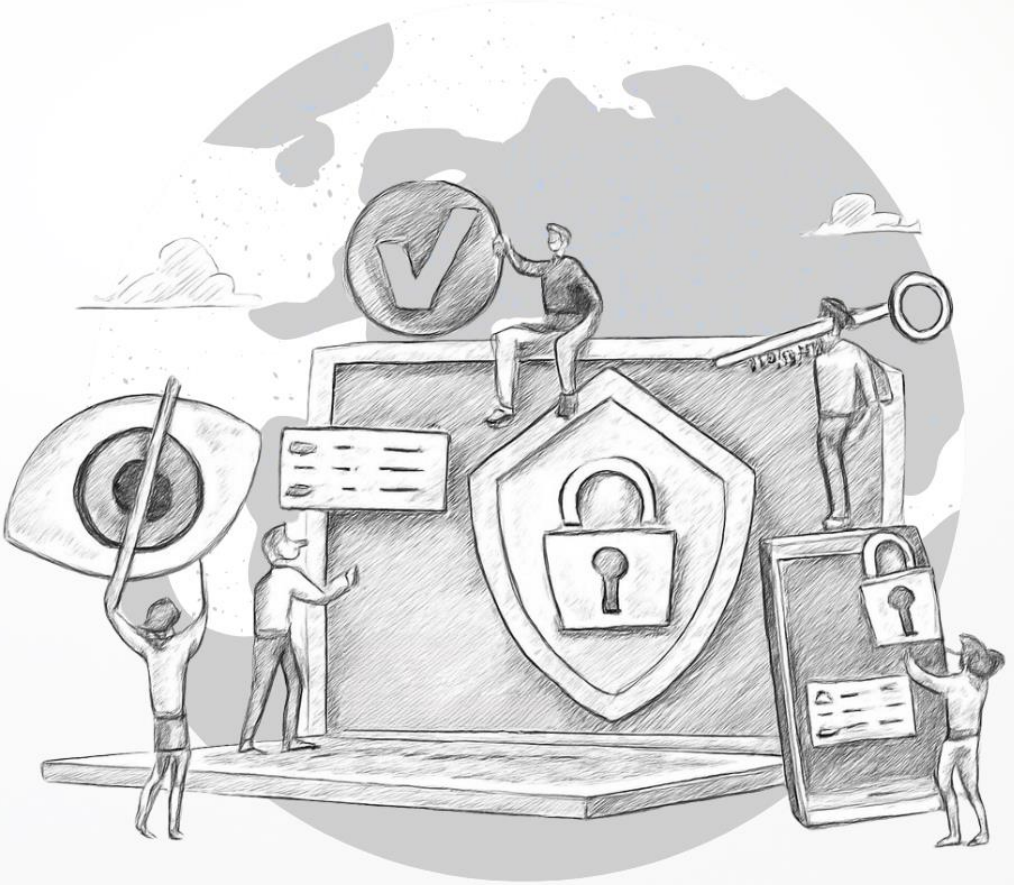
Bank of Thailand. (2023). Third Party Risk Management Implementation Guideline. BOT.

Electronic Transactions Development Agency (ETDA). (2023). แนวปฏิบัติว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก. ETDA.

ภาคผนวก

เครื่องมือประเมินความเสี่ยงบุคคลภายนอก (TPRM Assessment Toolkit)

ผู้ประกอบธุรกิจสามารถศึกษาและทดลองใช้ตัวอย่างเครื่องมือประเมินความเสี่ยงบุคคลภายนอกได้ตามไฟล์ Excel ที่แนบ ภาคผนวก-เครื่องมือประเมินความเสี่ยงบุคคลภายนอก



สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร
กรุงเทพมหานคร 10900
www.sec.or.th

SEC Cyberteam
Cyberteam@sec.or.th