กรอบการประเมินระดับความพร้อม
ด้านการรับมือภัยคุกคามทางไซเบอร์
(Cyber Resilience Assessment Framework: CRAF)
สำหรับบริษัทประกันภัย

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย
ปี ๒๕๖๕

สารบัญ

กรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework: CRAF) ที่เหมาะสมกับธุรกิจประกันภัย

ปัจจุบันบริษัทประกันภัยนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจ เพื่อช่วยพัฒนาการดำเนินงาน พัฒนาผลิตภัณฑ์ และบริการเพื่อตอบสนองความต้องการของลูกค้า รวมทั้งสร้างความได้เปรียบในการแข่งขันและลดต้นทุนในการดำเนินงาน นอกจากนี้ เทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่องและรวดเร็ว ส่งผลให้บริษัทต้องปรับตัวให้เข้ากับการเปลี่ยนแปลงสภาพแวดล้อมในการดำเนินธุรกิจ และสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศที่มีความซับซ้อนมากขึ้น ทำให้บริษัทประกันภัยต้องเผชิญกับความเสี่ยงจากการบริหารจัดการเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีรูปแบบที่เปลี่ยนแปลงอย่างต่อเนื่อง ซับซ้อน ตรวจจับได้ยาก และสามารถส่งผลกระทบเป็นวงกว้างต่อทั้งบริษัทและอุตสาหกรรมโดยรวม ด้วยเหตุนี้ บริษัทประกันภัยจึงควรมีความตระหนักถึงความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ รวมทั้งมีความสามารถในการรับมือต่อการเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศและการบุกรุกโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ เพื่อให้ทั้งบริษัทและอุตสาหกรรมมีความพร้อมในการรับมือกับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์อย่างเหมาะสม

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) จึงได้กำหนดกรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework: CRAF) ที่เหมาะสมกับธุรกิจประกันภัยขึ้น โดยอ้างอิงจาก (๑) ประกาศ คปภ. เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๓ (ประกาศ IT risk management) (๒) แนวปฏิบัติ เรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๔ (๓) แนวปฏิบัติเรื่อง หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๔ และ (๔) กรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานกำกับดูแลอื่น ๆ ในอุตสาหกรรม ได้แก่ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) Hong Kong Monetary Authority (HKMA) และ Federal Financial Institutions Examination Council (FFIEC) ประเทศสหรัฐอเมริกา

กรอบ CRAF ที่เหมาะสมกับธุรกิจประกันภัยนี้ มุ่งเน้นให้มีการประเมินระดับความเสี่ยงตั้งต้นหรือระดับความเสี่ยงสืบเนื่อง (Inherent Risk: IR) และ การประเมินระดับการควบคุม (Control Maturity: CM) เพื่อให้บริษัทมีระดับการควบคุมที่เหมาะสมกับระดับความเสี่ยงสืบเนื่องของบริษัท โดยมีสาระสำคัญสรุปได้ดังนี้

<u>ส่วนที่ ๑ การประเมินระดับความเสี่ยงตั้งต้นหรือระดับความเสี่ยงสืบเนื่อง (Inherent Risk: IR)</u>

เพื่อให้บริษัททราบถึงประเภทและระดับความเสี่ยงสืบเนื่องของตนเอง กรอบ CRAF ประเมินระดับความเสี่ยงสืบเนื่องจากปัจจัยความเสี่ยงพื้นฐานทางเทคโนโลยีสารสนเทศใน ๕ มุมมอง ได้แก่

- **IR1 เทคโนโลยีและการเชื่อมต่อ (Technologies and Connection)** เป็นปัจจัยเสี่ยงที่พิจารณาจากรูปแบบการเชื่อมต่อ และการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท รวมถึงลักษณะการใช้งานระบบงาน อุปกรณ์ และโครงสร้างพื้นฐานทางด้านสารสนเทศของบริษัท โดยในมุมมองนี้ประกอบด้วยมุมมองย่อย ๖ ข้อ ได้แก่ (๑) การเชื่อมต่อ (Connection) (๒) การเข้าถึงโดยผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT outsource access) (๓) การเข้าถึงระบบเครือข่ายภายในพื้นที่ของบริษัท (Onsite access) (๔) การเข้าถึงด้วยอุปกรณ์เคลื่อนที่ส่วนบุคคล (Bring your own device: BYOD) (๕) ระบบงาน (Application) และ (๖) เทคโนโลยีสารสนเทศโครงสร้างพื้นฐาน (Infrastructure)
- **IR2 ช่องทางการให้บริการ (Delivery Channels)** เป็นปัจจัยเสี่ยงที่พิจารณาจากช่องทางที่บริษัทให้บริการแก่ลูกค้าหรือผู้เอาประกันภัย โดยมีการเชื่อมต่อกับระบบเครือข่ายภายนอก โดยเฉพาะเครือข่ายอินเทอร์เน็ต เช่น Website, Mobile Application หรือ social media เป็นต้น
- **IR3 ลักษณะผลิตภัณฑ์และการให้บริการ (Products & Technology Services)** เป็นปัจจัยเสี่ยงที่พิจารณาจากอัตราส่วนของผลิตภัณฑ์ และบริการที่บริษัทให้บริการผ่านระบบ Online รวมถึงการนำเอาเทคโนโลยีใหม่มาใช้เป็นครั้งแรก
- **IR4 ขนาด และลักษณะเฉพาะขององค์กร (Business Size & Organization Characteristics)** เป็นปัจจัยเสี่ยงที่พิจารณาจากขนาดของบริษัททั้งในด้านของสถานที่ตั้ง บุคลากร และรายการทางธุรกิจ รวมทั้งการจัดโครงสร้างองค์กรทางด้านสารสนเทศของบริษัท ซึ่งในมุมมองนี้ประกอบด้วยมุมมองย่อย ได้แก่ ขนาดของธุรกิจ (Business Size) โครงสร้างบุคลากร (HR Structure) และ ผู้ใช้งานที่มีสิทธิสูง (High-privileged users)
- **IR5 ประวัติการถูกคุกคามทางไซเบอร์ (Cyber Threats Records)** เป็นปัจจัยเสี่ยงที่พิจารณาจากจำนวนการถูกโจมตีทางไซเบอร์ประเภทต่างๆ ของบริษัทที่เคยเกิดขึ้นในรอบระยะเวลา ๑๒ เดือน

ทั้งนี้ ระดับความเสี่ยงสืบเนื่องของบริษัทประกันภัย จะแบ่งออกเป็น ๓ ระดับตามลักษณะของปัจจัยเสี่ยงทั้ง ๕ มุมมองข้างต้น ดังนี้

ระดับ	ลักษณะของบริษัทประกันภัย
สูง	บริษัทประกันภัยมีกลยุทธ์การดำเนินธุรกิจทาง Electronic Business ในเชิงรุก และนำเทคโนโลยีที่มีความซับซ้อน และหลากหลายมาใช้ในการบริหารจัดการโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ การพัฒนาผลิตภัณฑ์ และการให้บริการมากขึ้น มีการดำเนินธุรกิจที่ครอบคลุมประเภทผลิตภัณฑ์ที่หลากหลาย และมีการให้บริการในปริมาณมาก มีการใช้และให้บริการระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอกจำนวนมาก และมีแนวโน้มที่จะตกเป็นเป้าหมายของการถูกคุกคามทางไซเบอร์เพิ่มและรุนแรงขึ้นอย่างต่อเนื่อง
ปานกลาง	บริษัทประกันภัยมีกลยุทธ์การทำธุรกิจที่เน้น Electronic Business ควบคู่ไปกับ Traditional Business โดยมีผลิตภัณฑ์และการให้บริการที่หลากหลาย มีเครือข่ายที่เชื่อมโยงกับบุคคลภายนอกทั้งลูกค้า ตัวแทน นายหน้า หรือผู้ให้บริการด้านเทคโนโลยีสารสนเทศผ่านเครือข่ายทั้งที่เป็นระบบปิด และระบบอินเทอร์เน็ต โดยเริ่มมีการนำเทคโนโลยีที่มีความซับซ้อน เช่น Cloud Computing มาใช้ มีการใช้ระบบเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอกจำนวนมาก และที่ผ่านมาเคยมีเหตุการณ์ผิดปกติทางไซเบอร์เกิดขึ้นอยู่เป็นระยะ
ต่ำ	บริษัทประกันภัยมีกลยุทธ์การทำธุรกิจบนพื้นฐานของ Traditional Business โดยมีผลิตภัณฑ์และการให้บริการธุรกรรมที่ไม่หลากหลาย และส่วนใหญ่ทำผ่านช่องทางเครือข่ายที่เป็นระบบปิด มีผลิตภัณฑ์และการให้บริการผ่านช่องทางอิเล็กทรอนิกส์ หรือผ่านช่องทางอินเทอร์เน็ตในวงจำกัด และไม่เคยตกเป็นเป้าโจมตีทางไซเบอร์อย่างรุนแรงในอดีต

ส่วนที่ ๒ การประเมินระดับการควบคุม (Control Maturity: CM)

เพื่อให้บริษัทประกันภัยทราบถึงระดับการควบคุมทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ของตนเอง โดยการประเมินระดับการควบคุมตามกรอบ CRAF ประกอบด้วย การประเมินหัวข้อการควบคุมด้านเทคโนโลยีสารสนเทศและไซเบอร์ของบริษัทใน ๖ หมวดหมู่ ได้แก่

- **CM1 การกำกับดูแล (Governance)** หมวดหมู่นี้เกี่ยวกับการกำกับดูแลด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่ดี โครงสร้างและบทบาทหน้าที่ด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่สอดคล้องตามหลัก Three lines of Défense การกำหนดนโยบายและแผนกลยุทธ์ รวมทั้งมีการติดตามการดำเนินงานด้านการกำกับดูแลและรายงานผลที่เหมาะสม เพื่อให้บริษัทประกันภัยมีแนวทางในการกำกับดูแลและบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ในภาพรวมที่มีมาตรฐาน ชัดเจน และตรวจสอบได้
- **CM2 การระบุความเสี่ยง (Identification)** หมวดหมู่นี้เกี่ยวกับการบริหารจัดการทรัพย์สินสารสนเทศ และ การกำหนดขอบเขตในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่รวมถึงข้อมูลส่วนบุคคล ซึ่งการกำหนดขอบเขตของทรัพย์สินสารสนเทศและการบริหารจัดการความเสี่ยงที่ครบถ้วน จะส่งผลให้การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ครอบคลุมและเหมาะสมตามระดับความเสี่ยงหรือระดับความสำคัญของทรัพย์สินสารสนเทศที่บริษัทกำหนด

- **CM3 การป้องกันความเสี่ยง (Protection)** หมวดหมู่นี้เกี่ยวกับการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ รวมไปถึงข้อมูลส่วนบุคคลที่อาจเกิดขึ้น เช่น การควบคุมทางด้านการเข้าถึง การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและปฏิบัติงานทางด้านสารสนเทศ รวมถึงการป้องกันความเสี่ยงทางด้านไซเบอร์ เป็นต้น โดยการควบคุมเกี่ยวกับการป้องกันความเสี่ยงนี้จะส่งผลให้บริษัทประกันภัยมีกระบวนการ มาตรการ และเครื่องมือที่ใช้เพื่อควบคุม หรือลดความรุนแรงของเหตุการณ์ด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และไซเบอร์ให้อยู่ในระดับที่องค์กรสามารถยอมรับได้
- **CM4 การตรวจสอบและเฝ้าระวัง (Detection)** หมวดหมู่นี้เกี่ยวกับมาตรการที่จะทำให้สามารถระบุหรือตรวจพบช่องโหว่หรือภัยคุกคามด้านเทคโนโลยีสารสนเทศ ด้านไซเบอร์ และข้อมูลส่วนบุคคลที่เกิดขึ้น หรืออาจเกิดขึ้น เพื่อให้บริษัทประกันภัยสามารถตรวจพบเหตุการณ์ผิดปกติได้อย่างทันท่วงที ซึ่งจะส่งผลให้บริษัทสามารถกำหนดแนวทางในการดำเนินการเพื่อตอบสนองต่อเหตุการณ์ได้อย่างหมาะสมต่อไป
- **CM5 การรับมือและตอบสนองเมื่อพบเหตุการณ์ (Response & Recovery)** หมวดหมู่นี้เกี่ยวกับการกำหนดแผนการรับมือต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ภัยคุกคามทางไซเบอร์ และการรั่วไหลของข้อมูลส่วนบุคคล การจำกัดความเสียหาย การสื่อสาร และการสืบสวนหาสาเหตุ รวมถึงการกู้คืนระบบหรือข้อมูลสารสนเทศให้สามารถกลับสู่สภาวะปกติ การควบคุมเหล่านี้ส่งผลให้บริษัทประกันภัยสามารถรับมือ และตอบสนองต่อเหตุการณ์ผิดปกติได้อย่างเหมาะสม โดยสามารถจำกัดหรือลดทอนความเสียหาย และลดผลกระทบต่อการดำเนินธุรกิจ รวมทั้งสืบหาสาเหตุเพื่อนำไปพัฒนาให้เกิดการป้องกันที่มีประสิทธิภาพในอนาคต
- **CM6 การบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ (Third Party Risk Management)** หมวดหมู่นี้เกี่ยวกับการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจตลอดทั้งกระบวนการตั้งแต่การคัดเลือก การจัดทำสัญญาและเงื่อนไขการให้บริการ การติดตาม รวมทั้งการควบคุมทางด้านความมั่นคงปลอดภัยของงานสารสนเทศที่ดำเนินการโดยผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจ เพื่อให้บริษัทประกันภัยสามารถมั่นใจได้ว่า ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจสามารถปฏิบัติงาน ได้ตามที่บริษัทคาดหวัง และมีมาตรการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่ได้มาตรฐานตามที่บริษัทต้องการ

ทั้งนี้ ระดับการควบคุมของบริษัทประกันภัย จะแบ่งออกเป็น ๓ ระดับ ตามหัวข้อการควบคุมด้านเทคโนโลยีสารสนเทศ และไซเบอร์ทั้ง ๖ หมวดหมู่ข้างต้น ดังนี้

ระดับ	คำจำกัดความ
Advance	ระดับการควบคุมที่การดำเนินงานทางด้านความมั่นคงปลอดภัยไซเบอร์ผนวกอยู่กับกระบวนการทางธุรกิจ มีการบริหารจัดการความเสี่ยงที่รวดเร็ว รวมทั้งมีการพัฒนากระบวนการดำเนินงาน และการควบคุมอย่างต่อเนื่อง ตลอดจนมีนวัตกรรมหรือการใช้งานเทคโนโลยีเพื่อเพิ่มศักยภาพในการควบคุมทางด้านไซเบอร์ รวมถึงเป็นผู้นำของกลุ่มอุตสาหกรรมในการพัฒนา และแบ่งปันข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์
Intermediate	ระดับการควบคุมที่เป็นทางการและมีเอกสารเป็นลายลักษณ์อักษร มีการปฏิบัติการควบคุม แล การตรวจสอบการดำเนินการควบคุมอย่างต่อเนื่องสม่ำเสมอ โดยการควบคุมจะดำเนินงานเพื่อตอบสนองต่อความเสี่ยง (Risk-driven) และกลยุทธ์ของบริษัท
Baseline	ระดับการควบคุมที่เป็นไปตามข้อกำหนดขั้นพื้นฐานตามกฎหมาย ระเบียบข้อบังคับ และกฎระเบียบของหน่วยงานกำกับดูแล โดยการปฏิบัติการควบคุมเป็นการดำเนินงานที่ค่อนข้างเป็นทางการ และมีเอกสารเป็นลายลักษณ์อักษร แต่ยังเป็นการปฏิบัติเพื่อสนองต่อวัตถุประสงค์ทางด้านการปฏิบัติตามกฎหมายเป็นหลัก

สำหรับระดับการควบคุมที่เหมาะสมของแต่ละบริษัท ควรอ้างอิงตามระดับความเสี่ยงสืบเนื่องของตนเอง เช่น บริษัทที่มีระดับความเสี่ยงสืบเนื่องอยู่ในระดับสูง ควรมีระดับการควบคุมที่เข้มงวดหรืออยู่ในระดับ Advance เป็นต้น

ส่วนที่ 1 การประเมินระดับความเสี่ยงตั้งต้น หรือระดับความเสี่ยงสืบเนื่อง (Inherent Risk)

ความเสี่ยงสืบเนื่องเป็นความเสี่ยงที่บริษัทประกันภัยมีอยู่จากการดำเนินงาน หรือการใช้งานเทคโนโลยีสารสนเทศของบริษัท โดยยังไม่ได้พิจารณาถึงการควบคุมที่บริษัทประกันภัยจัดให้มีขึ้น กรอบ CRAF จะประเมินระดับความเสี่ยงสืบเนื่องจาก ๕ มุมมอง ได้แก่ เทคโนโลยีและการเชื่อมต่อ ช่องทางการให้บริการ ลักษณะผลิตภัณฑ์และการให้บริการ ขนาดและลักษณะเฉพาะขององค์กร และประวัติการถูกคุกคามทางไซเบอร์ โดยผลการประเมินจะแบ่งเป็น ๓ ระดับ คือ ต่ำ ปานกลาง และสูง โดยรายละเอียดการประเมินมีดังนี้

IR1 เทคโนโลยีและการเชื่อมต่อ (Technologies and Connection)

เทคโนโลยีสารสนเทศและการเชื่อมต่อ อาจส่งผลต่อระดับความเสี่ยงสืบเนื่องของบริษัท โดยปริมาณการเข้าถึง ลักษณะการใช้งาน และลักษณะของเทคโนโลยี ส่งผลต่อความซับซ้อน ขนาด และความต้องการในการบริหารจัดการของบริษัทประกันภัย ซึ่งเป็นความเสี่ยงสืบเนื่องทางด้านไซเบอร์ รวมถึงเป็นความเสี่ยงสืบเนื่องของข้อมูลสำคัญที่จัดเก็บ ส่งผ่าน และ ใช้งานภายในระบบเทคโนโลยีสารสนเทศและการเชื่อมต่อดังกล่าว ปัจจัยเสี่ยงในมุมมองนี้ แบ่งออกเป็น ๖ มุมมองย่อย ได้แก่

- IR 1.1 การเชื่อมต่อ (Connection)
- IR 1.2 การเข้าถึงโดยผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsource Access)
- IR 1.3 การเข้าถึงระบบเครือข่ายภายในพื้นที่ของบริษัท (Onsite Access)
- IR 1.4 การเข้าถึงด้วยอุปกรณ์เคลื่อนที่ส่วนบุคคล (Bring Your Own Device: BYOD)
- IR 1.5 ระบบงาน (Application)
- IR 1.6 เทคโนโลยีสารสนเทศโครงสร้างพื้นฐาน (Infrastructure)

IR 1.1 การเชื่อมต่อ (Connection) - การเชื่อมต่อระหว่างระบบงาน หรือ ระบบเทคโนโลยีสารสนเทศของบริษัท เป็นปัจจัยบ่งชี้ถึงช่องทางที่ระบบสารสนเทศและข้อมูลสำคัญของบริษัทมีการเชื่อมต่อกับบุคคล หรือ หน่วยงานภายนอก ซึ่งจำนวนการเชื่อมต่อที่มากขึ้นย่อมจะบ่งชี้ถึงความเสี่ยงที่ระบบสารสนเทศและข้อมูลสำคัญของบริษัทอาจถูกเข้าถึงใช้งาน หรือ โจมตีจากหน่วยงานภายนอกที่มากขึ้น รวมทั้งลักษณะของเทคโนโลยีที่ใช้เพื่อการเชื่อมต่อ ซึ่งมีความปลอดภัยแตกต่างกัน ก็จะบ่งชี้ถึงภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นจากการเชื่อมต่ออีกด้วย โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๑.๑.๑	จำนวน Internet Service Provider (ISP) ที่เชื่อมต่อกับระบบเครือข่ายของบริษัท	จำนวน ISP	น้อยกว่า ๒	๒-๓	มากกว่า ๓		นับจากจำนวนผู้ให้บริการ ISP ในปัจจุบันทั้งที่ ศูนย์หลัก (DC) ศูนย์สำรอง (DR) และสาขา ทั้งนี้ ไม่รวมถึงจำนวน Private connection technology เช่น Leased Lines, MPLS และ Dark Fiber เป็นต้น
๑.๑.๒	จำนวน Public IP Address ของบริษัทที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต (ซึ่งรวมถึง Public IP ที่เชื่อมต่อระหว่างสาขาและระบบเครือข่ายหลักของบริษัท)	จำนวน IP Addresses	น้อยกว่า ๑๐	๑๐-๔๐	มากกว่า ๔๐		นับจากจำนวน IP Address ที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต และสามารถเข้าถึงผ่านทางอินเทอร์เน็ตได้ โดยไม่รวมถึง Private IP Address ที่ใช้อยู่ภายในองค์กร
๑.๑.๓	จำนวนองค์กรภายนอก (Third party) และ บริษัทในเครือที่มีการเชื่อมต่อกับเครือข่ายของบริษัท	จำนวนองค์กร / บริษัท	น้อยกว่า ๕	๕-๑๕	มากกว่า ๑๕		นับจากจำนวนองค์กร หรือบริษัทของบุคคลหรือนิติบุคคลภายนอก รวมถึงบริษัทในเครือ ที่มีการเชื่อมต่อกับระบบสารสนเทศที่สำคัญของบริษัท ผ่านช่องทางการเชื่อมต่อต่าง ๆ เช่น API หรือ VPN เป็นต้น ซึ่งเป็นการเชื่อมต่อแบบ System to system โดยไม่รวมถึง การเข้าถึงระบบงานผ่าน Application ในลักษณะของ End-User ผู้ใช้งานระบบงาน
๑.๑.๔	ลักษณะการเชื่อมต่อเครือข่ายกับองค์กรภายนอก	ลักษณะการเชื่อมต่อ	Private Link เช่น Leased Line, MPLS และ มีการเข้ารหัส เช่น	Private Link เช่น Leased Line, MPLS ที่ไม่มีการเข้ารหัส	การเชื่อมต่อผ่าน Public Internet ทั้งที่มีการเข้ารหัส		- ในกรณีที่บริษัทมีการเชื่อมต่อหลายช่องทาง ในหลายลักษณะ ให้เลือกจากลักษณะที่มีความเสี่ยงสูงที่สุด - ในกรณีของการเชื่อมต่อแบบ SD-WAN (Software-Defined WAN) จัดเป็นการเชื่อมต่อแบบ "การเชื่อมต่อผ่าน Public Internet ทั้งที่มีการเข้ารหัสและไม่เข้ารหัส"

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
			VPN หรือ ไม่มีการเชื่อมต่อเลย		และไม่เข้ารหัส		

IR 1.2 การเข้าถึงโดยผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsource Access) - ปริมาณ และลักษณะการเข้าถึงระบบงานและข้อมูลสำคัญในระบบงาน โดยผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsource) เป็นปัจจัยบ่งชี้ถึงความเสี่ยงจากการดำเนินงานที่ไม่เหมาะสม ขาดความระมัดระวังโดย ผู้ให้บริการภายนอกฯ และบ่งชี้ถึงโอกาสที่ระบบสารสนเทศ และข้อมูลของบริษัทอาจถูกเข้าถึง ใช้งาน หรือ โจมตีจากบุคคลภายนอก เนื่องจากผู้ให้บริการภายนอกฯ เหล่านี้ อาจไม่ได้รับการอบรมหรือไม่ได้ปฏิบัติงานภายใต้นโยบาย และมาตรฐานการควบคุมทางด้านความมั่นคงปลอดภัยสารสนเทศ เทียบเท่ากับพนักงานของบริษัท โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๑.๒.๑	จำนวนผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsource) ที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศภายในของบริษัท	จำนวนบริษัท	น้อยกว่า ๒	๒-๑๐	มากกว่า ๑๐		การเข้าถึงระบบสารสนเทศภายในของบริษัทให้พิจารณาจากระบบสารสนเทศทั้งหมด ทั้งในส่วนของระบบเครือข่าย (Network) ระบบปฏิบัติการ ระบบฐานข้อมูล และ ระบบงาน (Application และ Software) ต่าง ๆ
๑.๒.๒	ลักษณะการเข้าถึงระบบงานภายในบริษัทจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsource)	ลักษณะการเชื่อมต่อ	On-site หรือ ไม่มีผู้ให้บริการภายนอกฯ เลย	มีการเชื่อมต่อผ่าน private link หรือ การเชื่อมต่อที่มีการเข้ารหัส เช่น VPN	Internet access or Unknown หรือ อื่น ๆ (โปรดระบุในช่อง" คำอธิบายเพิ่มเติม")		- ในกรณีที่บริษัทมีลักษณะการเข้าถึงระบบงานภายในบริษัทหลายช่องทางในหลายลักษณะ ให้เลือกจากลักษณะที่มีความเสี่ยงสูงที่สุด - ในกรณีของการเชื่อมต่อแบบ VDI (Virtual Desktop Interface) จัดเป็นการเชื่อมต่อแบบ “มีการเชื่อมต่อผ่าน private link หรือ การเชื่อมต่อที่มีการเข้ารหัส เช่น VPN” - ในกรณีของการเชื่อมต่อแบบ remote desktop / AnyDesk จัดเป็นการเชื่อมต่อแบบ “Internet access”

IR 1.3 การเข้าถึงระบบเครือข่ายภายในพื้นที่ของบริษัท (Onsite Access) – ลักษณะการเข้าถึงระบบเครือข่ายทั้งแบบมีสาย และไร้สายจากภายในพื้นที่ของบริษัท บ่งชี้ถึงความเสี่ยงในการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต รวมถึงอาจเป็นที่มาของการบุกรุกโจมตีระบบเครือข่ายของบริษัท โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๑.๓.๑	ลักษณะการเข้าถึงเครือข่ายของบริษัท ของเจ้าหน้าที่ของบริษัท และ บุคคลภายนอกที่มาปฏิบัติงานในพื้นที่ของบริษัท	ลักษณะการเข้าถึง	เฉพาะเครื่องของบริษัท และเครื่องที่ลงทะเบียนสามารถเข้าถึงได้จากเครือข่ายมีสายเท่านั้น	เครื่องของบริษัท และเครื่องที่ลงทะเบียนสามารถเข้าถึงได้จากเครือข่ายมีสายและไร้สาย (WiFi)	เครื่องที่ไม่ได้ลงทะเบียนสามารถเข้าถึงได้จากเครือข่ายมีสายและไร้สาย (WiFi)		ในกรณีที่มีการเข้าถึงในหลายลักษณะ ให้เลือกลักษณะการเข้าถึงที่มีความเสี่ยงสูงที่สุด
๑.๓.๒	ลักษณะระบบเครือข่ายไร้สาย (WiFi) ของบริษัท ที่ให้บริการแก่เจ้าหน้าที่ของบริษัท และบุคคลภายนอกที่ใช้งานระบบเครือข่ายในพื้นที่ของบริษัท	ลักษณะระบบเครือข่ายไร้สาย	แยกระบบเครือข่ายออกจากกันทาง Physical (เช่น แยก Access Point, ISP) หรือ ไม่มีการใช้งานระบบเครือข่ายไร้สาย	แยกระบบเครือข่ายออกจากกันทาง Logical (เช่น แยก VLAN)	ใช้ระบบเครือข่ายร่วมกันทั้งผู้ใช้ภายในบริษัท และบุคคลภายนอก		บุคคลภายนอก ในที่นี้ให้รวมถึง ผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsource) บุคคลหรือนิติบุคคลภายนอก (Third Party) หรือ ลูกค้า

IR 1.4 การเข้าถึงด้วยอุปกรณ์เคลื่อนที่ส่วนบุคคล (Bring Your Own Device: BYOD) - การใช้งานอุปกรณ์เคลื่อนที่ส่วนบุคคลของพนักงานเพื่อการเชื่อมต่อมายังระบบสารสนเทศของบริษัท เป็นปัจจัยบ่งชี้ถึงความเสี่ยงอันอาจเกิดจากการเข้าถึงอย่างไม่ปลอดภัยหรือไม่ได้รับอนุญาต รวมทั้งยังบ่งชี้ถึงค วามเสี่ยงเกี่ยวกับการรั่วไหลของข้อมูลสำคัญผ่านอุปกรณ์เคลื่อนที่ดังกล่าว เนื่องจากการใช้งานอุปกรณ์เคลื่อนที่ส่วนตัวนี้อาจมีข้อจำกัดในการตั้งค่าความปลอดภัยตามมาตรฐานของบริษัท และสามารถเปลี่ยนการใช้งานจากบุคคลหนึ่งไปยังอีกบุคคลหนึ่งได้โดยง่าย รวมทั้งอุปกรณ์อาจสูญหายได้ง่าย โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๑.๔.๑	อุปกรณ์เคลื่อนที่ส่วนบุคคลของพนักงาน (BYOD) ที่อนุญาตให้ใช้เพื่อเข้าถึงระบบเครือข่ายของบริษัท เช่น Mobile with push mail, laptop/PC, Removable storage และอื่น ๆ	จำนวนพนักงาน	น้อยกว่า ๑๐	๑๐-๒๐๐	มากกว่า ๒๐๐		นับจากจำนวนพนักงานที่มีคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ส่วนตัว ที่สามารถใช้เพื่อเข้าถึงระบบเครือข่ายของบริษัท โดยในกรณีที่บริษัทเปิดให้มีการเข้าถึงแต่ไม่ได้จัดเก็บรายชื่อผู้ใช้อุปกรณ์เพื่อเข้าถึง ให้ใช้จำนวนพนักงานทั้งหมด
๑.๔.๒	ระบบงานสำคัญของบริษัทที่อนุญาตให้มีการเข้าถึงผ่าน BYOD	จำนวนระบบงาน	๐	๑-๓	มากกว่า ๓		นับจากจำนวนระบบงาน (Application) สำคัญที่อนุญาตให้พนักงานใช้อุปกรณ์ส่วนตัว เช่น คอมพิวเตอร์ส่วนตัว มือถือส่วนตัว หรือ แท็บเล็ตส่วนตัว เข้าไปใช้งานได้ อ้างอิงคำจำกัดความของ "ระบบงานสำคัญ" ใน “อภิธานศัพท์”

IR 1.5 ระบบงาน (Application) - จำนวนระบบงานสำคัญ รวมถึงประเภทของระบบงาน บ่งชี้ถึงความต้องการในการใช้ทรัพยากรของบริษัทเพื่อบริหารจัดการ และ ติดตั้งการควบคุมเพื่อความมั่นคงปลอดภัยที่เพียงพอเหมาะสมของระบบงานเหล่านั้น โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๑.๕.๑	จำนวนระบบงานสำคัญทั้งหมด	จำนวนระบบงาน	น้อยกว่า ๔	๔-๑๐	มากกว่า ๑๐		อ้างอิงคำจำกัดความของ "ระบบงานสำคัญ" ใน “อภิธานศัพท์”

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๑.๕.๒	จำนวนระบบงานสำคัญที่จัดเก็บข้อมูลส่วนบุคคล	จำนวนระบบงาน	น้อยกว่า ๓	๓-๑๐	มากกว่า ๑๐		อ้างอิงคำจำกัดความของ "ระบบงานสำคัญ" ใน “อภิธานศัพท์” อ้างอิงคำจำกัดความของ "ข้อมูลส่วนบุคคล" ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

IR 1.6 เทคโนโลยีสารสนเทศโครงสร้างพื้นฐาน (Infrastructure) - ระบบโครงสร้างพื้นฐาน เช่น ระบบปฏิบัติการ ระบบอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ปลายทาง หรืออุปกรณ์สารสนเทศต่าง ๆ เป็นองค์ประกอบสำคัญในระบบสารสนเทศที่ใช้เพื่อการปฏิบัติงาน การส่งผ่านข้อมูล และการประมวลผล ดังนั้นการใช้งานเทคโนโลยีนี้จึงเป็นปัจจัยที่บ่งชี้ถึงความเสี่ยงสืบเนื่อง อันอาจเกิดจากข้อจำกัดของระบบที่ใช้งานเทคโนโลยีที่ไม่ปลอดภัย ระบบที่ล้าสมัย นอกจากนี้ จำนวนอุปกรณ์และระบบโครงสร้างพื้นฐาน ยังบ่งชี้ถึงความซับซ้อนและความต้องการทรัพยากรในการบริหารจัดการ โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๑.๖.๑	จำนวน Public IP Addresses ของบริษัท ที่ให้บริการแบบ Unsecured Protocol เช่น FTP, Telnet, HTTP ผ่านเครือข่ายอินเทอร์เน็ต	จำนวน Public IP Addresses	๐	๑-๑๐	มากกว่า ๑๐		อ้างอิง secure protocol จากมาตรฐาน NIST ๘๐๐-๕๓ และ NIST Special Publication ๘๐๐-๑๒๓
๑.๖.๒	จำนวนระบบปฏิบัติการ (Operating System : OS) และ Software ของระบบงานสำคัญที่ End-of-Life หรือ End-of-Support (รวมถึง open source)	จำนวน OS หรือ Software	๐	๑-๕	มากกว่า ๕		นับจากจำนวน OS เช่น Windows XP, Windows ๗, Windows Server ๒๐๐๓, AIX ๕.๐ เป็นต้น จำนวน Software เช่น Microsoft Office ๒๐๐๗ เป็นต้น และ จำนวน OS หรือ firmware ที่ติดตั้งในอุปกรณ์เครือข่าย เช่น Router, switch, Firewall เป็นต้น รวมถึง อุปกรณ์ที่ใช้ Open Source เช่น Ubuntu Linux, CentOS Linux เป็นต้น โดยนับเฉพาะ Major Version (เช่น Windows Server ๒๐๐๘, และ ๒๐๐๘

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
							R๒ ให้ถือเป็นตัวเดียวกัน) และ กรณีของ Open Source นับแยกตาม version เช่น นับ CentOS ๖.๑๐ และ CentOS ๗.๓ แยกกัน เป็นต้น - ในกรณีที่มีหลายอุปกรณ์ที่ติดตั้ง OS ที่ End-of-Life ให้นับตามจำนวน OS ประเภทของ OS ที่ใช้งานอยู่ ไม่ใช่จำนวนอุปกรณ์ - ในกรณีที่เป็น Software ของระบบงานที่พัฒนาขึ้นเอง พัฒนาโดยผู้ให้บริการ ให้พิจารณาถึงความสามารถในการสนับสนุนการเปลี่ยนแปลงระบบงานเป็นสำคัญ ทั้งนี้ ถ้า Software หรือ ระบบงาน นั้นไม่มีพนักงาน หรือ บริษัทภายนอกที่สามารถสนับสนุนการเปลี่ยนแปลงได้แล้ว ให้พิจารณาเป็น Software ที่ End-of-Life หรือ End-of-Support
๑.๖.๓	จำนวนเครื่อง Server, Endpoint, Devices ที่ใช้ระบบปฏิบัติการ (Operating System : OS) และ Software ของระบบงานสำคัญที่ End-of-Life (รวมถึง open source)	จำนวนเครื่อง Server, Endpoint, Device	๐	๑-๒๐	มากกว่า ๒๐		นับจากจำนวนเครื่องหรืออุปกรณ์ อาทิ Devices, Servers หรือ Endpoints ที่ใช้งานกับ OS หรือ Software ที่ End-of-Life หรือ End-of-Support ในข้อ ๑.๖.๒ ข้างต้น
๑.๖.๔	จำนวนอุปกรณ์เครือข่าย (network devices) ได้แก่ Router, Switch, Access Point, Firewall, IPS/IDS หรืออุปกรณ์ที่เทียบเท่า	จำนวนอุปกรณ์เครือข่าย	น้อยกว่า ๒๐	๒๐-๑๕๐	มากกว่า ๑๕๐		- นับจากจำนวนอุปกรณ์ที่บริษัทใช้งานอยู่ในปัจจุบัน (รวมอุปกรณ์เช่าซื้อ) โดยพิจารณาจากอุปกรณ์ที่บริษัทสามารถดูแลและบริหารจัดการได้เอง รวมถึงอุปกรณ์ที่ใช้งานอยู่ที่สาขา - นับจำนวนอุปกรณ์ทั้งแบบ Hardware Appliance และ Virtual Appliance

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
							- ไม่นับรวมถึงอุปกรณ์ประเภท Unmanageable Device ที่ไม่มี OS หรือไม่มี Configuration Menu เช่น Hub, Modem บางประเภท เป็นต้น - ไม่นับรวมถึงอุปกรณ์หรือบริการด้านความปลอดภัยระบบเครือข่าย ที่ใช้บริการผ่านผู้ให้บริการภายนอก อาทิ DDoS Subscription หรือ บริการคลาวด์ภายนอก (AWS Cloudflare) เป็นต้น
๑.๖.๕	รูปแบบการใช้งานระบบคลาวด์ที่สนับสนุนระบบงานสำคัญ	รูปแบบการใช้งานระบบคลาวด์	ไม่มีการใช้งานระบบคลาวด์	คลาวด์แบบ Private cloud หรือ Hybird cloud	คลาวด์แบบ Public cloud		ในกรณีบริษัทมีการใช้งานระบบคลาวด์ในหลากหลายรูปแบบให้เลือกรูปแบบการใช้งานระบบงานคลาวด์ที่มีความเสี่ยงสูงที่สุด

IR2 ช่องทางการให้บริการ (Delivery Channels)

ช่องทางการให้บริการ เป็นมุมมองปัจจัยเสี่ยงที่พิจารณาถึงประเภทและลักษณะของช่องทางการให้บริการผลิตภัณฑ์และการทำธุรกรรมของบริษัทประกันภัย ที่มีการเชื่อมต่อกับระบบเครือข่ายภายนอก โดยเฉพาะเครือข่ายอินเทอร์เน็ต เช่น Website, Mobile Application หรือ Social Media เป็นต้น ซึ่งช่องทางการให้บริการที่เชื่อมต่อกับลูกค้าผ่านอินเทอร์เน็ตนี้ อาจก่อให้เกิดความเสี่ยงด้านไซเบอร์ในรูปแบบและระดับความรุนแรงที่แตกต่างกันไปตามลักษณะของช่องทาง จำนวนช่องทาง รูปแบบการให้บริการ ข้อมูลที่เกี่ยวข้องกับการให้บริการ รวมถึงเทคโนโลยีที่ใช้สำหรับช่องทางการให้บริการดังกล่าว โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๒.๑.๑	รูปแบบการให้บริการลูกค้าหรือผู้เอาประกันภัยผ่าน Website ของบริษัท	รูปแบบการให้บริการ	ไม่มีการให้บริการผ่าน Website ของบริษัท	เป็นการให้ข้อมูลเพียงอย่างเดียว	เป็นการให้บริการทำธุรกรรมต่าง ๆ (Underwriting / Policy issuance / Claim / Premium collection)		การให้บริการทำธุรกรรม ได้แก่ ๑) ลูกค้าสามารถได้รับกรมธรรม์แบบอัตโนมัติภายหลังจากที่สั่งซื้อผ่าน Website โดยไม่ต้องมีพนักงานบริษัทเข้ามามีส่วนร่วมในการพิจารณา ๒) ลูกค้าสามารถขอและรับทราบผลการอนุมัติการเรียกร้องค่าสินไหมผ่าน Website โดยไม่ต้องมีพนักงานบริษัทเข้ามามีส่วนร่วมในการพิจารณา ๓) ลูกค้าสามารถดำเนินการจ่ายเงินค่าเบี้ยประกันผ่าน Website ของบริษัทที่มีการเชื่อมต่อผ่านระบบ Payment gateway หรือ ระบบของธนาคาร ทั้งนี้ หาก Website ของบริษัทมีการให้บริการอย่างใดอย่างหนึ่งนี้ ให้ถือว่ามีการทำธุรกรรมผ่าน Website ของบริษัท
๒.๑.๒	จำนวน Domain และ Subdomain Website ของบริษัทที่ลูกค้าหรือผู้เอาประกันภัยสามารถเข้าถึงได้ผ่านเครือข่ายอินเทอร์เน็ต	จำนวน Domain และ Subdomain	น้อยกว่า ๑๐	๑๐-๕๐	มากกว่า ๕๐		**จำนวน Domain** หมายถึง จำนวนชื่อที่ใช้ในการอ้างอิงเพื่อไปยัง Website ของบริษัทบนเครือข่ายอินเทอร์เน็ต **จำนวน Subdomain** หมายถึง จำนวนเว็บย่อยของเว็บไซต์บริษัท เช่น - webboard.xxx.com - chat.xxx.com

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๒.๑.๓	รูปแบบการให้บริการลูกค้าหรือผู้เอาประกันภัยผ่าน Mobile Application ของบริษัท	รูปแบบการให้บริการ	ไม่มีการให้บริการผ่าน Mobile Application	เป็นการให้ข้อมูลเพียงอย่างเดียว	เป็นการให้บริการทำธุรกรรมต่าง ๆ (Underwriting / Policy issuance / Claim / Premium collection)		การให้บริการทำธุรกรรม ได้แก่ ๑) ลูกค้าสามารถได้รับกรมธรรม์แบบอัตโนมัติภายหลังจากที่สั่งซื้อผ่าน Mobile Application โดยไม่ต้องมีพนักงานบริษัทเข้ามามีส่วนร่วมในการพิจารณา ๒) ลูกค้าสามารถขอและรับทราบผลการอนุมัติการเรียกร้องค่าสินไหมผ่าน Mobile Application โดยไม่ต้องมีพนักงานบริษัทเข้ามามีส่วนร่วมในการพิจารณา ๓) ลูกค้าสามารถดำเนินการจ่ายเงินค่าเบี้ยประกันผ่าน Mobile Application ของบริษัทที่มีการเชื่อมต่อผ่านระบบ Payment gateway หรือ ระบบของธนาคาร ทั้งนี้ หาก Mobile Application ของบริษัทมีการให้บริการอย่างใดอย่างหนึ่งนี้ ให้ถือว่ามีการทำธุรกรรมผ่าน Mobile Application ของบริษัท
๒.๑.๔	จำนวน Mobile Application ของบริษัท ที่ให้บริการลูกค้าหรือผู้เอาประกันภัย	จำนวน Application	๐	๑	มากกว่า ๑		จำนวน Application ของบริษัททั้งหมดที่สามารถ Download ได้จาก App Store (iOS) / Google Play Store (Android)
๒.๑.๕	รูปแบบการให้บริการลูกค้าหรือผู้เอาประกันภัยผ่าน Social Media หรือ Instant Messaging ของบริษัท (Official account)	รูปแบบการให้บริการ	ไม่มีการให้บริการผ่าน Social Media หรือ Instant Messaging	เป็นการให้ข้อมูลเพียงอย่างเดียว	เป็นการให้บริการทำธุรกรรมต่าง ๆ (Underwriting / Policy issuance / Claim / Premium collection)		- ในกรณีที่ใช้ช่องทาง Social Media หรือ Instant Messaging เพื่อส่ง/รับข้อมูลต่าง ๆ ระหว่างบุคคล (อาทิ ระหว่างลูกค้าและพนักงานบริษัท) ให้ถือเป็น "การให้ข้อมูลเพียงอย่างเดียว" - ในกรณีที่ใช้ช่องทาง Social Media หรือ Instant Messaging เพื่อส่ง/รับข้อมูลต่าง ๆ ระหว่างบุคคลและระบบงาน (อาทิ ระหว่างลูกค้า และ บอต (Bot) เพื่อการส่งข้อมูลไปประมวลผลโดยอัตโนมัติ) ให้ถือเป็น "การให้บริการทำธุรกรรม"

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
							ทั้งนี้ ไม่รวมถึงบัญชี Social Media ส่วนตัวของพนักงานที่พนักงานใช้ติดต่อกับลูกค้า
๒.๑.๖	จำนวน Account (Official account) ของ Social Media หรือ Instant Messaging ที่ให้บริการลูกค้าหรือผู้เอาประกันภัย	จำนวน account	๐	๑-๒	มากกว่า ๒		-
๒.๑.๗	รูปแบบการให้บริการลูกค้าหรือผู้เอาประกันภัยทาง Website, Mobile Application หรือ Social Media ผ่านบุคคลหรือนิติบุคคลภายนอก (Third party)	รูปแบบการให้บริการ	ไม่มีการให้บริการผ่านบุคคลหรือนิติบุคคลภายนอก (Third party)	เป็นการให้ข้อมูลเพียงอย่างเดียว	เป็นการให้บริการทำธุรกรรมต่าง ๆ (Underwriting / Policy issuance / Claim / Premium collection)		ในกรณีที่บุคคลหรือนิติบุคคลภายนอก (Third party) มีรูปแบบการให้บริการที่หลากหลาย หรือ บริษัทมีบุคคลหรือนิติบุคคลภายนอกหลายราย ให้ตอบโดยเลือกการให้บริการที่มีความเสี่ยงสูงที่สุด
๒.๑.๘	จำนวนบุคคลหรือนิติบุคคลภายนอก (Third party) ที่ให้บริการลูกค้าหรือผู้เอาประกันภัยผ่านช่องทาง online อันได้แก่ Website, Mobile Application, Social Media หรือ Instant Messaging	จำนวน Third party (นับตาม legal entities)	๐	๑-๕	มากกว่า ๕		-

IR3 ลักษณะผลิตภัณฑ์และการให้บริการ (Products & Technology Services)

ลักษณะผลิตภัณฑ์และการให้บริการ เป็นมุมมองปัจจัยเสี่ยงที่พิจารณาขอบเขตและปริมาณการให้บริการผลิตภัณฑ์ที่ต้องพึ่งพาระบบสารสนเทศใ นการให้บริการ ซึ่งผลิตภัณฑ์ หรือ ธุรกรรมที่มีการให้บริการผ่านระบบ Online อาจมีความเสี่ยงทางด้านไซเบอร์ รวมถึงความปลอดภัยและความเป็นส่วนบุคคลของข้อมูลสำคัญ มากกว่าธุรกรรมที่มีการให้บริการในรูปแบบปกติ โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๓.๑.๑	ร้อยละของจำนวนกรมธรรม์ทั้งหมดที่มีการซื้อขายผ่านระบบ Online (ในรอบระยะเวลา ๑๒ เดือน)	ร้อยละของจำนวนกรมธรรม์	๐ %	ไม่เกิน ๕ %	มากกว่า ๕ %		คำนวณโดย (จำนวนกรมธรรม์ทั้งหมดที่มีการซื้อขายผ่านระบบ Online / จำนวนกรมธรรม์ทั้งหมด) จำนวนกรมธรรม์ พิจารณาจากกรมธรรม์ที่มีผลบังคับใช้ (Policy In-force) ทั้งที่เป็นกรมธรรม์ใหม่ และ ที่มีการต่ออายุ (Renew) ทั้งนี้ ไม่รวมถึงกรมธรรม์ที่ชำระเงินแล้วแต่ยังไม่บังคับใช้ และ ไม่รวมถึงกรมธรรม์ที่สิ้นอายุแล้ว
๓.๑.๒	ร้อยละของมูลค่ากรมธรรม์ (Sum Insured) ทั้งหมดที่มีการซื้อขายผ่านระบบ Online (ในรอบระยะเวลา ๑๒ เดือน)	ร้อยละของมูลค่ากรมธรรม์	๐ %	ไม่เกิน ๕ %	มากกว่า ๕ %		คำนวณโดย (มูลค่ากรมธรรม์ทั้งหมดที่มีการซื้อขายผ่านระบบ Online / มูลค่ากรมธรรม์ทั้งหมด) มูลค่ากรมธรรม์ พิจารณาจากกรมธรรม์ที่มีผลบังคับใช้ (Policy In-force) ทั้งที่เป็นกรมธรรม์ใหม่ และ ที่มีการต่ออายุ (Renew) ทั้งนี้ ไม่รวมถึงกรมธรรม์ที่ชำระเงินแล้วแต่ยังไม่บังคับใช้ และ ไม่รวมถึงกรมธรรม์ที่สิ้นอายุแล้ว
๓.๑.๓	ร้อยละของจำนวนรายการ Claim ทั้งหมดที่มีการร้องขอผ่านระบบ Online (ในรอบระยะเวลา ๑๒ เดือน)	ร้อยละของจำนวนรายการ Claim	๐ %	ไม่เกิน ๕ %	มากกว่า ๕ %		คำนวณโดย (จำนวนรายการ Claim ทั้งหมดที่มีการร้องขอผ่านระบบ Online / จำนวนรายการ Claim ทั้งหมด)
๓.๑.๔	ร้อยละของมูลค่ารายการ Claim ทั้งหมดที่มีการร้องขอผ่านระบบ	ร้อยละของมูลค่าการ Claim	๐ %	ไม่เกิน ๕ %	มากกว่า ๕ %		คำนวณโดย (มูลค่ารายการ Claim ทั้งหมดที่มีการร้องขอผ่านระบบ Online / มูลค่ารายการ Claim ทั้งหมด)

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
	Online (ในรอบระยะเวลา ๑๒ เดือน)						
๓.๑.๕	การให้บริการผลิตภัณฑ์อื่น ๆ ผ่าน Website/Mobile Application ของบริษัท (นอกเหนือจากผลิตภัณฑ์หลักของบริษัท)	การให้บริการผลิตภัณฑ์อื่น ๆ	ไม่มี หรือ มีเฉพาะผลิตภัณฑ์ของบริษัทที่เกี่ยวกับธุรกิจประกันภัยของบริษัทเท่านั้น	มีผลิตภัณฑ์อื่น ๆ ของบริษัทในเครือที่ไม่เกี่ยวกับธุรกิจประกันภัย	มีผลิตภัณฑ์อื่นๆ นอกกลุ่มบริษัทในเครือ		ตัวอย่างเช่น การให้บริการกองทุนสำรองเลี้ยงชีพ (Provident Fund) หรือ การให้บริการประเภท Customer Royalty Program เพื่อเป็นส่วนลดในการซื้อสินค้าและบริการต่าง ๆ ที่ไม่ใช่ผลิตภัณฑ์ประกันภัย เป็นต้น
๓.๑.๖	จำนวนเทคโนโลยีใหม่ที่บริษัทนำมาใช้เป็นครั้งแรก ในรอบ ๑๒ เดือน	จำนวนเทคโนโลยี	๐	๑-๒	มากกว่า ๒		นับตามจำนวนเทคโนโลยี เช่น Blockchain, Artificial Intelligence /Machine Learning, Robotic Process Automation หรือ Cloud เป็นต้น

IR4 ขนาด และลักษณะเฉพาะขององค์กร (Business Size & Organization Characteristics)

ขนาด และลักษณะเฉพาะขององค์กร เป็นมุมมองปัจจัยเสี่ยงที่พิจารณาจากขนาด และลักษณะเฉพาะในการดำเนินงานของบริษัทประกันภัย ซึ่งก่อให้เกิด ความเสี่ยงด้านไซเบอร์จากปัจจัยแวดล้อมที่แตกต่างกัน เช่น จำนวนสถานที่ปฏิบัติงาน จำนวนพนักงาน โครงสร้างการบริหารงานสารสนเทศ การเปลี่ยนแปลงของสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศ เป็นต้น ซึ่งรวมถึงการจ้างบริษัทผู้ให้บริการภายนอก หรือ บุคคลภายนอกที่รับผิดชอบดำเนินงานทางด้านเทคโนโลยีสารสนเทศแทนบริษัท ปัจจัยเสี่ยงในมุมมองนี้ แบ่งออกเป็น ๓ มุมมองย่อย ได้แก่

- IR 4.1 ขนาดของธุรกิจ (Business Size)
- IR 4.2 โครงสร้างบุคลากร (HR Structure)
- IR 4.3 ผู้ใช้งานที่มีสิทธิสูง (High-privileged users)

IR 4.1 ขนาดของธุรกิจ (Business Size) - ขนาดของธุรกิจหรือเครือข่ายสาขาเป็นปัจจัยที่จะบ่งชี้ถึงขอบเขตการบริหารจัดการ รวมทั้งผลกระทบที่อาจเกิดขึ้นในกร ณีที่มีเหตุการณ์ภัยคุกคาม หรือความเสี่ยงทางด้านไซเบอร์ เช่นในกรณีที่บริษัทมีเครือข่ายสาขาเป็นจำนวนมาก การบริหารจัดการทางด้านสารสนเทศและไซเบอร์ก็ต้องมีมากขึ้น โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๔.๑.๑	จำนวนสาขา	จำนวนสาขา	น้อยกว่า ๕	๕-๒๐	มากกว่า ๒๐		ไม่รวมการออกบูธ หรือ สำนักงานชั่วคราว
๔.๑.๒	จำนวนพนักงานของบริษัทที่เป็นพนักงานและลูกจ้างประจำทั้งหมด และจำนวนตัวแทนของบริษัท (Agent)	จำนวนพนักงาน และตัวแทน	น้อยกว่า ๕๐๐	๕๐๐-๕,๐๐๐	มากกว่า ๕,๐๐๐		-
๔.๑.๓	จำนวนกรมธรรม์ทั้งหมด	จำนวนกรมธรรม์	น้อยกว่า ๒๐๐,๐๐๐๐	๒๐๐,๐๐๐ - ๑,๐๐๐,๐๐๐	มากกว่า ๑,๐๐๐,๐๐๐		จำนวนกรมธรรม์ พิจารณาจากกรมธรรม์ที่มีผลบังคับใช้ (Policy In-force) ทั้งที่เป็นกรมธรรม์ใหม่ และ ที่มีการต่ออายุ (Renew) ทั้งนี้ ไม่รวมถึงกรมธรรม์ที่ชำระเงินแล้วแต่ยังไม่บังคับใช้ และ ไม่รวมถึงกรมธรรม์ที่สิ้นอายุแล้ว

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๔.๑.๔	มูลค่ากรมธรรม์ (Sum Insured) รวม (ในรอบระยะเวลา ๑๒ เดือน)	มูลค่า (ล้านบาท)	น้อยกว่า ๑๐๐,๐๐๐	๑๐๐,๐๐๐ - ๑,๐๐๐,๐๐๐	มากกว่า ๑,๐๐๐,๐๐๐		มูลค่ากรมธรรม์ พิจารณาจากกรมธรรม์ที่มีผลบังคับใช้ (Policy In-force) ทั้งที่เป็นกรมธรรม์ใหม่ และ ที่มีการต่ออายุ (Renew) ทั้งนี้ ไม่รวมถึงกรมธรรม์ที่ชำระเงินแล้วแต่ยังไม่บังคับใช้ และ ไม่รวมถึงกรมธรรม์ที่สิ้นอายุแล้ว
๔.๑.๕	มูลค่าเบี้ยประกันที่รับรวมทั้งหมด (ในรอบระยะเวลา ๑๒ เดือน)	มูลค่า (ล้านบาท)	น้อยกว่า ๑,๐๐๐	๑,๐๐๐ - ๕,๐๐๐	มากกว่า ๕,๐๐๐		- ในกรณีบริษัทประกันภัยทั่วไปให้พิจารณาจากเบี้ยประกันภัยรับโดยตรง (Direct Premium) - ในกรณีบริษัทรับประกันภัยต่อให้พิจารณาจากเบี้ยประกันภัยต่อ (Reinsurance Premium)

IR 4.2 โครงสร้างบุคลากร (HR Structure) - โครงสร้างบุคลากร และ จำนวนพนักงานสารสนเทศเป็นปัจจัยที่จะบ่งชี้ถึงลักษณะของหน่วยงานสารสนเทศ ได้แก่ (๑) จำนวนเจ้าหน้าที่สารสนเทศในแต่ละ line of defense เมื่อเปรียบเทียบกับพนักงานบริษัททั้งหมด อาจแสดงถึงความสามารถในการบริหารจัดการ และ การดูแลทางด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ว่าสามารถทำได้ทั่วถึงหรือไม่ (๒) อัตราการลาออกของพนักงาน อาจแสดงถึงความสามารถในการส่งต่อความรู้ ความเชี่ยวชาญในการบริหารจัดการระบบสารสนเทศ หรือ (๓) การใช้งานบุคลากรภายนอกทั้งที่เป็นบริษัทในเครือ ผู้ให้บริการ หรือ พนักงานชั่วคราวต่าง ๆ อาจแสดงถึงความซับซ้อนที่บริษัทจะต้องควบคุมการทำงานของบุคคลภายนอกเหล่านี้ ให้เป็นไปตามความมุ่งหวัง และ ความมั่นคงปลอดภัยที่บริษัทต้องการ โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๔.๒.๑	อัตราส่วนร้อยละของจำนวนพนักงาน IT (จากทุก Line of Defense) ต่อ จำนวนพนักงานของบริษัทที่เป็นพนักงานและลูกจ้างประจำทั้งหมด	อัตราส่วนร้อยละของพนักงาน IT ทั้งหมด ต่อ พนักงานบริษัททั้งหมด	มากกว่า ๑๐ %	๓-๑๐ %	น้อยกว่า ๓ %		คำนวณโดย (รวมจำนวนพนักงาน IT จากทุก Line of Defense / จำนวนพนักงานและลูกจ้างประจำทั้งหมด) พนักงาน IT จากทุก Line of Defense ครอบคลุมถึงพนักงานที่ปฏิบัติงานทางด้านสารสนเทศ พนักงานที่ปฏิบัติงานทางด้านความปลอดภัยสารสนเทศ (IT / Cyber

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
							Security) พนักงานที่ปฏิบัติงานทางด้านการกำกับดูแลด้านสารสนเทศ (IT Compliance) พนักงานที่ปฏิบัติงานทางด้านความเสี่ยงด้านสารสนเทศ (IT Risk) และ พนักงานที่ปฏิบัติงานทางด้านการตรวจสอบสารสนเทศ (IT Audit) เป็นต้น
๔.๒.๒	อัตราส่วนร้อยละของจำนวนพนักงาน IT ที่ลาออกเฉลี่ย (จากทุก Line of Defense) (ในรอบระยะเวลา ๑๒ เดือน)	อัตราส่วนร้อยละของพนักงาน IT ที่ลาออกเฉลี่ยทั้งปี	น้อยกว่า ๑ %	๑-๕ %	มากกว่า ๕ %		คำนวณโดย ค่าเฉลี่ย ๑๒ เดือนจากร้อยละของ (จำนวนพนักงานสารสนเทศจากทุก Line of Defense ที่ลาออกทั้งหมดในแต่ละเดือน / จำนวนพนักงานสารสนเทศ ณ ต้นเดือนแต่ละเดือน)
๔.๒.๓	จำนวนบริการทางด้านสารสนเทศที่บริษัทใช้บริการจากบริษัทในเครือ และ ผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsource)	จำนวนผู้ให้บริการ (นับตาม Legal Entities)	น้อยกว่า ๓	๓-๑๐	มากกว่า ๑๐		กรณีที่ผู้ให้บริการเป็นบริษัทในเครือเดียวกัน แต่มีให้บริการมากกว่า ๑ บริการ ให้นับตาม Legal Entities หรือในกรณีนี้คือให้นับ ๑

IR 4.3 ผู้ใช้งานที่มีสิทธิสูง (High-privileged users) - ผู้ใช้งานที่มีสิทธิสูง หรือ High-privileged users เป็นบัญชีผู้ใช้งานที่ได้รับสิทธิพิเศษที่สามารถปฏิบัติงานในระบบสารสนเทศได้มากกว่าบัญชีผู้ใช้งานทั่วไป ซึ่งบัญชีผู้ใช้งานเหล่านี้อาจก่อให้เกิดความเสี่ยง และ ความเสียหายแก่ระบบสารสนเทศได้มากกว่าบัญชีผู้ใช้งานทั่วไป โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองย่อยนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๔.๓.๑	อัตราส่วนร้อยละของจำนวนพนักงานของบริษัท พนักงานของบริษัทในเครือ และบริษัทภายนอก	อัตราส่วนร้อยละของ	น้อยกว่า ๑ %	๑-๘ %	มากกว่า ๘%		ในกรณีที่มีพนักงาน ๑ ท่าน ถือบัญชี Privileged ID มากกว่า ๑ บัญชี ให้นับเป็น ๑ ตามจำนวนบุคคลเป็นหลัก คำนวณโดย (รวมจำนวนพนักงานสารสนเทศ พนักงานของ

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
	ที่ถือครองบัญชีที่มีสิทธิสูง (High-privileged users) ในระบบงานสำคัญ อาทิ Administrator, Root, User administrator, Network Administrator, DBA, เป็นต้น	พนักงานที่มีสิทธิสูง					บริษัทในเครือและบริษัทภายนอกที่ถือครองบัญชีที่มีสิทธิสูง (High-privileged Users) ในระบบงานสำคัญ / จำนวนพนักงานและลูกจ้างประจำทั้งหมด) บัญชีที่มีสิทธิสูง (High-privileged Users) ได้แก่ บัญชีผู้ใช้งานที่สามารถบริหารจัดการระบบ หรือ บริหารจัดการผู้ใช้งานในระบบได้ อาทิ Administrator, Root, User Administrator, Network Administrator, DBA เป็นต้น ทั้งนี้ ไม่รวมถึงบัญชีผู้ใช้งานทั่วไป (End Users) ที่ได้สิทธิสูงในกระบวนการทางธุรกิจ เช่น สิทธิการอนุมัติ หรือ สิทธิการเข้าถึงข้อมูลหรือเมนูในระดับระบบงาน (Application หรือ Software)
๔.๓.๒	อัตราส่วนร้อยละของจำนวนพนักงานของบริษัทที่ถือครองบัญชีที่มีสิทธิสูง (High-privileged Users) ในระบบงานสำคัญ ที่ลาออก (ในรอบระยะเวลา ๑๒ เดือน)	อัตราส่วนร้อยละของพนักงานลาออกเฉลี่ยทั้งปี	๐%	ไม่เกิน ๕ %	มากกว่า ๕ %		คำนวณโดย ค่าเฉลี่ย ๑๒ เดือนจากร้อยละของ (จำนวนพนักงานลาออกที่ถือครองบัญชีที่มีสิทธิสูง (High-privileged Users) ในระบบงานสำคัญในแต่ละเดือน/ จำนวนพนักงานที่ถือครองบัญชีที่มีสิทธิสูง (High-privileged Users) ในระบบงานสำคัญทั้งหมด ณ ต้นเดือนแต่ละเดือน)

IR5 ประวัติการถูกคุกคามทางไซเบอร์ (Cyber Threats Records)

ประวัติการถูกคุกคามทางไซเบอร์ เป็นมุมมองปัจจัยเสี่ยงของบริษัทที่มีแนวโน้ม หรือ เคยตกเป็นเป้าของการโจมตีทางไซเบอร์ในอดีต เช่น Phishing, Malware, Social Engineering, DDoS หรือ Data Breach เป็นต้น โดยประเภทการโจมตี และปริมาณการโจมตีในอดีตเป็นปัจจัยที่อาจแสดงถึงความเป็นไปได้ (Likelihood) ที่บริษัทอาจตกเป็นเป้าโจมตี หรือ ถูกโจมตีในอนาคต โดยรายละเอียดการประเมินระดับความเสี่ยงสืบเนื่องในมุมมองนี้ประกอบด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๕.๑.๑	จำนวนการโจมตีทางไซเบอร์ (Cyber Attack) ต่อระบบสารสนเทศของบริษัทประเภท Malware / Virus (ในรอบระยะเวลา ๑๒ เดือน)	จำนวนการโจมตี	น้อยกว่า ๕๐๐	๕๐๐–๑๐,๐๐๐	มากกว่า ๑๐,๐๐๐ หรือไม่มีข้อมูล		พิจารณาโดยให้นับจำนวนครั้งที่ตรวจพบ Malware หรือ Virus ในรอบ ๑๒ เดือนที่ผ่านมา ทั้งที่มีความเสียหายและไม่มีความเสียหาย โดยนับข้อมูลจากระบบ Anti-Malware เช่น Antivirus Software, Firewall, IDS, IPS เป็นต้น ในกรณีที่บริษัทไม่มีการติดตั้งระบบ Antivirus หรือ ระบบที่ทำงานในลักษณะเดียวกัน และไม่มีกระบวนการประเมินติดตาม หรือจัดเก็บข้อมูลมาก่อน ให้ถือว่าบริษัทไม่มีข้อมูลในข้อนี้
๕.๑.๒	จำนวนการโจมตีทางไซเบอร์ (Cyber Attack) ต่อระบบสารสนเทศของบริษัทประเภท Phishing / Social Engineering (ในรอบระยะเวลา ๑๒ เดือน)	จำนวนการโจมตี	น้อยกว่า ๕๐๐	๕๐๐–๑๐,๐๐๐	มากกว่า ๑๐,๐๐๐ หรือไม่มีข้อมูล		พิจารณาโดยให้นับตามจำนวนครั้งที่เกิด ทั้งที่ก่อให้เกิดความเสียหายและไม่ก่อให้เกิดความเสียหายจาก Social Engineering หรือ การทำ Phishing ผ่านช่องทางต่าง ๆ ของระบบสารสนเทศ อาจจะเป็นอีเมล URL เว็บไซต์ปลอม เป็นต้น โดยนับจากการแจ้งจากผู้ใช้งานระบบ หรือโปรแกรมตรวจจับที่ติดตั้งอยู่ในองค์กร เช่น Antivirus Software, Email Security เป็นต้น ในกรณีที่บริษัทไม่มีกระบวนการเพื่อตรวจพบ แจ้งเหตุ ประเมิน หรือจัดเก็บข้อมูลมาก่อน ให้ถือว่าบริษัทไม่มีข้อมูลในข้อนี้

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
							ทั้งนี้ พิจารณาเฉพาะการโจมตีประเภท Phishing / Social Engineering ที่เกิดขึ้นกับระบบ Email หรือ ระบบสารสนเทศของบริษัทเท่านั้น ไม่รวมการโจมตีประเภท Phishing / Social Engineering โดยตรงไปยัง Email ของลูกค้า
๕.๑.๓	จำนวนการโจมตีทางไซเบอร์ (Cyber Attack) ต่อระบบสารสนเทศของบริษัทประเภท DoS / DDoS (ในรอบระยะเวลา ๑๒ เดือน)	จำนวนการโจมตี	น้อยกว่า ๑๐๐	๑๐๐–๕,๐๐๐	มากกว่า ๕,๐๐๐ หรือ ไม่มีข้อมูล		พิจารณาโดยให้นับจำนวนครั้งที่มี Bandwidth หรือ Requests Per Second เกิน Threshold ที่บริษัทกำหนดไว้ หากมีจำนวนครั้งเกินติดต่อกันเป็นระยะเวลานาน ให้นับเป็น ๑ ครั้ง โดยดูจากข้อมูลในรอบ ๑๒ เดือนที่ผ่านมา และนับทั้งที่มีความเสียหายและไม่มีความเสียหาย โดยนับข้อมูลจาก DDoS Protection Service Provider หรือ DDoS Protection ที่ติดตั้งเอง หรืออาจนับจากข้อมูล Log ของอุปกรณ์ ที่มี Pattern ที่สามารถตรวจจับการโจมตีแบบ DDoS ได้ เช่น Firewall, IDS, IPS เป็นต้น ในกรณีที่บริษัทไม่มีกระบวนการเพื่อตรวจพบ ประเมิน หรือจัดเก็บข้อมูลมาก่อน ให้ถือว่าบริษัทไม่มีข้อมูลในข้อนี้
๕.๑.๔	จำนวนการโจมตีทางไซเบอร์ (Cyber Attack) ต่อระบบสารสนเทศของบริษัทประเภท SQL Injection, XSS, CSRF (ในรอบระยะเวลา ๑๒ เดือน)	จำนวนการโจมตี	น้อยกว่า ๑,๐๐๐	๑,๐๐๐–๑๐๐,๐๐๐	มากกว่า ๑๐๐,๐๐๐ หรือ ไม่มีข้อมูล		พิจารณาโดยให้นับจำนวนครั้งที่เกิดกับ Web Application / Mobile Application ที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต ที่เกิดขึ้นภายในรอบ ๑๒ เดือนที่ผ่านมา โดยนับทั้งที่มีความเสียหายและไม่มีความเสียหาย โดยนับจาก Log ของอุปกรณ์ IDS, IPS, Web Application Firewall, Next-generation Firewall หรือ Firewall ที่ทำงานในระดับ Application Layer ในกรณีที่บริษัทไม่มีกระบวนการเพื่อตรวจพบ ประเมิน หรือจัดเก็บข้อมูลมาก่อน ให้ถือว่าบริษัทไม่มีข้อมูลในข้อนี้

ปัจจัยเสี่ยง		หน่วยนับ	ระดับความเสี่ยง			ระดับความเสี่ยง	การพิจารณา
			ต่ำ	ปานกลาง	สูง		
๕.๑.๕	จำนวนเหตุการณ์ประเภท Data Breach และการรั่วไหลของข้อมูลส่วนบุคคลที่เกิดขึ้นแล้ว (ในรอบระยะเวลา ๑๒ เดือน)	จำนวนครั้งที่เหตุการณ์เกิดขึ้นแล้ว	๐	๑	มากกว่า ๑		พิจารณา โดยให้นับตามจำนวนครั้งที่เกิดภายในรอบ ๑๒ เดือนที่ผ่านมา ทั้งในกรณีที่ข้อมูลรั่วไหลจากการโจมตีทางไซเบอร์ หรือ จากอุบัติเหตุ จากการทุจริตหรือความผิดพลาดของระบบจากกระบวนการหรือพนักงานภายในขององค์กร โดยนับจากเหตุการณ์ข้อมูลรั่วไหลที่ก่อให้เกิดความเสียหาย และ ถูกตรวจพบจากกระบวนการหรือเครื่องมือขององค์กร รวมถึงเหตุการณ์ในกรณีที่บริษัทตรวจพบการรั่วไหลของข้อมูลจากแหล่งที่มาภายนอก (External Source) ที่อาจไม่ถูกตรวจจับโดยกระบวนการหรือเครื่องมือขององค์กรด้วย ทั้งนี้ ให้พิจารณาเฉพาะการโจมตีประเภท Data Breach ที่เกิดขึ้นกับระบบสารสนเทศของบริษัทเท่านั้น ไม่รวม Data Breach ที่เกิดจากลูกค้าเอง

สรุปผลการประเมินระดับความเสี่ยงตั้งต้น หรือ ระดับความเสี่ยงสืบเนื่อง (Inherent Risk : IR)

ระดับความเสี่ยงของแต่ละมุมมองความเสี่ยง คิดจากค่าเฉลี่ยของผลการประเมินความเสี่ยงในแต่ละปัจจัยของหัวข้อมุมมองความเสี่ยงนั้น ซึ่งมีวิธีการคำนวณดังนี้

๑. แทนค่าความเสี่ยงของแต่ละปัจจัยเสี่ยงโดยให้ ระดับความเสี่ยง “สูง” มีค่า ๓ ระดับความเสี่ยง “ปานกลาง” มีค่า ๒ และ ระดับความเสี่ยง “ต่ำ” มีค่า ๑
๒. หาค่าเฉลี่ยรวมของแต่ละหัวข้อมุมมองความเสี่ยง โดยที่
   - มุมมองความเสี่ยงที่มีค่าเฉลี่ยสูงกว่า ๒.๓๓ ถือเป็น ระดับความเสี่ยง “สูง”
   - มุมมองความเสี่ยงที่มีค่าเฉลี่ยอยู่ระหว่าง ๑.๖๗ - ๒.๓๓ ถือเป็น ระดับความเสี่ยง “ปานกลาง”
   - มุมมองความเสี่ยงที่มีค่าเฉลี่ยต่ำกว่า ๑.๖๗ ถือเป็น ระดับความเสี่ยง “ต่ำ”

เมื่อได้ผลระดับความเสี่ยงสืบเนื่องตามมุมมองความเสี่ยงแล้ว ให้คำนวณระดับความเสี่ยงสืบเนื่องรวมของบริษัท โดยมีขั้นตอนดังนี้

๑. แทนค่าความเสี่ยงของแต่ละหัวข้อมุมมองความเสี่ยงโดยให้ ระดับความเสี่ยง “สูง” มีค่า ๓ ระดับความเสี่ยง “ปานกลาง” มีค่า ๒ และ ระดับความเสี่ยง “ต่ำ” มีค่า ๑
๒. ถ่วงน้ำหนักของแต่ละหัวข้อมุมมองความเสี่ยง ดังนี้

หัวข้อมุมมองความเสี่ยง	การถ่วงน้ำหนัก
IR1 เทคโนโลยีและการเชื่อมต่อ (Technologies and Connection)	ร้อยละ ๒๕
IR2 ช่องทางการให้บริการ (Delivery Channels)	ร้อยละ ๒๕
IR3 ลักษณะผลิตภัณฑ์และการให้บริการ (Products & Technology Services)	ร้อยละ ๒๐
IR4 ขนาด และลักษณะเฉพาะขององค์กร (Business Size & Organization Characteristics)	ร้อยละ ๑๕
IR5 ประวัติการถูกคุกคามทางไซเบอร์ (Cyber Threats Records)	ร้อยละ ๑๕

๓. หาค่าเฉลี่ยรวมของความเสี่ยงสืบเนื่องของบริษัท โดย
   - ค่าเฉลี่ยรวมที่สูงกว่า ๒.๓๓ ถือเป็น ระดับความเสี่ยง “สูง”
   - ค่าเฉลี่ยรวมที่อยู่ระหว่าง ๑.๖๗ - ๒.๓๓ ถือเป็น ระดับความเสี่ยง “ปานกลาง”
   - ค่าเฉลี่ยรวมที่ต่ำกว่า ๑.๖๗ ถือเป็น ระดับความเสี่ยง “ต่ำ”

ส่วนที่ 2 การประเมินระดับการควบคุม (Control Maturity)

ระดับการควบคุมพิจารณาจากการควบคุมที่บริษัทจัดให้มีขึ้น โดยบริษัทต้องพิจารณาว่าการควบคุมที่กำหนดในแบบประเมินนั้นตรงกับลักษณะใดดังต่อไปนี้ (๑) จัดให้มีขึ้นทั้งหมด (Yes) (๒) จัดให้มีขึ้นมากกว่ากึ่งหนึ่ง (Partial) (๓) ไม่ได้จัดให้มีขึ้นหรือจัดให้มีขึ้นไม่ถึงกึ่งหนึ่ง (No) หรือ (๔)เป็นการควบคุมที่ไม่เกี่ยวข้องกับการดำเนินงานหรือเทคโนโลยีสารสนเทศของบริษัท (N/A)

กรอบ CRAF แบ่งหมวดหมู่การควบคุมทางเทคโนโลยีสารสนเทศและไซเบอร์ออกเป็น ๖ หมวดหมู่ ได้แก่ การกำกับดูแล การระบุความเสี่ยง การป้องกันความเสี่ยง การตรวจสอบและเฝ้าระวัง การรับมือและตอบสนองเมื่อพบเหตุการณ์ และ การบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุ รกิจ โดยแบ่งผลการประเมินเป็น ๓ ระดับ คือ Baseline Intermediate และ Advance ซึ่งมีรายละเอียดการควบคุมในแต่ละหมวดหมู่ ดังนี้

CM1 การกำกับดูแล (Governance)

วัตถุประสงค์ : เพื่อให้บริษัทประกันภัยมีการกำกับดูแลและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์อย่างเพียงพอเหมาะสม โดยมีโครงสร้างและบทบาทหน้าที่ที่สอดคล้องตามหลัก Three lines of defense มีการกำหนดนโยบายและแผนกลยุทธ์การดำเนินงานด้านเทคโนโลยีสารสนเทศและไซเบอร์ ที่สอดคล้องกับการกำกับดูแลในภาพรวมของบริษัท รวมทั้งมีการติดตามการดำเนินงานด้านการกำกับดูแลและรายงานผลที่เหมาะสม

CM 1.1 การกำกับดูแลด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
๑.๑.๑ โครงสร้างการกำกับดูแล และบทบาทหน้าที่		
Baseline	๑.๑.๑.๑	บริษัทมีโครงสร้างการกำกับดูแลทางด้านสารสนเทศและไซเบอร์ที่สอดคล้องตามหลักการผู้รับผิดชอบสามระดับ (Three lines of defense) อันได้แก่ (๑) 1st line of defense: ส่วนงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศหรือไซเบอร์ และผู้ใช้งานเทคโนโลยีสารสนเทศ (๒) 2nd line of defense: ส่วนงานที่ทำหน้าที่บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และ ส่วนงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมาย (๓) 3rd line of defense: ส่วนงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
	๑.๑.๑.๒	บริษัทมีการมอบหมายหน้าที่ความรับผิดชอบในการกำกับดูแลทางด้านสารสนเทศและไซเบอร์ของบริษัทให้แก่คณะกรรมการบริษัทอย่างชัดเจน และเป็นลายลักษณ์อักษร ทั้งนี้ คณะกรรมการบริษัทอาจมอบหมายให้คณะกรรมการชุดย่อยทำหน้าที่แทนได้ ซึ่งการมอบหมายหน้าที่นี้ ต้องมีการกำหนดบทบาทหน้าที่อย่างชัดเจน และเป็นลายลักษณ์อักษร
	๑.๑.๑.๓	คณะกรรมการบริษัทได้รับการอบรมความรู้เกี่ยวกับแนวโน้มการเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ รวมทั้งความเสี่ยง ผลกระทบ และแนวทางการป้องกันความเสี่ยงจากเหตุการณ์ดังกล่าว
Intermediate	๑.๑.๑.๔	คณะกรรมการบริษัทอย่างน้อย ๑ ท่าน เป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศหรือด้านการกำกับดูแลเทคโนโลยีสารสนเทศ (IT Governance) โดยอาจพิจารณาจากประวัติการศึกษา ประสบการณ์ในการทำงาน และประสบการณ์ในการเป็นคณะกรรมการหรือคณะทำงาน ที่เกี่ยวข้องทางด้านเทคโนโลยีสารสนเทศ หรือปัจจัยอื่น ๆ ที่เกี่ยวข้อง
Advance	๑.๑.๑.๕	บริษัทกำหนดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท (อาทิ กำหนดให้มี Chief Information Security Officer : CISO หรือ เทียบเท่า) เป็นการเฉพาะ และเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ โดยมีอำนาจในการกำกับดูแลความเสี่ยงและการควบคุมด้านสารสนเทศและไซเบอร์
	๑.๑.๑.๖	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย กำหนดให้หน่วยงานธุรกิจรับผิดชอบดูแลความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้อง รวมทั้งสื่อสารเกี่ยวกับบทบาทหน้าที่ในการดูแลความเสี่ยงด้านไซเบอร์อย่างทั่วถึงทั้งบริษัท
๑.๑.๒ กลยุทธ์ และนโยบาย		
Baseline	๑.๑.๒.๑	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย มีบทบาทหน้าที่ในการกำกับดูแลให้บริษัทมีการกำหนดกลยุทธ์ นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมเรื่องความมั่นคงปลอดภัยสารสนเทศและไซเบอร์และสอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัท รวมทั้งดูแลและติดตามให้มีการปฏิบัติงานตามกลยุทธ์ นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม
	๑.๑.๒.๒	คณะกรรมการบริษัทและคณะกรรมการที่ได้รับมอบหมาย มีบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลให้บริษัทจัดทำนโยบายทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ ซึ่งอย่างน้อยประกอบด้วย (๑) นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT/Cyber Risk management policy) (๒) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy)

ระดับการควบคุม	การควบคุม	
	๑.๑.๒.๓	บริษัทจัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ที่มีรายละเอียดครอบคลุมเรื่อง (๑) การบริหารจัดการทรัพย์สินสารสนเทศ (IT asset management) (๒) การควบคุมการเข้าถึงข้อมูลหรือระบบ (access control) (๓) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) (๔) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security) (๕) การจัดจ้างผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ (third party management) (๖) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT continuity) (๗) แนวทางในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (cybersecurity) โดยนโยบายข้างต้นนี้ได้รับการอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายแล้ว
	๑.๑.๒.๔	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายกำกับดูแลให้บริษัทมีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security procedure) ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) รวมทั้ง ติดตามให้มีการปฏิบัติตามอย่างเหมาะสม โดยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy and procedure)ได้รับการทบทวนเป็นประจำอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
	๑.๑.๒.๕	คณะกรรมการบริษัทแต่งตั้งคณะกรรมการชุดย่อยเพื่อกำกับดูแลและบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ (เช่น Risk management committee) โดยคณะกรรมการชุดย่อยนี้ ดำเนินงานกำกับดูแลความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ตามที่ประกาศของสำนักงาน คปภ. กำหนด และ รายงานผลการกำกับดูแลในเรื่องดังกล่าวกลับไปยังคณะกรรมการบริษัท
	๑.๑.๒.๖	บริษัทจัดทำนโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT/Cyber Risk management policy) ที่ครอบคลุมเรื่อง (๑) บทบาทหน้าที่และความรับผิดชอบ (๒) กระบวนการหรือขั้นตอนในการประเมินความเสี่ยงและจัดการความเสี่ยง (๓) ระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) (๔) เกณฑ์การประเมินความเสี่ยง โดยครอบคลุมระดับของผลกระทบ และระดับของโอกาสการเกิดเหตุการณ์ (๕) วิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (๖) การกำหนดดัชนีชี้วัดความเสี่ยง (IT risk indicator) รวมถึงการจัดให้มีการติดตาม และรายงานผลดัชนีชี้วัดความเสี่ยงดังกล่าวต่อผู้ที่มีหน้าที่รับผิดชอบ

ระดับการควบคุม	การควบคุม	
		(๗) การรายงานความเสี่ยง (risk reporting) โดยนโยบายข้างต้นนี้ได้รับการอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย
	๑.๑.๒.๗	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย กำหนดให้มีการจัดทำแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ (IT/Cyber Risk management procedure) ที่สอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT/Cyber Risk management policy) รวมทั้ง ติดตามให้มีการปฏิบัติตามอย่างเหมาะสม โดยนโยบายและแนวปฏิบัติดังกล่าวได้รับการทบทวนเป็นประจำอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญ
	๑.๑.๒.๘	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย กำหนดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจ ซึ่งเป็นความเสี่ยงหลักที่สำคัญในภาพรวมระดับองค์กร และให้เป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวม (Enterprise Risk Management : ERM)
	๑.๑.๒.๙	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย จัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ อย่างสม่ำเสมอและเพียงพอ
Intermediate	๑.๑.๒.๑๐	คณะกรรมการบริษัทแต่งตั้งคณะกรรมการชุดย่อยเพื่อกำกับดูแลและบริหารจัดการการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศและไซเบอร์โดยเฉพาะ เพื่อให้มั่นใจว่าการดำเนินงานทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ของบริษัทสอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัท โดยคณะกรรมการชุดย่อยนี้มีหน้าที่รายงานผลการกำกับดูแลในเรื่องที่ได้รับมอบหมายกลับไปยังคณะกรรมการบริษัทด้วย
	๑.๑.๒.๑๑	นอกจากข้อกำหนดขั้นต่ำตามประกาศของหน่วยงานกำกับดูแล บริษัทมีการกำหนดนโยบายของบริษัท อาทิ IT Risk management policy, IT security policy หรือ IT continuity ให้ครอบคลุมและสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป (อาทิ อ้างอิงหลักการควบคุมที่ดีตามมาตรฐาน ISO27001 กรอบ Cobit5 หรือ NIST800-53 เป็นต้น) รวมทั้งมีการปรับปรุงนโยบายเมื่อมีการเปลี่ยนแปลงมาตรฐานสากลที่เกี่ยวข้อง
	๑.๑.๒.๑๒	นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) มีรายละเอียดครอบคลุมเรื่อง (๑) การบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (human resource security) (๒) การกำหนดแนวปฏิบัติด้านการเข้ารหัสข้อมูล (cryptography) (๓) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัท (network and communication security) (๔) การกำหนดหลักเกณฑ์และกระบวนการในการจัดหาและการพัฒนาระบบ (system acquisition and development) (๕) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)
	๑.๑.๒.๑๓	คณะกรรมการบริษัทได้แต่งตั้งคณะกรรมการหรือผู้บริหารระดับสูงให้รับผิดชอบทางด้านการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องทางด้านสารสนเทศและไซเบอร์

ระดับการควบคุม	การควบคุม	
	๑.๑.๒.๑๔	บริษัทมีแนวทางในการกำกับดูแลและเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (Cyber resilience) ที่สอดคล้องตามกฎหมายว่าด้วยการรักษาความปลอดภัยทางไซเบอร์ โดยมีการดำเนินการเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ที่สอดคล้องกับความเสี่ยงทางด้านไซเบอร์ และ ลักษณะการดำเนินธุรกิจของบริษัท
	๑.๑.๒.๑๕	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายกำหนดและอนุมัติข้อความที่แสดงถึงระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่ยอมรับได้ (IT / Cyber Risk Appetite Statement) เพื่อใช้ในการบริหารความเสี่ยงขององค์กร
	๑.๑.๒.๑๖	บริษัทจัดสรรงบประมาณในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้ครอบคลุม ระบบงาน (application) ข้อมูล (information) โครงสร้างพื้นฐาน (infrastructure) เครื่องมือ และ บุคลากร โดยสอดคล้องและเพียงพอตามระดับความเสี่ยงที่บริษัทมี
Advance	๑.๑.๒.๑๗	บริษัทกำหนดให้กลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของกลยุทธ์การบริหารจัดการความเสี่ยงขององค์กร
	๑.๑.๒.๑๘	นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) หรือนโยบายอื่นที่เกี่ยวข้อง ครอบคลุมถึงการบริหารจัดการทางด้านไซเบอร์อย่างเฉพาะเจาะจง อาทิ การแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์กับองค์กรภายนอก (Cyber Threat Intelligence Sharing) หรือ การบริหารจัดการเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์โดยแยกจาก IT incident response plan
	๑.๑.๒.๑๙	บริษัทพิจารณากระบวนการจัดสรรงบประมาณทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ เป็นส่วนหนึ่งของการจัดสรรงบประมาณของหน่วยงานธุรกิจ
๑.๑.๓ การจัดให้มีการรายงาน		
Baseline	๑.๑.๓.๑	บริษัทกำหนดวาระการรายงานต่อคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย ให้ครอบคลุมถึงเรื่อง (๑) ผลการบริหารจัดการความเสี่ยงทางเทคโนโลยีสารสนเทศและไซเบอร์ (๒) ปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่สำคัญ ที่อาจส่งผลกระทบในวงกว้างต่อชื่อเสียงของบริษัท หรือการดำเนินงานและการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (๓) ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
Intermediate	๑.๑.๓.๒	บริษัทกำหนดให้มีการรายงานสถานการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศ และ ภัยคุกคามทางไซเบอร์ที่บริษัทเผชิญ ให้คณะกรรมการบริษัทและคณะกรรมการที่เกี่ยวข้องรับทราบเป็นประจำอย่างน้อยไตรมาสละ ๑ ครั้ง และในกรณีที่เกิดเหตุการณ์หรือความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อบริษัทในวงกว้าง หรือส่งผลกระทบต่อชื่อเสียงของบริษัท จะมีการรายงานให้คณะกรรมการบริษัทและคณะกรรมการที่เกี่ยวข้องได้รับทราบอย่างไม่ชักช้าเพื่อร่วมกันตัดสินใจแก้ไขปัญหา

ระดับการควบคุม	การควบคุม	
Advance	๑.๑.๓.๓	บริษัทรายงานสถานการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศ และ ภัยคุกคามทางไซเบอร์ที่บริษัทมีแนวโน้มจะเผชิญจากผลการวิเคราะห์ข้อมูลการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ต่อคณะกรรมการบริษัทและคณะกรรมการที่เกี่ยวข้อง เพื่อให้มีการกำหนดแนวทางการรับมือเรื่องดังกล่าวจากคณะกรรมการบริษัทและคณะกรรมการที่เกี่ยวข้อง

CM 1.2 การบริหารโครงการด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
Baseline	๑.๒.๑.๑	บริษัทประเมินความเสี่ยงและจัดลำดับความสำคัญของโครงการด้านเทคโนโลยีสารสนเทศโดยพิจารณาจาก (๑) ความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ (๒) การเลือกใช้งานเทคโนโลยีและการนำเทคโนโลยีใหม่มาใช้งานครั้งแรก (๓) การประเมินความเสี่ยงและผลกระทบ (๔) การจัดระดับความสำคัญโครงการ (๕) การอนุมัติจากคณะกรรมการหรือผู้บริหารที่เหมาะสม
	๑.๒.๑.๒	บริษัทมีกรอบในการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศที่ชัดเจน และเป็นลายลักษณ์อักษร ตลอดจนมีรายละเอียดที่ครอบคลุมในเรื่อง (๑) การเริ่มโครงการ (๒) การดำเนินงาน (๓) การควบคุมโครงการ (๔) การปิดโครงการ และ (๕) การสอบทานโครงการ
	๑.๒.๑.๓	บริษัทกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (Project Governance) มีคณะกรรมการกำกับดูแลโครงการเพื่อกำกับดูแลและติดตามความคืบหน้าการดำเนินงานของโครงการ รวมทั้งให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้โครงการสามารถดำเนินการได้ตามแผนที่กำหนดไว้
Intermediate	๑.๒.๑.๔	บริษัทกำหนดคณะกรรมการที่มีหน้าที่กำกับดูแลโครงการ (Project Governance) อย่างเฉพาะเจาะจง ซึ่งคณะกรรมการนี้ อาจประกอบด้วย ผู้บริหารที่เกี่ยวข้อง คณะทำงานโครงการ (Project Management Office: PMO) และ ผู้จัดการโครงการ (Project Manager)

CM 1.3 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
Baseline	๑.๓.๑.๑	บริษัทมีนโยบายและแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่ระบุบริบท ขอบเขต และเกณฑ์การบริหารความเสี่ยงดังต่อไปนี้

ระดับการควบคุม	การควบคุม	
		(๑) การระบุบริบทและขอบเขตในการประเมินความเสี่ยง (Risk Universe) ให้ครอบคลุมถึง แผนงาน งานประจำ การนำเทคโนโลยีสารสนเทศมาใช้ และผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ (๒) เกณฑ์การบริหารความเสี่ยง และเกณฑ์การประเมินความเสี่ยง ตามระดับของผลกระทบและโอกาสเกิด (๓) ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่ยอมรับได้ (IT/Cyber Risk Appetite) (๔) กระบวนการประเมินความเสี่ยง (Risk Evaluation) (๕) กระบวนการจัดการความเสี่ยง และมาตรการในการจัดการความเสี่ยง รวมถึงการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Treatment Plan)
	๑.๓.๑.๒	บริษัทกำหนดกระบวนการในการระบุและประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และ ไซเบอร์ โดย (๑) ระบุความเสี่ยง (Risk Identification) ด้านเทคโนโลยีสารสนเทศและไซเบอร์ การควบคุมที่มีในปัจจุบัน และผู้รับผิดชอบหรือเจ้าของความเสี่ยง (Risk Owners) โดยพิจารณาสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร ปัจจัยภายนอก ผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจ (๒) วิเคราะห์ความเสี่ยง (Risk Analysis) ด้านเทคโนโลยีสารสนเทศและไซเบอร์ โดยประเมินระดับของผลกระทบ และระดับของโอกาสการเกิด เพื่อจัดลำดับความสำคัญ (๓) ประเมินค่าความเสี่ยง (Risk Evaluation) โดยการพิจารณาระดับความเสี่ยงกับระดับความเสี่ยงที่ยอมรับได้ (IT Risk Appetite) เพื่อจัดลำดับและหาแนวทางในการตอบสนองความเสี่ยงที่เหมาะสม
	๑.๓.๑.๓	บริษัทระบุให้มีการวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นจากความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และไซเบอร์โดยพิจารณาจากหลักเกณฑ์ ดังนี้ (๑) ด้านการรักษาความลับ (Confidentiality) (๒) ด้านการรักษาความถูกต้องเชื่อถือได้ (Integrity) (๓) ด้านการรักษาสภาพพร้อมใช้งาน (Availability) และ (๔) ด้านการปฏิบัติตามกฎเกณฑ์ (Law & Regulation Compliance)
	๑.๓.๑.๔	บริษัทมีการบริหารจัดการความเสี่ยง (Risk Treatment) โดยมีแนวทางในการจัดการ ควบคุม และป้องกัน ความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ ทั้งนี้ การกำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ ควรคำนึงถึงความคุ้มค่าและวิธีการที่เหมาะสม
	๑.๓.๑.๕	บริษัทมีกระบวนการติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ด้านเทคโนโลยีสารสนเทศและไซเบอร์ โดยกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ (IT/Cyber Key Risk Indicators) เพื่อใช้ติดตามระดับความเสี่ยง และทบทวนมาตรการในการควบคุมหรือจัดการความเสี่ยงที่บริษัทดำเนินการอยู่ในปัจจุบันได้อย่างมีประสิทธิภาพ

ระดับการควบคุม	การควบคุม	
Intermediate	๑.๓.๑.๖	นโยบาย และ แนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ของบริษัท มีความสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงในภาพรวมของบริษัท อาทิ การประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ครอบคลุมผลกระทบที่อาจเกิดขึ้นในด้านอื่น ๆ ตามเกณฑ์การประเมินความเสี่ยงในภาพรวมของบริษัท เช่น ผลกระทบต่อกลยุทธ์ การดำเนินธุรกิจ หรือชื่อเสียง เป็นต้น
	๑.๓.๑.๗	บริษัทระบุความเสี่ยง (Risk Identification) ด้านเทคโนโลยีสารสนเทศและไซเบอร์ โดยครอบคลุมรายละเอียดของ (๑) ผู้กระทำให้เกิดความเสี่ยง และเหตุการณ์ความเสี่ยง (๒) ประเภทของความเสี่ยง (๓) สาเหตุของการเกิดเหตุการณ์ (๔) การควบคุมที่มีการดำเนินการอยู่ในปัจจุบัน
	๑.๓.๑.๘	บริษัทระบุให้มีการประเมินผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงทางด้านสารสนเทศและไซเบอร์อย่างรอบด้าน โดยพิจารณาถึง ผลกระทบด้าน (๑) วัตุประสงค์ในการรักษาความมั่นคงปลอดภัย (ได้แก่ Confidentiality, Integrity และ Availability) (๒) การเงิน (๓) ทรัพย์สินและทรัพยากร (๔) การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และการดำเนินธุรกิจ (๕) กลยุทธ์ และ (๖) ชื่อเสียง
	๑.๓.๑.๙	บริษัทมีหน่วยงาน ทีมงาน หรือผู้รับผิดชอบที่ชัดเจนในการทำหน้าที่รับผิดชอบดูแลและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะ
	๑.๓.๑.๑๐	บริษัทมีการประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment) เพื่อให้บริษัททราบถึงประเภทและระดับความเสี่ยงของตนเอง (Risk Profile) รวมทั้งมีแนวทางการกำกับดูแลการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ที่สอดคล้องกับระดับความเสี่ยงตั้งต้นของบริษัท (Inherent Risk) ทั้งนี้บริษัทอาจใช้การประเมิน CRAF นี้ เพื่อประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ และ ระดับการควบคุมทางไซเบอร์ โดยในกรณีที่บริษัทมีระดับการควบคุมที่ไม่สอดคล้องกับระดับความเสี่ยง บริษัทได้ดำเนินการปรับปรุงการควบคุมเหล่านั้นอย่างเหมาะสม
Advance	๑.๓.๑.๑๑	บริษัทมีการตรวจสอบกระบวนการจัดทำ ข้อความที่แสดงถึงระดับความเสี่ยงด้านไซเบอร์ที่ยอมรับได้ (Cyber Risk Appetite Statement) เพื่อให้มั่นใจว่าการกำหนด Cyber Risk Appetite Statement สอดคล้องกับขนาดและความซับซ้อนของธุรกิจ รวมถึงเปรียบเทียบความพร้อมในการรับมือภัยไซเบอร์ของบริษัท (Cyber Resilience Readiness) กับ Cyber Risk Appetite Statement ที่บริษัทกำหนด
	๑.๓.๑.๑๒	บริษัทรวบรวมและรายงานข้อมูลความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ได้อย่างรวดเร็วและน่าเชื่อถือ เพื่อใช้ในการติดตามและรายงานความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ได้อย่างมีประสิทธิภาพ โดยเฉพาะขณะที่เกิดเหตุการณ์ผิดปกติ

CM 1.4 การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
Baseline	๑.๔.๑.๑	ส่วนงานผู้มีหน้าที่รับผิดชอบในการกำกับดูแลการปฏิบัติตามและทำความเข้าใจกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) มีกระบวนการในการ (๑) ติดตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ (๒) สื่อสารและสร้างความรู้ความเข้าใจแก่ผู้ที่เกี่ยวข้อง (๓) มีการตรวจสอบหรือติดตามการการปรับปรุงนโยบายหรือแนวทางการปฏิบัติงาน ให้สอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
	๑.๔.๑.๒	บริษัทได้นำข้อกำหนดตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และ กฎหมายคุ้มครองข้อมูลส่วนบุคคลมาพิจารณาเพื่อปรับปรุงแนวทางการกำกับดูแลทางด้านสารสนเทศและไซเบอร์ของบริษัทอย่างครบถ้วน อาทิ มีการปรับปรุงนโยบายและ แนวทางปฏิบัติให้สอดคล้องกับข้อกำหนดตามกฎหมายดังกล่าว

CM 1.5 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
Baseline	๑.๕.๑.๑	บริษัทจัดให้มีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศและไซเบอร์ (ซึ่งอาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบจากภายนอกก็ได้) ที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญในการตรวจสอบในเรื่องดังกล่าว นอกจากนั้นผู้ปฏิบัติงานตรวจสอบต้องมีความเป็นอิสระจากผู้ปฏิบัติงานเทคโนโลยีสารสนเทศและไซเบอร์ใน 1st Line of Defense และ 2nd Line of Defense
	๑.๕.๑.๒	คณะกรรมการตรวจสอบ พิจารณาอนุมัติแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศและไซเบอร์ ที่ครอบคลุมความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ของบริษัทอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
	๑.๕.๑.๓	บริษัทดำเนินการตรวจสอบทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ตามแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่ได้รับอนุมัติ และเมื่อมีเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่สำคัญ
	๑.๕.๑.๔	บริษัทต้องจัดให้มีการรายงานผลการตรวจสอบไปยังคณะกรรมการตรวจสอบ โดยในกรณีที่พบประเด็นจากการตรวจสอบ บริษัทดำเนินการติดตามผลการตรวจสอบและรายงานผลการติดตามการแก้ไขประเด็นไปยังฝ่ายงานที่เกี่ยวข้อง และคณะกรรมการตรวจสอบ
Intermediate	๑.๕.๑.๕	บริษัทกำหนดแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศและไซเบอร์ ตามความเสี่ยง (Risk Based IT Audit Plan) โดยพิจารณาถึงความเพียงพอของการบริหารจัดการและการควบคุมความเสี่ยงกับระดับความเสี่ยง และ รอบระยะเวลาการตรวจสอบสำหรับเทคโนโลยีสารสนเทศที่มีความสำคัญ อาทิ ตรวจสอบกระบวนการด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่มีระดับความเสี่ยงสูง เป็นประจำทุกปี

ระดับการควบคุม	การควบคุม	
	๑.๕.๑.๖	รายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและไซเบอร์ของบริษัท ระบุถึงข้อตรวจพบ สาเหตุที่แท้จริง (Root Cause) ผลกระทบต่อธุรกิจ และคำแนะนำในการปรับปรุงแก้ไข โดยบริษัทได้กำหนดแนวทางและระยะเวลาในการปรับปรุงแก้ไขที่ชัดเจน รวมทั้ง ดำเนินการติดตามสถานะการปรับปรุงแก้ไขอย่างสม่ำเสมอ เพื่อให้การปรับปรุงแก้ไขเป็นไปตามกำหนดเวลาที่กำหนดและมีประสิทธิภาพ
Advance	๑.๕.๑.๗	บริษัทมีการปรับปรุงแผนการตรวจสอบและกำหนดขอบเขตการตรวจสอบทางด้านเทคโนโลยีสารสนเทศและไซเบอร์อย่างทันท่วงที เมื่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่เกี่ยวข้องเปลี่ยนไป หรือ เมื่อมีการเปลี่ยนแปลงรูปแบบภัยคุกคามทางไซเบอร์ในภาคธุรกิจที่เกี่ยวข้อง

CM2 การระบุความเสี่ยง (Identification)

วัตถุประสงค์ : เพื่อให้บริษัทประกันภัยมีการกำหนดขอบเขตในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่รวมถึงข้อมูลส่วนบุคคลอย่า ง ครอบคลุมครบถ้วน รวมทั้งสามารถเชื่อมโยงไปยังการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ได้อย่างเหมาะสม

CM 2.1 การบริหารจัดการทรัพย์สินสารสนเทศ

ระดับการควบคุม	การควบคุม	
Baseline	๒.๑.๑.๑	บริษัทจัดทำทะเบียนทรัพย์สินสารสนเทศที่มีความถูกต้อง ครบถ้วน ทันสมัย และ สามารถใช้เพื่อการบำรุงรักษาทรัพย์สินสารสนเทศ รวมทั้ง ใช้เพื่อกำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้ โดยครอบคลุมถึง (๑) ทรัพย์สินสารสนเทศประเภทระบบ (๒) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ (๓) ทรัพย์สินสารสนเทศประเภทข้อมูล รวมทั้ง กำหนดเจ้าของทรัพย์สิน หรือผู้รับผิดชอบทรัพย์สิน
	๒.๑.๑.๒	บริษัทมีกระบวนการในการตรวจนับ **หรือ** พิสูจน์ความครบถ้วนของทะเบียนทรัพย์สินสารสนเทศ (อาทิ การใช้งาน Discovery Tools) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจในความครบถ้วนของทะเบียนทรัพย์สินสารสนเทศ
	๒.๑.๑.๓	บริษัทมีมาตรการด้านการรักษาความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และ อุปกรณ์อื่น ๆ ที่มีการเชื่อมต่อกับระบบเครือข่ายของบริษัท ซึ่งรวมถึง อุปกรณ์ส่วนตัว (BYOD) และ อุปกรณ์จัดเก็บแบบพกพา (Removable storage) ต่าง ๆ โดยมาตรการในที่นี้**อาจ**รวมถึง การมีแนวทางการปฏิบัติงานที่เกี่ยวข้อง และการใช้งานเครื่องมือ (Tools) เพื่อการควบคุมทางเทคนิค ที่บริษัทจะสามารถตรวจสอบการใช้งาน และ ระงับความเสียหายได้อย่างทันท่วงทีเมื่อมีเหตุการณ์ทางด้านความมั่นคงปลอดภัยเกิดขึ้น
	๒.๑.๑.๔	บริษัทจัดให้มีแนวปฏิบัติในการจัดชั้นสารสนเทศ (Information Classification) ที่เหมาะสม และกำหนดระดับการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลทุกประเภท ได้แก่ (๑) ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at Endpoint) (๒) ข้อมูลที่อยู่ระหว่างการส่งผ่านเครือข่าย (Data in Transit) (๓) ข้อมูลที่อยู่บนระบบและสื่อบันทึกข้อมูล (Data at Rest) โดยพิจารณาความเหมาะสมตามระดับชั้นความลับ รวมทั้ง ระบุอย่างชัดเจนในทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูล

ระดับการควบคุม	การควบคุม	
	๒.๑.๑.๕	บริษัทระบุทรัพย์สินสารสนเทศประเภทข้อมูล ที่เป็นข้อมูลส่วนบุคคล และ ข้อมูลส่วนบุคคลอ่อนไหว อย่างชัดเจนในทะเบียนทรัพย์สินสารสนเทศ รวมทั้ง กำหนดระดับการรักษาความมั่นคงปลอดภัยตามที่กฎหมายกำหนด
	๒.๑.๑.๖	บริษัทมีแนวทางหรือระเบียบปฏิบัติ รวมถึงการกำหนดบทบาทหน้าที่ในการบริหารจัดการทรัพย์สินสารสนเทศประเภทข้อมูลอย่างมั่นคงปลอดภัยตลอดวงจรชีวิตข้อมูล (Data Lifecycle) ตั้งแต่การสร้าง ใช้งาน ประมวลผล ส่งผ่าน จัดเก็บ และ ทำลาย โดยแนวปฏิบัตินี้มีความสอดคล้องกับระดับการรักษาความมั่นคงปลอดภัย ตามระดับชั้นความลับของข้อมูล
	๒.๑.๑.๗	บริษัทจัดทำทะเบียนการทำลายข้อมูลสำคัญ และข้อมูลส่วนบุคคลที่เหมาะสมและมั่นคงปลอดภัยตามระดับชั้นความลับ โดยระบุผู้รับผิดชอบในการทำลายข้อมูล วันที่ เวลา ชนิดของสื่อบันทึกข้อมูล Serial Number และวิธีการที่ใช้ในการทำลายข้อมูล
Intermediate	๒.๑.๑.๘	ทะเบียนทรัพย์สินสารสนเทศของบริษัทมีรายละเอียดครอบคลุมถึง (๑) เลขทะเบียนทรัพย์สินสารสนเทศ (๒) ชื่อ รายละเอียด และ ประเภทของทรัพย์สินสารสนเทศ (๓) ระดับความมั่นคงปลอดภัย (๔) ผู้เป็นเจ้าของ หรือ ผู้รับผิดชอบ (๕) ที่ตั้ง หรือ สถานที่จัดเก็บ อีกทั้ง บริษัทมีกระบวนการในการปรับปรุงทะเบียนรายการทรัพย์สินสารสนเทศให้เป็นปัจจุบันอยู่เสมอ
	๒.๑.๑.๙	บริษัทมีกระบวนการในการระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (End-of-Life) หรือสิ้นสุดการให้บริการ (End-of-Support) ได้อย่างครบถ้วน และทันท่วงที รวมทั้งกำหนดแผนการเปลี่ยนทรัพย์สิน และ/หรือ การดำเนินการเพื่อลดความเสี่ยงที่อาจเกิดขึ้นอย่างชัดเจน
	๒.๑.๑.๑๐	บริษัทมีกระบวนการติดตามและบริหารจัดการการใช้งาน Shadow IT หรือการใช้ทรัพย์สินสารสนเทศประเภทระบบ หรือ อุปกรณ์ ที่เป็นการบริหารจัดการเองโดยหน่วยงานทางธุรกิจ หรือ เป็นการใช้งานโดยไม่ได้รับอนุญาต (Shadow IT คือ การใช้ทรัพย์สินสารสนเทศประเภทระบบ หรือ อุปกรณ์ โดยหน่วยงานทางธุรกิจโดยไม่ได้รับอนุญาต ไม่ได้แจ้งให้ทางหน่วยงานสารสนเทศรับทราบ หรือ ไม่ได้นำมาบริหารจัดการแบบรวมศูนย์โดยหน่วยงานสารสนเทศ)
	๒.๑.๑.๑๑	ทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูลของบริษัทที่เป็นข้อมูลส่วนบุคคล มีการระบุรายละเอียดที่ครอบคลุมถึง (๑) ข้อมูลส่วนบุคคลที่รวบรวมไว้ (๒) ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล (๓) วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล (๔) ระยะเวลาเก็บรักษาข้อมูลส่วนบุคคล (๕) การเปิดเผยและวัตถุประสงค์ในการโอนข้อมูลส่วนบุคคล

ระดับการควบคุม	การควบคุม	
		(๖) มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล (๗) ข้อจำกัดในการเข้าถึงและสำเนาข้อมูลส่วนบุคคล (๘) ป้ายชื่อ (Labelling)
	๒.๑.๑.๑๒	บริษัทจัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อความต้องการทางธุรกิจ และ จัดเก็บในระยะเวลา (Retention Period) ขั้นต่ำเท่านั้น ในกรณีที่ต้องมีการเก็บข้อมูลส่วนบุคคลในระยะยาว จะต้องมีการพิจารณาการดำเนินการตามแนวปฏิบัติที่ดี เช่น การทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้ หรือเทคนิคเทียบเท่าอื่น ๆ
Advance	๒.๑.๑.๑๓	บริษัทมีเครื่องมือและกระบวนการที่ใช้บันทึกรายละเอียดทรัพย์สินสารสนเทศ (อาทิ รุ่น เวอร์ชัน จำนวนลิขสิทธิ์) ติดตาม (Tracking) ปรับปรุง (Updating) จัดลำดับความสำคัญ (Prioritizing) ในทะเบียนทรัพย์สินสารสนเทศ และสามารถจัดทำรายงานทรัพย์สินด้านเทคโนโลยีสารสนเทศได้ตามความต้องการใช้งาน ทั้งนี้เครื่องมือที่บริษัทใช้งานอาจอยู่ในรูปแบบของระบบงานหรือ Spreadsheet ก็ได้
	๒.๑.๑.๑๔	ในการจัดซื้อจัดจ้างทรัพย์สินด้านเทคโนโลยีสารสนเทศที่สำคัญมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารนเทศและไซเบอร์อย่างเพียงพอ

CM 2.2 การระบุและประเมินความเสี่ยงด้านไซเบอร์

ระดับการควบคุม	การควบคุม	
Baseline	๒.๒.๑.๑	บริษัทมีขอบเขตและวิธีการประเมินความเสี่ยงทางไซเบอร์ ที่สอดคล้องหรือเป็นกระบวนการเดียวกันกับการบริหารจัดการความเสี่ยงทางสารสนเทศ และ การบริหารจัดการความเสี่ยงเกี่ยวกับห่วงโซ่ของผู้ให้บริการภายนอก (Supply Chain Risk Management)
	๒.๒.๑.๒	การบริหารจัดการความเสี่ยงทางด้านสารสนเทศและไซเบอร์ของบริษัท ครอบคลุมถึง ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ต่อข้อมูลลูกค้า
Intermediate	๒.๒.๑.๓	บริษัทมีกระบวนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่สามารถระบุระบบงานด้านสารสนเทศที่สำคัญ หรือธุรกรรมที่มีความเสี่ยงสูงที่จำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศและไซเบอร์อย่างเข้มงวด
	๒.๒.๑.๔	บริษัทกำหนดให้หน่วยงานเจ้าของความเสี่ยง (Risk Owners) มีหน้าที่ติดตามภัยคุกคามใหม่ และประเมินโอกาสที่จะเกิดขึ้นเพื่อปรับปรุงแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ได้อย่างทันท่วงที
Advance	๒.๒.๑.๕	บริษัทจัดทำ Risk Metrics เพื่อแสดงถึงทรัพย์สินสารสนเทศที่มีความเสี่ยงสูง และประเมินประสิทธิภาพและความเหมาะสมของมาตรการควบคุมต่อทรัพย์สินเหล่านั้น

CM3 การป้องกันความเสี่ยง (Protection)

วัตถุประสงค์ : เพื่อให้บริษัทประกันภัยมีกระบวนการในการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์รวมไปถึงข้อมูล ส่วนบุคคลที่อาจส่งผลต่อการดำเนินธุรกิจหรือการให้บริการแก่ลูกค้า และมีกระบวนการในการป้องกันต่อการเข้าถึง รั่วไหล และใช้งานข้อมูลส่วนบุคคลอย่างปลอดภัย

CM 3.1 การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคล

ระดับการควบคุม	การควบคุม	
Baseline	๓.๑.๑.๑	บริษัทกำหนดคุณสมบัติและลักษณะงานของเจ้าหน้าที่สารสนเทศในระดับต่าง ๆ ในทุก Line of Defense รวมทั้งมีกระบวนการในการคัดเลือกบุคลากรที่จะมาปฏิบัติงานด้านสารสนเทศเพื่อให้พนักงานสารสนเทศมีความรู้ความสามารถในการปฏิบัติงาน และ มีคุณสมบัติตรงตามที่กำหนดไว้
	๓.๑.๑.๒	บริษัทกำหนดเงื่อนไขในสัญญาจ้าง หรือ กฎระเบียบข้อบังคับสำหรับพนักงาน ที่ครอบคลุมถึงการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท การใช้งานระบบสารสนเทศอย่างมั่นคงปลอดภัย และการระวังตัวจากภัยคุกคามไซเบอร์
	๓.๑.๑.๓	บริษัทสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน เพื่อให้มั่นใจถึงการจำกัดสิทธิการเข้าถึงระบบสารสนเทศ และระงับการครอบครองทรัพย์สินสารสนเทศของบริษัทอย่างทันท่วงที
	๓.๑.๑.๔	บริษัทจัดอบรมและพัฒนาทักษะ ความรู้ ด้านความเสี่ยง และการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศและไซเบอร์ ให้แก่พนักงานในทุกส่วนงาน และทุกระดับตามความเหมาะสม
	๓.๑.๑.๕	บริษัทจัดอบรมเพื่อการเสริมสร้างความตระหนัก (Awareness Program) ด้านความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และการรักษาความลับของข้อมูลส่วนบุคคล ให้แก่คณะกรรมการบริษัท ผู้บริหาร และพนักงานภายในบริษัทอย่างต่อเนื่อง รวมทั้ง มีการทดสอบความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ เช่น การทดสอบเรื่อง Social Engineering และ การทดสอบเรื่อง Phishing เป็นต้น
Intermediate	๓.๑.๑.๖	ในการคัดเลือกพนักงานด้านสารสนเทศ บริษัทจะพิจารณาคุณสมบัติและความเหมาะสมของพนักงานในด้านต่าง ๆ เช่น ประวัติการศึกษา ประสบการณ์การทำงานและประกาศนียบัตรเฉพาะด้าน ประวัติอาชญากรรม ข้อมูลเครดิตบูโร ข้อมูลการทุจริต รวมทั้งมีการสุ่มตรวจสอบ หรือ Background Check ในเรื่องดังกล่าว
	๓.๑.๑.๗	บริษัทมีแนวทางและแผนในการสรรหา ดูแลรักษา และ จัดหาทดแทนพนักงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่สำคัญอย่างชัดเจน
	๓.๑.๑.๘	บริษัทจัดให้มีการทดสอบและประเมินระดับความตระหนักของพนักงาน ที่มีต่อเหตุการณ์ทางด้านไซเบอร์ในสถานการณ์เสมือนจริง รวมทั้งมีการอบรมเพิ่มเติมรายบุคคลในกรณีที่พบบุคคลที่มีอัตราการถูกโจมตี หรือ ถูกหลอกโดย Social Engineering บ่อยครั้ง

ระดับการควบคุม	การควบคุม	
	๓.๑.๑.๙	บริษัทมีกระบวนการในการประเมินความเหมาะสมของคุณสมบัติและศักยภาพของบุคลากรที่มีหน้าที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมทั้งมีกระบวนการหรือเครื่องมือในการตรวจสอบพฤติกรรมของบุคลากรดังกล่าว เช่น (๑) มีการกำหนดคุณสมบัติและระดับความสามารถตามหน้าที่งานที่ชัดเจนเพื่อให้สามารถตรวจวัดและเปรียบเทียบความเหมาะสมได้ (๒) มีกระบวนการในการคัดกรองความรู้ความสามารถและจริยธรรมของพนักงาน หรือ (๓) มีกระบวนการในการติดตามและประเมินผลการปฏิบัติงานอย่างสม่ำเสมอ หรือ มีเครื่องมือ/กระบวนการเพื่อติดตามตรวจจับพฤติกรรมที่น่าสงสัย เป็นต้น

CM 3.2 การควบคุมการเข้าถึงระบบ ข้อมูลและทรัพย์สินสารสนเทศ

ระดับการควบคุม	การควบคุม	
Baseline	๓.๒.๑.๑	บริษัทกำหนดให้ทุกบัญชีผู้ใช้งานมีการพิสูจน์ตัวตนที่มีความซับซ้อนและเหมาะสมตามระดับความเสี่ยง (เช่น การใช้รหัสผ่าน) เพื่อการเข้าถึงระดับ Physical และ Logical ของระบบสารสนเทศ ทั้งระบบปฏิบัติการ (Operating System) ระบบงาน (Application) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) ระบบเครือข่ายสื่อสาร (Communication Network) การเข้าถึงจากระยะไกล (Remote Access) และการเข้าถึงผ่านระบบไร้สาย (Wireless Access)
	๓.๒.๑.๒	บริษัทสอบทาน และ ปรับปรุงสิทธิการเข้าถึงระบบสารสนเทศ ทั้งการเข้าถึงระดับ Physical และ Logical บนระบบปฏิบัติการ (Operating System) ระบบงาน (Application) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) ระบบเครือข่ายสื่อสาร (Communication Network) การเข้าถึงจากระยะไกล (Remote Access) และการเข้าถึงผ่านระบบไร้สาย (Wireless Access) ตามระยะเวลาที่สอดคล้องกับระดับความเสี่ยงของระบบตามที่บริษัทกำหนด อาทิ สอบทานบัญชีผู้ใช้งานที่ไม่ได้เข้าใช้ระบบเป็นระยะเวลานานทุก ๖ เดือน หรือทำการสอบทานบัญชีสิทธิสูงอย่างน้อยทุก ๓ เดือน เป็นต้น
	๓.๒.๑.๓	บริษัทกำหนดให้มีกระบวนการในการพิจาณาความเหมาะสมของสิทธิการเข้าถึงระบบสารสนเทศตามข้อกำหนดทางธุรกิจ ทั้งการเข้าถึงระดับ Physical และ Logicalบนระบบปฏิบัติการ (Operating System) ระบบงาน (Application) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) ระบบเครือข่ายสื่อสาร (Communication Network) การเข้าถึงจากระยะไกล (Remote Access) และการเข้าถึงผ่านระบบไร้สาย (Wireless Access) เมื่อมีการสร้าง หรือ เปลี่ยนแปลงแก้ไขบัญชีผู้ใช้งาน หรือสิทธิการเข้าถึง (อาทิ การอนุมัติการสร้าง หรือเปลี่ยนแปลงบัญชีผู้ใช้งานโดยผู้มีอำนาจ เป็นต้น)
	๓.๒.๑.๔	บริษัทกำหนดให้มีกระบวนการเปลี่ยนแปลง และ ยกเลิกสิทธิการเข้าถึงระบบ ทั้งการเข้าถึงระดับ Physical และ Logical บนระบบปฏิบัติการ (Operating System) ระบบงาน (Application) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) ระบบเครือข่ายสื่อสาร (Communication Network) การเข้าถึงจากระยะไกล (Remote Access) และการเข้าถึงผ่านระบบไร้สาย (Wireless Access) ของพนักงานและบุคคลภายนอก เมื่อมีการโยกย้ายหรือสิ้นสภาพการเป็นพนักงานหรือสิ้นสุดการจ้างโดยไม่ชักช้า ในกรณีของการขอเข้าใช้งานชั่วคราว ต้องมีการยกเลิกสิทธิการเข้าถึงอย่างทันท่วงทีภายหลังจากปฏิบัติงานเสร็จสิ้น
Intermediate	๓.๒.๑.๕	บริษัทกำหนดสิทธิที่เหมาะสม หรือ จัดทำตารางสิทธิมาตรฐาน (Authorization Matrix) ในการเข้าถึงระบบสารสนเทศในระดับ ระบบปฏิบัติการ (Operating System) ระบบงาน (Application) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) ระบบเครือข่ายสื่อสาร (Communication

ระดับการควบคุม	การควบคุม	
		Network) การเข้าถึงจากระยะไกล (Remote Access) และการเข้าถึงผ่านระบบไร้สาย (Wireless Access) ของพนักงานและบุคลภายนอกในแต่ละตำแหน่งหน้าที่ให้เป็นไปตามความจำเป็น (Least Privilege) และเป็นไปตามหลักการแบ่งแยกหน้าที่ที่ดี (Segregation of Duty) รวมทั้งมอบหมายสิทธิการเข้าถึงแก่ผู้ใช้งานตามตารางสิทธิมาตรฐานที่ได้จัดทำไว้ โดยตารางสิทธิมาตรฐานนี้มีการทบทวนความเหมาะสมอย่างสม่ำเสมอ
	๓.๒.๑.๖	บริษัทจัดทำมาตรฐานบัญชีผู้ใช้งานและรหัสผ่านของบริษัทที่อย่างน้อยครอบคลุมเรื่อง (๑) การกำหนดนโยบายรหัสผ่าน (Password Policy) (อาทิ อายุรหัสผ่าน ความยาวและระดับความซับซ้อนของรหัสผ่าน จำนวนครั้งสูงสุดของการใส่รหัสผ่านผิดเงื่อนไขการตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม การเปลี่ยนรหัสผ่านตั้งต้น (Default Password) หรือ รหัสผ่านมีการจัดเก็บด้วยการเข้ารหัส เป็นต้น) (๒) การจำกัดการใช้งานบัญชีผู้ใช้งานร่วมกัน (Shared User Account) (๓) การจำกัดการใช้งานบัญชีผู้ใช้งานตั้งต้น (Default Account) (๔) การแยกบัญชีผู้ใช้งานบนระบบที่ไม่ได้ใช้งานจริง (Non-Production) และระบบที่ใช้งานจริง (Production) ออกจากกัน
	๓.๒.๑.๗	บริษัทมีกระบวนการป้องกันการเปลี่ยนแปลงสิทธิของบัญชีผู้ใช้งานที่มีความเสี่ยงสูงบนระบบสารสนเทศสำคัญ อาทิ การสอบทานความเหมาะสมของบัญชีผู้ใช้งานและสิทธิที่ได้รับอย่างสม่ำเสมอกว่าบัญชีผู้ใช้งานทั่วไป และ/หรือ การสอบทานบันทึกเหตุการณ์ (Log) การเข้าถึง และกิจกรรมที่ผิดปกติ เป็นต้น
	๓.๒.๑.๘	บริษัทแยกบัญชีผู้ใช้งานที่มีสิทธิสูงออกจากบัญชีผู้ใช้งานทั่วไปอย่างชัดเจน โดยมีกระบวนการบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิสูง และมาตรฐานการพิสูจน์ตัวตนที่รัดกุม เข้มงวด และมั่นคงปลอดภัยกว่าบัญชีผู้ใช้งานปกติ
	๓.๒.๑.๙	บริษัทมีมาตรการในการบริหารจัดการบัญชีผู้ใช้งานของลูกค้าอย่างมั่นคงปลอดภัย โดยกำหนดให้มีการพิสูจน์ตัวตนอย่างเหมาะสมกับความเสี่ยงของธุรกรรมที่ทำผ่านระบบเครือข่ายอินเทอร์เน็ต มีมาตรฐานในการพิสูจน์ตัวตนอย่างเหมาะสมผ่าน Call Center หรือช่องทางการติดต่ออื่น ๆ รวมถึงมีมาตรการเพื่อรักษาความเป็นส่วนบุคคลของข้อมูลลูกค้าที่ใช้เพื่อการพิสูจน์ตัวตนดังกล่าว
	๓.๒.๑.๑๐	บริษัทมีมาตรการในการป้องกันการใช้งานอุปกรณ์ของบริษัท และ อุปกรณ์เคลื่อนที่ส่วนบุคคลของพนักงาน อาทิ เครื่องคอมพิวเตอร์พกพา โทรศัพท์มือถือ Tablet และ Handy Drive หรือ Portable Device ต่าง ๆ ที่นำมาเชื่อมต่อกับระบบสารสนเทศของบริษัท โดยคำนึงถึงการใช้งานเฉพาะผู้ได้รับอนุญาต การเชื่อมต่ออย่างมั่นคงปลอดภัย การป้องกันการรั่วไหลของข้อมูล และ การแพร่กระจายของโปรแกรมไม่ประสงค์ดีผ่านอุปกรณ์ดังกล่าว
	๓.๒.๑.๑๑	บริษัทติดตั้งอุปกรณ์ควบคุม เช่น Mobile Device Management (MDM) หรือ Mobile Application Management (MAM) บนอุปกรณ์เคลื่อนที่ส่วนบุคคลของพนักงาน อาทิ เครื่องคอมพิวเตอร์พกพา โทรศัพท์มือถือ Tablet ต่าง ๆ เพื่อให้มั่นใจว่ามีการกำหนดการตั้งค่าในระดับอุปกรณ์ และ ระดับการเข้าถึงระบบสารสนเทศของบริษัทที่มั่นคงปลอดภัย สามารถป้องกันการรั่วไหลของข้อมูลสำคัญ กำหนด Version ที่เหมาะสมของอุปกรณ์ ลบข้อมูลเมื่อเครื่องสูญหาย รวมทั้งติดตามตรวจสอบการใช้งานและการตั้งค่าได้จากส่วนกลางโดยหน่วยงานสารสนเทศ
Advance	๓.๒.๑.๑๒	บริษัทกำหนดการเชื่อมต่อของอุปกรณ์ และ อุปกรณ์เคลื่อนที่ส่วนบุคคล เพื่อเข้าถึงข้อมูลลับ ข้อมูลส่วนบุคคลอ่อนไหว และระบบสารสนเทศสำคัญ โดยให้อยู่ภายใต้สภาพแวดล้อมที่ไม่มีการเชื่อมต่อไปยังระบบเครือข่าย อินเทอร์เน็ต หรือมีมาตรการการควบคุมที่เหมาะสมรัดกุมเทียบเท่า

ระดับการควบคุม	การควบคุม	
	๓.๒.๑.๑๓	บริษัทมีการสอบสวน และลงโทษในกรณีที่ตรวจพบการเข้าถึง หรือ ความพยายามเข้าถึงระบบสารสนเทศของบริษัท หรือระบบงานสำคัญด้วยอุปกรณ์และอุปกรณ์เคลื่อนที่ส่วนบุคคลที่ไม่ได้รับอนุญาต
	๓.๒.๑.๑๔	สำหรับระบบสารสนเทศหรือบัญชีผู้ใช้งานที่มีความเสี่ยงสูง บริษัทมีระบบแจ้งเตือนแบบอัตโนมัติเมื่อมีการเปลี่ยนแปลงสิทธิของผู้ใช้งานให้ผู้ที่เกี่ยวข้องทราบ เช่น การแจ้งเตือนผ่าน Email หรือ SMS เป็นต้น

CM 3.3 การเข้ารหัสข้อมูล

ระดับการควบคุม	การควบคุม	
Baseline	๓.๓.๑.๑	บริษัทมีมาตรฐานหรือแนวปฏิบัติด้านการเข้ารหัสข้อมูล ที่ครอบคลุมถึง (๑) บทบาทหน้าที่และความรับผิดชอบ (๒) วิธีการเข้ารหัสข้อมูลที่ปลอดภัยตามมาตรฐานสากล และสอดคล้องกับระดับความสำคัญของระบบ หรือ ระดับชั้นความลับของข้อมูล รวมถึงข้อมูลที่เป็นข้อมูลส่วนบุคคล (๓) การบริหารจัดการกุญแจเข้ารหัสตลอดทั้งกระบวนการ (Key Management Lifecycle) โดยมาตรฐานหรือแนวปฏิบัติด้านการเข้ารหัสข้อมูลนี้ควรมีการพิจารณาทบทวนอย่างสม่ำเสมอ เพื่อให้มั่นใจในความแข็งแรงเพียงพอ
	๓.๓.๑.๒	บริษัทมีมาตรฐานหรือแนวปฏิบัติในการบริหารจัดการกุญแจเข้ารหัสตลอดทั้งกระบวนการ (Key Management Lifecycle) ตั้งแต่ (๑) การสร้าง หรือ คัดเลือกกุญแจเข้ารหัสที่มั่นคงปลอดภัย (๒) การติดตั้ง และจัดเก็บอย่างปลอดภัย รวมทั้ง จำกัดการเข้าถึง และ การสำรองกุญแจเข้ารหัส (๓) การเปลี่ยนแปลงเมื่อหมดอายุการใช้งาน หรือกุญแจเข้ารหัสไม่อยู่ในมาตรฐานที่มั่นคงปลอดภัยแล้ว รวมทั้งการทำลายกุญแจเข้ารหัสอย่างเหมาะสม
	๓.๓.๑.๓	บริษัทมีการเข้ารหัสข้อมูลสำคัญและข้อมูลส่วนบุคคลในขณะรับส่งผ่านเครือข่ายสาธารณะหรือเครือข่ายที่ไม่น่าเชื่อถือภายนอก
Intermediate	๓.๓.๑.๔	บริษัทมีระบบ อุปกรณ์ หรื กระบวนเพื่อใช้รักษาความปลอดภัย (อาทิ HSM: Hardware Security Module ระบบ หรือกระบวนการอื่นที่เทียบเท่า) เพื่อการรักษาความมั่นคงปลอดภัยของกุญแจเข้ารหัสที่ใช้สำหรับระบบงาน และ ระบบสารสนเทศสำคัญ หมายเหตุ - กระบวนการเพื่อใช้รักษาความปลอดภัย เช่น การจัดทำทะเบียน และกระบวนการเบิกใช้ มีการจำกัดการเข้าถึงอย่างเหมาะสม การเข้ารหัสกุญแจเข้ารหัส การแยกเก็บกุญแจเข้ารหัสออกมาเพื่อไม่ให้เก็บปะปนกับข้อมูลอื่น ๆ และผู้มีสิทธิเข้าถึงไม่ควรเป็นผู้ที่สามารถถอดรหัสกุญแจเข้ารหัสได้ เป็นต้น
	๓.๓.๑.๕	บริษัทเข้ารหัสสื่อบันทึกข้อมูลของ เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา และอุปกรณ์เคลื่อนที่ (Mobile Devices) รวมถึงสื่อบันทึกข้อมูลอื่นที่ใช้บันทึกข้อมูลที่เป็นความลับ โดยพิจารณาตามระดับความเสี่ยง หรือ ระดับความสำคัญของข้อมูล

ระดับการควบคุม	การควบคุม	
Advance	๓.๓.๑.๖	บริษัทจัดให้มีการตรวจสอบและติดตามว่าข้อมูลสำคัญ รวมทั้ง ข้อมูลในระดับชั้นความลับ หรือข้อมูลส่วนบุคคลที่มีการจัดเก็บ และ/หรือ ส่งผ่านทางช่องทางต่าง ๆ ได้รับการเข้ารหัสตามมาตรฐานของบริษัทอย่างครบถ้วนและเหมาะสม (โดยอาจพิจารณาความครบถ้วนโดยเปรียบเทียบจากทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูล และ ความเหมาะสมโดยเปรียบเทียบจากข้อกำหนดของบริษัท)

CM 3.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

ระดับการควบคุม	การควบคุม	
Baseline	๓.๔.๑.๑	บริษัทมีมาตรการควบคุมการรักษาความมั่นคงปลอดภัยทางกายภาพเพื่อป้องกันการเข้าถึงอุปกรณ์เทคโนโลยีสารสนเทศ และระบบเครือข่ายสื่อสารของบริษัท โดยไม่ได้รับอนุญาต โดยมีการกำหนดระเบียบปฏิบัติการเข้าถึงศูนย์คอมพิวเตอร์อย่างเป็นลายลักษณ์อักษร มีการควบคุมการเข้าออก และการจำกัดสิทธิอย่างเหมาะสม รวมทั้งมีการบันทึกและจัดเก็บข้อมูลการเข้าออก
	๓.๔.๑.๒	บริษัทมีการติดตั้งระบบป้องกัน และ บำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้อง ได้แก่ (๑) ระบบไฟฟ้า และ ไฟฟ้าสำรอง (๒) ระบบควบคุมอุณหภูมิ ความชื้น และ ระบบท่อน้ำเย็น (๓) ระบบป้องกัน หรือ เตือนภัยไฟไหม้ (๔) ระบบตรวจจับน้ำรั่วซึม (๕) กล้องวงจรปิด
Intermediate	๓.๔.๑.๓	บริษัทออกแบบสถานที่และการจัดวางอุปกรณ์เทคโนโลยีสารสนเทศ และระบบเครือข่ายสื่อสารของบริษัท โดยแยกตามประเภทการใช้งาน และ/หรือ ระดับความสำคัญ โดยพิจารณาให้มีการควบคุมทางด้านกายภาพที่มั่นคงปลอดภัยและสอดคล้องกับระดับความสำคัญของอุปกรณ์สารสนเทศ
	๓.๔.๑.๔	บริษัทกำหนดที่ตั้ง และ ออกแบบการพิสูจน์ตัวตนเพื่อเข้าถึงศูนย์คอมพิวเตอร์อย่างมั่นคงปลอดภัยโดยพิจารณาถึง (๑) ความเสี่ยงจากภัยธรรมชาติ (๒) ระยะห่างระหว่างศูนย์หลัก และ ศูนย์สำรอง (๓) การควบคุมพื้นที่รอบศูนย์คอมพิวเตอร์ (๔) การแจ้งเตือนให้ผู้ที่เกี่ยวข้องรับทราบ เมื่อมีเหตุขัดข้องของอุปกรณ์ หรือมีการบุกรุกพื้นที่ (๕) การเข้าถึงและพิสูจน์ตัวตนที่ซับซ้อน อาทิ MFA หรือ การจำกัดจำนวนผู้ถือกุญแจ (๖) การตรวจสอบบันทึกการเข้าถึงอย่างสม่ำเสมอ (๗) การบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้อง (MA/PM) อย่างสม่ำเสมอ

CM 3.5 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร

ระดับการควบคุม	การควบคุม	
Baseline	๓.๕.๑.๑	บริษัทมีการแบ่งระบบเครือข่าย (ทั้งมีสายและไร้สาย) สำหรับบุคคลภายนอก ออกจากระบบเครือข่ายภายในบริษัทอย่างชัดเจน โดยสำหรับระบบเครือข่ายภายในมีการแบ่งเป็นโซน (Network Segmentation) ตามระดับความสำคัญ รวมทั้ง มีการวางมาตรการการป้องกันตามระดับความสำคัญ และความเสี่ยงจากการถูกโจมตีทางไซเบอร์
	๓.๕.๑.๒	บริษัทมีอุปกรณ์ป้องกันเครือข่าย เช่น Firewall เป็นต้น ติดตั้งไว้ในจุดที่มีความเสี่ยง หรือ มีการเชื่อมต่อระหว่างเครือข่ายภายใน เครือข่าย DMZ และเครือข่ายภายนอก โดยที่บริษัทสามารถควบคุมข้อมูลจราจรคอมพิวเตอร์ (Traffic) ที่ส่งผ่าน เฝ้าระวังการบุกรุก รวมทั้งตรวจจับโปรแกรมไม่ประสงค์ดีได้
	๓.๕.๑.๓	บริษัทมีมาตรฐานและวิธีปฏิบัติในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารทั้งระหว่างบริษัท และ ภายในบริษัท โดยพิจารณาถึงการเข้าถึง การเปลี่ยนแปลงแก้ไข หรือการสร้างความเสียหายแก่ข้อมูลโดยไม่ได้รับอนุญาต การป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี และการตรวจสอบผู้ใช้งานเฉพาะที่ได้รับอนุญาตเท่านั้น
Intermediate	๓.๕.๑.๔	บริษัทมีกระบวนการบริหารจัดการการตั้งค่าในอุปกรณ์เครือข่ายที่สำคัญ โดยจัดทำเอกสารการตั้งค่ามาตรฐาน (Security Baseline) สำหรับอุปกรณ์เครือข่ายที่สำคัญ รวมทั้งกำหนดให้มีการตรวจสอบความถูกต้องของการตั้งค่าอุปกรณ์ป้องกันเครือข่าย เช่น Firewall Rules ตามรอบระยะเวลาที่เหมาะสมกับความสำคัญของอุปกรณ์ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
	๓.๕.๑.๕	บริษัทติดตั้งอุปกรณ์ในการตรวจจับและปิดกั้นการโจมตีหรือการบุกรุกโดยไม่ได้รับอนุญาต เช่น Intrusion Detection หรือ Prevention System (IDS/IPS) รวมทั้ง มีมาตรการเพื่อป้องกันและลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ ที่ก่อให้เกิดการหยุดชะงักในการให้บริการของระบบงานที่สำคัญ เช่น DDoS เป็นต้น
	๓.๕.๑.๖	บริษัทมีมาตรการเชิงเทคนิคหรือเครื่องมือเพื่อใช้ป้องกันการเชื่อมต่อและ/หรือการเข้าถึงระบบเครือข่ายภายในของบริษัท โดยอุปกรณ์หรือการเชื่อมต่อ (Traffic) ที่ไม่ได้รับอนุญาต
	๓.๕.๑.๗	บริษัทออกแบบระบบเครือข่ายและมีการตั้งค่าอุปกรณ์ให้สามารถจำกัดและติดตามการรับส่งข้อมูลระหว่าง Trusted และ Untrusted Zone ได้
	๓.๕.๑.๘	บริษัทมีการตั้งค่าการเข้าถึงจากระยะไกล (Remote Access) ให้สามารถติดตามตรวจจับการเชื่อมต่อและการเข้าถึงได้ โดยกำหนดมาตรการควบคุม Session สอบทานการเข้าถึงของผู้ใช้งาน และมีกลไกการตัดการเชื่อมต่อหรือระงับสิทธิการเข้าถึงอย่างทันท่วงทีเมื่อพบความผิดปกติ
	๓.๕.๑.๙	บริษัทติดตั้งเครื่องมือ และ/หรือ กระบวนการควบคุมการรั่วไหลของข้อมูล (เช่น DLP) เพื่อป้องกัน (Block) การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลส่วนบุคคลไปยังภายนอกองค์กร
Advance	๓.๕.๑.๑๐	บริษัทมีกระบวนการและเครื่องมือเพื่อป้องกันการเข้าถึงจากอุปกรณ์คอมพิวเตอร์ที่ไม่ได้ Patch ของพนักงานและของบุคคลภายนอก
	๓.๕.๑.๑๑	บริษัทมีการติดตามตรวจสอบการเชื่อมต่อระยะไกลอย่างมีประสิทธิภาพ โดย (๑) จำกัดการใช้ชุดคำสั่งพิเศษ (Privileged Commands) เฉพาะผู้ที่มีความจำเป็นเท่านั้น (๒) ตรวจสอบและระงับการเชื่อมต่อระยะไกลทันทีเมื่อพบความผิดปกติ (๓) สอบทานหลักฐานการขอใช้งานการเชื่อมต่อระยะไกลอย่างสม่ำเสมอ

CM 3.6 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
๓.๖.๑ การบริหารจัดการการเปลี่ยนแปลง		
Baseline	๓.๖.๑.๑	บริษัทจัดให้มีกระบวนการในการเปลี่ยนแปลงระบบสารสนเทศ โดยให้มีการอนุมัติการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร
	๓.๖.๑.๒	บริษัทมีการทดสอบการเปลี่ยนแปลงแก้ไขระบบสารสนเทศจนกระทั่งมั่นใจถึงความถูกต้องครบถ้วนในการประมวลผลก่อนนำโปรแกรมขึ้นใช้งานจริง (Migration) โดยในกรณีที่มีความจำเป็นในการดำเนินการเปลี่ยนแปลงแก้ไขบนระบบงานจริง เจ้าหน้าที่ผู้เชี่ยวชาญได้พิจารณาผลกระทบที่อาจเกิดขึ้นอย่างเหมาะสมแล้ว
Intermediate	๓.๖.๑.๓	บริษัทมีการพิจารณาความเสี่ยง ผลกระทบ หรือความต้องการทางด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่เกี่ยวข้องในการแก้ไขเปลี่ยนแปลงก่อนดำเนินการ รวมทั้งพิจารณาการแก้ไขเปลี่ยนแปลงให้สอดคล้องกับความต้องการทางด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ดังกล่าว
Advance	๓.๖.๑.๔	บริษัทมีเครื่องมือหรือระบบเพื่อประเมินความเสี่ยงและผลกระทบของทรัพย์สินสารสนเทศที่เกี่ยวข้องและอาจได้รับผลกระทบจากการเปลี่ยนแปลง (เช่น บริษัทอาจมีระบบ CMDB (Configuration Management Database) FIM (File Integrity Monitoring) หรือทะเบียนทรัพย์สินสารสนเทศที่มีรายละเอียดข้อมูลครบถ้วน เพื่อสามารถพิจารณาการเชื่อมต่อหรือผลกระทบจากการเปลี่ยนแปลงได้อย่างครอบคลุม)
	๓.๖.๑.๕	บริษัทมีเครื่องมือที่จะแจ้งเตือนแก่ผู้ที่เกี่ยวข้องเมื่อเกิดการเปลี่ยนแปลงแก้ไขในระบบสารสนเทศที่สำคัญโดยไม่ได้รับอนุญาต อีกทั้ง บริษัทมีกระบวนการในการติดตามและตรวจสอบการแก้ไขที่ไม่ได้รับอนุญาตนี้ (เช่น FIM: File Integrity Monitoring หรือ ระบบที่ช่วยวิเคราะห์ Log และ Alert เมื่อมีการเปลี่ยนแปลงที่กำหนดไว้)
๓.๖.๒ การบริหารจัดการขีดความสามารถของระบบ		
Baseline	๓.๖.๒.๑	บริษัทมีกระบวนการหรืออุปกรณ์เพื่อการเก็บข้อมูลขีดความสามารถของระบบสารสนเทศที่สำคัญ จากนั้นมีการติดตามสถานะข้อมูลขีดความสามารถของระบบสารสนเทศที่สำคัญอย่างสม่ำเสมอ โดยในกรณีที่พบปัญหาหรือแนวโน้มปัญหาทางด้านขีดความสามารถของระบบสารสนเทศดังกล่าว บริษัทมีแผนการบริหารจัดการที่สามารถแก้ไขปัญหาดังกล่าวได้
Intermediate	๓.๖.๒.๒	บริษัทมีการวางแผนการเกี่ยวกับขีดความสามารถของระบบสารสนเทศที่สำคัญ และ ระบบสาธารณูปโภค ตั้งแต่เริ่มต้นการพัฒนาระบบงาน และมีการประมาณการล่วงหน้าอย่างสม่ำเสมอ โดยมีการจัดหาและเตรียมการระบบสารสนเทศ รวมถึงระบบสารสนเทศพื้นฐานที่เกี่ยวข้อง ให้สามารถรองรับขีดความสามารถของระบบสารสนเทศที่สำคัญได้ตามแผนที่บริษัทตั้งเป้าหมายไว้
๓.๖.๓ การรักษาความมั่นคงปลอดภัยเครื่องแม่ข่าย		
Baseline	๓.๖.๓.๑	บริษัทมีมาตรฐานในการบริหารจัดการความมั่นคงปลอดภัยของเครื่องแม่ข่าย โดยกำหนดให้มีอุปกรณ์ หรือ การบริหารจัดการเรื่อง (๑) การบริหารจัดการการตั้งค่าระบบ (System Configuration Management) อาทิ Password, Ports, Functions, Protocols หรือ Services (๒) การบริหารจัดการ Patch (๓) การบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิสูง

ระดับการควบคุม	การควบคุม	
		(๔) การติดตั้ง และ บริหารจัดการ Antivirus / Antimalware (๕) การป้องกันการติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต
Intermediate	๓.๖.๓.๒	บริษัทมีกระบวนการในการติดตามความครบถ้วนในการติดตั้งโปรแกรม Antivirus / Antimalware ทั้งในเครื่องแม่ข่าย และ เครื่องคอมพิวเตอร์ ของทุกผลิตภัณฑ์ (Windows และ ผลิตภัณฑ์อื่น ๆ) ว่าทุกเครื่องแม่ข่าย หรือ เครื่องคอมพิวเตอร์ได้รับการติดตั้งโปรแกรม Antivirus / Antimalware อย่างครบถ้วน และ Virus / malware Pattern ได้รับการปรับปรุงให้มีความทันสมัย
	๓.๖.๓.๓	บริษัทจัดทำเอกสารการตั้งค่ามาตรฐาน (Security Baseline) สำหรับเครื่องแม่ข่าย เครื่องคอมพิวเตอร์ หรือ ระบบสารสนเทศที่เกี่ยวข้องอื่น ๆ ที่นำมาเชื่อมต่อหรือใช้งานกับระบบงานสำคัญ รวมทั้งมีการตรวจสอบการตั้งค่าในปัจจุบันโดยเปรียบเทียบกับเอกสารการตั้งค่ามาตรฐานอย่างสม่ำเสมอตามรอบระยะเวลาที่เหมาะสมหรือตามแผนการดำเนินงานของบริษัท (รอบระยะเวลาที่เหมาะสมอาจพิจารณาตามความสำคัญของระบบหรืออุปกรณ์)
	๓.๖.๓.๔	บริษัทมีกระบวนการในการบริหารจัดการและติดตั้ง Patch โดยครอบคลุม (๑) การติดตามข่าวสารการปรับปรุง Patch Version จากบริษัทผู้ผลิตอย่างสม่ำเสมอ (๒) มาตรฐานหรือความถี่ในการปรับปรุง Patch ที่เหมาะสมกับระดับความเสี่ยง (๓) การทดสอบหรือพิจารณาผลกระทบอย่างรอบคอบก่อนการติดตั้ง (๔) การพิจารณาความเสี่ยง และการดำเนินการควบคุมทดแทนกรณีไม่สามารถติดตั้ง Patch ได้ตามระยะเวลาที่เหมาะสม
	๓.๖.๓.๕	บริษัทมีกระบวนการหรือเครื่องมือเพื่อใช้ในการระบุ จัดลำดับความสำคัญ และติดตาม Patch ด้านการรักษาความปลอดภัยที่ยังไม่มีการติดตั้ง รวมถึงการไม่สามารถติดตั้ง Patch ได้เนื่องจากระบบ End-of-Life / End- of Support โดยบริษัทมีมาตรการควบคุมความเสี่ยงอย่างรัดกุมในส่วนที่ยังไม่ได้ติดตั้ง Patch
	๓.๖.๓.๖	บริษัทมีมาตรฐานความมั่นคงปลอดภัยในการใช้เทคโนโลยี Virtualization ที่เทียบเท่าระดับความปลอดภัยของเครื่องแม่ข่ายของบริษัท โดยพิจารณาถึงการสร้าง การตั้งค่าการจัดเก็บ การใช้งาน การยกเลิกการใช้งาน และการทำลาย Virtual Machine Images หรือ Snapshot
	๓.๖.๓.๗	บริษัทมีมาตรการในการป้องกันการแก้ไขเปลี่ยนแปลงการติดตั้งอุปกรณ์เพื่อรักษาความปลอดภัย และ การตั้งค่ามาตรฐานบนเครื่องแม่ข่าย และเครื่องคอมพิวเตอร์ (เช่น การระงับสิทธิ Local Admin เป็นต้น) หรือ มาตรการในการตรวจสอบให้มีการติดตั้งอุปกรณ์เพื่อรักษาความปลอดภัยและมีการตั้งค่าอย่างเหมาะสมอยู่ตลอดเวลา
Advance	๓.๖.๓.๘	บริษัทติดตั้งโปรแกรมหรืออุปกรณ์เพื่อความปลอดภัยของเครื่องแม่ข่าย เครื่องคอมพิวเตอร์ หรือ อุปกรณ์เคลื่อนที่อื่น ๆ ที่นำมาเชื่อมต่อกับระบบสารสนเทศของบริษัท อาทิ (๑) Harddisk Encryption (๒) DLP Agent (๓) CASB Agent (ถ้ามีการใช้งานระบบคลาวด์) (๔) MDM หรือ MAM (ถ้ามีการใช้งานอุปกรณ์เคลื่อนที่)

ระดับการควบคุม	การควบคุม	
		รวมทั้งมีการตั้งค่า Configuration เพื่อรักษาความมั่นคงปลอดภัย และตรวจจับรายการผิดปกติที่เหมาะสม โดยมีเจ้าหน้าที่ผู้เชี่ยวชาญติดตามการใช้งานและการแจ้งเตือนต่าง ๆ อย่างสม่ำเสมอ รวมทั้งดำเนินการแก้ไขโดยไม่ชักช้าเมื่อพบเหตุการณ์ผิดปกติ
	๓.๖.๓.๙	บริษัทติดตั้ง Patch Monitoring Software ที่ใช้ติดตาม Patch ด้านการรักษาความปลอดภัยที่ยังไม่มีการติดตั้ง และ/หรือ มีเครื่องมือที่สามารถจัดลำดับความสำคัญของการติดตั้ง Patch โดยให้คำนึงถึงระดับความรุนแรงของช่องโหว่ ระดับความสำคัญของระบบงาน และเชื่อมโยงจากแหล่งข้อมูลจาก Threat Intelligence (Threat Intelligence คือ หน่วยงานภายในหรือภายนอกองค์กรที่เผยแพร่ข้อมูลข่าวสาร ผลการวิเคราะห์ วิธีการหรือรูปแบบ รวมทั้งข้อเสนอแนะในการลดและควบคุมความเสี่ยงจากภัยคุกคามทางด้านสารสนเทศและไซเบอร์ เช่น Thai CERT, Ti-CERT, ETDA หรือ TB-CERT เป็นต้น)

CM 3.7 การจัดหาและพัฒนาระบบ

ระดับการควบคุม	การควบคุม	
Baseline	๓.๗.๑.๑	บริษัทมีหลักเกณฑ์ในการประเมินและคัดเลือกผู้ขาย หรือผู้รับจ้างพัฒนาระบบที่ชัดเจน และครอบคลุมเรื่อง (๑) ความน่าเชื่อถือของระบบ และผู้ให้บริการ (๒) การรับรองมาตรฐานทางด้านความมั่นคงปลอดภัย (๓) บริการ หรือ การสนับสนุนการดำเนินงานภายหลังการขาย (๔) ความมั่นคงปลอดภัยของระบบ (๕) ผลการจัดทำ Proof of Concept (POC) สำหรับระบบสำคัญ (๖) ลิขสิทธิ์ และการใช้งาน
	๓.๗.๑.๒	บริษัทคำนึงถึงความต้องการทางด้านความมั่นคงปลอดภัยสารสนเทศในการพัฒนาระบบงาน โดยมีการระบุอย่างชัดเจนในเอกสารความต้องการของระบบงาน และ กำหนดเป็นหัวข้อหรือเงื่อนไขในการทดสอบระบบสารสนเทศก่อนนำมาใช้ ทั้งนี้เอกสารความต้องการของระบบงานได้รับการพิจารณาอนุมัติจากทุกฝ่ายที่เกี่ยวข้อง รวมถึง (๑) ส่วนงาน IT Security เพื่อพิจารณาด้านการรักษาความปลอดภัยของระบบ และ (๒) ส่วนงานกฎหมาย หรือ DPO เพื่อพิจารณาด้านการบริหารจัดการข้อมูลส่วนบุคคล
	๓.๗.๑.๓	บริษัทมีกระบวนการหรือเครื่องมือในการควบคุม Version ของ Source Code (Source Code Version Control) รวมถึงเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (Non-production) ให้มีความปลอดภัยตามระดับความเสี่ยงเพื่อป้องกันการเข้าถึงและแก้ไข Source Code โดยไม่ได้รับอนุญาต
	๓.๗.๑.๔	บริษัทแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (Development) และการทดสอบ (Testing) ออกจากระบบงานที่ให้บริการจริง (Production) ทั้งนี้อาจเป็นการแบ่งแยกแบบ Physical หรือ Logical ก็ได้ นอกจากนี้ บริษัทควบคุมสภาพแวดล้อมของระบบงานอย่างรัดกุม โดย (๑) สภาพแวดล้อมของระบบงานที่ให้บริการจริง (Production): ไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (Development Tools) และเครื่องมือแปลโปรแกรม (Compilers)

ระดับการควบคุม	การควบคุม	
		(๒) สภาพแวดล้อมของระบบงานที่ใช้สำหรับการทดสอบ (Testing): มีสภาพเหมือน หรือใกล้เคียงกับระบบงานที่ให้บริการจริงเพื่อความเชื่อถือได้ของการทดสอบระบบ รวมทั้งในกรณีที่มีการนำข้อมูลสำคัญหรือข้อมูลส่วนบุคคลมาใช้ในการทดสอบ จะต้องมีการรักษาความปลอดภัยเสมือนเป็นระบบงานจริง หรือ มีการ Masking ข้อมูลทุกครั้ง
	๓.๗.๑.๕	บริษัทมีการแบ่งแยกหน้าที่ระหว่าง (๑) นักพัฒนาระบบ (Developer) ที่สามารถเข้าถึง Source Code เพื่อการพัฒนาปรับแต่งระบบ และ (๒) เจ้าหน้าที่ผู้ดูแลระบบที่ได้รับสิทธิในการดูแลระบบ (System Administrator) และสามารถนำโปรแกรมขึ้นใช้งานจริง (Migration) โดยจะต้องกำหนดสิทธิในระบบสารสนเทศให้ตรงตามหน้าที่ และไม่มีเจ้าหน้าที่ท่านใดที่มีสิทธิในระบบสารสนเทศในการปฏิบัติหน้าที่ทั้งสองหน้าที่ร่วมกัน ในกรณีที่นักพัฒนาระบบมีความจำเป็นต้องนำโปรแกรมขึ้นใช้งานจริง ให้มีการจัดเก็บบันทึกเหตุการณ์และสอบทานอย่างรัดกุมโดยผู้สอบทานที่เป็นอิสระ
	๓.๗.๑.๖	บริษัทกำหนดแผนการทดสอบ และ ดำเนินการทดสอบระบบสำคัญที่จัดหาและพัฒนาขึ้นโดยพิจารณาจากทุกมุมมองทั้ง (๑) ทางด้านการใช้งาน (Functionality) อาทิ Unit Test, Integration Test, User Acceptance Test (๒) ทางด้านความมั่นคงปลอดภัย (Security) อาทิ Security Test, Pentest (๓) ทางด้านความสามารถในการประมวลผล (Availability) อาทิ Stress Test, Performance Test สำหรับระบบที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ (๔) ทางด้านการปฏิบัติตามกฎหมาย เช่น PDPA โดย Test Case และ Test Script ที่ใช้ในการทดสอบ ต้องครอบคลุมตามความต้องการทางธุรกิจ (Business Requirements) เป็นขั้นต่ำ
	๓.๗.๑.๗	บริษัทกำหนดให้มีการลงนามอนุมัติจากผู้มีอำนาจหน้าที่ก่อนการนำระบบขึ้นใช้งานจริง ซึ่งอย่างน้อยระบบจะต้องผ่านการทดสอบจากฝ่ายงานที่เกี่ยวข้องอย่างครบถ้วน
	๓.๗.๑.๘	เมื่อมีระบบใหม่ หรือ มีการเปลี่ยนแปลงที่สำคัญ บริษัทจัดทำคู่มือระบบ ทั้งคู่มือการใช้งาน (System Manual) และ เอกสารทางเทคนิค (Technical Document) รวมทั้ง จัดการอบรมการใช้งานระบบแก่ผู้ใช้งาน และ จัดการอบรมการดูแลระบบแก่เจ้าหน้าที่สารสนเทศผู้ดูแลระบบ
	๓.๗.๑.๙	ในกรณีที่บริษัทใช้กระบวนการพัฒนาระบบแบบ Agile บริษัทควรมีการกำหนดกระบวนการที่ชัดเจน รวมทั้ง ตั้งค่าในระบบ Workflow ให้เป็นไปตามกระบวนการที่กำหนด โดยพิจารณาถึงวัตถุประสงค์ในการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัยและเชื่อถือได้ตามกระบวนการปกติ (เช่น การพัฒนาแบบ DevSecOps เป็นต้น)
Intermediate	๓.๗.๑.๑๐	บริษัทมีมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบ ที่ครอบคลุมถึงการพัฒนาระบบอย่างปลอดภัย (Secure Coding) และการสอบทานความปลอดภัยของการพัฒนาระบบ (Secure Code Review) ที่นักพัฒนาระบบปฏิบัติตาม รวมทั้งในกรณีของการจ้างพัฒนาผู้รับจ้างก็ต้องปฏิบัติตามเช่นกัน
	๓.๗.๑.๑๑	บริษัทมีกระบวนการประเมินความจำเป็นในการจัดทำสัญญาและข้อตกลงการรับฝากทรัพย์สิน (Escrow Agreement) ซึ่งรวมถึง Source Code ในระบบงานสำคัญ

ระดับการควบคุม	การควบคุม	
	๓.๗.๑.๑๒	ในกรณีที่เป็นการพัฒนาระบบใหม่ หรือ การเปลี่ยนแปลงที่สำคัญ (๑) บริษัทมีการทดสอบ Vulnerabilities Assessment สำหรับระบบสำคัญ (๒) บริษัทมีการทดสอบการเจาะระบบ (Pentest) สำหรับระบบงานที่มีการเชื่อมต่อกับอินเทอร์เน็ต (๓) บริษัทมีการทดสอบประสิทธิภาพ (Performance Test) สำหรับระบบที่ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ หรือ เชื่อมโยงกับระบบอื่นจำนวนมาก ทั้งนี้ ข้อตรวจพบและช่องโหว่จากการทดสอบข้างต้นได้รับการแก้ไขก่อนการใช้งานระบบจริง
Advance	๓.๗.๑.๑๓	สำหรับโปรแกรมหรือระบบที่มีการเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต หรือ มีการเชื่อมต่อกับระบบภายนอกผ่านเทคโนโลยี API บริษัทมีการทดสอบความเชื่อมโยงของระบบดังกล่าวอย่างรัดกุมก่อนการใช้งานจริง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงสำคัญ

CM 3.8 การป้องกันความเสี่ยงด้านไซเบอร์

ระดับการควบคุม	การควบคุม	
Baseline	๓.๘.๑.๑	บริษัทกำหนดแนวทางในการรวบรวมและวิเคราะห์ข้อมูลภัยคุกคามไซเบอร์ และกำหนดวิธีการรวมทั้งช่องทางในการแลกเปลี่ยนข้อมูล เพื่อการบริหารจัดการ และรับมือภัยคุกคามทางไซเบอร์ทั้งภายในและภายนอกองค์กร
Intermediate	๓.๘.๑.๒	บริษัทเป็นสมาชิกกลุ่มหรือสมาคมที่แบ่งปันข้อมูลภัยคุกคามไซเบอร์ โดยบริษัทมีการกำหนดแนวทางในการดำเนินงานเพื่อตอบสนองต่อข้อมูลภัยคุกคามใหม่ ๆ ที่ได้รับ เพื่อป้องกันเหตุการณ์ภัยคุกคามที่อาจเกิดขึ้น
Advance	๓.๘.๑.๓	บริษัทเป็นผู้ที่มีบทบาทในการชี้แนะ แนะนำ นำเสนอ แบ่งปันข่าวสารข้อมูลภัยคุกคามไซเบอร์ให้แก่กลุ่มหรือสมาคมที่ให้ข้อมูลภัยคุกคามไซเบอร์ หรือ บริษัทอื่น ๆ ในกลุ่มอุตสาหกรรม

CM4 การตรวจสอบและเฝ้าระวัง (Detection)

วัตถุประสงค์ : เพื่อให้บริษัทประกันภัยมีมาตรการที่สามารถระบุหรือตรวจพบช่องโหว่หรือภัยคุกคามด้านเทคโนโลยีสารสนเทศ ไซเบอร์ และ ข้อมูลส่วนบุคคลที่เกิดขึ้นหรืออาจเกิดขึ้น และมีกระบวนการที่สามารถรองรับสถานการณ์เหล่านั้นได้อย่างเหมาะสมทันท่วงที

CM 4.1 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
๔.๑.๑ การจัดเก็บข้อมูลบันทึกเหตุการณ์		
Baseline	๔.๑.๑.๑	บริษัทมีมาตรการในการจัดเก็บข้อมูลบันทึกการเข้าถึงระบบ (Access Log) และบันทึกการดำเนินงาน (Activity Log) ของ ระบบงาน ระบบฐานข้อมูล เครื่องแม่ข่าย และอุปกรณ์เครือข่ายที่สำคัญ ไว้ย้อนหลังอย่างน้อย ๙๐ วัน หรือตามกฎหมายที่เกี่ยวข้องได้กำหนดไว้ โดยมีรายละเอียดที่เพียงพอเพื่อสามารถใช้เป็นหลักฐานในการตรวจสอบและระบุตัวผู้กระทำได้ เช่น บัญชีผู้ใช้งาน วันเวลาที่เข้าใช้งาน/วันเวลาที่มีการใช้งาน ความพยายามในการเข้าใช้งาน หมายเลขประจำเครื่องที่ใช้งาน (IP Address) ที่อยู่ของเว็บไซต์ (URL) และบันทึกการเรียกดูแลหรือการแก้ไขข้อมูล เป็นต้น
	๔.๑.๑.๒	บริษัทมีการสอบทาน Access Log และ Activity Log อย่างสม่ำเสมอ เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูล เช่น การสอบทาน System Administrator Log เพื่อให้มั่นใจได้ว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมายเท่านั้น หรือ การสอบทานบันทึกการเข้าถึงและเปลี่ยนแปลงข้อมูลสำคัญ เป็นต้น
	๔.๑.๑.๓	ข้อมูลบันทึกเหตุการณ์ ถูกจัดเก็บไว้ที่เครื่องแม่ข่ายหรือระบบที่แยกเฉพาะ และมีการควบคุมการเข้าถึง เพื่อป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ
	๔.๑.๑.๔	บริษัทมีการใช้ระบบในการควบคุมค่าเวลา (Clock Synchronization) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสาร ให้ตรงกับเครื่องเซิร์ฟเวอร์ Network Time Protocol: NTP เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์ (Log) จากทุกแหล่งที่มามีความถูกต้องตรงกัน ซึ่งเครื่องเซิร์ฟเวอร์ NTP ต้องเทียบเวลาจากแหล่งที่มาที่มีความน่าเชื่อถือ
Intermediate	๔.๑.๑.๕	บริษัทมีเครื่องมือ กระบวนการ หรือ จัดจ้างผู้ให้บริการสำหรับตรวจจับเหตุการณ์ผิดปกติที่เกิดขึ้นกับระบบ และแจ้งเตือนไปยังผู้ที่รับผิดชอบเมื่อมีเหตุการณ์น่าสงสัย หรือ เมื่อถึง Thresholds ที่กำหนดไว้ เพื่อดำเนินการแก้ไขอย่างทันท่วงที (อาทิ การเข้าถึงโดยไม่ได้รับอนุญาตหรือมีการพยายามเข้าถึงอย่างผิดปกติ การขโมยข้อมูล เป็นต้น)
	๔.๑.๑.๖	ในกรณีที่ข้อมูลใน Log ประกอบไปด้วยข้อมูลส่วนบุคคล บริษัทได้พิจารณาถึงความเหมาะสม และ การจัดเก็บ Log ดังกล่าวเท่าที่จำเป็นตามข้อกำหนดทางกฎหมาย นอกจากนี้ ในกรณีที่ต้องมีการจัดเก็บเป็นเวลานาน บริษัทเพิ่มความปลอดภัยด้วยการเปลี่ยนแปลงข้อมูลส่วนบุคคลให้ไม่สามารถระบุตัวตนได้ เช่น Masking หรือ Blinding

ระดับการควบคุม	การควบคุม	
	๔.๑.๑.๗	บริษัทมีมาตรการควบคุมเชิงเทคนิคที่ใช้ Defense-in-Depth ในการตรวจจับและรับมือการโจมตีระบบเครือข่ายที่อาจมีรูปแบบของการรับส่งข้อมูลเข้าออกที่ผิดปกติ และ/หรือการโจมตีแบบ DDoS ได้อย่างทันกาล
Advance	๔.๑.๑.๘	บริษัทติดตั้งเครื่องมือตรวจจับภัยคุกคาม (SIEM) หรือ จัดจ้างผู้ให้บริการ Security Operation Center (SOC) เพื่อให้นำข้อมูลบันทึกเหตุการณ์ (Log) และการแจ้งเตือน (Alert) จากอุปกรณ์คอมพิวเตอร์และอุปกรณ์ด้านความมั่นคงปลอดภัยต่าง ๆ มาประมวลผลเชื่อมโยง (Correlation) เพื่อตรวจจับและป้องกันการโจมตีในลักษณะต่าง ๆ
๔.๑.๒ การติดตามดูแลระบบเฝ้าระวังภัยคุกคาม		
Baseline	๔.๑.๒.๑	บริษัทดำเนินการ Vulnerabilities Assessment ที่ครอบคลุมระบบงานสำคัญอย่างสม่ำเสมอตามระดับความเสี่ยง โดยดำเนินงานอย่างน้อยปีละ ๑ ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมทั้งรายงานไปยังผู้ที่รับผิดชอบ เพื่อดำเนินการแก้ไขหรือปิดช่องโหว่อย่างเหมาะสม
	๔.๑.๒.๒	บริษัททำการทดสอบการเจาะระบบ (Penetration Testing) ที่ครอบคลุมระบบงานสำคัญที่เชื่อมต่อกับภายนอก หรือ เชื่อมต่อกับอินเทอร์เน็ตอย่างน้อยปีละ ๑ ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ รวมทั้ง รายงานผลการทดสอบไปยังผู้ที่รับผิดชอบ เพื่อดำเนินการแก้ไขหรือปิดช่องโหว่อย่างเหมาะสม ทันท่วงที นอกจากนี้ บริษัทได้จัดเก็บรวบรวมข้อมูลผลการทดสอบเจาะระบบ เพื่อวิเคราะห์ช่องโหว่ทางด้านเทคนิคที่ตรวจพบ และใช้ประกอบการพิจารณากำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบงานที่บริษัทจะพัฒนาต่อไปในอนาคต
Intermediate	๔.๑.๒.๓	บริษัทกำหนดให้หน่วยงานอิสระ เช่น หน่วยงานตรวจสอบภายใน หรือหน่วยงานบริหารความเสี่ยง มีส่วนร่วมในการประเมินความเหมาะสมของขอบเขต กระบวนการดำเนินงาน คุณภาพผู้ทดสอบ และผลการทดสอบการเจาะระบบ (Penetration Testing) รวมทั้ง ติดตามดูแลให้มีการแก้ไขช่องโหว่ที่พบภายในกรอบเวลาที่กำหนด
Advance	๔.๑.๒.๔	บริษัทมีกระบวนการทดสอบเจาะระบบในลักษณะ Red Team ที่ครอบคลุมการบริหารจัดการ กระบวนการป้องกัน ตรวจจับ รับมือ กู้คืน รวมถึงรวมข้อมูลการรายงานเหตุการณ์จากการถูกโจมตีหรือภัยคุกคามทางไซเบอร์ จาก Cyber Threat Intelligence มาออกแบบสถานการณ์จำลองให้อยู่ในรูปแบบเสมือนจริง (Simulation Cyber Attack) และมีการทดสอบเจาะระบบโดยไม่มีการแจ้งเตือนหน่วยงานเฝ้าระวังการรักษาความมั่นคงปลอดภัยล่วงหน้า (Silent Mode) เพื่อให้มั่นใจได้ว่าบริษัทสามารถรับมือเมื่อมีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้นจริง
	๔.๑.๒.๕	บริษัทมีกระบวนการตรวจหา (Scan) และวิเคราะห์ช่องโหว่และพฤติกรรมการทำงานที่ผิดปกติของอุปกรณ์ Endpoint (เช่น EDR Solution เป็นต้น) และระบบงานที่สำคัญตามระดับความเสี่ยง เพื่อให้ได้รับทราบถึงช่องโหว่ด้านการรักษาความปลอดภัยของอุปกรณ์ได้อย่างทันการณ์

CM 4.2 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

ระดับการควบคุม	การควบคุม	
Baseline	๔.๒.๑.๑	บริษัทมีมาตรฐาน กระบวนการ และช่องทางในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม รวมทั้ง รายงานช่องโหว่ จุดอ่อน เหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ทั้งสำหรับหน่วยงานภายใน และ ภายนอก

ระดับการควบคุม	การควบคุม	
	๔.๒.๑.๒	บริษัทกำหนดบทบาทและหน้าที่ความรับผิดชอบของทั้งหน่วยงานภายในและภายนอก ที่เกี่ยวข้องกับการติดตาม ดูแล เฝ้าระวัง วิเคราะห์ ประสานงาน และเป็นศูนย์กลางในการรับแจ้ง และจัดการเหตุการณ์ผิดปกติทางไซเบอร์ รวมถึงรายงานการถูกคุกคามทางไซเบอร์และกิจกรรมต้องสงสัย
	๔.๒.๑.๓	บริษัทมีเครื่องมือ กระบวนการ เกี่ยวกับการตรวจจับเหตุการณ์ผิดปกติ (Incident) ที่กระทบต่อความมั่นคงปลอดภัยของระบบงานและระบบเครือข่ายสื่อสารที่สำคัญ รวมทั้งการแจ้งเตือนเมื่อพบเหตุการณ์ที่มีโอกาสเป็นการโจมตีทางไซเบอร์ เพื่อการรายงานไปยังผู้ที่เกี่ยวข้อง และ การรับมือได้อย่างทันเวลา
	๔.๒.๑.๔	บริษัทมีกระบวนการ หรือมาตรการ เกี่ยวกับการค้นหา หรือรับข้อมูลภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น และ วิธีการรับมือหรือป้องกัน จากแหล่งข้อมูลที่เชื่อถือได้ อาทิ เป็นสมาชิกหรือใช้บริการหน่วยงานที่ให้บริการ Cyber Threat Intelligence ซึ่งให้ข้อมูลข่าวสาร ผลการวิเคราะห์ วิธีการ รูปแบบ และข้อเสนอแนะในการลดและควบคุมความเสี่ยงจากภัยคุกคามทางไซเบอร์
	๔.๒.๑.๕	บริษัทมีกระบวนการในการตรวจจับเหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยพิจารณาถึงการแจ้งเตือนไปยังผู้ที่เกี่ยวข้อง
Intermediate	๔.๒.๑.๖	บริษัทมีศูนย์ประสานงานและการรับมือเหตุภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Computer Security Incident Response Team: CSIRT) หรือหน่วยงานที่เทียบเท่า ที่รับผิดชอบในการเฝ้าระวัง ติดตาม วิเคราะห์ ประสานงาน และเป็นศูนย์กลางในการจัดการเหตุการณ์ผิดปกติทางไซเบอร์
	๔.๒.๑.๗	บริษัทสื่อสารข้อมูลด้าน Cyber Threat Intelligence ที่สำคัญ หรือ อาจส่งผลกระทบต่อความเสี่ยงด้านธุรกิจ รวมทั้งให้ข้อแนะนำเพื่อการบริหารจัดการความเสี่ยงแก่หน่วยงานธุรกิจที่เกี่ยวข้อง
	๔.๒.๑.๘	บริษัทมีเครื่องมือและกระบวนการในการตรวจจับและแจ้งเตือน เมื่อตรวจพบพฤติกรรมหรือเหตุการณ์ที่ผิดปกติ โดยเชื่อมโยงข้อมูลจากหลายแหล่ง เช่น จากระบบเครือข่าย, ระบบงาน, Firewall และอุปกรณ์ Endpoint เป็นต้น เพื่อรายงานให้หน่วยงานหรือผู้มีหน้าที่รับผิดชอบในการรับมือเหตุการณ์ผิดปกติทางไซเบอร์ทราบและดำเนินการแก้ไข
	๔.๒.๑.๙	บริษัทมีเครื่องมือตรวจจับการรับส่งข้อมูลสำคัญผ่านช่องทางต่าง ๆ เช่น ระบบ Data Loss Prevention หรือ Data Leak Prevention เป็นต้น เพื่อตรวจจับและติดตามตรวจสอบการรั่วไหลข้อมูลสำคัญ
Advance	๔.๒.๑.๑๐	บริษัทมีเครื่องมือที่ใช้ตรวจจับการเปลี่ยนแปลงในการตั้งค่าและแก้ไขอุปกรณ์และระบบสารสนเทศโดยไม่ได้รับอนุญาต รวมทั้งมีกระบวนการ หรือ การตั้งค่าอัตโนมัติที่สามารถแจ้งเตือนไปยังหน่วยงานหรือผู้ที่เกี่ยวข้องเพื่อให้สามารถป้องกันหรือระงับเหตุการณ์ได้ทันท่วงที
	๔.๒.๑.๑๑	บริษัทวิเคราะห์ภัยคุกคาม (Threat Analysis System) โดยเชื่อมโยงข้อมูลภัยคุกคามต่าง ๆ และแจ้งเตือนไป ยังผู้รับผิดชอบที่เกี่ยวข้อง ตามระดับความเสี่ยงที่เกิดขึ้น นอกจากนี้ นำผลการวิเคราะห์ Threat Intelligence มาวิเคราะห์และพิจารณาความเสี่ยงด้านไซเบอร์และแนวทางการรับมือภัยคุกคาม เพื่อดำเนินการดังต่อไปนี้ (๑) ปรับปรุงข้อมูล Risk Profile ขององค์กรและระดับความเสี่ยงที่ยอมรับได้ (๒) ปรับปรุงสถาปัตยกรรมการรักษาความมั่นคงปลอดภัย (IT Security Architecture) และการกำหนดมาตรฐานการตั้งค่าระบบเทคโนโลยีสารสนเทศ (๓) คาดการณ์แนวโน้มและวางแผนป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต

ระดับการควบคุม	การควบคุม	
	๔.๒.๑.๑๒	บริษัทแลกเปลี่ยนข้อมูล Cyber Threat Intelligence ในเชิงรุกให้แก่บริษัทประกันภัยอื่น หน่วยงานกำกับดูแลหรือหน่วยงานที่บังคับใช้กฎหมายโดยทันที เมื่อพบข้อมูลภัยคุกคามทางไซเบอร์ที่อาจจะกระทบต่อกลุ่มอุตสาหกรรม โดยการดำเนินงานนี้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้อง รวมทั้ง บริษัทมีกระบวนการในการสื่อสารและร่วมมือเกี่ยวกับภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอก รวมถึงมีการสื่อสารกับบุคคลภายนอกตามความเหมาะสม

CM5 การรับมือและตอบสนองเมื่อพบเหตุการณ์ (Response & Recovery)

วัตถุประสงค์ : เพื่อให้บริษัทประกันภัยมีแผนการรับมือต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ภัยคุกคามทางไซเบอร์ และการรั่วไหลของข้อมูล ส่วนบุคคล โดยสามารถกู้คืนระบบหรือข้อมูลสารสนเทศให้สามารถกลับมาเป็นปกติภายในระยะเวลาที่ยอมรับได้ รวมทั้งสามารถจำกัดความเสียหาย สื่อสาร เมื่อพบเหตุการณ์ผิดปกติ และสืบสวนหาสาเหตุได้อย่างมีประสิทธิภาพ

CM 5.1 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
๕.๑.๑ การสำรองข้อมูล		
Baseline	๕.๑.๑.๑	บริษัทมีกระบวนการในการสำรองข้อมูลที่สำคัญ และ ระบบงานที่สำคัญ (ทั้งในระดับระบบงาน ระบบปฏิบัติการ และ ระบบฐานข้อมูล) โดยต้องรองรับการกู้คืนข้อมูลตามความเหมาะสมทางธุรกิจ และ ตามเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายได้ (Recovery Point Objective: RPO) อีกทั้ง บริษัทต้องมีการเฝ้าติดตามกระบวนการสำรองข้อมูลที่สำคัญเพื่อให้มั่นใจว่าการสำรองข้อมูลเป็นไปตามที่กำหนดไว้
	๕.๑.๑.๒	บริษัทจัดเก็บข้อมูลสำรองที่สำคัญ หรือมีการทำสำเนาข้อมูลสำคัญ และจัดเก็บไว้ในพื้นที่ภายนอกบริษัทอย่างมั่นคงปลอดภัย รวมทั้ง มีการทดสอบการกู้คืนข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสื่อบันทึกข้อมูล และ ข้อมูลที่ทำการสำรองหรือทำสำเนาไว้พร้อมใช้งานอยู่เสมอตามความต้องการทางธุรกิจ
Advance	๕.๑.๑.๓	บริษัทมีการเชื่อมต่อเพื่อปรับปรุงข้อมูลระหว่างศูนย์คอมพิวเตอร์หลัก (DC) และ ศูนย์คอมพิวเตอร์สำรอง (DR) ตลอดเวลา (Real Time Replication / Synchronization) เพื่อให้ศูนย์คอมพิวเตอร์สำรองมีข้อมูลที่เทียบเท่าศูนย์คอมพิวเตอร์หลักและสามารถใช้งานระบบสำคัญที่เกี่ยวข้องกับการให้บริการลูกค้าผ่านช่องทาง online ได้ทันที เมื่อมีเหตุการณ์เกิดขึ้น

CM 5.2 การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา

ระดับการควบคุม	การควบคุม	
Baseline	๕.๒.๑.๑	บริษัทจัดทำวิธีปฏิบัติ ขั้นตอนปฏิบัติ หรือแผนรองรับในการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ (IT Incident and Problem Management) และเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์ (Cyber Incident) พร้อมทั้งระบุช่องทางการรายงานที่ใช้ในการแจ้งเหตุการณ์ผิดปกติที่พบ และปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ
	๕.๒.๑.๒	บริษัทบันทึกและวิเคราะห์เหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ รวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์ โดยบริษัทสามารถวิเคราะห์และระบุสาเหตุที่แท้จริง (Root Cause) เพื่อประกอบการพิจารณากำหนดแนวทางในการแก้ไขและป้องกันการเกิดเหตุการณ์ซ้ำในอนาคต

ระดับการควบคุม	การควบคุม	
	๕.๒.๑.๓	บริษัทกำหนดแนวทางในการส่งต่อเหตุการณ์ผิดปกติ (Escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติไปยังผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้อง หรือคณะกรรมการบริษัท โดยพิจารณาให้เหมาะสมสอดคล้องกับระดับความรุนแรงของเหตุการณ์ที่เกิดขึ้น ทั้งนี้ ในกรณีที่มีเหตุการณ์ผิดปกติสำคัญที่ส่งผลกระทบต่อชื่อเสียงและการดำเนินธุรกิจอย่างมีนัยสำคัญ เช่น ระบบสำคัญไม่สามารถดำเนินการได้ตามปกติ หรือกระทบกับการให้บริการผู้เอาประกันภัยเกินกว่าระยะเวลาที่บริษัทยอมรับได้ เป็นต้น บริษัทได้รายงานเหตุการณ์ดังกล่าวไปยังผู้บริหาร และ คณะกรรมการที่เกี่ยวข้องโดยไม่ชักช้า
	๕.๒.๑.๔	บริษัทมีกระบวนการ และ แผนการตอนสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด รวมทั้ง มีการทดสอบเพื่อความมั่นใจว่าสามารถดำเนินการได้ตามแผน ภายใน ๗๒ ชั่วโมง
Intermediate	๕.๒.๑.๕	บริษัทมีศูนย์รับแจ้งเหตุ หรือ บุคคลผู้ทำหน้าที่รับแจ้งเหตุ หรือ รับรายงานด้านความมั่นคงปลอดภัยทางสารสนเทศและไซเบอร์ที่ชัดเจน และสื่อสารให้พนักงานและผู้ที่เกี่ยวข้องภายนอกบริษัทรับทราบ

CM 5.3 แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

ระดับการควบคุม	การควบคุม	
Baseline	๕.๓.๑.๑	บริษัทจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity Plan) และ/หรือ แผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) ที่มีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น โดยแผน IT Continuity Plan และ แผน DRP จะต้องได้รับการอนุมัติจากคณะกรรมการบริษัท หรือคณะกรรมการ/คณะทำงานที่ได้รับมอบหมาย รวมทั้งได้รับการทบทวนและปรับปรุงอย่างน้อยปีละ ๑ ครั้ง หรือ เมื่อมีเหตุการณ์เปลี่ยนแปลงที่สำคัญ อาทิ การพัฒนาระบบใหม่ หรือ เปลี่ยนแปลงระบบอย่างมีสาระสำคัญ การเปลี่ยนแปลงกลยุทธ์ การเปลี่ยนแปลงในการบริหารความเสี่ยงของบริษัท เป็นต้น
	๕.๓.๑.๒	แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity Plan) ของบริษัทครอบคลุมถึง (๑) การประเมินความเสี่ยงและผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) หรือวิธีการประเมินอื่น ๆ เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจส่งผลกระทบต่อการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ และทราบถึงผลกระทบที่อาจเกิดขึ้นจากการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ รวมถึงสามารถกำหนดลำดับความสำคัญของระบบงานที่ต้องกู้คืนได้อย่างเหมาะสม (๒) การกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) รวมถึง ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Period of Disruption: MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัท และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ
	๕.๓.๑.๓	บริษัทจัดให้มีศูนย์คอมพิวเตอร์สำรอง (Disaster Recovery Site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลักหยุดชะงัก โดยอาจเป็นศูนย์คอมพิวเตอร์สำรองในรูปแบบของ Cold Site, Warm Site หรือ Hot Site ก็ได้ ทั้งนี้ ศูนย์คอมพิวเตอร์สำรองอยู่ห่างจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะไม่ให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง และภัยธรรมชาติ เป็นต้น

ระดับการควบคุม	การควบคุม	
	๕.๓.๑.๔	บริษัททดสอบกระบวนการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity Plan) และ/หรือ แผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) ปีละ ๑ ครั้ง โดยรายงานผลการทดสอบไปยังผู้บริหาร และ คณะกรรมการที่เกี่ยวข้อง ในกรณีที่พบข้อบกพร่องในการดำเนินงาน เพื่อให้บริษัทดำเนินการปรับปรุงข้อบกพร่องดังกล่าวได้อย่างเหมาะสม
Intermediate	๕.๓.๑.๕	บริษัทจัดทำขั้นตอนปฏิบัติ คู่มือ หรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งทำการประชาสัมพันธ์แผนฯ และจัดฝึกอบรม โดยขั้นตอนปฏิบัติ คู่มือ หรือเอกสารดังกล่าว อย่างน้อยควรครอบคลุมในเรื่องดังต่อไปนี้ - ชื่อแผน วัตถุประสงค์ ขอบเขต และความเชื่อมโยงกับแผนอื่น ๆ ที่เกี่ยวข้อง - ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่ และความรับผิดชอบ และผู้ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่หลักไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกและการเปลี่ยนแปลงของแผน - รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพแสดงระบบเครือข่ายสื่อสาร เป็นต้น - ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ การตอบสนองต่อเหตุการณ์ฉุกเฉิน และแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ - ขั้นตอนในการกู้คืนระบบ ควรจัดทำเป็นเอกสารหรือคู่มือประกอบ โดยควรระบุรายละเอียดที่ชัดเจนเพียงพอ เพื่อใช้ควบคุมการกู้คืนระบบไม่ให้มีการข้ามหรือไม่ปฏิบัติตามขั้นตอนที่กำหนดไว้ และควรปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
	๕.๓.๑.๖	บริษัททดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity Plan) หรือ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) โดยให้ครอบคลุมถึงการทดสอบสถานการณ์จำลอง (Scenario) ของภัยคุกคามทางไซเบอร์รูปแบบใหม่ ๆ ที่มีโอกาสเกิดขึ้น โดยพิจารณาการทดสอบในรูปแบบที่เหมาะสม เช่น ลักษณะ table top หรือการจำลองการโจมตีทางไซเบอร์ (Simulation) เป็นต้น
Advance	๕.๓.๑.๗	บริษัทมีกระบวนการเพื่อบันทึกและรวบรวมปัญหาที่พบในระหว่างการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT continuity Plan) และ/หรือ แผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) โดยนำปัญหานั้นมาวิเคราะห์และระบุสาเหตุที่แท้จริง (Root Cause) เพื่อให้พนักงานมีข้อมูลที่เพียงพอที่จะสามารถแก้ไขปัญหาได้อย่างเหมาะสมในการปฏิบัติงานจริง
	๕.๓.๑.๘	การทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT continuity Plan) และ/หรือ แผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) ครอบคลุมการย้ายศูนย์ประมวลผล การเปลี่ยนแปลงกระบวนการทำงาน การเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ โดยไม่ก่อให้เกิดความเสียหายต่อข้อมูลของบริษัท

CM 5.4 การรับมือและตอบสนองเมื่อตรวจพบภัยคุกคามไซเบอร์

ระดับการควบคุม	การควบคุม	
Baseline	๕.๔.๑.๑	บริษัทมีแผน มาตรฐาน และระเบียบวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ซึ่งรวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital (Digital Forensics) ไว้อย่างชัดเจน

ระดับการควบคุม	การควบคุม	
	๕.๔.๑.๒	บริษัทมีแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ (Cyber Incident Response Plan: CIRP) ที่มีขอบเขตครอบคลุมภัยคุกคามทางไซเบอร์ และระบบงานสำคัญ และระบบที่เชื่อมต่อกับบุคคลภายนอกที่เกี่ยวข้อง โดยระบุถึงกระบวนการจัดการ การเตรียมความพร้อมในการรับมือและการตอบสนองต่อเหตุการณ์ และการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ ทั้งนี้ แผนดังกล่าวได้รับอนุมัติจากคณะกรรมการบริษัท หรือ คณะกรรมการ ที่ได้รับมอบหมาย รวมทั้ง แผนนี้ได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
	๕.๔.๑.๓	บริษัทซักซ้อม หรือ ทดสอบแผนรับมือภัยคุกคามทางไซเบอร์ (Cyber Drill) อย่างน้อยปีละ ๑ ครั้ง โดยครอบคลุมถึงภัยคุกคามทางไซเบอร์ และระบบงานสำคัญ และระบบที่เชื่อมต่อกับบุคคลภายนอก โดยจัดให้มีการสืบสวน วิเคราะห์สาเหตุการแก้ปัญหา และรายงานผลการทดสอบต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย
	๕.๔.๑.๔	บริษัทกำหนดช่องทาง บุคลากร และวิธีการสื่อสารเพื่อดำเนินการแก้ไข และส่งต่อข้อมูลเหตุการณ์ทางไซเบอร์ไปยังผู้ที่เกี่ยวข้อง รวมทั้ง จัดทำระเบียบ วิธีปฏิบัติในกรณีที่ต้องแจ้งลูกค้า หน่วยงานกำกับดูแล และหน่วยงานที่บังคับใช้กฎหมาย เมื่อเกิดเหตุการณ์ผิดปกติทางไซเบอร์ เช่น มีการเข้าถึงหรือ ใช้ข้อมูลลูกค้าจากผู้ไม่ประสงค์ดี เป็นต้น
Intermediate	๕.๔.๑.๕	บริษัทมีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ที่ครอบคลุมเหตุการณ์ทางด้านไซเบอร์ โดยการจัดทำแผนดังกล่าว ควรครอบคลุมกระบวนการอย่างน้อยดังนี้ (๑) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) (๒) การประเมินความเสี่ยง (Risk Analysis) (๓) การวางกลยุทธ์สำหรับแผนฉุกเฉิน (๔) การจัดทำแผนฉุกเฉิน (๕) การสื่อสารและฝึกอบรมให้แก่ผู้ที่เกี่ยวข้องทั้งภายในและภายนอก (๖) การทดสอบ ปรับปรุง และสอบทานแผน
	๕.๔.๑.๖	บริษัทมีแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan: CIRP) และคู่มือการตอบสนอง (Playbook) สำหรับเหตุการณ์ไซเบอร์ที่สำคัญที่บริษัทมีโอกาสเผชิญ โดยสอดคล้องและเชื่อมโยงกับแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) และแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP)
	๕.๔.๑.๗	บริษัทนำผลการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity Plan) แผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) และ แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan: CIRP) มาทบทวนและปรับปรุงกระบวนการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางสารสนเทศและไซเบอร์ที่เกี่ยวข้องทั้งหมดให้สอดคล้องกัน และมีประสิทธิภาพยิ่งขึ้น

ระดับการควบคุม	การควบคุม	
	๕.๔.๑.๘	บริษัทมีกระบวนการประเมินประสิทธิภาพ ความพร้อม และศักยภาพ (Due Diligence) ของบุคคลภายนอก หรือ ที่ปรึกษาที่จะมาให้บริการที่เป็นส่วนหนึ่งของกระบวนการกู้คืนระบบสารสนเทศอย่างสม่ำเสมอ เพื่อความมั่นใจในความพร้อมในการดำเนินงานหรือการให้บริการเมื่อมีเหตุการณ์ผิดปกติทางสารสนเทศและไซเบอร์เกิดขึ้น
	๕.๔.๑.๙	บริษัทมีกระบวนการหรือเครื่องมือที่บันทึกบทเรียน (Lesson Learned) ที่ได้เรียนรู้ภายหลังจากเหตุการณ์ผิดปกติทางสารสนเทศและไซเบอร์เกิดขึ้นทั้งภายในและภายนอกบริษัท และนำ Lesson Learned มาใช้เป็นแหล่งข้อมูลประกอบการรับมือภัยคุกคามทางไซเบอร์ โดยการจัดเก็บข้อมูล Lesson Learned พิจารณาถึงการบันทึกและจัดเก็บอย่างครบถ้วน รวมทั้ง สามารถเรียกใช้อย่างทันท่วงที
	๕.๔.๑.๑๐	บริษัทกำหนดตัวชี้วัดและประเมินประสิทธิภาพการทำงานของหน่วยงานที่มีหน้าที่รับมือเหตุการณ์ผิดปกติและภัยคุกคามไซเบอร์ (Computer Security Incident Response Team: CSIRT) (อาทิ การปฏิบัติงานรับมือได้ตามระยะเวลาที่กำหนด การดำเนินการมีประสิทธิภาพเป็นไปตามกระบวนการที่วางไว้ในแต่ละขั้นตอน เป็นต้น) และ นำผลการประเมินดังกล่าวมาปรับปรุงกระบวนการทำงาน และรายงานให้คณะกรรมการที่เกี่ยวข้องรับทราบ
Advance	๕.๔.๑.๑๑	บริษัทเชื่อมโยงข้อมูล และวิเคราะห์ข้อมูล Threat Intelligence อย่างมีประสิทธิภาพและมีการบูรณาการ โดยมีการสื่อสารและดำเนินการเพื่อเตรียมรับมือภัยคุกคามและตอบสนองในเชิงรุกต่อเหตุการณ์ผิดปกติที่อาจเกิดขึ้น
	๕.๔.๑.๑๒	บริษัททดสอบแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ โดยจำลองสถานการณ์ทางไซเบอร์ที่ซับซ้อนซึ่งเคยเกิดขึ้นกับองค์กรอื่น รวมทั้ง ทดสอบถึงศักยภาพ (Stress test) ในการบริหารจัดการความเสี่ยงด้านไซเบอร์ โดยพิจารณาว่าในกรณีที่เกิดเหตุการณ์ผิดปกติทางไซเบอร์ที่ส่งผลต่อการให้บริการอย่างต่อเนื่อง หรือก่อให้เกิดความเสียหายที่รุนแรง บริษัทมีทรัพยากรและขีดความสามารถในการบริหารจัดการได้ตามความคาดหวังหรือไม่ (การทดสอบถึงศักยภาพ หรือ Stress test เป็นการทดสอบขีดความสามารถขั้นสูงสุดที่ระบบงานหรือกระบวนการทำงานสามารถรองรับได้ โดยวัตถุประสงค์ในการทดสอบนี้ เพื่อให้มั่นใจว่าเมื่อเกิดเหตุการณ์ขึ้นแล้วขีดความสามารถที่บริษัทสามารถดำเนินการได้อยู่ในระดับที่คาดหวังไว้)
	๕.๔.๑.๑๓	บริษัทเข้าร่วมซักซ้อมหรือทดสอบแผนรับมือภัยคุกคามทางไซเบอร์ (Cyber Drill) ที่จัดขึ้นในระดับอุตสาหกรรม และได้นำเอาปัญหาและข้อเสนอแนะจากการทดสอบดังกล่าว มาปรับปรุงแผนรับมือของบริษัทให้มีความรัดกุมเทียบเท่ามาตรฐานที่มีการปฏิบัติในอุตสาหกรรม

CM 5.5 แนวทางฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์

ระดับการควบคุม	การควบคุม	
Baseline	๕.๕.๑.๑	บริษัทมีแผนหรือแนวทางในการในการฟื้นฟูความเสียหายจากเหตุการณ์ หรือสถานการณ์จากภัยคุกคามทางไซเบอร์ เพื่อป้องกันความเสี่ยง (Protection) การตรวจจับความเสี่ยง (Detection) และการรับมือและฟื้นฟูความเสียหาย (Response and Recovery) จากภัยคุกคามทางไซเบอร์ โดยแผนการดำเนินงานนี้สอดคล้องกับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ของบริษัท
	๕.๕.๑.๒	บริษัทมีแผน วิธีการ และช่องทางในการติดต่อสื่อสาร รวมถึง ผังการติดต่อพนักงาน (Call Tree) และผู้เกี่ยวข้องทั้งภายในและภายนอกบริษัท โดยกำหนดผู้รับผิดชอบในการสื่อสาร และรายละเอียดข้อมูลที่จะเปิดเผยแก่ผู้เกี่ยวข้องอย่างชัดเจน ในกรณีที่เป็นเหตุการณ์ที่กระทบถึงลูกค้า บริษัทต้องแจ้งหรือทำการ

ระดับการควบคุม	การควบคุม	
		ประชาสัมพันธ์ให้ลูกค้าและผู้เกี่ยวข้องทราบถึงสถานการณ์ ผลกระทบที่จะเกิดขึ้น รวมทั้งมีช่องทางที่ลูกค้าหรือผู้เกี่ยวข้องสามารถติดต่อใช้บริการหรือสื่อสารกับบริษัทได้ตลอดระยะเวลาที่เกิดสถานการณ์
Intermediate	๕.๕.๑.๓	บริษัทมีกระบวนการ หรือเครื่องมือที่สามารถตรวจพบเหตุการณ์ผิดปกติ หรือการโจมตีตั้งแต่ช่วงแรก รวมทั้งสามารถวิเคราะห์ และดำเนินการรับมือกับเหตุการณ์ผิดปกติหรือการโจมตีได้อย่างทันท่วงที
	๕.๕.๑.๔	บริษัทมีกระบวนการที่ครอบคลุมถึงเหตุการณ์ผิดปกติหรือภัยคุกคามที่เกิดกับหน่วยงานภายนอกที่เกี่ยวข้องกับบริษัท รวมทั้งมีแผนการรับมือในกรณีที่เกิดเหตุการณ์ดังกล่าว
	๕.๕.๑.๕	บริษัทมีกระบวนการในการบริหารจัดการทรัพย์สินสารสนเทศที่ได้รับผลกระทบจากเหตุการณ์ผิดปกติ หรือภัยคุกคามไซเบอร์ อาทิ การทำลายหรือยกเลิกการใช้งาน การจำกัดหรือตัดการเข้าถึงจากระบบสารสนเทศของบริษัท การล้างเครื่องหรือตั้งค่าใหม่ก่อนนำกลับมาใช้งาน เป็นต้น
Advance	๕.๕.๑.๖	เมื่อตรวจพบเหตุการณ์ผิดปกติหรือการโจมตี บริษัทสามารถจำกัดความเสียหาย (Containment) และการกำจัด (Eradication) ภัยคุกคามทางไซเบอร์ได้ทันทีเมื่อเหตุการณ์เกิดขึ้น

CM 5.6 การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบสารสนเทศ

ระดับการควบคุม	การควบคุม	
Baseline	๕.๖.๑.๑	บริษัทกำหนดขั้นตอน หรือ แนวทางการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบสารสนเทศ ที่ครอบคลุมถึงการรายงานเหตุการณ์ต่อสำนักงาน คปภ. เมื่อเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญ ดังนี้ (๑) ปัญหาหรือเหตุการณ์ที่ส่งผลกระทบต่อการให้บริการ หรือระบบสารสนเทศ (๒) ปัญหาหรือเหตุการณ์ที่ส่งผลกระทบต่อข้อมูลผู้เอาประกันภัย (๓) ปัญหาหรือเหตุการณ์ที่ส่งผลกระทบต่อชื่อเสียงของบริษัท (๔) ปัญหาหรือเหตุการณ์ที่ระบบเทคโนโลยีสารสนเทศที่สำคัญของบริษัทถูกโจมตี หรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ (๕) ปัญหาหรือเหตุการณ์ที่บริษัทต้องรายงานให้ผู้บริหารสูงสุดของบริษัททราบ นอกจากนี้ การรายงานต้องดำเนินการทันทีเมื่อเกิดเหตุ หรือ รับทราบเหตุการณ์นั้น โดยข้อมูลที่ต้องรายงานประกอบด้วย (๑) รายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น (๒) ผลกระทบที่คาดว่าจะเกิดขึ้น (๓) การดำเนินการแก้ไขปัญหา (๔) ผลการแก้ไขปัญหา และระยะเวลาในการแก้ไข (๕) แนวทางป้องกันในอนาคต

ระดับการควบคุม	การควบคุม	
	๕.๖.๑.๒	บริษัทกำหนดขั้นตอน หรือ แนวทางการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ครอบคลุมถึงการแจ้งเหตุการณ์ในระดับต่าง ๆ ไปยังหน่วยงานกำกับดูแล หน่วยงานของรัฐ และ องค์กรที่จัดตั้งขึ้นตามกฎหมายอย่างเหมาะสม ภายในระยะเวลาที่กำหนด โดยให้สอดคล้องกับกฎหมายและระเบียบข้อบังคับ
	๕.๖.๑.๓	บริษัทกำหนดขั้นตอน หรือ แนวทางการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบสารสนเทศ โดยพิจารณาถึงการสืบค้น และ จัดเตรียมข้อมูลที่ถูกต้องเหมาะสม เพื่อจัดทำและรายงาน "แบบฟอร์มรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศสำหรับบริษัทประกันภัย" ตามที่สำนักงาน คปภ. กำหนด

CM6 การบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ (Third Party Risk Management)

วัตถุประสงค์ : เพื่อให้บริษัทประกันภัยมีกระบวนการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจตลอดทั้งกระบวนการ

CM 6.1 การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ

ระดับการควบคุม	การควบคุม	
Baseline	๖.๑.๑.๑	บริษัทมีแนวทางการบริหารจัดการผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ ซึ่งประกอบด้วย (๑) กระบวนการและหลักเกณฑ์ในการคัดเลือก (๒) การจัดทำสัญญา (๓) เงื่อนไขในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท (๔) ข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) (๕) การตรวจสอบ และ ติดตามการให้บริการ รวมไปถึงบริษัทจัดให้มีโครงสร้างและกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับการบริหารจัดการผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจภายในบริษัทประกันภัย โดยให้เป็นไปตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (Three Lines of Defense)
	๖.๑.๑.๒	บริษัทสามารถระบุทรัพย์สินสารสนเทศ และ กระบวนการทางธุรกิจที่สำคัญที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจ โดยมีแผนภาพที่แสดงการเชื่อมโยง การเชื่อมต่อ และการไหลผ่านของข้อมูล (Data Flow) เพื่อให้มั่นใจในขอบเขตการบริหารจัดการผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจที่ครบถ้วน
Intermediate	๖.๑.๑.๓	บริษัทมีการกำหนดกลยุทธ์ที่ชัดเจนในการตัดสินใจใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และ มีการกำกับดูแลให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจของบริษัท โดยการใช้บริการจากผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจด้านงานเทคโนโลยีสารสนเทศนั้น ไม่ขัดต่อกฎหมายและข้อบังคับของบริษัท และไม่ก่อให้เกิดช่องโหว่ที่นำไปสู่การเกิดการทุจริต หรือภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอก
	๖.๑.๑.๔	กรณีที่การใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจเป็นงานด้านเทคโนโลยีสารสนเทศที่มีความสำคัญต่อบริษัท บริษัทมีกระบวนการในการประเมินความเสี่ยง และ พิจารณาเห็นชอบโดยคณะกรรมการบริษัท คณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย ก่อนเริ่มใช้บริการ เมื่อมีการเปลี่ยนการใช้บริการที่สำคัญ หรือ เมื่อมีการต่ออายุสัญญา
	๖.๑.๑.๕	บริษัทมีแนวทางการบริหารจัดการผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจที่มีการรับช่วงการให้บริการแก่ผู้ให้บริการภายนอกรายอื่น ๆ (Subcontract) เพื่อให้มั่นใจถึงความสามารถในการให้บริการ การปฏิบัติตามกฎหมายและระเบียบข้อบังคับต่าง ๆ รวมถึง การรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศและไซเบอร์

ระดับการควบคุม	การควบคุม	
	๖.๑.๑.๖	ในกรณีที่ต้องมีการเชื่อมต่อระบบสารสนเทศของบริษัทกับระบบสารสนเทศของผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจ หรือ ในกรณีที่เป็นผู้ให้บริการระบบคลาวด์ บริษัทมีการพิจารณาและตรวจสอบการเชื่อมต่อดังกล่าวว่ามีความปลอดภัย เช่น (๑) การติดตามความพร้อมใช้งานของการเชื่อมต่อและระบบของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ (๒) จำกัดการเชื่อมต่อเครือข่ายภายนอกตามความจำเป็น (Least Privilege) (๓) มีมาตรการเชิงเทคนิคหรือเครื่องมือเพื่อใช้ป้องกันการเชื่อมต่อและ/หรือการเข้าถึงระบบเครือข่ายภายในของบริษัทจากภายนอกที่ไม่ได้รับอนุญาต (๔) มีมาตรการการรักษาความปลอดภัย และ ป้องกันการบุกรุกผ่านการเชื่อมต่อ รวมทั้งมีอุปกรณ์ป้องกันเครือข่าย เช่น Firewall, Web Application Firewall, IPD, IDS เป็นต้น ติดตั้งไว้ทุกจุดที่มีการรับส่งข้อมูลกับเครือข่ายภายนอก
	๖.๑.๑.๗	บริษัทมีแนวทางการบริหารจัดการผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจซึ่งครอบคลุมถึงกระบวนการในการยกเลิกและเปลี่ยนแปลงผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจ รวมทั้งการบริหารจัดการข้อมูลและ สินทรัพย์สารสนเทศของบริษัทที่ถูกจัดเก็บหรือถือครองโดยผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจ ในกรณีมีการยกเลิกและเปลี่ยนแปลง
Advance	๖.๑.๑.๘	บริษัทกำหนดหน่วยงานหรือผู้รับผิดชอบในการประสานงานกับผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ เพื่อการร่วมมือในกระบวนการการรักษาความมั่นคงปลอดภัยสารสนเทศและการเชื่อมต่อ

CM 6.2 การบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ

ระดับการควบคุม	การควบคุม	
Baseline	๖.๒.๑.๑	บริษัทประเมินและบริหารจัดการความเสี่ยงจากการใช้งานผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจโดยครอบคลุมเรื่อง (๑) ความเสี่ยงในการใช้บริการระบบคลาวด์ (๒) ความเสี่ยงที่เกี่ยวข้องกับการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) (๓) การพึ่งพิงการใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ จนอาจทำให้การเปลี่ยนแปลงหรือยกเลิกการใช้บริการทำได้ยาก (Vendor Lock-in) (๔) ผลกระทบต่อระบบงานที่สำคัญของบริษัทb (๕) ความเสี่ยงอันอาจเกิดจากการใช้งานผู้ให้บริการในต่างประเทศ อาทิ การขัดข้องหรือการปิดกั้นเครือข่ายสื่อสาร หรือระบบสื่อสารระหว่างประเทศ (Information Access Risk) ความเสี่ยงด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติตามหลักเกณฑ์ของต่างประเทศ (Cross-border Compliance) เป็นต้น โดยการประเมินความเสี่ยงนี้คำนึงถึงความเสี่ยงที่อาจเกิดขึ้นภายใต้กรอบหลักการด้านเทคโนโลยี ๓ ประการ คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และ ความพร้อมใช้งาน (Availability)

ระดับการควบคุม	การควบคุม	
Intermediate	๖.๒.๑.๒	บริษัทนำข้อมูลจากทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศมาจัดทำ Diagrams ที่แสดงถึงการจัดเก็บข้อมูล (Data Repositories) การไหลผ่านของข้อมูล (Data Flow) และโครงสร้างระบบเครือข่าย (Network Infrastructure) ของการใช้บริการ การเชื่อมต่อ การเข้าถึงข้อมูลจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และจุดที่มีความเสี่ยงอื่น ๆ ตามความเสี่ยงที่เหมาะสม

CM 6.3 หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ

ระดับการควบคุม	การควบคุม	
๖.๓.๑ การคัดเลือกผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ		
Baseline	๖.๓.๑.๑	บริษัทมีหลักเกณฑ์ในการประเมินเพื่อคัดเลือกผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ โดยพิจารณาครอบคลุมถึง (๑) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการ และระบบการบริหารงานภายใน (๒) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน (๓) ศักยภาพและความสามารถในการให้บริการทั้งในภาวะปกติและไม่ปกติ โดยเฉพาะอย่างยิ่งกรณีที่มีการให้บริการแก่ผู้ใช้บริการหลายราย (Concentration Risk) (๔) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (๕) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ (๖) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง (๗) การปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ และการรับรองการปฏิบัติตามมาตรฐานสากล (๘) ปัจจัยภายนอกที่อาจกระทบต่อการให้บริการของบุคคลภายนอก (๙) การใช้เทคโนโลยีแบบเปิด (Open Technology) เพื่อให้สามารถใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (Interoperability) โดยการตัดสินใจในการใช้บริการที่มีความเสี่ยงหรือมีนัยสำคัญ ต้องได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย
Intermediate	๖.๓.๑.๒	สัญญาที่จัดทำกับผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจด้านเทคโนโลยีสารสนเทศ มีการระบุสิทธิเรียกร้องค่าเสียหายในกรณีที่บุคคลภายนอกไม่สามารถปฏิบัติตามข้อกำหนดที่บริษัทกำหนดไว้
Advance	๖.๓.๑.๓	บริษัทประเมินความเสี่ยง และ การรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจที่มีความสำคัญ โดยนำประกาศนียบัตรทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ รายงานการตรวจสอบจากผู้ตรวจสอบอิสระ (Third Party Assurance Report เช่น SOC ๒ Type ๒ Report) มาใช้หรือ มีการเข้าไปตรวจสอบการควบคุมด้วยตนเอง เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจที่มีความสำคัญ มีมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบเท่ามาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท
๖.๓.๒ การจัดทำสัญญาและข้อตกลงการให้บริการ		

ระดับการควบคุม	การควบคุม	
Baseline	๖.๓.๒.๑	บริษัทจัดทำสัญญากับผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร รวมทั้ง มีการระบุถึงข้อตกลงระดับการให้บริการ หรือ Service Level Agreement (SLA) ที่ตรวจวัดได้ โดยให้ครอบคลุมในเรื่องดังต่อไปนี้ (๑) ขอบเขตงานและเงื่อนไขในการให้บริการ รวมทั้งบทบาทหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ (๒) มาตรฐานขั้นต่ำในการปฏิบัติงานสำหรับผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ รวมถึงการปฏิบัติตามนโยบายการรักษาความปลอดภัยสารสนเทศของบริษัท (๓) ระบบการควบคุมภายในของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ (๔) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศสำหรับการใช้บริการที่สอดคล้องกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของบริษัท (๕) การติดตามและรายงานผลการปฏิบัติงาน ซึ่งครอบคลุมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการ (๖) ความรับผิดชอบของบริษัทและผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ ในกรณีที่เกิดปัญหาในการให้บริการ เงื่อนไขหรือแนวทางในการเปลี่ยนแปลงหรือยกเลิกสัญญา (๗) การระบุสิทธิในการเข้าตรวจสอบของบริษัท สำนักงาน คปภ. ผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากบริษัทหรือสำนักงาน คปภ.
	๖.๓.๒.๒	ในกรณีที่ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจทางด้านเทคโนโลยีสารสนเทศอยู่ภายนอกประเทศไทย บริษัทจัดทำสัญญาโดยพิจารณาถึงการปฏิบัติตามกฎหมายไทยที่เกี่ยวข้อง อาทิ พ.ร.บ. PDPA
๖.๓.๓ การติดตามการดำเนินงาน		
Baseline	๖.๓.๓.๑	บริษัททบทวน ประเมิน และ ตรวจสอบศักยภาพ ผลการปฏิบัติงาน และความเสี่ยงของการใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจอย่างสม่ำเสมอตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ โดยการประเมินพิจารณาถึง (๑) ความสามารถในการดำเนินการตามแนวทางหรือมาตรฐานที่ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจได้ตกลงไว้กับบริษัท (๒) ประสิทธิภาพการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ ตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ของบริษัท และกฎหมายที่เกี่ยวข้อง ที่ครอบคลุมความเสี่ยงอย่างน้อยตามกรอบหลักการ ๓ ประการ ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องเชื่อถือได้ (Integrity) และ ความพร้อมใช้งาน (Availability) (๓) การรายงานเหตุการณ์ผิดปกติจากการให้บริการของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจมายังบริษัทโดยไม่ชักช้า โดยผลการประเมินนี้รายงานให้คณะกรรมการหรือผู้บริหารที่รับผิดชอบรับทราบภายในระยะเวลาที่เหมาะสม
Intermediate	๖.๓.๓.๒	ในกรณีที่ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจมีการรับช่วงการให้บริการแก่ผู้ให้บริการภายนอกรายอื่น ๆ (Subcontract) บริษัทมีกระบวนการติดตามเพื่อให้มั่นใจว่าผู้ให้บริการภายนอกรายอื่น ๆ นั้นจะรับผิดชอบต่อการให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บริษัท เสมือนกับที่ผู้ให้บริการภายนอกหรือพันธมิตรเป็นผู้ให้บริการด้วยตนเอง

ระดับการควบคุม	การควบคุม	
Advance	๖.๓.๓.๓	บริษัทมีการตรวจสอบ หรือสอบทานรายงานการตรวจสอบจากผู้ตรวจสอบอิสระ (Third Party Assurance report) ตามมาตรฐานสากล (เช่น SOC ๒ Type ๒ Report) เพื่อประเมินความเพียงพอของการควบคุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจที่สำคัญ อย่างสม่ำเสมอ และเป็นส่วนหนึ่งของการติดตามการดำเนินงานของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ
๖.๓.๔ การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ		
Baseline	๖.๓.๔.๑	บริษัทกำหนดให้มีกระบวนการในการรับมือกับเหตุการณ์ผิดปกติหรือเหตุการณ์สำคัญที่ครอบคลุมถึงเหตุการณ์ที่อาจเกิดขึ้นจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และกำหนดให้ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจรายงานเหตุการณ์ผิดปกติจากการให้บริการที่เกิดขึ้นอย่างทันการณ์ เพื่อประเมินผลกระทบที่อาจเกิดขึ้นอย่างมีนัยสำคัญ ต่อการดำเนินธุรกิจของบริษัท
Intermediate	๖.๓.๔.๒	บริษัทกำหนดบทบาทหน้าที่และความรับผิดชอบระหว่างบริษัทและผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจอย่างชัดเจน และ มีแนวทางในการรับมือกับเหตุการณ์ผิดปกติหรือเหตุการณ์สำคัญที่ครอบคลุมถึงเหตุการณ์ที่อาจเกิดขึ้นจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ โดยพิจารณาให้ (๑) บริษัทมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติที่ส่งผลกระทบต่อการดำเนินธุรกิจของบริษัทอย่างมีนัยสำคัญ (๒) มีช่องทาง ระบบ หรือเครื่องมือเพื่อให้บริษัทสามารถรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศให้ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจทราบ และสามารถติดตามสถานการณ์และการดำเนินการแก้ไขของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจได้ (๓) มีผู้ประสานงานหลักของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ เพื่อสื่อสารและประสานงานเกี่ยวกับการดำเนินการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ
๖.๓.๕ การบริหารความต่อเนื่องทางธุรกิจ		
Baseline	๖.๓.๕.๑	บริษัทมีการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และ แผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) ที่ครอบคลุมถึงเหตุการณ์อันเกิดจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ โดยคำนึงถึงปัจจัยสำคัญหรือความเสี่ยงที่อาจเกิดขึ้นที่ส่งผลต่อการหยุดชะงักของการให้บริการและการดำเนินธุรกิจ
Intermediate	๖.๓.๕.๒	บริษัทมีกระบวนการสอบทานแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) หรือ เอกสารที่เกี่ยวข้องของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ โดยพิจารณาความสอดคล้องกับแผนของบริษัท เช่น การกำหนด Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น
Advance	๖.๓.๕.๓	ในกรณีที่บริษัทมีการใช้บริการทางด้านสารสนเทศที่สำคัญจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ บริษัทมีการดำเนินการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) และ แผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) และ แผนรับมือภัยคุกคามและ

ระดับการควบคุม	การควบคุม	
		ตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan: CIRP) ร่วมกับผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ เพื่อให้มั่นใจว่าเมื่อเกิดเหตุการณ์ขึ้น การดำเนินงานต่าง ๆ จะยังสามารถดำเนินงานได้อย่างราบรื่น และบรรลุตามวัตถุประสงค์การกู้คืนระบบของบริษัท
๖.๓.๖ การรักษาความมั่นคงปลอดภัยสารสนเทศในการใช้งานผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ		
Advance	๖.๓.๖.๑	บริษัทมีการติดตามการเข้าถึงข้อมูลสำคัญโดยบุคคลภายนอก ทั้งข้อมูลที่อยู่ในระบบของบริษัท และระบบที่ใช้บริการจากบุคคลภายนอก โดยให้เป็นไปตามหลักการการให้สิทธิเท่าที่จำเป็น (Least Privilege)
๖.๓.๗ การคุ้มครองผู้ใช้บริการของบริษัท		
Intermediate	๖.๓.๗.๑	บริษัทมีช่องทางหรือระบบเพื่อให้ผู้ใช้บริการของบริษัทร้องเรียนปัญหา เหตุขัดข้อง หรือเหตุการณ์ผิดปกติ และมีการรายงานเหตุร้องเรียนเหล่านั้นแก่คณะกรรมการหรือผู้บริหารที่ได้รับมอบหมายอย่างเหมาะสม โดยบริษัทมีแผนรองรับในการชดเชยความเสียหาย ในกรณีที่ผู้ใช้บริการของบริษัทเกิดความเสียหาย
	๖.๓.๗.๒	บริษัทมีมาตรการในการป้องกันไม่ให้ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจนำข้อมูลของลูกค้าหรือข้อมูลบริษัทไปเปิดเผยโดยไม่ได้รับอนุญาต เช่น มีการลงนามสัญญาไม่เปิดเผยข้อมูล (Non Disclosure Agreement: NDA)

CM 6.4 การรายงานต่อสำนักงาน คปภ.

ระดับการควบคุม	การควบคุม	
Baseline	๖.๔.๑.๑	กระบวนการบริหารจัดการผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจของบริษัท ครอบคลุมถึง การรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ ที่ส่งผลกระทบต่อบริษัทประกันภัยตามเงื่อนไขในประกาศฯ และแนวปฏิบัติของสำนักงาน คปภ. แก่สำนักงาน คปภ. โดยไม่ชักช้า

สรุปผลการประเมินระดับการควบคุม (Control Maturity : CM)

ระดับการควบคุมของแต่ละหมวดหมู่ คิดจากร้อยละของจำนวนการควบคุมที่บริษัทจัดให้มีขึ้น ซึ่งมีวิธีการคำนวณดังนี้

๑. แต่ละการควบคุมจะถูกให้คะแนนตามตัวเลือกที่บริษัทประกันภัยเลือก ดังนี้
   - การควบคุมที่บริษัทจัดให้มีขึ้นทั้งหมดและใช้การควบคุมนั้นกับทุกระบบงานสำคัญ[๑] (Yes) มีคะแนน ๑ คะแนนเต็ม
   - การควบคุมที่บริษัทจัดให้มีขึ้นมากกว่ากึ่งหนึ่ง หรือ ใช้การควบคุมนั้นกับระบบงานสำคัญมากกว่ากึ่งหนึ่ง[๒] (Partial) มีคะแนน ๐.๕ คะแนน
   - การควบคุมที่บริษัทไม่ได้จัดให้มีขึ้น จัดให้มีขึ้นไม่ถึงกึ่งหนึ่ง หรือ ใช้การควบคุมนั้นกับระบบงานสำคัญน้อยกว่ากึ่งหนึ่ง[๓] (No) มีคะแนน ๐ คะแนน
   - การควบคุมที่ไม่เกี่ยวข้องกับการดำเนินงานหรือเทคโนโลยีสารสนเทศของบริษัท[๔] (N/A) จะถูกตัดออกจากการคำนวณ

๒. คะแนนรวมของการควบคุมทั้งหมดในแต่ละระดับ ต่อ จำนวนข้อการควบคุมเฉพาะที่เกี่ยวข้องในแต่ละระดับ จะถูกนำมาคำนวณเป็นอัตราร้อยละของการควบคุมในแต่ละระดับการควบคุมของหมวดหมู่นั้นๆ

๓. เมื่อได้ร้อยละของการควบคุมในแต่ละระดับการควบคุมในหมวดหมู่นั้น ๆ แล้ว การจัดระดับการควบคุมของบริษัทจะเป็นไปตามเกณฑ์ดังต่อไปนี้
   - **บริษัทที่อยู่ในระดับ Baseline คือบริษัทที่ได้คะแนนร้อยละ 100 ในการควบคุมของระดับ Baseline**
   - **บริษัทที่อยู่ในระดับ Intermediate คือบริษัทที่ได้คะแนนร้อยละ 100 ในการควบคุมของระดับ Baseline และ Intermediate**

---

[1] ตัวอย่างเช่น ในกรณีที่การควบคุมระบุให้ต้องมีกิจกรรม ๓ ส่วน ได้แก่ การกำหนดนโยบาย การทบทวนอย่างสม่ำเสมอ และการประกาศใช้งาน หากบริษัทประกันภัยมีกิจกรรมครบทั้ง ๓ ส่วนตามที่ระบุและใช้การควบคุมนั้นครอบคลุมทุกระบบงานสำคัญ บริษัทสามารถพิจารณาได้ว่าเป็นการควบคุมที่บริษัทจัดให้มีขึ้นทั้งหมด

[๒] อ้างอิงจากตัวอย่างกิจกรรมการควบคุม ๓ ส่วนข้างต้น บริษัทประกันภัยสามารถพิจารณาว่าเป็นการควบคุมที่บริษัทจัดให้มีขึ้นมากกว่ากึ่งหนึ่ง หรือ ใช้การควบคุมนั้นกับระบบงานสำคัญมากกว่ากึ่งหนึ่ง เมื่อบริษัทดำเนินการควบคุมเพียง ๒ กิจกรรม คือ มีเพียงการจัดทำนโยบายและการทบทวน โดยที่ยังไม่มีการประกาศใช้งาน หรือ บังคับใช้นโยบายกับระบบงานสำคัญจำนวน ๓ จาก ๕ ระบบงานสำคัญ

[๓] อ้างอิงจากตัวอย่างกิจกรรมการควบคุม ๓ ส่วนข้างต้น บริษัทประกันภัยสามารถพิจารณาว่าเป็นการควบคุมที่บริษัทไม่ได้จัดให้มีขึ้น จัดให้มีขึ้นไม่ถึงกึ่งหนึ่ง หรือ ใช้การควบคุมนั้นกับระบบงานสำคัญน้อยกว่ากึ่งหนึ่ง เมื่อบริษัทดำเนินการควบคุมเพียง ๑ กิจกรรม คือ มีเพียงการจัดทำนโยบายเท่านั้น หรือ บังคับใช้นโยบายกับระบบงานสำคัญเพียงส่วนน้อยไม่ถึงครึ่งของระบบงานสำคัญทั้งหมด หรือ ไม่มีนโยบายเลย

[๔] การควบคุมที่ไม่เกี่ยวข้องกับการดำเนินงานหรือเทคโนโลยีสารสนเทศของบริษัท อาจเป็นเป็นเทคโนโลยีหรือกระบวนการที่บริษัทไม่มีการใช้งาน เช่น เป็นการควบคุมเกี่ยวกับการพัฒนาระบบงานด้วยวิธีการดำเนินงานแบบ Agile แต่บริษัทยังไม่มีการนำวิธีการดำเนินงานดังกล่าวเข้ามาใช้งานภายในบริษัท เป็นต้น

- บริษัทที่อยู่ในระดับ Advance คือบริษัทที่ได้คะแนนร้อยละ ๑๐๐ ในการควบคุมของระดับ Baseline Intermediate และ Advance

ทั้งนี้ ในกรณีที่บริษัทได้คะแนนไม่ถึงร้อยละ ๑๐๐ ในการควบคุมของระดับ Baseline จะถูกจัดอยู่ในระดับ Below Baseline

การคำนวณระดับการควบคุมรวมของบริษัทอ้างอิงจากค่าระดับการควบคุมในหมวดหมู่ที่มีค่าต่ำที่สุด อาทิ ระดับการควบคุมของหมวดหมู่ที่ ๑ มีค่า Baseline ในขณะที่ระดับการควบคุมในหมวดหมู่อื่นๆ มีค่า Intermediate หรือ Advance ให้ถือว่าบริษัทมีระดับการควบคุมในระดับ Baseline

อย่างไรก็ดี บริษัทควรมีระดับการควบคุมที่เหมาะสมโดยสอดคล้องตามระดับความเสี่ยงสืบเนื่องของบริษัท ซึ่งในกรณีที่บริษัทพบว่าระดับการควบคุมโดยรวมของบริษัทยังต่ำกว่าระดับความเสี่ยง บริษัทควรพิจารณากำหนดแนวทางการดำเนินงานเพื่อยกระดับให้บริษัทมีระดับการควบคุมที่เหมาะสมกับระดับความเสี่ยง

อภิธานศัพท์

คำศัพท์	คำอธิบาย
ระบบงานสำคัญ	ระบบงาน (Application หรือ Software) ที่สนับสนุนบริการหรือกิจกรรมที่ให้บริการในประเทศไทย ได้แก่ (๑) การพัฒนาผลิตภัณฑ์ประกันภัย และการกำหนดเบี้ยประกัน (๒) การเสนอขายและการเก็บเบี้ยประกัน (๓) การพิจารณารับประกันภัย (๔) การประเมินสำรองประกันภัย (๕) การบริหารจัดการค่าสินไหมทดแทนและผลประโยชน์ตามกรมธรรม์ประกันภัย (๖) การประกันภัยต่อ (๗) การลงทุนประกอบธุรกิจอื่น (๘) การบริหารสินทรัพย์และหนี้สิน รวมถึง ระบบงาน (Application หรือ Software) ที่จัดเก็บ ประมวลผล และ ส่งผ่านข้อมูลส่วนบุคคลของลูกค้า หรือผู้เอาประกันภัย ซึ่งรวมถึง ระบบอีเมลที่ใช้เพื่อการทำธุรกรรมทางด้านประกันภัยข้างต้น อาทิ การส่ง E-policy หรือ E-invoice ผ่านอีเมลไปยังลูกค้า หรือผู้เอาประกันภัย ทั้งนี้ ระบบงานสำคัญไม่รวมถึงระบบอีเมลที่ใช้ในการสื่อสารภายในบริษัท หรือ ระบบเพื่อการบริหารจัดการอื่น ๆ ที่อาจมีข้อมูลส่วนบุคคลรวมอยู่ด้วย ตัวอย่างการพิจารณา - ในกรณีที่บริษัทมีระบบ Core Insurance ที่ให้บริการทั้ง ๘ กิจกรรมข้างต้น ให้นับระบบ Core Insurance เป็น ๑ ระบบงาน - ในกรณีที่บริษัทมีระบบงานแยกย่อย อาทิ ระบบงาน A ให้บริการการพัฒนาผลิตภัณฑ์ประกันภัย และ ระบบงาน B ที่ให้บริการการพัฒนาผลิตภัณฑ์ประกันภัยเช่นเดียวกัน ให้นับระบบ A และ B แยกกันเป็น ๒ ระบบงาน - ในกรณีที่กิจกรรมบางส่วนไม่มีระบบงาน หรือ อาจเป็นการคำนวณผ่าน Spreadsheet เช่น MS Excel ไม่ถือว่าเป็นระบบงาน **อ้างอิง** กิจกรรมที่เกี่ยวข้องตามประกาศเรื่อง หลักเกณฑ์ วิธีการ และ เงื่อนไขในการบริหารจัดการความเสี่ยงแบบองค์รวมและการประเมินความเสี่ยง ฯ
ข้อมูลสำคัญ	ข้อมูลที่จัดเก็บ ส่งผ่าน และ ประมวลผลบนระบบงานสำคัญ เช่น ข้อมูลผู้เอาประกันภัย ข้อมูลลูกค้า ข้อมูลเกี่ยวกับแผนธุรกิจ ข้อมูลทางการเงิน ข้อมูลเกี่ยวกับการพัฒนาผลิตภัณฑ์หรือเทคโนโลยีสารสนเทศ เป็นต้น รวมถึง ข้อมูลที่เข้าข่ายข้อมูลส่วนบุคคลของลูกค้า หรือ ผู้เอาประกันภัย **อ้างอิง** คำจำกัดความของข้อมูลส่วนบุคคลให้อ้างอิงตามแนวปฏิบัติในการคุ้มครองข้อมูล ส่วนบุคคลของลูกค้า ของสำนักงาน

คำศัพท์	คำอธิบาย
ผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT outsource)	ผู้ให้บริการภายนอกที่ดำเนินการด้านงานเทคโนโลยีสารสนเทศของบริษัทซึ่งโดยปกติแล้วบริษัทต้องดำเนินการเอง และ ให้รวมถึงผู้ให้บริการภายนอกที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญของบริษัทหรือของลูกค้าของบริษัทได้ รวมถึง การใช้บริการระบบคลาวด์ (cloud computing) และ IT third party ด้วย **อ้างอิง** แนวปฏิบัติเรื่อง หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ของสำนักงาน
บุคคลหรือนิติบุคคลภายนอก / พันธมิตรทางธุรกิจ (Third party)	บุคคลหรือนิติบุคคลภายนอก รวมถึงบริษัทในเครือ ซึ่งเป็นผู้ให้บริการหรือเป็นผู้ที่มีการเชื่อมต่อและเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทประกันภัย หรือ เป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของบริษัทประกันภัยหรือข้อมูลของลูกค้าที่ควบคุมโดยบริษัทประกันภัยได้ อาทิ ตัวแทน นายหน้า อู่ซ่อมรถ ธนาคาร โรงพยาบาล Surveyor เป็นต้น ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์และบริการของบริษัทประกันภัย
บริษัทในเครือ	(๑) บริษัทแม่ของบริษัทประกันภัย (๒) นิติบุคคลที่บริษัทประกันภัย หรือ บริษัทแม่ของบริษัทประกันภัย ถือหุ้น มีอำนาจในการบริหารจัดการ หรือ มีอำนาจในการแต่งตั้งถอดถอนกรรมการได้ อาทิ บริษัทแม่ของบริษัทประกันภัยจัดตั้งบริษัททางด้าน IT เพื่อพัฒนาระบบงานที่ใช้งานโดยบริษัทประกันภัยทุกสำนักงานเครือข่าย ให้ถือว่าบริษัททางด้าน IT นั้นเป็นบริษัทในเครือ
การทำธุรกรรมผ่านระบบ Online	(๑) ธุรกรรมที่ลูกค้าติดต่อเพื่อดำเนินรายการทางธุรกิจ เช่น ซื้อกรมธรรม์ หรือ เรียกร้องค่าสินไหมผ่านระบบสารสนเทศที่บริษัทจัดเตรียมให้โดยตรง เช่น Website, Mobile Application, Social media โดยไม่ได้มีการติดต่อผ่านเจ้าหน้าที่ของบริษัท (๒) ธุรกรรมที่ลูกค้าติดต่อเพื่อดำเนินรายการทางธุรกิจ เช่น ซื้อกรมธรรม์ หรือ เรียกร้องค่าสินไหมผ่านระบบสารสนเทศที่ตัวแทนหรือนายหน้าจัดเตรียมให้โดยตรง เช่น Website, Mobile Application, Social media โดยไม่ได้มีการติดต่อผ่านเจ้าหน้าที่ของตัวแทนหรือนายหน้า (๓) กรณีที่เป็นการสแกนเอกสารและส่งเรื่องผ่านทางอีเมล ไม่จัดเป็นการทำธุรกรรมผ่านระบบ Online

เอกสารอ้างอิง

๑. ประกาศ คปภ. เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๓ (ประกาศ IT risk management)
๒. แนวปฏิบัติ เรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๔
๓. แนวปฏิบัติเรื่อง หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๔
๔. คู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการกำกับดูแลตามความเสี่ยง IT Audit Manual – Risk Based Supervision
๕. The Cyber Resilience Assessment Framework ของ Hong Kong Monetary Authority ซึ่งเป็นหน่วยงานกำกับดูแลสถาบันการเงินในฮ่องกง
๖. FFIEC Cybersecurity Assessment Tool ของ Federal Financial Institutions Examination Council ซึ่งเป็นหน่วยงานกำกับดูแลสถาบันการเงินในสหรัฐอเมริกา
๗. กรอบการประเมินความพร้อมด้าน Cyber Resilience ของธนาคารแห่งประเทศไทย
๘. Cyber Resilience Maturity Assessment Tool ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
9. NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations
10. ISO27001:2013 Information technology - Security techniques – Information Security Management Systems