FAQ:

กรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework: CRAF) สำหรับบริษัทประกันภัย

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

มิถุนายน 2565

สารบัญ

บทนำ

จากที่สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (“สำนักงาน” หรือ “สำนักงาน คปภ.”) ได้จัดทำกรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์สำหรับบริษัทประกันภัย (Cyber Resilience Assessment Framework: CRAF หรือ “กรอบ CRAF”) สำหรับบริษัทประกันภัยขึ้น รวมทั้ง ได้จัดการประชุมหารือ อบรม และได้นำส่งแบบประเมินตามกรอบ CRAF ไปยังบริษัทประกันภัยแล้วนั้น สำนักงานได้จัดทำเอกสาร FAQ: กรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework: CRAF) สำหรับบริษัทประกันภัยขึ้น โดยรวบรวมคำถาม-คำตอบที่เกี่ยวข้องกับแบบประเมินตามกรอบ CRAF จากการประชุมหารือ อบรม ต่าง ๆ เพื่อเป็นข้อมูลให้บริษัทประกันภัยสามารถใช้อ้างอิงเพิ่มเติมในการประเมินตนเองตามกรอบ CRAF

คำถาม-คำตอบที่อยู่ในเอกสาร FAQ: กรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework: CRAF) สำหรับบริษัทประกันภัยนี้ ถูกรวบรวมมาจากคำถาม-คำตอบและข้อคิดเห็นเพิ่มเติมจากบริษัทประกันภัยในระหว่างการจัดทำและประเมินตามกรอบ CRAF ซึ่งประกอบด้วย

- การประชุมเพื่อขอข้อมูลปัจจัยความเสี่ยงสืบเนื่องจากบริษัทประกันภัย ในวันที่ 28 กุมภาพันธ์ 2565
- คำถามและข้อคิดเห็นเพิ่มเติมจากบริษัทประกันภัยระหว่างการให้ข้อมูลปัจจัยความเสี่ยงสืบเนื่องในระหว่างวันที่ 1-25 มีนาคม 2565
- การประชุมกลุ่มย่อย (Focus Group) ในระหว่างวันที่ 31 มีนาคม – 5 เมษายน 2565
- คำถามและข้อคิดเห็นเพิ่มเติมจากบริษัทประกันภัยภายหลังจากการพิจารณาแบบประเมินตามกรอบ CRAF ฉบับร่างในระหว่างวันที่ 5 -20 เมษายน 2565
- การอบรมเกี่ยวกับกรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework: CRAF) สำหรับบริษัทประกันภัย ในระหว่างวันที่ 19 และ 24 พฤษภาคม 2565
- คำถามเพิ่มเติมจากบริษัทประกันภัยในระหว่างการประเมินตนเองตามแบบประเมินตามกรอบ CRAF ในระหว่างวันที่ 1 มิถุนายน -29 กรกฎาคม 2565

เอกสาร FAQ: กรอบการประเมินระดับความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework: CRAF) สำหรับบริษัทประกันภัย แบ่งออกเป็น 3 ส่วน ได้แก่

1. คำถามเกี่ยวกับแบบประเมินตามกรอบ CRAF ในภาพรวม
2. คำถามเกี่ยวกับแบบประเมินระดับความเสี่ยงสืบเนื่อง (Inherent Risk: IR)
3. คำถามเกี่ยวกับแบบประเมินระดับการควบคุม (Control Maturity: CM)

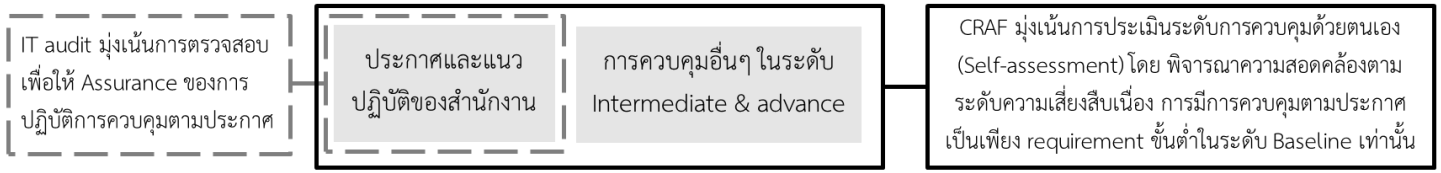
ในกรณีที่บริษัทประกันภัยมีคำถามหรือต้องการข้อมูลเพิ่มเติม สามารถสอบถามมาทางสำนักงานได้ที่ อีเมล itriskmgt@oic.or.th

คำถามเกี่ยวกับแบบประเมินตามกรอบ CRAF ในภาพรวม

ข้อ	เรื่อง	ถาม - ตอบ
1	ผู้ประเมิน และ การลงนามในแบบประเมิน	**ถาม:** หน่วยงานที่เป็นผู้ประเมินความเสี่ยงตามกรอบ CRAF ควรเป็นหน่วยงานใด **ตอบ:** จากการประเมินตามกรอบ CRAF ของหน่วยงานกำกับดูแลอื่น ๆ พบว่า บริษัทส่วนใหญ่ให้หน่วยงานเทคโนโลยีสารสนเทศเป็นผู้ประเมินหลัก อย่างไรก็ตาม อาจมีบางคำถามที่หน่วยงานที่เกี่ยวข้องอื่น ๆ ต้องเป็นผู้ให้ข้อมูล เช่น หน่วยงานความเสี่ยง หน่วยงานตรวจสอบ หน่วยงานทรัพยากรบุคคล เป็นต้น **ถาม:** การลงนามอนุมัติแบบประเมิน และการจัดส่งมายังสำนักงาน คปภ. มีวิธีการอย่างไร **ตอบ:** สามารถดำเนินการได้ใน 2 รูปแบบ คือ • พิมพ์หน้าหนังสือนำส่งให้ผู้มีอำนาจลงนาม จากนั้นสแกนเป็นรูปภาพหรือ PDF กลับมายังสำนักงาน พร้อมไฟล์ Excel ที่กรอกแบบประเมินครบถ้วน • นำส่งไฟล์หน้าหนังสือนำส่งให้ผู้มีอำนาจลงนามบนหน้าจอแท็บเล็ต จากนั้น นำหน้าที่ลงนามเรียบร้อยแล้วส่งกลับมายังสำนักงาน พร้อมไฟล์ Excel ที่กรอกแบบประเมินครบถ้วน ทั้งนี้ ไม่สามารถใช้อีเมลเป็นหลักฐานการอนุมัติได้ **ถาม:** แบบประเมิน CRAF สามารถใส่ผู้สอบทาน 2 ท่านได้หรือไม่ **ตอบ:** สามารถทำได้ เนื่องจากข้อกำหนดขั้นต่ำคือ 1 ท่าน โดยบริษัทสามารถเพิ่มบรรทัด (Row) ในหนังสือนำส่ง และใส่ข้อมูลเพิ่มเติมได้เอง **ถาม:** กรรมการผู้มีอำนาจลงนามต้องมีกี่ท่าน สามารถลงนามเพียง 1 ท่านตามแบบฟอร์มได้หรือไม่ **ตอบ:** ผู้ลงนามคือ คณะกรรมการผู้มีอำนาจลงนามของบริษัท จึงขึ้นอยู่กับแต่ละบริษัทว่ากำหนดให้มีคณะกรรมการผู้มีอำนาจลงนามกี่ท่าน **ถาม:** หนังสือนำส่งต้องประทับตราบริษัทด้วยหรือไม่ **ตอบ:** ประทับตราหรือไม่ก็ได้ แต่ต้องลงนามโดยกรรมการผู้มีอำนาจเท่านั้น

ข้อ	เรื่อง	ถาม - ตอบ
		ถาม: ต้องระบุเลขที่หนังสือของบริษัทหรือไม่ **ตอบ:** ตามแบบประเมินไม่ได้กำหนดหรือบังคับ แต่ถ้าทางบริษัทระบุเลขที่หนังสือก็สามารถทำได้ **ถาม:** ใช้ลายเซ็นเป็นรูปภาพได้หรือไม่ **ตอบ:** ขอความกรุณาลงลายมือชื่อจริง (ไม่ใช้รูปลายเซ็นแปะลงบนเอกสาร) เพื่อแสดงว่ากรรมการผู้มีอำนาจ ได้รับทราบและพิจารณาก่อนนำส่งมายังสำนักงาน คปภ. **ถาม:** ผู้ประเมินจำเป็นต้องเป็นผู้เชี่ยวชาญด้าน IT หรือไม่ **ตอบ:** ไม่จำเป็น แต่ควรพิจารณาให้ผู้ประเมิน ควรเป็นบุคคลที่มีความรู้ความเข้าใจในปัจจัยความเสี่ยง และการควบคุมทางด้านสารสนเทศของบริษัท เพื่อให้สามารถสืบค้นข้อมูลเพื่อทำการประเมินตามแบบประเมินได้ **ถาม:** กรณีให้ IT Outsource เป็นผู้ประเมิน ต้องระบุชื่อ ตำแหน่ง และอีเมลด้วยหรือไม่ **ตอบ:** ในกรณีที่เป็นการจ้าง IT Outsource เพื่อทำแบบประเมินนี้ สามารถใส่ชื่อ IT Outsource เป็นผู้ประเมินได้ เพื่อให้ทราบว่าผู้ใดทำแบบประเมินนี้ อย่างไรก็ตาม แบบประเมินต้องมีการสอบทานความถูกต้องโดยผู้สอบทานของบริษัทอีกครั้ง **ถาม:** ผู้ประเมินและผู้สอบทาน เป็นคนเดียวกันได้หรือไม่ **ตอบ:** ในกรณีที่มีการคาบเกี่ยวกันระหว่างหน้าที่ของผู้สอบทานและผู้ประเมิน บริษัทสามารถใส่ชื่อบุคลากรเป็นทั้งผู้สอบทานและผู้ประเมิน ซึ่งเป็นเรื่องที่เกิดขึ้นได้ หากมีผู้สอบทานและผู้ประเมินหลายท่าน <u>แต่ไม่ควรเป็นลักษณะที่บริษัทดำเนินการทั้งสอบทานและประเมินโดยบุคลากรเพียง 1 ท่าน</u>
2	การประเมินระดับความเสี่ยงสืบเนื่อง	**ถาม:** การประเมินระดับความเสี่ยงสืบเนื่องตามกรอบ CRAF ทดแทนการประเมินความเสี่ยงทางด้านสารสนเทศ ได้หรือไม่ **ตอบ:** ทดแทนกันไม่ได้ เนื่องจาก การประเมินความเสี่ยงสืบเนื่องตามกรอบ CRAF มีวัตถุประสงค์เพื่อประเมินความเสี่ยงสืบเนื่องและจัดกลุ่มตามระดับความเสี่ยงในทั้งภาคอุตสาหกรรม โดย • ตัวชี้วัดจะเป็นปัจจัยเสี่ยงโดยภาพรวมของทั้งธุรกิจ • แบ่งกลุ่มความเสี่ยงโดยเปรียบเทียบระหว่างบริษัทในกลุ่มธุรกิจเดียวกัน

ข้อ	เรื่อง	ถาม - ตอบ
		แต่การประเมินความเสี่ยงของบริษัทโดยส่วนใหญ่จะพิจารณาทั้งความเสี่ยงสืบเนื่อง (Inherent Risk) และความเสี่ยงภายหลังการควบคุม (Residual Risk) รวมทั้ง การประเมินความเสี่ยงทางด้านสารสนเทศ หรือไซเบอร์ของบริษัท จะมีตัวบ่งชี้และเกณฑ์การประเมินที่อ้างอิงจากกลยุทธ์ Risk Appetite (ระดับความเสี่ยงที่ยอมรับได้) และมีลักษณะเฉพาะเจาะจงสำหรับแต่ละบริษัท อย่างไรก็ดี การประเมินความเสี่ยงทั้ง 2 แบบนี้ สามารถนำมาเป็นแนวทางเพื่อการบริหารจัดการความเสี่ยง และจัดให้มีการควบคุมที่เหมาะสมของแต่ละบริษัทได้
3	CRAF Alignment	**ถาม:** อยากเสนอให้สำนักงาน คปภ. นำผลการประเมิน CRAF แจ้งไปทาง ก.ล.ต. เพื่อลดความซ้ำซ้อนในการทำแบบประเมิน CRAF **ตอบ:** สำนักงาน คปภ. คำนึงถึงภาระที่เพิ่มขึ้นของบริษัท และต้องการลดความซ้ำซ้อน จึงมีแนวทางในการจัดทำกรอบ CRAF ให้สอดคล้องกับหน่วยงานกำกับดูแลอื่น ทั้งนี้ การแบ่งปันข้อมูลระหว่างหน่วยงานกำกับดูแลอยู่ในขั้นตอนการพิจารณาและหารือร่วมกับสำนักงาน ก.ล.ต. ต่อไป
4	ความเกี่ยวข้องระหว่างกรอบ CRAF, IT Audit และประกาศของสำนักงาน	**ถาม:** CRAF มีความเกี่ยวข้องอย่างไรกับงาน IT Audit และ ประกาศความเสี่ยงทางด้านเทคโนโลยีของสำนักงาน คปภ. **ตอบ:** เป้าหมายในการจัดทำกรอบ CRAF คือ การประเมินระดับความเสี่ยงสืบเนื่องและระดับการควบคุมของบริษัท โดยเป็นการประเมินด้วยตนเอง (Self-assessment) ในขณะที่งาน IT Audit เป็นงานที่มุ่งเน้นการตรวจสอบเพื่อให้ความมั่นใจถึงการปฏิบัติตามประกาศของสำนักงาน อย่างไรก็ตาม การควบคุมในแบบประเมิน CRAF ระดับ Baseline และ การควบคุมตามคู่มือ IT Audit อ้างอิงจากแหล่งเดียวกัน นั่นคือ ประกาศความเสี่ยงทางด้านเทคโนโลยีของสำนักงาน คปภ. ดังแสดงในแผนภาพด้านล่าง

<table>
<tr><th>ข้อ</th><th>เรื่อง</th><th>ถาม - ตอบ</th></tr>
<tr><td></td><td></td><td>
ความเชื่อมโยง


ความเหมือน

พัฒนาโดยอ้างอิงจากประกาศ และ แนวปฏิบัติของสำนักงาน คปภ.
ดำเนินการปีละ 1 ครั้ง

ความต่าง
<table>
<tr><th>CRAF</th><th>IT audit</th></tr>
<tr><td>Self-Assessment ที่ดำเนินการโดย Process owner
เป็นการประเมินการจัดให้มีการควบคุมในปัจจุบัน
มุ่งเน้นให้บริษัทมีการควบคุมที่สอดคล้องกับระดับความเสี่ยงสืบเนื่อง โดยบริษัทสามารถนำไปวางแผนการพัฒนาการควบคุมให้เหมาะสมกับระดับความเสี่ยงสืบเนื่อง</td><td>Assurance report ที่ดำเนินงานโดย Independent Auditor
เป็นการประเมินการปฏิบัติการควบคุมย้อนหลังเป็นระยะเวลา 1 ปี
มุ่งเน้นให้บริษัทมีการควบคุมตามที่ประกาศกำหนด โดยบริษัทควรต้องปรับปรุงการควบคุมให้เป็นไปตามที่ประกาศกำหนด</td></tr>
</table>
</td></tr>
<tr><td>5</td><td>การประเมิน และ กรอบระยะเวลา</td><td>
ถาม: สำนักงาน คปภ. สามารถกำหนดเวลาส่งแบบประเมิน CRAF และ IT Audit ให้เป็นเวลาเดียวกันหรือใกล้เคียงกันได้หรือไม่ เนื่องจากมีคำถามบางข้อเหมือนกัน จะได้ไม่เป็นการทำงานที่ซ้ำซ้อนถึง 2 รอบ
ตอบ: เนื่องจากปีนี้ ทางสำนักงานดำเนินการประเมิน CRAF เป็นปีแรก จึงยังไม่ได้กำหนดให้มีการส่งในช่วงเวลาเดียวกับ IT Audit แต่ในปีถัดไป สำนักงานอาจมีการปรับให้เป็นช่วงเวลาเดียวกัน

ถาม: จะมีการจัดทำแบบประเมินเป็นภาษาอังกฤษหรือไม่
ตอบ: ในปัจจุบัน ยังไม่มีการจัดทำแบบประเมินเป็นภาษาอังกฤษ

ถาม: เนื่องจากข้อมูลบางส่วนเป็นข้อมูลเชิงลึกที่บริษัทมีข้อจำกัดในการส่ง ทางสำนักงาน คปภ. มีแนวทางแก้ไขปัญหานี้อย่างไร
ตอบ: บริษัทสามารถติดต่อสำนักงาน คปภ. เพื่อปรึกษาปัญหาในส่วนของข้อมูลความลับเป็นรายกรณี โดยทางสำนักงานอาจให้ความช่วยเหลือในการหาทางออกเพิ่มเติม
</td></tr>
</table>

ข้อ	เรื่อง	ถาม - ตอบ
		ถาม: ในกรณีที่บริษัทต้องการนำแบบประเมินไปแปลเป็นภาษาอังกฤษ บริษัทสามารถขอแบบประเมินในรูปแบบไฟล์ที่แก้ไขได้ (Editable File) ล่วงหน้าได้หรือไม่ **ตอบ:** บริษัทสามารถติดต่อมายังสำนักงาน คปภ. เพื่อให้จัดส่ง Editable File เป็นรายบริษัท เนื่องจากไฟล์แบบประเมินจะมีการล็อกเซลล์เพียงบางส่วนที่จำเป็นเพื่อป้องกันความคลาดเคลื่อนของข้อมูล **ถาม:** บริษัทจะต้องส่งแบบประเมินเมื่อไร เอกสารที่ต้องนำส่งมีอะไรบ้าง และเงื่อนไขการประเมินเป็นอย่างไร **ตอบ:** สำนักงานจะจัดส่งหนังสือเกี่ยวกับการประเมินตามกรอบ CRAF ไปยังกรรมการผู้จัดการของบริษัท พร้อมกันนี้ จะมีหนังสือนำส่งที่ระบุกำหนดการจัดส่งแบบประเมินกลับมายังสำนักงาน โดยในการประเมินตามกรอบ CRAF นี้เป็นการประเมินตนเอง บริษัทจึงไม่ต้องมีเอกสารหลักฐานประกอบเหมือนการทำ IT Audit และในส่วนของกรอบระยะเวลาในเบื้องต้น สำนักงานจะให้เวลาบริษัททำแบบประเมินประมาณ 2 เดือน นั่นคือ ช่วงเดือนมิถุนายน ถึง กรกฎาคม **ถาม:** สามารถส่งแบบประเมินล่าช้า หรือ ไม่ส่งแบบประเมินได้หรือไม่ **ตอบ:** ในกรณีที่บริษัทมีข้อติดขัดหรือความจำเป็นที่ทำให้ต้องส่งแบบประเมินล่าช้า หรือไม่สามารถส่งแบบประเมินได้ บริษัทสามารถแจ้งต่อสำนักงาน คปภ. พร้อมให้เหตุผลเป็นรายกรณี **ถาม:** บริษัทจะต้องประเมินเป็นประจำทุกปีหรือไม่ **ตอบ:** ในเบื้องต้นจะมีการประเมินเป็นประจำทุกปี แต่ช่วงเวลาจะมีการพิจารณาให้สอดคล้องกับ IT Audit **ถาม:** หากระหว่างการประเมินบริษัทมีข้อสงสัย สามารถสอบถามผ่านช่องทางใด **ตอบ:** สามารถสอบถามทางอีเมล itriskmgt@oic.or.th
6	การสื่อสารผลการประเมิน	**ถาม:** หลังจากสำนักงาน คปภ. รวบรวมข้อมูลการประเมินเรียบร้อยแล้ว จะมีการแบ่งปันผลการประเมินในภาพรวมของอุตสาหกรรมแก่บริษัทประกันหรือไม่ เมื่อใด **ตอบ:** เบื้องต้นทางสำนักงานอาจขอพิจารณาผลในภาพรวมก่อน จากนั้นจึงพิจารณาการแบ่งปันผลดังกล่าว ซึ่งอาจเป็นช่วงไตรมาส 3 หรือไตรมาส 4

<table>
<tr><th>ข้อ</th><th>เรื่อง</th><th>ถาม - ตอบ</th></tr>
<tr><td>7</td><td>การคำนวณผลระดับความเสี่ยงสืบเนื่อง</td><td>
ถาม: ขอทราบตัวอย่างการคำนวณผลระดับความเสี่ยงสืบเนื่อง
ตอบ: ตัวอย่างวิธีการคำนวณ มีดังนี้
1. แทนค่าความเสี่ยงรายปัจจัยโดย
• สูง = 3
• ปานกลาง = 2
• ต่ำ = 1
เช่น ความเสี่ยงสืบเนื่องในมุมมอง IR3 ลักษณะผลิตภัณฑ์และการให้บริการ (Products & Technology Services) ที่มีปัจจัยเสี่ยงทั้งหมด 6 ข้อ มีผลการประเมินดังนี้
<table>
<tr><th colspan="2">ปัจจัยเสี่ยง</th><th>ผลการประเมินระดับความเสี่ยง</th><th>แทนค่า</th></tr>
<tr><td>3.1.1</td><td>ร้อยละของจำนวนกรมธรรม์ทั้งหมดที่มีการซื้อขายผ่านระบบ Online (ในรอบระยะเวลาตั้งแต่วันที่ 1 ม.ค. - 31 ธ.ค. 2564)</td><td>ปานกลาง</td><td>2</td></tr>
<tr><td>3.1.2</td><td>ร้อยละของมูลค่ากรมธรรม์ (Sum Insured) ทั้งหมดที่มีการซื้อขายผ่านระบบ Online (ในรอบระยะเวลาตั้งแต่วันที่ 1 ม.ค. - 31 ธ.ค. 2564)</td><td>ปานกลาง</td><td>2</td></tr>
<tr><td>3.1.3</td><td>ร้อยละของจำนวนรายการ Claim ทั้งหมดที่มีการร้องขอผ่านระบบ Online (ในรอบระยะเวลาตั้งแต่วันที่ 1 ม.ค. - 31 ธ.ค. 2564)</td><td>ปานกลาง</td><td>2</td></tr>
<tr><td>3.1.4</td><td>ร้อยละของมูลค่ารายการ Claim ทั้งหมดที่มีการร้องขอผ่านระบบ Online (ในรอบระยะเวลาตั้งแต่วันที่ 1 ม.ค. - 31 ธ.ค. 2564)</td><td>ต่ำ</td><td>1</td></tr>
<tr><td>3.1.5</td><td>การให้บริการผลิตภัณฑ์อื่น ๆ ผ่าน Website/Mobile Application ของบริษัท (นอกเหนือจากผลิตภัณฑ์หลักของบริษัท)</td><td>สูง</td><td>3</td></tr>
<tr><td>3.1.6</td><td>จำนวนเทคโนโลยีใหม่ที่บริษัทนำมาใช้เป็นครั้งแรก ในรอบ 12 เดือน</td><td>ต่ำ</td><td>1</td></tr>
<tr><td colspan="2"></td><td>มีค่ารวม</td><td>11</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>ข้อ</th><th>เรื่อง</th><th>ถาม - ตอบ</th></tr>
<tr><td></td><td></td><td>
2. หาค่าเฉลี่ย (Average) ของแต่ละหมวดหมู่ปัจจัยเสี่ยงโดย

สูง = ค่าเฉลี่ยมากกว่า 2.33
ปานกลาง = ค่าเฉลี่ยระหว่าง 1.67 - 2.33
ต่ำ = ค่าเฉลี่ยต่ำกว่า 1.67

เช่น จากความเสี่ยงสืบเนื่องในมุมมอง IR3 ที่มีค่ารวม 11 จาก 6 ปัจจัยเสี่ยงข้างต้น จะมีค่าเฉลี่ย 1.83 ทำให้ความเสี่ยงสืบเนื่องในมุมมอง IR3 นี้ อยู่ในระดับความเสี่ยง “ปานกลาง”
3. แทนค่ารายมุมมองความเสี่ยงสืบเนื่อง โดย

สูง = 3
ปานกลาง = 2
ต่ำ = 1

เช่น
<table>
<tr><th>มุมมองความเสี่ยงสืบเนื่อง</th><th>ระดับความเสี่ยงสืบเนื่อง</th><th>แทนค่า</th></tr>
<tr><td>1 เทคโนโลยีและการเชื่อมต่อ</td><td>สูง</td><td>3</td></tr>
<tr><td>2 ช่องทางการให้บริการ</td><td>ปานกลาง</td><td>2</td></tr>
<tr><td>3 ลักษณะผลิตภัณฑ์และการให้บริการ</td><td>ปานกลาง</td><td>2</td></tr>
<tr><td>4 ขนาด และลักษณะเฉพาะขององค์กร</td><td>ปานกลาง</td><td>2</td></tr>
<tr><td>5 ประวัติการถูกคุกคามทางไซเบอร์</td><td>สูง</td><td>3</td></tr>
</table>
4. นำค่าความเสี่ยงรายหมวดหมู่มาถ่วงน้ำหนัก เช่น
<table>
<tr><th>มุมมองความเสี่ยงสืบเนื่อง</th><th>ระดับความเสี่ยงสืบเนื่อง</th><th>แทนค่า</th><th>ถ่วงน้ำหนัก</th><th>คะแนนรวม</th></tr>
<tr><td>1 เทคโนโลยีและการเชื่อมต่อ</td><td>สูง</td><td>3</td><td>25%</td><td>0.75 (=3 x 0.25)</td></tr>
<tr><td>2 ช่องทางการให้บริการ</td><td>ปานกลาง</td><td>2</td><td>25%</td><td>0.50 (=2 x 0.25)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>ข้อ</th><th>เรื่อง</th><th>ถาม - ตอบ</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>3 ลักษณะผลิตภัณฑ์และการให้บริการ</td><td>ปานกลาง</td><td>2</td><td>20%</td><td>0.40 (=2 x 0.20)</td></tr>
<tr><td>4 ขนาด และลักษณะเฉพาะขององค์กร</td><td>ปานกลาง</td><td>2</td><td>15%</td><td>0.30 (=2 x 0.15)</td></tr>
<tr><td>5 ประวัติการถูกคุกคามทางไซเบอร์</td><td>สูง</td><td>3</td><td>15%</td><td>0.45 (=3 x 0.15)</td></tr>
<tr><td colspan="4">รวม ค่าเฉลี่ย</td><td>2.4</td></tr>
</table>
5. หาค่าเฉลี่ย (Average) ความเสี่ยงรวมของบริษัทโดย
• สูง = ค่าเฉลี่ยมากกว่า 2.33
• ปานกลาง = ค่าเฉลี่ยระหว่าง 1.67 - 2.33
• ต่ำ = ค่าเฉลี่ยต่ำกว่า 1.67
จากตัวอย่าง บริษัทอยู่ในระดับความเสี่ยง “สูง”
</td></tr>
<tr><td>8</td><td>การคำนวณผลระดับการควบคุม</td><td>
ถาม: ขอทราบตัวอย่างการคำนวณผลระดับการควบคุม
ตอบ: ตัวอย่างวิธีการคำนวณ มีดังนี้
1. กำหนดคะแนนของคำตอบในแต่ละข้อการควบคุม โดย
• Yes - 1 คะแนน
• Partial - 0.5 คะแนน
• No - 0 คะแนน
• N/A - ตัดออกจากการคำนวณ
เช่น บริษัทมีผลการประเมินในหมวดหมู่ CM2 การระบุความเสี่ยง (Identification) ที่มีการควบคุมทั้งหมด 19 ข้อ ประกอบด้วย
• การควบคุมในระดับ Baseline 9 ข้อ
• การควบคุมในระดับ Intermediate 7 ข้อ
• การควบคุมในระดับ Advance 3 ข้อ
ดังนี้
<table>
<tr><th>คำตอบการควบคุมในแต่ละระดับ</th><th>ค่ารวมคะแนนการควบคุมในแต่ละระดับ</th></tr>
<tr><td>การควบคุมในระดับ Baseline 9 ข้อ มีคำตอบ</td><td>รวม 8 คะแนน จากการควบคุม 8 ข้อ ได้แก่</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>ข้อ</th><th>เรื่อง</th><th>ถาม - ตอบ</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>• Yes 8 ข้อ
• N/A 1 ข้อ</td><td>• คำตอบ Yes 8 ข้อ ได้ 8 คะแนน (= 8 x 1)
• ตัด N/A 1 ข้อ ออกจากการคำนวณ</td></tr>
<tr><td>การควบคุมในระดับ Intermediate 7 ข้อ มีคำตอบ
• Yes 3 ข้อ
• Partial 1 ข้อ
• No 3 ข้อ</td><td>รวม 3.5 คะแนน จากการควบคุม 7 ข้อ ได้แก่
• คำตอบ Yes 3 ข้อ ได้ 3 คะแนน (= 3 x 1)
• คำตอบ Partial 1 ข้อ ได้ 0.5 คะแนน (= 1 x 0.5)
• คำตอบ No 3 ข้อ ได้ 0 คะแนน (= 3 x 0)</td></tr>
<tr><td>การควบคุมในระดับ Advance 3 ข้อ มีคำตอบ
• Yes 1 ข้อ
• Partial 1 ข้อ
• No 1 ข้อ</td><td>รวม 1.5 คะแนน จากการควบคุม 3 ข้อ ได้แก่
• คำตอบ Yes 1 ข้อ ได้ 1 คะแนน (= 1 x 1)
• คำตอบ Partial 1 ข้อ ได้ 0.5 คะแนน (= 1 x 0.5)
• คำตอบ No 1 ข้อ ได้ 0 คะแนน (= 1 x 0)</td></tr>
</table>
2. คำนวณระดับการควบคุมในแต่ละหมวดหมู่การควบคุม จากร้อยละของคะแนนการควบคุมในการควบคุมแต่ละระดับ เช่น
<table>
<tr><th>ระดับการควบคุม</th><th>ร้อยละของคะแนนการควบคุม</th></tr>
<tr><td>Baseline</td><td>100% (8 คะแนน จากการควบคุม 8 ข้อ)</td></tr>
<tr><td>Intermediate</td><td>50% (3.5 คะแนน จากการควบคุม 7 ข้อ)</td></tr>
<tr><td>Advance</td><td>50% (1.5 คะแนน จากการควบคุม 3 ข้อ)</td></tr>
</table>
โดยบริษัทจะต้องได้ 100 % ในระดับการควบคุมนั้น และ ระดับการควบคุมที่ต่ำกว่า จึงจะถือว่าอยู่ในระดับการควบคุมนั้น
จากตัวอย่าง จึงสรุปได้ว่าระดับการควบคุมของบริษัทในหมวดหมู่ CM2 นี้ อยู่ในระดับ “Baseline”
3. คำนวณระดับการควบคุมภาพรวม จากร้อยละของคะแนนการควบคุมทั้งหมด (โดยไม่แยกนับตามกลุ่มการควบคุม) เช่น
<table>
<tr><th>คำตอบการควบคุมในแต่ละระดับ
(จากทุกหมวดหมู่)</th><th>ค่ารวมคะแนนการควบคุม
ในแต่ละระดับ</th><th>ร้อยละ</th></tr>
<tr><td>การควบคุมในระดับ Baseline 106 ข้อ มีคำตอบ
• Yes 100 ข้อ
• No 4 ข้อ</td><td>รวม 100 คะแนน จากการควบคุม 104 ข้อ ได้แก่
• คำตอบ Yes 100 ข้อ ได้ 100 คะแนน (= 100 x 1)
• คำตอบ No 4 ข้อ ได้ 0 คะแนน (= 4 x 0)</td><td>96%</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>ข้อ</th><th>เรื่อง</th><th>ถาม - ตอบ</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>• N/A 2 ข้อ</td><td>• ตัด N/A 2 ข้อ ออกจากการคำนวณ</td><td></td></tr>
<tr><td>การควบคุมในระดับ Intermediate 90 ข้อ มีคำตอบ
• Yes 50 ข้อ
• Partial 15 ข้อ
• No 25 ข้อ</td><td>รวม 57.5 คะแนน จากการควบคุม 90 ข้อ ได้แก่
• คำตอบ Yes 50 ข้อ ได้ 50 คะแนน (= 50 x 1)
• คำตอบ Partial 15 ข้อ ได้ 7.5 คะแนน (= 15 x 0.5)
• คำตอบ No 25 ข้อ ได้ 0 คะแนน (= 25 x 0)</td><td>64%</td></tr>
<tr><td>การควบคุมในระดับ Advance 42 ข้อ มีคำตอบ
• Yes 15 ข้อ
• Partial 10 ข้อ
• No 17 ข้อ</td><td>รวม 20 คะแนน จากการควบคุม 42 ข้อ ได้แก่
• คำตอบ Yes 15 ข้อ ได้ 15 คะแนน (= 15 x 1)
• คำตอบ Partial 10 ข้อ ได้ 5 คะแนน (= 10 x 0.5)
• คำตอบ No 17 ข้อ ได้ 0 คะแนน (= 17 x 0)</td><td>48%</td></tr>
<tr><td colspan="3">จากตัวอย่าง เนื่องจากบริษัทยังไม่ได้ 100 % ในระดับการควบคุม Baseline จึงสรุปได้ว่าระดับการควบคุมในภาพรวมของบริษัทอยู่ในระดับ “Below Baseline”</td></tr>
</table>
</td></tr>
</table>

คำถามเกี่ยวกับแบบประเมินระดับความเสี่ยงสืบเนื่อง (Inherent Risk: IR)

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
IR 1. เทคโนโลยีและการเชื่อมต่อ (Technologies and Connection)			
1.1.1	จำนวน Internet Service Provider (ISP) ที่เชื่อมต่อกับระบบเครือข่ายของบริษัท	จำนวน ISP	**ถาม:** ถ้าบริษัทมีการแบ่งแยก ISP ของบริษัท และ บุคคลภายนอก จะต้องนับการแบ่งแยกระบบเครือข่ายอย่างไร และการแยก ISP ลักษณะนี้ จะทำให้จำนวน ISP เพิ่มมากขึ้น และเป็นการเพิ่มความเสี่ยงของบริษัทหรือไม่ **ตอบ:** ในกรณีที่มีการแบ่งแยก ISP ของบริษัท และ บุคคลภายนอก ให้นับระบบเครือข่ายโดยใช้เกณฑ์การแยกระบบเครือข่ายทาง Physical ซึ่งการแยกในลักษณะนี้อาจทำให้บริษัทมีจำนวน ISP เพิ่มขึ้น ส่งผลให้บริษัทมีความเสี่ยงในข้อของ ISP มากขึ้น
1.3.1	ลักษณะการเข้าถึงเครือข่ายของบริษัท ของเจ้าหน้าที่ของบริษัท และ บุคคลภายนอกที่มาปฏิบัติงานในพื้นที่ของบริษัท	ลักษณะการเข้าถึง	**ถาม:** อยากให้สำนักงานระบุให้ชัดเจนว่า การเข้าถึงเครือข่ายของบริษัท ไม่เกี่ยวข้องกับระบบงานใดบ้าง **ตอบ:** ในเอกสารแบบประเมินจะมีคำอธิบายเพิ่มเติมถึงขอบเขตและวิธีการประเมิน โดยในข้อ 1.3 นี้ จะเป็นการเข้าถึงเครือข่ายของบริษัทจากภายในพื้นที่ของบริษัท **ถาม:** ข้อนี้ระบุถึงการเข้าถึงผ่าน VPN หรือไม่ **ตอบ:** ข้อนี้จะระบุถึงการเข้าถึงเครือข่ายของบริษัทจากภายในพื้นที่ของบริษัทเท่านั้น ไม่นับรวม VPN
1.4.1	อุปกรณ์เคลื่อนที่ส่วนบุคคลของพนักงาน (BYOD) ที่อนุญาตให้ใช้เพื่อเข้าถึงระบบเครือข่ายของบริษัท เช่น Mobile with push mail, laptop/PC, Removable storage และอื่นๆ	จำนวน พนักงาน	**ถาม:** หากอนุญาตให้พนักงานทุกคนเข้าระบบอีเมลได้ แต่ไม่สามารถเข้าระบบอื่น ๆ ได้ ต้องตอบแบบประเมินอย่างไร **ตอบ:** ในข้อ 1.4.1 เรื่องการนับจำนวนการเข้าถึงโดย BYOD จะครอบคลุมถึง Mobile with push mail ด้วย ดังนั้นจึงให้ตอบด้วยจำนวนพนักงานทั้งหมดที่สามารถเข้าถึงระบบอีเมลได้ ในข้อ 1.4.2 เรื่องระบบงานสำคัญที่สามารถเข้าถึงผ่าน BYOD ได้ ให้พิจารณาเพิ่มเติมว่าหากบริษัทประกันภัยไม่มีการใช้ระบบอีเมลเพื่อให้บริการประกันภัยที่มีข้อมูลส่วนบุคคลของ

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ลูกค้า เช่น ไม่มีการส่ง E-Policy หรือ E-invoice ผ่านอีเมล อาจไม่นับว่าระบบอีเมล เป็นระบบงานสำคัญที่อนุญาตให้ใช้ผ่าน BYOD **ถาม:** หาก ณ ช่วงที่ต้องกรอกข้อมูลกลับ อยู่ในช่วงระหว่างยกเลิกสิทธิการ Mobile Push mail จะต้องกรอกข้อมูลกลับในรูปแบบใด **ตอบ:** ให้กรอกข้อมูล ณ ปัจจุบัน หากมีการยกเลิกสิทธิแต่ยังดำเนินการไม่เสร็จสิ้น จะถือว่ายังมีการใช้งานอยู่ **ถาม:** บริษัทมีระบบเดียวที่ให้เข้าผ่าน BYOD คือ ระบบอีเมลของบริษัท นอกนั้นถือเป็นการเข้าถึงผ่าน Internet หรือ Web browser ซึ่งลักษณะการเข้าถึงด้วย Web browser นี้ นับเป็นการใช้งาน BYOD ด้วยหรือไม่ **ตอบ:** การนับระบบงานที่ใช้งาน BYOD ให้นับตามวัตถุประสงค์การเข้าถึงผ่าน BYOD ว่าระบบงานนั้นๆ ถูกออกแบบมาเพื่อการเข้าถึงโดย BYOD หรือไม่ อาทิ ถ้าเป็น Mobile push mail ก็สมควรนับเป็นระบบงานที่ใช้งาน BYOD แต่ถ้าเป็นการเข้าถึงด้วย Web browser ก็ไม่ควรนับ
1.5.1	จำนวนระบบงานสำคัญทั้งหมด	จำนวน ระบบงาน	**ถาม:** หากระบบอีเมลที่ใช้งานได้แยก Domain และ SMTP ออกจากกัน ระหว่าง corporate (สำหรับพนักงานบริษัท) กับ Domain เพื่อทำการส่งกรมธรรม์ให้กับลูกค้า ระบบที่อยู่ในขอบเขตจะมีเพียง Domain ที่ทำธุรกรรมในการส่ง policy ให้กับลูกค้าใช่หรือไม่ **ตอบ:** ใช่ ระบบที่จัดอยู่ในขอบเขตจะมีเพียงระบบที่ทำธุรกรรมให้ลูกค้าเท่านั้น **ถาม:** มีการพิจารณาอย่างไรว่าเป็นระบบงานสำคัญในกลุ่มของ Infrastructure เช่น AD จัดว่าเป็นระบบงานสำคัญหรือไม่

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ตอบ: ถ้าเป็น Core Application สำหรับการดำเนินธุรกิจในกิจกรรมหลัก 8 ด้าน จะจัดว่าเป็นระบบงานสำคัญ ในส่วนของ Infrastructure เช่น AD และ Network ไม่นับเป็นระบบงานหรือ Application software แต่จะอยู่ในส่วนของระบบสารสนเทศที่สนับสนุนระบบสำคัญ **ถาม:** สามารถนับระบบอีเมลเป็นระบบงานสำคัญของบริษัทได้หรือไม่ **ตอบ**: อ้างอิงจากคำจำกัดความของระบบงานสำคัญ หากพิจารณาแล้วเห็นว่าระบบอีเมลนั้นใช้เพื่อการจัดส่งกรมธรรม์ การเรียกร้องค่าสินไหมทดแทน (Claim) หรือการให้บริการกิจกรรมประกันภัยของบริษัท ให้นับระบบอีเมลว่าเป็นระบบงานสำคัญ **ถาม:** ในกรณีที่ใช้อีเมลส่งกรมธรรม์โดยตรงผ่าน Gateway ระบบอีเมลในที่นี้ไม่นับเป็นระบบงานสำคัญที่ใช้ผ่าน BYOD ใช่หรือไม่ **ตอบ**: ในกรณีที่การส่งกรรมธรรม์เป็นการส่งตรงผ่าน Gateway ส่งผลให้ระบบอีเมลใช้เพื่อการสื่อสารภายในบริษัทเท่านั้น สามารถไม่รวมระบบอีเมลดังกล่าวเป็นระบบงานสำคัญได้ **ถาม:** ระบบ Outlook via Mobile ที่มีการ sync ผ่าน MDM นับเป็นการใช้งาน BYOD หรือไม่ **ตอบ**: นับ เนื่องจากเป็นระบบที่ใช้งานผ่าน Mobile device โดยเฉพาะ
1.6.1	จำนวน Public IP Addresses ของบริษัท ที่ให้บริการแบบ Unsecured Protocol เช่น FTP, Telnet, HTTP ผ่านเครือข่ายอินเทอร์เน็ต	จำนวน Public IP Addresses	**ถาม:** สำหรับ Public IP Address ที่ใช้งาน Unsecured Protocol หากแต่มีการล็อก Public IP Address แล้ว เช่น ล็อก Source IP และ Destination IP ต้องนับรวมด้วยหรือไม่ **ตอบ:** ให้นับรวมกรณีดังกล่าวด้วย เนื่องจากเป็นการพิจารณาความเสี่ยงโดยไม่รวมถึงการควบคุมที่บริษัทมี
1.6.2	จำนวนระบบปฏิบัติการ (Operating System : OS) และ Software ของระบบงานสำคัญที่	จำนวน OS หรือ Software	**ถาม:** ถ้ามีการใช้ Virtual Patch ให้ถือว่าไม่มีเครื่องที่ใช้ระบบปฏิบัติการ (OS) ที่ End-of-Support ใช่หรือไม่

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
	End-of-Life หรือ End-of-Support (รวมถึง open source)		**ตอบ:** ไม่ใช่ การประเมินความเสี่ยงสืบเนื่องจะยังไม่พิจารณาถึงการควบคุม ดังนั้น การใช้งาน Virtual Patch ซึ่งเป็นการควบคุมที่ดำเนินการโดยบริษัทเอง จะไม่นำมาพิจารณาร่วมด้วย เนื่องจากพื้นฐานของระบบดังกล่าวเป็นลักษณะ End-of-Life หรือ End-of-Support อยู่แล้ว **ถาม:** ระบบที่ไม่มีการประกาศ End-of-Life หรือ End-of-Support จากเจ้าของผลิตภัณฑ์ จะมีวิธีการพิจารณาอย่างไร **ตอบ:** ให้พิจารณาจากคำจำกัดความของ End-of-Life หรือ End-of-Support เป็นหลัก เช่น สำหรับ Software ที่พัฒนาขึ้นเอง หรือ จ้างพัฒนา ที่จะไม่มีการประกาศ End-of-Life หรือ End-of-Support ให้พิจารณาว่า หากบริษัทต้องการเปลี่ยนแปลงแก้ไขหรือมีความเสี่ยงเกิดขึ้น สามารถแก้ไข หรือ จัดหา Patch เพื่อปิดความเสี่ยงที่เกิดขึ้นได้หรือไม่ ซึ่งหากพิจารณาแล้วไม่สามารถดำเนินการได้ ให้จัดเป็น Software ประเภท End-of-Life และ End-of-Support
1.6.5	รูปแบบการใช้งานระบบคลาวด์ที่สนับสนุนระบบงานสำคัญ	รูปแบบการใช้งานระบบคลาวด์	**ถาม:** ถ้าบริษัทมีการใช้งานระบบคลาวด์ทั้ง 3 แบบ จะตอบแบบประเมินอย่างไร **ตอบ:** ถ้าบริษัทใช้งานระบบคลาวด์ทั้ง 3 แบบ ให้ตอบแบบที่มีความเสี่ยงสูงที่สุด นั่นคือ Public Cloud **ถาม:** ช่วยอธิบายเพิ่มเติมเกี่ยวกับ Hybrid Cloud **ตอบ:** Hybrid Cloud เป็นการใช้งานระบบคลาวด์แบบ Public Cloud ร่วมกับ Private Cloud ในหนึ่งระบบงาน ที่พบได้บ่อยจะเป็น O365 แบบ hybrid ที่มีการติดตั้ง Exchange server ที่ local เพื่อให้ Authentication ภายในบริษัท แต่ใช้งานระบบอีเมล บน Public Cloud **ถาม:** พิจารณาประเภทของ Managed Public Cloud อย่างไร เนื่องจากเป็น Public Cloud ที่มีการบริหารจัดการด้าน security เพิ่มเติมแล้ว

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ตอบ: เป็นรูปแบบ Public Cloud เนื่องจากการประเมินระดับความเสี่ยงสืบเนื่องเป็นการประเมินความเสี่ยงก่อนการควบคุม ดังนั้น แม้บริษัทจะมีการบริหารจัดการด้าน security เพิ่มเติม ตัวระบบยังคงเป็น Public Cloud **ถาม:** การใช้ Virtualization ของ VMware ถือว่าเป็น Private Cloud ด้วยหรือไม่ **ตอบ:** ระบบคลาวด์ จะพิจารณาจากระบบที่มีการเชื่อมต่อและเข้าถึงผ่านระบบ Internet ดังนั้นถ้าบริษัทใช้ VMware ภายใน Data Center ของบริษัทเอง ซึ่งไม่ใช่ Private Cloud ก็จะไม่นับว่า Data Center เป็นระบบคลาวด์ ในขณะเดียวกันถ้าบริษัทใช้งาน VMware บน Public Cloud ก็จัดว่าเป็น Public Cloud **ถาม:** ถ้าบริษัทใช้งานทั้ง Local Cloud ในประเทศ และ Azure กับ AWS ถือว่าเป็น Hybrid Cloud หรือไม่ **ตอบ:** Hybrid Cloud พิจารณาจากระบบคลาวด์ที่มีการใช้งานผสมผสานทั้ง Private และ Public Cloud ในระบบงานเดียว ทั้งนี้ ในกรณีที่บริษัทใช้งานระบบคลาวด์หลากหลาย แต่มีการแยกระบบงาน อาทิ ระบบ A บน Local Private Cloud และ ระบบ B อยู่บน AWS ที่เป็น Public Cloud ให้บริษัทตอบข้อนี้ว่าเป็น Public Cloud เนื่องจากมีความเสี่ยงสูงสุด **ถาม:** เหตุใด Public Cloud จึงมีความเสี่ยงสูง เนื่องจากในปัจจุบัน Public Cloud มีความปลอดภัยมากกว่าระบบที่ทางบริษัทจัดการด้วยตนเอง **ตอบ:** การพิจารณาว่า Public Cloud มีความปลอดภัยกว่าหรือไม่นั้น ขึ้นอยู่กับการควบคุมและบริหารจัดการด้านความมั่นคงปลอดภัยซึ่งเป็นการควบคุมของบริษัท ดังนั้น ในการประเมินความเสี่ยงสืบเนื่องจึงพิจารณาความเสี่ยงก่อนการควบคุมว่า ระบบ Public Cloud เพิ่ม

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ความเสี่ยง เนื่องจากเป็นช่องทางการเชื่อมต่อผ่าน Internet รวมทั้งเป็นการจัดเก็บระบบและข้อมูลไว้ที่ผู้ให้บริการภายนอก **ถาม:** ถ้ามองว่าระบบคลาวด์ที่บริหารจัดการโดยบุคคลภายนอกถือว่ามีความเสี่ยง แต่ในหัวข้อเรื่องอุปกรณ์เครือข่าย กำหนดให้นับรวมเฉพาะอุปกรณ์ที่บริหารจัดการโดยบริษัท ถือว่ามีความขัดแย้งกันเองหรือไม่ **ตอบ:** ในแบบประเมินนี้ ปัจจัยในแต่ละหมวดหมู่ แต่ละข้อ จะมีวัตถุประสงค์ในการวัดผลที่แตกต่างกันออกไป โดยในหัวข้อเรื่องคลาวด์ เป็นการวัดการใช้งานระบบคลาวด์ที่มีการบริหารจัดการโดยพึ่งพาผู้ให้บริการภายนอกที่แตกต่างกัน ซึ่งยิ่งระบบคลาวด์พึ่งพาผู้ให้บริการภายนอกมากเท่าไร ก็จะยิ่งมีความเสี่ยงในส่วนของการพึงพาผู้ให้บริการภายนอกและการบริหารจัดการ เช่นเดียวกับอุปกรณ์เครือข่ายที่มีปริมาณมาก บริษัทต้องอาศัยทรัพยากรที่เพิ่มขึ้นเพื่อการบริหารจัดการให้เหมาะสม รวมทั้งอุปกรณ์ที่มีปริมาณมากยิ่งเพิ่มโอกาสในการเข้าถือครองโดยผู้ไม่ประสงค์ดีโดยไม่ได้รับอนุญาต
IR 2. ช่องทางการให้บริการ (Delivery Channels)			
2.1.1	รูปแบบการให้บริการลูกค้าหรือผู้เอาประกันภัยผ่าน Website ของบริษัท	รูปแบบการให้บริการ	**ถาม:** ความหมายของความเสี่ยงระดับกลาง ที่ระบุว่า เป็นการให้ข้อมูลเพียงอย่างเดียว คืออะไร **ตอบ:** การให้ข้อมูลเพียงอย่างเดียว เป็นการให้ข้อมูลผลิตภัณฑ์หรือสินค้า หรือข้อมูลเกี่ยวกับการประกันภัยต่าง ๆ ซึ่งลูกค้าสามารถเข้ามาอ่านข้อมูลได้จาก Website, Mobile Application หรือ Social Media แต่ไม่สามารถทำธุรกรรมได้ เช่น ซื้อ-ขาย ดำเนินการเรื่องเคลม หรือ จ่ายค่าเบี้ยประกัน เป็นต้น

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ถาม: การเก็บเบี้ยประกันผ่านช่องทาง Payment Gateway ของบริษัทเอกชน หรือธนาคารจัดเป็นการทำธุรกรรมผ่านบุคคลที่สาม (Third Party) ด้วยหรือไม่ **ตอบ:** ถ้ารายการดังกล่าวทำผ่านเว็บไซต์ของบริษัท แล้วมีการ Redirect ไปยัง Payment Gateway ของธนาคารหรือบริษัทเอกชนเพื่อทำการจ่ายเงิน จะจัดว่าเป็นการทำธุรกรรมอยู่บนเว็บไซต์ของบริษัท แต่ถ้าลูกค้าโอนเงินผ่าน Application ของธนาคารโดยตรงและส่งหลักฐานมายังบริษัท กรณีนี้จะไม่เข้าข่ายและจัดว่าเป็นการดำเนินการแบบ Manual **ถาม:** Website ที่ให้ข้อมูลเกี่ยวกับบริษัท ช่องทางการติดต่อ และข้อมูลนักลงทุนสัมพันธ์ ที่ไม่มีการให้ข้อมูลผลิตภัณฑ์ใด ๆ ถือว่าเป็นการให้ข้อมูลหรือไม่ **ตอบ:** ไม่ เนื่องจากพิจารณาจากการให้ข้อมูลผลิตภัณฑ์ประกันภัยของบริษัทเป็นสำคัญ
2.1.5	รูปแบบการให้บริการลูกค้าหรือผู้เอาประกันภัยผ่าน Social Media หรือ Instant Messaging ของบริษัท (Official account)	รูปแบบการให้บริการ	**ถาม:** LINE Application หรือ Application ที่ใช้บน LINE platform ให้นับเป็น Mobile Application ด้วยหรือไม่ หรือว่าเป็น Official Social Media Account (บัญชีโซเชียลมีเดียอย่างเป็นทางการ) **ตอบ:** LINE Application นับเป็น Social Media ทั้งนี้ Social Media จะนับเฉพาะ Official Account เท่านั้น ในส่วนของการพิจารณาว่าเป็น Mobile Application หรือไม่ ให้พิจารณาเฉพาะที่สามารถดาวน์โหลดได้จาก Google Play หรือ App Store แต่หากใช้งานผ่าน Web Browser ให้จัดเป็น Website
2.1.8	จำนวนบุคคลหรือนิติบุคคลภายนอก (Third party) ที่ให้บริการลูกค้าหรือผู้เอาประกันภัยผ่านช่องทาง online อันได้แก่ Website, Mobile Application, Social Media หรือ Instant Messaging	จำนวน Third party (นับตาม legal entities)	**ถาม:** บริษัทประกันมีการส่งข้อมูลลูกค้าไปยัง Third party ที่เป็นบริษัทตรวจสอบข้อมูลผู้เอาประกัน โดยการตรวจสอบเป็นรูปแบบกระดาษเท่านั้น (manual) จัดว่าเข้าข่ายที่จะต้องระบุในแบบประเมิน CRAF หรือไม่ **ตอบ:** หากเป็นเพียงการส่งข้อมูลแบบ Manual Process จะไม่เข้าข่ายกรอบการประเมิน CRAF ในหัวข้อนี้ เนื่องจากหัวข้อนี้จะมุ่งเน้นที่ช่องทาง Online

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ถาม: กรณีดังต่อไปนี้ถือเป็น Third party หรือไม่ (1) Website และ Mobile Application ของตัวแทน (2) Website ที่บริษัททำให้ตัวแทนใช้ในการขายผลิตภัณฑ์ให้กับลูกค้า (ไม่ใช่ broker) (3) Web Application ที่ตัวแทนใช้งานเพื่อช่วยในการทำงาน เช่น ตรวจสอบงานที่นำส่ง กรมธรรม์ที่อนุมัติ เบี้ยครบกำหนดของลูกค้า เป็นต้น **ตอบ:** การจะระบุว่าเป็น Third party หรือไม่ ให้บริษัทพิจารณาจากการเข้าถึงของลูกค้าหรือผู้เอาประกันภัยเป็นสำคัญ กล่าวคือ ในกรณีที่เป็น Website และ Mobile Application ที่ตัวแทนใช้เพื่อการให้บริการผลิตภัณฑ์ของบริษัทแก่ลูกค้า โดยลูกค้าหรือผู้เอาประกันภัยสามารถเข้าถึงข้อมูลหรือทำรายการผ่านระบบนั้นโดยตรง ให้ถือเป็น Third party แต่ในกรณีที่ระบบงานของบริษัทใช้เพื่ออำนวยความสะดวกในการทำงานแก่ตัวแทน โดยที่ลูกค้าหรือผู้เอาประกันภัยไม่ได้เข้าถึงโดยตรง ไม่นับเป็น Third party
IR 3. ลักษณะผลิตภัณฑ์และการให้บริการ (Products & Technology Services)			
3.1.3	ร้อยละของจำนวนรายการ Claim ทั้งหมดที่มีการร้องขอผ่านระบบ Online (ในรอบระยะเวลาตั้งแต่วันที่ 1 ม.ค. - 31 ธ.ค. 2564)	ร้อยละของจำนวนรายการ Claim	**ถาม:** ถ้าเป็นการทำรายการผ่าน Third Party เช่น การ Claim ผ่านอู่รถยนต์ หรือ ออกกรมธรรม์ (Issue Policy) ผ่าน Broker นับเป็นการทำรายการ Online หรือไม่ **ตอบ:** จะนับเป็นรายการ Online ก็ต่อเมื่อทำรายการผ่าน Website, Mobile Application หรือ Social Media เป็นหลัก แต่หากเป็นการทำรายการผ่าน Broker และดำเนินการในรูปแบบกระดาษ เช่น Broker ไปเก็บเอกสารคำร้องของลูกค้าและส่งผ่านเอกสารเหล่านี้เพื่อดำเนินการ เป็นต้น จะจัดว่าเป็นการทำรายการแบบ Manual
3.1.6	จำนวนเทคโนโลยีใหม่ที่บริษัทนำมาใช้เป็นครั้งแรก ในรอบ 12 เดือน	จำนวนเทคโนโลยี	**ถาม:** การนับจำนวนเทคโนโลยีใหม่ (New Technology) ที่บริษัทนำมาใช้เป็นครั้งแรกในรอบ 12 เดือน ให้พิจารณาเพียง Application โดยไม่รวม Security Tool ใช่หรือไม่ **ตอบ:** ให้นับจากชนิดของเทคโนโลยี เช่น การใช้งาน Security Tool บน Cloud (DDOS) และบริษัทไม่เคยใช้งานบริการ Cloud มาก่อนหน้า กรณีนี้จะพิจารณาเป็นการใช้งานเทคโนโลยีใหม่ เป็นต้น แต่หากเป็นการซื้อ Physical Firewall ตัวใหม่ จะไม่นับเนื่องจากเป็นเทคโนโลยีเดิม

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ถาม: หากมีการใช้งาน SIEM เป็นครั้งแรก ต้องนับรวมในจำนวนเทคโนโลยีใหม่ที่บริษัทนำมาใช้เป็นครั้งแรกในรอบ 12 เดือน หรือไม่ **ตอบ:** ถ้าเป็นการใช้ SIEM ที่ดำเนินการเองภายในบริษัท ให้นับรวมด้วย แต่หากเป็นการใช้งาน SIEM ของผู้ให้บริการภายนอก ไม่นับเป็นเทคโนโลยีใหม่ **ถาม:** ในส่วนของ Public Cloud ปัจจุบันบริษัทใช้งาน PaaS และจะเปลี่ยนเป็น FaaS ถือว่าเป็นเทคโนโลยีใหม่หรือไม่ **ตอบ:** ไม่ถือว่าเป็นเทคโนโลยีใหม่ เนื่องจากเป็น Public Cloud เหมือนเดิม แต่มีการปรับเปลี่ยนการตั้งค่า หรือ แนวทางการใช้งานเท่านั้น **ถาม:** O365 เป็นเทคโนโลยีใหม่ หรือไม่ **ตอบ:** O365 เป็น Cloud Technology โดยถ้าบริษัทยังไม่เคยมีการใช้งานระบบคลาวด์มาก่อน ก็ถือว่าเป็นเทคโนโลยีใหม่ **ถาม:** Move to Cloud ถือว่าเป็นเทคโนโลยีใหม่ หรือไม่ **ตอบ:** ถ้าบริษัทยังไม่เคยมีการใช้งานระบบคลาวด์มาก่อน ก็ถือว่าเป็นเทคโนโลยีใหม่ **ถาม:** บริษัทมีการเปลี่ยนระบบอีเมล จาก Gmail เป็น O365 ถือเป็นเทคโนโลยีใหม่ หรือไม่ **ตอบ:** ไม่ เนื่องจากเป็นระบบอีเมลบนระบบคลาวด์เหมือนเดิม แค่มีการเปลี่ยนผู้ให้บริการเท่านั้น
IR 4. ขนาด และลักษณะเฉพาะขององค์กร (Business size & Organization characteristics)			
4.1.3	จำนวนกรมธรรม์ทั้งหมด (ณ วันที่ xxx)	จำนวนกรมธรรม์	**ถาม:** จำนวนกรมธรรม์ นับทุกผลิตภัณฑ์เฉพาะที่ Active ใช่หรือไม่ **ตอบ:** ใช่ นับรวมทุกผลิตภัณฑ์ที่มีผลบังคับใช้ (policy in-force)

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
4.2.1	อัตราส่วนร้อยละของจำนวนพนักงาน IT (จากทุก Line of Defense) ต่อ จำนวนพนักงานของบริษัทที่เป็นพนักงานและลูกจ้างประจำทั้งหมด (ณ วันที่ xxx)	อัตราส่วนร้อยละของพนักงาน IT ทั้งหมด ต่อ พนักงานบริษัททั้งหมด	**ถาม:** ถ้าแผนก Information Security ไม่ได้รวมอยู่ในแผนก IT จะจัดเป็น Line of Defense หรือไม่ **ตอบ:** พนักงานในแผนก Information Security จัดว่าเป็นพนักงาน IT แต่หากไม่ได้อยู่ในแผนก IT บริษัทประกันภัยต้องพิจารณาว่าจะจัดกลุ่มพนักงานดังกล่าวอยู่ใน Line of Defense ใด ซึ่งไม่ว่าจะอยู่ใน Line of Defense ใด ก็จะพิจารณาว่าเป็นพนักงานที่ทำหน้าที่เกี่ยวกับ IT
4.2.1	อัตราส่วนร้อยละของจำนวนพนักงาน IT (จากทุก Line of Defense) ต่อ จำนวนพนักงานของบริษัทที่เป็นพนักงานและลูกจ้างประจำทั้งหมด (ณ วันที่ xxx)	อัตราส่วนร้อยละของพนักงาน IT ทั้งหมด ต่อ พนักงานบริษัททั้งหมด	**ถาม:** การนับจำนวนพนักงาน IT รวมถึงกรรมการบริษัทที่มีความรู้ด้าน IT ด้วยหรือไม่ **ตอบ:** ไม่รวมกรรมการบริษัท จะนับเฉพาะพนักงานเท่านั้น **ถาม:** ถ้ามีพนักงาน IT Security หรือ พนักงานทางด้าน IT อื่นๆ ที่เป็น Shared Service ของต่างประเทศ หรือของบริษัทแม่ ต้องนับรวมเป็นพนักงาน IT ด้วยหรือไม่ **ตอบ:** ในกรณีของพนักงานด้าน IT ที่เป็น Shared Service จะไม่ถูกนับรวมเป็นพนักงาน IT เว้นแต่ว่า Shared Service มีการแบ่งแยก Head Count ที่ชัดเจนสำหรับผู้ให้บริการทางด้าน IT ที่ทำงานให้บริษัทอย่างเฉพาะเจาะจง **ถาม:** ถ้ามีแผนกอื่นอยู่ในส่วนงาน IT เช่น Digital Partnership หรือ IT Project Management พนักงานในแผนกเหล่านี้จัดว่าเป็นพนักงาน IT หรือไม่ **ตอบ:** ให้พิจารณาจากความรับผิดชอบหรือหน้าที่งานของแผนกดังกล่าวว่ามีการให้บริการเกี่ยวกับเทคโนโลยีสารสนเทศหรือไม่ หากมี ให้นับรวมแผนกดังกล่าวด้วย เช่น ถ้า Digital Partnership สนับสนุนงาน IT ทางด้านการจัดหาและบริหารจัดการ IT Vendor ก็สามารถนับรวมได้ หรือ ถ้า IT Project Management มีหน้าที่ในการบริหารจัดการ IT Project ซึ่งจัดว่าเป็นการให้บริการทางด้าน IT ก็สามารถนับรวมได้เช่นกัน

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ถาม: ช่วยอธิบายคำจำกัดความของพนักงาน IT เพิ่มเติม เช่น พนักงาน Data Governance นับรวมเป็นพนักงาน IT ด้วยหรือไม่ และ พนักงาน Data Governance ที่ดูแลทั้งด้าน IT และ Non-IT นับว่าเป็นพนักงาน IT หรือไม่ เนื่องจากเป็นแค่การประสานงานกับแผนก IT เท่านั้น **ตอบ:** ในแต่ละบริษัทอาจมีโครงสร้างทีมที่แตกต่างกันออกไป เช่น Data Governance Team อาจประกอบไปด้วยพนักงาน IT รวมอยู่กับพนักงานที่เป็น Business User อย่างไรก็ตาม ให้บริษัทยึดหลักว่า พนักงาน IT คือ เจ้าหน้าที่ที่ให้บริการทางด้าน IT (IT service) ไม่ว่าจะอยู่ในทีมใดก็ตาม **ถาม:** พนักงาน IT รวมถึง IT Helpdesk ด้วยหรือไม่ **ตอบ:** รวม เนื่องจาก IT Helpdesk ทำงานให้บริการทางด้าน IT ภายในบริษัท โดยเป็น First Tier รับเรื่องด้าน IT Problems / IT incident แต่ในกรณีที่เป็น Helpdesk ในแผนก CRM ที่รับเรื่องจากลูกค้า ไม่นับเป็นพนักงาน IT **ถาม:** พนักงาน IT ให้นับรวมพนักงาน IT Outsource ด้วยหรือไม่ **ตอบ:** ไม่นับ ให้นับเฉพาะพนักงานของบริษัทเท่านั้น **ถาม:** พนักงาน IT นับเฉพาะ IT Security, IT Risk และ IT Audit ใช่หรือไม่ และนับรวมไปถึง IT Application หรือไม่ **ตอบ:** นับรวม IT Application ด้วย โดยยึดหลักว่า พนักงาน IT คือ เจ้าหน้าที่ที่ให้บริการทางด้าน IT (IT service) ไม่ว่าจะอยู่ทีมใดก็ตาม ในกรณีนี้ IT Application ให้บริการ

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ทางด้าน Application development, Application Support หรือ Application Admin จึงถือเป็น พนักงาน IT **ถาม:** กรุณาอธิบายเหตุผลประกอบ กรณีสัดส่วน (%) ของพนักงาน IT ต่อพนักงานทั้งหมดอยู่ในเกณฑ์น้อย ถือว่ามีความเสี่ยงสูง **ตอบ:** จำนวนพนักงานที่มากขึ้น สามารถทำให้บริษัทมีทรัพยากรในการบริหารจัดการทางด้านสารสนเทศได้มากขึ้น ทำให้มีความเสี่ยงลดลง
4.2.2	อัตราส่วนร้อยละของจำนวนพนักงาน IT ที่ลาออกเฉลี่ย (จากทุก Line of Defense) (ในรอบระยะเวลา 12 เดือนย้อนหลัง)	อัตราส่วนร้อยละของพนักงาน IT ที่ลาออกเฉลี่ยทั้งปี	**ถาม:** พนักงาน IT ที่มีกำหนดสัญญาจ้างเป็นช่วงระยะเวลาที่ชัดเจน เช่น 1 ปี ต้องนับเป็นพนักงานที่ลาออกหรือไม่ **ตอบ:** นับรวมเป็นพนักงานลาออก และให้นับรวมทั้งจากการเลิกจ้าง ลาออก และหมดสัญญา โดยในข้อนี้มองว่าเกิดความเสี่ยงของความต่อเนื่องในการให้บริการ และการสูญเสียความรู้ระหว่างการเปลี่ยนถ่ายบุคลากรในองค์กร **ถาม:** พนักงาน IT ย้ายแผนกไปหน่วยงานธุรกิจอื่น นับเป็นการลาออกหรือไม่ **ตอบ:** นับว่าเป็นการลาออก เนื่องจากไม่ได้ปฏิบัติงานด้าน IT แล้ว **ถาม:** พนักงานบริษัทในเครือที่ให้บริการทางด้าน IT ต้องนำมารวมคำนวณอัตราการลาออกด้วยหรือไม่ และถ้า High Privilege ถือโดยบริษัทในเครือ จำนวนพนักงานทั้งหมด (ตัวหารในสูตร) ต้องนำพนักงานของบริษัทในเครือมารวมคำนวณด้วยหรือไม่ **ตอบ:** ให้พิจารณาก่อนว่า พนักงานบริษัทในเครือ หรือ High Privilege นั้นเป็น Head Count ที่เฉพาะเจาะจงที่นำมานับรวมเป็นพนักงาน IT ของบริษัทหรือไม่ ซึ่งถ้าพิจารณาแล้วว่าเป็นพนักงาน IT ของบริษัท ควรนำมารวมคำนวณอัตราการลาออกด้วย

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
4.3.1	อัตราส่วนร้อยละของจำนวนพนักงานของบริษัท พนักงานของบริษัทในเครือ และบริษัทภายนอก ที่ถือครองบัญชีที่มีสิทธิสูง (High-privileged users) ในระบบงานสำคัญ อาทิ Administrator, Root, User administrator, Network Administrator, DBA, เป็นต้น (ณ วันที่ 31 ธ.ค. 2564)	อัตราส่วนร้อยละของพนักงานที่มีสิทธิสูง	**ถาม:** กรุณาอธิบายคำจำกัดความเพิ่มเติมของพนักงานที่มีสิทธิสูง **ตอบ:** พนักงานที่มีสิทธิสูง เปรียบเทียบได้กับ Administrator ที่สามารถบริหารจัดการระบบได้ทั้งระบบ หรือบริหารจัดการผู้ใช้งานในระบบได้ เช่น User Admin ที่สามารถบริหารจัดการเพิ่ม-ลดสิทธิในระบบได้, Root, Administrator, QSECOFCR ในระดับ Operating system, DBA ในระดับ Database หรือ firewall/Device admin ในอุปกรณ์เครือข่าย **ถาม:** ปัจจุบันบริษัทควบคุม High-Privileged Users ผ่าน PAM Tools ที่ต้องขออนุมัติการใช้งานเป็นรายครั้ง จะนับบัญชีผู้ใช้งานอย่างไร **ตอบ:** ในกรณีการใช้ PAM (Privileged Access Management) ให้นับตามจำนวนพนักงานที่สามารถร้องขอใช้งานบัญชีผู้ใช้งานที่มีสิทธิสูงได้ ทั้งนี้ เนื่องจากการพิจารณาความเสี่ยงสืบเนื่องจะพิจารณาก่อนการควบคุม ดังนั้น การใช้การควบคุมผ่าน PAM จึงไม่นำมาพิจารณาร่วมในการประเมินนี้ นอกจากนี้ ในกรณีที่พนักงาน IT 1 คน ถือครองมากกว่า 1 User ID ให้นับตามจำนวนพนักงาน เช่น มีพนักงาน 10 คน ที่สามารถร้องขอใช้งาน Admin ได้ 5 ระบบ ให้นับเป็นบัญชีผู้ใช้งาน 10 คน
IR 5. ประวัติการถูกคุกคามทางไซเบอร์ (Cyber threats records)			
	คำถามในภาพรวม		**ถาม:** กลุ่มที่พยายามโจมตีแต่ไม่สำเร็จ และโดน Block ไปก่อนที่จะเข้ามายังระบบ Network ของบริษัท ไม่นับว่าเป็น Attempt ใช่หรือไม่ **ตอบ:** ความพยายามโจมตีที่ไม่สำเร็จหรือโดน Block ไปก่อนเข้ามายังระบบ Network ของบริษัทได้นั้น จัดว่าเป็น Attempt ซึ่ง Attempt ยังไม่นับเป็นเหตุการณ์ที่ต้องนำมาตอบในแบบประเมินที่จะนำมาพิจารณาเป็นปัจจัยความเสี่ยง เนื่องจาก เหตุการณ์ที่ต้องนำมาตอบในแบบประเมินจะเริ่มนับจากการโจมตีที่สำเร็จแล้ว หรือที่สามารถล่วงล้ำเข้ามายังระบบ Network ของบริษัทได้สำเร็จแล้วเท่านั้น

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ถาม: จำนวนครั้งของความพยายามโจมตีแต่ไม่สำเร็จ เช่น การสแกนที่พบเจอในแต่ละวัน จะนับจำนวนอย่างไร **ตอบ:** จะไม่ถูกนับเป็นปัจจัยเสี่ยง เนื่องจากถือเป็นการโจมตีที่ไม่สำเร็จ เป็นเพียงแค่ความพยายามในการโจมตีเท่านั้น **ถาม:** จำนวนการถูกโจมตีนับอย่างไร เฉพาะรายการที่สร้างความเสียหาย หรือนับรวมทั้งหมด เนื่องจากบางการโจมตีบริษัทสามารถป้องกันได้แบบเบ็ดเสร็จ เช่น การทำ Port Scan สำหรับความพยายามโจมตีจำนวนหมื่นครั้ง แต่ทางบริษัทสามารถป้องกันได้ทั้งหมด **ตอบ:** ปัจจัยความเสี่ยงในมุมมองนี้จะเริ่มนับจากการโจมตีที่สำเร็จแล้ว หรือที่สามารถล่วงล้ำเข้ามายังระบบ Network ของบริษัทได้สำเร็จแล้วเท่านั้น โดยจะมีการแบ่งประเภทการโจมตีเป็น 5 ประเภท ได้แก่ (1) Malware / Virus (2) Phishing/ Social engineering (3) DDOS (4) SQL Injection / XSS / CSRF และ (5) Data Breach ซึ่งปัจจัยข้อ 1-4 จะพิจารณาจากจำนวนการโจมตีที่สำเร็จแล้ว ทั้งที่ทำให้เกิด และไม่เกิดความเสียหาย แต่ในประเภทที่ 5 (จำนวนเหตุการณ์ประเภท Data Breach และการรั่วไหลของข้อมูลส่วนบุคคลที่เกิดขึ้นแล้ว) จะพิจารณาจำนวนการโจมตีที่สำเร็จแล้ว และทำให้เกิดความเสียหายร่วมด้วย ดังนั้น การโจมตีที่บริษัทสามารถป้องกันได้แบบเบ็ดเสร็จ และยังไม่ล่วงล้ำเข้ามาในระบบ Network ของบริษัท จึงไม่นับรวมในการประเมิน **ถาม:** ในกรณีที่ข้อมูลเกี่ยวกับการโจมตี มีการดูแลโดยบริษัทแม่ที่ต่างประเทศ โดย (1) การเชื่อมต่อ Internet ของบริษัทในประเทศไทยจะเชื่อมต่อผ่านไปยังต่างประเทศเพื่อออก Internet ที่บริษัทแม่ แต่ทางบริษัทแม่ไม่สามารถให้ข้อมูลการโจมตีดังกล่าวได้ ในกรณีนี้จะต้องปฏิบัติอย่างไร (2) ในกรณีที่บริษัทแม่ไม่สามารถเปิดเผยข้อมูลนี้ได้ อาจทำให้บริษัท

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			มีความเสี่ยงสูงกว่าความเป็นจริง จะต้องปฏิบัติอย่างไร และ (3) ในส่วนของ Action Plan บริษัทควรต้องกรอกข้อมูลอย่างไร เนื่องจากบริษัทแม่ได้ดำเนินการควบคุมทางด้านไซเบอร์ให้แล้ว **ตอบ:** บริษัทอาจขอข้อมูลในลักษณะ Range ของจำนวนการโจมตี มาจากบริษัทแม่เพื่อให้สามารถประเมินระดับความเสี่ยงได้ และ ใส่คำอธิบายเพิ่มเติมในแบบประเมิน ทั้งนี้ หากบริษัทแม่ไม่สามารถให้ข้อมูลได้เลย ให้บริษัทประเมินเป็น "ไม่มีข้อมูล" และใส่คำอธิบายเพิ่มเติมในแบบประเมิน นอกจากนี้ แบบประเมิน CRAF จะประเมินระดับความเสี่ยง และ ระดับการควบคุมแยกออกจากกัน ถ้าบริษัทมีความเสี่ยงสูงแต่บริษัทแม่มีการควบคุมที่ดี ก็จะสะท้อนในภาพรวมว่าบริษัทมีการควบคุมที่เหมาะสมกับระดับความเสี่ยงแล้ว อย่างไรก็ตาม ถ้าผลการประเมินทำให้บริษัทอาจต้องมีการดำเนินงานการควบคุมเพิ่มเติมที่ไม่สะท้อนกับความเป็นจริง บริษัทสามารถปรึกษากับสำนักงานเพิ่มเติมได้
5.1.2	จำนวนการโจมตีทางไซเบอร์ (Cyber Attack) ต่อระบบสารสนเทศของบริษัทประเภท Phishing / Social Engineering (ในรอบระยะเวลา 12 เดือนย้อนหลัง)	จำนวนการโจมตี	**ถาม:** ถ้าเกิดการฟิชชิงทางอีเมล (Email Phishing) ของบริษัท แต่ผู้ใช้งานทราบว่าเป็นการ Phishing จึงไม่เกิดความเสียหายใดๆ ขึ้น ให้ถือเป็นเหตุการณ์ที่ต้องนำมาตอบในแบบประเมินหรือไม่ หากต้องตอบ ให้นับเป็นจำนวนเหตุการณ์ หรือ นับตามจำนวนอีเมลที่ได้รับและต้องทำอย่างไร **ตอบ:** ถ้าพนักงานบริษัทได้รับ Email Phishing ถือว่าการโจมตีนั้นได้เข้ามายังระบบ Network ของบริษัทได้แล้ว จึงนับเป็นเหตุการณ์ที่ต้องนำมาตอบในแบบประเมิน โดยวิธีการนับจะนับจากจำนวนอีเมลที่ได้รับ ซึ่งทางสำนักงานมีเผื่อค่า Threshold ในส่วนนี้ไว้แล้ว **ถาม:** กรณีบริษัทถูกปลอมอีเมล และส่งไปหาบุคคลอื่น ถือว่าเป็นการ Phishing ด้วยหรือไม่ และต้องรายงานเหตุการณ์ดังกล่าวหรือไม่

ปัจจัยเสี่ยง		หน่วยนับ	ถาม - ตอบ
			ตอบ: ไม่นับเป็นเหตุการณ์ Phishing ที่ต้องนำมาตอบในแบบประเมิน เนื่องจากตามเกณฑ์คือการนับการโจมตีที่มุ่งมายังระบบเครือข่ายของบริษัทเท่านั้น ในส่วนของการรายงานมายังสำนักงาน ให้พิจารณาจากเงื่อนไขของสำนักงานว่า กรณี Phishing นั้นเป็นเหตุการณ์สำคัญที่ต้องรายงานไปยัง CEO หรือไม่ ถ้าต้องรายงานไปยัง CEO ให้ถือว่าเป็นเหตุการณ์ที่ต้องรายงานต่อสำนักงานเช่นกัน

คำถามเกี่ยวกับแบบประเมินระดับการควบคุม (Control Maturity: CM)

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
CM 1. การกำกับดูแล (Governance)					
1.1 การกำกับดูแลด้านเทคโนโลยีสารสนเทศ	1.1.1 โครงสร้างการกำกับดูแลและบทบาทหน้าที่	Baseline	1.1.1.3	คณะกรรมการบริษัทได้รับการอบรมความรู้เกี่ยวกับแนวโน้มการเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ รวมทั้งความเสี่ยง ผลกระทบ และแนวทางการป้องกันความเสี่ยงจากเหตุการณ์ดังกล่าว	**ถาม:** คณะกรรมการบริษัทในที่นี้ หมายถึง บางท่านหรือทุกท่าน **ตอบ:** ทุกท่าน **ถาม:** คณะกรรมการบริษัท คือ Board of Directors ใช่หรือไม่ ส่วนคณะกรรมการบริหาร (Executive Board) ไม่ถือเป็นคณะกรรมการบริษัทใช่หรือไม่ **ตอบ:** คณะกรรมการบริษัท คือ Board of Directors ซึ่งเป็นคนละกลุ่มกับ คณะกรรมการบริหาร (Executive Board) แต่ในบางบริษัทคณะกรรมการบริหารบางท่านอาจเป็นคณะกรรมการบริษัทด้วย ขึ้นอยู่กับโครงสร้างองค์กร เช่น CEO อาจมีชื่ออยู่ทั้งในคณะกรรมการบริษัท และคณะกรรมการบริหาร เป็นต้น
1.1 การกำกับดูแลด้านเทคโนโลยีสารสนเทศ	1.1.1 โครงสร้างการกำกับดูแลและบทบาทหน้าที่	Intermediate	1.1.1.4	คณะกรรมการบริษัทอย่างน้อย 1 ท่าน เป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศหรือด้านการกำกับดูแลเทคโนโลยีสารสนเทศ (IT Governance) โดยอาจพิจารณาจากประวัติการศึกษา ประสบการณ์ในการทำงาน และประสบการณ์ในการเป็นคณะกรรมการหรือคณะทำงาน ที่เกี่ยวข้องทางด้านเทคโนโลยีสารสนเทศ หรือปัจจัยอื่น ๆ ที่เกี่ยวข้อง	**ถาม:** ราชกิจจาฯ ระบุว่า คณะกรรมการบริษัทอย่างน้อย 1 ท่าน "ควร" เป็นผู้ที่มีความรู้ฯ จึงไม่เห็นด้วยในการนำมาตั้งเป็นเกณฑ์การควบคุม **ตอบ:** สำนักงาน คปภ. ได้ปรับการควบคุมข้อนี้เป็น Intermediate

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
1.1 การกำกับดูแลด้านเทคโนโลยีสารสนเทศ	1.1.1 โครงสร้างการกำกับดูแลและบทบาทหน้าที่	Advance	1.1.1.5	บริษัทกำหนดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท (อาทิ กำหนดให้มี Chief Information Security Officer : CISO หรือเทียบเท่า) เป็นการเฉพาะ และเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ โดยมีอำนาจในการกำกับดูแลความเสี่ยงและการควบคุมด้านสารสนเทศและไซเบอร์	**ถาม 1:** กรณีนี้ ถ้าไม่ใช่ Chief แต่เป็น Department Head ที่ดูแลเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ได้หรือไม่ **ถาม 2:** หากเป็น Chief แล้วบริษัทจะต้องปฏิบัติตามข้อนี้ เข้าใจว่าจะส่งผลกระทบต่อหลายบริษัท เพราะโครงสร้างของบริษัทหลาย ๆ แห่งในปัจจุบัน IT Security Head อยู่ภายใต้ Chief of IT ซึ่ง Chief of IT ไม่ได้ดูแลเฉพาะ IT Security แต่ยังครอบคลุมถึง Departments อื่น ๆ อีกด้วย เช่น IT Support, IT Infrastructure, IT Development เป็นต้น **ตอบ:** เนื่องจากข้อนี้เป็น Advance ดังนั้นผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทต้องเป็นระดับ Chief หรือ เทียบเท่า **ถาม:** อยากให้กำหนดคำนิยาม (Definition) ของคำว่า "ผู้บริหารระดับสูง" **ตอบ:** ผู้บริหารระดับหัวหน้าส่วนงานที่มีอำนาจในการตัดสินใจ และควบคุมการดำเนินงานภายในส่วนงานนั้นๆ โดยตามความหมายของการควบคุมข้อนี้ ผู้บริหารระดับสูงดังกล่าว ให้เทียบเคียงระดับ CISO

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
					ถาม: CISO อยู่บริษัทแม่ ได้หรือไม่ จำเป็นต้องอยู่ในประเทศไทยเท่านั้นหรือไม่ **ตอบ:** ให้บริษัทพิจารณาจากบทบาทหน้าที่ในการทำงานเป็นหลัก โดยหาก CISO อยู่ในบริษัทแม่ แต่มีอำนาจในการบริหารจัดการทางด้าน IT Security ของบริษัทโดยตรง ก็สามารถถือว่าบริษัทมี CISO ได้ **ถาม:** CTO (Chief Technology Officer) สามารถทดแทน CISO ได้หรือไม่ ถ้าไม่ได้ แสดงว่า CTO ไม่ได้รับอนุญาตให้ทำหน้าที่เดียวกับ CISO ใช่หรือไม่ **ตอบ:** CISO (Chief Information Security Officer) ทำหน้าที่ดูแลด้านการรักษาความปลอดภัยสารสนเทศ ในขณะที่ CTO จะดูแลภาพรวมของระบบสารสนเทศทั้งหมด ซึ่งเป็นคนละบทบาทหน้าที่กัน ทั้งนี้ ในบางกรณี CTO อาจทำหน้าที่ CISO ได้หรือมีทีมงาน IT Security อยู่ภายใต้ CISO อย่างไรก็ตาม ในการควบคุมข้อนี้ เป็นการควบคุมระดับ Advance สำหรับบริษัทที่มีความเสี่ยงสืบเนื่องสูง จึงกำหนดให้แยก CISO ออกมาจาก CTO ให้เป็นอิสระต่อกัน เพื่อที่จะสามารถสอบทานทางด้าน IT Security ได้อย่างเป็นอิสระ

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
1.1 การกำกับดูแลด้านเทคโนโลยีสารสนเทศ	1.1.1 โครงสร้างการกำกับดูแลและบทบาทหน้าที่	Advance	1.1.1.6	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย กำหนดให้หน่วยงานธุรกิจรับผิดชอบดูแลความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้อง รวมทั้งสื่อสารเกี่ยวกับบทบาทหน้าที่ในการดูแลความเสี่ยงด้านไซเบอร์อย่างทั่วถึงทั้งบริษัท	**ถาม:** หน่วยงานธุรกิจในที่นี้ หมายความถึงอะไร เช่น แผนกขาย (Sales) ต้องรับผิดชอบดูแลความเสี่ยงด้านไซเบอร์ของแผนกเองใช่หรือไม่ **ตอบ:** ใช่ ข้อนี้เป็นการควบคุมระดับ Advance เนื่องจาก หน่วยงานธุรกิจ จะเป็นผู้มีความรู้ความสามารถ ในการระบุ และประเมินความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้องกับขอบเขตงานของตนเองได้ ซึ่งจะเป็นการ Integrate การบริหารจัดการระหว่างความเสี่ยงทางธุรกิจ (Business Risk) กับความเสี่ยงทางไซเบอร์ (Cyber Risk)
1.1 การกำกับดูแลด้านเทคโนโลยีสารสนเทศ	1.1.2 กลยุทธ์และนโยบาย	Intermediate	1.1.2.16	บริษัทจัดสรรงบประมาณในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้ครอบคลุมระบบงาน (Application) ข้อมูล (Information) โครงสร้างพื้นฐาน (Infrastructure) เครื่องมือ และบุคลากร โดยสอดคล้องและเพียงพอตามระดับความเสี่ยงที่บริษัทมี	**ถาม:** กรุณาอธิบายข้อความนี้เพิ่มเติม "สอดคล้องและเพียงพอตามระดับความเสี่ยงที่บริษัทมี" **ตอบ:** ตัวอย่างเช่น บริษัทมีการพิจารณาอนุมัติงบประมาณในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ให้เพียงพอต่อการปิดความเสี่ยงที่เกินกว่าระดับความเสี่ยงที่ยอมรับได้
1.3 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ		Intermediate	1.3.1.10	บริษัทมีการประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment) เพื่อให้บริษัททราบถึงประเภทและระดับความเสี่ยงของตนเอง (Risk Profile) รวมทั้งมีแนวทางการกำกับดูแลการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ที่สอดคล้องกับระดับความเสี่ยงตั้งต้นของบริษัท (Inherent Risk) ทั้งนี้บริษัทอาจใช้การประเมิน CRAF นี้ เพื่อประเมินระดับความเสี่ยงตั้ง	**ถาม:** ในกรณีที่กลยุทธ์ในการบริหารจัดการความเสี่ยงด้านไซเบอร์ถูกกำหนดมาจากบริษัทแม่ รวมทั้งมีการนำนโยบาย และกระบวนการด้านการกำกับดูแลสารสนเทศจากบริษัทแม่มาปรับใช้กับบริษัท โดยบริษัทมีความเสี่ยงที่ยอมรับได้ในระดับต่ำ ทุกหน่วยงานจึงถูกบังคับใช้การควบคุมตามนโยบายและกระบวนการของบริษัท ได้หรือไม่

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
				ต้นด้านไซเบอร์ และ ระดับการควบคุมทางไซเบอร์ โดยในกรณีที่บริษัทมีระดับการควบคุมที่ไม่สอดคล้องกับระดับความเสี่ยง บริษัทได้ดำเนินการปรับปรุงการควบคุมเหล่านั้นอย่างเหมาะสม	**ตอบ:** สำนักงานมีความคาดหวังให้บริษัทมีการควบคุมที่สอดคล้องกับระดับความเสี่ยงสืบเนื่อง โดยเรื่องการดำเนินงานตามนโยบายของบริษัท บริษัทสามารถพิจารณาเองได้ตามความเหมาะสม
1.3 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ		Advance	1.3.1.11	บริษัทมีการตรวจสอบกระบวนการจัดทำ ข้อความที่แสดงถึงระดับความเสี่ยงด้านไซเบอร์ที่ยอมรับได้ (Cyber Risk Appetite Statement) เพื่อให้มั่นใจว่าการกำหนด Cyber Risk Appetite Statement สอดคล้องกับขนาดและความซับซ้อนของธุรกิจ รวมถึงเปรียบเทียบความพร้อมในการรับมือภัยไซเบอร์ของบริษัท (Cyber Resilience Readiness) กับ Cyber Risk Appetite Statement ที่บริษัทกำหนด	**ถาม 1:** "การตรวจสอบกระบวนการจัดทำ Cyber Risk Appetite Statement เพื่อให้มั่นใจว่าการกำหนด Cyber Risk Appetite Statement สอดคล้องกับขนาดและความซับซ้อนของธุรกิจ" ในที่นี้ หมายถึงอะไร และทำอย่างไรเพื่อให้มีความเพียงพอ **ถาม 2:** "เปรียบเทียบความพร้อมในการรับมือภัยไซเบอร์ของบริษัท (Cyber Resilience Readiness) กับ Cyber Risk Appetite Statement ที่บริษัทกำหนด" ในที่นี้ สำนักงานหมายถึงอะไร และทำอย่างไรเพื่อให้มีความเพียงพอ **ถาม 3:** รบกวนขอตัวอย่าง Cyber Risk Appetite Statement ว่าเป็นอย่างไร ต้องคำนึงถึงมุมใดบ้าง และใช้ Threshold ประเภทใดบ้าง **ตอบ:** ตัวอย่างเช่น ● ในกรณีที่บริษัทมีการซื้อขายผลิตภัณฑ์ผ่านระบบ online เป็นจำนวนมาก บริษัทอาจกำหนด Cyber Risk Appetite Statement เช่น "บริษัทไม่สามารถยอมรับให้ระบบที่ให้บริการสำคัญหยุดชะงักเกินกว่าระยะเวลาในการกู้คืนระบบ (Maximum recovery time)

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
					ที่กำหนดไว้" นอกจากนี้ บริษัทยังมีการทดสอบความมั่นคงปลอดภัยไซเบอร์ และความสามารถในการกู้คืนอย่างรวดเร็วของระบบซื้อขายผลิตภัณฑ์ online เพื่อให้มั่นใจว่าการให้บริการของบริษัทมีความพร้อม และสอดคล้องตามที่ Cyber Risk Appetite Statement กำหนดไว้ หรือ ● ในกรณีที่บริษัทมีระบบสำคัญเพื่อการให้บริการลูกค้าที่ซับซ้อน และมีการแก้ไขเปลี่ยนแปลงจำนวนมาก บริษัทอาจกำหนด Cyber Risk Appetite Statement เช่น "บริษัทไม่สามารถยอมรับเหตุการณ์ผิดปกติ (Incident) ที่เกิดขึ้นกับระบบสารสนเทศและการให้บริการสำคัญที่เกิดจากกระบวนการแก้ไขเปลี่ยนแปลงที่ไม่เหมาะสม" นอกจากนี้ บริษัทยังมีการทดสอบการควบคุมทางด้านการแก้ไขเปลี่ยนแปลงและพัฒนาโปรแกรมอย่างเข้มข้น เป็นต้น **ถาม:** สำนักงานจะมีแนวปฏิบัติ (Guideline) เชิงปริมาณ (Quantifiable) มากกว่านี้หรือไม่ **ตอบ:** การประเมินการควบคุมบางส่วนต้องพิจารณาจากลักษณะของแต่ละบริษัท แนวทางการปฏิบัติงานและแนวทางการประเมินที่เกี่ยวข้อง ดังนั้น จึงไม่

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
					สามารถกำหนดเป็นแนวปฏิบัติ (Guideline) ที่ตายตัว เพื่อให้ทุกบริษัทสามารถใช้ร่วมกันได้ โดยทางสำนักงานจะพยายามใช้การยกตัวอย่างให้เห็นภาพ ทั้งนี้ หากมีคำถามเพิ่มเติม บริษัทสามารถสอบถามมายังสำนักงานได้
CM 2. การระบุความเสี่ยง (Identification)					
2.1 การบริหารจัดการทรัพย์สินสารสนเทศ		Baseline	2.1.1.3	บริษัทมีมาตรการด้านการรักษาความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์อื่น ๆ ที่มีการเชื่อมต่อกับระบบเครือข่ายของบริษัท ซึ่งรวมถึง อุปกรณ์ส่วนตัว (BYOD) และอุปกรณ์จัดเก็บแบบพกพา (Removable storage) ต่าง ๆ โดยมาตรการในที่นี้**อาจ**รวมถึง การมีแนวทางการปฏิบัติงานที่เกี่ยวข้อง และการใช้งานเครื่องมือ (Tools) เพื่อการควบคุมทางเทคนิค ที่บริษัทจะสามารถตรวจสอบการใช้งาน และ ระงับความเสียหายได้อย่างทันท่วงทีเมื่อมีเหตุการณ์ทางด้านความมั่นคงปลอดภัยเกิดขึ้น	**ถาม:** หัวข้อนี้ หมายความว่า หากบริษัทมีการใช้งาน BYOD จะเป็นการบังคับให้มีระบบ MDM (Mobile Device Management) หรือไม่ **ตอบ:** การควบคุมใช้คำว่า "อาจ" ดังนั้น บริษัทอาจมี MDM หรือใช้กระบวนการ หรือเครื่องมืออื่นๆ ทดแทนได้
2.1 การบริหารจัดการทรัพย์สินสารสนเทศ		Intermediate	2.1.1.11	ทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูลของบริษัทที่เป็นข้อมูลส่วนบุคคล มีการระบุรายละเอียดที่ครอบคลุมถึง (1) ข้อมูลส่วนบุคคลที่รวบรวมไว้ (2) ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล (3) วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล	**ถาม:** ข้อมูลใน (3) อยู่ในระบบบันทึก consent ไม่ควรนำมาเก็บปะปนกับทะเบียนทรัพย์สิน ใช่หรือไม่ **ตอบ:** แต่ละข้อมูลอาจมีวัตถุประสงค์ในการจัดเก็บและประมวลผลที่แตกต่างกัน การบันทึกในทะเบียนทรัพย์สินจะทำให้ทราบว่าข้อมูลนั้น ๆ ถูกจัดเก็บหรือประมวลผลด้วยฐานอะไร

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
				(4) ระยะเวลาเก็บรักษาข้อมูลส่วนบุคคล (5) การเปิดเผยและวัตถุประสงค์ในการโอนข้อมูลส่วนบุคคล (6) มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล (7) ข้อจำกัดในการเข้าถึงและสำเนาข้อมูลส่วนบุคคล (8) ป้ายชื่อ (Labelling)	**ถาม:** ข้อมูลใน (4) (5) (6) (7) อยู่ใน Privacy Policy ไม่ควรมานำมาเก็บปะปนกับทะเบียนทรัพย์สิน ใช่หรือไม่ **ตอบ:** ข้อมูลแต่ละชุดอาจมี (4) ระยะเวลาและข้อจำกัดของเวลาในการจัดเก็บ (5) เงื่อนไขการเปิดเผยและการโอนย้าย (6) มาตรฐานการรักษาความปลอดภัย เช่น บางชุดใช้ Restrict Access, Encryption หรือ Masking เป็นต้น และ (7) ข้อจำกัดในการเข้าถึงที่แตกต่างกัน ดังนั้นจึงควรบันทึกข้อมูลไว้ในทะเบียนเพื่อให้ง่ายต่อการบริหารจัดการ อย่างไรก็ตามการกำหนดข้อ (4), (5), (6), และ (7) ของข้อมูลแต่ละชุดในทะเบียนต้องสอดคล้องตามกฎหมายและนโยบายของบริษัท **ถาม:** ขอให้อธิบายการดำเนินการตามข้อ (8) พร้อมยกตัวอย่างประกอบ **ตอบ:** การติดป้ายชื่อของข้อมูลนั้นๆ เพื่อให้ง่ายต่อการสืบค้นและหาเจอ เช่น ป้าย Tape Backup **ถาม:** บริษัทสามารถใช้ ROPA แทนทะเบียนทรัพย์สินข้อมูลส่วนบุคคลได้หรือไม่ **ตอบ:** สามารถใช้ทดแทนกันได้ ถ้า ROPA ของบริษัท มีการบันทึกข้อมูลครบถ้วนตามที่การควบคุมระบุ

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
2.1 การบริหารจัดการทรัพย์สินสารสนเทศ		Advance	2.1.1.13	บริษัทมีเครื่องมือและกระบวนการที่ใช้บันทึกรายละเอียดทรัพย์สินสารสนเทศ (อาทิ รุ่น เวอร์ชัน จำนวนลิขสิทธิ์) ติดตาม (Tracking) ปรับปรุง (Updating) จัดลำดับความสำคัญ (Prioritizing) ในทะเบียนทรัพย์สินสารสนเทศ และสามารถจัดทำรายงานทรัพย์สินด้านเทคโนโลยีสารสนเทศได้ตามความต้องการใช้งาน ทั้งนี้เครื่องมือที่บริษัทใช้งานอาจอยู่ในรูปแบบของระบบงานหรือ Spreadsheet ก็ได้	**ถาม:** หากใช้ Spreadsheet ในการทำ Inventory Tracking ถือว่าเพียงพอหรือไม่ **ตอบ:** สามารถใช้ Spreadsheet ได้
2.2 การระบุและประเมินความเสี่ยงด้านไซเบอร์		Advance	2.2.1.5	บริษัทจัดทำ Risk Metrics เพื่อแสดงถึงทรัพย์สินสารสนเทศที่มีความเสี่ยงสูง และประเมินประสิทธิภาพและความเหมาะสมของมาตรการควบคุมต่อทรัพย์สินเหล่านั้น	**ถาม:** อยากให้สำนักงานอธิบายการควบคุมข้อนี้เพิ่มเติม **ตอบ:** การควบคุมนี้ระบุให้ บริษัทใช้ผลการประเมินระดับความสำคัญหรือระดับความเสี่ยงของทรัพย์สินสารสนเทศในทะเบียนทรัพย์สิน และนำความเสี่ยงของทรัพย์สินที่ถูกจัดว่ามี ความเสี่ยงสูง หรือ มีความสำคัญสูง มาพิจารณาความเหมาะสมของการควบคุมว่ามีการบริหารจัดการความเสี่ยงได้อย่างเหมาะสมหรือไม่
CM 3. การป้องกันความเสี่ยง (Protection)					
3.2 การควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ		Intermediate	3.2.1.7	บริษัทมีกระบวนการป้องกันการเปลี่ยนแปลงสิทธิของบัญชีผู้ใช้งานที่มีความเสี่ยงสูงบนระบบสารสนเทศสำคัญ อาทิ การสอบทานความเหมาะสมของบัญชีผู้ใช้งานและสิทธิที่ได้รับอย่างสม่ำเสมอกว่าบัญชีผู้ใช้งานทั่วไป และ/หรือ การสอบทาน	**ถาม:** กรณีที่ระบบสารสนเทศหรือบัญชีผู้ใช้งานที่มีความเสี่ยงสูงไม่มีการแจ้งเตือนอัตโนมัติ ทางสำนักงานมีคำแนะนำในเรื่องของ Mitigation Action อย่างไร **ตอบ:** บริษัทอาจใช้การสอบทานความเหมาะสมของบัญชีผู้ใช้งานและสิทธิที่ได้รับ ประกอบกับการสอบทาน Log การเข้าถึงที่ผิดปกติ

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
				บันทึกเหตุการณ์ (Log) การเข้าถึง และกิจกรรมที่ผิดปกติ เป็นต้น	**ถาม:** ขอเสนอให้แยกการควบคุมออกเป็นระดับ Advance **ตอบ:** สำนักงานได้ปรับการควบคุม โดยเพิ่มการควบคุมแบบ Manual ลงไปในการควบคุมข้อนี้ และแยกการควบคุมแบบ Automate ออกมาเป็นระดับ Advance ในข้อ 3.2.1.14 **ถาม:** "การเปลี่ยนแปลงสิทธิของบัญชีผู้ใช้งาน" ในที่นี้หมายถึงอะไร เนื่องจากเป็นระบบ/บัญชีที่มีความเสี่ยงสูงอยู่แล้ว **ตอบ:** ตัวอย่างเช่น มีผู้ที่ได้รับสิทธิสูงเพิ่มเติม มีการปรับเปลี่ยนสิทธิสูงเพิ่มเติม เป็นต้น **ถาม:** ถ้าบริษัทมีกระบวนการในการสอบทาน Log และบัญชีผู้ใช้งานสิทธิสูง สามารถตีความได้ว่าบริษัทได้ปฏิบัติการควบคุมข้อนี้ได้เลยหรือไม่ **ตอบ:** ได้ โดยจะต้องมีกระบวนการสอบทาน Log และบัญชีผู้ใช้งานสิทธิสูงที่ครบถ้วนทุกระบบงาน รวมทั้งมีความถี่ในการสอบทานที่เหมาะสมด้วย
3.2 การควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ		Intermediate	3.2.1.11	บริษัทติดตั้งอุปกรณ์ควบคุม เช่น Mobile Device Management (MDM) หรือ Mobile Application Management (MAM) บนอุปกรณ์เคลื่อนที่ส่วนบุคคลของพนักงาน อาทิ เครื่องคอมพิวเตอร์พกพา โทรศัพท์มือถือ Tablet ต่าง ๆ เพื่อให้มั่นใจว่ามีการ	**ถาม:** ข้อนี้เป็นการบังคับให้มี MDM สำหรับอุปกรณ์ BYOD หรือไม่ **ตอบ:** ใช่ สำหรับบริษัทที่มีการใช้งาน BYOD และเป็นบริษัทที่มีความเสี่ยงสืบเนื่องระดับปานกลางขึ้นไป

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
				กำหนดการตั้งค่าในระดับอุปกรณ์ และ ระดับการเข้าถึงระบบสารสนเทศของบริษัทที่มั่นคงปลอดภัย สามารถป้องกันการรั่วไหลของข้อมูลสำคัญ กำหนด Version ที่เหมาะสมของอุปกรณ์ ลบข้อมูลเมื่อเครื่องสูญหาย รวมทั้งติดตามตรวจสอบการใช้งานและการตั้งค่าได้จากส่วนกลางโดยหน่วยงานสารสนเทศ	
3.2 การควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ		Advance	3.2.1.12	บริษัทกำหนดการเชื่อมต่อของอุปกรณ์ และอุปกรณ์เคลื่อนที่ส่วนบุคคล เพื่อเข้าถึงข้อมูลลับ ข้อมูลส่วนบุคคลอ่อนไหว และระบบสารสนเทศสำคัญ โดยให้อยู่ภายใต้สภาพแวดล้อมที่ไม่มีการเชื่อมต่อไปยังระบบเครือข่าย อินเทอร์เน็ต หรือมีมาตรการการควบคุมที่เหมาะสมรัดกุมเทียบเท่า	**ถาม:** บริษัทจำเป็นต้องติดตั้ง Air gap ในระบบงานหรือไม่ เนื่องจากบริษัทคิดว่า ธุรกิจประกันชีวิตอาจจะไม่ได้มีความสำคัญเท่ากับหน่วยงานด้านความมั่นคง และในสถานการณ์โรคระบาด อาจทำให้บริษัทไม่สามารถให้บริการลูกค้าได้ **ตอบ:** การควบคุมข้อนี้ไม่ได้จำกัดเฉพาะ Air gap เท่านั้น บริษัทอาจใช้การควบคุมที่เทียบเท่า เช่น การเชื่อมต่อโดยมีการเข้ารหัสข้อมูลที่แข็งแรง เป็นต้น **ถาม:** ขอทราบรายละเอียดเพิ่มเติม หรือตัวอย่าง รวมทั้งความแตกต่างจาก MDM ในข้อ 3.2.1.11 **ตอบ:** ข้อนี้ไม่ได้กล่าวถึงการติดตั้ง MDM แต่เป็นการเข้าถึงข้อมูลลับหรือระบบสำคัญโดยไม่ผ่าน Internet (Air gap)
3.3 การเข้ารหัสข้อมูล		Intermediate	3.3.1.4	บริษัทมีระบบ อุปกรณ์ หรือ กระบวนการเพื่อใช้รักษาความปลอดภัย (อาทิ HSM: Hardware Security Module ระบบ หรือกระบวนการอื่นที่	**ถาม:** กรณีที่ใช้เป็น Software ไม่ใช่ Hardware (อุปกรณ์) ได้หรือไม่ **ตอบ:** ได้ ถ้ามีการตั้งค่าที่ดี เทียบเท่ากับ HSM

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
				เทียบเท่า) เพื่อการรักษาความมั่นคงปลอดภัยของกุญแจเข้ารหัสที่ใช้สำหรับระบบงาน และ ระบบสารสนเทศสำคัญ หมายเหตุ - กระบวนการเพื่อใช้รักษาความปลอดภัย เช่น การจัดทำทะเบียน และกระบวนการเบิกใช้ มีการจำกัดการเข้าถึงอย่างเหมาะสม การเข้ารหัสกุญแจเข้ารหัส การแยกเก็บกุญแจเข้ารหัสออกมาเพื่อไม่ให้เก็บปะปนกับข้อมูลอื่นๆ และผู้มีสิทธิเข้าถึงไม่ควรเป็นผู้ที่สามารถถอดรหัสกุญแจเข้ารหัสได้ เป็นต้น	**ถาม:** ข้อนี้เป็นการกำหนดให้ใช้ Hardware ในการเก็บรักษา Encryption Key หรือไม่ ทางบริษัทเห็นว่าควรจัดอยู่ใน Advance Level **ตอบ**: ข้อนี้พิจารณาถึงการเก็บรักษา Encryption Key เป็นสำคัญ ถึงแม้บริษัทไม่มี HSM แต่มีการควบคุมที่เทียบเท่าก็ถือว่ามีการควบคุมในข้อนี้ได้ อย่างไรก็ดี ได้มีการปรับปรุงรายละเอียดเกี่ยวกับการควบคุมใหม่เพื่อให้ชัดเจนว่า ไม่เน้นเรื่องการมี HSM แต่เน้นถึงการควบคุมที่ปลอดภัย
3.3 การเข้ารหัสข้อมูล		Intermediate	3.3.1.5	บริษัทเข้ารหัสสื่อบันทึกข้อมูลของ เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา และอุปกรณ์เคลื่อนที่ (Mobile Devices) รวมถึงสื่อบันทึกข้อมูลอื่นที่ใช้บันทึกข้อมูลที่เป็นความลับ โดยพิจารณาตามระดับความเสี่ยง หรือระดับความสำคัญของข้อมูล	**ถาม:** ข้อนี้เป็นการบังคับให้บริษัทต้องมี MDM สำหรับ Mobile Devices หรือไม่ **ตอบ**: ไม่เสมอไป เนื่องจาก ● ถ้าเป็น Mobile Devices ของบริษัท อาจสามารถเข้ารหัส (Encrypt) ได้โดยไม่ต้องใช้ MDM ● ถ้าบริษัทไม่อนุญาตให้จัดเก็บข้อมูลความลับใน Mobile Devices บริษัทก็อาจไม่ต้องมีการเข้ารหัส แต่ในกรณีที่มีการใช้งาน Mobile Devices เพื่อจัดเก็บข้อมูลสำคัญ บริษัทก็ควรจะเข้ารหัสข้อมูลสำคัญ ไม่ว่าจะโดย MDM หรือ อุปกรณ์และวิธีการอื่นๆ

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
3.3 การเข้ารหัสข้อมูล		Advance	3.3.1.6	บริษัทจัดให้มีการตรวจสอบและติดตามว่าข้อมูลสำคัญ รวมทั้ง ข้อมูลในระดับชั้นความลับ หรือข้อมูลส่วนบุคคลที่มีการจัดเก็บ และ/หรือ ส่งผ่านทางช่องทางต่าง ๆ ได้รับการเข้ารหัสตามมาตรฐานของบริษัทอย่างครบถ้วนและเหมาะสม (โดยอาจพิจารณาความครบถ้วนโดยเปรียบเทียบจากทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูลและความเหมาะสมโดยเปรียบเทียบจากข้อกำหนดของบริษัท)	**ถาม:** อยากให้สำนักงานอธิบายการควบคุมข้อนี้เพิ่มเติม **ตอบ:** ข้อมูลในระดับชั้นความลับ หรือ ข้อมูลส่วนบุคคลที่มีการจัดเก็บ และ/หรือ ส่งผ่านช่องทางต่าง ๆ จะต้องได้รับการเข้ารหัสตามมาตรฐานของบริษัทอย่างเหมาะสม และบริษัทควรตรวจสอบความครบถ้วนของข้อมูลสำคัญเหล่านี้ว่าได้รับการเข้ารหัสครบถ้วนโดยเปรียบเทียบกับทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูล (Data Inventory)
3.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม		Intermediate	3.4.1.3	บริษัทออกแบบสถานที่และการจัดวางอุปกรณ์เทคโนโลยีสารสนเทศ และระบบเครือข่ายสื่อสารของบริษัท โดยแยกตามประเภทการใช้งาน และ/หรือ ระดับความสำคัญ โดยพิจารณาให้มีการควบคุมทางด้านกายภาพที่มั่นคงปลอดภัยและสอดคล้องกับระดับความสำคัญของอุปกรณ์สารสนเทศ	**ถาม:** ข้อนี้อาจส่งผลกระทบต่อการออกแบบ Data Center ของบริษัทที่มีการวางอุปกรณ์ Network เอาไว้สำหรับแต่ละตู้ Rack ซึ่งทางบริษัทเห็นว่าการติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศที่สำคัญไว้ในห้อง Data Center ก็น่าจะเพียงพอแล้ว ข้อนี้กำหนดให้ต้องแยก Subnet ของระบบสำคัญออกจากระบบทั่วไปด้วยหรือไม่ **ตอบ:** สำนักงาน คปภ. ได้ปรับปรุงการควบคุมโดยใช้คำว่า "หรือ" ด้วย ดังนั้น บริษัทจึงสามารถจัดวางอุปกรณ์ตามประเภทการใช้งานได้ เพื่อความสะดวกในการใช้งานและเก็บรักษา อย่างไรก็ตามให้เน้นเรื่องวัตถุประสงค์ในการรักษาความปลอดภัยทางกายภาพตามระดับความสำคัญ
3.5 การรักษาความมั่นคงปลอดภัยของ		Intermediate	3.5.1.5	บริษัทติดตั้งอุปกรณ์ในการตรวจจับและปิดกั้นการโจมตีหรือการบุกรุกโดยไม่ได้รับอนุญาต เช่น	**ถาม:** เนื่องจาก IPS มีความสามารถในการป้องกัน DoS Attack ได้ในระดับหนึ่ง แต่ไม่สามารถป้องกัน DDoS

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
ระบบเครือข่ายสื่อสาร				Intrusion Detection หรือ Prevention System (IDS/IPS) รวมทั้ง มีมาตรการเพื่อป้องกันและลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ ที่ก่อให้เกิดการหยุดชะงักในการให้บริการของระบบงานที่สำคัญ เช่น DDoS เป็นต้น	ได้ ข้อนี้กำหนดให้ต้องมีการป้องกันสำหรับ DDoS โดยตรงหรือไม่ **ตอบ:** ในกรณีที่ระบบงานสำคัญมีความเสี่ยงจากการหยุดชะงักอันเป็นผลมาจากการโจมตี เช่น มีระบบซื้อขายผ่าน Internet หรือ มีระบบสำคัญที่เป็น Web Application และสามารถเข้าถึงผ่าน Internet บริษัทก็ควรจะพิจารณาเรื่องการป้องกันการโจมตีด้วย DDoS โดยอาจเป็น service หรือ อุปกรณ์ป้องกัน DDoS โดยตรง หรือใช้งานอุปกรณ์อื่นๆ ทั้งนี้ ให้พิจารณาอุปกรณ์ที่เหมาะสมกับความเสี่ยงและมีความเพียงพอเพื่อป้องกันไม่ให้ระบบเกิดการหยุดชะงักเป็นสำคัญ
3.5 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร		Intermediate	3.5.1.9	บริษัทติดตั้งเครื่องมือ และ/หรือ กระบวนการควบคุมการรั่วไหลของข้อมูล (เช่น DLP) เพื่อป้องกัน (Block) การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลส่วนบุคคลไปยังภายนอกองค์กร	**ถาม:** ข้อนี้ถือเป็นการกำหนดให้บริษัทต้องติดตั้งระบบ DLP หรือไม่ **ตอบ:** ไม่จำเป็นเสมอไป ตัวอย่างเช่น บริษัทอาจใช้วิธีการปิดช่องทางการเชื่อมต่อ เช่น ไม่อนุญาตให้มีการใช้งาน Portable Device และใช้ Proxy ปิดการเข้าถึง Public Mail และ Public Shared Drive เพื่อการป้องกันการรั่วไหลของข้อมูลสำคัญ เป็นต้น ทั้งนี้ความจำเป็นในการติดตั้ง DLP ของบริษัทขึ้นอยู่กับการใช้งานระบบสารสนเทศ และความเสี่ยงทางด้านข้อมูลของแต่ละบริษัทด้วย
3.6 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน	3.6.3 การรักษาความมั่นคง	Advance	3.6.3.9	บริษัทติดตั้ง Patch Monitoring Software ที่ใช้ติดตาม Patch ด้านการรักษาความปลอดภัยที่ยังไม่มีการติดตั้ง และ/หรือ มีเครื่องมือที่สามารถจัดลำดับ	**ถาม:** ช่วยขยายความ "เชื่อมโยงจากแหล่งข้อมูลจาก Threat Intelligence"

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
เทคโนโลยีสารสนเทศ	ปลอดภัยเครื่องแม่ข่าย			ความสำคัญของการติดตั้ง Patch โดยให้คำนึงถึงระดับความรุนแรงของช่องโหว่ ระดับความสำคัญของระบบงาน และเชื่อมโยงจากแหล่งข้อมูลจาก Threat Intelligence (Threat Intelligence คือ หน่วยงานภายในหรือภายนอกองค์กรที่เผยแพร่ข้อมูลข่าวสาร ผลการวิเคราะห์ วิธีการหรือรูปแบบ รวมทั้งข้อเสนอแนะในการลดและควบคุมความเสี่ยงจากภัยคุกคามทางด้านสารสนเทศและไซเบอร์ เช่น Thai CERT, Ti-CERT, ETDA หรือ TB-CERT เป็นต้น)	**ตอบ:** คือ การรับข้อมูลจาก Threat Intelligence ทั้งแบบ Manual และ Auto Deploy เพื่อเชื่อมโยงไปยังอุปกรณ์สารสนเทศที่เกี่ยวข้อง ทั้งนี้ การเชื่อมโยงข้อมูลจาก Threat Intelligence สามารถช่วยระบุถึงความสำคัญจำเป็นที่ควรติดตั้ง Patch อย่างทันท่วงที เพื่อลดช่องโหว่ของระบบ นอกจากนี้ จะยังช่วยให้บริษัทมีข้อมูลเพื่อบริหารจัดการ และติดตั้งการควบคุมทดแทนในกรณีที่ไม่สามารถติดตั้ง Patch ได้ทันที
3.7 การจัดหาและพัฒนาระบบ		Baseline	3.7.1.6	บริษัทกำหนดแผนการทดสอบ และ ดำเนินการทดสอบระบบสำคัญที่จัดหาและพัฒนาขึ้นโดยพิจารณาจากทุกมุมมองทั้ง (1) ทางด้านการใช้งาน (Functionality) อาทิ Unit test, integration test, User Acceptance Test (2) ทางด้านความมั่นคงปลอดภัย (Security) อาทิ Security Test, Pentest (3) ทางด้านความสามารถในการประมวลผล (Availability) อาทิ Stress Test, Performance Test สำหรับระบบที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ (4) ทางด้านการปฏิบัติตามกฎหมาย เช่น PDPA โดย Test Case และ Test Script ที่ใช้ในการทดสอบ ต้องครอบคลุมตามความต้องการทางธุรกิจ (Business Requirements) เป็นขั้นต่ำ	**ถาม:** ขอเสนอให้ข้อนี้ครอบคลุมเฉพาะระบบที่สำคัญ เนื่องจากระบบงานเล็กๆ อาจไม่มีความจำเป็นที่จะต้องดำเนินการทดสอบให้ครบตามที่กำหนดทุกข้อ **ตอบ:** ข้อนี้อยู่ในหัวข้อการจัดหาและพัฒนาระบบ ดังนั้นจึงไม่ครอบคลุมการแก้ไขเปลี่ยนแปลงระบบย่อย นอกจากนี้ การควบคุมไม่ได้กำหนดให้บริษัทต้องทำการทดสอบในทุกด้านที่การควบคุมระบุไว้ แต่ให้บริษัทพิจารณาการทดสอบให้ครอบคลุมทุกมุมมอง ซึ่งในกรณีที่บริษัทได้พิจารณาอย่างรอบคอบแล้วว่าการทดสอบบางส่วนไม่เกี่ยวข้อง อาจไม่ต้องมีการทดสอบส่วนนั้นได้

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
3.7 การจัดหาและพัฒนาระบบ		Intermediate	3.7.1.11	บริษัทมีกระบวนการประเมินความจำเป็นในการจัดทำสัญญาและข้อตกลงการรับฝากทรัพย์สิน (Escrow Agreement) ซึ่งรวมถึง Source Code ในระบบงานสำคัญ	**ถาม:** ข้อนี้เป็นการกำหนดให้ต้องมีบุคคลที่สามที่เป็นอิสระ (Independent third party) ทำหน้าที่ในส่วนของ Escrow Agreement หรือไม่ **ตอบ:** บริษัทต้องมีการประเมินความจำเป็นในเบื้องต้น โดยถ้าบริษัทพบว่า มีความจำเป็น ก็ควรกำหนด Independent third party ในการจัดทำสัญญาและข้อตกลงการรับฝากทรัพย์สิน (Escrow Agreement)
3.8 การป้องกันความเสี่ยงด้านไซเบอร์		Intermediate	3.8.1.2	บริษัทเป็นสมาชิกกลุ่มหรือสมาคมที่แบ่งปันข้อมูลภัยคุกคามไซเบอร์ โดยบริษัทมีการกำหนดแนวทางในการดำเนินงานเพื่อตอบสนองต่อข้อมูลภัยคุกคามใหม่ๆ ที่ได้รับ เพื่อป้องกันเหตุการณ์ภัยคุกคามที่อาจเกิดขึ้น	**ถาม:** การเป็นสมาชิกของ Ti-CERT เพียงพอแล้วหรือไม่ **ตอบ:** เพียงพอ นอกจากนี้บริษัทต้องมีแนวทางในการดำเนินงานเพื่อตอบสนองต่อภัยคุกคามด้วย
3.8 การป้องกันความเสี่ยงด้านไซเบอร์		Advance	3.8.1.3	บริษัทเป็นผู้ที่มีบทบาทในการชี้แนะ แนะนำ นำเสนอ แบ่งปันข่าวสารข้อมูลภัยคุกคามไซเบอร์ให้แก่กลุ่มหรือสมาคมที่ให้ข้อมูลภัยคุกคามไซเบอร์ หรือ บริษัทอื่นๆ ในกลุ่มอุตสาหกรรม	**ถาม:** การควบคุมข้อนี้ค่อนข้างเป็นการผูกมัดบริษัทโดยที่ไม่ได้เกี่ยวข้องกับศักยภาพในการป้องกันความเสี่ยงด้านไซเบอร์ของบริษัท **ตอบ:** ข้อนี้เข้าเงื่อนไข เนื่องจากเป็นการควบคุมในการยกระดับอุตสาหกรรมโดยรวม
CM 4. การตรวจสอบและเฝ้าระวัง (Detection)					
4.1 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	4.1.1 การจัดเก็บข้อมูลบันทึกเหตุการณ์	Intermediate	4.1.1.6	ในกรณีที่ข้อมูลใน Log ประกอบไปด้วยข้อมูลส่วนบุคคล บริษัทได้พิจารณาถึงความเหมาะสม และการจัดเก็บ Log ดังกล่าวเท่าที่จำเป็นตามข้อกำหนดทางกฎหมาย นอกจากนี้ ในกรณีที่ต้องมีการจัดเก็บเป็นเวลานาน บริษัทเพิ่มความปลอดภัยด้วยการ	**ถาม:** ช่วยขยายความ "Log ประกอบไปด้วยข้อมูลส่วนบุคคล" **ตอบ:** ตัวอย่างเช่น Log ที่มีการบันทึกชื่อผู้ใช้งาน ข้อมูลส่วนบุคคลของลูกค้า ต่าง ๆ

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
				เปลี่ยนแปลงข้อมูลส่วนบุคคลให้ไม่สามารถระบุตัวตนได้ เช่น Masking หรือ Blinding	**ถาม:** กรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นเวลานาน การเข้ารหัสข้อมูล และการ masking เมื่อแสดงผล ถือว่าเพียงพอหรือไม่ **ตอบ:** เพียงพอ เนื่องจากการรักษาความปลอดภัยโดยการเข้ารหัสเป็นสิ่งที่บริษัทควรทำตามระดับความลับของข้อมูลอยู่แล้ว เมื่อเพิ่มเติมเรื่องการ Masking เข้าไปจึงถูกต้องตามรายละเอียดการควบคุม
4.2 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์		Baseline	4.2.1.5	บริษัทมีกระบวนการในการตรวจจับเหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยพิจารณาถึงการแจ้งเตือนไปยังผู้ที่เกี่ยวข้อง	**ถาม:** หมายถึง Incident Management Process ใช่หรือไม่ **ตอบ:** ใช่ โดย Incident Management Process ต้องครอบคลุมตั้งแต่วิธีการที่จะตรวจจับ ไปจนถึงการแจ้งเหตุ
4.2 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์		Intermediate	4.2.1.9	บริษัทมีเครื่องมือตรวจจับการรับส่งข้อมูลสำคัญผ่านช่องทางต่างๆ เช่น ระบบ Data Loss Prevention หรือ Data Leak Prevention เป็นต้น เพื่อตรวจจับและติดตามตรวจสอบการรั่วไหลข้อมูลสำคัญ	**ถาม:** ข้อนี้ถือเป็นการกำหนดให้บริษัทต้องติดตั้งระบบ DLP หรือไม่ **ตอบ:** ใช่
4.2 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์		Advance	4.2.1.12	บริษัทแลกเปลี่ยนข้อมูล Cyber Threat Intelligence ในเชิงรุกให้แก่บริษัทประกันภัยอื่น หน่วยงานกำกับดูแลหรือหน่วยงานที่บังคับใช้กฎหมายโดยทันทีเมื่อพบข้อมูลภัยคุกคามทางไซเบอร์ที่อาจจะกระทบต่อกลุ่มอุตสาหกรรม โดยการดำเนินงานนี้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้อง รวมทั้ง บริษัทมีกระบวนการในการ	**ถาม:** ข้อนี้ทางสำนักงาน คปภ. ควรมีส่วนร่วมในการจัดทำให้เกิดขึ้นหรือไม่ **ตอบ:** ทางสำนักงาน คปภ. มี Ti-CERT ที่สนับสนุนบริษัทประกันภัยในเรื่องนี้อยู่แล้ว โดยทางบริษัทอาจพิจารณากระบวนการเพิ่มเติมเพื่อสื่อสารกับทางสำนักงาน คปภ. ทั้งการแจ้งเหตุ และ รับทราบข้อมูลข่าวสาร

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
				สื่อสารและร่วมมือเกี่ยวกับภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอก รวมถึงมีการสื่อสารกับบุคคลภายนอกตามความเหมาะสม	**ถาม:** การควบคุมนี้ค่อนข้างเป็นการผูกมัดบริษัท โดยที่ไม่ได้เกี่ยวข้องกับศักยภาพในการป้องกันความเสี่ยงด้านไซเบอร์ของบริษัท **ตอบ:** ข้อนี้เข้าเงื่อนไข เนื่องจากเป็นการควบคุมในการยกระดับอุตสาหกรรมโดยรวม
CM 5. การรับมือและตอบสนองเมื่อพบเหตุการณ์ (Response & Recovery)					
5.1 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	5.1.1 การสำรองข้อมูล	Advance	5.1.1.3	บริษัทมีการเชื่อมต่อเพื่อปรับปรุงข้อมูลระหว่างศูนย์คอมพิวเตอร์หลัก (DC) และ ศูนย์คอมพิวเตอร์สำรอง (DR) ตลอดเวลา (Real Time Replication / Synchronization) เพื่อให้ศูนย์คอมพิวเตอร์สำรองมีข้อมูลที่เทียบเท่าศูนย์คอมพิวเตอร์หลักและสามารถใช้งานระบบสำคัญที่เกี่ยวข้องกับการให้บริการลูกค้าผ่านช่องทาง online ได้ทันที เมื่อมีเหตุการณ์เกิดขึ้น	**ถาม:** การเชื่อมต่อเพื่อปรับปรุงข้อมูลระหว่างศูนย์คอมพิวเตอร์หลัก (DC) และ ศูนย์คอมพิวเตอร์สำรอง (DR) ตลอดเวลา (Real Time Replication / Synchronization) เพื่อให้ศูนย์คอมพิวเตอร์สำรองมีข้อมูลที่เทียบเท่าศูนย์คอมพิวเตอร์หลัก ควรกำหนดตามระยะเวลาในการกู้คืนข้อมูล (อาทิ ภายใน 4 ชม.) ไม่ใช่ Real Time จึงรบกวนพิจารณาให้แก้ไขเปลี่ยนเป็นระยะเวลาที่ทางศูนย์คอมพิวเตอร์สำรอง สามารถกู้คืนข้อมูลธุรกิจภายในระยะเวลาที่บริษัทยอมรับความเสี่ยงได้และตกลงกันไว้ **ตอบ:** ถ้าเป็นลักษณะของการกู้คืนข้อมูลตามระยะเวลาที่กำหนด ได้ถูกระบุไว้ในการควบคุมข้อ 5.3.1.3 แล้ว จุดประสงค์ของการควบคุมข้อนี้เพื่อการเชื่อมต่อและปรับปรุงข้อมูลแบบ Real Time อย่างไรก็ตาม สำนักงานได้เปลี่ยนการควบคุมข้อนี้ให้จำกัดเฉพาะระบบสำคัญที่ให้บริการลูกค้าเท่านั้น

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
					ถาม: การ Sync ข้อมูลระหว่างศูนย์หลัก-ศูนย์สำรอง ทุก 1-2 ชั่วโมง แทนแบบ Real Time บริษัทสามารถตอบข้อนี้เป็น Partial ได้หรือไม่ **ตอบ:** ในข้อนี้ วัตถุประสงค์ของการควบคุมคือ การ Replicate ข้อมูลแบบ Real Time เพื่อไม่ให้ระบบสำคัญที่ให้บริการลูกค้าหยุดชะงักแต่อย่างใด ดังนั้น การ Sync ข้อมูลระหว่างศูนย์หลัก-ศูนย์สำรอง ทุก 1-2 ชั่วโมงถือว่าไม่เป็นการบรรลุวัตถุประสงค์การควบคุม จึงไม่สามารถตอบเป็น Partial ได้
5.4 การรับมือและตอบสนองเมื่อตรวจพบภัยคุกคามไซเบอร์		Intermediate	5.4.1.8	บริษัทมีกระบวนการประเมินประสิทธิภาพ ความพร้อม และศักยภาพ (Due Diligence) ของบุคคลภายนอก หรือ ที่ปรึกษาที่จะมาให้บริการที่เป็นส่วนหนึ่งของกระบวนการกู้คืนระบบสารสนเทศอย่างสม่ำเสมอ เพื่อความมั่นใจในความพร้อมในการดำเนินงานหรือการให้บริการเมื่อมีเหตุการณ์ผิดปกติทางสารสนเทศและไซเบอร์เกิดขึ้น	**ถาม:** ช่วยขยายความ การทำ Due Diligence ที่เหมาะสมด้วย **ตอบ:** อ้างอิงวิธีการคัดเลือก Third Party ใน CM6 **ถาม:** ข้อนี้รวมถึง Due Diligence สำหรับผู้ให้บริการ DC และ DR หรือไม่ รบกวนอธิบายเพิ่มเติม **ตอบ:** ถ้าบริษัทใช้บริการ Colocation หรือ Third Party ที่ให้บริการ DC/DR ก็ให้รวมด้วย
CM 6. การบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ (Third party risk management)					
6.3 หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ	6.3.1 การคัดเลือกผู้ให้บริการภายนอกหรือ	Advance	6.3.1.3	บริษัทประเมินความเสี่ยง และ การรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจที่มีความสำคัญ โดยนำประกาศนียบัตรทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ รายงานการตรวจสอบจากผู้	**ถาม:** รายงานการตรวจสอบจากผู้ตรวจสอบอิสระ (Third Party Assurance Report) หมายถึง เอกสารใดของผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจที่มีความสำคัญ

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
	พันธมิตรทางธุรกิจ			ตรวจสอบอิสระ (Third Party Assurance Report เช่น SOC 2 Type 2 Report) มาใช้หรือ มีการเข้าไปตรวจสอบการควบคุมด้วยตนเอง เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจที่มีความสำคัญ มีมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบเท่ามาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท	**ตอบ**: ตัวอย่างของ Third Party Assurance Report เช่น SOC report หรือ CIS Benchmarks เป็นต้น **ถาม:** หากไม่มี Third Party Assurance Report สามารถใช้ Due Diligent Report แทนได้หรือไม่ **ตอบ:** ถ้า Due Diligent Report ของบริษัทมีการตรวจสอบหรือสามารถทำให้มั่นใจได้ว่า ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจที่มีความสำคัญ มีมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบเท่ามาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท ก็สามารถใช้แทนได้ **ถาม:** บริษัทสามารถใช้ ISO ประจำปี ทดแทน SOC report ได้หรือไม่ **ตอบ:** ใช้ได้ แต่บริษัทควรต้องพิจารณา Scope ของ ISO Certification ด้วยว่าครอบคลุมหรือไม่ เช่น ISO 27001 ของ Data Center ของ Third Party ที่ให้บริการ Colocation สามารถพิจารณาได้ว่ามีความเพียงพอ ในขณะที่ ISO 27001 ของ Data Center ของ Third Party ที่ให้บริการ IT Operation Service อาจไม่เพียงพอ เพราะไม่ครอบคลุมบริการทางด้านสารสนเทศที่บริษัทใช้งานจาก Third Party รายนั้น

หัวข้อการควบคุม		ระดับ	รายละเอียดการควบคุม		ถาม - ตอบ
					ถาม: รบกวนอธิบาย Definition ของ Third Party เพิ่มเติม และระบุว่างานใด ที่ต้องใช้ SOC Report **ตอบ:** ตามคำจำกัดความของ Third Party คือ หน่วยงานภายนอกที่เชื่อมต่อและเข้าถึงระบบสารสนเทศของบริษัท หรือเป็นหน่วยงานภายนอกที่เข้าถึงข้อมูลของบริษัท โดยบริษัทจะต้องพิจารณาว่าการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานภายนอกเทียบเท่ากับนโยบายของบริษัทเป็นสำคัญ เช่น การนำ SOC Report มาใช้ ทั้งนี้ บริษัทสามารถนำเอกสารหรือ ข้อมูลอื่นๆ มาใช้งานทดแทน SOC Report ได้ เช่น IT Audit Report, Certification เป็นต้น
6.4 การรายงานต่อสำนักงาน คปภ.		Baseline	6.4.1.1	กระบวนการบริหารจัดการผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจของบริษัท ครอบคลุมถึง การรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้บริการจากผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ ที่ส่งผลกระทบต่อบริษัทประกันภัยตามเงื่อนไขในประกาศฯ และแนวปฏิบัติของสำนักงาน คปภ. แก่สำนักงาน คปภ. โดยไม่ชักช้า	**ถาม:** จากข้อนี้ หากพบปัญหาหรือเหตุการณ์ผิดปกติ เช่น ผู้ให้บริการภายนอกไม่สามารถให้บริการได้ (Downtime) หรือเกิดเหตุการณ์ข้อมูลรั่วไหล จำเป็นต้องรายงานแก่สำนักงาน คปภ. หรือไม่ กรุณายกตัวอย่างเหตุการณ์อื่นๆ และอธิบายเพิ่มเติม **ตอบ:** อ้างอิงตามประกาศฯ และแนวปฏิบัติของสำนักงาน