ประเด็นคำถาม - คำตอบ
แนบท้ายประกาศ เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๓

ประเด็นคำถาม	ความเห็น / คำตอบ
๑. การพิจารณาคุณสมบัติของกรรมการ ตามที่ร่างประกาศฯ กำหนดว่า “บริษัทควรมีกรรมการที่มีความรู้ หรือ ประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างน้อย ๑ คน” เพื่อให้สอดคล้องกับเจตนารมณ์ของสำนักงาน และนำไปพิจารณาประกอบการสรรหากรรมการที่มีคุณสมบัติดังกล่าวต่อไป	แนวทางการพิจารณาคุณสมบัติของกรรมการที่มีความรู้ หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ ให้บริษัทพิจารณาอย่างน้อยในประเด็นดังต่อไปนี้ (๑) จบการศึกษา ในสาขาด้านเทคโนโลยีสารสนเทศหรือสาขาที่เกี่ยวข้อง (๒) มีประสบการณ์ในตำแหน่งหัวหน้าหน่วยงานหรือมีหน้าที่รับผิดชอบเป็นผู้บริหาร / ผู้ปฏิบัติงานหลักที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศตามโครงสร้างองค์กร (๓) มีประสบการณ์หรือได้รับแต่งตั้งเป็นสมาชิกในคณะกรรมการหรือคณะทำงานที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศขององค์กร ทั้งนี้ คุณสมบัติดังกล่าวข้างต้น **<u>เป็นคำแนะนำ</u>**เพื่อเป็นแนวทางให้บริษัทนำไปประยุกต์ใช้ประกอบกับเกณฑ์ด้านอื่นในการพิจารณาตามที่บริษัทเห็นสมควร ซึ่งอาจมีความแตกต่างกันไปตามลักษณะความหลากหลายขององค์ประกอบของคณะกรรมการบริษัทในปัจจุบัน กรณี กรรมการที่เคยเข้าร่วมการอบรม หรือสัมมนาในด้านที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ สำนักงาน มีความเห็นว่า เป็นการอบรมเสริมความรู้และสร้างความตระหนักเพื่อให้กรรมการเข้าใจสถานการณ์ความเสี่ยง และการเปลี่ยนแปลงของเทคโนโลยีที่เกิดขึ้นเท่านั้น ซึ่งอาจจะยังไม่เพียงพอในการกำหนดทิศทางหรือให้ความเห็นในการกำกับดูแลการใช้เทคโนโลยีของบริษัท ทั้งนี้ ขอให้บริษัทพิจารณาคุณสมบัติหรือปัจจัยด้านอื่นประกอบการพิจารณาเป็นสำคัญ
๒. บริษัท**<u>ควรมี</u>**กรรมการที่มีความรู้ หรือประสบการณ์เกี่ยวข้องด้านเทคโนโลยีสารสนเทศอย่างน้อย ๑ ท่าน เพื่อสามารถกำหนดทิศทางการดำเนินธุรกิจสอดคล้องกับบริบทในปัจจุบัน และกำกับดูแลการใช้เทคโนโลยีสอดรับกับกลยุทธ์ในการดำเนินธุรกิจ มีความรู้เท่าทันความเสี่ยง และพัฒนาการด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป” **คำว่า “ควรมี” ประกาศไม่ได้กำหนดให้ต้องมีใช่หรือไม่**	การที่ใช้คำว่า “ควรมี” นั้น ไม่ได้มีวัตถุประสงค์เพื่อใช้บังคับว่าทุกบริษัทจะต้องมีกรรมการที่มีความรู้ประสบการณ์ด้าน IT แต่สำนักงาน ขอให้ทุกบริษัทพิจารณาตามความเหมาะสมและความจำเป็น เช่น หากบริษัทมีแผนธุรกิจที่จะมุ่งไปทางดิจิทัล มุ่งเน้นการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจ หรือบริการลูกค้า บริษัทก็ควรพิจารณากรรมการที่มีความรู้ความสามารถเพื่อมาช่วยในการกำกับดูแลในเรื่องดังกล่าว เป็นต้น
๓. บริษัทสามารถพิจารณาคุณสมบัติของกรรมการที่มีความรู้หรือประสบการณ์ด้าน IT ได้หรือไม่ **ในกรณีที่มี**ประสบการณ์ในการเป็นกรรมการหรือผู้บริหารระดับสูงในบริษัทที่<u>ดำเนินธุรกิจอัน</u>	๑) กรณีที่กรรมการ เคยมีประสบการณ์เป็น กรรมการหรือผู้บริหารระดับสูง ในบริษัทที่ดำเนินธุรกิจอันเกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือ ในบริษัทที่ต้องใช้เทคโนโลยีสารสนเทศเป็นแกนหลักในการขับเคลื่อนธุรกิจ

ประเด็นคำถาม	ความเห็น / คำตอบ
เกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือในบริษัทที่ต้องใช้เทคโนโลยีสารสนเทศเป็นแกนหลักในการขับเคลื่อนธุรกิจ หรือเคยเข้าร่วมการอบรมในหลักสูตรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศจากสมาคมส่งเสริมสถาบันกรรมการบริษัทไทย (IOD) หรือสถาบันอื่นใดซึ่งเป็นที่ยอมรับโดยทั่วไปได้หรือไม่	สำนักงาน มีความเห็นว่า กรรมการท่านดังกล่าวอาจได้รับประสบการณ์หรือมุมมองจากการมีส่วนร่วมในด้านการการกำหนดทิศทาง/นโยบาย กลยุทธ์ในการดำเนินธุรกิจหรือการตัดสินใจ หรือได้มีส่วนร่วมในการแสดงความคิดเห็นให้ข้อเสนอแนะในการประชุมคณะกรรมการบริษัทในภาพกว้างที่เกี่ยวข้องกับเรื่องเทคโนโลยีสารสนเทศ ซึ่งอาจมีประโยชน์ต่อการกำกับดูแลของบริษัท อย่างไรก็ตาม ขอให้บริษัทพิจารณาคุณสมบัติด้านอื่นๆ ประกอบเพิ่มเติม ๒) การเข้ารับการอบรม สำนักงาน มีความเห็นว่า เป็นการอบรมเสริมความรู้และสร้างความตระหนักเพื่อให้กรรมการเข้าใจสถานการณ์ความเสี่ยง และการเปลี่ยนแปลงของเทคโนโลยีที่เกิดขึ้นเท่านั้น ซึ่งอาจจะยังไม่เพียงพอในการกำหนดทิศทางหรือให้ความเห็นในการกำกับดูแลการใช้เทคโนโลยีของบริษัท
๔. บริษัทสามารถเพิ่มบทบาทหน้าที่ของคณะกรรมการบริหารความเสี่ยง เพื่อมากำกับดูแลการใช้เทคโนโลยีสารสนเทศในการดำเนินงานของบริษัทให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจในภาพรวมทั้งหมดได้หรือไม่	ในประเด็นนี้ สำนักงาน มีความเห็นว่า บริษัทควรกำหนดหน้าที่ความรับผิดชอบตามหลักการ 3 line of defense ให้ชัดเจน โดยคณะกรรมการบริหารความเสี่ยง ควรมีหน้าที่ในการกำกับดูแลการบริหารจัดการความเสี่ยงทั้งหมดของบริษัท ซึ่งไม่ควรทำหน้าที่กำกับดูแลการใช้เทคโนโลยีสารสนเทศในการดำเนินงานให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจควบคู่ไปกับเรื่องความเสี่ยงของบริษัท แต่ทั้งนี้ คณะกรรมการบริหารความเสี่ยง อาจมีความเห็นหรือให้ข้อเสนอแนะเพิ่มเติมได้ใน**มุมมองของความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศที่อาจไม่เป็นไปตามที่คณะกรรมการบริษัทให้นโยบายไว้ หรือกลยุทธ์ที่กำหนด** แต่**ไม่ควรมีส่วนเกี่ยวข้องในการกำกับดูแล หรือตัดสินใจ**การใช้เทคโนโลยีสารสนเทศในแง่มุมความเหมาะสมหรือสอดคล้องกับกลยุทธ์ที่บริษัทกำหนด **การทำหน้าที่กำกับดูแลการใช้เทคโนโลยีสารสนเทศในการดำเนินงานให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ** สำนักงาน ขอให้บริษัทควรพิจารณาบทบาทหน้าที่ความรับผิดชอบของคณะกรรมการชุดย่อยอื่นๆ ที่เกี่ยวข้องในการบริหารจัดการดำเนินธุรกิจทำหน้าที่ในส่วนนี้แทน
๕. คณะกรรมการบริษัท สามารถเข้าอบรมหลักสูตรจากองค์กรภายนอกได้หรือไม่ และในกรณีที่บริษัทจัดอบรมดังกล่าวเอง สามารถจัดทำเป็น e-training ได้หรือไม่ รวมถึงความถี่ที่เหมาะสมในการจัดอบรม	๑) คณะกรรมการบริษัทสามารถเข้ารับการอบรมให้ความรู้เกี่ยวกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ แนวโน้มการเปลี่ยนแปลงของเทคโนโลยี แนวโน้มภัยคุกคามทางไซเบอร์ และความเสี่ยงที่เกี่ยวข้องทั้งจากองค์กรภายนอกได้ ๒) กรณีที่บริษัทมีการจัดทำหลักสูตรอบรมสำหรับ

ประเด็นคำถาม	ความเห็น / คำตอบ
	คณะกรรมการบริษัทในรูปแบบ e-training สำนักงานมีความเห็นว่า เป็นสิ่งที่ดีในการปรับรูปแบบการดำเนินการให้เหมาะสมกับลักษณะ New Normal ในปัจจุบัน แต่ทั้งนี้ บริษัทควรพิจารณาความมีประสิทธิภาพและประสิทธิผลที่ผู้เข้ารับการอบรมในลักษณะนี้จะได้รับ โดยบริษัทอาจพิจารณากำหนดให้มีการวัดหรือประเมินผลหลังจากการอบรม เพื่อเพิ่มความมั่นใจว่า กรรมการบริษัทที่เข้ารับการอบรมมีความรู้ความเข้าใจในเรื่องดังกล่าวมากขึ้น ๓) ระยะเวลาในการจัดอบรม สำนักงาน มีความเห็นว่า บริษัทควรพิจารณาให้กรรมการบริษัทควรได้รับการอบรมในเรื่องดังกล่าวอย่างน้อยปีละ ๑ ครั้ง เพื่ออัพเดทความรู้ความเข้าใจรวมทั้งแนวโน้มของความเสี่ยงหรือเทคโนโลยีต่างๆ ที่เปลี่ยนแปลงไปในปัจจุบัน
๖. สำหรับกรณีที่บริษัทระบุว่ามีการปฏิบัติตาม ISO27001 จะมีส่วนช่วยให้ระดับความเสี่ยงลดลง และอยู่ในเกณฑ์ที่ คปภ. มีระดับความเชื่อมั่นวางใจในการบังคับให้ผ่อนคลายลงหรือไม่	วัตถุประสงค์ของประกาศฉบับนี้ มุ่งหวังให้บริษัทมีการกำกับดูแลและมีการบริหารจัดการ มีการควบคุมความเสี่ยงอันเกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานทั้งระบบงานหน้าบ้านและหลังบ้านทั่วทั้งองค์กร เพื่อเป็นพื้นฐานของการรักษาความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีและบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ สำหรับกรณีที่บริษัทระบุว่า ปัจจุบัน บริษัทดำเนินการปฏิบัติตามมาตรฐาน ISO27001 อยู่แล้วนั้น สำนักงานมีความเห็นว่า เป็นสิ่งที่ดีในการปฏิบัติตามมาตรฐานนี้ ซึ่งทำให้การรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศของบริษัทสอดคล้องตามข้อกำหนดของประกาศในหมวดที่ ๓ เรื่อง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) แต่ทั้งนี้ สำนักงาน ขอให้บริษัทพิจารณาเพิ่มเติมในด้านอื่นที่เกี่ยวข้อง ซึ่งจะช่วยเพิ่มระดับของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทให้มีความแข็งแกร่งขึ้น และครอบคลุมความเสี่ยงที่อาจเกิดขึ้นได้อย่างรอบด้าน เช่น ความเสี่ยงจากภัยคุกคามทางไซเบอร์ เป็นต้น โดยบริษัทสามารถพิจารณามาตรฐานสากลนอกเหนือจากมาตรฐาน ISO 27001 เช่น NIST Cybersecurity Framework เป็นต้น
๗. การบริหารจัดการการเปลี่ยนแปลง (Change Management) ในการอนุมัติการเปลี่ยนแปลงทุกอย่างเป็นลายลักษณ์อักษร ควรจะเป็นการอนุมัติการเปลี่ยนแปลงทุกอย่างผ่านผู้บริหารที่ได้รับมอบหมาย บริษัทมองว่าไม่ควรมีการระบุว่าเป็นลายลักษณ์อักษร เนื่องจากในบางครั้งการอนุมัติทำผ่านระบบหรือ email แต่หากคำว่า	ในข้อกำหนด เรื่อง การบริหารจัดการการเปลี่ยนแปลง (Change Management) มุ่งหวังให้มีกระบวนการพิจารณาของผู้ที่มีอำนาจในการตัดสินใจหรือควบคุมดูแลการเปลี่ยนแปลงของระบบ IT ของบริษัทอย่างเหมาะสม เพื่อป้องกันความเสี่ยงหรือความผิดพลาดที่อาจเกิดขึ้นกับระบบ หากไม่มีการควบคุมดูแลการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นต่อระบบ IT

ประเด็นคำถาม	ความเห็น / คำตอบ
ลายลักษณ์อักษรครอบคลุมถึงการอนุมัติผ่านระบบหรือ email บริษัทจะถือว่าไม่มีประเด็น	จากกรณีที่บริษัทสอบถาม สำนักงานมีความเห็นว่า บริษัทสามารถทำได้ แต่ควรแสดง**เอกสารหรือหลักฐานที่ทำให้ทราบว่าการ change ที่เกิดขึ้นได้ผ่านการพิจารณาอนุมัติจากผู้ที่มีอำนาจในการพิจารณาตามสิทธิที่บริษัทกำหนดเรียบร้อยแล้วเมื่อสำนักงานร้องขอ**
๘. แนวทางการกำกับดูแลการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ (cyber resilience) บริษัทจะสามารถพิจารณาใช้มาตรฐานอื่นนอกเหนือจาก NIST Cybersecurity Framework ในการกำหนดแนวทางการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ได้หรือไม่	สำนักงาน มีความเห็นว่า บริษัทสามารถพิจารณาใช้แนวทางของมาตรฐานอื่นๆ ที่เกี่ยวข้องได้ นอกเหนือจาก NIST Cybersecurity Framework ในการกำหนดแนวทางการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ แต่ทั้งนี้ บริษัทควรพิจารณาความเหมาะสมสอดคล้องให้เป็นไปตามที่ประกาศกำหนดเป็นสำคัญ
๙. การพิจารณาการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ บริษัทต้องพิจารณาข้อมูลแบบไหนเพื่อประกอบการประเมินศักยภาพของผู้ให้บริการว่าเพียงพอหรือไม่	ตัวอย่างเอกสารหรือข้อมูลที่มีรายละเอียดที่บริษัทควรพิจารณาประกอบการตัดสินใจในการคัดเลือกผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ - ข้อมูลฐานะทางการเงิน - ทุนจดทะเบียน - ความรู้และประสบการณ์ของพนักงาน - ไม่อยู่ในรายชื่อผู้ทิ้งงาน - การได้รับการรองรับตามมาตรฐานสากลที่เกี่ยวข้องเช่น ISO 27001 - การใช้เทคโนโลยีที่ไม่เป็นระบบปิดหรือระบบที่พัฒนาขึ้นใช้เองโดยเฉพาะ (Proprietary System) เพื่อไม่ให้เป็นข้อจำกัดของบริษัทในการพัฒนา หรือเชื่อมโยงข้อมูลกับระบบงานอื่นในอนาคต
๑๐. การพิจารณาบริการที่มีความเสี่ยงหรือนัยสำคัญ	บริการที่มีความเสี่ยงหรือนัยสำคัญ ในมุมมองของสำนักงาน หมายถึง บริการหรือระบบที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือระบบงานด้านเทคโนโลยีสารสนเทศที่มีการเชื่อมต่อ หรือมีการเข้าถึงจากบุคคลภายนอก โดยจะมีการเข้าถึงข้อมูลที่มีความสำคัญ เช่น ข้อมูลผู้เอาประกันภัย ข้อมูลลูกค้า ข้อมูลเกี่ยวกับแผนธุรกิจ ข้อมูลทางการเงิน ข้อมูลเกี่ยวกับการพัฒนาผลิตภัณฑ์หรือเทคโนโลยี เป็นต้น
๑๑. การทบทวนและทดสอบแผนรองรับการดำเนินธุรกิจและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้สามารถปฏิบัติงานได้จริง รวมทั้งสอบทานแผนของผู้ให้บริการภายนอก โดยควรพิจารณาความสอดคล้องกับแผนของบริษัท เนื่องจากข้อมูลแผน BCM ของผู้ให้บริการภายนอกอาจเป็นข้อมูลความลับที่ไม่สามารถแชร์ให้บริษัทได้ ฉะนั้นการ	ในการที่ สำนักงาน กำหนดให้บริษัทพิจารณาแผน BCM/BCP ของผู้ให้บริการภายนอกให้มีความสอดคล้องกับแผน BCM/BCP ของบริษัท **มีวัตถุประสงค์เพื่อ**ให้ระบบเทคโนโลยีสารสนเทศที่บริษัทใช้บริการจากผู้ให้บริการภายนอกสามารถให้บริการได้อย่างต่อเนื่อง เช่น ข้อกำหนดเรื่องระยะเวลาในการกู้คืนระบบให้กลับมาใช้งานได้ตามปกติ ซึ่งหากมีความแตกต่างหรือไม่สอดคล้องระหว่างบริษัทและผู้ให้บริการภายนอกก็จะส่งผลให้ระบบของบริษัทไม่สามารถกลับมาให้บริการได้ตามปกติตาม

ประเด็นคำถาม	ความเห็น / คำตอบ
สอบทานแผนของผู้ให้บริการภายนอกจึงอาจไม่สามารถปฏิบัติได้จริง ขอเสนอให้ทบทวนหลักเกณฑ์ดังกล่าว	ระยะเวลาที่กำหนด เป็นต้น ดังนั้น การพิจารณาในส่วนนี้ **บริษัทอาจไม่มีความจำเป็นต้องกำหนดให้ผู้ให้บริการภายนอกส่งแผน BCP มาให้พิจารณาทั้งฉบับ** แต่บริษัทควรพิจารณาประเด็นหรือข้อกำหนดต่างๆ ที่จำเป็นต้องสอดคล้องกับแผน BCP ของบริษัทเป็นสำคัญ
๑๒. ตัวอย่างที่ปรากฏใน แนวปฏิบัติเรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๓ และ แนวปฏิบัติเรื่อง หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๓ **บริษัทจำเป็นต้องกำหนดครบทุกข้อตามที่ตัวอย่างกำหนดไว้หรือไม่** เช่น - การจัดโครงสร้างการกำกับดูแลและบริหารจัดการที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ - การกำหนดระดับความเสี่ยงที่ยอมรับได้ - ตารางทะเบียนทรัพย์สินสารสนเทศ - แนวทางการควบคุมความมั่นคงปลอดภัยทางกายภาพของศูนย์คอมพิวเตอร์ - เกณฑ์ในการประเมินและจัดระดับความรุนแรงและผลกระทบของเหตุการณ์ หรือสถานการณ์การถูกโจมตีทางไซเบอร์	ตัวอย่างที่ปรากฏในแนวปฏิบัติทั้ง ๒ ฉบับดังกล่าวนั้น เป็นข้อมูลที่กำหนดหรือสมมติขึ้นเพื่อสร้างความเข้าใจและช่วยให้บริษัทเห็นภาพมากขึ้นในการนำข้อกำหนดต่างๆ ในประกาศไปปฏิบัติจริง ซึ่งสำนักงานมุ่งหวังให้เกิดประโยชน์แก่บริษัท และเป็นข้อมูลตั้งต้นเพื่อช่วยสนับสนุนผู้ที่มีส่วนในการกำกับดูแลหรือรับผิดชอบในการดำเนินการของบริษัทในส่วนต่างๆ ตามที่ประกาศกำหนดสามารถเข้าใจ ดำเนินการได้เร็วและมีประสิทธิภาพ