-ร่าง-

คู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศ ตามแนวทางการกำกับดูแลตามความเสี่ยง (IT Audit Manual - Risk Based Supervision)

.....

สำนักงาน คปภ.
๑๕ ธันวาคม ๒๕๖๐

๑. วัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้น โดยมีวัตถุประสงค์เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามการใช้เทคโนโลยีสารสนเทศของบริษัทประกันภัยให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ และเพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทประกันภัยควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม โดยเอกสารฉบับนี้ได้รวมถึงตัวอย่างการควบคุมหลักที่บริษัทประกันภัยควรถือปฏิบัติ ซึ่งเป็นเพียงตัวอย่างแนวทางการควบคุมเท่านั้น บริษัทประกันภัยสามารถเลือกที่จะใช้การควบคุมที่เหมาะสมหรือดีกว่าได้ ทั้งนี้ เพื่อให้บริษัทประกันภัยบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

๒. หน้าที่ความรับผิดชอบของสำนักงาน คปภ.

๑) กำหนดเป้าหมาย ทิศทาง ภารกิจงานตรวจสอบ เพื่อสนับสนุนการบริหารงานและการดำเนินงานด้านต่างๆ ของบริษัทประกันภัย โดยให้สอดคล้องกับนโยบายของบริษัท และกฎระเบียบที่ออกโดยสำนักงาน คปภ. หรือหน่วยงานกำกับดูแลอื่นๆ โดยคำนึงถึงประสิทธิภาพของการควบคุมภายในระบบเทคโนโลยีสารสนเทศของบริษัทประกันภัย รวมทั้งวิเคราะห์และประเมินผลการบริหารและการปฏิบัติงานของบริษัทประกันภัย

๒) กำกับดูแลและควบคุมเพื่อให้การปฏิบัติงานของบริษัทประกันภัย เป็นไปโดยมีประสิทธิภาพ ประสิทธิผล และมีความเหมาะสม รวมทั้งเสนอแนะเพื่อป้องกันมิให้เกิดความเสียหายหรือการทุจริตเกี่ยวกับการเงินหรือทรัพย์สินต่างๆ ของบริษัทประกันภัย

๓) ติดตามและกำกับดูแลเพื่อให้การปรับปรุงแก้ไขของบริษัทประกันภัยถูกต้องตามที่ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศแนะนำ

๔) ประสานงานหรือร่วมประชุมกับบริษัทประกันภัย เกี่ยวกับขอบเขตงาน แผนงาน ผลการตรวจสอบ ข้อจำกัดและปัญหาต่างๆ ที่ตรวจพบ รวมทั้งหารือเพื่อระดมความคิดเห็นและข้อเสนอแนะ ถึงวิธีการหรือมาตรการในการปรับปรุงแก้ไข เพื่อให้การปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศของบริษัทประกันภัยบรรลุเป้าหมายและเป็นไปอย่างมีประสิทธิภาพ

๕) พัฒนากรอบการกำกับดูแลและส่งเสริมให้บริษัทประกันภัยมีระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและสนับสนุนให้บริษัทประกันภัยมีการใช้เทคโนโลยีในการพัฒนาธุรกิจประกันภัยอย่างมั่นคงปลอดภัย ตลอดจนสร้างความเชื่อมั่นให้กับสาธารณชน

๖) ปฏิบัติงานอื่นด้านการตรวจสอบเทคโนโลยีสารสนเทศ ตามภารกิจที่เกี่ยวข้อง

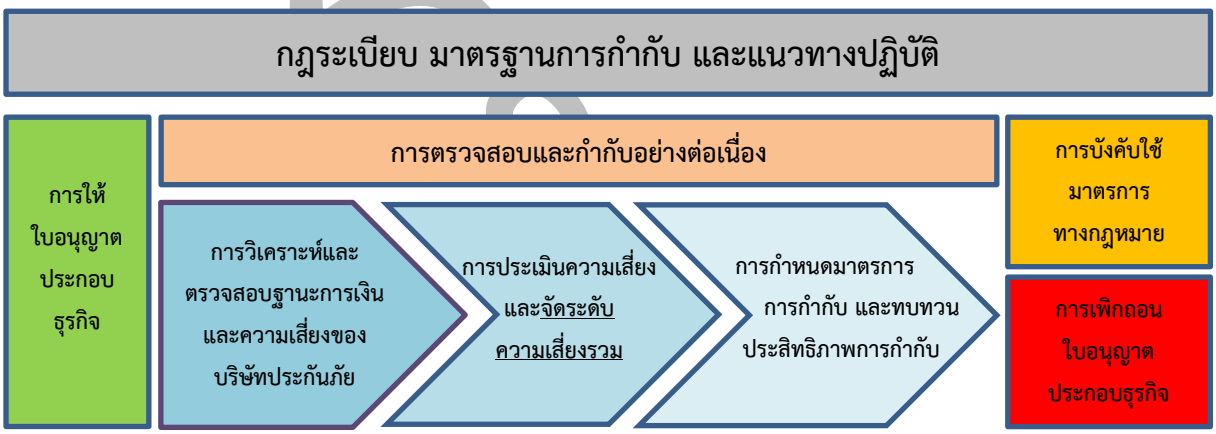
๓. คำจำกัดความ

๑) การตรวจสอบด้านเทคโนโลยีสารสนเทศ หมายถึง กิจกรรมการสร้างความเชื่อมั่น (Assurance) ต่อระบบเทคโนโลยีสารสนเทศ และการให้ข้อเสนอแนะรวมถึงแนวทางการปรับปรุงระบบงานด้านเทคโนโลยีสารสนเทศของบริษัทประกันภัยให้มีความสอดคล้องกับกฎ ระเบียบ และความเสี่ยงภัย รวมถึงการตรวจสอบเพื่อช่วยให้บริษัทประกันภัยบรรลุเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการการควบคุมทั่วไปของระบบเทคโนโลยีสารสนเทศและการควบคุมเฉพาะระบบงาน

๒) การควบคุมภายในระบบเทคโนโลยีสารสนเทศ หมายถึง กระบวนการหรือขั้นตอนการทำงานที่เป็นผลมาจากการออกแบบ โดยคณะกรรมการ ผู้บริหาร หรือบุคลากรอื่นๆ ของบริษัทประกันภัย เพื่อก่อให้เกิดความมั่นใจได้อย่างสมเหตุสมผลว่าบริษัทจะสามารถบรรลุวัตถุประสงค์ความมีประสิทธิภาพ และประสิทธิผลของการดำเนินงานระบบเทคโนโลยีสารสนเทศ

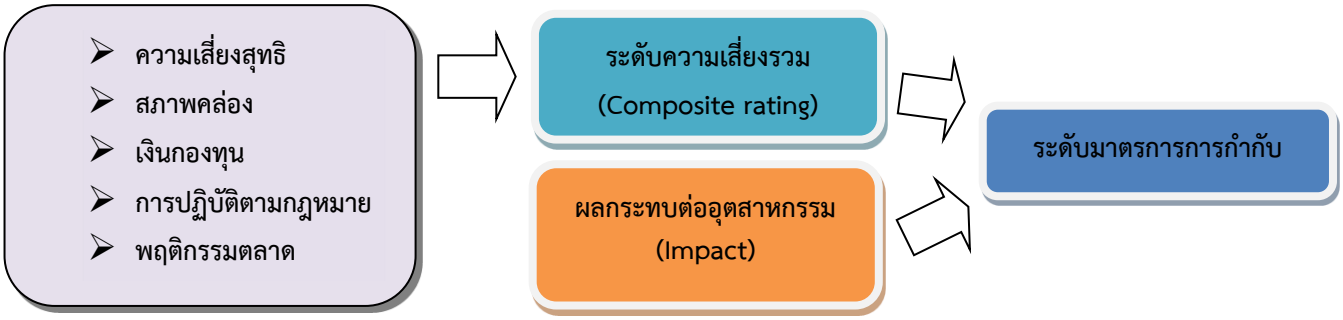
๔. การตรวจสอบด้านเทคโนโลยีสารสนเทศตามระดับความเสี่ยง

ปัจจุบัน สำนักงาน คปภ. กำกับดูแลบริษัทประกันภัยโดยใช้แนวทางการกำกับดูแลตามความเสี่ยง (Risk Based Supervision : RBS) และการจัดระดับความเสี่ยงรวม (Composite Risk Rating) ซึ่งเป็นการกำหนดกลยุทธ์การกำกับดูแลบริษัทประกันภัย โดยพิจารณาจากระดับความเสี่ยง โดยการกำกับดูแลตามความเสี่ยงนี้เป็นแนวทางที่ช่วยให้สำนักงาน คปภ. สามารถเข้าดำเนินการแทรกแซงหรือดำเนินมาตรการใดๆ ที่ช่วยป้องกันความเสียหายต่อผู้เอาประกันภัยและภาคอุตสาหกรรมได้อย่างทันท่วงที



รูปที่ ๑ : กระบวนการการกำกับดูแลตามความเสี่ยง

ในการตรวจสอบและกำกับบริษัทประกันภัย จะมีการประเมินความเสี่ยงและจัดระดับความเสี่ยงรวม (Composite Risk Rating) โดย มีองค์ประกอบที่ใช้ในการพิจารณา ดังนี้



รูปที่ ๒ : องค์ประกอบในการพิจารณากำหนดระดับความเสี่ยงรวม (Composite rating) และระดับมาตรการการกำกับ

ภายใต้แผนพัฒนาการประกันภัย ฉบับที่ ๓ (พ.ศ. ๒๕๕๙ – ๒๕๖๓) สำนักงาน คปภ. ได้กำหนดมาตรการเพื่อเพิ่มศักยภาพให้กับอุตสาหกรรมประกันภัยโดยการส่งเสริม สนับสนุน และกำกับการใช้เทคโนโลยีดิจิทัลในการดำเนินธุรกิจ ซึ่งการพัฒนาเพื่อมุ่งสู่ระบบดิจิทัลดังกล่าว ย่อมส่งผลกระทบต่อการดำเนินธุรกิจของบริษัทประกันภัย โดยเฉพาะในเรื่องการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงาน คปภ. จึงกำหนดนโยบายในการนำความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันภัยมาเป็นอีกองค์ประกอบหนึ่งในการจัดระดับความเสี่ยงรวม (Composite Risk Rating) โดยพัฒนากรอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit Framework) รวมถึงแนวทางการให้คะแนนความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Scoring) เพื่อใช้ในการกำกับดูแลและติดตามบริษัทประกันภัย

๕. ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑) ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ (IT Management Risk)

๒) ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (Operation Risk)

- ๒.๑ ความเสี่ยงที่เกี่ยวกับการรักษาความปลอดภัย (Security)
- ๒.๒ ความเสี่ยงที่เกี่ยวกับความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)
- ๒.๓ ความเสี่ยงที่เกี่ยวกับความพร้อมใช้งาน (Availability)
- ๒.๔ ความเสี่ยงด้านชื่อเสียงและการปฏิบัติตามกฎหมาย (Reputation and Regulation)

๖. แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยพิจารณาตามขอบเขตการตรวจสอบ

๑) ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ

๑.๑) การควบคุมดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยคณะกรรมการบริษัท รวมถึงผู้บริหารของบริษัท (Oversight of Technology Risks by Board of Directors and Senior Management)

๑.๒) การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risk Management)

๒) ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ

๒.๑) การรักษาความปลอดภัย (Security)

๒.๑.๑) การรักษาความปลอดภัยให้กับโครงสร้างพื้นฐานของระบบปฏิบัติการ (Operational Infrastructure Security Management) และ การควบคุมการเข้าถึง (Access Control)

๒.๑.๒) การควบคุมและป้องกันศูนย์ข้อมูล (Data Centers Protection and Controls)

๒.๑.๓) การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (Management of IT Outsourcing Risks)

๒.๒) ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)

๒.๒.๑) การสร้างและพัฒนาระบบข้อมูล (Acquisition and Development of Information Systems)

๒.๓) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability)

๒.๓.๑) การบริหารจัดการบริการทางด้านเทคโนโลยีสารสนเทศ (IT Service Management)

๒.๓.๒) การทำให้ระบบเทคโนโลยีสารสนเทศมีความน่าเชื่อถือ พร้อมใช้งาน และสามารถนำกลับมาใช้งานใหม่ได้หากเกิดกรณีฉุกเฉิน (Systems Reliability, Availability and Recoverability)

รูปที่ ๓ : แสดงความเชื่อมโยงระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๗. ตารางความเสี่ยงและตัวอย่างการควบคุมหลัก

<u>หมายเหตุ</u>: ตารางความเสี่ยงและตัวอย่างการควบคุมต่อไปนี้ เป็นการชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวทางการควบคุมหลักที่บริษัทประกันภัยควรถือปฏิบัติ ซึ่งเป็นเพียงตัวอย่างการควบคุมหลักเท่านั้น บริษัทประกันภัยสามารถเลือกใช้การควบคุมที่เหมาะสมกับสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศของบริษัทฯ ได้

กระบวนการ	ความเสี่ยง	ตัวอย่างการควบคุมหลัก
๑. การบริหารงานเทคโนโลยีสารสนเทศ		
๑.๑ การควบคุมดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยคณะกรรมการบริษัท รวมถึงผู้บริหารของบริษัท (Oversight of Technology Risks by Board of Directors and Senior Management)		
OV.๐๑ การบริหารจัดการโครงสร้างและทรัพยากรของหน่วยงานเทคโนโลยีสารสนเทศของบริษัทประกันภัย	OVR.๐๑ การจัดโครงสร้างและทรัพยากรของหน่วยงานเทคโนโลยีสารสนเทศของบริษัทประกันภัยอาจไม่เหมาะสมทำให้การแบ่งหน้าที่ไม่ถูกต้อง เป็นสาเหตุให้สามารถที่จะกระทำความผิด หรือสามารถปกปิดการกระทำความผิดได้ รวมถึงอาจไม่ได้รับทรัพยากรบุคคลที่เพียงพอเพื่อรองรับการกำกับดูแลด้านเทคโนโลยีสารสนเทศ	OVC.๐๑ มีการจัดทำ IT Organization Chart ที่มีการแบ่งแยกหน้าที่ และโครงสร้างที่สำคัญ (เช่น หน่วยงานพัฒนาระบบ (Developer) แยกจากหน่วยงานบริหารจัดการระบบ (IT Administrator)) รวมถึงต้องมีการสื่อสาร ทบทวน และอนุมัติ IT Organization Chart
	OVR.๐๒ หน่วยงานเทคโนโลยีสารสนเทศของบริษัทประกันภัยอาจไม่ได้รับการสนับสนุนจากผู้บริหารทำให้ไม่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ หรืออาจดำเนินการได้ไม่สอดคล้องตามวิสัยทัศน์ของผู้บริหาร	OVC.๐๒ มีการจัดตั้งคณะกรรมการด้านเทคโนโลยีสารสนเทศเพื่อกำกับดูแลงานด้านเทคโนโลยีสารสนเทศของบริษัทประกันภัย
	OVR.๐๓ หน้าที่รับผิดชอบงานที่สำคัญอาจไม่ได้ถูกมอบหมาย เนื่องจากไม่มีการกำหนดหน้าที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศที่ชัดเจน	OVC.๐๓ มีการจัดทำ Job Description ที่มีรายละเอียดหน้าที่ความรับผิดชอบที่สำคัญอย่างชัดเจน เป็นแนวทางให้พนักงานสามารถดำเนินงานได้ตามหน้าที่ โดยจะต้องมีการสื่อสาร ทบทวน และอนุมัติ Job Description
	OVR.๐๔ การปฏิบัติงานด้านเทคโนโลยีสารสนเทศของพนักงานอาจไม่ตรงกัน หรือไม่สอดคล้องตามวิสัยทัศน์ของผู้บริหาร	OVC.๐๔ มีการจัดทำนโยบายและขั้นตอนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีความละเอียดเพียงพอ เหมาะสม โดยมีการสื่อสาร ทบทวน และอนุมัติ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงแก้ไขที่เป็นสาระสำคัญ
	OVR.๐๕ กลยุทธ์ทางด้านเทคโนโลยีสารสนเทศอาจไม่สอดคล้องกับกลยุทธ์ทางด้านธุรกิจ ทำให้การจัดสรรทรัพยากรทางด้านเทคโนโลยีสารสนเทศไม่เหมาะสม	OVC.๐๕ มีการจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (IT Strategy Plan) ที่สอดคล้องกับแผนกลยุทธ์ด้านธุรกิจ (Business Strategy Plan) โดยแผนกลยุทธ์ฯ ต้องได้รับการสื่อสารและอนุมัติ จากผู้บริหารทางธุรกิจ OVC.๐๖ มีการรายงานแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (IT Strategy Plan) ไปยังผู้บริหารเป็นประจำ
๑.๒ การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risk Management)		
TR.๐๑ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ	TRR.๐๑ การปฏิบัติงานด้านการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอาจไม่ตรงกันหรือไม่สอดคล้องตามวิสัยทัศน์ของผู้บริหาร	TRC.๐๑ มีการจัดทำเอกสารแนวทางปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีความละเอียดเพียงพอ เหมาะสม โดยจะต้องมีการสื่อสาร ทบทวน และอนุมัติ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงแก้ไขที่เป็นสาระสำคัญ
	TRR.๐๒ ไม่มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทำให้ไม่สามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม	TRC.๐๒ มีการระบุความเสี่ยง และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันภัย โดยจะต้องได้รับการอนุมัติโดยคณะกรรมการด้านเทคโนโลยีสารสนเทศของบริษัท

กระบวนการ	ความเสี่ยง	ตัวอย่างการควบคุมหลัก
	TRR.๐๓ ไม่มีการจัดทำแผนตอบสนองต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่ได้ถูกบริหารจัดการอย่างเหมาะสม	TRC.๐๓ มีการจัดทำแผนตอบสนองต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศ และได้รับการอนุมัติโดยคณะกรรมการด้านเทคโนโลยีสารสนเทศของบริษัท
	TRR.๐๔ ไม่มีการประเมินการควบคุมด้านเทคโนโลยีสารสนเทศที่มีอยู่ในปัจจุบัน ทำให้ไม่สามารถทราบได้ถึงประสิทธิภาพของการควบคุมด้านเทคโนโลยีสารสนเทศในปัจจุบัน และอาจไม่สามารถบริหารจัดการ ปรับปรุงหรือแก้ไขได้	TRC.๐๔ มีการประเมินการควบคุมด้านเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบภายใน / ผู้ตรวจสอบอิสระ และรายงานผลการตรวจสอบต่อผู้บริหาร อย่างน้อยปีละ ๑ ครั้ง TRC.๐๕ มีการรายงานสถานะของการปรับปรุง แก้ไขการควบคุมเพื่อตอบสนองต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อผู้บริหารเป็นประจำ
๒. ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ		
๒.๑ การรักษาความปลอดภัย (Security)		
๒.๑.๑ การรักษาความปลอดภัยให้กับโครงสร้างพื้นฐานของระบบปฏิบัติการ (Operational Infrastructure Security Management) และการควบคุมการเข้าถึง (Access Control)		
OA.๐๑ นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและขั้นตอนการปฏิบัติงาน	OAR.๐๑ การปฏิบัติงานด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศอาจไม่ตรงกัน หรือไม่สอดคล้องตามวิสัยทัศน์ของผู้บริหาร	OAC.๐๑ มีการจัดทำเอกสารนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และขั้นตอนการปฏิบัติงานที่มีความละเอียดเพียงพอ เหมาะสม โดยจะต้องมีการสื่อสาร ทบทวน และอนุมัติ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงแก้ไขที่เป็นสาระสำคัญ
OA.๐๒ การบริหารจัดการบัญชีผู้ใช้งาน (User Access Request)	OAR.๐๒ มีการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต	OAC.๐๒.๐๑ มีการอนุมัติคำร้องขอการเข้าถึงระบบสารสนเทศโดยหัวหน้างานของผู้ใช้งาน (Requester Head) OAC.๐๒.๐๒ มีการสอบทานการกำหนดสิทธิของผู้ใช้งานโดยผู้ที่เหมาะสมและลงนามเป็นหลักฐานในใบคำร้องขอการเข้าถึงระบบสารสนเทศ (User Access Request)
OA.๐๓ การกำหนดสิทธิพื้นฐานในการเข้าถึงระบบสารสนเทศตามหน้าที่และความรับผิดชอบ (User Authorization Matrix)	OAR.๐๓ มีการกำหนดสิทธิในการเข้าถึงระบบสารสนเทศผิดพลาด ทำให้ผู้ใช้งานได้รับสิทธิเกินหน้าที่และความรับผิดชอบ	OAC.๐๓.๐๑ มีการกำหนดสิทธิพื้นฐานในการเข้าถึงระบบสารสนเทศตามหน้าที่และความรับผิดชอบ (User Authorization Matrix) เป็นลายลักษณ์อักษร OAC.๐๓.๐๒ มีการสอบทานเอกสารการกำหนดสิทธิพื้นฐานในการเข้าถึงระบบสารสนเทศตามหน้าที่และความรับผิดชอบ (User Authorization Matrix) โดยหน่วยงานเจ้าของระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และลงนามเป็นหลักฐานในเอกสารการสอบทานสิทธิ
OA.๐๔ การทบทวนสิทธิ และรหัสผู้ใช้งาน (User Profile Review)	OAR.๐๔ รหัสผู้ใช้งานของพนักงานที่ลาออก และรหัสผู้ใช้งานที่ไม่มีความจำเป็นในการเข้าถึงระบบสารสนเทศ (เช่น พนักงานโอนย้าย) รวมถึงรหัสผู้ใช้งานที่ได้รับสิทธิเกินหน้าที่และความรับผิดชอบ อาจไม่ถูกตรวจพบและแก้ไขได้อย่างทันท่วงที	OAC.๐๔.๐๑ มีการจัดทำรายงานการทบทวนสิทธิและรหัสผู้ใช้งานจากระบบสารสนเทศ เพื่อความครบถ้วนและถูกต้องของรหัสผู้ใช้งาน OAC.๐๔.๐๒ มีการทบทวนสิทธิ และรหัสผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง
OA.๐๕ การระงับสิทธิผู้ใช้งาน	OAR.๐๕ รหัสผู้ใช้งานของพนักงานที่ลาออก อาจไม่ได้รับการระงับการเข้าถึงอย่างทันท่วงที ทำให้มีพนักงานอื่นนำรหัสผู้ใช้งานของพนักงานที่ลาออก / โอนย้ายไปใช้งาน หรือดำเนินการในสิ่งที่ไม่เหมาะสม	OAC.๐๕.๐๑ ควรแจ้งให้หน่วยงานทรัพยากรบุคคลจัดส่งรายชื่อพนักงานลาออก / โอนย้ายมาที่ฝ่ายสารสนเทศ (IT) ก่อนวันที่พ้นสภาพ / โอนย้าย

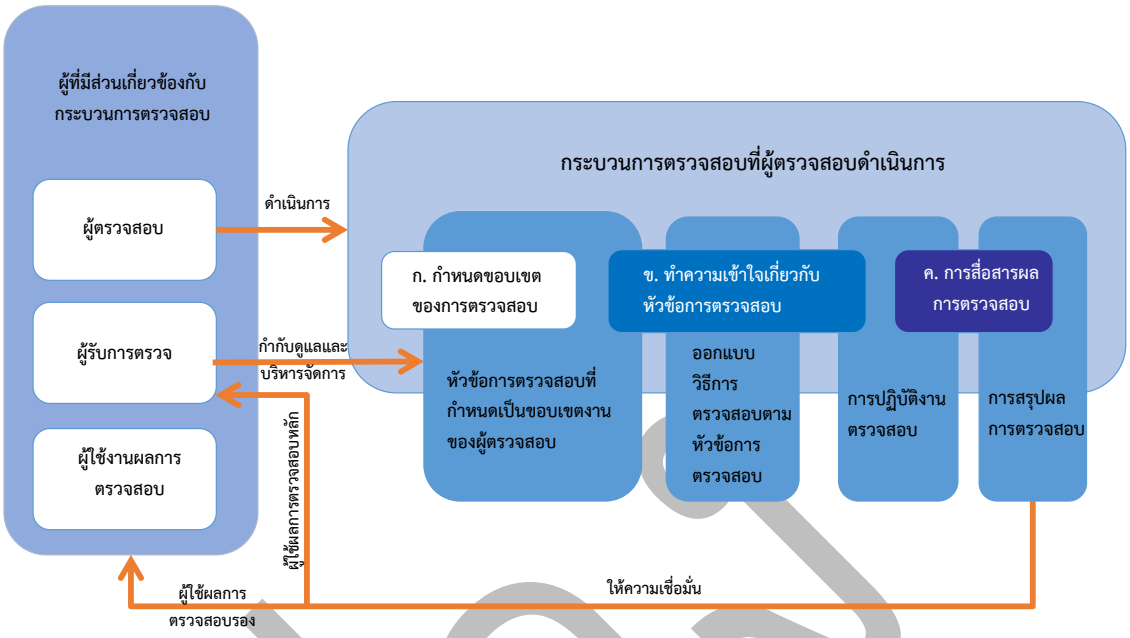
กระบวนการ	ความเสี่ยง	ตัวอย่างการควบคุมหลัก
		OAC.๐๕.๐๒ พนักงานที่มีหน้าที่บริหารจัดการสิทธิ และรหัสผู้ใช้งาน (User Admin) ทำการลบ หรือปรับปรุงสิทธิการเข้าถึงระบบสารสนเทศของพนักงานลาออก / โอนย้ายอย่างทันท่วงที
OA.๐๖ การตั้งค่าการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ	OAR.๐๖ มีการเข้าถึงระบบสารสนเทศ และข้อมูลสารสนเทศ โดยไม่ได้รับอนุญาตเนื่องจากการตั้งค่าการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ไม่เข้มแข็ง	OAC.๐๖.๐๑ มีการเปลี่ยนแปลงค่าเริ่มต้นของระบบสารสนเทศ (Default setting) และการตั้งค่ากลางของระบบสารสนเทศ (Global setting) อย่างเหมาะสม และมีความปลอดภัย OAC.๐๖.๐๒ มีการตั้งค่าการรักษาความปลอดภัย และการควบคุมรหัสผ่านอย่างเหมาะสม (Password setting) OAC.๐๖.๐๓ มีการปรับแต่งค่าการรักษาความปลอดภัย และการควบคุมรหัสผ่านแต่ละผู้ใช้งาน (Customized Profile) อย่างเหมาะสม OAC.๐๖.๐๔ มีการตั้งค่าการรักษาความปลอดภัย และจำกัดสิทธิการใช้งานของผู้ใช้งานที่มีสิทธิสูงอย่างเหมาะสม (High Privileged ID Restriction) OAC.๐๖.๐๕ มีการตั้งค่าการรักษาความปลอดภัย และจำกัดสิทธิการเข้าถึงไฟล์ และข้อมูลที่สำคัญบนระบบสารสนเทศที่ใช้งานจริง (File Permission) หมายเหตุ: การตั้งค่าการรักษาความปลอดภัย และการควบคุมหลักทั้งหมดควรดำเนินการในระดับระบบปฏิบัติการ (Operating System) ระบบงานสารสนเทศ (Application) ฐานข้อมูล (Database) และระบบเครือข่าย (Network)
OA.๐๗ การควบคุมรหัสผู้ใช้งานที่มีสิทธิสูงสุด และการเบิกใช้รหัสผู้ใช้งานที่มีสิทธิสูง	OAR.๐๗.๐๑ ไม่สามารถใช้งานรหัสผู้ใช้งานที่มีสิทธิสูงสุดได้ในกรณีฉุกเฉิน เช่น การแก้ไขปัญหาที่จำเป็นต้องใช้รหัสผู้ใช้งานที่มีสิทธิสูงสุดเท่านั้น	OAC.๐๗.๐๑ มีการจัดเก็บรหัสผู้ใช้งานและรหัสผ่านของผู้ใช้งานที่มีสิทธิสูงสุด อย่างเหมาะสม และมีความปลอดภัย พร้อมใช้งานในกรณีฉุกเฉิน
	OAR.๐๗.๐๒ มีการใช้งานรหัสผู้ใช้งานที่มีสิทธิสูงโดยไม่ได้รับอนุญาต เช่น การแก้ไขข้อมูลและระบบสารสนเทศ	OAC.๐๗.๐๒ มีการอนุมัติการเบิกใช้รหัสผู้ใช้งานที่มีสิทธิสูงตามความจำเป็น และถอนสิทธิคืนอย่างทันท่วงที
OA.๐๘ การติดตั้งอุปกรณ์รักษาความปลอดภัยทางด้านระบบเครือข่าย และการสื่อสาร	OAR.๐๘ มีการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต เนื่องจากมีการติดตั้งอุปกรณ์รักษาความปลอดภัยทางด้านระบบเครือข่ายและการสื่อสารที่ไม่เหมาะสม	OAC.๐๘ มีการติดตั้งอุปกรณ์รักษาความปลอดภัยทางด้านระบบเครือข่าย เช่น Firewall เพื่อป้องกันระบบสารสนเทศและฐานข้อมูล จากการเข้าถึงโดยไม่ได้รับอนุญาตจากเครือข่ายภายนอก
OA.๐๙ การเข้าถึงระบบสารสนเทศจากระยะไกล (Remote Access) รวมถึงการเชื่อมต่อจากเครือข่ายภายนอก	OAR.๐๙ มีการเข้าถึงระบบสารสนเทศจากระยะไกล (Remote Access) โดยไม่ได้รับอนุญาต	OAC.๐๙.๐๑ มีการจำกัดสิทธิการเข้าถึงระบบสารสนเทศจากระยะไกล (Remote Access) OAC.๐๙.๐๒ มีการควบคุมความปลอดภัยในการเชื่อมต่อระบบเครือข่ายจากภายนอก (เช่น การใช้งานเครือข่ายเสมือน (Virtual Private Network : VPN) โดยได้รับการอนุมัติให้เข้าถึงอย่างเหมาะสม

กระบวนการ	ความเสี่ยง	ตัวอย่างการควบคุมหลัก
OA.๑๐ มาตรการและกระบวนการป้องกัน ตรวจจับ และแก้ไขภัยคุกคาม	OAR.๑๐ มีภัยคุกคามด้านความปลอดภัยของข้อมูลสารสนเทศ อันเนื่องมาจากพนักงานขาดความรู้ความเข้าใจด้านการป้องกันภัยคุกคาม รวมถึงไม่สามารถตรวจจับ และแก้ไขภัยคุกคามได้อย่างทันท่วงที	OAC.๑๐.๐๑ มีการจัดอบรมความรู้ด้านการรักษาความปลอดภัยเบื้องต้น หรือการป้องกันภัยคุกคาม (Security Awareness) เป็นประจำ เพื่อให้พนักงานเข้าใจลักษณะของภัยคุกคาม และการป้องกันภัยคุกคาม OAC.๑๐.๐๒ มีมาตรการและกระบวนการป้องกัน ตรวจจับ และแก้ไขภัยคุกคาม โดยจัดทำเป็นลายลักษณ์อักษร และมีการสื่อสารทบทวน อย่างน้อยปีละ ๑ ครั้ง
OA.๑๑ การจัดเก็บและสอบทาน Log ด้านความปลอดภัยเทคโนโลยีสารสนเทศ	OAR.๑๑ มีการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต หรือการกระทำ / รายการที่ผิดปกติ อาจไม่ได้ถูกตรวจพบ และแก้ไขอย่างทันท่วงที	OAC.๑๑.๐๑ มีการจัดเก็บ Log เพื่อสอบทานอย่างเพียงพอ และมีการป้องกันการแก้ไข หรือทำลาย Log OAC.๑๑.๐๒ มีการสอบทาน Log ด้านความปลอดภัยเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
๒.๑.๒ การควบคุมและป้องกันศูนย์ข้อมูล (Data Centers Protection and Controls)		
DC.๐๑ การควบคุมและป้องกันศูนย์ข้อมูล	DCR.๐๑ มีบุคคลที่ไม่ได้รับอนุญาตเข้าถึงเครื่องแม่ข่าย (Server) และอุปกรณ์เทคโนโลยีสารสนเทศที่สำคัญ	DCC.๐๑.๐๑ มีการจัดทำระเบียบปฏิบัติการเข้าถึงศูนย์ข้อมูล (Data Centers) เป็นลายลักษณ์อักษร DCC.๐๑.๐๒ มีการจำกัดสิทธิการเข้าถึงศูนย์ข้อมูล (Data Centers) อย่างเหมาะสม โดยศูนย์ข้อมูล (Data Centers) ควรเป็นห้องปิดที่ป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต DCC.๐๑.๐๓ มีการบันทึกการเข้า-ออกศูนย์ข้อมูล (Data Centers) ของผู้เยี่ยมชม (Visitor log book)
	DCR.๐๒ ระบบงานสารสนเทศหยุดชะงัก เนื่องจากไฟฟ้าดับ หรือไฟฟ้ากระชาก ทำให้ข้อมูลสารสนเทศหรืออุปกรณ์เทคโนโลยีสารสนเทศเสียหาย	DCC.๐๒.๐๑ มีการติดตั้งอุปกรณ์สนับสนุนสภาพแวดล้อมของศูนย์ข้อมูล (Data Centers) อย่างเหมาะสม เช่น เครื่องปรับอากาศ อุปกรณ์ดับเพลิง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) และกล้องวงจรปิด (CCTV) เป็นต้น DCC.๐๒.๐๒ มีการจัดทำทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียดของอุปกรณ์ และสถานะของการบำรุงรักษา (Maintenance Agreement) โดยจะต้องปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
๒.๑.๓ การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (Management of IT Outsourcing Risks)		
MO.๐๑ การบริหารจัดการผู้ให้บริการภายนอก (Managing Outsource)	MOR.๐๑ การบริหารจัดการผู้ให้บริการภายนอกอาจไม่สอดคล้องตามวิสัยทัศน์ของผู้บริหาร	MOC.๐๑ มีการกำหนดกระบวนการและหลักเกณฑ์ในการประเมินและคัดเลือกผู้ให้บริการภายนอก
	MOR.๐๒ ไม่สามารถควบคุมและกำกับดูแลผู้ให้บริการภายนอกได้ ทำให้ไม่ได้รับการบริการที่ตอบสนองต่อความต้องการทางธุรกิจ	MOC.๐๒ มีการจัดทำสัญญาจ้างในการให้บริการ โดยมีการกำหนดเงื่อนไขให้ผู้ให้บริการภายนอกปฏิบัติตามนโยบายการรักษาความปลอดภัย และกำหนดข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่สอดคล้องตามวิสัยทัศน์ของผู้บริหาร
	MOR.๐๓ การให้บริการของผู้ให้บริการภายนอกที่ไม่สอดคล้องกับความต้องการด้านธุรกิจอาจไม่ถูกตรวจพบและแก้ไขอย่างทันท่วงที	MOC.๐๓ มีการตรวจสอบ ติดตามการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ (เทียบกับข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)

กระบวนการ	ความเสี่ยง	ตัวอย่างการควบคุมหลัก
๒.๒ ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)		
๒.๒.๑ การพัฒนาระบบงานและโปรแกรม รวมถึงการควบคุมการจัดซื้อระบบงาน (Acquisition and Development Control)		
AD.๐๑ การพัฒนาระบบงานและโปรแกรม รวมถึงการควบคุมการจัดซื้อระบบงาน (Acquisition and Development)	ADR.๐๑ ฟังก์ชันงาน หรือการควบคุมเฉพาะที่จำเป็นของระบบงาน อาจไม่ได้ถูกพัฒนา	ADC.๐๑ มีการจัดทำเอกสารความต้องการของระบบงาน (Requirement) โดยจะต้องมีการสอบทานความต้องการและอนุมัติโดยผู้ใช้งานที่เป็นเจ้าของระบบงาน
	ADR.๐๒ ระบบงานที่ถูกพัฒนาอาจทำงานไม่ถูกต้องหรือไม่เหมาะกับการปฏิบัติงาน หรือมีการทำงานที่ผิดพลาด ส่งผลให้ข้อมูลเสียหาย	ADC.๐๒ มีการทดสอบการใช้งานของระบบงานที่พัฒนาโดยผู้ใช้งาน (User Acceptance Test) และลงนามโดยผู้ใช้งาน (หรือผู้ร้องขอให้พัฒนาระบบงาน) ไว้เป็นหลักฐาน รวมถึงมีการอนุมัติให้ใช้งานจริง (Go-live)
	ADR.๐๓ การโอนย้ายฐานข้อมูล หรือการนำข้อมูลจากระบบงานเก่า ไปนำเข้าระบบงานใหม่อาจไม่ครบถ้วนถูกต้อง	ADC.๐๓ มีการทดสอบความครบถ้วนและถูกต้องของข้อมูล และลงนามโดยเจ้าของข้อมูลไว้เป็นหลักฐาน
	ADR.๐๔ การบำรุงรักษาระบบงาน หรือการแก้ไขเปลี่ยนแปลงระบบงาน เช่น Bug Fix ไม่สามารถทำได้เนื่องจากระบบงานมีความซับซ้อน และไม่มีการจัดทำเอกสารทางเทคนิคของระบบงาน	ADC.๐๔ มีการจัดทำเอกสารทางเทคนิคของระบบงาน และมีการทบทวน ปรับปรุงเมื่อมีการเปลี่ยนแปลง หรือตามระยะเวลาที่เหมาะสม
	ADR.๐๕ ผู้ใช้งานปฏิบัติงานด้วยระบบงานใหม่ผิดพลาดเนื่องจากขาดการอบรมผู้ใช้งาน หรือคู่มือการใช้งานไม่เหมาะสม มีข้อผิดพลาดหรือไม่ครบถ้วน	ADC.๐๕ มีการอบรมผู้ใช้งานในการใช้งานระบบงานใหม่ และ/หรือมีการจัดทำคู่มือการใช้งานที่เหมาะสม
PM.๐๑ การบริหารจัดการและติดตามการพัฒนาระบบงาน (Project and Change Monitoring)	PMR.๐๑ ความเสี่ยง / ปัญหาในการพัฒนาระบบงานและการแก้ไขระบบงาน อาจไม่ได้รับการบริหารจัดการอย่างเหมาะสมและทันท่วงที	PMC.๐๑ มีการติดตามผลการดำเนินการในการพัฒนาระบบงานและบริหารจัดการความเสี่ยง / ปัญหา โดยมีการรายงานผลการดำเนินการต่อผู้บริหารเป็นประจำ PMC.๐๒ มีการติดตามสถานะของการร้องขอการเปลี่ยนแปลง (Change Request) มีการจัดลำดับความสำคัญ การประเมินความเสี่ยงและผลกระทบ และรายงานผลต่อผู้บริหารเป็นประจำ
SC.๐๑ การบริหารจัดการ Source Code (Source Code Control)	SCR.๐๑ การแก้ไข ปรับปรุง ระบบงาน / โปรแกรมผิดพลาด เนื่องจากการนำ Source Code ที่ผิดพลาดมาดำเนินการ	SCC.๐๑ มีการจำกัดสิทธิผู้ที่สามารถดำเนินการ Check-in / Check-out source code SCC.๐๒ มีการอนุมัติ และสอบทานการ Check-in / Check-out source code ทุกครั้ง ในระหว่างกระบวนการพัฒนา และการปรับปรุงเปลี่ยนแปลง
CM.๐๑ การบริหารจัดการการเปลี่ยนแปลง (Change Management)	CMR.๐๑ การเปลี่ยนแปลงระบบงานโดยไม่ได้รับอนุญาตอาจทำให้ระบบงานทำงานผิดพลาด หรือทำให้ข้อมูลเสียหาย	CMC.๐๑ มีการอนุมัติให้เปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยผู้บริหารทางด้านธุรกิจ หรือเจ้าของระบบงาน CMC.๐๒ มีการอนุมัติให้เปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยผู้บริหารฝ่ายสารสนเทศ
	CMR.๐๒ ระบบงานที่เปลี่ยนแปลง อาจทำงานไม่ถูกต้องหรือไม่เหมาะกับการปฏิบัติงาน หรือมีการทำงานที่ผิดพลาด ส่งผลให้ข้อมูลเสียหาย	CMC.๐๓ มีการทดสอบระบบงานที่เปลี่ยนแปลงโดยผู้ใช้งาน (User Acceptance Test) และลงนามโดยผู้ใช้งาน (หรือผู้ร้องขอให้เปลี่ยนแปลงระบบงาน) ไว้เป็นหลักฐาน รวมถึงมีการอนุมัติให้นำระบบงานที่เปลี่ยนแปลงมาใช้งานจริง (Production)

กระบวนการ	ความเสี่ยง	ตัวอย่างการควบคุมหลัก
๒.๓ ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability)		
๒.๓.๑ การบริหารจัดการบริการทางด้านเทคโนโลยีสารสนเทศ (IT Service Management)		
SM.๐๑ การบริหารจัดการคำร้องขอบริการด้านเทคโนโลยีสารสนเทศ	SMR.๐๑ การให้บริการ หรือการแก้ไขปัญหาด้านเทคโนโลยีสารสนเทศอาจไม่ทันท่วงที ทำให้ระบบงานสารสนเทศทำงานผิดพลาด หรือไม่สามารถทำงานได้เป็นระยะเวลานาน หรือระบบงานไม่ตอบสนองต่อความต้องการทางธุรกิจ	SMC.๐๑ มีการจัดทำขั้นตอนการปฏิบัติงานเรื่องการร้องขอบริการด้านเทคโนโลยีสารสนเทศที่มีความละเอียดเพียงพอเหมาะสม โดยจะต้องมีการสื่อสาร ทบทวน และอนุมัติ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงแก้ไขที่เป็นสาระสำคัญ SMC.๐๒ มีการบันทึกเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ แก้ไข และติดตามผลการแก้ไข SMC.๐๓ มีการวิเคราะห์หาสาเหตุของเหตุการณ์ผิดปกติ และจัดเตรียมมาตรการป้องกันและแนวทางการแก้ไข
๒.๓.๒ การทำให้ระบบเทคโนโลยีสารสนเทศมีความน่าเชื่อถือ พร้อมใช้งาน และสามารถนำกลับมาใช้งานใหม่ได้หากเกิดกรณีฉุกเฉิน (Systems Reliability, Availability and Recoverability)		
BK.๐๑ การสำรองข้อมูล	BKR.๐๑ ข้อมูลที่สำคัญอาจไม่ถูกสำรองไว้อย่างเพียงพอต่อการดำเนินธุรกิจในกรณีฉุกเฉิน	BKC.๐๑ มีการออกแบบกระบวนการสำรองข้อมูลที่ครอบคลุมระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบงาน (Application) , ระบบปฏิบัติการ (Operating System) และฐานข้อมูล (Database) เป็นต้น โดยจะต้องรองรับการกู้คืนข้อมูลตามความเหมาะสมทางธุรกิจ
	BKR.๐๒ ข้อมูลที่สำรองไว้ อาจไม่พร้อมใช้งานเมื่อเกิดกรณีฉุกเฉิน	BKC.๐๒ มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่อย่างปลอดภัย โดยข้อมูลสำรองจะต้องพร้อมใช้งานอยู่เสมอ
JS.๐๑ การติดตามการสำรองข้อมูล และตารางงาน (Job Schedule)	JSR.๐๑ ตารางงาน (Job Schedule) และกระบวนการสำรองข้อมูลที่สำคัญอาจดำเนินการไม่แล้วเสร็จ หรือไม่ถูกต้องครบถ้วน หรือมีข้อผิดพลาด โดยไม่ได้ถูกแก้ไขอย่างทันท่วงที หรือตามความต้องการทางธุรกิจ ทำให้ข้อมูลที่สำรองผิดพลาดไม่สามารถนำกลับมาใช้งานได้	JSC.๐๑ มีการเฝ้าติดตามตารางงาน (Job schedule) และกระบวนการสำรองข้อมูลที่สำคัญ โดยเจ้าหน้าที่ด้านสารสนเทศ (IT Operator) รวมถึงการบันทึกผลการติดตามประจำวันบนเอกสารการติดตามงาน (run sheet) รวมถึงมีการสอบทานผลการติดตามและลงนามโดยผู้สอบทานไว้เป็นหลักฐาน
RT.๐๑ การทดสอบการกู้คืนข้อมูล	RTR.๐๑ ข้อมูลที่สำรองไว้ อาจไม่สามารถนำมากู้คืนได้ในกรณีฉุกเฉิน หรือมีความจำเป็นต้องกู้คืน เนื่องจากข้อมูลที่สำรองนั้นผิดพลาดหรือไม่ครบถ้วน	RTC.๐๑ มีการทดสอบการกู้คืนข้อมูลสำรองเป็นประจำอย่างน้อยปีละ ๑ ครั้ง
DR.๐๑ การทดสอบแผนการกู้คืนระบบสารสนเทศ (Disaster recovery plan)	DRR.๐๑ การกู้คืนระบบสารสนเทศอาจทำได้ล่าช้า หรือไม่สามารถกู้คืนระบบสารสนเทศได้ หรือการกู้คืนระบบทำให้ข้อมูลเสียหาย หรือการกู้คืนระบบทำให้ระบบงานทำงานผิดพลาด ระบบงานไม่สามารถใช้งานได้เป็นเวลานานส่งผลกระทบต่อธุรกิจ	DRP.๐๑ มีการจัดทำแผนการกู้คืนระบบสารสนเทศ (Disaster Recovery Plan) เป็นลายลักษณ์อักษร โดยจะต้องมีการสื่อสาร ทบทวน และอนุมัติ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงแก้ไขที่เป็นสาระสำคัญ DRP.๐๒ มีการทดสอบแผนการกู้คืนระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง และรายงานผลการทดสอบต่อผู้บริหารให้รับทราบ
MA.๐๑ การบริหารจัดการข้อตกลงการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (Maintenance Agreement)	MAR.๐๑ อาจไม่สามารถซ่อมบำรุงอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศได้ หรือต้องซ่อมบำรุงโดยมีค่าดำเนินการที่สูง เนื่องจากไม่มีข้อตกลงการบำรุงรักษากับผู้ให้บริการ หรือข้อตกลงหมดอายุ	MAC.๐๑ มีการติดตามระยะเวลาของข้อตกลงการบำรุงรักษาอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศ และรายงานผลการติดตามต่อผู้บริหารด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๘. กระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ



* แหล่งที่มา : COBIT ๕ for Assurance ของสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA)

รูปที่ ๔ : กระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ

สำหรับกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ จะมีผู้ที่เกี่ยวข้องหลัก ดังนี้

๑) ผู้ตรวจสอบ (Assurance Professional) หมายถึง บุคคลซึ่งเป็นผู้รับผิดชอบกิจกรรมการให้ความเชื่อมั่นระบบเทคโนโลยีสารสนเทศ และออกรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศให้แก่ผู้รับการตรวจและผู้ใช้งาน

๒) ผู้รับการตรวจ (Accountable Party) หมายถึง บุคคลหรือกลุ่มบุคคล รวมถึงผู้บริหาร ที่รับผิดชอบในการปฏิบัติงานหรือขอบเขตงานที่ถูกตรวจสอบโดยผู้ตรวจสอบ

๓) ผู้ใช้งานผลการตรวจสอบ (User) หมายถึง ผู้มีส่วนได้ส่วนเสียที่ใช้ผลลัพธ์จากกิจกรรมการให้ความเชื่อมั่นระบบเทคโนโลยีสารสนเทศ ได้แก่ ผู้บริหารงานด้านระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นผู้ใช้ผลการตรวจสอบหลัก และผู้ถือหุ้น เจ้าหนี้ ลูกค้า คณะกรรมการบริหาร คณะกรรมการตรวจสอบ หน่วยงานกำกับดูแล ซึ่งเป็นผู้ใช้งานผลการตรวจสอบรอง

กระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ แบ่งออกเป็น ๕ ขั้นตอน ดังนี้

๑) การกำหนดขอบเขตงานตรวจสอบระบบเทคโนโลยีสารสนเทศ คือ การระบุเรื่องการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยขอบเขตงานตรวจสอบอาจเป็นได้ทั้งระบบงาน กระบวนการ หรือการปฏิบัติตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒) การวางแผนงานตรวจสอบระบบเทคโนโลยีสารสนเทศ คือ การวางแผนงานตรวจสอบของสำนักงาน คปภ. รวมถึงการวางแผนงานร่วมกับบริษัทประกันภัย โดยมีรายละเอียดอย่างย่อ ดังนี้

- การวางแผนในรายละเอียดของโครงการตรวจสอบเทคโนโลยีสารสนเทศกับบริษัทประกันภัย โดยการยืนยันความเข้าใจเบื้องต้น การเข้าพบผู้บริหารของบริษัทประกันภัย และการจัดทำและนำเสนอแผนงานในรายละเอียด

- การชี้แจงและทำความเข้าใจในเบื้องต้นภายในทีมงานตรวจสอบของสำนักงาน คปภ. โดยการยืนยันบทบาทและหน้าที่ของบุคลากรภายในทีมตรวจสอบ และการจัดการประชุมชี้แจงในเบื้องต้นของทีมตรวจสอบ

๓) การปฏิบัติงานตรวจสอบระบบเทคโนโลยีสารสนเทศ มีรายละเอียดการปฏิบัติงาน ดังนี้

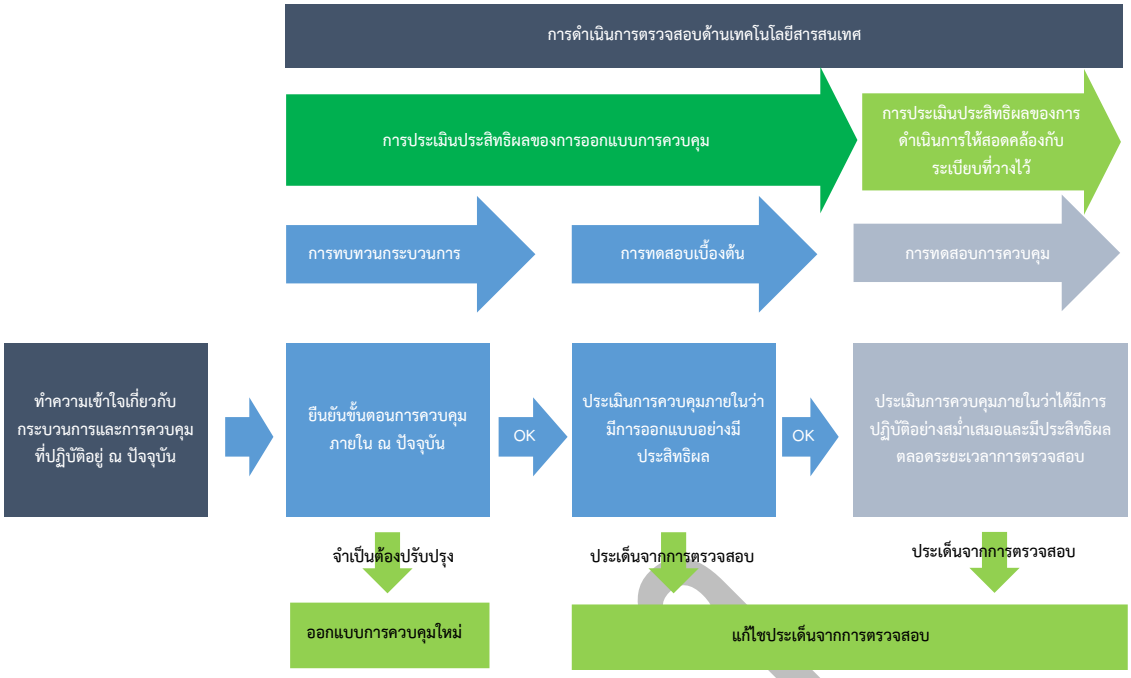
- ทำความเข้าใจเพิ่มเติม และประเมินความเสี่ยงและการควบคุมที่เกี่ยวข้องกับกระบวนการทางเทคโนโลยีสารสนเทศของบริษัทประกันภัย

- การประเมินประสิทธิผลของการออกแบบการควบคุม (Design Effectiveness Assessment) ก่อนดำเนินการทดสอบการควบคุมด้านเทคโนโลยีสารสนเทศและวิเคราะห์ในรายละเอียด ซึ่งสำนักงาน คปภ. จะทบทวนกระบวนการด้านเทคโนโลยีสารสนเทศและทดสอบทางเดินของข้อมูล/เอกสาร โดยมีรายละเอียดการปฏิบัติงานในแต่ละขั้นตอน ดังนี้

❖ <u>การทบทวนกระบวนการด้านเทคโนโลยีสารสนเทศ</u> สำนักงาน คปภ. จะดำเนินการทบทวนกระบวนการด้านเทคโนโลยีสารสนเทศที่อยู่ภายใต้ขอบเขตของงานตรวจสอบ โดยพิจารณาถึงการออกแบบและการควบคุม โดยขั้นตอนดังกล่าวจะช่วยระบุการควบคุมด้านเทคโนโลยีสารสนเทศและช่องว่างในกระบวนการที่อาจจะเกิดความเสี่ยงต่อบริษัทประกันภัย

❖ <u>การทดสอบทางเดินของข้อมูล/เอกสาร</u> สำหรับการทดสอบทางเดินของข้อมูล/เอกสารนั้น สำนักงาน คปภ. จะทดสอบโดยการติดตามกิจกรรมการปฏิบัติงานตั้งแต่เริ่มการดำเนินการตลอดจนเสร็จสิ้นกระบวนการของข้อมูล/เอกสารนั้นๆ เพื่อให้มั่นใจว่ามีการออกแบบการควบคุมภายในที่มีประสิทธิภาพ โดยหากประสิทธิผลของการออกแบบไม่เหมาะสม สำนักงาน คปภ. จะบ่งชี้ถึงจุดที่มีความเสี่ยง และข้อเสนอแนะหรือแนวทางการปรับปรุงแก้ไข หรือแนวทางการออกแบบการควบคุมใหม่

- การประเมินประสิทธิผลของการดำเนินการให้สอดคล้องกับระเบียบที่วางไว้ (Operating Effectiveness Assessment) สำหรับการควบคุมด้านเทคโนโลยีสารสนเทศที่ออกแบบมาได้อย่างมีประสิทธิภาพ สำนักงาน คปภ. จะดำเนินการทดสอบรายการและวิเคราะห์เปรียบเทียบอย่างละเอียด โดยใช้วิธีการสัมภาษณ์ สังเกตขั้นตอนการดำเนินการ ปฏิบัติงานซ้ำ และการทดสอบรายการโดยใช้เทคนิคการตรวจสอบของสำนักงาน คปภ. เพื่อให้เกิดความเชื่อมั่นว่าการควบคุมที่มีประสิทธิภาพจะได้รับการปฏิบัติโดยบุคคลที่มีหน้าที่รับผิดชอบของแต่ละส่วนงาน ซึ่งหากประสิทธิผลของการดำเนินงานไม่สอดคล้องกับระเบียบที่วางไว้นั้น สำนักงาน คปภ. จะชี้แจงถึงจุดที่มีความเสี่ยง และข้อเสนอแนะเพื่อให้เกิดประสิทธิภาพกับการควบคุมด้านเทคโนโลยีสารสนเทศต่อไป



รูปที่ ๕ : การดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศ

๔) การสรุปผลการตรวจสอบระบบเทคโนโลยีสารสนเทศ มีขั้นตอน ดังนี้

- หารือและยืนยันความเข้าใจสำหรับประเด็นที่ตรวจพบกับบริษัทประกันภัย
- จัดทำรายงานผลการตรวจสอบฉบับสมบูรณ์นำเสนอผู้บริหารสำนักงาน คปภ.
- จัดเตรียมเอกสารการประชุมและนำเสนอรายงานผลการตรวจสอบต่อผู้บริหารระดับสูงของสำนักงาน คปภ. (ถ้ามี)
- จัดทำหนังสือแจ้งผลการตรวจสอบให้บริษัทประกันภัยรับทราบ เพื่อดำเนินการปรับปรุงแก้ไขประเด็นที่ตรวจพบ

๕) การติดตามผลการตรวจสอบ มีขั้นตอน ดังนี้

- เข้าพบผู้บริหารของบริษัทประกันภัย เพื่อแจ้งกระบวนการในการติดตามผลการตรวจสอบ
- ติดตามแผนการดำเนินการแก้ไขและสอบทานวิธีการแก้ไขปรับปรุง

<u>ที่มา/เอกสารอ้างอิง</u>

๑) สายวิเคราะห์ธุรกิจประกันภัย สำนักงาน คปภ.. (๒๕๖๐). ผลการวิเคราะห์แบบสอบถามเกี่ยวกับระบบเทคโนโลยีสารสนเทศของบริษัทประกันภัย

๒) สายพัฒนามาตรฐานการกำกับ สำนักงาน คปภ. . (๒๕๖๐). ร่างแนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity)

๓) สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย. (๒๕๕๑). การตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยง (Information Technology – Risk Based Supervision)

๔) Monetary Authority of Singapore (MAS). (๒๐๑๓). Technology Risk Management Guidelines

๕) Federal Financial Institutions Examination Council (FFIEC). (๒๐๑๒). Information Technology Examination Handbook (IT Handbook)

๖) COBIT (Control Objectives for information and related Technology) for Assurance ของสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA)

๗) Global Technology Audit Guide (GTAG) ของสมาคมผู้ตรวจสอบภายใน (IIA)

.....