กรอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ
ตามแนวทางการกำกับดูแลตามความเสี่ยง
(IT Audit - Risk Based Supervision)

.....

สำนักงาน คปภ.
๒๖ กันยายน ๒๕๖๐

๑. วัตถุประสงค์

กรอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit) ฉบับนี้จัดทำขึ้น โดยมีวัตถุประสงค์เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามการใช้เทคโนโลยีสารสนเทศของบริษัทประกันภัยให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงเพื่อเป็นแนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยพิจารณาตามขอบเขตการตรวจสอบสำหรับบริษัทประกันภัย ทั้งนี้เพื่อให้บริษัทประกันภัยบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

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 รวมทั้งหารือเพื่อระดมความเห็นและข้อเสนอแนะ ถึงวิธีการหรือมาตรการในการปรับปรุงแก้ไข เพื่อให้การปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศของบริษัทประกันภัย บรรลุเป้าหมายและเป็นไปอย่างมีประสิทธิภาพ

๕) พัฒนากรอบการกำกับดูแลและส่งเสริมให้บริษัทประกันภัยมีระบบเทคโนโลยีที่มีประสิทธิภาพและสนับสนุนให้บริษัทประกันภัยมีการใช้เทคโนโลยีในการพัฒนาธุรกิจประกันภัยอย่างมั่นคงปลอดภัย ตลอดจนสร้างความเชื่อมั่นให้กับสาธารณชน

๖) ปฏิบัติงานอื่นด้านการตรวจสอบเทคโนโลยีสารสนเทศ ตามภารกิจที่เกี่ยวข้อง

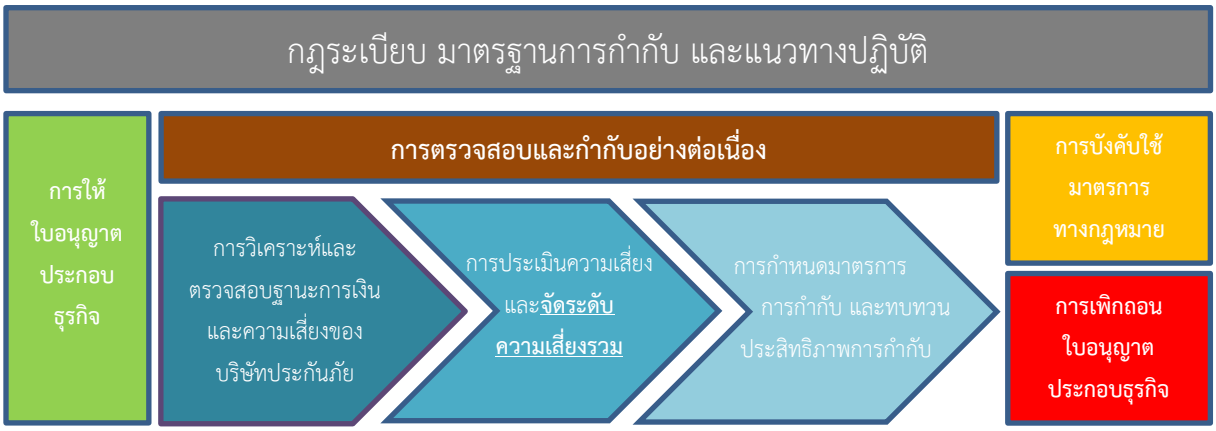
๓. คำจำกัดความ

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

๒) การควบคุมภายในระบบเทคโนโลยีสารสนเทศ หมายถึง กระบวนการหรือขั้นตอนการทำงานที่เป็นผลมาจากการออกแบบ โดยคณะกรรมการ ผู้บริหาร หรือบุคลากรอื่นๆ ของบริษัทประกันภัย เพื่อก่อให้เกิดความมั่นใจได้อย่างสมเหตุสมผลว่าบริษัทจะสามารถบรรลุวัตถุประสงค์ความมีประสิทธิผล และประสิทธิภาพของการดำเนินงานระบบเทคโนโลยีสารสนเทศ

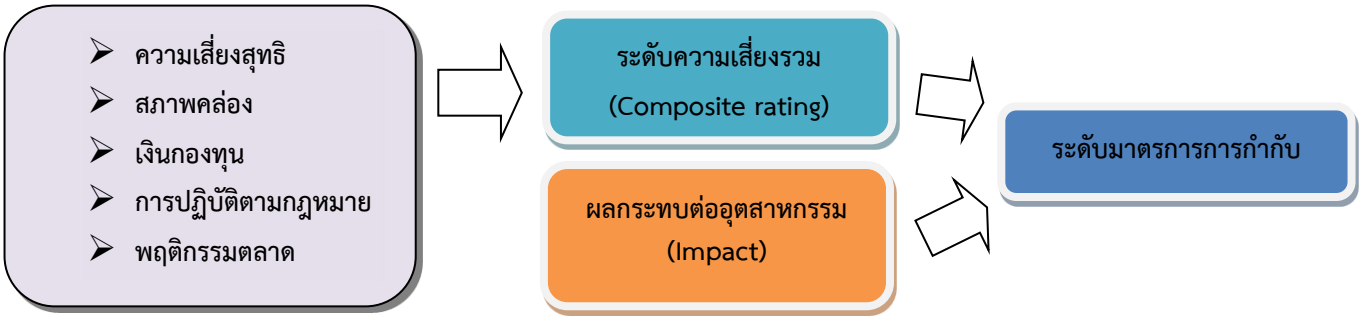
๔. การตรวจสอบด้านเทคโนโลยีสารสนเทศตามระดับความเสี่ยง

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) การบริหารงานเทคโนโลยีสารสนเทศ

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

- โครงสร้างและทรัพยากรของหน่วยงานเทคโนโลยีสารสนเทศของบริษัทประกันภัยควรสอดคล้องกับโครงสร้างโดยรวมของบริษัทประกันภัย มีความชัดเจนในการแบ่งแยกอำนาจและหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ มีการปรับปรุงทบทวนให้รองรับการทำงานอยู่เสมอ
- มีการกำหนดนโยบาย ระเบียบ และขั้นตอนการปฏิบัติงานต่างๆ ให้ครอบคลุมทุกด้านที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ และสื่อสารให้กับพนักงานภายในบริษัทรับทราบ

๑.๒) การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risk Management)

- มีการกำหนดกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และวิธีปฏิบัติในการบริหารความเสี่ยงเพื่อประเมินการควบคุม ติดตามความเสี่ยงที่เกิดจากงานด้านเทคโนโลยีสารสนเทศ และมีการตรวจสอบอย่างเพียงพอ
- มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศ

๒) ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ

๒.๑) การรักษาความปลอดภัย (Security)

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

- มีการกำหนดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) และขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง
- มีการกำหนดกระบวนการในการบริหารจัดการบัญชีผู้ใช้งาน (User Account Management)
- มีการกำหนดสิทธิในการเข้าถึงระบบสารสนเทศตามหน้าที่และความรับผิดชอบ รวมถึงกำหนดให้มีการทบทวนสิทธิอย่างสม่ำเสมอ
- มีการกำหนดให้มีการตั้งค่าการรักษาความปลอดภัย (เช่น การควบคุมด้านรหัสผ่านการเข้าถึงไฟล์ที่สำคัญ เป็นต้น) ที่ระดับระบบงาน ระบบปฏิบัติการ ระบบฐานข้อมูล และระบบเครือข่าย รวมถึงการควบคุมการรับ-ส่งข้อมูลสารสนเทศ (Information Transfer) อย่างปลอดภัย
- มีการติดตั้งอุปกรณ์การรักษาความปลอดภัยทางด้านระบบเครือข่าย และการสื่อสาร
- มีการควบคุมการเข้าถึงระบบสารสนเทศจากระยะไกล (Remote Access) รวมถึงการเชื่อมต่อจากเครือข่ายภายนอก
- มีมาตรการและกระบวนการป้องกัน ตรวจจับ และแก้ไขภัยคุกคาม เช่น โปรแกรมไม่ประสงค์ดี (Malware) เป็นต้น
- มีการจัดเก็บประวัติการทำรายการในระบบสารสนเทศที่สำคัญ เช่น Transaction Log , Security Log , System Log เป็นต้น รวมถึงมีการกำหนดกระบวนการในการสอบทานประวัติการทำรายการ

ในระบบ เช่น Transaction ที่ผิดปกติหรือน่าสงสัย การเข้าถึงข้อมูลหลัก (Master Data) ที่สำคัญ เป็นต้น อย่างสม่ำเสมอ

๒.๑.๒) การควบคุมและป้องกันศูนย์ข้อมูล (Data Centres Protection and Controls)

- มีการกำหนดระเบียบและวิธีปฏิบัติในการเข้า – ออกศูนย์ข้อมูล
- มีการจำกัดสิทธิการเข้าถึงศูนย์ข้อมูลเฉพาะผู้ได้รับอนุญาตเท่านั้น
- มีการควบคุมด้านสภาพแวดล้อมภายในศูนย์ข้อมูลที่เหมาะสม เช่น เครื่องปรับอากาศ ระบบเตือนภัยต่างๆ กล้องวงจรปิด ระบบไฟฟ้าสำรอง ระบบดับเพลิง เป็นต้น

๒.๑.๓) การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (Management of IT Outsourcing Risks)

- มีการกำหนดกระบวนการและหลักเกณฑ์ในการประเมินและคัดเลือกผู้ให้บริการภายนอก
- มีการจัดทำสัญญาว่าจ้างการให้บริการและกำหนดเงื่อนไขต่างๆ ต่อผู้ให้บริการภายนอก (Outsource) ที่ช่วยในการบริหารจัดการด้านเทคโนโลยีสารสนเทศ
- มีการกำหนดกระบวนการในการติดตาม ดูแล ประสานงาน ประเมินผล รายงาน และตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๒.๒) ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)

๒.๒.๑) การสร้างและพัฒนาระบบข้อมูล (Acquisition and Development of Information Systems)

- มีการกำหนดกระบวนการในการบริหารจัดการโครงการที่เกี่ยวข้องกับการพัฒนาระบบงานและโปรแกรม (Project Management)
- มีการกำหนดกระบวนการการควบคุมการพัฒนาระบบงานและโปรแกรม รวมทั้งการควบคุมการจัดซื้อระบบงาน (Acquisition and Development Control) เช่น กระบวนการอนุมัติคำร้องขอ การทดสอบระบบงานที่พัฒนาหรือเปลี่ยนแปลง การตรวจสอบช่องโหว่ การอนุมัติก่อนการเปลี่ยนแปลงในระบบงานจริง การควบคุม Source Code และเวอร์ชันของโปรแกรม การจัดทำเอกสารประกอบระบบงาน เป็นต้น

๒.๓) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability)

๒.๓.๑) การบริหารจัดการบริการทางด้านเทคโนโลยีสารสนเทศ (IT Service Management)

- มีการกำหนดกระบวนการในการบริหารจัดการคำร้องขอบริการด้านเทคโนโลยีสารสนเทศ (IT service)
- มีการกำหนดกระบวนการในการบริหารจัดการคำร้องขอที่เกี่ยวกับ Incident และ Problem ตั้งแต่การบันทึกคำขอ การจัดประเภท การวิเคราะห์ การบันทึกผลการแก้ไข การเฝ้าติดตามสถานะ และการปิดคำร้องขอ

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

- มีการกำหนดกระบวนการในการสำรองข้อมูลและโปรแกรมระบบงานอย่างสม่ำเสมอ

- มีการจัดเก็บสื่อสำรองข้อมูลไว้นอกสถานที่

- มีการทดสอบความพร้อมใช้งานของสื่อสำรองข้อมูลอย่างสม่ำเสมอ

- มีการกำหนดแผนการเตรียมความพร้อมสำหรับเหตุการณ์ฉุกเฉินและภัยพิบัติ รวมถึงแผนการกู้คืนระบบ และสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ

- มีการทดสอบแผนสำรองฉุกเฉินและการรายงานผลการทดสอบต่อผู้บริหารระดับสูง

- มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบงานสารสนเทศ (System Maintenance) อย่างสม่ำเสมอ

๒.๔. ความเสี่ยงด้านชื่อเสียงและการปฏิบัติตามกฎหมาย (Reputation and Regulation)

- บริษัทประกันภัยต้องมีการรักษาความลับและข้อมูลส่วนบุคคล

- บริษัทประกันภัยต้องมีการควบคุมและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้เป็นไปตามกฎหมาย กฎระเบียบของสำนักงาน คปภ. และหน่วยงานกำกับอื่นๆ ที่เกี่ยวข้อง

๗. แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อใช้ในการจัดระดับความเสี่ยงรวม

๑) ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ (IT Management Risk) พิจารณาจาก

- การวางแผนกลยุทธ์และการดำเนินงานด้านเทคโนโลยีสารสนเทศ มีระบบการจัดการ การบริหารความเสี่ยง และแผนการดำเนินงานที่มีความชัดเจน รวมถึงต้องมีการสื่อสารเป้าหมาย นโยบาย และแผนการดำเนินงานไปยังผู้ปฏิบัติงานทุกระดับ และผู้ปฏิบัตินำไปปฏิบัติอย่างมีประสิทธิผล

- การบริหารจัดการบุคลากรทางด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการแบ่งแยกหน้าที่การปฏิบัติงาน และการฝึกอบรมเพื่อพัฒนาทักษะในการปฏิบัติงาน

- การจัดให้มีการตรวจสอบและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมกิจกรรมสำคัญของธุรกิจประกันภัย

๒) ความเสี่ยงที่เกี่ยวกับการรักษาความปลอดภัย (Security) พิจารณาจาก

- ปริมาณ ของธุรกรรมทางด้านการประกันภัย หรือกิจกรรมที่ใช้เทคโนโลยีสารสนเทศในการให้บริการ รวมถึงวิธีการหรือกระบวนการที่ใช้เทคโนโลยีในการให้บริการ

- นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ครอบคลุมกิจกรรมสำคัญที่ใช้เทคโนโลยีในการดำเนินการ

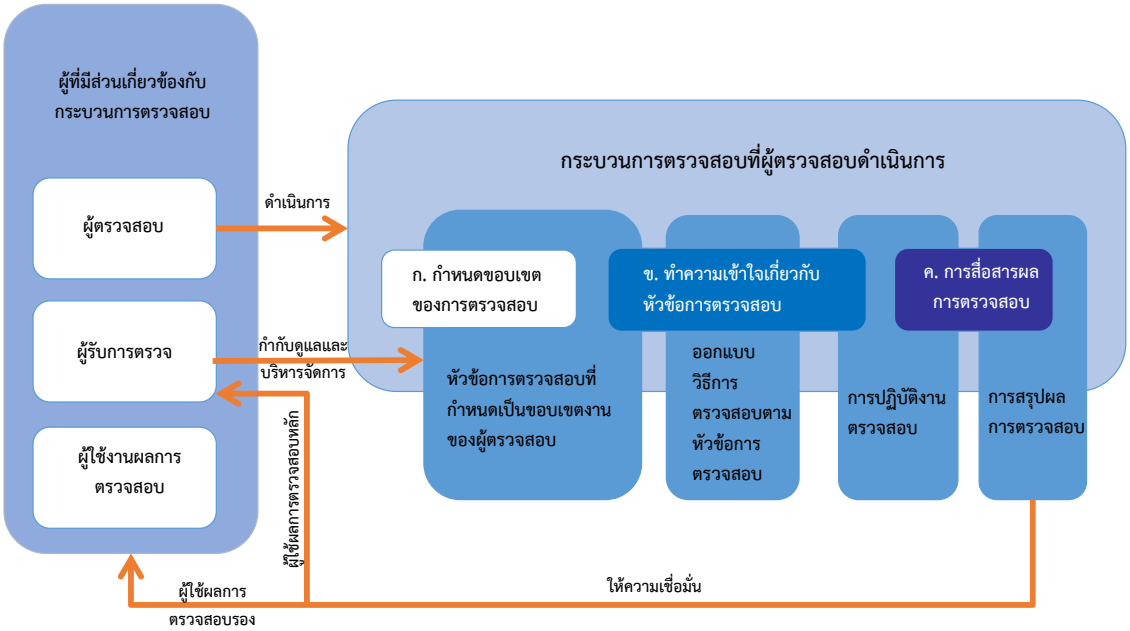
- ความเหมาะสมของโครงสร้างระบบเทคโนโลยีสารสนเทศ และเครือข่ายสื่อสาร ในการรองรับการให้บริการ รวมถึงการจัดให้มีอุปกรณ์ และการบำรุงรักษาที่เหมาะสม

๓) ความเสี่ยงที่เกี่ยวกับความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity) พิจารณาจาก การบริหารจัดการการพัฒนาระบบงาน การเชื่อมโยงข้อมูลในแต่ละกิจกรรมของการประกันภัย เพื่อป้องกันการข้อผิดพลาดของข้อมูลและรายงานที่ออกจากระบบงาน รวมถึงการควบคุม หรือมาตรการป้องกันข้อผิดพลาดจากการแก้ไข หรือเปลี่ยนแปลงระบบงาน

๔) ความเสี่ยงที่เกี่ยวกับความพร้อมใช้งาน (Availability) พิจารณาจาก การควบคุมการให้บริการเทคโนโลยีสารสนเทศเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ซึ่งรวมถึงการจัดทำแผนสำรองฉุกเฉิน และการทดสอบการกู้คืนระบบ

๕) ความเสี่ยงด้านชื่อเสียงและการปฏิบัติตามกฎหมาย (Reputation and Regulation)
พิจารณาจาก การปฏิบัติตามหลักเกณฑ์ กฎ ระเบียบ ที่มีสาระสำคัญและมีผลกระทบโดยรวมต่อบริษัท รวมถึงความสามารถและแนวทางในการลดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท

๘. กระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ



* แหล่งที่มา : COBIT ๕ for Assurance ของสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA)

รูปที่ ๓ : กระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ

สำหรับกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ จะมีผู้เกี่ยวข้องหลัก 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

โดยกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ แบ่งออกเป็น ๕ ขั้นตอน ดังนี้

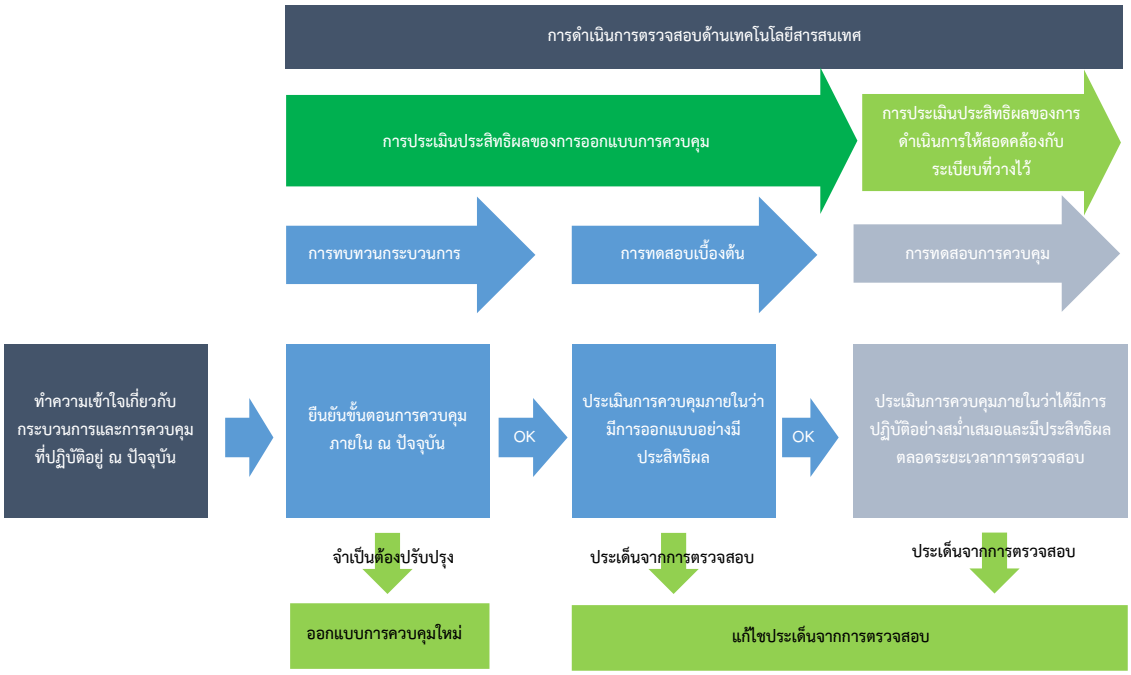
๑) การกำหนดขอบเขตงานตรวจสอบระบบเทคโนโลยีสารสนเทศ คือ การระบุเรื่องการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยขอบเขตงานตรวจสอบอาจเป็นได้ทั้งระบบงาน กระบวนการ หรือการปฏิบัติตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒) การวางแผนงานตรวจสอบระบบเทคโนโลยีสารสนเทศ คือ การวางแผนงานตรวจสอบของสำนักงาน คปภ. รวมถึงการวางแผนงานร่วมกับบริษัทประกันภัย โดยมีรายละเอียดอย่างย่อ ดังนี้

- การวางแผนในรายละเอียดของโครงการตรวจสอบเทคโนโลยีสารสนเทศกับบริษัทประกันภัย โดยการยืนยันความเข้าใจเบื้องต้น การเข้าพบผู้บริหารของบริษัทประกันภัย และการจัดทำและนำเสนอแผนงานในรายละเอียด
- การชี้แจงและทำความเข้าใจในเบื้องต้นภายในทีมงานตรวจสอบของสำนักงาน คปภ. โดยการยืนยันบทบาทและหน้าที่ของสมาชิกในทีมตรวจสอบ และการจัดการประชุมชี้แจงในเบื้องต้นของทีมตรวจสอบ

๓) การปฏิบัติงานตรวจสอบระบบเทคโนโลยีสารสนเทศ มีรายละเอียดการปฏิบัติงาน ดังนี้

- ทำความเข้าใจเพิ่มเติม และประเมินความเสี่ยงและการควบคุมที่เกี่ยวข้องกับกระบวนการทางเทคโนโลยีสารสนเทศ
- การประเมินประสิทธิผลของการออกแบบการควบคุม (Design Effectiveness Assessment) ก่อนดำเนินการทดสอบการควบคุมด้านเทคโนโลยีสารสนเทศและวิเคราะห์ในรายละเอียด สำนักงาน คปภ. จะทบทวนกระบวนการด้านเทคโนโลยีสารสนเทศและทดสอบทางเดินของข้อมูล/เอกสาร โดยมีรายละเอียดการปฏิบัติงานในแต่ละขั้นตอนดังนี้
  - <u>การทบทวนกระบวนการด้านเทคโนโลยีสารสนเทศ</u> สำนักงาน คปภ. จะดำเนินการทบทวนกระบวนการด้านเทคโนโลยีสารสนเทศที่อยู่ภายใต้ขอบเขตของงานตรวจสอบโดยพิจารณาถึงการออกแบบและการควบคุม โดยขั้นตอนดังกล่าว จะช่วยระบุการควบคุมด้านเทคโนโลยีสารสนเทศและช่องว่างในกระบวนการที่อาจจะเกิดความเสี่ยงต่อองค์กร
  - การทดสอบทางเดินของข้อมูล/เอกสาร สำหรับการทดสอบทางเดินของข้อมูล/เอกสารนั้น สำนักงาน คปภ. จะทดสอบโดยการติดตามกิจกรรมการปฏิบัติงานตั้งแต่เริ่มการดำเนินการตลอดจนเสร็จสิ้นกระบวนการของข้อมูล/เอกสารนั้นๆ เพื่อให้มั่นใจว่ามีการออกแบบการควบคุมภายในที่มีประสิทธิภาพหากประสิทธิผลของการออกแบบไม่เหมาะสม สำนักงาน คปภ. จะบ่งชี้ถึงจุดที่มีความเสี่ยง และข้อเสนอแนะหรือแนวทางการปรับปรุงแก้ไขหรือออกแบบการควบคุมใหม่
- การประเมินประสิทธิผลของการดำเนินการให้สอดคล้องกับระเบียบที่วางไว้ (Operating Effectiveness Assessment) สำหรับการควบคุมด้านเทคโนโลยีสารสนเทศที่ออกแบบมาได้อย่างมีประสิทธิภาพ สำนักงาน คปภ. จะดำเนินการทดสอบรายการและวิเคราะห์เปรียบเทียบอย่างละเอียด โดยใช้วิธีการสัมภาษณ์ สังเกตขั้นตอนการดำเนินการ ปฏิบัติงานซ้ำ และการทดสอบรายการโดยใช้เทคนิคการตรวจสอบของสำนักงาน คปภ. เพื่อให้เกิดความเชื่อมั่นการควบคุมที่มีประสิทธิภาพจะได้รับการปฏิบัติโดยบุคคลที่มีหน้าที่รับผิดชอบของแต่ละฝ่าย ซึ่งหากประสิทธิผลของการดำเนินงานไม่สอดคล้องกับระเบียบที่วางไว้นั้น สำนักงาน คปภ. จะชี้แจงถึงจุดที่มีความเสี่ยง และข้อเสนอแนะเพื่อให้เกิดประสิทธิภาพกับการควบคุมด้านเทคโนโลยีสารสนเทศต่อไป



รูปที่ ๔ : การดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศ

๔) การสรุปผลงานตรวจสอบระบบเทคโนโลยีสารสนเทศ มีขั้นตอนการดังนี้

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

๕) การติดตามผลการตรวจสอบ มีขั้นตอน ดังนี้

- เข้าพบผู้บริหารของบริษัทประกันภัย เพื่อแจ้งกระบวนการในการติดตามผลการตรวจสอบ
- ติดตามแผนการดำเนินการแก้ไขและสอบทานวิธีการแก้ไขปรับปรุง

ที่มา/เอกสารอ้างอิง

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

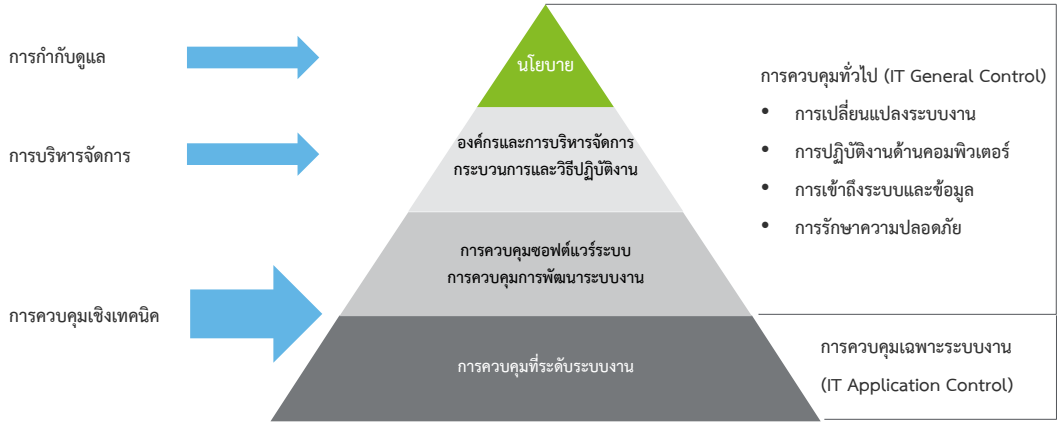
๕) Federal Financial Institutions Examination Council (FFIEC). (๒๐๑๒). Information Technology Examination Handbook (IT Handbook)

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

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

.....

ภาคผนวก ก: ประเภทการควบคุมภายในระบบเทคโนโลยีสารสนเทศ



รูปที่ ๑ : หลักการควบคุมภายในระบบเทคโนโลยีสารสนเทศ

แผนภาพข้างต้นแสดงหลักการจากบนสู่ล่าง (top-down approach) ซึ่งใช้เป็นหลักการพื้นฐานสำหรับการพิจารณาในการนำการตรวจสอบการควบคุมด้านเทคโนโลยีสารสนเทศมาใช้ปฏิบัติในองค์กร การควบคุมแต่ละระดับจะเชื่อมโยงและเกี่ยวเนื่องกัน โดยการควบคุมด้านเทคโนโลยีสารสนเทศจะเริ่มจากระดับนโยบายที่ถูกกำหนดจากฝ่ายบริหารและได้รับการสนับสนุนโดยคณะกรรมการบริษัทไปจนถึงการควบคุมเฉพาะเรื่องที่มีอยู่ในระบบงานที่ระดับผู้ปฏิบัติงาน โดยรายละเอียดของการควบคุมแต่ละระดับสามารถนำเสนอได้ดังนี้

๑. การควบคุมด้านการกำกับดูแล (Governance Control)

ความรับผิดชอบหลักสำหรับการควบคุมประเภทนี้จะอยู่ที่คณะกรรมการบริษัท (Board of Director) ซึ่งมีหน้าที่ในการจัดให้มีการกำกับดูแลกิจการที่ดี โดยการควบคุมด้านเทคโนโลยีสารสนเทศที่ระดับนี้จะเกี่ยวข้องกับการบริหารจัดการที่มีประสิทธิผล การกำหนดให้มีหลักการ นโยบาย และกระบวนการด้านการรักษาความปลอดภัย รวมถึงกระบวนการทำงานและการติดตามการปฏิบัติงานเพื่อสนับสนุนกรอบการทำงานดังกล่าว

การควบคุมด้านการกำกับดูแลจะถูกนำไปปฏิบัติโดยทั้งคณะกรรมการบริษัท Board of Director) และผู้บริหารระดับสูง (Executive Management) โดยการควบคุมเหล่านี้จะมีความเกี่ยวข้องกับการกำกับดูแลกิจการที่ดี ซึ่งนำไปสู่การบรรลุเป้าหมายและกลยุทธ์ขององค์กร รวมถึงหน่วยงานกำกับดูแล (Regulator)

ความแตกต่างระหว่างการควบคุมด้านการกำกับดูแลและการบริหารจัดการ คือ หน้าที่ความรับผิดชอบของคณะกรรมการบริษัทจะเป็นผู้เฝ้าติดตามผลการควบคุมมากกว่าดำเนินกิจกรรมการควบคุมด้วยตนเอง เช่น คณะกรรมการตรวจสอบ (Audit Committee) จะไม่ทำหน้าที่ในการตรวจสอบ แต่จะเป็นผู้เฝ้าติดตามผลการตรวจสอบจากผู้ตรวจสอบภายในและภายนอกขององค์กร เป็นต้น ตัวอย่างของการควบคุมด้านการกำกับดูแลสามารถสรุปได้ดังนี้

๑.๑ นโยบาย (Policies)

ทุกองค์กรต้องมีการกำหนดจุดหมาย (Goal) และวัตถุประสงค์ (Objective) ผ่านทางแผนกลยุทธ์ (Strategic Plan) และแถลงการณ์นโยบาย (Policy Statement) โดยองค์กรที่มีจุดหมายและวัตถุประสงค์ที่ชัดเจนจะประสบความสำเร็จ

เนื่องจากงานด้านเทคโนโลยีสารสนเทศมีความสำคัญต่อการดำเนินงานขององค์กร แถลงการณ์นโยบายที่ชัดเจนเกี่ยวกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ควรได้รับการอนุมัติจากฝ่ายบริหารและรับรองโดยคณะกรรมการบริษัท รวมถึงสื่อสารให้กับพนักงานทุกคนในองค์กร สำหรับรายละเอียดของแถลงการณ์นโยบายจะขึ้นอยู่กับขนาดองค์กรและขอบเขตการใช้งาน โดยองค์กรขนาดเล็ก การใช้แถลงการณ์นโยบายฉบับเดียวอาจเพียงพอที่จะครอบคลุมงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องทั้งหมด แต่สำหรับองค์กรขนาดใหญ่ อาจต้องกำหนดนโยบายที่มีรายละเอียดและความเฉพาะเจาะจงมากขึ้น ตามงานด้านเทคโนโลยีสารสนเทศที่ให้บริการแก่ผู้ใช้งานในองค์กร

องค์กรอาจพิจารณาให้มีแถลงการณ์นโยบายด้านเทคโนโลยีสารสนเทศ ดังนี้:

- นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) ซึ่งใช้ในการกำหนดระดับระดับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรโดยนโยบายนี้ควรถูกกำหนดให้สอดคล้องกับกฎหมายที่เกี่ยวข้อง และควรระบุระดับการควบคุมและการรักษาความปลอดภัยตามความสำคัญของระบบและข้อมูลที่ถูกประมวลผลขององค์กร
- นโยบายการจัดชั้นข้อมูลและสิทธิการเข้าถึงข้อมูลในแต่ละระดับ ซึ่งใช้ในการกำหนดขอบเขตการใช้ข้อมูลตามการอนุมัติการเข้าถึงข้อมูลในแต่ละระดับ
- คำนิยามของเจ้าของข้อมูลและระบบงาน รวมถึงสิทธิในการสร้าง แก้ไข และลบข้อมูล
- นโยบายด้านบุคคล (Personnel Policy) ซึ่งกำหนดหน้าที่ความรับผิดชอบของพนักงานองค์กรในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยอาจกำหนดให้มีการให้ลงนามในสัญญาจ้างงานโดยระบุถึงความรับผิดชอบในการรักษาความปลอดภัยและความลับข้อมูลขององค์กร
- นโยบายด้านการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Planning) ซึ่งนโยบายนี้ควรพิจาณาภาพรวมขององค์กรในการรับมือกรณีที่ระบบหยุดชะงักหรือเกิดภัยพิบัติ โดยไม่ใช่นำแค่ด้านเทคโนโลยีสารสนเทศมาพิจารณาเท่านั้น

๑.๒ มาตรฐาน (Standard)

โดยทั่วไป มาตรฐานจะถูกกำหนดขึ้นเพื่อสนับสนุนความต้องการของนโยบาย ซึ่งมาตรฐานจะถูกอนุมัติโดยฝ่ายบริหารเพื่อนำไปใช้เพื่อกำหนดวิธีการทำงานให้บรรลุวัตถุประสงค์ขององค์กร รวมถึงสื่อสารให้กับผู้เกี่ยวข้องรับทราบถึงการมีอยู่ของมาตรฐาน นอกจากนี้ มาตรฐานยังช่วยให้องค์กรสามารถปฏิบัติงานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพมากขึ้น

องค์กรอาจพิจารณาให้มีมาตรฐานด้านเทคโนโลยีสารสนเทศ ดังนี้

- กระบวนการพัฒนาระบบ เมื่อองค์กรมีการพัฒนาระบบงานเพื่อใช้สนับสนุนธุรกิจขององค์กร มาตรฐานสำหรับการพัฒนาระบบควรถูกกำหนดขึ้นเพื่อใช้ในกระบวนการออกแบบ พัฒนา ทดสอบ การนำไปใช้งาน และการบำรุงรักษาระบบงานและโปรแกรม กรณีที่องค์กรมีการว่าจ้างผู้ให้บริการภายนอกในการพัฒนาระบบงาน (outsource application development) หรือ ซื้อระบบงานจากผู้ให้บริการซอฟต์แวร์ (Software vendor) มาตรฐานในการกำหนดข้อตกลง (Agreement) ระหว่างองค์กรและผู้ให้บริการควรถูกจัดทำขึ้นเพื่อใช้เป็นแนวทางในการว่าจ้างผู้ให้บริการดังกล่าว และทำให้มั่นใจว่าข้อตกลงที่จัดทำขึ้นสอดคล้องและเป็นไปตามความต้องการขององค์กร
- การกำหนดการตั้งค่าซอฟต์แวร์ระบบ (System Software Configuration) เนื่องจากซอฟต์แวร์ระบบ (System Software) เป็นองค์ประกอบหลักในการควบคุมสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ การกำหนดค่ามาตรฐานที่เกี่ยวข้องกับการตั้งค่าการรักษาความปลอดภัยที่ระดับระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (Database) และระบบเครือข่าย (Network) จะช่วยให้สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศขององค์กรมีความปลอดภัยมากขึ้น และช่วยระบุจุดอ่อนที่นำมาใช้ปรับปรุงให้ดีขึ้นได้

๒. การควบคุมด้านการบริหารจัดการ (Management Control)

หน้าที่ความรับผิดชอบของฝ่ายบริหารสำหรับการควบคุมด้านเทคโนโลยีสารสนเทศ คือ การเข้าไปมีส่วนร่วมในทุกด้านขององค์กร และมุ่งเน้นไปที่ระบบงานและข้อมูลที่มีความสำคัญ ดังนั้น การทำงานร่วมกันระหว่างคณะกรรมการบริษัทและฝ่ายบริหารเป็นสิ่งสำคัญ ฝ่ายบริหารต้องทำให้มั่นใจว่าความควบคุมด้านเทคโนโลยีสารสนเทศที่นำมาใช้บรรลุวัตถุประสงค์องค์กร มีความน่าเชื่อถือ และถูกนำไปปฏิบัติอย่างต่อเนื่อง

องค์การและการจัดการมีบทบาทสำคัญในภาพรวมระบบการควบคุมด้านไอทีเช่นเดียวกับทุกด้านการดำเนินการขององค์กร โครงสร้างองค์กรที่เหมาะสมจะช่วยให้สามารถกำหนดสายการบังคับบัญชาและความรับผิดชอบได้อย่างมีประสิทธิผล

๒.๑ การแบ่งแยกหน้าที่ (Segregation of duties)

การแบ่งแยกหน้าที่เป็นองค์ประกอบที่สำคัญของการควบคุมส่วนใหญ่ขององค์กร โดยทั่วไป องค์กรไม่ควรมอบหมายหน้าที่ความรับผิดชอบของทั้งกระบวนการให้แก่บุคคลหรือแผนกเดียว หน้าที่งานในส่วนของการเริ่มต้น (Initiating) การอนุมัติ (Authorizing) การนำเข้า (Input) การประมวลผล (Processing) และการเช็คสอบ (Checking) ควรถูกแบ่งแยกออกจากกัน เพื่อป้องกันข้อผิดพลาด การละเว้น หรือความผิดปกติของรายการ โดยการแบ่งแยกหน้าที่สำหรับระบบงาน สามารถกำหนดได้โดยจำกัดสิทธิ์การเข้าถึงระบบงานและข้อมูลที่มีความสำคัญตามบทบาทและหน้าที่ความรับผิดชอบที่ได้รับมอบหมายเท่านั้น

การแบ่งแยกหน้าที่ด้านเทคโนโลยีสารสนเทศเบื้องต้น คือ การแบ่งแยกหน้าที่ระหว่างผู้พัฒนาระบบงาน (Development) และผู้ดำเนินงาน (Operation) โดยผู้ดำเนินงานจะเป็นผู้รับผิดชอบในการประมวลผลข้อมูล การนำโปรแกรมที่เปลี่ยนแปลงแก้ไขเข้าสู่ระบบงานจริง (Production System) โดยไม่มีความเกี่ยวข้องกับกระบวนการพัฒนาระบบ รวมถึงถูกจำกัดสิทธิ์ไม่ให้เข้าถึงหรือแก้ไขโปรแกรมและข้อมูล ในทางกลับกัน ผู้พัฒนาระบบงานจะถูกจำกัดไม่ให้เข้าถึงระบบงานจริง (Production System) เช่นกัน สำหรับองค์กรขนาดใหญ่ อาจมีการพิจารณาการแบ่งแยกหน้าที่เพิ่มเติม เช่น การจำกัดผู้ใช้งานของบัญชีผู้ใช้งานที่มีสิทธิ์สูง เป็นต้น

๒.๒ การจัดการการเปลี่ยนแปลง (Change management)

กระบวนการจัดการการเปลี่ยนแปลงควรถูกกำหนดขึ้นเพื่อให้มั่นใจว่าการเปลี่ยนแปลงสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ ซอฟต์แวร์ระบบ ระบบงาน และข้อมูล มีการควบคุมที่เหมาะสมทั้งในเรื่องของการแบ่งแยกหน้าที่ การอนุมัติการร้องขอการเปลี่ยนแปลง การทดสอบการเปลี่ยนแปลง การอนุมัติก่อนนำการเปลี่ยนแปลงไปใช้งานจริง และการเฝ้าติดตามผลการเปลี่ยนแปลงหลังนำไปใช้งานจริง นอกจากนี้ กระบวนการดังกล่าวยังช่วยป้องกันไม่ให้เกิดการเปลี่ยนแปลงที่ไม่เป็นไปตามวัตถุประสงค์องค์กร รวมถึงความผิดพลาดที่อาจเกิดจากการเปลี่ยนแปลง ในภาพรวม การจัดการการเปลี่ยนแปลงเป็นกิจกรรมที่มีความสำคัญสำหรับการควบคุมด้านเทคโนโลยีสารสนเทศ ซึ่งอาจส่งผลกระทบต่อการใช้ระบบงานทั้งในแง่ของความถูกต้องของข้อมูลและความพร้อมใช้งานของระบบถ้ามีการบริหารจัดการกระบวนการได้ไม่ดีพอ

๒.๓ การควบคุมด้านกายภาพและสภาพแวดล้อม (Physical and Environmental controls)

ปัจจุบันองค์กรส่วนใหญ่มีการลงทุนกับอุปกรณ์ด้านเทคโนโลยีสารสนเทศเป็นจำนวนเงินที่เพิ่มมากขึ้น ดังนั้น การควบคุมด้านกายภาพและสภาพแวดล้อมจึงมีความจำเป็นเพิ่มมากขึ้นเพื่อช่วยปกป้องอุปกรณ์ด้านเทคโนโลยีสารสนเทศให้สามารถใช้งานได้อย่างต่อเนื่องและสนับสนุนการดำเนินงานทางธุรกิจขององค์กร

ตัวอย่างของการควบคุมด้านกายภาพและสภาพแวดล้อม ได้แก่

- สถานที่ตั้งของเครื่องแม่ข่ายหรือเครื่องประมวลผลหลัก (Server) ต้องอยู่ในสถานที่ที่มีการจำกัดการเข้าถึงและปิดล็อคตลอดเวลา
- การเข้าถึงห้องเครือข่าย (Server room) จะถูกจำกัดการเข้าถึงเฉพาะบุคคลผู้ได้รับอนุญาตเท่านั้น
- การติดตั้งอุปกรณ์ตรวจจับและป้องกันเพลิงไหม้
- การติดตั้งอุปกรณ์ควบคุมอุณหภูมิ เช่น เครื่องปรับอากาศ และเครื่องตรวจวัดความชื้น เป็นต้น
- การติดตั้งอุปกรณ์ไฟฟ้าสำรอง เช่น UPS และ Generator เป็นต้น

นอกเหนือจากการควบคุมข้างต้น องค์กรควรพิจารณากำหนดให้มีแผนกู้คืนระบบ (Disaster Recovery Plan) เพื่อตอบสนองต่อเหตุภัยพิบัติ เช่น ไฟไหม้ หรือ น้ำท่วม และนำระบบงานกลับสู่การทำงานปกติ โดยระยะเวลาการกู้คืนระบบ ควรสอดคล้องกับนโยบายด้านการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Planning) เพื่อไม่ให้กระทบต่อการดำเนินธุรกิจในภาพรวม

๓. การควบคุมด้านเทคนิค (Technical Control)

การควบคุมด้านเทคนิคเป็นพื้นฐานการควบคุมด้านเทคโนโลยีสารสนเทศของทุกองค์กร ตัวอย่างที่ทำให้เห็นภาพชัดเจน ได้แก่ กรณีองค์กรต้องการป้องกันการเข้าถึงระบบงานหรือบุกรุกโดยไม่ได้รับอนุญาต องค์กรต้องจัดให้มีกระบวนการพิสูจน์ตัวตน (Authentication) ก่อนการเข้าถึงระบบงาน รวมถึงจัดเก็บหลักฐานการเปลี่ยนแปลงข้อมูลและการพิสูจน์ตัวตนของระบบงานทั้งหมด โดยทั่วไป การควบคุมด้านเทคนิคนี้จะเป็นไปตามเทคโนโลยีซึ่งใช้ในโครงสร้างพื้นฐาน (Infrastructure) และ นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) ขององค์กร

๓.๑ การควบคุมซอฟต์แวร์พื้นฐาน (System software control)

ซอฟต์แวร์ระบบ (System Software) เป็นส่วนประกอบด้านเทคโนโลยีสารสนเทศที่ช่วยให้ระบบงานสามารถใช้งานเพื่อสนับสนุนการทำงานของผู้ใช้งาน ผลิตภัณฑ์ของซอฟต์แวร์ระบบ ได้แก่ ระบบปฏิบัติการ (Operating System) เช่น Windows UNIX และ Linux ระบบเครือข่าย (Network) เช่น Firewall Anti-virus และระบบจัดการฐานข้อมูล (Database Management System) เช่น Oracle และ DB๒

ซอฟต์แวร์ระบบสามารถตั้งค่าเพื่อสนับสนุนการทำงานเฉพาะทางและการรักษาความปลอดภัยระดับสูง การตั้งค่าจะช่วยในเรื่องการควบคุมการเข้าถึงระบบงาน การแบ่งแยกหน้าที่งาน การจัดเก็บบันทึกหรือร่องรอยการตรวจสอบ (Audit log and trail) รวมถึงการนำไปประยุกต์ใช้ในการควบคุมความถูกต้องของข้อมูล

ตัวอย่างการควบคุมด้านเทคนิคที่เกี่ยวข้องกับซอฟต์แวร์ระบบมีดังนี้

- สิทธิการเข้าถึงระบบและข้อมูลตามนโยบายองค์กร
- การแบ่งแยกหน้าที่งานตามสิทธิที่กำหนดผ่านซอฟต์แวร์ระบบและการตั้งค่าอื่นๆ
- การตั้งค่าให้จัดเก็บบันทึกของระบบ (Audit log) และกำหนดให้มีการสอบทานอย่างต่อเนื่อง
- การตั้งค่าให้เข้ารหัสข้อมูลที่เป็นความลับขององค์กร
- บริการการเข้ารหัสที่ใช้ในกรณีที่เป็นความลับคือระบุความต้องการ
- การบริหารจัดการการติดตั้ง Patch เพื่อให้มั่นใจว่ามีการนำ Patch หรือ การเปลี่ยนแปลงอื่นๆ ไปติดตั้งในระบบปฏิบัติการ ระบบเครือข่าย และระบบฐานข้อมูล รวมถึงมีการใช้งานอย่างเหมาะสม

๓.๒ การควบคุมการพัฒนาระบบงาน (System development controls)

องค์กรควรกำหนดให้มีกระบวนการการควบคุมการพัฒนาระบบงานที่ช่วยให้มีการควบคุมที่เหมาะสมและเพียงพอเพื่อให้มั่นใจว่าระบบงานทำงานได้ตรงตามหน้าที่งานและข้อมูลที่ประมวลผลมีความถูกต้อง

ตัวอย่างการควบคุมการพัฒนาระบบงานมีดังนี้

- เอกสารความต้องการของผู้ใช้งานควรถูกจัดทำขึ้นและมีการวัดผลสำเร็จของโครงการ
- การออกแบบระบบงานควรเป็นไปตามกระบวนการที่กำหนดไว้เพื่อให้มั่นใจว่าความต้องการของผู้ใช้งานและการควบคุมได้ถูกออกแบบให้เข้ากับระบบงาน
- การทดสอบควรทำให้ครอบคลุมทุกองค์ประกอบ รวมถึงการเชื่อมต่อข้อมูลกับระบบงานอื่น (System interface) และผู้ใช้งานต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบทำงานได้ตรงความต้องการของผู้ใช้งาน
- เทคนิคการบริหารจัดการโครงการ (Project Management) ควรถูกนำมาใช้ในกระบวนการพัฒนาระบบ เพื่อช่วยในการบริหารจัดการทรัพยากรโครงการได้อย่างมีประสิทธิผล

๓.๓ การควบคุมเฉพาะระบบงาน (Application based controls)

วัตถุประสงค์ของการควบคุมเฉพาะระบบงานคือการทำให้มั่นใจว่า:

- ข้อมูลนำเข้าทั้งหมดมีความแม่นยำ สมบูรณ์ อนุมัติ และถูกต้อง
- ข้อมูลทั้งหมดได้รับการประมวลผลตามที่ตั้งใจ
- ข้อมูลที่จัดเก็บทั้งหมดมีความถูกต้องและครบถ้วน

- ผลลัพธ์ทั้งหมดถูกต้องและสมบูรณ์
- มีการบันทึกเพื่อติดตามกระบวนการตั้งแต่การนำเข้าข้อมูลจนถึงแสดงผลลัพธ์

๓.๔ การตรวจสอบการควบคุมเฉพาะระบบงานจะต้องทำความเข้าใจกระบวนการทางธุรกิจและประเมินการควบคุมที่เป็นการควบคุมแบบอัตโนมัติ (Automated Control)

ตัวอย่างการควบคุมเฉพาะระบบงานมีดังนี้

- การควบคุมข้อมูลนำเข้า (Input control) – การควบคุมประเภทนี้จะถูกใช้ในการเช็คสอบความถูกต้องของข้อมูลนำเข้าระบบงานทั้งจากพนักงานบริษัทหรือระบบงานอื่น ข้อมูลนำเข้าจะถูกเช็คสอบตามเงื่อนไขและการตั้งค่าที่กำหนดไว้ในระบบงาน
- การควบคุมการประมวลผล (Process control) – การควบคุมประเภทนี้จะเป็นแบบอัตโนมัติเพื่อให้มั่นใจว่าการประมวลผลมีความสมบูรณ์และถูกต้อง
- การควบคุมผลลัพธ์ (Output control) - การควบคุมประเภทนี้จะควบคุมสิ่งที่เกี่ยวข้องกับข้อมูล คือ การเช็คสอบและเปรียบเทียบผลลัพธ์ข้อมูลกับข้อมูลนำเข้า
- การควบคุมความถูกต้อง (Integrity control) – การควบคุมประเภทนี้จะเฝ้าติดตามกระบวนการประมวลผลข้อมูล เพื่อให้มั่นใจว่าข้อมูลยังมีความสอดคล้องและถูกต้องตามกระบวนการที่กำหนดไว้
- ร่องรอยการตรวจสอบ (Management trail) – การควบคุมประเภทนี้ คือ การจัดเก็บบันทึกหรือร่องรอยการตรวจสอบเพื่อให้ฝ่ายบริหารสามารถเช็คสอบรายการตั้งแต่กระบวนการนำเข้าข้อมูลจนถึงขั้นตอนการแสดงผลลัพธ์ โดยการควบคุมลักษณะนี้ จะช่วยฝ่ายบริหารในการเฝ้าติดตามความมีประสิทธิผลของการควบคุมในภาพรวมและหาจุดผิดพลาดเพื่อนำมาใช้ปรับปรุงกระบวนการและการควบคุมต่อไป

๓.๕ การรักษาความปลอดภัยข้อมูล (Information security)

การรักษาความปลอดภัยข้อมูลเป็นส่วนสำคัญของการควบคุมด้านด้านเทคโนโลยีสารสนเทศ โดยการรักษาความปลอดภัยของข้อมูลจะถูกนำมาใช้กับทั้งโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและข้อมูล และเป็นส่วนประกอบที่ทำให้การควบคุมด้านเทคโนโลยีสารสนเทศมีความน่าเชื่อถือ โดยทั่งไป องค์ประกอบของการรักษาความปลอดภัยข้อมูลมีดังนี้

- การรักษาความลับ (Confidentiality) – ข้อมูลที่เป็นความลับต้องได้รับการปกป้องจากการเข้าถึงและเผยแพร่โดยไม่ได้รับอนุญาต โดยการรักษาความลับต้องนำหลักการเรื่องความเป็นส่วนตัว (Privacy) มาร่วมพิจารณาด้วย
- ความถูกต้อง (Integrity) – ความถูกต้องของข้อมูลจะต้องครอบคลุมทั้งในเรื่องความถูกต้องและความสมบูรณ์ของข้อมูล รวมถึงความน่าเชื่อถือของการประมวลผลและรายงานทางการเงินด้วย
- ความพร้อมใช้งาน (Availability) - ข้อมูลจะต้องพร้อมใช้งานสำหรับลูกค้าและคู่ค้าเมื่อมีความต้องการ ความพร้อมใช้งานยังรวมถึงความสามารถในการกู้คืนข้อมูลจากความสูญเสีย การหยุดชะงัก การล่มของระบบงาน และการเกิดเหตุภัยพิบัติกับศูนย์ประมวลผลหลักขององค์กร