รายงานสรุปผลการอบรม ครั้งที่ ๒
หัวข้อ "IT Audit"
ภายใต้โครงการจัดการความรู้เพื่อสร้างเครือข่ายในการทำงาน (KM Networking)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

กลุ่มตรวจสอบภายใน (กตส.) ได้จัดการอบรม ครั้งที่ ๒ ภายใต้โครงการจัดการความรู้เพื่อสร้างเครือข่ายในการทำงาน (KM Networking) ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ผ่านระบบประชุมทางไกล (VDO Conference) ในวันอังคารที่ ๒๔ สิงหาคม ๒๕๖๔ และวันพุธที่ ๒๕ สิงหาคม ๒๕๖๔ เวลา ๙.๐๐ – ๑๖.๐๐ น. โดยมีรายละเอียดสรุปได้ ดังนี้

หัวข้อการอบรม "IT Audit"

วัตถุประสงค์ของการอบรม เพื่อเสริมสร้างศักยภาพของทีมผู้ตรวจสอบภายใน สบน. และเครือข่ายผู้ตรวจสอบ ภายในสังกัดกระทรวงการคลัง ให้มีความรู้ความเข้าใจในขั้นตอนและกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ แนวทางการวางแผนการตรวจสอบด้านเทคโนโลยีสารสนเทศตามหลักการบริหารความเสี่ยง แนวปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศ รวมทั้งเทคนิคการตรวจสอบด้านเทคโนโลยีสารสนเทศ และมาตรฐานที่เกี่ยวข้อง รวมทั้งฝึกปฏิบัติ (Workshop) โดยใช้กรณีศึกษาของ สบน. เพื่อให้ผู้ตรวจสอบภายใน สบน. สามารถนำความรู้ที่ได้ไปประยุกต์ใช้ในการปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพและสอดคล้องกับบริบทขององค์กร

วิทยากร นายวราฤทธิ์ แสงแดง CIA, CISA บริษัท ศูนย์ประมวลผล จำกัด

ผู้เข้าร่วมการอบรม ประกอบด้วย ผู้ตรวจสอบภายใน สบน. และเครือข่ายตรวจสอบภายในกรมบัญชีกลาง สำนักงานปลัดกระทรวงการคลัง สำนักงานเศรษฐกิจการคลัง และสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ จำนวนทั้งสิ้น ๑๙ คน

สรุปสาระสำคัญของการอบรม

๑. ความสำคัญของเทคโนโลยีสารสนเทศ (Information Technology)

๑.๑ ปัจจุบันสังคมมีการพัฒนาไปทางด้านเทคโนโลยีสารสนเทศ (Information technology) ปรับเปลี่ยนจากสังคมอุตสาหกรรมกลายเป็นสังคมสารสนเทศ ส่งผลให้ระบบเศรษฐกิจเปลี่ยนจากระบบแห่งชาติไปเป็นเศรษฐกิจโลกที่ทำให้ระบบเศรษฐกิจของโลกผูกพันกับทุกประเทศ และความเชื่อมโยงของเครือข่ายสารสนเทศทำให้เกิดสังคมโลกาภิวัฒน์ เกิดการแลกเปลี่ยนข้อมูลได้ง่ายและรวดเร็ว สามารถตอบสนองความต้องการใช้เทคโนโลยีทุกรูปแบบ ทำให้เกิดสภาพการทำงานได้ทุกสถานที่และทุกเวลา ตัวอย่างบริษัท บิทคับ (Bitkub) มีการขับเคลื่อนเทคโนโลยีสารสนเทศเป็นตัวกลางในการดำเนินธุรกิจ

๑.๒ ความเสี่ยงของระบบสารสนเทศ (Information System Risk) คือ โอกาสที่จะเกิดข้อผิดพลาดความเสียหายที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในการขับเคลื่อนการดำเนินธุรกิจ โดยแบ่งความเสี่ยงได้ ดังนี้ ๑) ความเสี่ยงที่เกิดจากภายใน ได้แก่ การพัฒนาระบบ การใช้ระบบ ความเสี่ยงเกี่ยวกับอุปกรณ์ ความเสี่ยงจากบุคลากรภายใน เช่น การบันทึกข้อมูลผิดพลาด เป็นต้น ๒) ความเสี่ยงที่เกิดจากภายนอก เช่น การบุกรุกโจรกรรม และ ๓) ความเสี่ยงจากอุบัติภัยที่เกิดขึ้นโดยธรรมชาติหรือโดยฝีมือมนุษย์ เช่น โรคระบาด น้ำท่วม เป็นต้น

๑.๓ ความมั่นคงด้านสารสนเทศ (CIA in IT Security) ประกอบด้วย ๑) Confidentiality การรักษาความลับของข้อมูล ผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ๒) Integrity ความครบถ้วนถูกต้องของข้อมูล และ ๓) Availability ความพร้อมการใช้งาน

/๑.๔ ...

๑.๔ ความแตกต่างของ Information Security กับ Cybersecurity

Information Security เป็นการปกป้องโครงสร้างพื้นฐานด้าน IT และข้อมูลที่มีอยู่ภายในองค์กร เช่น Hardcopy and Electronic Data เป็นต้น

Cybersecurity การปกป้องจากกระบวนการจัดเก็บและส่งผ่านข้อมูลที่มีการเชื่อมต่อกับระบบภายนอกองค์กร เช่น ผ่านระบบอินเตอร์เน็ต เป็นต้น

๒. บทบาทและหน้าที่ของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ

๒.๑ การตรวจสอบระบบสารสนเทศ คือ การตรวจสอบการควบคุมการจัดการภายในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (Internal Controls) และแอปพลิเคชัน (Application Controls) ทางธุรกิจ โดยประเมินหลักฐานที่ได้รับว่าระบบข้อมูลมีการป้องกันทรัพย์สิน รักษาความสมบูรณ์ของข้อมูล และดำเนินการอย่างมีประสิทธิภาพเพื่อบรรลุเป้าหมายหรือวัตถุประสงค์ขององค์กร

๒.๒ ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit) แบ่งเป็น ๓ ประเภท คือ ๑) ผู้ตรวจสอบภายนอก (External IS Auditor) มีหน้าที่ดูและด้าน Financial statement เช่น การบัญชี การตลาด เป็นต้น ๒) ผู้ตรวจสอบภายใน (Internal IS Auditor) มีหน้าที่ดูแลระบบการควบคุมภายในทั้งหมด เช่น ระบบวันลาการเข้า-ออกงาน เป็นต้น และ ๓) ผู้ตรวจสอบกรณีพิเศษ (Special IS Auditor) มีความเชี่ยวชาญเฉพาะด้าน

๒.๓ IT Controls จำแนกตามวัตถุประสงค์ ประกอบด้วย ๑) General Control และ ๒) Application Control หรือ ๑) Preventive Control ๒) Detective Control และ ๓) Corrective Control หรือจำแนกตามหน้าที่ความผิดชอบ ประกอบด้วย ๑) ด้าน Governance ทำหน้าที่กำหนดนโยบายด้าน IT ๒) ด้าน Management ทำหน้าที่ กำหนดมาตรฐานการปฏิบัติงานด้าน IT โครงสร้างและการบริหารจัดการด้าน IT ควบคุมโครงสร้างพื้นฐานและสภาพแวดล้อมด้าน IT และ ๓) ด้าน Technical ทำหน้าที่ควบคุมระบบโปรแกรม การพัฒนาระบบโปรแกรมใหม่ รวมทั้งการควบคุมระบบงาน

ทั้งนี้ IT Domain มองเป็นภาพ ๓ มิติ คือ ๑) IT Management ควบคุมด้านคน ประกอบด้วย การวางแผน การแบ่งแยกหน้าที่ต่างๆ ๒) IT Controls ประกอบด้วย IT General Control การควบคุมทั่วไป เช่น พัฒนาระบบ เป็นต้น และ Application Control การควบคุมเฉพาะระบบงาน เช่น การตรวจสอบความถูกต้องของข้อมูล การแบ่งแยกหน้าที่ในแอปพลิเคชัน เป็นต้น และ ๓) Technical Layer เริ่มจากการวางโครงสร้างพื้นฐานด้าน IT และระบบ Network ขององค์กร ระบบการปฏิบัติงาน (Operation Systems) ระบบฐานข้อมูล (Database) และระบบงานต่างๆ (Application)

๒.๔ ตัวอย่าง IT for Business Process

สมาคมผู้ตรวจสอบภายในระดับโลก : โดยเริ่มจาก IT Infrastructure และ Applications มีการควบคุมโดย IT General Controls และ Application Controls ทั้งหมดนี้จะอยู่ภายใต้ Business Processes

๒.๕ ผู้ตรวจสอบภายในยุคปัจจุบันควรปรับบทบาทเป็นผู้ให้คำปรึกษาผ่านการให้คำแนะนำแก่หน่วยรับตรวจ เพื่อลดจุดอ่อนของการควบคุมภายในที่มีอยู่และปรับปรุงระบบการควบคุมให้มีประสิทธิภาพยิ่งขึ้น ซึ่งอาจเป็นการให้คำแนะนำในระหว่างการเข้าตรวจสอบได้

๓. IT General Controls (ITGC) และ Application Controls

๓.๑ IT General Controls (ITGC) การควบคุมทั่วไปเป็นการควบคุมที่กำหนดโครงสร้างโดยรวมที่มีต่อกิจกรรมประมวลผลทั้งหมด เป็นการควบคุมพื้นฐานที่ต้องมีเพื่อทำให้การควบคุมทุกระบบมีประสิทธิผล มีผลโดยตรงต่อความถูกต้องของข้อมูลในทุกระบบงาน

/- กรอบงาน ...

- กรอบงานตาม ITGC ประกอบด้วยการควบคุม ๔ เรื่อง ดังนี้ ๑) การพัฒนาระบบสารสนเทศ (Program development) ๒) การเปลี่ยนแปลงแก้ไขระบบสารสนเทศ (Program changes) ๓) การปฏิบัติการคอมพิวเตอร์ (Computer operation) และ ๔) การเข้าถึงโปรแกรมและข้อมูล (Access to programs and data)

- ISO ๒๗๐๐๑ ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ประกอบด้วย ๑) Requirement (Clause ๔-๑๐) ใช้หลักการ PDCA Model (Plan Do Check Action) ๒) Annex A Control (A.๕-A.๑๘) อธิบายวัตถุประสงค์การควบคุม ITGC ที่องค์กรสามารถนำไปใช้ในการควบคุม ITGC โดยมีองค์ประกอบ ดังนี้

A.๕ นโยบายความมั่นคงปลอดภัยขององค์กร เป็นแนวทางสำหรับผู้บริหารในด้านการสนับสนุนความปลอดภัยด้านสารสนเทศ เช่น เอกสารนโยบายความมั่นคงปลอดภัย และการตรวจสอบนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนด โดยให้มีการทบทวนนโยบายปีละ ๑ ครั้ง

A.๖ โครงสร้างของความมั่นคงปลอดภัยสำหรับสารสนเทศ เช่น การแบ่งแยกหน้าที่ความรับผิดชอบต่างๆ เอกสารนโยบายอุปกรณ์ประเภทพกพา และการปฏิบัติงานนอกสำนักงาน เป็นต้น

A.๗ ความมั่นคงปลอดภัยด้านทรัพยากรมนุษย์ เช่น การตรวจสอบข้อมูลก่อนจ้างงาน การกำหนดความรับผิดชอบระหว่างจ้างงาน และการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน เป็นต้น

A.๘ การบริหารจัดการทรัพย์สิน เช่น การจัดการบัญชีทรัพย์สิน การจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ เป็นต้น

A.๙ การควบคุมการเข้าถึง เช่น การควบคุมการเข้าถึงระบบสารสนเทศ การจัดการการเข้าถึงระบบของพนักงาน การควบคุมระบบและโปรแกรมประยุกต์ เป็นต้น

A.๑๐ การเข้ารหัสข้อมูล เช่น นโยบายการใช้งานการเข้ารหัสข้อมูล และการจัดการกุญแจที่ใช้ในการเข้ารหัส เป็นต้น

A.๑๑ ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร เช่น บริเวณที่ต้องมีการรักษาความปลอดภัย และการป้องกันอุปกรณ์ต่างๆ ขององค์กร เป็นต้น

A.๑๒ ความปลอดภัยในการปฏิบัติงาน เช่น การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน การป้องกันมัลแวร์ การติดตั้งโปรแกรมบนระบบปฏิบัติการ การบันทึก Log และการเฝ้าดู เป็นต้น

A.๑๓ ความปลอดภัยในด้านการสื่อสาร เช่น การป้องกันเครือข่าย การจัดแบ่งเครือข่ายภายในองค์กรกับภายนอกองค์กร การส่งข้อมูล เป็นต้น

A.๑๔ ความต้องการ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ เช่น การกำหนดความต้องการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขระบบ การป้องกันข้อมูลจริงที่ใช้ในการทดสอบระบบ เป็นต้น

A.๑๕ ความสัมพันธ์กับซัพพลายเออร์ เช่น ความปลอดภัยของข้อมูลสารสนเทศกับซัพพลายเออร์ และการบริหารซัพพลายเออร์ เป็นต้น

A.๑๖ การจัดการเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางสารสนเทศ เช่น ความรับผิดชอบและกระบวนการ การรายงานเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัย การตอบสนองต่อเหตุการณ์ การรวบรวมเหตุการณ์ เป็นต้น

A.๑๗ การบริหารความต่อเนื่องขององค์ในด้านความปลอดภัยของข้อมูลสารสนเทศ เช่น มีการวางแผน จัดทำแผน ตรวจสอบและการทบทวนแผนเพื่อสร้างความต่อเนื่องในการดำเนินงาน การเตรียมการอุปกรณ์ประมวลผลสำรอง เป็นต้น

A.๑๘ การปฏิบัติตามข้อกำหนดทางกฎหมาย และนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

/๓.๒ ...

๓.๒ Application Controls การควบคุมเฉพาะด้านระบบงาน ได้แก่ การควบคุมแบบ Manual หรือการควบคุมแบบ Automatic โดยโปรแกรม ซึ่งเป็นการควบคุมในระดับกระบวนการ โดยแบ่งได้ ๒ รูปแบบ คือ

๓.๒.๑ แบ่งตามวัตถุประสงค์

(๑) ความครบถ้วน (Completeness) เช่น รายการทุกรายการบันทึกเข้าระบบ และประมวลผลเพียงครั้งเดียว มีเทคนิคการควบคุม ได้แก่ ๑) Batch Totals ควบคุมความครบถ้วนของรายการโดยเปรียบเทียบยอดรวมระหว่างต้นทางและปลายทาง ๒) Sequence Checking ควบคุมความครบถ้วนของรายการโดยการตรวจสอบการเรียงลำดับตามหมายเลข ตามตัวอักษร หรือวันที่ ๓) Matching ควบคุมความครบถ้วนของรายการโดยการจับคู่รายการก่อนประมวลผล เช่น การบันทึกบัญชีทั้งสองด้าน (DR/CR) ๔) One for One Checking ตรวจสอบรายการที่ประมวลผลกับเอกสารต้นฉบับ

(๒) ความถูกต้อง (Accuracy) การควบคุมให้มีการบันทึกข้อมูลให้ครบทุกฟิลด์และถูกต้อง ระบบงานจึงจะรับรายการเข้าไปประมวลผล มีเทคนิคการควบคุม ได้แก่ ๑) Batch Totals Matching ๒) One for One Checking ๓) Programmed Check ควบคุมการบันทึกไม่สมเหตุสมผล ความไม่สอดคล้องกัน และตรวจสอบข้อมูลที่บันทึกว่าเกินระดับที่อนุมัติหรือไม่

(๓) การอนุมัติ (Validity) รายการที่บันทึกเข้าระบบเพื่อประมวลผลได้รับการอนุมัติจากผู้มีอำนาจอย่างเหมาะสม มีเทคนิคการควบคุม ได้แก่ ๑) One for One Checking การอนุมัติรายการบนเอกสาร ๒) Matching การอนุมัติรายการผ่านระบบ โดยระบบจะไปตรวจสอบว่าเจ้าหน้าที่อนุมัติมีอำนาจหรือไม่ ถ้ามีสามารถอนุมัติรายการนั้นได้หรือไม่

(๔) การจำกัดการเข้าถึงข้อมูล (Restricted Access) ระบบงานและข้อมูลมีการควบคุมเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขโดยที่ไม่ได้รับอนุญาต มีเทคนิคการควบคุม ได้แก่ การกำหนดสิทธิในระบบตามหน้าที่และความรับผิดชอบ การกำหนด Password rules

๓.๒.๒ แบ่งตามขั้นตอนการทำงานของระบบ

(๑) ควบคุมการนำเข้า (Input Controls) เป็นการควบคุมที่สำคัญ มีการนำข้อมูลเข้าสู่ระบบงาน ได้ ๒ วิธี ได้แก่ วิธี Manual entry และ Data transfer ทุกรายการที่นำเข้าได้รับการอนุมัติก่อนการประมวล ไม่มีรายการที่สูญหายและการนำเข้าซ้ำ

(๒) การควบคุมการประมวลผล (Progressing Controls) ควบคุมการประมวลผลให้เป็นไปตามระบบงาน ข้อมูลจะถูกสร้างขึ้นโดยอัตโนมัติ การประมวลผลจะเป็นไปตามข้อมูลที่นำเข้า ไม่มีการประมวลซ้ำหรือมีการเปลี่ยนแปลงอย่างไม่มีเหตุสมควร

(๓) การควบคุมผลลัพธ์จากการประมวลผล (Output Controls) เป็นการควบคุมระยะสุดท้ายเพื่อให้ได้ข้อมูลผลลัพธ์ และรายงานที่ถูกต้องจากระบบ มีการจำกัดการเข้าถึงหรือใช้ข้อมูลที่ส่งออกจากระบบคอมพิวเตอร์เฉพาะผู้ที่ได้รับอนุญาต

(๔) การควบคุมโดยสร้างร่องรอยการตรวจสอบ (Audit Trails) แฟ้มทะเบียนร่องรอยที่สร้างขึ้นเพื่อบันทึกกิจกรรมในระบบงาน เช่น การบันทึกเหตุการณ์ของการทำงานของผู้ใช้งานแต่ละคน

๔. การบริหารความเสี่ยง (IT Risk Management)

๔.๑ แนวทางการตรวจสอบการบริหารงานเทคโนโลยีสารสนเทศตามหลักธรรมาภิบาล (IT Governance)

๑) <u>บทบาทและหน้าที่ความรับผิดชอบของคณะกรรมการ</u> ควรมีคณะกรรมการที่มีความรู้หรือประสบการณ์ทางด้าน IT อย่างน้อย ๑ ท่าน ดูแลให้มีการกำหนดนโนบายรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (IT security policy) และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยี (IT risk management)

๒) <u>โครงสร้างการกำกับดูแล</u> มีโครงสร้างแบบ ๓ line of defense ประกอบด้วย IT Operation (๑^{st} Line) IT Risk & Compliance (๒^{nd} Line) และ IT Audit (๓^{rd} Line) แบ่งหน้าที่กันอย่างชัดเจน

/๓) ...

๓) นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประกอบด้วย IT security policy ครอบคลุมหัวข้อที่สำคัญและความมั่นคงปลอดภัยไซเบอร์ และ IT risk management กระบวนการบริหารและจัดการความเสี่ยงอย่างเหมาะสม

- กระบวนการ IT risk management

(๑) Assessment มีการระบุความเสี่ยงด้าน IT ที่คาดว่าเกิดขึ้น (Key Risk Indicator : KRI)

(๒) Treatment มีการจัดการความเสี่ยง และกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

(๓) Monitoring มีการติดตามจากรายงาน Risk Treatment Plan และมีการระบุความเสี่ยงล่วงหน้า

(๔) Reporting มีการสรุปภาพรวมของความเสี่ยงแต่ละ Level เสนอรายงานแก่ผู้บริหารเพื่อนำไปกำหนด KRI ในรอบใหม่

๔) การบริหารจัดการบุคลากร ข้อกำหนดหรือเงื่อนไขด้านความปลอดภัยเทคโนโลยีสารสนเทศที่มีคุณสมบัติเหมาะสมมีความรู้หรือประสบการณ์เพียงพอ

๕) การตระหนักถึงความเสี่ยงด้าน IT (IT Risk Awareness) การกำหนด Training program ที่เหมาะสมตามโครงสร้างแบบ ๓ line of defense และ Awareness program เช่น Social engineering และ Phishing ให้ครอบคลุมทุกระดับพนักงาน

๔.๒ แนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) ตามกรอบหลักการ CIA

๑) IT asset management กำหนดมาตราฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ปรับปรุงอย่างน้อยปีละ ๑ ครั้ง และจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

๒) Information security

- การรักษาความมั่นคงปลอดภัยของข้อมูล เช่น กำหนดให้มีเจ้าของข้อมูล การจัดชั้นความลับของข้อมูล เป็นต้น

- การบริหารจัดการการเข้ารหัสข้อมูล (Cryptography) มาตราฐานและระเบียบวิธีการปฏิบัติการบริหารจัดการการเข้าข้อมูล

๓) Access control มีการบริหารจัดการบัญชีสิทธิสูงและบัญชีผู้ใช้ภายในองค์กรตามความจำเป็นของการใช้งาน โดยสามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๔) Physical and environmental security

- การควบคุมการเข้าถึงศูนย์คอมพิวเตอร์และพื้นที่ต่างๆ ภายในศูนย์คอมพิวเตอร์ เช่น กำหนดการเข้าถึงพื้นที่สำคัญต่างๆ ภายในศูนย์คอมพิวเตอร์ด้วยระบบ Multi factor authentication เป็นต้น

- การบริหารจัดการศูนย์คอมพิวเตอร์ เช่น จัดให้ศูนย์คอมพิวเตอร์สำรองแยกจากศูนย์คอมพิวเตอร์หลักควรมีระยะห่างที่เพียงพอและไม่ใช้ระบบสาธารณูปโภคจากแหล่งเดียวกัน เป็นต้น

- ระบบไฟฟ้าสำหรับศูนย์คอมพิวเตอร์ เช่น การติดตั้งอุปกรณ์ UPS และGenerator เพื่อรองรับการทำงานของอุปกรณ์สำคัญในศูนย์คอมพิวเตอร์ ๒ ชุด เป็นต้น

๕) Communication security มีโครงสร้างของระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย มีการออกแบบระบบเครือข่ายที่เหมาะสมตามมาตราฐานสากล

๖) IT operation security

๖.๑ Change management เช่น การกำหนดบทบาทหน้าที่ความรับผิดชอบของผู้บริหารที่ได้รับมอบหมายหรือคณะกรรมการบริหารการจัดการ (Change Advisory Board: CAB) เพื่อป้องกันการแก้ไขโดยไม่ได้รับอนุญาต เป็นต้น

๖.๒ System Configuration management เช่น การจัดทำเอกสาร minimum baseline standard เป็นลายลักษณ์อักษร โดยมีการทบทวน ปรับปรุงเอกสารอย่างสม่ำเสมอ เป็นต้น

๖.๓ Patch management เช่น มีกระบวนการทดสอบ Patch ที่ออกใหม่ทุกครั้ง ไม่ควรซ้ำกับ Patch เดิม

๖.๔ Logging เช่น การจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายที่สำคัญด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนที่จะใช้เป็นหลักฐานการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้

๖.๕ Capacity Management เช่น มีการประเมินแนวโน้มการใช้ทรัพยากร IT เพื่อวางแผนรองรับการใช้งานในอนาคต เป็นต้น

๖.๖ Security Monitoring เช่น กำหนดกระบวนการหรือเครื่องมือในการตรวจสอบจับเหตุการณ์ผิดปกติ มีการวิเคราะห์และจัดการข้อมูลภัยคุกคามที่อาจเกิดต่อเนื่อง เป็นต้น

๖.๗ Vulnerability management and Penetration test เช่น มีกระบวนการและเครื่องมือการประเมินช่องโหว่ (VA) ควรจัดทำอย่างน้อยปีละ ๑ ครั้ง สามารถปิดช่องโหว่ด้วยการ Patch จนเหลือค่า VA ที่ต่ำ และการทดสอบเจาะระบบ (Penetration test) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระเท่านั้น

๖.๘ Data Backup เช่น มีกระบวนการสำรองทั้งระบบทุกครั้งภายหลังจากมีการเปลี่ยนแปลงระบบงาน เป็นต้น

๖.๙ Endpoint Security เช่น มีการกำหนดมาตราฐานระเบียบวิธีการรักษาความปลอดภัยในอุปกรณ์ปฏิบัติงานรวมถึงอุปกรณ์ส่วนตัว (BYOD)

๗) System acquisition and development

๗.๑ System acquisition เช่น การจัดหาซอฟแวร์ระบบมาใช้งานที่มีความปลอดภัย ทำสัญญาและข้อตกลงการรับฝากทรัพย์สิน (Escrow agreement)

๗.๒ System development มีขั้นตอน ๔ ขั้นตอน คือ ๑) การออกแบบระบบเป็นไปตามคุณสมบัติทางเทคนิคและ IT Security policy ๒) การพัฒนาระบบแบ่งแยกระบบงาน Development Testing และ Production ออกจากกัน ๓) การทดสอบระบบ ผ่าน nit test, sit test, UAT, performance test, security test และ ๔) การนำระบบขึ้นมาใช้ ผ่านกระบวนการ Change management รวมถึงระบบสำรองต้องมีความสอดคล้องกัน

๘) IT incident and problem management

๘.๑ IT incident management มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT

๘.๒ IT problem management มีกระบวนการติดตามหาสาเหตุที่แท้จริง ให้มีแนวทางป้องกันไม่ให้เกิดซ้ำ

๙) IT contingency plan ควรมีการประเมินความเสี่ยง โดยระบุเหตุการณ์ความเสี่ยง (Risk scenarios) ให้ครบทุกด้าน และจัดทำแผนฉุกเฉิน (BCP) มีการทบทวนอย่างน้อยปีละ ๑ ครั้ง รวมถึงการจัดทำรายงานนำเสนอ

๑๐) Third party risk management มีการประเมินความเสี่ยงและผลกระทบก่อนการใช้บริการจากบุคคลภายนอก

- การจัดให้มีการควบคุมและบริหารจัดการความเสี่ยงครอบคลุมวัฏจักรการบริหารจัดการบุคคลภายนอก (Third party management life cycle) มีรูปแบบการประเมินจาก ๑) การประเมินความเสี่ยง เช่น กลยุทธ์ ชื่อเสียง เป็นต้น ๒) การคัดเลือกบุคคลภายนอก เช่น ความเชี่ยวชาญ ใบอนุญาต เป็นต้น ๓) การจัดทำสัญญาหรือข้อตกลง เช่น ขอบเขตการให้บริการ แผนฉุกเฉิน PDPA เป็นต้น ๔) การติดตามผลปฏิบัติงานอย่างต่อเนื่อง เช่น เกณฑ์ที่ใช้ในการประเมิน เป็นต้น และ ๕) การยกเลิก/สิ้นสุดสัญญา หรือข้อตกลง เช่น กระบวนการยกเลิก การเรียกคืนทรัพย์สิน เป็นต้น

๕. IT Audit Plan และ Workshop

๕.๑ Audit Plan คือ แผนการตรวจสอบประจำปี ภาพรวมของแผนการตรวจสอบ

- ขั้นตอน IT Audit Plan ประกอบด้วย ๔ ขั้นตอน ดังนี้

(๑) Update Audit Universe เป็นการวางแผนสิ่งที่จะตรวจสอบทั้งหมด สามารถกำหนดได้หลายมิติ เช่น ตามหน่วยงาน/ภารกิจงาน กฎหมาย/ข้อบังคับ กระบวนการปฏิบัติงาน IT General Controls/ Application Controls เป็นต้น

(๒) Risk Assessment กำหนดเกณฑ์ในการประเมิน ปรึกษาฝ่ายบริหาร ศึกษางานตรวจสอบเดิม การเปลี่ยนแปลงภายใน/ภายนอก

(๓) Formalize Audit Plan ตรวจในกิจกรรมที่มีความเสี่ยงสูง

(๔) Approve Audit Plan นำเสนอกรรมการตรวจสอบเพื่ออนุมัติสอบแทนแผนดำเนินงานและการปรับปรุงแผน

๕.๒ Engagement Plan คือ แผนปฏิบัติงาน เป็นแผนย่อยของ Audit Plan

- ขั้นตอน Engagement Plan ประกอบด้วย ๘ ขั้นตอน ดังนี้

(๑) การสำรวจข้อมูลเบื้องต้น

(๒) การประเมินการควบคุมภายใน

(๓) การประเมินความเสี่ยง

(๔) การวางแผนการตรวจสอบ

(๕) การปฏิบัติงานตรวจสอบ

(๖) สรุปผลการตรวจสอบ

(๗) รายงานผลการตรวจสอบ

(๘) การติดตามผลการแก้ไข

๕.๓ ข้อแนะนำของวิทยากร

(๑) การจัดทำ IT Audit Plan สามารถเพิ่มหัวข้อการตรวจสอบ IT ใน Audit Universe เพื่อให้มีความครอบคลุม และควรตรวจสอบ IT General Controls ในลำดับแรก เนื่องจากเป็นเรื่องสำคัญและครอบคลุมการปฏิบัติงานด้าน IT ในภาพรวมขององค์กร

(๒) การจัดทำ Engagement Plan เป็นเรื่องสำคัญ เนื่องจากเป็นการกำหนดแนวทาง/วิธีการในการปฏิบัติงานตรวจสอบของผู้ตรวจสอบ

(๓) การให้คำปรึกษาแก่หน่วยรับตรวจสามารถดำเนินการได้ ๓ วิธี คือ ๑) การให้คำปรึกษาในระหว่างการปฏิบัติงานตรวจสอบ โดยผู้ตรวจสอบควรแจ้งหน่วยรับตรวจให้ทราบก่อนการปฏิบัติงานตรวจสอบ ๒) หัวหน้าผู้ตรวจสอบจัด Session ให้ความรู้แก่หน่วยรับตรวจที่เกี่ยวข้อง โดยพิจารณาจากจุดอ่อน/ข้อตรวจพบจากการตรวจสอบที่ผ่านมา และ ๓) การให้คำปรึกษาแบบเต็มรูปแบบ ซึ่งต้องมีการตกลงขอบเขตการให้คำปรึกษาร่วมกับหน่วยงานผู้ขอรับคำปรึกษาและจัดทำรายงานผลการให้คำปรึกษา