อบรมโครงการ KM Networking ประจำปีงบประมาณ พ.ศ. ๒๕๖๔
หัวข้อ “IT Audit”
ในวันอังคารที่ ๒๔ และวันพุธที่ ๒๕ สิงหาคม ๒๕๖๔ เวลา ๙.๐๐-๑๒.๐๐ น.
ผ่านสื่ออิเล็กทรอนิกส์ (โปรแกรม Webex) โดยกลุ่มตรวจสอบภายใน สำนักงานบริหารหนี้สาธารณะ

หลักการและเหตุผล

ตามที่ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ ได้เห็นชอบแนวทางการเพิ่มประสิทธิภาพการ ปฏิบัติงานตรวจสอบภายใน ของกลุ่มตรวจสอบภายใน (กตส.) สำนักงานบริหารหนี้สาธารณะ (สบน.) เพื่อให้เจ้าหน้าที่ กตส. สบน. ใช้เป็นแนวทางในการปฏิบัติงาน และภายใต้แนวทางดังกล่าวได้กำหนดให้มีการจัดการความรู้ด้านการตรวจสอบภายในโดยมีวัตถุประสงค์เพื่อพัฒนาขีดความสามารถของบุคลากร กตส. ส่งเสริมการแลกเปลี่ยนเรียนรู้ระหว่างเจ้าหน้าที่ให้สามารถปฏิบัติงานด้านตรวจสอบภายในทดแทนกัน รวมทั้งพัฒนาเครือข่ายการทำงานระหว่างบุคลากรของ กตส. และบุคลากรจากหน่วยรับตรวจ เพื่อนำไปสู่การปรับปรุง/พัฒนาการปฏิบัติงานให้มีประสิทธิภาพยิ่งขึ้น รวมทั้งบรรลุวัตถุประสงค์และเป้าหมายตามยุทธศาสตร์ของ สบน. โดยข้อเสนอแนะจากการตรวจสอบภายในหรือการให้คำแนะนำ/คำปรึกษาจาก กตส. จะช่วยสร้างมูลค่าเพิ่มให้แก่องค์กรและสนับสนุนผู้บริหารในการบริหารความเสี่ยง การควบคุม และการกำกับดูแล รวมทั้ง สนับสนุน สบน. ให้เป็นองค์กรธรรมาภิบาล มีความโปร่งใสและตรวจสอบได้ ซึ่งสอดคล้องกับยุทธศาสตร์ที่ ๔ ของ สบน. ในการพัฒนาบุคลากร ระบบบริหารจัดการ ระบบข้อมูลและเทคโนโลยี เพื่อส่งเสริมองค์กรสู่ความเป็นเลิศ และยุทธศาสตร์ของกระทรวงการคลังเป้าหมายที่ ๓ การรักษาความยั่งยืนทางการคลัง ในเรื่องส่งเสริมความโปร่งใสในการดำเนินงาน

วัตถุประสงค์

๑) เพื่อพัฒนาศักยภาพของบุคลากร กตส. ให้มีการพัฒนาตนเองอย่างต่อเนื่อง ส่งผลให้การปฏิบัติงานตรวจสอบภายในเกิดประสิทธิภาพ และผลงานตรวจสอบภายในสร้างคุณค่าเพิ่มให้แก่องค์กร

๒) เพื่อให้บุคลากร สบน. มีความรู้ ความเข้าใจ ในเรื่องที่เกี่ยวข้องกับการปฏิบัติงาน สามารถนำความรู้และประสบการณ์ที่ได้รับไปปรับใช้ในการปฏิบัติงานเพื่อให้เกิดประโยชน์สูงสุดต่อองค์กร รวมทั้งส่งเสริม ให้เกิดการมีส่วนร่วมในการแสดงความคิดเห็น การแลกเปลี่ยนความรู้ ประสบการณ์ ร่วมกับวิทยากร/ ผู้เชี่ยวชาญจากภายนอก

๓) เพื่อพัฒนาเครือข่ายด้านตรวจสอบภายใน โดยสร้างความสัมพันธ์ที่ดีระหว่างหน่วยงาน ตรวจสอบภายในและหน่วยรับตรวจ ผ่านการให้ความรู้ คำแนะนำ ที่สนับสนุนให้เกิดการปรับปรุง/พัฒนาการ ปฏิบัติงาน เพื่อให้หน่วยรับตรวจเกิดทัศนคติที่ดีต่องานตรวจสอบภายในและให้ความร่วมมือกับผู้ตรวจสอบ รวมทั้งพัฒนาเครือข่ายผู้ตรวจสอบภายในกับหน่วยงานภายนอกให้สามารถแลกเปลี่ยนความรู้ ประสบการณ์ ด้านตรวจสอบภายในร่วมกัน

ขอบเขตการดำเนินงาน

การจัดอบรม/อบรมเชิงปฏิบัติการ จำนวน ๒ หัวข้อ โดยเชิญวิทยากรจากภาคเอกชน ซึ่งเป็นผู้เชี่ยวชาญและมีประสบการณ์ในด้านที่เกี่ยวข้องมาถ่ายทอดความรู้และประสบการณ์ รวมถึงเปิดโอกาส ให้ผู้เข้ารับการอบรมได้แสดงความคิดเห็นร่วมกัน โดยมีรายละเอียดในแต่ละหัวข้อ ดังนี้

๑) หัวข้อ "PDMO : Transforming into Data-Driven Organization"

วัตถุประสงค์ เพื่อให้บุคลากร สบน. มีความรู้และเข้าใจเกี่ยวกับกรอบแนวคิดและกระบวนการพัฒนาองค์กรเพื่อก้าวไปสู่องค์กรที่ขับเคลื่อนด้วยข้อมูล (Data-Driven Organization) และ สนับสนุนให้บุคลากร สบน. ตระหนักถึงความสำคัญและเกิดแนวความคิดในการบริหารจัดการข้อมูลและบูรณาการข้อมูลระหว่างหน่วยงานภายในร่วมกัน เพื่อให้สามารถนำข้อมูล/สารสนเทศมาใช้ในกระบวนการ ตัดสินใจที่เกี่ยวข้องขององค์กร เพื่อให้เกิดประสิทธิภาพในการปฏิบัติงานยิ่งขึ้น รวมทั้งตอบสนองต่อการบรรลุ เป้าหมายตามยุทธศาสตร์ขององค์กร

รูปแบบการอบรม : จัดอบรมสัมมนา ๓ ชั่วโมง และอบรมแบบออนไลน์สำหรับบุคลากรที่ปฏิบัติงานที่บ้าน (Work from Home)

เนื้อหาการอบรม มีรายละเอียด ดังนี้

(๑) ความสำคัญของ Information Sharing

(๒) กรอบแนวคิดและกระบวนการพัฒนาองค์กรเพื่อก้าวไปสู่ Data-Driven Organization

(๓) ความท้าทายในการปรับเปลี่ยนองค์กรภาครัฐเพื่อไปสู่ Data-Driven Organization

(๔) กรณีศึกษาหน่วยงานที่ประสบความสำเร็จ (Best Practices)

วิทยากร : นายราเชน พานิชย์ดี Data Solutions Consultant บริษัท มิลเลนเนียม บิสซิเนส โซลูชั่น จำกัด

กลุ่มเป้าหมาย : ผู้บริหารและบุคลากร สบน. จำนวน ๕๐ คน

๒) หัวข้อ "IT Audit"

วัตถุประสงค์ เพื่อเสริมสร้างศักยภาพของทีมผู้ตรวจสอบภายใน สบน. และเครือข่ายผู้ตรวจสอบ ภายในสังกัดกระทรวงการคลัง ให้มีความรู้ความเข้าใจในขั้นตอนและกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ แนวทางการวางแผนการตรวจสอบด้านเทคโนโลยีสารสนเทศตามหลักการบริหารความเสี่ยง แนวปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศ รวมทั้งเทคนิคการตรวจสอบด้านเทคโนโลยีสารสนเทศและมาตรฐานที่เกี่ยวข้อง รวมทั้งฝึกปฏิบัติ (Workshop) โดยใช้กรณีศึกษาของ สบน. เพื่อให้ผู้ตรวจสอบภายใน สบน. สามารถนำความรู้ที่ได้ไปประยุกต์ใช้ในการปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ และสอดคล้องกับบริบทขององค์กร

รูปแบบการจัดอบรม : จัดอบรมสัมมนา ๑ วัน (๖ ชั่วโมง) และฝึกปฏิบัติ (Workshop) ๑ วัน (๖ ชั่วโมง)

เนื้อหาการอบรม มีรายละเอียด ดังนี้

(๑) บทบาทหน้าที่ของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ

(๒) ขั้นตอนและกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศในหน่วยงานภาครัฐ

- การวางแผนการตรวจสอบตามความเสี่ยง
- การปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศ
- การสรุปผลการตรวจสอบและการเขียนรายงาน

(๓) แนวทางการตรวจสอบการบริหารงานเทคโนโลยีสารสนเทศตามหลักธรรมาภิบาล

(๔) แนวทางการตรวจสอบการปฏิบัติงานเทคโนโลยีสารสนเทศ กรณีศึกษาและประสบการณ์ตรวจสอบ

(๕) แนวทางการตรวจสอบโครงการเทคโนโลยีสารสนเทศ กรณีศึกษาและประสบการณ์ตรวจสอบ

(๖) Workshop (เฉพาะผู้ตรวจสอบภายใน สบน.)

- การตรวจสอบนโยบายและแนวปฏิบัติด้านสารสนเทศ
- การตรวจสอบโครงการด้านเทคโนโลยีสารสนเทศ

วิทยากร : นายวราฤทธิ์ แสงแดง CIA, CISA บริษัท ศูนย์ประมวลผล จำกัด

กลุ่มเป้าหมาย :

- วันที่ ๑ (อบรมสัมมนา) ได้แก่ ผู้ตรวจสอบภายใน สบน. และเครือข่ายผู้ตรวจสอบภายใน สังกัดกระทรวงการคลัง (กรมบัญชีกลาง สำนักงานปลัดกระทรวงการคลัง สำนักงานเศรษฐกิจการคลัง และ สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ) จำนวน ๒๐ คน
- วันที่ ๒ (ฝึกปฏิบัติ) ได้แก่ ผู้ตรวจสอบภายใน สบน. จำนวน ๖ คน

ผลที่คาดว่าจะได้รับ

๑) เพิ่มศักยภาพในการปฏิบัติงานของผู้ตรวจสอบภายใน โดยผู้ตรวจสอบภายในมีการเรียนรู้ และพัฒนาตนเองอย่างต่อเนื่อง

๒) เพิ่มประสิทธิภาพการปฏิบัติงานของบุคลากรของหน่วยรับตรวจและผู้เกี่ยวข้อง ช่วยให้ บุคลากรของหน่วยรับตรวจและหน่วยงานที่เกี่ยวข้องสามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงาน ให้เกิดประสิทธิภาพบรรลุวัตถุประสงค์และเป้าหมาย และองค์กรได้รับประโยชน์สูงสุด

๓) เครือข่ายตรวจสอบภายในมีความเข้มแข็ง มีการประสานงานอย่างใกล้ชิดและแลกเปลี่ยน องค์ความรู้ที่เป็นประโยชน์ร่วมกัน

IT AUDIT

ความสำคัญของเทคโนโลยีสารสนเทศ

- ทำให้สังคมเปลี่ยนจากสังคมอุตสาหกรรมมาเป็นสังคมสารสนเทศ
- ทำให้ระบบเศรษฐกิจเปลี่ยนจากระบบแห่งชาติไปเป็นเศรษฐกิจโลกที่ผูกพันกับทุกประเทศ และเชื่อมโยงกันด้วยเครือข่ายสารสนเทศ
- ทำให้องค์กรมีการบังคับบัญชาแบบแนวราบมากขึ้น หน่วยธุรกิจมีขนาดเล็กลง และเชื่อมโยงกันกับหน่วยธุรกิจอื่นเป็นเครือข่าย การดำเนินธุรกิจมีการแข่งขันกันในด้านความเร็ว โดยอาศัยการใช้ระบบเครือข่ายคอมพิวเตอร์ และการสื่อสารโทรคมนาคมเป็นตัวสนับสนุน เพื่อให้เกิดการแลกเปลี่ยนข้อมูลได้ง่ายและรวดเร็ว
- ทำให้เกิดสภาพทางการทำงานแบบทุกสถานที่และทุกเวลา
- เทคโนโลยีสารสนเทศตอบสนองตามความต้องการการใช้เทคโนโลยีในรูปแบบใหม่ที่เลือกได้เอง

องค์ประกอบของระบบเทคโนโลยีสารสนเทศ

๑. **ฮาร์ดแวร์** ถือเป็นองค์ประกอบที่สำคัญ หมายถึง ตัวเครื่องคอมพิวเตอร์และอุปกรณ์ รอบข้างที่สามารถสัมผัสได้ โดยประกอบด้วยอุปกรณ์ทางอิเล็กทรอนิกส์ที่ควบคุมการประมวลผล การรับ และการแสดงผลของข้อมูล เช่น คอมพิวเตอร์ เม้าท์ คีย์บอร์ด CPU เป็นต้น

๒. **ซอฟต์แวร์** เป็นโปรแกรมชุดคำสั่งที่เขียนให้ฮาร์ดแวร์ปฏิบัติตามหรือลำดับขั้นตอน การทำงาน โดยคำสั่งของคอมพิวเตอร์

๓. **ข้อมูล Data** ถือเป็นส่วนที่จะนำจัดเก็บในคอมพิวเตอร์ เช่น ข้อมูลต่าง ๆ ที่นำเข้าสู่คอมพิวเตอร์เพื่อการประมวลผล

๔. **ขั้นตอนการปฏิบัติงาน** หรือคู่มือการปฏิบัติงาน คู่มือการคอมพิวเตอร์เพื่อให้เข้าใจกระบวนการทำงานอย่างเป็นระบบถูกต้อง

๕. **บุคลากร** เป็นบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ เช่น ผู้ใช้ ผู้บริหาร ผู้พัฒนาระบบ นักวิเคราะห์และนักเขียนโปรแกรม

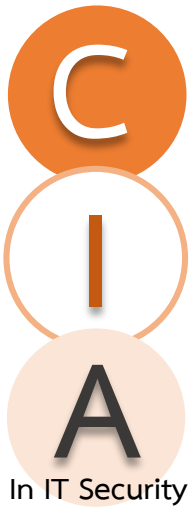
ความเสี่ยงของระบบสารสนเทศ

หมายถึง โอกาสที่จะเกิดข้อผิดพลาด ความเสียหาย การกระทำใด ๆ ที่ก่อให้เกิดการสูญเสียหรือทำลายฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลสารสนเทศหรือความสามารถในการประมวลผลข้อมูลของระบบสารสนเทศ ซึ่งแบ่งได้ ๓ ประเภท

๑. ความเสี่ยงที่เกิดจากภายใน การพัฒนาระบบ การใช้ระบบ ความเสี่ยงเกี่ยวกับอุปกรณ์ ความเสี่ยงจากบุคลากรภายใน

๒. ความเสี่ยงที่เกิดจากภายนอก ความเสี่ยงด้านข้อมูล ระบบสารสนเทศอาจประสบปัญหาได้หลายเรื่อง เช่น ไม่ได้ปิดระบบก่อนลุกออกจากโต๊ะทำงาน แฮคเกอร์บุกรุกเข้ามาทางระบบอินเตอร์เน็ตเพื่อทำลาย ซอฟต์แวร์ เว็บ หรือ ข้อมูล เป็นต้น

๓. ความเสี่ยงจากอุบัติภัย เกิดขึ้น โดยธรรมชาติหรือโดยฝีมือมนุษย์ เช่น เพลิงไหม้ น้ำท่วม โรคระบาด อุบัติเหตุ ระหว่างการขนย้าย



Confidentiality (ความลับ)

ผู้มีสิทธิและได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงข้อมูลได้ ถ้าสารสนเทศที่ถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิหรือไม่ไม่ได้รับอนุญาต จะถือว่าเป็นสารสนเทศที่เป็นความลับถูกเปิดเผย

Integrity (ความสมบูรณ์)

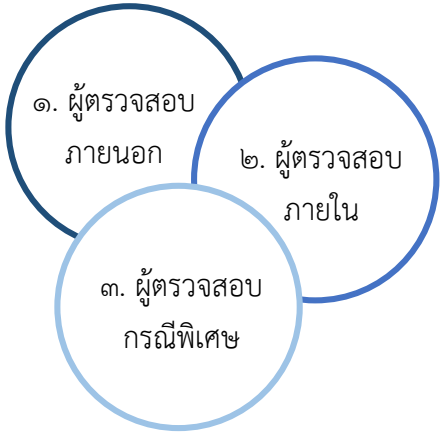
ความครบถ้วนถูกต้อง และไม่มีสิ่งปลอมปน ดังนั้น สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องและครบถ้วน

Availability (ความพร้อมใช้งาน)

สารสนเทศที่ถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ที่ไม่รับอนุญาตการเข้าถึงก็จะล้มเหลวถูกขัดขวาง

การตรวจสอบระบบสารสนเทศ

หมายถึง การตรวจสอบการควบคุมการจัดการภายในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และแอปพลิเคชั่นทางธุรกิจ การประเมินหลักฐานที่ได้รับ จะเป็นตัวกำหนดว่าระบบข้อมูลมีการปกป้องทรัพย์สิน รักษาความสมบูรณ์ของข้อมูล และดำเนินการอย่างมีประสิทธิภาพ เพื่อให้บรรลุเป้าหมายหรือวัตถุประสงค์ขององค์กร ความคิดเห็นเหล่านี้อาจจะดำเนินการร่วมกับการตรวจสอบงบทางการเงิน ตรวจสอบภายใน หรือ รูปแบบอื่น ๆ ที่ได้รับการรับรอง แบ่งได้ ๓ ประเภท

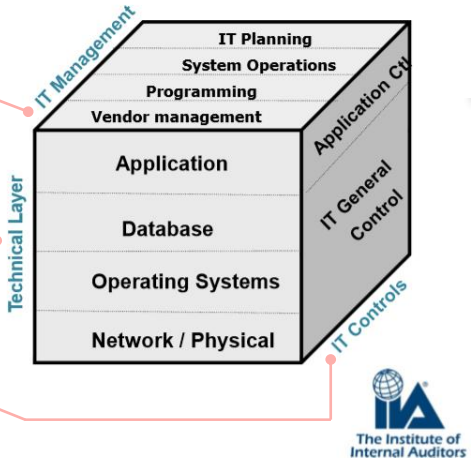


ภาพรวมของเทคโนโลยีสารสนเทศ

บุคคล นโยบาย และขั้นตอน ที่เกี่ยวข้องในการจัดการเทคโนโลยีสารสนเทศ

แอปพลิเคชั่นธุรกิจและโครงสร้างพื้นฐานด้าน IT ที่รองรับสนับสนุนให้สามารถใช้งานแอปพลิเคชั่น

การควบคุมภายในทั่วไป (General Controls) และการควบคุมภายในเฉพาะงาน (Application Control)



IT General Control การควบคุมทั่วไป

หรือ ITGC เป็นการควบคุมที่กำหนดโครงสร้างโดยรวมของการควบคุมที่มีต่อกิจกรรมประมวลผลทั้งหมด เป็นการควบคุมพื้นฐานที่ต้องมีเพื่อทำให้การควบคุมทุกระบบงานมีประสิทธิผล มีผลโดยตรงต่อ ความถูกต้องของข้อมูลในทุกระบบงาน

ISMS

ISMS หรือ ISO๒๗๐๐๑ คือมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล

- ISMSเป็นหนึ่งในตัวเลือกของกรอบการควบคุมสำหรับ ITGC
- เป็นระบบการจัดการความปลอดภัยของข้อมูลให้มีประสิทธิผลทั้ง ๓ ด้าน (Confidentiality, Integrity, Availability)
- ใช้หลักการวงจรคุณภาพ PDCA Model (Plan Do Check Action) ซึ่งเป็นโครงสร้างเดียวกับระบบการบริหารที่เป็นสากล
- สามารถขอใบรับรอง เพื่อให้มีการรับรองมาตรฐานปฏิบัติงานได้

ISMR ประกอบด้วย Requirement (Clause ๔ - ๑๐) และ Annex A Control (A.๕ – A.๑๘)

Requirement (Clause ๔ - ๑๐)

Clause ๔

บริบทขององค์กร ประกอบด้วย

- ทำความเข้าใจองค์กรและบริบทขององค์กร
- กำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง
- การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

Clause ๕

ภาวะผู้นำ ประกอบด้วย

- ภาวะผู้นำและการให้ความสำคัญ
- นโยบาย
- บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่

Clause ๖

การวางแผน ประกอบด้วย

- การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส
- วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์

Clause ๗

การสนับสนุน ประกอบด้วย

- ทรัพยากร
- สมรรถนะ
- การสร้างความตระหนัก
- การสื่อสาร
- เอกสารสารสนเทศ

Clause ๘

การดำเนินการ ประกอบด้วย

- การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม
- การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

Clause ๙

การประเมินประสิทธิภาพและประสิทธิผล ประกอบด้วย

- การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน
- การตรวจประเมินภายใน
- การทบทวนของผู้บริหาร

Clause ๑๐

การปรับปรุง ประกอบด้วย

- ความไม่สอดคล้องและการดำเนินการแก้ไข
- การปรับปรุงอย่างต่อเนื่อง

Annex A Control (A.๕ – A.๑๘)

A.๕ นโยบายความมั่นคงปลอดภัยขององค์กร
A.๖ โครงสร้างของความมั่นคงปลอดภัยสำหรับสารสนเทศ
A.๗ ความมั่นคงปลอดภัยด้านทรัพยากรมนุษย์
A.๘ การบริหารจัดการทรัพย์สิน
A.๙ การควบคุมการเข้าถึง
A.๑๐ การเข้ารหัสข้อมูล
A.๑๑ ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร
A.๑๒ ความปลอดภัยในการปฏิบัติงาน
A.๑๓ ความปลอดภัยในด้านการสื่อสาร
A.๑๔ ความต้องการ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
A.๑๕ ความสัมพันธ์กับซัพพลายเออร์
A.๑๖ การจัดการเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางสารสนเทศ
A.๑๗ การบริหารความต่อเนื่องขององค์กรในด้านความปลอดภัยของข้อมูลสารสนเทศ
A.๑๘ การปฏิบัติตามข้อกำหนดทางกฎหมาย และนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

Application Control การควบคุมเฉพาะด้านระบบงาน

เป็นการควบคุมแบบ Manual หรือการควบคุมแบบ Automatic โดยโปรแกรม ซึ่งเป็นการควบคุมในระดับกระบวนการหรือรายการธุรกิจ

การแบ่งตามวัตถุประสงค์

๑. ความควบถ้วน (Completeness) คือ การบันทึกรายการทุกรายเข้าในระบบ และประมวลผลอย่างสมบูรณ์เพียงครั้งเดียว ระบบปฏิเสธการบันทึกและประมวลผลซ้ำ มีการตรวจสอบและแก้ไข รายการที่ระบบปฏิเสธการบันทึกและประมวลผล

๒. ความถูกต้อง (Accuracy) คือ การควบคุมให้มีการบันทึกข้อมูลให้ครบทุกฟิลด์ และถูกต้อง ระบบงานจึงจะรับรายการเข้าไปประมวลผล

๓. การอนุมัติ (Validity) คือ รายการที่บันทึกเข้าระบบเพื่อประมวลผลได้รับการอนุมัติจากผู้มีอำนาจอย่างเหมาะสม

๔. การจำกัดการเข้าถึงข้อมูล (Restricted Access) คือ ระบบงานและข้อมูลมีการควบคุมเพื่อป้องกันการเข้าถึง หรือการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต การเข้าถึงข้อมูลลับหรือทรัพย์สินเฉพาะผู้ที่ได้รับการอนุญาต

การแบ่งตามขั้นตอนการทำงานของระบบ

๑. การควบคุมการนำเข้า (Input Controls) เป็นการควบคุมที่สำคัญ เนื่องจากเป็นต้นทางของความถูกต้องเชื่อถือได้ของข้อมูลทั้งหมด

๒. การควบคุมการประมวลผล (Processing Controls) เป็นการควบคุมเพื่อให้การประมวลผลของระบบถูกต้อง

๓. การควบคุมผลลัพธ์ที่ได้จากการประมวลผล (Output Controls) เป็นการควบคุมระยะสุดท้ายเพื่อให้ได้ข้อมูลผลลัพธ์และรายงานที่ถูกต้องจากระบบ การควบคุมผลลัพธ์จะขึ้นอยู่กับความเชื่อถือได้ของการควบคุมการนำเข้าและการประมวลผล โดยหากมีการควบคุมที่ดีตั้งแต่ต้น ก็จะเพื่อความเชื่อถือได้ของผลลัพธ์อย่างมาก

๔. การควบคุมด้วยแฟ้มร่องรอยการตรวจสอบ (Audit Trails) คือการจัดทำแฟ้มทะเบียนร่องรอบที่สร้างขึ้น เพื่อบันทึกกิจกรรมในระดับระบบงาน หรือผู้ใช้งาน โดยหากมีการออกแบบและใช้งานที่ดี จะเป็นวิธีควบคุมแบบค้นพบ (detective controls) ที่มีประสิทธิภาพ เช่น การบันทึกเหตุการณ์สำคัญสำหรับรหัสผู้ใช้ ได้แก่ ความพยายามเข้าระบบ (invalid log-on) ทรัพยากรบนระบบที่ใช้งาน เป็นต้น