การตรวจสอบ ด้านเทคโนโลยีสารสนเทศ

ในการดำเนินงานขององค์กรจะมีระบบงานต่างๆที่จะขับเคลื่อนให้การทำงานขององค์กรสามารถบรรลุผลสำเร็จ โดยอาศัยระบบเทคโนโลยีสารสนเทศเป็นเครื่องมือช่วยสนับสนุนการปฏิบัติงานให้เกิดความสะดวก คล่องตัว และรวดเร็วยิ่งขึ้น โดยผ่านระบบ Application ซึ่งเป็นโปรแกรมการปฏิบัติงานต่างๆ ภายในระบบเทคโนโลยีสารสนเทศความเสี่ยง เริ่มตั้งแต่การนำข้อมูลเข้า เช่น งานจัดเก็บรายได้ของกรมสรรพสามิต อาจมีความเสี่ยงระบบล่ม ไม่สามารถบันทึกข้อมูลได้ หรือระบบถูกบุคคลที่ไม่ได้รับอนุญาตเข้าใช้ข้อมูล

การควบคุมภายในด้านเทคโนโลยีสารสนเทศประกอบด้วยการควบคุมทั่วไป (General Control) และการควบคุมเฉพาะระบบงาน (Application Control)

การควบคุมทั่วไป (General Control) หมายถึง การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุมนโยบายและวิธีการในการควบคุมระบบสารสนเทศ การควบคุมความปลอดภัย การควบคุมการพัฒนาและปรับปรุง และการป้องกัน/ลดความเสียหายของระบบ เป็นการควบคุมภายในสำหรับองค์กรในภาพรวม

1 การกำหนดนโยบายในการใช้สารสนเทศ

- มีนโยบายการรักษาความปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศที่ชัดเจนว่าใครต้องการเข้าถึงข้อมูลอะไร เมื่อไหร่
- การให้สิทธิในการเข้าถึงข้อมูลเฉพาะบุคคลที่มีสิทธิในการเข้าถึงข้อมูลนั้น

2 การแบ่งแยกหน้าที่งานในระบบสารสนเทศ

มีการแบ่งแยกหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในระบบงานคอมพิวเตอร์ให้ชัดเจน เช่น แยกหน้าที่การพัฒนาระบบออกจากหน้าที่ผู้ปฏิบัติการคอมพิวเตอร์ผู้บริหารฐานข้อมูล (Database Administrator) ต้องไม่ทำหน้าที่อื่น ผู้พัฒนาระบบออกจากผู้ดูแลบำรุงรักษาระบบ

3 การควบคุมโครงการพัฒนาระบบสารสนเทศ

โดยกำหนดแผนระยะยาว แผนงานพัฒนาระบบ กำหนดการประมวลผลข้อมูล มอบหมายหน้าที่ และความรับผิดชอบ การประเมินผลงานระหว่างการดำเนินโครงการ การสอบทานภายหลังการติดตั้งระบบ และนำระบบมาใช้งาน การวัดผลการดำเนินงานของระบบ

4 การควบคุมการเปลี่ยนแปลงแก้ไขระบบ

โดยการกำหนดระเบียบวิธีปฏิบัติในการแก้ไขระบบที่เป็นลายลักษณ์อักษร มีการศึกษาถึงผลกระทบต่างๆ มีการทดสอบระบบที่แก้ไขแล้วก่อนนำไปใช้จัดทำเอกสารคู่มือประกอบการแก้ไข และประเมินผลและสอบทานระบบงานภายหลังเริ่มใช้งาน

5 การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์

การประมวลผลข้อมูลของระบบงานต่างๆ มีความถูกต้องครบถ้วน การกู้ระบบและการสำรองข้อมูล การทดสอบ และการจัดการกับปัญหาของระบบ จัดทำแผนสำรอง

6 การควบคุมเข้าถึงอุปกรณ์คอมพิวเตอร์

มีสถานที่จัดเก็บอุปกรณ์คอมพิวเตอร์มิดชิด ไม่มีอากาศร้อน ชื้น และแม่เหล็ก มีการรักษาความปลอดภัยหนาแน่น กำหนดการเข้าออกได้เฉพาะผู้เกี่ยวข้อง กำหนดนโยบายรักษาความปลอดภัยที่ชัดเจน ติดระบบเตือนภัย กรณีมีผู้บุกรุก จะจำกัดให้ใช้โทรศัพท์เฉพาะเรื่องที่เกี่ยวกับงาน ติดอุปกรณ์ป้องกันเครื่องคอมพิวเตอร์

7 การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ

การกำหนดผู้ใช้ (User Views or Subschema) ตารางแสดงสิทธิในการเข้าถึงฐานข้อมูล (Database Authorization Table) และการเข้ารหัสข้อมูล (Data Encryption)

8 การควบคุมการเข้าถึงระบบงาน มีดังนี้

- การพิสูจน์ตัวจริง (Authentication) โดยกำหนดรหัสผ่าน (Password) การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ (Physical Possession Identification)
- การกำหนดสิทธิ (Authorization)
- การบันทึกกิจกรรมต่างๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)

การควบคุมเฉพาะระบบงาน (Application Control)

การควบคุมรายการข้อมูลในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของข้อมูล เป็นแนวทางในการกำหนดขอบเขตการควบคุม เช่น ระบบ GFMIS

การควบคุมการนำเข้าข้อมูล

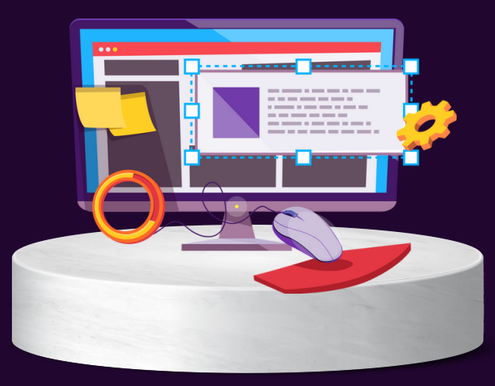
การควบคุมเกี่ยวกับงานจัดทำข้อมูลก่อนป้อนเข้าสู่ระบบคอมพิวเตอร์ การเตรียมข้อมูลนำเข้า การป้องกันข้อผิดพลาด การค้นหาข้อผิดพลาด และการแก้ไขข้อผิดพลาด เช่น การตรวจสอบตัวเลขตรวจสอบ (Check digit) ว่าเป็นตัวเลขที่ถูกหรือไม่ โดยเลขประจำตัว หรือรหัสสินค้า หรือเลขที่บัญชี

การควบคุมการทำรายการป้อนเข้าสู่ระบบงาน

โดยข้อมูลที่ป้อนเข้าสู่ระบบจะต้องถูกหลักเกณฑ์ในการทำรายการ นอกจากนี้ยังรวมถึงเรื่องที่เกี่ยวกับการกระทบยอดข้อมูลนำเข้าเพื่อพิสูจน์ความถูกต้อง

การควบคุมการสื่อสารข้อมูล

ให้มีความถูกต้องและครบถ้วน ซึ่งจะต้องคำนึงถึง Hardware และ Software ที่ใช้ในการสื่อสารข้อมูลการมอบอำนาจ



การควบคุมการประมวลผลด้วยคอมพิวเตอร์

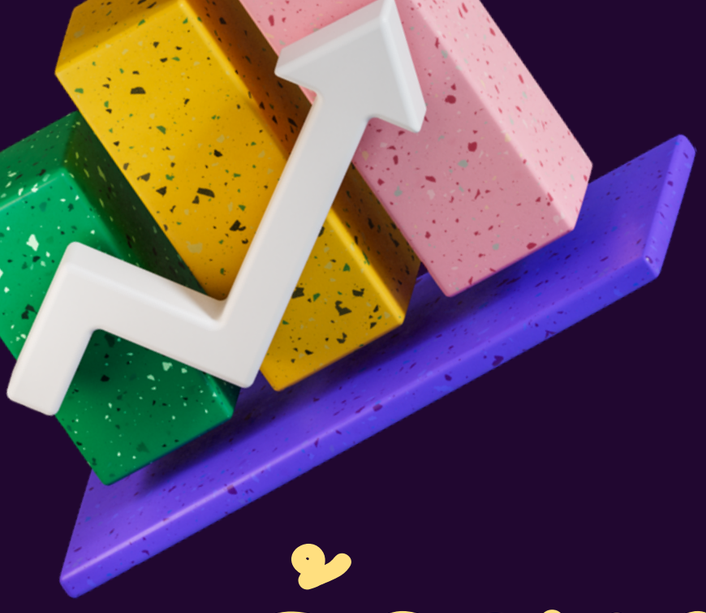
ให้มีความแม่นยำ ถูกต้อง และครบถ้วน เป็นไปตามหลักเกณฑ์ การใช้แฟ้มข้อมูล การชี้แนะให้เห็นข้อผิดพลาด และการรายงาน

การควบคุมการจัดเก็บข้อมูลไว้ในระบบ

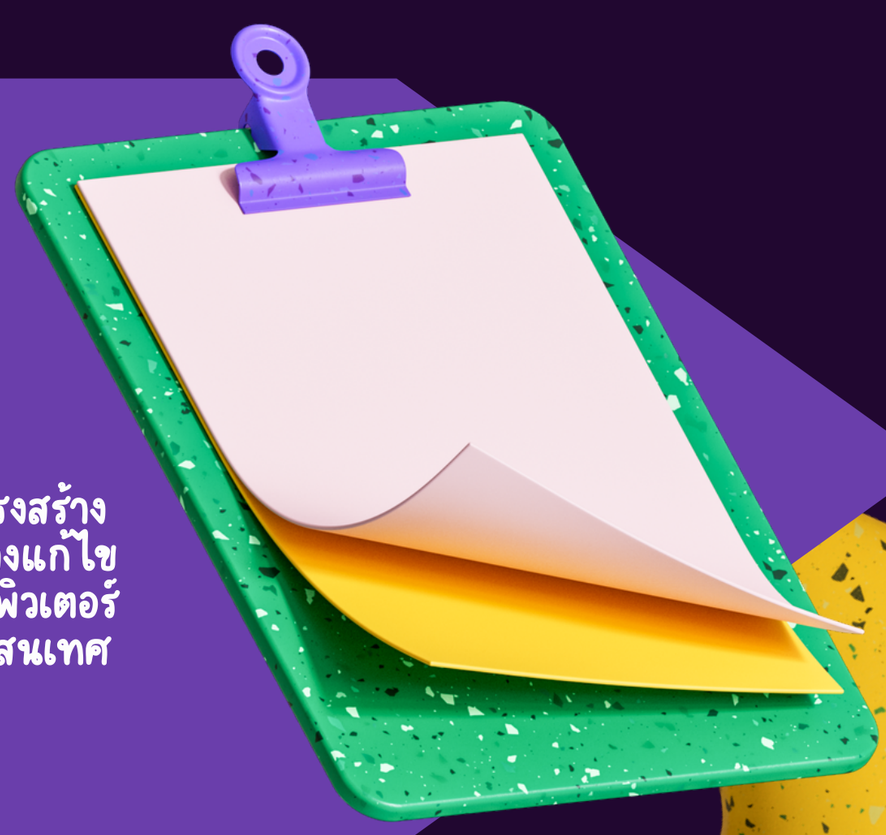
การกำหนดสิทธิการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การสำรองข้อมูล และการกำหนดอายุการจัดเก็บแฟ้มข้อมูล

การควบคุมผลลัพธ์

การกระทบยอดข้อมูลนำเข้าและผลลัพธ์ เพื่อพิสูจน์ความถูกต้องด้วยระบบ Manual ซึ่งเป็นหน้าที่โดยตรงของหน่วยงานควบคุมคุณภาพข้อมูล



การตรวจสอบ ด้านเทคโนโลยีสารสนเทศ



การตรวจสอบ การควบคุมทั่วไป

โดยตรวจสอบในเรื่อง การวางแผนระยะยาวและแผนระยะสั้น การจัดโครงสร้างงานสารสนเทศ มีความเหมาะสมชัดเจน การพัฒนาและการเปลี่ยนแปลงแก้ไขระบบงาน การรักษาความปลอดภัยระบบสารสนเทศ การปฏิบัติการคอมพิวเตอร์ (การปิดเปิดระบบ การบำรุงรักษา การจัดเก็บ) การจัดทำแผนกู้ระบบสารสนเทศ

การตรวจสอบ การควบคุมเฉพาะระบบงาน

โดยการตรวจสอบในเรื่อง การกำหนดสิทธิในการใช้งานมีความเหมาะสมกับหน้าที่ความรับผิดชอบหรือไม่ การแบ่งแยกหน้าที่ในระบบงานสารสนเทศ การนำเข้าข้อมูลและรายการ การรับส่งข้อมูลระหว่างระบบงาน การประมวลผล การนำผลลัพธ์ไปใช้งานครบถ้วน ถูกต้องหรือไม่ มีการจัดเก็บเหมาะสมหรือไม่

กระบวนการตรวจสอบ ระบบสารสนเทศ

มีกระบวนการเช่นเดียวกับตรวจสอบภายในประเภทอื่นๆ โดยเริ่มตั้งแต่ผู้ตรวจสอบภายในศึกษาทำความเข้าใจระบบงานสารสนเทศ (การควบคุมและความเสี่ยง) ประเมินความเสี่ยงเพื่อวางแผนการตรวจสอบ จัดทำแผนตามผลประเมินความเสี่ยง จัดทำแผนการตรวจสอบระยะยาว แผนการตรวจสอบประจำปี แผนการปฏิบัติงาน จัดทำกระดาษทำการ สรุปข้อเท็จจริง รายงานผลการตรวจสอบ และการติดตามผลการตรวจสอบ ทั้งนี้ ผู้ตรวจสอบระบบสารสนเทศต้องมีความรู้ ความเชี่ยวชาญเกี่ยวกับระบบเทคโนโลยีสารสนเทศ เช่น ตรวจสอบระบบ GFMIS ต้องมีความรู้ ความเข้าใจในระบบ SAP และความเสี่ยงการควบคุมภายในของระบบเทคโนโลยีสารสนเทศ โดยพิจารณาจาก FLOWCHART การทดสอบความเชื่อมโยงของระบบ เป็นต้น

รายงานสรุปองค์ความรู้
การพัฒนาความรู้ของผู้ปฏิบัติงานด้านการตรวจสอบภายในสำหรับหน่วยงานรัฐ
ประจำปีงบประมาณ พ.ศ. ๒๕๖๗
หลักสูตรผู้ปฏิบัติงานตรวจสอบภายใน (หลักสูตรพัฒนาความรู้ต่อเนื่อง)
ผ่านช่องทางออนไลน์ในรูปแบบ Microsoft Teams Live

ผู้เข้ารับการอบรม นางสาววรานิษฐ์ ศิริพรอมาตย์ **อายุ** ๒๘ ปี

ตำแหน่ง นักวิเคราะห์นโยบายและแผน **ระดับ** –

สังกัด กลุ่มตรวจสอบภายใน **โทร** ๐๒ ๑๔๒ ๑๓๕๗

ผู้เข้ารับการอบรม นางสาวอริศรา ปราณีตพลารักษ์ **อายุ** ๒๗ ปี

ตำแหน่ง เจ้าหน้าที่การเงินและบัญชี **ระดับ** –

สังกัด กลุ่มตรวจสอบภายใน **โทร** ๐๒ ๑๔๒ ๑๓๕๗

ผู้เข้ารับการอบรม นางสาวภูษณิศา ไกรสุทรังค์ **อายุ** ๒๖ ปี

ตำแหน่ง เจ้าหน้าที่การเงินและบัญชี **ระดับ** –

สังกัด กลุ่มตรวจสอบภายใน **โทร** ๐๒ ๑๔๒ ๑๓๕๗

รายงานการฝึกอบรมการพัฒนาความรู้ของผู้ปฏิบัติงานด้านการตรวจสอบภายใน

สำหรับหน่วยงานของรัฐ หลักสูตรผู้ปฏิบัติงานตรวจสอบภายใน (หลักสูตรพัฒนาความรู้ต่อเนื่อง)

หลักการและเหตุผล

กระทรวงการคลังโดยกรมบัญชีกลาง ได้กำหนดหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ ในส่วนของมาตรฐานการตรวจสอบภายในสำหรับหน่วยงานของรัฐ รหัส ๑๒๑๐ กำหนดให้ผู้ตรวจสอบภายในเข้ารับการฝึกอบรมและแสวงหาความรู้จากองค์กรในทางวิชาชีพ เพื่อให้ได้รับวุฒิบัตรที่เกี่ยวข้องกับการปฏิบัติงานตรวจสอบภายในที่แสดงให้เห็นถึงความเชี่ยวชาญ และรหัส ๑๒๓๐ ผู้ตรวจสอบภายในต้องหมั่นศึกษาหาความรู้ ทักษะและความสามารถอื่นๆ เพิ่มเติมตลอดเวลาเพื่อให้เกิดการพัฒนาวิชาชีพอย่างต่อเนื่อง กระทรวงการคลังโดยกรมบัญชีกลางจึงได้จัดฝึกอบรมพัฒนาความรู้ของผู้ปฏิบัติงานด้านการตรวจสอบภายในสำหรับหน่วยงานของรัฐประจำปีงบประมาณ พ.ศ. ๒๕๖๖ ขึ้นเพื่อการพัฒนาขีดสมรรถนะและศักยภาพของผู้ตรวจสอบภายในปฏิบัติงานให้เป็นมืออาชีพ

วัตถุประสงค์

เพื่อให้ผู้ปฏิบัติงานด้านการตรวจสอบภายในมีความรู้ทักษะ และความสามารถอื่นๆ ที่จำเป็นต่อการปฏิบัติงานด้านการตรวจสอบภายใน

วิธีการฝึกอบรม

รับฟังการบรรยาย ๘ หลักสูตรย่อย วิชาละ ๓ ชั่วโมง

การเข้าร่วมฝึกอบรม ในฐานะผู้รับการฝึกอบรม

วันที่ ๒๘ ธันวาคม ๒๕๖๖ เวลา ๑๓.๐๐ น. – ๑๖.๐๐ น.
หลักสูตรผู้ปฏิบัติงานตรวจสอบภายใน (หลักสูตรพัฒนาความรู้ต่อเนื่อง)
วิชา การตรวจสอบเทคโลยีสารสนเทศ
โดยกรมบัญชีกลาง กองตรวจสอบภาครัฐ

การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ในการดำเนินงานขององค์กรจะมีระบบงานต่างๆ ที่จะขับเคลื่อนให้การทำงานขององค์กรสามารถบรรลุผลสำเร็จ โดยอาศัยระบบเทคโนโลยีสารสนเทศเป็นเครื่องมือช่วยสนับสนุนการปฏิบัติงานให้เกิดความสะดวกคล่องตัว และรวดเร็วยิ่งขึ้น โดยผ่านระบบ Application ซึ่งเป็นโปรแกรมการปฏิบัติงานต่างๆ ภายในระบบเทคโนโลยีสารสนเทศความเสี่ยง เริ่มตั้งแต่การนำข้อมูลเข้า เช่น งานจัดเก็บรายได้ของกรมสรรพสามิต อาจมีความเสี่ยงระบบล่ม ไม่สามารถบันทึกข้อมูลได้ หรือระบบถูกบุคคลที่ไม่ได้รับอนุญาตเข้าใช้ข้อมูล

การควบคุมภายในด้านเทคโนโลยีสารสนเทศ ประกอบด้วย การควบคุมทั่วไป (General Control) และการควบคุมเฉพาะระบบงาน (Application Control)

การควบคุมทั่วไป (General Control) หมายถึง การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุมนโยบายและวิธีการในการควบคุมระบบสารสนเทศ การควบคุมความปลอดภัย การควบคุมการพัฒนาและปรับปรุง และการป้องกัน/ลดความเสียหายของระบบ เป็นการควบคุมภายในสำหรับองค์กรในภาพรวม

๑. การกำหนดนโยบายในการใช้สารสนเทศ

- มีนโยบายการรักษาความปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศที่ชัดเจนว่าใครต้องการเข้าถึง ข้อมูลอะไร เมื่อไหร่ ในระบบงานใด
- การให้สิทธิในการเข้าถึงข้อมูลเฉพาะบุคคลที่มีสิทธิในการเข้าถึงข้อมูลนั้น

๒. การแบ่งแยกหน้าที่งานในระบบสารสนเทศ มีการแบ่งแยกหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในระบบงานคอมพิวเตอร์ให้ชัดเจน เช่น แยกหน้าที่การพัฒนาระบบออกจากหน้าที่ผู้ปฏิบัติการคอมพิวเตอร์ผู้บริหารฐานข้อมูล (Database Administrator) ต้องไม่ทำหน้าที่อื่น ผู้พัฒนาระบบออกจากผู้ดูแลบำรุงรักษาระบบ

๓. การควบคุมโครงการพัฒนาระบบสารสนเทศ โดยกำหนดแผนระยะยาว แผนงานพัฒนาระบบ กำหนดการประมวลผลข้อมูล มอบหมายหน้าที่ และความรับผิดชอบ การประเมินผลงานระหว่างการดำเนินโครงการ การสอบทานภายหลังการติดตั้งระบบ และนำระบบมาใช้งาน การวัดผลการดำเนินงานของระบบ

๔. การควบคุมการเปลี่ยนแปลงแก้ไขระบบ โดยการกำหนดระเบียบวิธีปฏิบัติในการแก้ไขระบบที่เป็นลายลักษณ์อักษร มีการศึกษาถึงผลกระทบต่างๆ มีการทดสอบระบบที่แก้ไขแล้วก่อนนำไปใช้จัดทำเอกสารคู่มือประกอบการแก้ไข และประเมินผลและสอบทานระบบงานภายหลังเริ่มใช้งาน

๕. การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์ การประมวลผลข้อมูลของระบบงานต่างๆ มีความถูกต้องครบถ้วน การกู้ระบบและการสำรองข้อมูล การทดสอบ และการจัดการกับปัญหาของระบบ จัดทำแผนสำรอง

๖. การควบคุมเข้าถึงอุปกรณ์คอมพิวเตอร์ มีสถานที่จัดเก็บอุปกรณ์คอมพิวเตอร์มิดชิด ไม่มีอากาศร้อนชื้น และแม่เหล็ก มีการรักษาความปลอดภัยหนาแน่น กำหนดการเข้าออกได้เฉพาะผู้เกี่ยวข้อง กำหนดนโยบาย

รักษาความปลอดภัยที่ชัดเจน ติดระบบเตือนภัย กรณีมีผู้บุกรุก จะจำกัดให้ใช้โทรศัพท์เฉพาะเรื่องที่เกี่ยวกับงาน ติดอุปกรณ์ป้องกันเครื่องคอมพิวเตอร์

๗. การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ การกำหนดผู้ใช้ (User Views or Subschema) ตารางแสดงสิทธิในการเข้าถึงฐานข้อมูล (Database Authorization Table) และการเข้ารหัสข้อมูล (Data Encryption)

๘. การควบคุมการเข้าถึงระบบงาน ดังนี้

- การพิสูจน์ตัวจริง (Authentication) โดยกำหนดรหัสผ่าน (Password) การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ (Physical Possession Identification)

- การกำหนดสิทธิ (Authorization)

- การบันทึกกิจกรรมต่างๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)

การควบคุมเฉพาะระบบงาน (Application Control)

การควบคุมรายการข้อมูลในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของข้อมูลเป็นแนวทางในการกำหนดขอบเขตการควบคุม เช่น ระบบ GFMIS

๑) การควบคุมการนำเข้าข้อมูล การควบคุมเกี่ยวกับงานจัดทำข้อมูลก่อนป้อนเข้าสู่ระบบคอมพิวเตอร์ การเตรียมข้อมูลนำเข้า การป้องกันข้อผิดพลาด การค้นหาข้อผิดพลาด และการแก้ไขข้อผิดพลาด เช่น การตรวจสอบตัวเลขตรวจสอบ (Check digit) ว่าเป็นตัวเลขที่ถูกหรือไม่ โดยเลขประจำตัว หรือรหัสสินค้า หรือเลขที่บัญชี

๒) การควบคุมการทำรายการป้อนเข้าสู่ระบบงาน โดยข้อมูลที่ป้อนเข้าสู่ระบบจะต้องถูกหลักเกณฑ์ในการทำรายการ นอกจากนี้ยังรวมถึงเรื่องที่เกี่ยวกับการกระทบยอดข้อมูลนำเข้าเพื่อพิสูจน์ความถูกต้อง

๓) การควบคุมการสื่อสารข้อมูลให้มีความถูกต้องและครบถ้วน ซึ่งจะต้องคำนึงถึง Hardware และ Software ที่ใช้ในการสื่อสารข้อมูลการมอบอำนาจ

๔) การควบคุมการประมวลผลด้วยคอมพิวเตอร์ให้มีความแม่นยำ ถูกต้อง และครบถ้วน เป็นไปตามหลักเกณฑ์ การใช้แฟ้มข้อมูล การชี้แนะให้เห็นข้อผิดพลาด และการรายงาน

๕) การควบคุมการจัดเก็บข้อมูลไว้ในระบบ การกำหนดสิทธิการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การสำรองข้อมูล และการกำหนดอายุการจัดเก็บแฟ้มข้อมูล

๖) การควบคุมผลลัพธ์ การกระทบยอดข้อมูลนำเข้าและผลลัพธ์ เพื่อพิสูจน์ความถูกต้องด้วยระบบ Manual ซึ่งเป็นหน้าที่โดยตรงของหน่วยงานควบคุมคุณภาพข้อมูล

การตรวจสอบการควบคุมทั่วไป

โดยตรวจสอบในเรื่อง การวางแผนระยะยาวและแผนระยะสั้น การจัดโครงสร้างงานสารสนเทศ มีความเหมาะสมชัดเจน (การแบ่งแยกหน้าที่เหมาะสม) การพัฒนาและการเปลี่ยนแปลงแก้ไขระบบงาน การรักษาความปลอดภัยระบบสารสนเทศ การปฏิบัติการคอมพิวเตอร์ (การปิดเปิดระบบ การบำรุงรักษา การจัดเก็บ) การจัดทำแผนกู้ระบบสารสนเทศ

การตรวจสอบการควบคุมเฉพาะระบบงาน

โดยการตรวจสอบในเรื่อง การกำหนดสิทธิในการใช้งานมีความเหมาะสมกับหน้าที่ความรับผิดชอบหรือไม่ การแบ่งแยกหน้าที่ในระบบงานสารสนเทศ การนำเข้าข้อมูลและรายการ การรับส่งข้อมูลระหว่างระบบงาน การประมวลผลในระบบงาน การนำผลลัพธ์ไปใช้งานครบถ้วน ถูกต้องหรือไม่ มีการจัดเก็บเหมาะสมหรือไม่

กระบวนการตรวจสอบระบบสารสนเทศ

มีกระบวนการเช่นเดียวกับตรวจสอบภายในประเภทอื่นๆ โดยเริ่มตั้งแต่ผู้ตรวจสอบภายในศึกษาทำความเข้าใจระบบงานสารสนเทศ (การควบคุมและความเสี่ยง) ประเมินความเสี่ยงเพื่อวางแผนการตรวจสอบ จัดทำแผนตามผลประเมินความเสี่ยง จัดทำแผนการตรวจสอบระยะยาว แผนการตรวจสอบประจำปี แผนการปฏิบัติงาน จัดทำกระดาษทำการ สรุปข้อเท็จจริง รายงานผลการตรวจสอบ และการติดตามผลการตรวจสอบ ทั้งนี้ ผู้ตรวจสอบระบบสารสนเทศต้องมีความรู้ ความเชี่ยวชาญเกี่ยวกับระบบเทคโนโลยีสารสนเทศ เช่น ตรวจสอบระบบ GFMIS ต้องมีความรู้ ความเข้าใจในระบบ SAP และความเสี่ยงการควบคุมภายในของระบบเทคโนโลยีสารสนเทศ โดยพิจารณาจาก Flowchart การทดสอบความเชื่อมโยงของระบบ เป็นต้น

สรุปผลการเข้าฝึกอบรม

จากผลการเข้าฝึกอบรม ทำให้ผู้อบรมทราบถึงการนำระบบเทคโนโลยีสารสนเทศ มาเป็นเครื่องมือในการช่วยสนับสนุนการปฏิบัติงานให้เกิดความสะดวก คล่องตัว และรวดเร็วยิ่งขึ้น ตั้งแต่การนำข้อมูลเข้า การควบคุมระบบการทำงานต่างๆ การตรวจสอบการควบคุมระบบ เป็นต้น ซึ่งการนำระบบเทคโนโลยีมาใช้ในการปฏิบัติงานส่งผลให้การดำเนินงานสามารถบรรลุวัตถุประสงค์ตามแผนการตรวจสอบได้อย่างมีประสิทธิภาพ

การนำองค์ความรู้ไปใช้ในการปฏิบัติงาน

องค์ความรู้ที่ได้สามารถนำไปใช้เป็นแนวทางในการปฏิบัติงาน เพื่อให้การปฏิบัติงานตรวจสอบภายในมีความทันสมัย และความถูกต้องครบถ้วนมากยิ่งขึ้น โดยการนำระบบเทคโนโลยีสารสนเทศมาใช้ร่วมในการปฏิบัติงานสามารถช่วยประหยัดเวลาในการค้นหาหรือตรวจสอบข้อมูล รวมถึงมีความถูกต้องและแม่นยำสูง ส่งผลให้การปฏิบัติงานตรวจสอบภายในบรรลุผลสำเร็จ