รายงานผลการเข้ารับการฝึกอบรม

หลักสูตร
กระบวนการตรวจสอบแอพพลิเคชันด้านไอที
(IT Application Audit Process)

จัดโดย

สถาบันวิทยาการ สวทช.
อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)
ถนนพระรามที่ 6 เขตราชเทวี กรุงเทพมหานคร

วันที่ 16-18 พฤษภาคม พ.ศ. 2561

ผู้จัดทำ
รองศาสตราจารย์ทัศนีย์วรรณ์ ศรีประดิษฐ์
สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ได้รับทุนสนับสนุนจากกองทุนพัฒนาบุคลากรมหาวิทยาลัยสุโขทัยธรรมาธิราช
ประจำปีงบประมาณ 2561

รายงานการไปฝึกอบรม ดูงาน ประชุม / สัมมนา

ตามระเบียบมหาวิทยาลัยสุโขทัยธรรมาธิราช ว่าด้วยการให้ทุนฝึกอบรม ดูงาน

และประชุมทางวิชาการแก่ข้าราชการมหาวิทยาลัยสุโขทัยธรรมาธิราช

---

1. ผู้เข้ารับการฝึกอบรม

ชื่อ นางสาวทัศนีย์วรรณ์ ศรีประดิษฐ์ ตำแหน่ง รองศาสตราจารย์ ระดับ 9

สังกัด สาขาวิชาวิทยาศาสตร์และเทคโนโลยี โทร. 8290

ไปเข้าร่วม การฝึกอบรมหลักสูตรกระบวนการตรวจสอบแอพพลิเคชันด้านไอที
(IT Application Audit Process)
ณ อาคารสำนักงานพัฒนาวิทยาศาสาตร์และเทคโนโลยีแห่งชาติ (สวทช.)
ถนนพระรามที่ 6 เขตราชเทวี กรุงเทพมหานคร

จัดโดย สถาบันวิทยาการ สวทช.

ตั้งแต่วันที่ 16 พฤษภาคม 2561 ถึงวันที่ 18 พฤษภาคม 2561 รวมระยะเวลา 3 วัน

2. รายละเอียดเกี่ยวกับการเข้ารับการฝึกอบรม

2.1 หัวข้อเรื่อง..กระบวนการตรวจสอบแอพพลิเคชันด้านไอที (IT Application Audit Process)

วิทยากรในการอบรม คือ อาจารย์ภิธันปติ์ ถิรสัตยาพิทักษ์

2.2 วัตถุประสงค์ของการฝึกอบรม

1) เพื่อให้มีความรู้ ความเข้าใจในความจำเป็นของการตรวจสอบระบบงานด้านเทคโนโลยีสารสนเทศ
2) เพื่อให้มีความรู้ ความเข้าใจในกระบวนการตรวจสอบระบบงานด้านเทคโนโลยีสารสนเทศ
3) เพื่อให้มีความรู้ ความเข้าใจในการวางแผนตรวจสอบระบบงานด้านเทคโนโลยีสารสนเทศ
4) เพื่อให้มีความรู้ ความเข้าใจในการประเมินความเสี่ยงของระบบงานด้านเทคโนโลยีสารสนเทศ
5) เพื่อให้มีความรู้ ความเข้าใจในการควบคุมระบบงานด้านเทคโนโลยีสารสนเทศ
6) เพื่อให้มีความรู้ ความเข้าใจในการติดตามและประเมินผลการควบคุม

2.3 วิธีการฝึกอบรม

ฟังวิทยากรบรรยาย และฝึกปฏิบัติ Case Study

3. สรุปเนื้อหาสาระสำคัญ ที่ได้รับจากการเข้ารับการฝึกอบรม

- **องค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**
  นิยมใช้ตัวย่อว่า CIA ซึ่งเป็นองค์ประกอบ 3 ส่วน ดังนี้

1) **C***onfidentiality : การรักษาความลับของสารสนเทศ* เพื่อให้มั่นใจได้ว่า สารสนเทศขององค์กรจะสามารถล่วงรู้ เข้าถึง และใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตและมีสิทธิ์ตามที่องค์กรกำหนดไว้เท่านั้น
2) **I***ntegrity : การรักษาความคงสภาพเดิมของสารสนเทศ* เพื่อให้มั่นใจได้ว่า สารสนเทศมีความถูกต้องและสมบูรณ์ครบถ้วน ไม่ถูกแก้ไขเปลี่ยนแปลง นับตั้งแต่สารสนเทศได้รับการสร้างขึ้นหรือถูกทำลายจากผู้ที่ไม่มีสิทธิ์ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม
3) ***A****vailability : การรักษาความพร้อมใช้งานของสารสนเทศ* เพื่อให้มั่นใจว่า สารสนเทศมีความพร้อมที่จะให้ผู้ที่มีสิทธิ์เข้าถึงสารสนเทศ และสามารถเข้าถึงและใช้งานสารสนเทศได้ทุกเมื่อที่ต้องการ

- **ปัจจัยความเสี่ยงต่อความไม่มั่นคงปลอดภัยด้าน IT** เกิดขึ้นได้จาก 3 ส่วน คือ
  1) *People Risk :* เกิดจากตัวบุคคล ทั้งที่เป็นบุคลากรภายในและภายนอกองค์กร ซึ่งเป็นผู้ก่อให้เกิดความไม่มั่นคงปลอดภัยกับสารสนเทศขององค์กร
  2) *Process Risk :* เกิดจากการที่องค์กรไม่ดำเนินการจัดทำขั้นตอนปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ หรืออาจดำเนินการโดยขาดวิธีการควบคุมที่รัดกุมเพียงพอ หรือเกิดจากการละเลยไม่ปฏิบัติตาม
  3) *Technology Risk :* เกิดจากการที่องค์กรควบคุมการทำงานของเทคโนโลยีสารสนเทศไม่ดีพอ ทำให้เกิดช่องโหว่และมีผู้ไม่ประสงค์ดีเข้ามาคุกคาม สร้างความเสียหายให้แก่องค์กรได้

- **ความเสี่ยงด้าน IT** ประกอบด้วยความเสี่ยง 6 ด้าน ได้แก่
  1) *ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม* หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติ เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม สิ่งแวดล้อมที่มนุษย์กระทำขึ้น ทั้งโดยเจตนาและไม่เจตนา เช่น กระแสไฟฟ้าขัดข้อง เพลิงไหม้ ไม่มีระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์

2) *ความเสี่ยงด้านบุคลากร* หมายถึง ความเสี่ยงที่เกิดจากบุคลากรดำเนินงานหรือใช้งานเทคโนโลยีสารสนเทศขององค์กรโดยไม่ได้รับอนุญาตหรือไม่ได้รับสิทธิในการเข้าถึงและใช้งานระบบสารสนเทศ รวมถึงการก่อให้เกิดความเสียหายกับสารสนเทศขององค์กรไม่ว่าจะเจตนาหรือไม่ก็ตาม
3) *ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ* หมายถึง ความเสี่ยงที่เกิดจากช่องโหว่ จุดอ่อน หรือความผิดพลาดของอุปกรณ์ รวมถึงการปรับแต่งค่าต่างๆ ที่ไม่เหมาะสมกับสภาพการใช้งานจริง การติดตั้งอุปกรณ์ในพื้นที่ที่ไม่เหมาะสม ง่ายต่อการถูกคุกคามจากแฮกเกอร์ และไวรัสคอมพิวเตอร์
4) *ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์* หมายถึง ความเสี่ยงที่เกิดจากโปรแกรมระบบงานที่ได้จัดทำและพัฒนาขึ้น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดจากการเขียนโปรแกรม โปรแกรมมีจุดอ่อนหรือช่องโหว่จนทำให้ผู้บุรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่งหรือทำลายระบบได้
5) *ความเสี่ยงด้านระบบเครือข่าย* หมายถึง ความเสี่ยงที่จากการบุกรุกระบบเครือข่ายหรือภัยต่างๆ ที่เกิดขึ้นกับระบบเครือข่ายขององค์กรจนทำให้การสื่อสารข้อมูลระหว่างต้นทางกับปลายทางเกิดการผิดพลาดขึ้น หรือทำให้ไม่สามารถสื่อสารข้อมูลภายในระบบเครือข่ายได้
6) *ความเสี่ยงด้านข้อมูล* หมายถึง ความเสี่ยงที่จากฐานข้อมูลในระบบสารสนเทศได้รับความเสียหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุก การโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล

- **ระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ**

  (Information Security Management System – ISMS)
  - เป็นแนวทางการปรับปรุงองค์กรให้สามารถจัดการกับการเกิดปัญหาด้านความมั่นคงปลอดภัยได้
  - เป็นการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบ โดยมุ่งเน้นส่วนที่เกิดความเสี่ยงสูง
  - ลดความเสี่ยงจากการถูกฟ้องร้อง เนื่องจกการละเลยต่อการปฏิบัติตามกฎหมาย

- **การตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit)**

  หมายถึง กระบวนการรวบรวมหลักฐานและประเมินหลักฐาน เพื่อแสดงความเห็นเกี่ยวกับความถูกต้องเชื่อถือได้ การรักษาความปลอดภัย การปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผลตามวัตถุประสงค์ที่กำหนดไว้

- **หน้าที่ของผู้ตรวจสอบเทคโนโลยีสารสนเทศ (IT Auditor)**

  ผู้ตรวจสอบเทคโนโลยีสารสนเทศ มีหน้าที่ในการประเมินและแสดงความเห็นว่า ระบบการควบคุมที่ได้ถูกกำหนดไว้ มีความเพียงพอ มีการปฏิบัติตาม และได้ผลตามวัตถุประสงค์ที่กำหนดไว้หรือไม่ และรายงานจุดอ่อนของการควบคุมที่มีสาระสำคัญ รวมทั้งการให้ข้อเสนอแนะในการปรับปรุงแก้ไข

- **การควบคุมเทคโนโลยีสารสนเทศ** แบ่งออกเป็น 2 ส่วน คือ
  1) การควบคุมทั่วไป (General Control)
  2) การควบคุมระบบงาน (Application Control)

- **การควบคุมทั่วไป (General Control)**

หมายถึง การควบคุมในส่วนที่เกี่ยวกับ สภาพแวดล้อมของการควบคุม นโยบายและวิธีการในการควบคุม การควบคุมความปลอดภัย การควบคุมการพัฒนาและปรับปรุงระบบ และการป้องกัน/ลดความเสียหายของระบบ ซึ่งเป็นการควบคุมภายในสำหรับองค์กรในภาพรวมหรือควรมีในทุกๆ ส่วนของเทคโนโลยีสารสนเทศ

1) *การกำหนดนโยบายในการใช้เทคโนโลยีสารสนเทศ* ควรมีการกำนหดนโยบายที่ชัดเจนว่า ใครบ้างที่สามารถเข้าถึงข้อมูลอะไร ในระบบงานใด และเมื่อใด ใช้หลัก “need to know” ในการให้สิทธิเข้าถึงข้อมูล นั่นคือ บุคคลใดที่ไม่มีหน้าที่ต้องใช้ข้อมูลนั้น บุคคลนั้นก็ไม่มีสิทธิเข้าถึงข้อมูลนั้น
2) *การแบ่งแยกหน้าที่งานในระบบสารสนเทศ* ต้องกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานแต่ละคนให้ชัดเจน แยกหน้าที่การพัฒนาระบบออกจากหน้าที่ผู้ปฏิบัติการคอมพิวเตอร์
3) *การควบคุมโครงการพัฒนาระบบสารสนเทศ* ต้องมีแผนแม่บทระยะยาว แผนงานพัฒนาระบบ กำหนดการประมวลผลข้อมูล มอบหมายหน้าที่ความรับผิดชอบ ประเมินผลงานระหว่างการดำเนินโครงการ สอบทานภายหลังการติดตั้งระบบและนำระบบมาใช้งาน การวัดผลการดำเนินงาน
4) *การควบคุมการเปลี่ยนแปลงแก้ไขระบบ* โดยกำหนดระเบียบวิธีปฏิบัติในการแก้ไขระบบเป็นลายลักษณ์อักษร มีการศึกษาถึงผลกระทบ มีการทดสอบระบบก่อนนำไปใช้ จัดทำเอกสารคู่มือประกอบการแก้ไข ประเมินผลและสอบทานระบบภายหลังใช้งานแล้ว
5) *การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์* โดยควบคุมการประมวลผลข้อมูลของระบบงานต่างๆ การสำรองข้อมูล การจัดการกับปัญหาของระบบ
6) *การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์* กำหนดสถานที่จัดวางที่ปลอดภัย มีการรักษาความปลอดภัย ควบคุมการเข้า-ออก กำหนดนโยบายรักษาความปลอดภัยที่ชัดเจนเป็นลายลักษณ์อักษร ติดตั้งระบบเตือนภัยกรณีมีผู้บุกรุก จำกัดให้ใช้โทรศัพท์เฉพาะเรื่องที่เกี่ยวกับงานเท่านั้น ติดตั้งอุปกรณ์ป้องกัน และควบคุมสภาพแวดล้อมในการทำงาน
7) *การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ* ด้วยการกำหนดให้ผู้ใช้แต่ละระดับมองเห็นมุมมองของข้อมูลแตกต่างกัน กำหนดสิทธิในการเข้าถึงฐานข้อมูล การเข้ารหัสข้อมูล การควบคุมการนำข้อมูลไปใช้
8) *การควบคุมการเข้าถึงระบบงาน* ด้วยการพิสูจน์ตัวจริง (authentication) ใช้รหัสผ่าน การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ การกำหนดสิทธิ และการบันทึกกิจกรรมต่างๆ ในระบบเพื่อการตรวจสอบภายหลัง
9) *การควบคุมการจัดเก็บข้อมูล* ด้วยการระบุประเภทของข้อมูล กำหนดระดับของการป้องกันที่จำเป็น ควบคุมสถานที่จัดเก็บข้อมูลให้เหมาะสม ติดตั้งอุปกรณ์ป้องกันอัคคีภัย ฝุ่น ความร้อน และความชื้น
10) *การควบคุมการสื่อสารข้อมูล* เพื่อลดข้อผิดพลาดระหว่างการสื่อสารข้อมูล เช่น การเข้ารหัสข้อมูล การติดตั้งกระบวนการพิสูจน์เส้นทางการส่งข้อมูล การเพิ่มข้อมูลพิเศษระหว่างจัดส่ง การใช้เทคนิคส่งข้อความตอบกลับ

- **การควบคุมระบบงาน (Application Control)**

  เป็นการควบคุมเพื่อให้มั่นใจในความครบถ้วน สมบูรณ์ ถูกต้อง ของรายการทั้งหมดที่นำเข้าสู่การประมวลผล การได้รับอนุญาตและเกิดขึ้นอย่างถูกต้องตามกฎหมาย ระเบียบและนโยบาย ความถูกต้องของการประมวลผล และการแสดงผลลัพธ์ การควบคุมนี้ต้องเริ่มดำเนินการตั้งแต่ขั้นตอนการออกแบบระบบ ไม่ควรควบคุมภายหลังจากที่ระบบได้รับการออกแบบหรือถูกใช้งานแล้ว

  โดยแบ่งการควบคุมระบบงาน ออกเป็น 4 ประเภท ดังนี้

  1) *การควบคุมข้อมูลเบื้องต้น* ได้แก่
     a. *การพิสูจน์การป้อนข้อมูล* โดยกำหนดให้พนักงานมากกว่า 1 คน ป้อนข้อมูลที่สำคัญซ้ำกัน แล้วนำมาเปรียบเทียบกันว่าตรงกันหรือไม่
     b. *การใช้ตัวเลขตรวจสอบ* โดยกำหนดตัวเลขสำหรับใช้ตรวจสอบความถูกต้องไว้ที่หลักแรกหรือหลักสุดท้ายของข้อมูลที่สำคัญ เช่น เลขประจำตัว เลขที่บัญชี รหัสสินค้า เพื่อช่วยป้องกันความผิดพลาดในการบันทึกข้อมูล
  2) *โปรแกรมตรวจสอบความถูกต้องของข้อมูลนำเข้า* ใช้ตรวจสอบความสมเหตุสมผลและความถูกต้องของข้อมูลนำเข้า เช่น การตรวจสอบฟิลด์ที่ขาดข้อมูล (missing data check) การตรวจสอบเครื่องหมาย (sign check) การตรวจสอบความถูกต้อง (validity check) การตรวจสอบขีดจำกัด (limit check) การตรวจสอบโดยใช้ข้อมูลมากกว่าหนึ่งฟิลด์ (redundant data check) การตรวจสอบการเรียงลำดับ (sequence check) การตรวจสอบชนิดของฟิลด์ (field type check) การทดสอบความสมเหตุสมผล เช่น อัตราค่าแรงที่นำเข้ากับตำแหน่งงาน เป็นต้น
  3) *การควบคุมการประมวลผลข้อมูลและการเก็บรักษาแฟ้มข้อมูล* เช่น การตรวจสอบความเป็นปัจจุบันของข้อมูล การกำหนดค่าเริ่มต้น การจับคู่ข้อมูล การแสดงรายงานเมื่อพบสิ่งผิดปกติ การกระทบยอดรวม การกระทบยอดบัญชีคุม
  4) *การควบคุมผลลัพธ์* เพื่อป้องกันไม่ให้เกิดการสูญหายของข้อมูลผลลัพธ์ การป้องกันไม่ให้ผู้อื่นเห็นข้อมูลที่เป็นความลับ การกำจัดรายงานที่ไม่ใช้แล้วโดยใช้เครื่องย่อยทำลาย การกรองข้อมูลให้เหมาะสมก่อนส่งให้ผู้ใช้ การส่งข้อมูลให้กับผู้รับที่มีสิทธิถูกต้อง ผู้ใช้ต้องรับผิดชอบต่อความถูกต้องของข้อมูลในรายงานต่างๆ

- **การตรวจสอบการควบคุมระบบงานคอมพิวเตอร์**

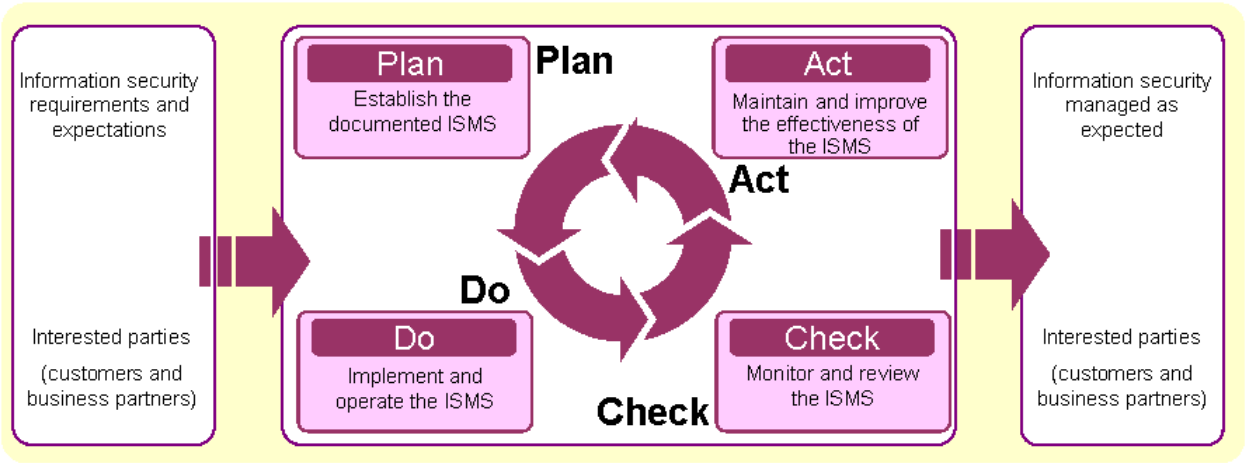
  แบ่งออกเป็น 2 วิธี ได้แก่

  1) *การตรวจสอบนอกระบบ (Audit around the computer)* หรือ *Black Box approach* วิธีนี้ผู้ตรวจสอบจะนำเอกสารเบื้องต้นมาประมวลผลด้วยมือ แล้วนำมาเปรียบเทียบกับผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ โดยไม่สนใจว่าระบบคอมพิวเตอร์จะทำการประมวลผลเช่นใด วิธีนี้เหมาะกับการตรวจสอบรายการที่ไม่ซับซ้อน

2) *การตรวจสอบผ่านระบบ (Audit through the computer)* หรือ *White Box approach* วิธีนี้ต้องใช้คอมพิวเตอร์ช่วยในการตรวจสอบ ผู้ตรวจสอบต้องเข้าใจตรรกะที่อยู่ภายในโปรแกรมประมวลผล เพื่อทำการตรวจสอบว่า

- ผู้ใช้เป็นบุคคลที่มีสิทธิในการใช้งานที่แท้จริงหรือไม่
- ตรวจสอบความครบถ้วนสมบูรณ์ของรายการต่างๆ
- ตรวจสอบว่ามีข้อมูลใดได้รับการประมวลผลซ้ำหรือไม่
- ตรวจสอบการเข้าถึงระบบ
- ตรวจสอบว่าระบบมีการเก็บบันทึกร่องรอยการตรวจสอบไว้ครบถ้วนหรือไม่
- ตรวจสอบการปัดเศษว่าเป็นไปตามหลักเกณฑ์ที่กำหนดหรือไม่

- **กระบวนการตรวจสอบระบบงานด้าน IT ด้วย PDCA Cycle Process**



Plan : การวางแผน

โดยกำหนดขอบเขตของการตรวจสอบ กำหนดนโยบายการตรวจสอบ กำหนดวิธีการประเมินความเสี่ยง ระบุความเสี่ยง ประเมินความเสี่ยง วิเคราะห์แนวทางในการแก้ปัญหาความเสี่ยง กำหนดวัตถุประสงค์ในการควบคุมและมาตรการในการควบคุม และจัดทำรายงานแนวทางการนำมาประยุกต์ใช้งาน

Do : การลงมือทำ

โดยกำหนดแผนการกำจัดความเสี่ยง ปฏิบัติตามแผนลดความเสี่ยง ติดตั้งระบบควบคุม ฝึกอบรมพนักงานเพื่อให้เกิดความรู้ ความเข้าใจ และความตระหนัก บริหารการปฏิบัติการ บริหารทรัพยากร กำหนดขั้นตอนการปฏิบัติเพื่อตรวจจับและตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย

Check : การตรวจสอบ

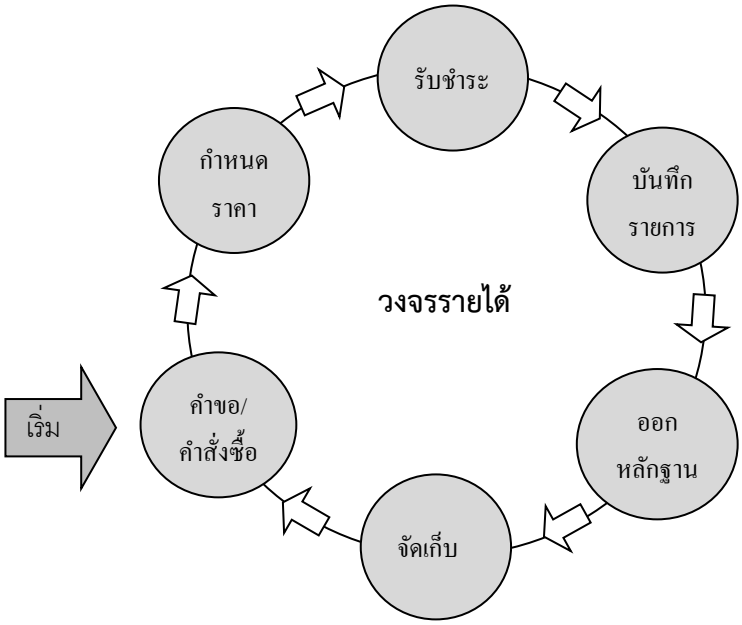
โดยปฏิบัติตามขั้นตอนการเฝ้าระวัง ตรวจพิจารณาว่ามาตรการควบคุมมีประสิทธิภาพเพียงพอหรือไม่ ตรวจพิจารณาว่าความเสี่ยงยังอยู่ในระดับที่ยอมรับได้หรือไม่ ตรวจสอบมาตรการควบคุมภายใน ตรวจสอบพิจารณาการบริหารงานปกติของมาตรการควบคุม บันทึกการปฏิบัติและเหตุการณ์ที่มีผลกระทบต่อมาตรการควบคุม

Act : การปรับปรุงแก้ไข

โดยปรับปรุงส่วนที่มีปัญหา แก้ไขปัญหาที่เกิดขึ้น และป้องกันไม่ให้เกิดขึ้นอีก ประยุกต์ใช้เกี่ยวกับองค์ความรู้ที่ได้รับ เผยแพร่องค์ความรู้ที่ได้รับให้กับผู้ที่เกี่ยวข้องทราบ ทำให้แน่ใจว่าการปรับปรุงระบบนั้นบรรลุวัตถุประสงค์ที่ตั้งไว้

Case Study

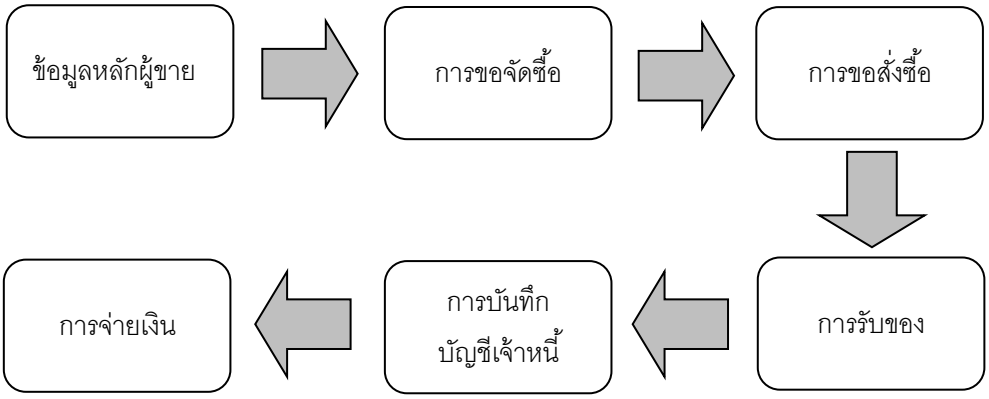
- **การควบคุมวงจรรายได้**



แนวทางการควบคุมวงจรรายได้

ขั้นตอน	วัตถุประสงค์การควบคุม	วิธีการควบคุม
รับคำขอ/คำสั่งซื้อ (input)	● ความเป็นจริงของรายการ ● ความครบถ้วนของรายการ	● ให้เลขที่ลำดับคำขอ ● ควบคุมจำนวนรายการที่รับเข้า
การกำหนด/คำนวณราคา	● ความถูกต้องของราคาตามอัตราที่กำหนดไว้	● กำหนดตารางราคาในระบบหรือหน่วยงานกำหนดราคา
รับชำระ	● ครบถ้วนและถูกต้อง	● ออกใบรับ
การบันทึกรายการ	● ครบถ้วนและถูกต้อง	● ระบบบันทึก ● รายงานประจำวัน
ออกหลักฐาน	● เป็นจริง ถูกต้อง ครบถ้วน	● Pre-number
จัดเก็บ	● ความครบถ้วน	● จำกัดผู้รับผิดชอบ ● ตรวจนับ

- **การควบคุมวงจรรายจ่าย**



แนวทาง<u>การควบคุมทั่วไป</u>ของวงจรรายจ่าย

ขั้นตอน	วัตถุประสงค์การควบคุม	วิธีการควบคุม
การแบ่งแยกหน้าที่อย่างเหมาะสม	ผู้ปฏิบัติงานได้รับสิทธิเหมาะสมตามงานที่ได้รับมอบหมาย	มีการแบ่งแยกหน้าที่ความรับผิดชอบระหว่างหน่วยงานจัดหา หน่วยงานจัดซื้อ หน่วยงานรับพัสดุ หน่วยงานการเงิน และหน่วยงานบัญชี
การเข้าถึงข้อมูลหลักผู้ขาย	การเข้าถึงกระบวนการหรือข้อมูลของวงจรรายจ่ายถูกจำกัดไว้เฉพาะผู้เกี่ยวข้องที่ได้รับสิทธิเท่านั้น	มีการกำหนดสิทธิของผู้ปฏิบัติงานในระบบอย่างเหมาะสม ตามอำนาจหน้าที่
	การขอสร้างหรือขอเปลี่ยนแปลงข้อมูลหลักผู้ขายต้องได้รับอนุมัติและมีการนำเข้าอย่างครบถ้วน ถูกต้อง และไม่ซ้ำซ้อน	- การขอสร้าง ลบ หรือเปลี่ยนแปลงข้อมูลหลัก ต้องกรอกแบบฟอร์มขอเปลี่ยนแปลง และได้รับอนุมัติอย่างครบถ้วนสมบูรณ์ - การขอเปลี่ยนแปลงข้อมูลหลักมีการบันทึก จัดเก็บ และตรวจสอบความสมเหตุสมผล - มีการสอบทานข้อมูลอย่างสม่ำเสมอ
การจัดทำระเบียบปฏิบัติ	การจัดซื้อจัดหามีการควบคุม และเป็นมาตรฐานเดียวกัน	มีการจัดทำระเบียบปฏิบัติงาน โดยมีเนื้อหาครอบคลุมเรื่องต่างๆ ดังนี้ - นโยบายการจัดซื้อ ผู้มีอำนาจอนุมัติ - วิธีคัดเลือกผู้ขาย - การทำสัญญา - การประเมินผู้ขาย - ขั้นตอนการจัดหา - ขั้นตอนการตรวจรับ

แนวทาง<u>การควบคุมเฉพาะ</u>ของวงจรรายจ่าย

ขั้นตอน	วัตถุประสงค์การควบคุม	วิธีการควบคุม
การควบคุมการจัดซื้อจัดหา	- การขอจัดซื้อจัดหาปฏิบัติตามกฎระเบียบอย่างเคร่งครัด - การซื้อสินค้าและบริการได้รับการอนุมัติอย่างถูกต้อง	- มีการทำเอกสารอย่างเป็นทางการโดยระบุรายละเอียดอย่างครบถ้วน ชัดเจน และผ่านการอนุมัติอย่างถูกต้อง - กำหนดจุดสั่งซื้อ (reorder point) และแจ้งจัดซื้อเมื่อถึงจุดที่กำหนด - ตรวจสอบรายการวัสดุคงคลังก่อนแจ้งจัดหา เพื่อรักษาระดับสินค้าในคลังให้มีปริมาณที่พอเหมาะ (safety stock) - ปฏิบัติตามขั้นตอนการคัดเลือกผู้ขายที่ดีที่สุด ตามที่ระบุในกฎระเบียบปฏิบัติ - มีการแบ่งแยกหน้าที่ของผู้จัดหาและผู้ตรวจรับออกจากกัน - จัดทำทะเบียนประวัติผู้ขาย รวมถึงราคาและปริมาณของที่สั่งซื้อ
การควบคุมการสั่งซื้อ	- การสั่งซื้อได้ปฏิบัติตามกฎระเบียบอย่างเคร่งครัด - การสั่งซื้อสินค้าและบริการได้รับการอนุมัติอย่างถูกต้องและตรงกับใบขอจัดซื้อ	- มีการทำเอกสารอย่างเป็นทางการโดยระบุรายละเอียดอย่างครบถ้วน ชัดเจน และผ่านการอนุมัติอย่างถูกต้อง - ใบสั่งซื้อควรมีข้อมูลครบถ้วนและมีเลขที่เรียงลำดับพิมพ์ไว้ล่วงหน้า - มีการเช็คซ้ำว่าใบสั่งซื้อได้ถูกส่งไปยังผู้ค้าที่ถูกคัดเลือกไว้อย่างถูกต้อง
การควบคุมการรับของ	สินค้าหรือบริการที่รับถูกต้อง ครบถ้วน ตรงกับที่สั่งซื้อและคุณภาพได้มาตรฐาน	- ผู้รับสินค้าตรวจนับและตรวจเช็คสินค้าเทียบกับรายการในใบส่งของและใบสั่งซื้อ (3-way matching) - กำหนดผู้มีอำนาจในการตรวจรับและควรลงนามผู้ตรวจรับร่วมกันอย่างน้อย 2 คน - จัดทำรายงานสิ่งที่ผิดปกติ เช่น สินค้าไม่ครบ เสียหาย หรือไม่ได้คุณภาพ - ควรมีเอกสารลดหนี้จากผู้ขายเมื่อมีการคืนสินค้า

แนวทางการควบคุมเฉพาะของวงจรรายจ่าย *(ต่อ)*

ขั้นตอน	วัตถุประสงค์การควบคุม	วิธีการควบคุม
การควบคุมการบันทึกบัญชีเจ้าหนี้	มีการบันทึกบัญชีอย่างถูกต้อง ครบถ้วน และทันกาล	- มีการบันทึกบัญชีอย่างทันกาลและได้รับอนุมัติอย่างถูกต้อง หลังจากที่ตรวจรับและตรวจสอบเอกสารเรียบร้อยแล้ว - เจ้าหน้าที่บัญชีตรวจสอบความครบถ้วนถูกต้องของตัวเลขในปัญชีฝั่งเจ้าหนี้ก่อนจะทำการยืนยันในระบบ
การควบคุมการจ่ายเงิน	ชำระหนี้ไปยังผู้ขายอย่างถูกต้อง ครบถ้วน และทันกาล	- มีการตรวจสอบและอนุมัติการชำระหนี้ - ชำระหนี้ตามกำหนดเวลาและเงื่อนไขของผู้ขาย - ใบสำคัญที่ชำระเงินแล้วจะต้องมีการทำเครื่องหมายเพื่อป้องกันการจ่ายซ้ำ - เก็บเอกสารหลักฐานการทำจ่ายเพื่อเป็นหลักฐานและเพื่อการตรวจสอบ

5. ข้อเสนอแนะ

บุคลากรที่มีหน้าที่ให้ความรู้หรือปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสาร ควรได้รับการฝึกอบรมในหลักสูตรที่เกี่ยวข้องกับการปฏิบัติงานอย่างสม่ำเสมอ เนื่องจากเทคโนโลยีสารสนเทศและการสื่อสารเปลี่ยนแปลงไปอย่างรวดเร็วตลอดเวลา