บันทึกข้อความ

ส่วนราชการ ฝ่ายตรวจสอบ ๒ กลุ่มตรวจสอบภายใน โทร. ๐๒-๕๙๐๔๑๐๐๒ โทรสาร. ๐๒-๕๙๐๔๑๐๐๑
ที่ สธ ๐๙๒๕.๐๓/ ~ **วันที่** ๑๐ กันยายน ๒๕๖๐
เรื่อง รายงานการอบรมหลักสูตรประกาศนียบัตรผู้ตรวจสอบภายในภาครัฐ (CGIA) หลักสูตร Intermediate ด้าน Information Technology

เรียน ผู้อำนวยการกลุ่มตรวจสอบภายใน (ผ่านหัวหน้าฝ่ายตรวจสอบ ๒)

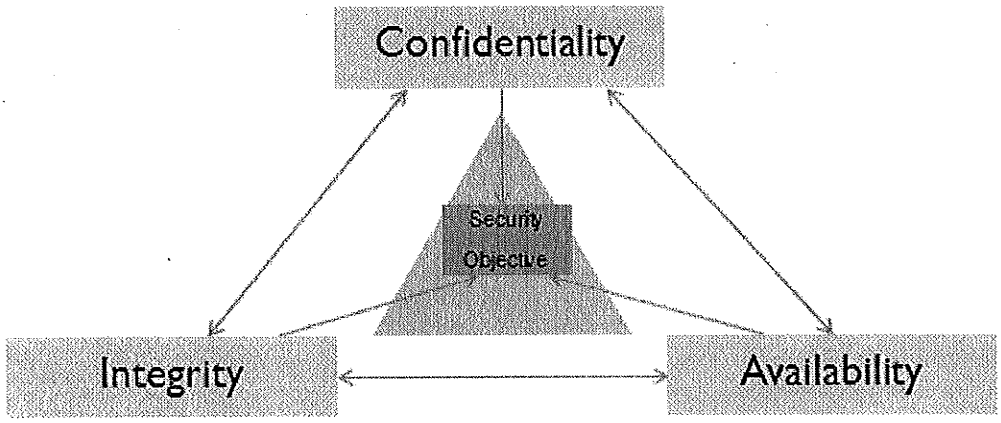
ตามที่ได้เข้ารับการอบรมโครงการอบรมหลักสูตรประกาศนียบัตรผู้ตรวจสอบภายในภาครัฐ (CGIA) หลักสูตร Intermediate ด้าน Information Technology ระหว่างวันที่ ๓๐ มกราคม – ๙ กุมภาพันธ์ ๒๕๖๐ นั้น สรุปผลการอบรมได้ดังนี้

๑. การปฏิบัติการระบบสารสนเทศ (Information System Operation)

ปัจจุบันทุกองค์กรนำระบบสารสนเทศเข้ามาช่วยเพิ่มประสิทธิภาพการดำเนินงานให้กับองค์กร ระบบสารสนเทศถูกเชื่อมต่อภายนอกองค์กรด้วยเครือข่าย Internet ทำให้องค์กรเกิดความไม่มั่นคงปลอดภัย มีความเสี่ยงจากการถูกคุกคาม ถูกบุกรุก และถูกโจมตีจากแฮกเกอร์และไวรัสคอมพิวเตอร์ องค์กรควรมีมาตรการป้องกันความเสี่ยงที่เป็นมาตรฐานสากลมาประยุกต์ใช้เพื่อจัดการความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดเป็นนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

ความมั่นคงปลอดภัยของสารสนเทศนั้นมีองค์ประกอบด้วยกัน ๓ ประการ คือ ความลับ (Confidentiality) ความถูกต้องสมบูรณ์(Integrity) และความพร้อมใช้งาน (Availability) หรือเรียกว่า C-I-A

ทรัพย์สิน (Asset) ที่มีความมั่นคงปลอดภัยนั้นต้องประกอบด้วยองค์ประกอบทั้งสามอย่างครบถ้วน ไม่ว่าทรัพย์สินนั้นจะเป็นสิ่งที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย หรือทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูล เป็นต้น



- ความลับ (Confidentiality)

การรักษาความลับให้กับข้อมูลเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ หลักการสำคัญของการรักษาความลับคือ ผู้ที่มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ภาคธุรกิจให้ความสำคัญกับการรักษาความลับทางธุรกิจ ประชาชนทั่วไปก็ต้องการปกป้องข้อมูลส่วนตัวตามสิทธิขั้นพื้นฐานเช่นเดียวกัน

๒/...

ระบบรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีประสิทธิภาพ ต้องมีมาตรการตรวจสอบสิทธิก่อนเข้าถึง เพื่อยืนยันให้แน่ใจก่อนว่าผู้ที่ร้องขอนั้นมีสิทธิหรือได้รับอนุญาตให้เข้าถึงสารสนเทศ หรือระบบงานนั้นได้ กลไกพื้นฐานที่คุ้นเคยกันเป็นอย่างดี คือการใช้รหัสผ่าน(Password) ในการพิสูจน์ตัวตนและสิทธิที่ได้รับอนุญาต นอกจากมาตรการตรวจสอบสิทธิแล้วการกำหนดชั้นความลับเป็นระดับต่างๆ ตามความสำคัญช่วยให้บริหารจัดการมีประสิทธิภาพมากขึ้น มาตรการทางเทคนิคที่ใช้ในการปกป้องความลับ เช่น การเข้ารหัส (Encryption) อาจถูกนำมาใช้เสริมความแข็งแกร่งให้กับมาตรการปกป้องสารสนเทศที่ต้องการมาตรการดูแลอย่างเข้มงวด

- ความถูกต้องสมบูรณ์ (Integrity)

การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ (Integrity) เป็นสิ่งสำคัญส่งผลถึงความน่าเชื่อถือของสารสนเทศนั้นๆ ทำอย่างไรให้ข้อมูลมีความถูกต้องและน่าเชื่อถือเป็นสิ่งที่ผู้ดูแลระบบต้องหาคำตอบและดำเนินการให้เกิดขึ้น คำตอบในเชิงหลักการคือระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใดๆ ต่อข้อมูลนั้น

- ความพร้อมใช้งาน (Availability)

การทำให้ระบบตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ อุปสรรคที่บั่นทอนความพร้อมใช้งานของระบบคอมพิวเตอร์จำแนกได้ ๒ แบบ คือ

- การที่ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service)
- ระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of data processing capability)

ปัจจัยการเกิดความเสี่ยงต่อความไม่มั่นคงปลอดภัยสารสนเทศ

- People Risk เป็นความเสี่ยงที่เกิดจากตัวบุคคลทั้งที่เป็นบุคลากรภายในองค์กรและบุคคลจากภายนอกองค์กร
- Process Risk เป็นความเสี่ยงที่เกิดจากการที่องค์กรไม่ได้ดำเนินการจัดทำขั้นตอนปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือขาดวิธีการควบคุมที่รัดกุมเพียงพอ หรือการละเลยไม่ปฏิบัติตาม
- Technology Risk เป็นความเสี่ยงที่เกิดจากการที่องค์กรควบคุมการทำงานระบบเทคโนโลยีสารสนเทศไม่ดีพอ ทำให้เกิดช่องโหว่ให้ผู้ไม่ประสงค์ดีเข้ามาคุกคามสร้างความเสียหายแก่องค์กรได้

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ได้ทราบบทบาทหน้าที่ ความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ ซึ่งหน่วยงานของรัฐต้องถือปฏิบัติ ดังนี้

๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
๒) การจัดให้มีระบบสารสนเทศและระบบสำรอง และจัดทำแผนเตรียมพร้อมสำหรับกรณีฉุกเฉิน
๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

การควบคุมความปลอดภัย

- การควบคุมความปลอดภัยด้านกายภาพ (สิ่งที่จับต้องได้) เช่น บัตรเข้าออก ประตูปิด-เปิด การจำกัดพื้นที่การใช้งานเฉพาะบุคคล รปภ. คล้องโซ่และกุญแจ ระบบโทรทัศน์วงจรปิด
- การควบคุมทางด้านตรรกะ (Logical Control) เป็นการควบคุมด้วยการเข้ารหัส โดยมีหลักเกณฑ์คือ รหัสผ่านต้องมีการกำหนดความยาวที่เหมาะสม ไม่กำหนดรหัสผ่านโดยใช้คำที่มีการคาดเดาได้ง่าย

๓/...

- การควบคุมด้านการบริหารจัดการ (Administration Control) เกี่ยวกับนโยบายและขั้นตอนปฏิบัติด้านสารสนเทศ การอบรมให้ตระหนักถึงความปลอดภัยในระบบ และการตรวจสอบ มีระบบการแจ้งเตือนและประเมินผลประสิทธิภาพสม่ำเสมอ

๒. การใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

Computer – Assisted Audit Tools and Techniques – CAATTs

- ***ก่อนการนำเทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ***

การควบคุมระบบงานคอมพิวเตอร์ (Computer Application Control) จำแนกได้ ๓ องค์ประกอบ คือ

๑.๑ การควบคุมข้อมูลนำเข้า (Input Control) เพื่อให้แน่ใจว่าข้อมูลของรายการที่ต้องการประมวลผลได้รับการบันทึกอย่างถูกต้องครบถ้วน และข้อมูลที่ผิดพลาดได้รับการตรวจพบและแก้ไขให้ถูกต้องก่อนส่งกลับเข้าประมวลผล ประเภทของการควบคุมข้อมูลนำเข้า

- การควบคุมเอกสารเบื้องต้น
- การควบคุมการแปลงข้อมูล
- การควบคุม Batch
- การควบคุมความถูกต้อง
- การแก้ไขข้อผิดพลาด

๑.๒ การควบคุมการประมวลผล (Processing Control) เพื่อให้แน่ใจว่ารายการต่างๆ ไม่สูญหายไปในระหว่างที่ทำการประมวลผล

- การใช้ยอดรวมของค่า Batch ต่างๆ มาทำการกระทบยอดในแต่ละการประมวลผล (Run-to-Run Controls)

- ลดการแทรกแซงการทำงานของระบบด้วยบุคคลให้น้อยที่สุดเพื่อลดโอกาสที่จะเกิดข้อผิดพลาดในระบบ (operator Intervention Controls)

- การเก็บร่องรอยการตรวจสอบต่างๆ (Log) ไว้เพื่อเป็นประโยชน์สำหรับกาตรวจสอบ

๑.๓ การควบคุมข้อมูลส่งออก (Output Control) เพื่อป้องกันไม่ให้เกิดการสูญหายของข้อมูลส่งออก

- การควบคุมข้อมูลส่งออกแบบ Batch
- การควบคุมข้อมูลส่งออกแบบ Real-time

- การตรวจสอบการควบคุมระบบงานคอมพิวเตอร์

- การตรวจสอบนอกระบบ (Audit around the computer) หรือ Black Box Approach คือ การตรวจสอบโดยไม่สนใจว่าระบบคอมพิวเตอร์จะทำการประมวลผลเช่นใด ผู้ตรวจสอบจะนำเอกสารเบื้องต้นมาประมวลผลด้วยมือแล้วนำมาเปรียบเทียบกับผลที่ได้จากระบบคอมพิวเตอร์ เหมาะสมกับการตรวจสอบรายการที่ไม่ซับซ้อน

- การตรวจสอบผ่านระบบ (Audit through the computer) หรือ White Box Approach ต้องมีการใช้เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ (Computer-Aided Auditing Tools & Techniques or Computer Assisted Audit Techniques : CAATs) คือ การตรวจสอบ ดังนี้

- ตรวจสอบผู้ใช้เป็นบุคคลที่มีสิทธิ์ในการทำงานกับโปรแกรมที่แท้จริง
- ตรวจสอบ Application controls

๔/...

- ตรวจสอบความครบถ้วนสมบูรณ์ของรายการต่างๆ
- ตรวจสอบว่ามีข้อมูลใดๆ ได้รับการประมวลผลซ้ำหรือไม่
- ตรวจสอบการเข้าถึงระบบ
- ตรวจสอบว่าระบบได้มีการเก็บร่องรอยการตรวจสอบครบถ้วนหรือไม่
- ตรวจสอบการปัดเศษว่าเป็นไปตามหลักเกณฑ์ที่กำหนดหรือไม่

- เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ (Computer Assisted Audit Techniques : CAATs)

หมายถึง การนำเทคโนโลยีทางคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟท์แวร์และระบบการจัดการฐานข้อมูลมาช่วยในการตรวจสอบ ที่นิยมอย่างแพร่หลาย ได้แก่

๓.๑ การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป (Generalized Audit Software : GAS) เกิดจากการนำระบบคอมพิวเตอร์มาใช้งานมากขึ้น ปัญหาความหลากหลายของชนิดซอฟท์แวร์ ฮาร์ดแวร์ที่ผู้รับการตรวจใช้ ซึ่งผู้ตรวจสอบภายในจำเป็นต้องดึงข้อมูลที่จัดเก็บมาตรวจสอบ

๓.๒ การใช้ข้อมูลทดสอบ คือ การที่ผู้ตรวจสอบใช้ข้อมูลรายการที่เป็นตัวอย่างชุดหนึ่ง (Sample of Transactions) ที่ผู้ตรวจสอบจัดทำขึ้นมาเพื่อตรวจสอบโปรแกรมที่ใช้งานอยู่ว่ามีการประมวลผลถูกต้องและมีจุดควบคุมต่างๆ ตามที่ระบุไว้หรือไม่

ประโยชน์ของการใช้คอมพิวเตอร์เพื่อช่วยในการตรวจสอบ

- ทำให้เห็นภาพรวมของระบบและการเคลื่อนไหวของรายการ
- ช่วยในการจัดเก็บข้อมูล
- ช่วยให้การวิเคราะห์รายการที่ผิดปกติง่ายยิ่งขึ้น
- ผู้ตรวจสอบจำเป็นต้องใช้ CAATs ในการตรวจสอบระบบที่ใช้เทคโนโลยีสารสนเทศ
- ช่วยลดระดับความเสี่ยงซึ่งเกิดจากการตรวจสอบ
- ช่วยเพิ่มความเป็นอิสระจากผู้รับการตรวจสอบ
- สามารถเพิ่มขอบเขตการตรวจสอบให้ครอบคลุมมากยิ่งขึ้น
- ช่วยเพิ่มโอกาสในการประเมินและวิเคราะห์เชิงปริมาณเพื่อค้นหาจุดอ่อนของการควบคุม
- ช่วยเพิ่มประสิทธิผลในการตรวจสอบในกรณีการตรวจสอบสิ่งผิดปกติรายการทุจริต
- ลดค่าใช้จ่ายและระยะเวลาในการตรวจสอบ

๓. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

<u>ความจำเป็นในการตรากฎหมายธุรกรรมฯ</u>

หลักฐานที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ไม่สามารถนำมาเป็นหลักฐานได้ เพราะกฎหมายฉบับอื่นกำหนดให้ต้องทำในรูปของหนังสือ หลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง และมูลค่าจำนวนการทำธุรกรรมทางอิเล็กทรอนิกส์ มีแนวโน้มสูงขึ้นทุกปีประกอบกับสังคมไทยกำลังเป็นสังคมสารสนเทศเต็มรูปแบบ จึงนำไปสู่ปัญหาว่าจะป้องกันมิให้เกิดความเสี่ยงอันกระทบต่อความมั่นคงทางเศรษฐกิจหรือการทำธุรกรรมทางออนไลน์ได้อย่างไร

<u>ธุรกรรมทางอิเล็กทรอนิกส์</u>

หมายถึง ธุรกรรมที่กระทำขึ้น โดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

๕/...

ข้อมูลอิเล็กทรอนิกส์

หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

หลักเกณฑ์ในการเก็บรักษาข้อมูลอิเล็กทรอนิกส์ตามกฎหมายต้องการ คือ

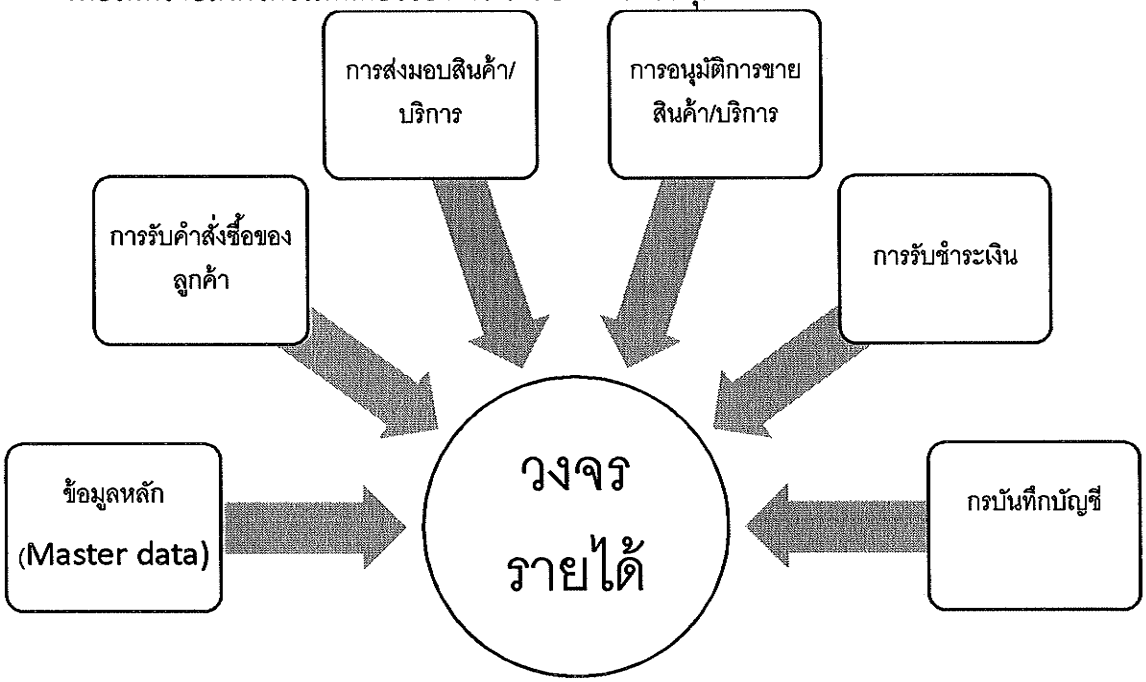
- ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง
- ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้น ให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์ หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับ ปรากฏอย่างถูกต้อง
- ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง และปลายทางของข้อมูลอิเล็กทรอนิกส์ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว

ลักษณะของลายมือชื่อลิเล็กทรอนิกส์ที่ถือว่าเชื่อถือได้

- ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้ภาพที่นำมาใช้
- ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ โดยไม่มีการควบคุมของบุคคลอื่น
- การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้
- ในกรณีกฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้น สามารถตรวจพบได้นับแต่เวลาที่ลายมือชื่ออิเล็กทรอนิกส์

๔. การตรวจสอบวงจรรายได้

เพื่อให้ทราบถึงกิจกรรมที่เกี่ยวข้อง ความเสี่ยง การควบคุมภายใน และวิธีการตรวจสอบวงจรรายได้



ความเสี่ยงของวงจรรายจ่ายแบ่งเป็น ๒ ชนิด ดังนี้

๑. ความเสี่ยงทั่วไป ได้แก่ การแบ่งแยกหน้าที่ความรับผิดชอบ การไม่มีการจัดระเบียบการปฏิบัติงาน การไม่มีการควบคุมการเข้าถึงข้อมูล

๒. ความเสี่ยงเฉพาะ ได้แก่ การทุจริตในการสั่งซื้อสินค้าหรือบริการ การซื้อสินค้าที่ไม่เหมาะสม การตรวจรับสินค้าไม่ตรงกับของที่สั่งซื้อ การทุจริตในการจ่ายเงินให้กับผู้ขาย

แนวทางการควบคุม

๑. การควบคุมทั่วไป

๑.๑ การแบ่งแยกหน้าที่อย่างเหมาะสม

๑.๒ การควบคุมการเข้าถึงข้อมูล

๑.๓ การจัดทำระเบียบการปฏิบัติงาน

๒. การควบคุมเฉพาะ

๒.๑ การควบคุมการจัดซื้อ-จัดหา

๒.๒ การควบคุมการสั่งซื้อ

๒.๓ การควบคุมการรับของ

๒.๔ การควบคุมการบันทึกบัญชีเจ้าหนี้

๒.๕ การควบคุมการจ่ายเงิน

กิจกรรมการควบคุม	จุดประสงค์การควบคุม	วิธีการควบคุม
๑. การควบคุมทั่วไป		
๑.๑ การแบ่งแยกหน้าที่อย่างเหมาะสม	๑. ผู้ปฏิบัติได้รับสิทธิ์เหมาะสมกับงานที่ได้รับมอบหมาย	๑. แบ่งแยกหน้าที่รับผิดชอบระหว่างหน่วยงาน ระหว่าง จัดหา-จัดซื้อ-ตรวจรับ-บัญชี
๑.๒ การควบคุมการเข้าถึงข้อมูล	๑. การเข้ากระบวนการหรือข้อมูลวงจรรายจ่ายจำกัดเฉพาะผู้เกี่ยวข้อง ๒. การขอสร้างหรือเปลี่ยนแปลงข้อมูลหลักผู้ขายต้องได้รับการอนุมัติ	๑. กำหนดสิทธิ์ผู้ปฏิบัติงานอย่างเหมาะสม ๒. การขอสร้างหรือเปลี่ยนแปลงข้อมูลหลักผู้ขายมีการกรอกแบบฟอร์มขอเปลี่ยนแปลง มีการบันทึกจัดเก็บและตรวจสอบตลอดจนสอบทานข้อมูลอย่างสม่ำเสมอ
๑.๓ การจัดทำระเบียบการปฏิบัติงาน	๑. การจัดซื้อ-จัดหามีการควบคุมและเป็นมาตรฐานเดียวกัน	๑. จัดทำระเบียบปฏิบัติงาน เมื่อจัดทำแล้วต้องประกาศให้ทุกคนรับทราบและถือปฏิบัติตาม
๒. การควบคุมเฉพาะ		
๒.๑ การควบคุมการจัดซื้อ-จัดหา	๑. การขอจัดซื้อ-จัดหาปฏิบัติตามระเบียบ ๒. การซื้อสินค้าและบริการได้รับการอนุมัติอย่างถูกต้อง	๑. จัดทำเอกสารอย่างเป็นทางการถูกต้องและผ่านการอนุมัติ ๒. กำหนดจุดสั่งซื้อ Reorder Point

๘/...

กิจกรรมการควบคุม	จุดประสงค์การควบคุม	วิธีการควบคุม
		๓. ตรวจสอบรายการวัสดุคงคลังก่อนแจ้งจัดหาเพื่อให้สินค้าคงคลังมีปริมาณที่เหมาะสม ๔. ปฏิบัติตามขั้นตอนการคัดเลือกผู้ค้าตามระเบียบ ๕. แบ่งแยกหน้าที่ของผู้จัดหากับผู้ตรวจรับ ๖. จัดทำทะเบียนประวัติผู้ขาย รวมทั้งราคาและปริมาณที่สั่งซื้อ
๒.๒ การควบคุมการสั่งซื้อ	๑. การสั่งซื้อปฏิบัติตามระเบียบ ๒. การสั่งซื้อสินค้าและบริการได้รับการอนุมัติอย่างถูกต้องและตรงกับใบขอซื้อ	๑. จัดทำเอกสารอย่างเป็นทางการถูกต้องและผ่านการอนุมัติ ๒. ใบสั่งซื้อควรมีเลขที่เรียงลำดับพิมพ์ไว้ล่วงหน้า ๓. มีการเช็คซ้ำว่าใบสั่งซื้อถูกส่งไปยังผู้ค้าที่ถูกคัดเลือกจริง
๒.๓ การควบคุมการรับของ	๑. สินค้าและบริการได้รับมาถูกต้องครบถ้วนตรงตามที่สั่งซื้อ และคุณภาพได้มาตรฐาน	๑. ผู้รับสินค้า ตรวจนับสินค้าเทียบกับใบส่งของและใบสั่งซื้อ (๓ Way Matching) ๒. มีผู้ลงนามตรวจรับร่วมกันอย่างน้อย ๒ คน ๓. ทำรายงานสิ่งผิดปกติ เช่น วัสดุหดหายเสียหาย ๔. ควรมีเอกสารลดหนี้จากผู้ขายเมื่อคืนสินค้า
๒.๔ การควบคุมการบันทึกบัญชีเจ้าหนี้	๑. มีการบันทึกบัญชีอย่างถูกต้อง ครบถ้วนและทันกาล	๑. มีการบันทึกบัญชีอย่างทันกาล ๒. เจ้าหน้าที่บัญชี ควรตรวจเช็คความครบถ้วนในบัญชีฝั่งเจ้าหนี้ก่อนยืนยันในระบบ
๒.๕ การควบคุมการจ่ายเงิน	๑. การชำระหนี้ไปยังผู้ขายถูกต้อง ครบถ้วน	๑. มีการตรวจสอบและอนุมัติการชำระหนี้ ๒. ชำระหนี้ตามกำหนดเวลาและเงื่อนไข ๓. ใบสำคัญที่ชำระแล้วต้องมีการทำเครื่องหมายป้องกันการจ่ายซ้ำ ๔. เก็บหลักฐานการจ่ายไว้เพื่อตรวจสอบ

จึงเรียนมาเพื่อโปรดทราบ และพิจารณาสั่งการต่อไป จะเป็นพระคุณ

(นางจรัญญา สะเริญรัมย์)
นักวิชาการตรวจสอบภายในปฏิบัติการ

เรียน ผู้อำนวยการกลุ่มตรวจสอบภายใน
เพื่อโปรดทราบ และพิจารณาสั่งการต่อไป จะเป็นพระคุณ

(นางสาวอรุณี มนปราณีต)
นักวิชาการตรวจสอบภายในชำนาญการ
หัวหน้าฝ่ายตรวจสอบ ๒

(นางสาวพิมพ์กวดี ศรีจันทร์)