สรุปการฝึกอบรม

โครงการอบรมหลักสูตรประกาศนียบัตรผู้ตรวจสอบภายในภาครัฐ (CGIA)

หลักสูตร Intermediate ด้าน Information Technology

วันที่ ๓๑ มกราคม - ๘ กุมภาพันธ์ ๒๕๖๒

ณ ห้องกษัตริย์ศึก ๑ ชั้น ๔ โรงแรมเดอะ ทวิน ทาวเวอร์

ถนนรองเมือง เขตปทุมวัน กรุงเทพฯ

****

วันที่ ๓๑ มกราคม ๒๕๖๒ : การใช้คอมพิวเตอร์ช่วยในการตรวจสอบ
(อ.มานิต พาณิชย์กุล)

วันที่ ๑ กุมภาพันธ์ ๒๕๖๒: การตรวจสอบวงจรรายได้ , การตรวจสอบวงจรรายจ่าย
(อ.สุรพงษ์ ชูรังสฤษฏ์, อ.รินทร์ วัฒกานนท์)

วันที่ ๔ กุมภาพันธ์ ๒๕๖๒: ระบบการปฏิบัติการ , การพัฒนาและดูแลระบบสารสนเทศ
(อ.ภิธันปดิ์ ถิรสัตยาพิทักษ์)

วันที่ ๕ กุมภาพันธ์ ๒๕๖๒: การรักษาความปลอดภัยของระบบสารสนเทศ
(อ.ภิธันปดิ์ ถิรสัตยาพิทักษ์)

วันที่ ๖ กุมภาพันธ์ ๒๕๖๒: ระบบจัดการฐานข้อมูล
(อ.ภิธันปดิ์ ถิรสัตยาพิทักษ์)

วันที่ ๗ กุมภาพันธ์ ๒๕๖๒: ระบบการสื่อสารข้อมูล, พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔
(อ.ภิธันปดิ์ ถิรสัตยาพิทักษ์)

วันที่ ๘ กุมภาพันธ์ ๒๕๖๒: ความรู้เกี่ยวกับกฎหมายด้านการพิทักษ์สิทธิของบุคคล
(อ.ภิธันปดิ์ ถิรสัตยาพิทักษ์)

<u>การใช้คอมฯ ช่วยในการตรวจสอบ</u>

การใช้คอมพิวเตอร์ช่วยในการตรวจสอบ CAATs (Computer Assisted Audit Techniques) มี ๓ องค์ประกอบ ได้แก่

๑) การควบคุมข้อมูลนำเข้า (Input Control) เป็นการควบคุมแบบป้องกัน Prevention เป็นการควบคุมที่มีความสำคัญมากที่สุด ได้แก่

๑.๑ การควบคุมเอกสารเบื้องต้น เช่น ต้องมีเลขที่เอกสารที่พิมพ์ไว้ล่วงหน้า และเรียงเลขหน้า โดยแต่ละใบต้องมีการใช้งาน

๑.๒ การควบคุมข้อผิดพลาดจากการเปลี่ยนแปลงข้อมูลด้วยการเพิ่มตัวเลขอีกหนึ่งหลัก Check Digits ควรใช้กับข้อมูลที่สำคัญ ๆ เช่น Primary Key เนื่องจากใช้พื้นที่ในการจัดเก็บจำนวนมาก

๑.๓ การควบคุม Batch เพื่อให้แน่ใจว่าทุกเอกสารใน Batch ได้มีการประมวลผล โดยหลักการบันทึกข้อมูลการนำเข้าของ Batch ประกอบด้วย ๓ หลักที่สำคัญ คือ

- จำนวนเอกสารใน Batch (Record count) เพื่อให้ทราบว่าทุกรายการผ่านการนำเข้าครบถ้วน
- ยอดรวมจำนวนตัวเลขที่เป็นตัวเงิน Amount control total
- ยอดรวมจำนวนตัวเลขที่ไม่ใช่ตัวเงิน Hash total

ดังนั้นเพื่อให้แน่ใจ ว่าไม่มีเอกสารใด ๆ ที่ประมวลผลมากกว่า ๑ ครั้ง มีร่องรอยการตรวจสอบ (Audit Trail) ตลอดการทำงานตั้งแต่นำเข้า การประมวลผล การส่งข้อมูลออก และหากมีกรณีที่ Batch ไม่ตรงต้องยกเลิกใหม่ทั้งหมด

๑.๔ การควบคุมความถูกต้องของข้อมูลนำเข้ามี ๓ ระดับ ได้แก่

๑.๔.๑ ระดับ Field

- Validity check ความมีอยู่จริง
- Field check
- Limit Check จำกัดค่าสูงสุด
- Range check ช่วงของค่าต่ำสุด - สูงสุด

๑.๔.๒ ระดับ Record ตั้งแต่ ๒ Field ขึ้นไป

เช่น การตรวจสอบความสมเหตุสมผลของข้อมูล รายการที่นำเข้ามีความสัมพันธ์กับ Field อื่นที่เก็บอยู่ในระบบงานอย่างเหมาะสมหรือไม่ เช่น ลูกจ้างกับข้าราชการเมื่อเราคีย์ข้อมูลเข้ารหัสในระบบ จะต้องรู้ว่ารหัสที่คีย์นั้นเป็นรหัสของใคร แล้วจะสามารถส่งไปยังข้อมูลอัตราเงินเดือนที่ถูกต้อง

๑.๔.๓ ระดับ File

๑.๕ การแก้ไขข้อผิดพลาด ทำได้ ๓ แบบ

- แก้ไขทันที
- แยกข้อมูลที่ผิดออก แล้วทำการแก้ไข แล้วจึงนำเข้าใหม่
- ในกรณีที่ยอดรวม Batch ไม่ตรงกัน จะต้องทำการ Reject ใหม่ทั้งหมด

๒) การควบคุมการประมวลผล (Processing Control) เป็นการควบคุมแบบติดตาม Detective หลักการคือ การแทรกแซงการทำงานของระบบด้วยตัวบุคคลต้องลดให้น้อยที่สุด และมีการจัดเก็บร่องรอยการตรวจสอบไว้ (Log) แบ่งเป็น ๒ ประเภท

๒.๑ การตรวจสอบนอกระบบ Black Box Approach ตรวจสอบภายนอกที่ไม่ซับซ้อน (Audit around the computer)

๒.๒ การตรวจสอบผ่านระบบ White Box Approach ต้องมีเทคนิคการใช้คอมฯ ช่วยในการตรวจสอบ เช่น การตรวจสอบระบบว่ามีการเก็บร่องรอยการตรวจสอบครบถ้วนหรือไม่

การใช้เทคนิคคอมฯ ช่วยในการตรวจสอบ กลุ่ม Historical Data Techniques เป็นเครื่องมือที่ตรวจสอบข้อมูลในอดีต นำข้อมูลที่ผ่านการปฏิบัติงานจริงมาใช้ในการตรวจสอบ ได้แก่

เทคนิค Generalized Audit Software หรือ GAS เป็นโปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป เป็นโปรแกรมสำเร็จรูปที่ใช้ในการตรวจสอบที่ขายตามท้องตลาด

การใช้ GAS คือโปรแกรมสำเร็จรูป ในการตรวจสอบทั่วไป ซึ่งในการนำมาใช้ต้องกำหนดวัตถุประสงค์เป็นอันดับแรก โดยใช้ตรวจสอบ ๔ ด้าน

- ตรวจสอบคุณภาพการควบคุมภายในของระบบข้อมูล
- ตรวจสอบคุณภาพและควบคุมภายในของระบบประมวลผล
- ตรวจสอบความมีอยู่จริงของทรัพย์สิน
- วิเคราะห์เปรียบเทียบ

ประโยชน์ GAS

- ประหยัดเวลา
- สามารถทำได้อย่างรวดเร็วในกรณีที่มีการเปลี่ยนวัตถุประสงค์ในการตรวจสอบ
- ผู้ตรวจสอบไม่มีความชำนาญในเรื่องการเขียนโปรแกรมสามารถใช้ GAS ได้

ข้อจำกัดของ GAS

- ตรวจสอบได้เฉพาะหลังเกิดรายการแล้ว
- ตรวจ Processing logic ได้เฉพาะที่ไม่สลับซับซ้อนมากนัก
- ไม่สามารถบอกถึงแนวโน้มที่ระบบอาจมีข้อผิดพลาด
- จำเป็นต้องใช้ข้อมูลจากระบบ โดยให้ความเชื่อถือว่าข้อมูลที่ได้มามีความครบถ้วน/สามบูรณ์ (ยืนยันยอดกับ GL)

การใช้ข้อมูลทดสอบมี ๒ ประเภทที่สำคัญ

๑. การใช้ข้อมูลทดสอบแบบ Test Data ใช้กับประมวลผลแบบกลุ่ม (Batch) เป็นการ Copy ระบบงานจริงมาไว้บนเครื่องคอมฯ ของผู้ตรวจสอบและใช้ข้อมูลที่สร้างขึ้นเอง/จำลอง มาทดลอง

ขั้นตอนการทำ Test Data

๑.๑ สร้างข้อมูลทดสอบหรือรายการจำลอง

๑.๒ คำนวณผลการประมวลที่คาดว่าจะได้รับ (คำนวณไว้ก่อนเพื่อไว้เปรียบเทียบกับข้อ ๑.๓)

๑.๓ ประมวลผลโดยใช้เครื่องผู้ตรวจ แต่ copy ระบบงานจริงมา

ข้อดี ผู้ตรวจสอบมีความมั่นใจมากขึ้นในความเชื่อถือได้ของโปรแกรมที่ผู้รับตรวจใช้ปฏิบัติงานจริง

ข้อเสีย ๑. ไม่สามารถทำให้แน่ใจว่าการควบคุมภายในมีประสิทธิผล

๒. โปรแกรมที่ผู้ตรวจสอบ copy สามารถทำงานได้เฉพาะอยู่ในขอบเขต Test Data

๓. สามารถทดสอบจำกัดเพียงฟังค์ชั่นที่มีอยู่ในโปรแกรมลูกค้า

๒. การใช้ข้อมูลทดสอบแบบ Integrated Text Facility = ITF ซึ่งเป็นการทดสอบบนระบบงานจริงแต่ใช้ข้อมูลสมติ (Dummy)

ข้อเสีย การไม่ลบข้อมูลจำลองอาจทำให้เกิดข้อผิดพลาดขึ้นในข้อมูลจริงโดยไม่ตั้งใจ

เทคนิค Snap shop

ข้อดี เป็นเทคนิคที่สามารถดูเนื้อหาขณะประมวลผลได้

ข้อเสีย ต้องมีความชำนาญทางด้านเทคนิคสูง

เทคนิค การอ่านสอบทานโปรแกรม Desk checking

ข้อดี มีผลในทางจิตวิทยาในการป้องกัน programmer ไม่ให้ทำการแก้ไขเปลี่ยนแปลงโปรแกรมโดยไม่ได้รับอนุญาต

ข้อเสีย ๑. ผู้ตรวจสอบต้องมีความรู้ในการเขียนโปรแกรมสูง

๒. ใช้เวลาและค่าใช้จ่ายสูง

๓. ปกติจะเป็นการยากกว่า Program ที่เช็คอยู่เป็น version ล่าสุด

เทคนิค การเปรียบเทียบโปรแกรม

ข้อดี ๑. ง่าย เสียค่าใช้จ่ายในการทำงานน้อย

๒. มี copy โปรแกรม ป้องกัน programmer แก้ไขก่อนได้รับอนุญาต

ข้อเสีย ต้องมีความรู้ในการเขียนโปรแกรมสูง

Mapping ช่วยให้ตรวจพบส่วนของคำสั่งที่เป็น time bomb หรือ ม้าโทรจัน (Trojan horse) โดยดูจากคำสั่งที่ไม่มีการเรียกใช้งานนาน ๆ

Parallel Simulation การจำลองแบบคู่ขนาน เป็นการนำข้อมูลจริงของลูกค้ามาประมวลผลบนโปรแกรมที่ผู้ตรวจสอบจัดทำขึ้นเพื่อเปรียบเทียบกัน

เหตุผลที่ผู้ตรวจสอบใช้โปรแกรมอรรถประโยชน์ คือ การใช้ GAS หรือ Audit Software อื่นๆ ที่ผู้ตรวจสอบต้องใช้โปรแกรมอรรถประโยชน์ช่วยในการจัดรูปแบบ Format และ Download ข้อมูล

ประโยชน์ของการใช้ CAATs การประยุกต์ใช้คอมฯ เพื่อช่วยในการตรวจสอบ

๑. ทำให้เห็นภาพรวมของระบบและการเคลื่อนไหวของรายการ

๒. ช่วยลดระดับความเป็นอิสระจากผู้รับการตรวจสอบ

๓. ช่วยเพิ่มความเป็นอิสระจากผู้รับการตรวจ

๔. ลดค่าใช้จ่ายและระยะเวลาในการตรวจสอบ

๓) การควบคุมข้อมูลส่งออก (Output Control) เป็นการควบคุมแบบแก้ไข Corrective

การตรวจสอบรายได้

วงจรรายได้ ประกอบด้วย

๑. Master data ข้อมูลหลัก

๒. การรับคำสั่งซื้อของลูกค้า

๓. การอนุมัติการขายสินค้า/บริการ

๔. การส่งมอบสินค้า/บริการ

๕. การรับชำระเงินจากลูกค้า

๖. การบันทึกบัญชีเป็นรายได้ของกิจการ

การควบคุม Control ประเภทของการควบคุม Type of control แบ่งเป็น ๒ ประเภท

๑. การควบคุมแบบป้องกัน preventive control เป็นการควบคุมที่ต้องการป้องกันไม่ให้เกิดความผิดพลาด และเป็นการควบคุมที่เกิดขึ้นก่อนที่เหตุการณ์ไม่พึงปรารถนาจะเกิดขึ้น ได้แก่

- การแบ่งแยกหน้าที่
- การจัดโครงสร้างองค์กร
- ผู้จัดการแผนกสินเชื่ออนุมัติการขายทางระบบ
- การฝึกอบรม
- การจัดให้มีคู่มือการปฏิบัติงาน
- การออกแบบระบบโดยการบังคับให้ต้องเติมข้อความหรือตัวเลขในฟิลด์บางฟิลด์บนหน้าจอคอมพิวเตอร์ก่อนการประมวล

๒. การควบคุมแบบค้นหา Detective Control การควบคุมนี้เกิดขึ้นเพราะต้องการค้นหาข้อผิดพลาดหลังจากที่ความผิดเหล่านั้นได้เกิดขึ้นแล้ว

๒.๑ การจัดทำงบกระทบยอดบัญชีเงินฝากธนาคาร

๒.๒ การสอบทาน Audit logs

๒.๓ ทุกสิ้นเดือน เจ้าหน้าที่สอบทานคำสั่งซื้อที่ยังดำเนินการไม่เสร็จสมบูรณ์

วิธีการตรวจสอบ Testing steps คือ สิ่งที่ผู้ตรวจสอบภายในกระทำเพื่อเก็บรวบรวมข้อมูลในการตรวจสอบ เช่น การสัมภาษณ์และสอบถาม การสังเกตการณ์ การตรวจสอบ การตรวจรับ การยืนยันยอด

ความเสี่ยงของวงจรรายได้ คือ เรียกเก็บเงินน้อย/มากกว่า , เรียกเก็บไม่ครบ การบันทึกบัญชีมาก/น้อยกว่าที่ได้รับมา, การไม่นำเข้าบัญชีในวันที่ได้รับมา เป็นต้น

ประเด็นที่เราต้องไปตรวจสอบ

- ดูเรื่องการ control
- การควบคุมมีปัญหา
- ผลการควบคุมที่มีอยู่ (ใช้วิธี check list)
- ดูเรื่องการรับชำระ การนำเงินเข้าบัญชี Pay in , statement, ใบเสร็จรับเงิน, การรับชำระด้วยเช็คมีการขีดคร่อมหรือไม่ มีการสอบทาน pay in กับสมุดบัญชี

<u>การตรวจสอบรายจ่าย</u>

ถ้าการควบคุมวงจรรายจ่ายไม่มีประสิทธิภาพ อาจส่งผลกระทบดังต่อไปนี้

๑. ธุรกิจผลิต จะกระทบกับระบบสินค้าคงคลังล้นหรือขาด

๒. ธุรกิจซื้อขาย จะกระทบกับการทุจริตในการจ่ายเงินเจ้าหนี้หรือคู่ค้า

๓. ระบบงานของวงจรรายจ่าย (จ่ายผ่าน PO) ข้อมูลผู้ขาย การขอซื้อ การสั่งซื้อ การรับของการบันทึกบัญชี การจ่ายเงิน

๔. ความเสี่ยงของวงจรรายจ่าย

๔.๑ ความเสี่ยงทั่วไป เช่น ไม่มีการแยกหน้าที่ ไม่มีการควบคุมการเข้าถึง

๔.๒ ความเสี่ยงเฉพาะ เช่น มีการทุจริตในการสั่งซื้อ ตรวจรับของไม่ตรง ทุจริตในการจ่ายเงิน

๕. การควบคุม

๕.๑ ควบคุมทั่วไป แบ่งแยกหน้าที่เหมาะสม แยกหน้าที่จัดหา ซื้อ จ่ายเงิน บัญชี คนละคนกัน

๕.๒ ควบคุมเฉพาะ ได้แก่ การควบคุมในแต่ละกระบวนงาน ๕ กระบวนงาน ได้แก่

- การจัดซื้อจัดจ้าง ได้แก่ เอกสารเป็นทางการ ผ่านการอนุมัติ มีการตรวจสอบวัสดุคงคลัง เลือกผู้ขายที่ดีที่สุด ทำประวัติผู้ขาย ราคา ปริมาณการสั่งซื้อ
- การสั่งซื้อ ได้แก่ อนุมัติถูกต้อง ใบสั่งซื้อมีข้อมูลครบถ้วน มีเลขที่ลำดับ มีการเช็คว่าใบสั่งซื้อผู้ขาย/รับจ้างได้หรือไม่
- การรับของ ได้แก่ มีการทำรายงานความผิดปกติ มีใบกรรมการตรวจรับตั้งกรรมการตรวจรับ และตรวจนับของ เป็นต้น
- การบันทึกบัญชีเจ้าหนี้ ได้แก่ การบันทึกเป็นปัจจุบัน ได้รับอนุมัติเรียบร้อยแล้ว มีการตรวจสอบเอกสาร และตัวเลขก่อนยืนยันในระบบ
- การจ่ายเงิน ได้แก่ มีการตรวจสอบและอนุมัติจ่ายเงิน ชำระเงินตามสัญญาใบสำคัญให้ทำเครื่องหมายป้องกันกันจ่ายซ้ำ (จ่ายเงินแล้ว) มีการจัดเก็บเอกสารเพื่อรอการตรวจสอบ เป็นต้น

การปฏิบัติการระบบสารสนเทศ (Information System Operation)

๑. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นนโยบายที่จะทำให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และได้รับทราบบาทบาทหน้าที่ความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมถึงแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบายความไม่มั่นคงปลอดภัยต่อการปฏิบัติงาน โดยจะ<u>เน้นที่บุคลากร</u> หน่วยงานต้องกำหนดหลักเกณฑ์ วิธีการในการทำธุรกรรมของอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โดยจัดทำแนวนโยบาย แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเนื้อหา ต้องประกอบด้วย

- การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

- การจัดให้มีระบบสารสนเทศ ,มีระบบสำรองข้อมูล ให้อยู่ในภาพพร้อมใช้งาน, การจัดทำ

- แผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้ใช้งานได้อย่างต่อเนื่อง

- การตรวจสอบ และประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๒. การนำระบบสารสนเทศมาช่วยเพิ่มประสิทธิภาพ มีความเสี่ยงคือ ระบบสารสนเทศถูกเชื่อมต่อออกสู่ภายนอกด้วยเครือข่ายอินเตอร์เน็ต ทำให้ถูกคุกคามบุกรุก ถูกโจมตีจาก แฮกเกอร์ ไวรัสคอมพิวเตอร์ดังนั้น ควรมีมาตรการป้องกันที่เป็นมาตรฐานสากลมาประยุกต์ใช้โดยกำหนดเป็นนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓. ปัจจัยการเกิดความเสี่ยง

- people risk เกิดจากตัวบุคคลที่เป็นบุคคลากรภายใน/ภายนอกองค์กร เป็นผู้ก่อให้เกิดความเสี่ยง เป็นความเสี่ยงที่เกิดจากตัวบุคคล ทั้งบุคลากรภายใน/ภายนอกองค์กร ผู้มีส่วนได้เสีย (พนักงาน, ผู้ถือหุ้น, คู่แข่ง Partner และ Outsource) คิดเป็นเปอร์เซ็นต์สูงที่สุด แต่สำหรับบุคคลเป็นการลงทุนน้อยที่สุดแต่ได้ผลดีที่สุด

- process risk เกิดจากองค์กรไม่ดำเนินการทำขั้นตอนปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยขาดวิธีการควบคุมที่รัดกุมเพียงพอ หรือเกิดจากบุคลากรละเลยไม่ปฏิบัติตาม

- Technology risk เกิดจากองค์กรควบคุมภายทำงานระบบเทคโนโลยีไม่ดีพอ ทำให้ระบบเกิดช่องโหว่ให้ผู้ไม่ประสงค์ดีเข้ามาคุกคามสร้างความเสียหายให้แก่องค์กรได้

๔. องค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย ๓ ประการ คือ C-I-A

- Confidentiality (การรักษาความลับ) ปกป้องรักษาสารสนเทศขององค์กรเป็นความลับ สามารถล่วงรู้ เข้าถึง ให้ใช้งานได้เฉพาะผู้ที่รับได้อนุญาต เท่านั้น และผู้เข้าใช้งานต้องได้รับสิทธิให้เข้าใช้งานได้ตามที่องค์กรกำหนดไว้เท่านั้น

- Integrity (การรักษาสภาพเดิมของสารสนเทศ) ปกป้องให้มั่นใจว่าข้อมูลที่มีอยู่ถูกต้องสมบูรณ์ ครบถ้วน ไม่ถูกแก้ไข หรือถูกทำลายจากผู้ไม่มีสิทธิ ไม่ว่าจะมีเจตนาหรือไม่ก็ตาม

- Availability (การรักษาความพร้อมใช้งาน) ปกป้องให้มั่นใจว่าสารสนเทศมีความพร้อมให้ผู้มีสิทธิเข้าถึงสารสนเทศ ใช้งานได้ทุกเมื่อที่ต้องการ

๕. โครงสร้างความมั่นคงปลอดภัยภายในองค์กร ได้แก่

- การกำหนดบทบาท หน้าที่ ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ <u>ต้องมีความชัดเจน ไม่ซ้ำซ้อน</u>

- การแบ่งแยกหน้าที่ความรับผิดชอบ

- การติดต่อกับหน่วยงานผู้มีอำนาจ ต้องมีการแต่งตั้งเจ้าหน้าที่ ผู้รับผิดชอบ จัดทำรายชื่อมอบอำนาจ และต้องแจ้งให้แต่ละหน่วยทราบด้วย (ป้องกันการปลอมตัวเข้าระบบ)

๖. ขั้นตอนการแบ่งแยกหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ

- จัดทำโครงสร้างองค์กร ได้แก่ การกำหนดบทบาทหน้าที่ของบุคลากร ซึ่งต้องไม่ขัดแย้งในการความรับผิดชอบ ต้องมีบุคคลสำรองกรณีบุคคลหลักไม่อยู่

- จัดทำรายละเอียดของงาน หน้าที่ของงาน

- จัดทำ แต่งตั้งผู้รับผิดชอบ

๗. การสร้างความมั่นคงปลอดภัยในองค์กรระดับบุคลากร

จุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับผู้ใช้บริการภายนอกหรือหน่วยงานภายนอกมีหลักเกณฑ์ดังนี้

- กำหนดบทบาท หน้าที่ ความรับผิดชอบ ทางด้านความปลอดภัยไว้ในสัญญาอย่างชัดเจน มีการติดตามผลการปฏิบัติงานเป็นรายบุคคล

- กำหนดข้อตกลงการรักษาความลับขององค์กร โดยห้ามมิให้นำข้อมูลขององค์กรไปเผยแพร่ให้แก่บุคคลอื่น ซึ่งต้องสอดคล้องกับสัญญาการว่าจ้าง

- อบรมให้ จนท. ตระหนักถึงความสำคัญของการรักษาความปลอดภัยสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงานที่สนับสนุนนโยบายความปลอดภัยขององค์กร

- รายงานผลเหตุการณ์ที่ซึ่งผลกระทบต่อความปลอดภัยขององค์กรให้แก่ผู้บริหารได้รับทราบโดยด่วนเพื่อพัฒนาหาแนวทางแก้ไข