

ข้อสอบจำลอง

การทดสอบความรู้ของผู้ขอขึ้นทะเบียนเป็นผู้สอบบัญชีรับอนุญาต

ครั้งที่ 12 (3/2551)

วิชา การสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์ (ส่วนอำนวยการ)

วันที่ พฤศจิกายน 2551

เวลา 13.00 – 16.00 น.

สถานที่ทดสอบ -

ข้อสอบมี 3 ข้อ

แยกสมุดคำตอบข้อละ 1 เล่ม

ข้อ 2

ก. ตามมาตรฐานการสอบบัญชี 1008 เกี่ยวกับการพัฒนาระบบสารสนเทศที่ใช้คอมพิวเตอร์ มีข้อแตกต่างในการออกแบบและการกำหนดวิธีการปฏิบัติงานระหว่างระบบสารสนเทศที่ใช้คอมพิวเตอร์ กับระบบงานซึ่งจัดทำด้วยมือ ให้ระบุข้อแตกต่างมา 3 ลักษณะ พอสั่งเขป (6 คะแนน)

ข. ผู้สอบบัญชีสอบทานและประเมินการควบคุมขั้นต้นพบว่าระบบรายได้ และระบบเงินเดือนเชื่อถือได้ จึงตัดสินใจจึงการควบคุมกับระบบดังกล่าว แต่เมื่อทำการตรวจสอบแล้วพบว่า

1) บริษัท มีนโยบายสอบทานรหัสของผู้ใช้งานปีละ 2 ครั้ง จากการสอบทานพบว่า รหัสของผู้ใช้งานที่ไม่เคยใช้งานในระบบเลยเป็นเวลานาน 6 เดือน มีจำนวน 25 ราย และพบรหัสผู้ใช้งานที่ลาออกไปแล้ว 8 ราย จากการรหัสของผู้ใช้งานทั้งหมด 600 ราย

2) ผู้ที่สามารถเข้าโปรแกรมและข้อมูลจริงทั้งหมด คือ ผู้จัดการฝ่ายคอมพิวเตอร์ นักพัฒนาระบบ และเจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ ซึ่งทั้ง 3 คน ใช้รหัสผู้ใช้งานและรหัสผ่านเดียวกันในการเข้าระบบงาน นอกจากนี้รหัสผู้ใช้งานและรหัสผ่านดังกล่าว ไม่เคยเปลี่ยนแปลงตั้งแต่ติดตั้งระบบ

ให้ท่านระบุจุดอ่อน และความเสี่ยงที่อาจเกิดขึ้นและจะยังใช้ผลการควบคุมที่ผ่านมาอ้างอิงได้หรือไม่จนบอกเหตุผล และท่านจะดำเนินการในขั้นต่อไปอย่างไร (14 คะแนน)

แนวคำตอบข้อสอบจำลอง
การทดสอบความรู้ของผู้ขอขึ้นทะเบียนเป็นผู้สอบบัญชีรับอนุญาต
ครั้งที่ 12 (3/2551)
วิชา การสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์

ข้อ 2

ก. การวิเคราะห์ประเด็น โจทย์ให้ตอบลักษณะเชิงหลักการ และท่งจำ ของแนวปฏิบัติงานสอบบัญชี รหัส 1008 ซึ่งไม่เคยออกมานานมาก

ตามมาตรฐานการสอบบัญชี 1008 เกี่ยวกับการพัฒนาระบบสารสนเทศที่ใช้คอมพิวเตอร์ มีข้อแตกต่างในการออกแบบและการกำหนดวิธีการปฏิบัติงานระหว่างระบบสารสนเทศที่ใช้คอมพิวเตอร์ กับระบบงานซึ่งจัดทำด้วยมือ มีลักษณะที่แตกต่างกันพอสังเขป ดังนี้

1. รายการทางบัญชีรายการเดียวอาจนำไปปรับปรุงฐานข้อมูลหรือเพิ่มข้อมูลคอมพิวเตอร์ได้มากกว่าหนึ่งแฟ้ม

ข้อมูลรายการเดียวที่นำเข้าสู่ระบบบัญชีอาจปรับปรุงข้อมูลทางบัญชีที่เกี่ยวข้องกับรายการนั้นได้พร้อมกันทั้งหมดโดยอัตโนมัติ เช่น เอกสารประกอบการส่งสินค้าอาจใช้ปรับปรุงแฟ้มข้อมูลขาย ลูกหนี้ และสินค้าคงเหลือ เป็นต้น ดังนั้น โอกาสที่จะเกิดความผิดพลาดในการปรับปรุงข้อมูลดังกล่าวจะลดลง ในทางตรงกันข้าม ถ้าข้อมูลที่นำเข้าคอมพิวเตอร์ผิดพลาด รายการบัญชีนั้นอาจก่อให้เกิดความผิดพลาดต่อข้อมูลทางบัญชีมากกว่าหนึ่งรายการได้เช่นเดียวกัน

2. รายการที่สร้างขึ้นจากระบบงาน

รายการบางรายการอาจสร้างจากระบบสารสนเทศที่ใช้คอมพิวเตอร์ โดยไม่ต้องใช้เอกสารเป็นสื่อในการนำข้อมูลเข้าคอมพิวเตอร์ การอนุมัติรายการดังกล่าวอาจไม่มีเอกสารหลักฐาน ซึ่งจะแตกต่างจากการอนุมัติรายการที่ไม่ได้ใช้คอมพิวเตอร์ เช่น การคำนวณดอกเบี้ยแล้วผ่านรายการไปยังบัญชีลูกค้าโดยอัตโนมัติตามคำสั่งที่กำหนดเงื่อนไขการอนุมัติไว้ในโปรแกรมคอมพิวเตอร์ ดังนั้น จึงจำเป็นต้องมีการควบคุมการออกแบบระบบงานและวิธีการปฏิบัติงานให้เป็นไปตามที่อนุมัติไว้

3. สื่อที่ใช้ในการเก็บโปรแกรมและข้อมูลมีโอกาสเสียหายได้ง่าย

ข้อมูลจำนวนมากและโปรแกรมคอมพิวเตอร์ที่ใช้ในการประมวลผลข้อมูล อาจเก็บอยู่ในสื่อที่เคลื่อนย้ายได้หรือไม่ได้ เช่น แผ่นดิสก์หรือเทปแม่เหล็ก สื่อข้อมูลเหล่านี้อาจถูกโจรกรรม สูญหาย หรือถูกทำลายได้ง่ายทั้งโดยเจตนาและไม่เจตนา ดังนั้นจึงจำเป็นต้องมีการออกแบบมาตรการรักษาความปลอดภัยของสื่อเหล่านี้โดยรัดกุม

ข. การวิเคราะห์ประเด็น โจทย์ให้ตอบกระบวนการประเมินการควบคุมชั้นปลาย (บทที่ 2) ซึ่งต้องเข้าใจว่าเมื่อสอบทานและประเมินการควบคุมแล้วพบว่ามีความเสี่ยงและความเสี่ยงแสดงว่าระบบงานนั้นไม่น่าเชื่อถือ หรือมีความเสี่ยงสูงให้ข้ามขั้นตอนการทดสอบการควบคุมไปทดสอบสาระสำคัญ

จุดอ่อนและความเสี่ยงที่อาจเกิดขึ้นจากการสอบทาน

จุดอ่อน	ความเสี่ยงที่อาจเกิดขึ้น
1. ไม่ได้กำหนดให้ระบบ lock รหัสผ่าน (password) และรหัสผู้ใช้งานของผู้ที่ไม่ได้นำรหัสผู้ใช้งานของตนมาใช้นานเกินไป	- รหัสผ่าน (password) อาจถูกล้วงรู้โดยบุคคลที่ไม่เกี่ยวข้องกับระบบงาน
2. กรณีพนักงานลาออก ระบบไม่ได้ delete รหัสผ่าน (password) ออกจากระบบทันทีที่วันลาออกมีผล	- อาจมีบุคคลที่ไม่เกี่ยวข้อง (พนักงานที่ลาออก) เข้าระบบงานโดยไม่ได้รับอนุญาต
3. ให้ผู้ที่ไม่มีความเกี่ยวข้องสามารถเข้าถึงโปรแกรมและข้อมูลจริงซึ่งได้แก่ นักพัฒนาระบบ และเจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์	- นักพัฒนาระบบ และเจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์อาจเข้าไปทำลายข้อมูล หรือนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต
4. ไม่ได้กำหนดอายุการใช้งานรหัสผ่าน (password) อย่างเหมาะสม เช่น ให้เปลี่ยนรหัสผ่าน (password) ทุก 3 เดือน	- รหัสผ่าน (password) อาจถูกล้วงรู้โดยบุคคลที่ไม่เกี่ยวข้องกับระบบงาน
5. ให้ผู้ใช้งาน (User) หลายคนใช้รหัสผ่าน (password) และรหัสผู้ใช้งานร่วมกัน	- กรณีที่มีการฝ่าฝืนเข้าไปแก้ไขโปรแกรมหรือข้อมูลโดยไม่ได้รับอนุญาตไม่สามารถระบุได้ว่าผู้ใช้งาน (User) คนใดเป็นผู้กระทำเนื่องจาก รหัสผ่าน (password) และรหัสผู้ใช้งานนี้ใช้ร่วมกันหลายคน
6. ไม่ได้กำหนดให้มีการสอบทานรหัสผ่าน (password) และรหัสผู้ใช้งาน อย่างสม่ำเสมอ เช่น สอบทานรหัสผ่าน (password) และรหัสผู้ใช้งานทุกเดือน	- หากโปรแกรมและข้อมูลได้รับความเสียหายไม่สามารถแก้ไขได้ทันที

ตามที่ได้กล่าวข้างต้นผู้สอบบัญชีไม่สามารถอ้างอิงการควบคุมที่ผ่านมาได้เนื่องจากมีการสอบทานและประเมินการควบคุมในขั้นต่อมาแล้วพบว่ามีความเสี่ยงที่แสดงว่าระบบการควบคุมไม่น่าเชื่อถือ ผู้สอบบัญชีจะต้องเสนอแนะวิธีการควบคุมจุดอ่อนและความเสี่ยงที่อาจเกิดขึ้นต่อผู้บริหารของกิจการดังนี้

1. กำหนดให้ระบบ lock รหัสผ่าน (password) และรหัสผู้ใช้งาน
2. เมื่อมีพนักงานลาออกต้องกำหนดให้ระบบ Delete รหัสผ่าน (password) และรหัสผู้ใช้งานออกทันที
3. กำหนดให้เฉพาะผู้ที่มีความเกี่ยวข้องเท่านั้นที่ได้รับสิทธิเข้าสู่โปรแกรม และข้อมูลจริงตามความจำเป็น
4. กำหนดอายุการใช้งานของรหัสผ่าน (password) เช่น ให้เปลี่ยนรหัสผ่าน (password) ทุก 3 เดือน
5. กำหนดให้รหัสผ่าน (password) และรหัสผู้ใช้งาน รายเดี่ยวนั้นมีเจ้าของเพียงคนเดียว
6. กำหนดให้มีผู้รับผิดชอบในการสอบทานรหัสผ่าน (password) และรหัสผู้ใช้งาน อย่างสม่ำเสมอทุกเดือน

เมื่อผู้สอบบัญชีไม่สามารถอ้างอิงการควบคุมที่ผ่านมาได้เนื่องจากระบบไม่น่าเชื่อถือ ผู้สอบบัญชีไม่จำเป็นต้องทดสอบการควบคุม แต่ให้ทำการทดสอบสาระสำคัญ (Substantive Test) แทนโดยขยายขอบเขต ลักษณะการทดสอบและระยะเวลา

แนวคำตอบโดย อ.พัฒนา บุญสุข
สถาบัน PC Center