ประจำตัวสอบ.....

ข้อสอบจำลอง

การทดสอบความรู้ของผู้ขอขึ้นทะเบียนเป็นผู้สอบบัญชีรับอนุญาต

ครั้งที่ 17 (2/2553)

วิชา การสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์ (ส่วนอัตนัย)

วันที่ กรกฎาคม 2553 เวลา 13.00 – 16.00 น.

สถานที่ทดสอบ - ข้อสอบมี 3 ข้อ

แยกสมุดคำตอบข้อละ 1 เล่ม

.....

ข้อ 1 บริษัท KYC เป็นบริษัทผู้ผลิตอุปกรณ์คอมพิวเตอร์ มีพนักงานทั้งหมด 60 คน เป็นโปรแกรมเมอร์จำนวน 10 คน บริษัทใช้ระบบโปแกรม The manager ซึ่งโปรแกรมเมอร์ที่เป็นพนักงานประจำของบริษัทเป็นผู้พัฒนาโปรแกรมดังกล่าวใช้สำหรับทุกส่วนงานของบริษัท ในช่วงที่ผ่านมา มีผู้ร้องขอให้ปรับปรุงโปรแกรมดังกล่าวบ่อยครั้งเนื่องจากโปรแกรมมีปัญหา

ในฐานะที่ท่านเป็นผู้สอบบัญชีของบริษัทแห่งนี้ พบว่าโปรแกรมเมอร์ของบริษัทได้ทำการเปลี่ยนแปลงแก้ไขโปรแกรม รวมทั้งทดสอบก่อนทำการย้ายโปรแกรมนี้ไปที่โฟลเดอร์(Folder)ที่เก็บโปรแกรมระบบงานจริง(Production) โดยทำการ Copy ทับโปรแกรมเดิมซึ่งมีชื่อเดียวกัน และยังพบว่าตั้งแต่เปิดบริษัทมา 6 ปี แล้วพนักงานยังไม่เคยเปลี่ยนรหัสผ่าน โดยผู้บริหารให้เหตุผลว่าเป็นการยุ่งยากที่จะต้องมาคอย Reset รหัสผ่านอยู่เรื่อยๆเนื่องจากมีพนักงาน 60 คน นอกจากนี้พนักงานทั้งหมดอาทิ ผู้บริหารระดับสูง ผู้บริหาร ผู้จัดการ และพนักงานทุกระดับ สามารถเข้าระบบงาน The manager ได้เท่ากันหมด เพื่อความสะดวกในการปฏิบัติงานของบริษัท

คำสั่ง : ในฐานะที่ท่านเป็นผู้สอบบัญชีให้ท่านเสนอแนะวิธีการควบคุมทั่วไป มา 5 ข้อ

(20 คะแนน)

PC Center
Tutor CPA

แนวคำตอบข้อสอบจำลอง

การทดสอบความรู้ของผู้ขอขึ้นทะเบียนเป็นผู้สอบบัญชีรับอนุญาต

ครั้งที่ 17 (2/2553)

วิชา การสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์

ข้อ 1 การวิเคราะห์ประเด็น โจทย์เป็นการควบคุมทั่วไปเนื่องจากเป็นเหตุการณ์เกี่ยวกับการปฏิบัติงานของบุคคลากรด้านสารสนเทศ

วิธีการควบคุมทั่วไป มีดังต่อไปนี้

1. **การแบ่งแยกหน้าที่ (Segregations)** มีวิธีการควบคุมดังนี้

ต้องแบ่งแยกหน้าที่กันระหว่างเจ้าหน้าที่พัฒนาระบบ กับเจ้าหน้าที่บำรุงรักษา(Maintenance) การปรับปรุง หรือแก้ไขระบบงานควรกำหนดเป็นหน้าที่ของเจ้าหน้าที่บำรุงรักษา (Maintenance) การแบ่งแยกหน้าที่ดังกล่าว จะทำให้ Programmer คนเดิมไม่สามารถเข้าถึงโปรแกรมที่พัฒนาขึ้นและมีการนำมาใช้แล้วได้อีก ซึ่งจะช่วยป้องกันการทุจริตเกี่ยวกับโปรแกรมที่อาจเกิดขึ้น

2. **การควบคุมการเข้าถึงระบบงาน (Logical Access Control)** มีวิธีการควบคุมดังนี้

การควบคุมการเข้าถึงระบบงาน The manager ประกอบด้วย

2.1 การตรวจสอบความแท้จริง (Authentication) โดยการกำหนดผู้มีสิทธิเข้าใช้ระบบงาน The manager เฉพาะผู้ที่ได้รับอนุมัติ ซึ่งการแสดงการเป็นผู้ใช้ สามารถใช้วิธี ดังต่อไปนี้

1) **รหัสผ่าน** (Password) ใช้ควบคุมการระบุตัวตนของผู้ใช้ระบบงาน เพื่อแสดงสิทธิ์เข้าใช้ระบบงาน รหัสผ่านที่ป้อนอาจเป็น หมายเลขพนักงาน ชื่อ หรือชื่อตามบัญชีผู้ใช้ระบบ เป็นต้น ถ้าผู้ใช้ระบบงานป้อนชื่อผู้ใช้ระบบ และรหัสผ่านที่ตรงกันกับที่มีอยู่ในระบบงานแล้ว จะถือว่าเป็นการแสดงสิทธิ์ของผู้ใช้ระบบงาน

2) **การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ** (Physical Possession Identification) เช่น บัตรประจำตัว (ID Card) ที่มีการบันทึกข้อมูลบุคคล และสามารถอ่านได้ด้วยเครื่องคอมพิวเตอร์

3) **การระบุตัวตนด้วยค่าทางชีวภาพ** (Biometrics Identification) อุปกรณ์อ่านค่าทางชีววิทยา เพื่อระบุตัวตน แยกลักษณะบุคคลตามคุณสมบัติของร่างกาย เช่น ลายมือ เรตินา เสียง ลักษณะใบหน้า ข้อมูลร่างกายผู้ใช้ หรือคุณสมบัติทางชีวภาพที่ใช้ระบุตัวตนต้องตรงกับข้อมูลที่จัดเก็บในระบบงาน จึงจะได้รับอนุญาตเข้าใช้ระบบงาน

2.2 การกำหนดสิทธิ (Authorization) หลักการสำคัญในการให้สิทธิแก่บุคคลากรในการเข้าสู่ระบบงาน The manager นั้นควรจำกัดสิทธิ และระดับที่จะให้ใช้งานได้ตามหลักความ

PC Center

จำเป็นที่ต้องทำงานนั้นให้เสร็จ (On a Need Basis) และหลักให้สิทธิพิเศษน้อยที่สุด ไม่ควรให้ทุกคนสามารถเข้าระบบงาน The manager ได้เท่ากันทุกคน

2.3 การบันทึกกิจกรรมต่างๆในระบบเพื่อการตรวจสอบ (Audit Logging) เป็นการบันทึกกิจกรรมต่าง ๆ ที่ผู้ใช้ได้ดำเนินการในระบบ เพื่อให้สามารถตรวจสอบได้ และช่วยให้เกิดร่องรอยการตรวจสอบ (Audit Trail)

3. การเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ มีวิธีการควบคุมดังนี้

- จะต้องมีการขอและอนุมัติการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศอย่างเป็นทางการ โดยใช้ใบคำขอการเปลี่ยนแปลงที่เป็นแบบฟอร์มที่เตรียมไว้ล่วงหน้า โดยมีการบันทึกรายละเอียดอย่างชัดเจน เช่น ผู้ขอ ผู้อนุมัติ วันที่ขอ
- กำหนดระเบียบวิธีการปฏิบัติในการเปลี่ยนแปลงแก้ไขโปรแกรมที่เป็นลายลักษณ์อักษร
- ศึกษาผลกระทบต่าง ๆ ทั้งผลกระทบงานด้านเทคนิค ผลกระทบที่มีต่อโปรแกรมอื่น และความเสี่ยงจากการเปลี่ยนแปลง
- ทดสอบโปรแกรมที่แก้ไขแล้วก่อนนำมาใช้งาน โดยตัวแทนเจ้าของระบบงาน The manager
- การโอนย้ายระบบงานที่แก้ไขแล้ว ต้องมีการอนุมัติการโอนย้ายระบบงานไปใช้งานหลังจากทดสอบระบบงานเป็นที่พอใจเจ้าของระบบงานแล้ว เพื่อมั่นใจว่าระบบงานที่ย้ายไปใช้งานนั้นเป็นระบบงานเดียวกันกับระบบงานที่ได้รับการทดสอบแล้ว และไม่ควรให้ Programmer เป็นผู้โอนย้าย
- จัดทำคู่มือประกอบการแก้ไขเปลี่ยนแปลงทั้งหมด รวมทั้งมีการแก้ไขเอกสารประกอบระบบงานทั้งหมด
- ประเมินผลและสอบทานระบบงานหรือโปรแกรมภายหลังจากเริ่มใช้งานในระยะเวลาหนึ่ง

4. นโยบายการรักษาความปลอดภัยรหัสผ่าน(Password) มีวิธีการควบคุมดังนี้

- มีการกำหนดอายุการใช้งาน(Aging)ของ Password เช่น 30 วัน หรือ 60 วัน
- ไม่ควรให้หรือเปิดเผย Password ต่อผู้อื่นไม่ว่ากรณีใด ๆ ก็ตาม
- Password ที่เก็บอยู่ในแฟ้มข้อมูลจะต้องผ่านการแปลงรหัสประเภท one way Encryption ซึ่งไม่สามารถแปลงรหัสกลับได้
- มีการกำหนดความยาวขั้นต่ำของ Password เช่น 8 ตัว
- หากมีการใช้ Password ผิดเกิน 3 ครั้ง ระบบจะระงับการใช้ User - ID
- การขอเปลี่ยนแปลงจะต้องได้รับอนุมัติจากหัวหน้าโดยตรง และต้องได้รับความยินยอมจากเจ้าของระบบงาน
- การส่งมอบ Password จะต้องทำอย่างเหมาะสม และคำนึงถึงความปลอดภัยของ Password
- หลังจากได้รับ Password ผู้ใช้งานจะต้องเปลี่ยน Password ทันที
- การกำหนด Password ให้มีความซับซ้อน และยากแก่การคาดเดา เช่น ห้ามตั้งตามชื่อเล่น หรือวันเกิดตัวเอง

สงวนลิขสิทธิ์ สถาบันติว **PC Center**
www.tuecpa.com

- การกำหนด Password ไม่ควรใช้ Password เดิมที่ถูกเปลี่ยน หรือยกเลิกไปแล้ว และควรกำหนด Password ให้เฉพาะพนักงานที่เกี่ยวข้องเท่านั้น

- การกำหนดให้รหัส (Password) รายเดียวมีเจ้าของเพียงคนเดียว เพื่อการตรวจสอบว่าคนใดเป็นคนใช้งาน

- การกำหนดระดับ (LEVEL) ของ Password ในการใช้ข้อมูล หรือโปรแกรมให้เหมาะสมกับตำแหน่งและหน้าที่ความรับผิดชอบ

- บันทึก(Log)การใช้งานของ User - Id (ไม่ใช่ Password)ไว้ทุกครั้งเพื่อการตรวจสอบในภายหลัง

- Password จะถูกลบทิ้งหรือเปลี่ยนโดยอัตโนมัติ เมื่อพนักงานลาออก หรือย้ายหน่วยงาน

5. การสำรองข้อมูล มีวิธีการควบคุมดังนี้

กิจการต้องทำการสำรอง (Backup)ข้อมูลระบบโปแกรม The manager อย่างสม่ำเสมอ ดังต่อไปนี้

- กำหนดนโยบายเกี่ยวกับการสำรองข้อมูล การกู้คืนข้อมูล และการนำข้อมูลสำรองกลับมาใช้
- กำหนดระเบียบการปฏิบัติงานที่ชัดเจนสำหรับการสำรองข้อมูล และนำข้อมูล สำรองกลับมาใช้
- มีการจัดเก็บข้อมูลสำรองไว้ในที่ปลอดภัย ทั้งภายในและนอกสถานที่
- มีการทดสอบข้อมูลสำรอง รวมทั้งกำหนดเงื่อนไขในการนำเทปหรือดิสท์กลับมาใช้ใหม่
- มีการกำหนดขั้นตอนการทำงานที่เป็นลายลักษณ์อักษรในการกู้คืนข้อมูลและเริ่มต้นระบบงานใหม่
- จัดทำตารางการสำรองข้อมูล และโปรแกรมที่ ใช้ดำเนินการสำรอง และบันทึกรายละเอียด
- ผู้ควบคุมงานปฏิบัติการระบบสารสนเทศสอบทานตารางการสำรองข้อมูล ว่าครบถ้วนถูกต้อง

PC Center
TUCPA