ขประจำตัวสอบ.....

ข้อสอบจำลอง

การทดสอบความรู้ของผู้ขอขึ้นทะเบียนเป็นผู้สอบบัญชีรับอนุญาต

ครั้งที่ 15 (3/2552)

วิชา การสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์ (ส่วนอัตนัย)

วันที่ พฤศจิกายน 2552 เวลา 13.00 – 16.00 น.

สถานที่ทดสอบ - ข้อสอบมี 3 ข้อ

แยกสมุดคำตอบข้อละ 1 เล่ม

.....

ข้อ 1 ในห้องทำงานฝ่ายสารสนเทศ มีพื้นที่ทำงาน และมีห้อง Server ซึ่งมีกุญแจปิดล็อคได้ บริษัทมีพนักงาน 11 คน โดยเป็นผู้บริหารฝ่ายสารสนเทศ 1 คน มีผู้จัดการ 1 คน ซึ่งดูแลแผนกระบบเครือข่าย 3 คน และ แผนกรักษาความปลอดภัย 3 คน สำหรับแผนกปฏิบัติการเทคโนโลยีทั่วไปมี 3 คน รหัสผ่านของพนักงานในแต่ละแผนกถูกจัดเก็บโดยหัวหน้าหน่วยงาน การเข้าออกห้องทำงานฝ่ายสารสนเทศใช้บัตรพนักงานรูด สำหรับประตูห้อง Server ถูกเปิดโดยใช้ไม้เสียบไว้ที่ประตู จากการสอบถามพนักงานรักษาความปลอดภัยทราบว่า เพื่อให้เกิดความสะดวกในการปฏิบัติงาน เนื่องจากอยู่ระหว่างการพัฒนาระบบงานโดยเจ้าหน้าที่ปฏิบัติการเทคโนโลยีทั่วไป ซึ่งมีคนเข้าออกตลอดเวลา ส่วนบริเวณภายในพื้นที่ทำงานมีการติดตั้งกล้องวงจรปิดซึ่งผู้สอบบัญชียืนยันว่าไม่พบปัญหาใดๆ

ให้ท่านระบุจุดอ่อน และข้อเสนอแนะ

(20 คะแนน)

PC Center
Tutor CPA

แนวคำตอบข้อสอบจำลอง
การทดสอบความรู้ของผู้ขอขึ้นทะเบียนเป็นผู้สอบบัญชีรับอนุญาต
ครั้งที่ 15 (3/2552)
วิชา การสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์

ข้อ 1 **การวิเคราะห์ประเด็น** โจทย์ข้อนี้ดูเหมือนไม่มีอะไร แต่ให้สังเกตว่าทุกครั้งที่โจทย์อ้างเหตุผลมักเป็นข้อบกพร่อง หรือจุดอ่อนเสมอ ต้องใช้แนวคำตอบมาจากตำราใหม่ด้วย เช่น การจัดโครงสร้างขององค์กร และที่ตรงประเด็นคือเรื่อง Physical เต็มๆ

จุดอ่อนและข้อเสนอแนะ

ข้อที่	จุดอ่อน	ข้อเสนอแนะ
1	ไม่ได้แยกหน้าที่งานพัฒนาระบบงานออกจากงานปฏิบัติการทั่วไป (Computer Operation)	- องค์กรจะต้องแยกงานพัฒนาระบบงาน และงานปฏิบัติการทั่วไปออกจากกัน เพราะลักษณะงาน 2 กลุ่มนี้มีความแตกต่างกัน งานพัฒนาระบบงานนั้นต้องการใช้ระบบคอมพิวเตอร์ที่เตรียมไว้เพื่อการพัฒนาเท่านั้น ขณะที่งานปฏิบัติการทั่วไปจะต้องใช้ระบบงานที่เก็บข้อมูลจริงและประมวลผลข้อมูลจริง หากให้ผู้พัฒนาระบบงานทำงานปฏิบัติการทั่วไปด้วย อาจเป็นสาเหตุเอื้อต่อการเปลี่ยนแปลงโปรแกรมหรือข้อมูลที่สื่อไปในทางทุจริต
2	องค์กรมีการจัดวางงานรักษาความปลอดภัยระบบสารสนเทศให้อยู่ภายใต้การบริหารของผู้บริหารของฝ่ายสารสนเทศ	- องค์กรควรจัดงานรักษาความปลอดภัยระบบสารสนเทศให้อยู่ภายนอกฝ่ายระบบสารสนเทศ เพราะจะทำให้การรักษาความปลอดภัยเข้มแข็งมากขึ้น ทำให้การดำเนินกิจการต่าง ๆ ในงานด้านสารสนเทศได้รับการควบคุมดูแลความปลอดภัยที่เป็นอิสระมากขึ้น
3	องค์กรจัดวางห้อง sever (ศูนย์คอมพิวเตอร์)อยู่ในบริเวณที่ไม่เหมาะสมและปลอดภัย อาจทำให้บุคคลที่ไม่ได้รับอนุญาตเข้าไปในระบบได้	- องค์กรควรจัดวางห้อง Sever (ศูนย์คอมพิวเตอร์) ให้อยู่ในสถานที่ที่เหมาะสม เช่น ไม่จัดให้อยู่ในสถานที่ที่มีผู้คนพลุกพล่านจำนวนมาก เพราะอาจทำให้บุคคลที่ไม่ได้รับอนุญาตเข้าไปทำลายเครื่องคอมฯหรือเปลี่ยนแปลงแก้ไขโปรแกรมหรือข้อมูลในระบบคอมพิวเตอร์

PC Center Tutor CPA

		- ควรดำเนินการสำรองข้อมูลอย่างสม่ำเสมอและจัดเก็บไว้ทั้งในและนอกศูนย์คอมพิวเตอร์เพื่อให้สามารถทำการกู้ข้อมูลขึ้นมาใหม่กรณีข้อมูลถูกทำลาย - กำหนดให้ระบบปฏิบัติการตรวจสอบความมีตัวตน(Authentication)ของผู้ใช้(User)ในการเข้าสู่ระบบงาน - จำกัดสิทธิ(Authorization)การทำรายการของผู้ใช้(User)ในระบบงานตามความจำเป็น - บันทึกการทำรายการ(Audit Logging)ที่เกิดขึ้นเพื่อตรวจสอบรายการย้อนหลัง เมื่อมีเหตุน่าสงสัย
4	ไม่ได้จำกัดสิทธิบุคคลที่สามารถเข้าออกห้อง Server (ศูนย์คอมพิวเตอร์)เนื่องจากมีการเปิดประตูห้องโดยใช้ไม้เสียบไว้	- ควรจำกัดให้เฉพาะบุคคลที่มีสิทธิเท่านั้นที่สามารถเข้าออกห้อง Server (ศูนย์คอมพิวเตอร์) ได้ซึ่งได้แก่พนักงานปฏิบัติการทั่วไป - ควรจัดให้มีระเบียบการในการให้และยกเลิกบัตรหรืออุปกรณ์อื่น ๆ ที่ใช้ในการปิดเปิดประตูเข้าออกห้อง Server
5	หัวหน้าหน่วยงานของแต่ละแผนกเป็นผู้จัดเก็บรหัสผ่าน (Passwords) ของพนักงาน ทำให้รหัสผ่าน (Passwords)ของพนักงานแต่ละคนไม่เป็นความลับ	- รหัสผ่าน (Passwords) ของพนักงานแต่ละคนไม่ควรเปิดเผยต่อบุคคลอื่นไม่ว่ากรณีใดๆ ก็ตาม - ควรจัดทำนโยบายด้านการใช้รหัสผ่าน(Passwords) เช่น ไม่ควรเปิดเผยรหัสผ่านต่อผู้อื่น มีการคำนวณความยาวขั้นต่ำ, มีการกำหนดอายุการใช้งานของรหัสผ่านเป็นต้น และทำการสื่อสารข้อมูลให้ผู้ที่เกี่ยวข้องรับทราบเพื่อใช้เป็นแนวทางปฏิบัติทั่วกัน - สร้างความเข้าใจ และจิตสำนึกด้านรักษาความปลอดภัยโดยการจัดให้มีการฝึกอบรมเพื่อสร้างความเข้าใจ (Awareness Training)อย่างต่อเนื่องและสม่ำเสมอ
6	การเข้าออกห้องทำงานฝ่ายสารสนเทศสามารถทำได้โดยใช้บัตรพนักงานรูด ทำให้พนักงานฝ่ายงานอื่นที่ไม่เกี่ยวข้องสามารถเข้าออกได้	- การผ่านเข้าออกห้องทำงาน ฝ่ายสารสนเทศควรอนุญาตเฉพาะพนักงานด้านสารสนเทศ ไม่ควรอนุญาตให้พนักงานทุกคนที่มีบัตรพนักงานสามารถผ่านเข้าออกได้

PC Center Tutor ERP

7	ไม่ได้มีการควบคุมการขอเข้าศูนย์คอมพิวเตอร์เป็นการชั่วคราวจากบุคคลที่ไม่ได้รับอนุญาต	- ควรควบคุมการขอเข้าศูนย์คอมพิวเตอร์เป็นการชั่วคราวจากบุคคลที่ไม่ได้รับอนุญาต เช่น ผู้เยี่ยมชม ช่างเทคนิคของบริษัทผู้ค้าคอมพิวเตอร์ ผู้ตรวจสอบ เป็นต้น โดยจัดให้มีการอนุญาตอย่างเหมาะสมและมีการบันทึกข้อมูลการเข้าออกอย่างเพียงพอ
8	ไม่ได้ติดตั้งอุปกรณ์ควบคุมสภาวะแวดล้อมของการทำงานของระบบคอมพิวเตอร์ในศูนย์คอมพิวเตอร์	- ควรจัดให้มีการติดตั้งและทดสอบอุปกรณ์ควบคุมสภาวะแวดล้อมของการทำงานระบบคอมพิวเตอร์ในศูนย์คอมพิวเตอร์อย่างเพียงพอ เช่น มีการติดตั้งระบบปรับอุณหภูมิความชื้นและอุปกรณ์ในการควบคุมความคงที่และจัดให้มีไฟฟ้าใช้อย่างต่อเนื่อง

PC Center
Tutor CPA