

ข้อสอบจำลอง
การทดสอบความรู้ของผู้ขอขึ้นทะเบียนเป็นผู้สอบบัญชีรับอนุญาต
ครั้งที่ 10 (1/2551)

วิชา การสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์ (อัตร้อย)

วันที่ -----

เวลา - น.

สถานที่ทดสอบ -

ข้อสอบมี - ข้อ

รวม - หน้า

แยกสมุดคำตอบข้อละ 1 เล่ม

แต่ละข้อมีคะแนนเท่ากัน

- ข้อ 3. ก. จงอธิบายความหมายความเสี่ยงจากการขาดการควบคุมภายในที่ดี (Risk Exposure)
ข. ให้ระบุกิจกรรมของการควบคุมทั่วไป ความเสี่ยง และการควบคุมทั่วไปที่ควรมีมา 6 กิจกรรม ตามตัวอย่างตารางนี้

กิจกรรม	ความเสี่ยง	การควบคุมทั่วไป
การกำหนดนโยบายสารสนเทศ	- ขาดบูรณาการข้อมูล - ระบบล้มเหลว	- กำหนดนโยบายสารสนเทศ - การปรับปรุงนโยบาย

แนวคำตอบข้อสอบจำลอง
การทดสอบความรู้ของผู้ขอขึ้นทะเบียนเป็นผู้สอบบัญชีรับอนุญาต
ครั้งที่ 10 (1/2551)
วิชา การสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์ (อัตรัย)

ข้อ 3 ก. ความเสี่ยงของการขาดการควบคุมทั่วไปที่ดี (Risk Exposure)

ความเสี่ยงของการขาดการควบคุม (Control Risk) หมายถึง ความเสี่ยงที่มีนัยสำคัญและอาจนำไปสู่ข้อผิดพลาดที่สำคัญในงบการเงิน และเป็นความเสี่ยงที่เกิดจากการขาดการป้องกัน ค้นพบ หรือแก้ไขข้อผิดพลาดได้อย่างทันกาลในโครงสร้างการควบคุมภายใน โดยปกติความเสี่ยงสืบเนื่องจะลดลงได้จากการควบคุมที่เพียงพอและมีประสิทธิภาพ ระดับความเสี่ยงของการควบคุมอาจระบุได้เป็นเชิงปริมาณ เช่น ร้อยละ 100 ร้อยละ 60 เป็นต้น หรืออาจระบุเป็นเชิงคุณภาพ เช่น ระดับสูง ระดับปานกลาง หรือระดับต่ำ

ข้อ 3. ข.

ประเภทของการควบคุม	ความเสี่ยง	การควบคุมทั่วไป
การแบ่งแยกหน้าที่งานในระบบสารสนเทศ(Segregation)	บุคคลร่วมมือกันและปกปิดการทุจริตเกี่ยวกับคอมพิวเตอร์	แบ่งแยกอำนาจหน้าที่ และความรับผิดชอบอย่างชัดเจนระหว่างนักวิเคราะห์ระบบ โปรแกรมเมอร์ ผู้ปฏิบัติงานคอมพิวเตอร์ ผู้ใช้ บรรณารักษ์ ข้อมูลและกลุ่มผู้ควบคุมข้อมูล
การควบคุม โครงการพัฒนาระบบสารสนเทศ(Development)	- การพัฒนาระบบอาจไม่ตรงกับวัตถุประสงค์และความต้องการใช้งาน - การทำงานอาจเกิดข้อผิดพลาด - ระบบที่พัฒนาขึ้นอาจขาดการควบคุมภายในที่ดี	- แผนแม่บทสารสนเทศระยะยาว - แผนงาน โครงการพัฒนาระบบ - กำหนดการประมวลผล - การมอบหมายหน้าที่ความรับผิดชอบต่อผู้จัดการ โครงการและทีมงานพัฒนาระบบ - การประเมินผลเป็นระยะ ๆ - การสอบทานหลังการติดตั้งและนำระบบมาใช้งาน - การวัดผลการดำเนินงานของระบบ
การควบคุมการเปลี่ยนแปลงแก้ไขระบบ	- ความผิดพลาดในระบบ - การทุจริต - ข้อมูลไม่ถูกต้อง - ระบบล้มเหลวหรือหยุดชะงักการทำงาน	- กำหนดระเบียบวิธีการปฏิบัติในการเปลี่ยนแปลงแก้ไขโปรแกรมที่เป็นลายลักษณ์อักษรและมีการอนุมัติจากเจ้าของระบบงาน - ศึกษาผลกระทบต่าง ๆ ทั้งผลกระทบทางด้านเทคนิค ผลกระทบที่มีต่อ โปรแกรมอื่น

		<p>และความเสี่ยงจากการเปลี่ยนแปลง</p> <ul style="list-style-type: none"> - ทดสอบโปรแกรมที่แก้ไขแล้วก่อนนำมาใช้งาน - จัดทำเอกสารคู่มือประกอบการแก้ไขเปลี่ยนแปลงทั้งหมด และมีการแก้ไขเอกสารที่เกี่ยวข้อง - ประเมินผลและสอบทานระบบงานหรือโปรแกรมภายหลังจากเริ่มใช้งานในระยะเวลาหนึ่ง
การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์(Operation)	<ul style="list-style-type: none"> - ข้อมูลสูญหายหรือถูกทำลาย - ข้อมูลผิดพลาดหรือไม่สมบูรณ์ - ระบบหยุดชะงักการทำงาน 	<ul style="list-style-type: none"> - การประมวลผลระบบงาน โดยจัดทำตารางการประมวลผลและมีการบันทึกข้อมูลการทำงานเพื่อใช้ในการสอบทาน - การสำรองข้อมูลโดยกำหนดนโยบายเกี่ยวกับการสำรองข้อมูลและการกู้คืนข้อมูล จัดทำตารางเวลาการสำรองข้อมูล จัดเก็บข้อมูลสำรองไว้นอกสถานที่ มีการทดสอบข้อมูลสำรอง กำหนดเงื่อนไขในการนำเทปหรือดิสก์กลับมาใช้ใหม่ จัดทำสารบบสำหรับเทปหรือดิสก์ที่จัดเก็บไว้ และมีการกำหนดขั้นตอนการทำงานที่เป็นลายลักษณ์อักษร ในการกู้คืนข้อมูลและเริ่มต้นระบบงานใหม่รวมทั้งบันทึกการทำงานที่เกี่ยวข้องเพื่อใช้ในการสอบทาน - การจัดการปัญหาของระบบ ผู้ปฏิบัติงานคอมพิวเตอร์ควรมีการพิจารณาถึงสาเหตุของปัญหาหรือข้อผิดพลาดที่เกิดขึ้นเพื่อส่งต่อให้ผู้ที่เกี่ยวข้องทำการแก้ไข
การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์(Physical)	<ul style="list-style-type: none"> - ความเสียหายต่อคอมพิวเตอร์และเพิ่มข้อมูล - การเข้าถึงข้อมูลที่เป็นความลับไม่ได้อนุญาต 	<ul style="list-style-type: none"> - เก็บรักษาคอมพิวเตอร์ในห้องที่มีกุญแจปิดล็อกได้ - จำกัดการเข้าใช้งานเฉพาะบุคคลที่มีสิทธิ - ห้องคอมพิวเตอร์มีทางเข้าออกเพียง 1-2 ทางและมีการกำกับดูแลการผ่านเข้าออก - มีการตรวจสอบบัตรประจำตัวพนักงานเมื่อผ่านเข้าออกห้องคอมพิวเตอร์ - กำหนดให้ผู้เยี่ยมชมห้องคอมพิวเตอร์เซ็นชื่อในบันทึกเวลาเข้าออก

		<ul style="list-style-type: none"> - ติดตั้งระบบสัญญาณเตือนภัย - จำกัดสิทธิการใช้โทรศัพท์ เครื่องเทอร์มินัล และคอมพิวเตอร์ - ติดตั้งกุญแจล็อกเครื่องคอมพิวเตอร์และ อุปกรณ์
		<ul style="list-style-type: none"> - การควบคุมสภาพแวดล้อมในการทำงาน ของเครื่องคอมพิวเตอร์ เช่น การควบคุม อุณหภูมิ และการติดตั้งระบบป้องกันเพลิง ไหม้ เป็นต้น
การควบคุมการเข้าถึงระบบงาน (Logical Access)	เข้าใช้ระบบงานโดยไม่ได้ รับอนุญาต	<ul style="list-style-type: none"> - ตรวจสอบความมีตัวตน (Authentication) - การกำหนดสิทธิ (Authorization) - การบันทึกกิจกรรมต่าง ๆ (Audit Logging)