ครั้งที่55 3/2566

3.1 ให้บอกความเสี่ยง กับข้อเสนอแนะจากเหตุการณ์ต่อไปนี้

1) พนักงานลาออก ฝ่ายบบุคคลแจ้งฝ่ายสารสนเทศแล้ว แต่ฝ่ายสารสนเทศได้ลบข้อมูลพนักงานออกหลังจากนั้น 15 วัน

2) บริษัทมีการสำรองข้อมูลเพียงที่เดียวคือสำนักงานใหญ่

3) บริษัทมีวางแผนเพื่อกู้ระบบสารสนเทศ แต่ไม่เคยมีการปฏิบัติตามแผนที่กำหนดไว้

4) บริษัทไม่ได้แยกส่วนงานแก้ไขโปรแกรม กับระบบงานจริง และโปรแกรมเมอร์มีสิทธิ์เข้าระบบงานจริงได้

5) บริษัทมีระบบ Log file โดยมีการตั้งค่าให้มีการsave log ระบบจะเก็บรักษาไว้ทุก 90 วัน แต่serverแต่ละเครื่องตั้งเวลาในคอมไม่ตรงกัน

ความเสี่ยง	ข้อเสนอแนะ
1) พนักงานลาออก ฝ่ายบบุคคลแจ้งฝ่ายสารสนเทศแล้ว แต่ฝ่ายสารสนเทศได้ลบข้อมูลพนักงานออกหลังจากนั้น 15 วัน **ความเสี่ยง** ในช่วง 15 วันหลังจากพนักงานลาออก พนักงานดังกล่าวซึ่งถือเป็นคนที่ไม่มีสิทธิ์สามารถเข้าสู่ระบบงานบริษัท และทำการแก้ไขเปลี่ยนแปลงข้อมูลในระบบงานโดยไม่ได้รับอนุญาตได้ ทำให้งบการเงินไม่ถูกต้อง	บริษัทต้องกำหนดนโยบายควบคุมการใช้ Password โดยกำหนดให้เจ้าหน้าที่ฝ่ายระบบสารสนเทศ จะต้องลบข้อมูล และ Password ของพนักงานที่ลาออกทันทีที่มีผลตามวันที่ในใบลาออก เพื่อป้องกันไม่ให้คนที่ไม่มีสิทธิ์ซึ่งลาออกไปแล้ว เข้ามาแก้ไขเปลี่ยนแปลงข้อมูลในระบบงานของบริษัท
2) บริษัทมีการสำรองข้อมูลเพียงที่เดียวคือสำนักงานใหญ่ **ความเสี่ยง** หากข้อมูลสำรองไว้ที่สำนักงานใหญ่เสียหาย หรือถูกทำลาย บริษัทจะไม่สามารถดำเนินงานได้อย่างต่อเนื่อง	บริษัทควรสำรองข้อมูลอีก 1-2 ชุดไว้ในที่ปลอดภัย โดยแยกจัดเก็บต่างหากจากที่สำนักงานใหญ่ หากข้อมูลสำรองที่สำนักงานใหญ่เสียหาย หรือถูกทำลาย ก็สามารถนำข้อสำรองข้อมูลที่เก็บไว้ภายนอกมาลงในระบบ เพื่อดำเนินธุรกิจต่อไปได้อย่างต่อเนื่อง
3) บริษัทมีวางแผนเพื่อกู้ระบบสารสนเทศ แต่ไม่เคยมีการปฏิบัติตาม	บริษัทควรทำการทดสอบหรือซักซ้อมแผนการกู้ระบบสารสนเทศอย่างสม่ำเสมอทุกปี เพื่อเตรียมความพร้อมทั้งด้านระบบสำรองข้อมูล บุคลากร และสถานที่ เพื่อรองรับเหตุการณ์ที่อาจก่อให้เกิดความเสียหายที่รุนแรงต่อระบบคอมพิวเตอร์ เช่น ไฟไหม้ น้ำท่วม ระบบล่ม เป็นต้น การทดสอบแผนการกู้ระบบสารสนเทศเป็นการ

ความเสี่ยง - หากเกิดเหตุการณ์ภัยธรรมชาติหรือความเสียหายกับระบบคอมพิวเตอร์ของบริษัท จะทำให้ไม่สามารถกู้ระบบได้ภายในระยะเวลาที่เหมาะสม หรืออาจไม่สามารถกู้กลับมาใช้ใหม่ได้เลย - ระบบสารสนเทศ หรือธุรกิจอาจหยุดชะงัก ส่งผลกระทบต่อความอยู่รอดของบริษัท	ควบคุมเชิงแก้ไข จะช่วยทำให้บริษัทมีระบบสารสนเทศใช้งานอย่างต่อเนื่อง หรือสามารถกู้ระบบกลับมาใช้ใหม่ภายในระยะเวลาที่เหมาะสม
4) บริษัทไม่ได้แยกส่วนงานแก้ไขโปรแกรม กับระบบงานจริง โปรแกรมเมอร์มีสิทธิ์เข้าระบบงานจริงได้ **ความเสี่ยง** โปรแกรมเมอร์ ซึ่งเป็นผู้ที่ไม่มีหน้าที่เกี่ยวข้องกับระบบงานจริง สามารถเข้าไปแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือทำการทุจริตในระบบจริงได้ ทำให้งบการเงินไม่ถูกต้อง	บริษัทควรแบ่งแยกหน้าที่ระหว่างงานแก้ไขโปรแกรมของฝ่ายสารสนเทศ(IT) กับงานที่เกี่ยวข้องกับระบบงานจริงของผู้ใช้งาน(User) ให้ชัดเจน รวมถึงกำหนดลักษณะหน้าที่ความรับผิดชอบ (Job description)ของเจ้าหน้าที่ฝ่ายสารสนเทศ(IT)และผู้ใช้งาน(User)ด้วย ห้ามโปรแกรมเมอร์ เข้าสู่ระบบงานจริง ผู้ใช้งาน(User) เนื่องจากโปรแกรมเมอร์เป็นผู้ที่มีทักษะทางเทคนิคด้านคอมพิวเตอร์ สามารถแก้ไขระบบงานและข้อมูลได้ และถือเป็นผู้ที่ไม่มีหน้าที่เกี่ยวกับระบบงานจริง
5) บริษัทมีระบบ Log file โดยมีการตั้งค่าให้มีการ save log ระบบจะเก็บรักษาไว้ทุก 90 วัน และ serverแต่ละเครื่องตั้งเวลาไม่ตรงกัน **ความเสี่ยง** - ทำให้ข้อมูลใน Log fileถูกลบทิ้งหลังจากพ้นกำหนด 90 วันไปแล้ว ทำให้ไม่สามารถติดตามตรวจสอบรายการที่ผิดปกติ หรือน่าสงสัยย้อนหลังได้ - การที่ serverแต่ละเครื่องตั้งเวลาไม่ตรงกัน ทำให้ข้อมูลในระบบงานไม่ตรงความเป็นจริง ข้อมูลไม่น่าเชื่อถือ ยากในการตรวจสอบ และติดตามรายการที่ผิดปกติ หรือน่าสงสัยย้อนหลัง ส่งผลในการวิเคราะห์รายการผิดพลาด มีความล่าช้าในการตรวจสอบ และแก้ไขปัญหาไม่ทันเหตุการณ์	- บริษัทควรกำหนดระยะเวลาในการจัดเก็บ Log file ให้เหมาะสมตามความสำคัญ และความต้องการใช้ข้อมูล เช่น ข้อมูลที่ใช้บ่อยหรือไม่ใช้บ่อย หรือตามกฎหมายที่เกี่ยวข้อง เป็นต้น - บริษัทควรตรวจสอบและตั้งค่าเวลาserverให้สอดคล้องกันระหว่างเครื่องคอมพิวเตอร์ทุกเครื่องของบริษัท และให้มีการปรับเปลี่ยนเวลา serverให้ตรงกันในทุกเครื่อง และทุกครั้งที่มีการตั้งค่าหรือปรับเปลี่ยนเวลาในระบบ

3.2 ให้บอกความเสี่ยง และการใช้Programed control ช่วยในการควบคุมจากเหตุการณ์ต่อไปนี้ (10 คะแนน)

1) พนักงานบันทึกรายการขายผิด โดยบันทึกยอดติดลบ

2) ไม่สามารถคำนวณค่าเสื่อมราคาของPPE ได้ เพราะพนักงานใส่อายุการใช้งานเป็นตัวอักษร

3) พนักงานบันทึกยอดรับชำระเงินเกินกว่ายอดหนี้ของลูกหนี้ทำให้ลูกหนี้ติดลบ เนื่องจากไม่ได้ให้เครดิตไว้

4) พนักงานออกใบแจ้งหนี้ไม่ตรงกับใบส่งของ

5) ขายสินค้าให้กับลูกค้าที่ยังไม่เคยอนุมัติสินเชื่อ

ความเสี่ยง	Program check
1) พนักงานบันทึกรายการขายผิด โดยบันทึกยอดติดลบ	ใช้ Sign check ตรวจสอบหลังการทำรายการนั้น หากยอดคงเหลือติดลบ โปรแกรมระบบงานจะติดเครื่องหมาย (Flagged) ในรายการนั้น และปฏิเสธการทำรายการ แต่หากหลังการทำรายการนั้น ยอดคงเหลือไม่ติดลบระบบจะอนุมัติให้ทำรายการได้
2) ไม่สามารถคำนวณค่าเสื่อมราคาของPPE ได้ เพราะพนักงานใส่อายุการใช้งานเป็นตัวอักษร	ใช้ Type check การตรวจคาแรกเตอร์ของฟิลด์อายุการใช้งานที่บันทึกนำเข้าว่ามีค่าเป็นตัวเลขหรือไม่ หากมีตัวอักษรปนมาระบบจะไม่รับค่า แต่หากไม่มีตัวอักษรปนมาระบบจะอนุมัติให้ทำรายการได้
3) พนักงานบันทึกยอดรับชำระเงินเกินกว่ายอดหนี้ของลูกหนี้ทำให้ลูกหนี้ติดลบ เนื่องจากไม่ได้ให้วงเงินเครดิตไว้	ใช้ Limit check ตรวจปริมาณ และยอดหนี้ของลูกหนี้ที่บันทึกเกินกว่าวงเงินยอดหนี้ที่กำหนดไว้หรือไม่ หากเกินระบบจะปฏิเสธหรือส่งให้อนุมัติใหม่ แต่หากไม่เกินระบบจะอนุมัติให้ทำรายการได้ * บริษัทจะต้องกำหนดวงเงินเครดิตให้กับลูกหนี้แต่ละรายก่อน
4) พนักงานออกใบแจ้งหนี้ไม่ตรงกับใบส่งของ	ใช้ Relationship check การตรวจความสัมพันธ์ของข้อมูลใบแจ้งหนี้กับรายการใบส่งของ หากไม่ตรงกันระบบจะติดเครื่องหมาย (Flagged) ในรายการนั้นให้ทราบและปฏิเสธการทำรายการ แต่หากตรงกันระบบจะอนุมัติให้ทำรายการได้
5) ขายสินค้าให้กับลูกค้าที่ยังไม่เคยอนุมัติสินเชื่อ	ใช้ Existence ตรวจรหัสลูกค้าที่บันทึกนำเข้าระบบงานว่าเคยได้รับอนุมัติสินเชื่อ และบันทึกในระบบแล้วหรือไม่ หากเป็นรหัสลูกค้าที่ยังไม่เคยอนุมัติสินเชื่อ ระบบจะปฏิเสธการทำรายการ แต่หากเป็นรหัสลูกค้าที่เคยอนุมัติสินเชื่อแล้ว ระบบจึงจะอนุมัติให้ทำรายการได้