9

มุมมองของความเสี่ยงด้านคอมพิวเตอร์ จากกิจกรรมที่เกิดขึ้น และลักษณะของการควบคุมภายใน

ความเสี่ยงของการดำเนินงานด้านคอมพิวเตอร์ ที่มีผลกระทบต่อการควบคุม (Control risks)

ความเสี่ยง คือ เหตุการณ์ที่อาจเกิดขึ้นได้ภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลเสียหายหรือสร้างความล้มเหลวให้แก่ส่วนรวมหรือส่วนบุคคล ความเสี่ยงหรือมูลเหตุที่สร้างความเสียหายให้แก่ EDP หมายถึง เหตุการณ์ อุบัติเหตุ หรือการกระทำที่มีผลกระทบในทางที่เสียหายต่อ Computer system และ Data ซึ่งสามารถแบ่งออกเป็นประเภทใหญ่ได้ 6 ประเภท คือ

แนวความคิดในการศึกษาเรื่อง "ความเสี่ยง" ต่าง ๆ จะทำให้มีการวิเคราะห์ผลกระทบจากความเสี่ยงและความเสียหายต่าง ๆ ซึ่งจะทำให้ฝ่ายบริหารสามารถพิจารณาจุด "ควบคุม" และกำหนดระเบียบและกฎเกณฑ์ต่าง ๆ ขององค์กรได้อย่างเหมาะสม ดังนี้

1. ภัยธรรมชาติ เป็นเหตุการณ์ที่ไม่สามารถหลีกเลี่ยงได้ เช่น แผ่นดินไหว พายุ น้ำท่วม เป็นต้น การป้องกันความเสี่ยงประเภทนี้ได้แก่ พยายามหลีกเลี่ยงพื้นที่ที่คาดว่าจะเกิดเหตุที่กล่าว ข้อมูลทางสถิติเกี่ยวกับภัยพิบัติในพื้นที่ตั้ง Computer จึงมีประโยชน์อย่างมากต่อการประเมินเหตุการณ์ หรือกำหนด Emergency & Recovery plans ไว้ล่วงหน้า เพื่อบรรเทาความเสียหาย และกลับคืนสภาพปกติได้รวดเร็ว

2. มนุษย์ เป็นเหตุการณ์ที่เกิดจากการกระทำโดยตั้งใจและไม่ได้ตั้งใจ เช่น เจตนาทำลาย Computer, data, files หรือ programs ให้เสียหายจนใช้งานไม่ได้ หรือการปฏิบัติงานที่ไม่ถูกต้อง ไม่เหมาะสม ก็อาจนำไปสู่ความเสียหายได้เช่นกัน การป้องกันสามารถกระทำได้โดยการสร้างระบบการควบคุมและระเบียบการปฏิบัติงานที่รัดกุม

3. เทคโนโลยี เทคโนโลยีใหม่ ๆ มีส่วนทำให้การปฏิบัติมีประสิทธิภาพและอำนวยความสะดวกรวดเร็วให้แก่ผู้ใช้ แต่ในขณะเดียวกันก็เพิ่มความเสี่ยงใหม่ ๆ ขึ้น เช่น ข้อมูลอาจถูกทำลายหรือเปลี่ยนแปลงโดยสาเหตุจากความวิปริตของ Hardware จนเป็นเหตุให้แผ่น Disk เสียหาย เทคโนโลยีก่อให้เกิดความเสี่ยงทั้งทางด้าน Hardware และ Software ซึ่งอาจจะเนื่องมาจากตัวของมันเอง หรือจากผู้ใช้ที่ไม่มีความสามารถ การป้องกันสามารถทำได้โดยการเข้มงวดการเลือกระบบคอมพิวเตอร์ หรือจัดให้มี Maintenance program เป็นต้น

4. ระเบียบปฏิบัติงาน การปฏิบัติงานที่ไม่เป็นไปตามระเบียบและพิธีการที่กำหนด หรือการกำหนดระเบียบปฏิบัติงานที่ไม่เหมาะสม เป็นเหตุให้เกิดความผิดพลาดในการปฏิบัติงานได้ ซึ่งอาจมีผลกระทบต่อการบริหารและการดำเนินงาน ตลอดจนฐานะและความมั่นคงขององค์กรได้

5. การจัดองค์งาน เกิดจากการมอบหมายอำนาจหน้าที่ ความรับผิดชอบ และการติดต่อประสานงานที่ไม่เหมาะสม เช่น 2 หน่วยงานมีหน้าที่และความรับผิดชอบเหมือนกัน ผลก็คือจะไม่มีหน่วยงานใดปฏิบัติหน้าที่ได้อย่างสมบูรณ์ และก่อให้เกิดการผิดพลาด การป้องกันสามารถทำได้โดยการให้มีข้อบัญญัติเกี่ยวกับอำนาจ หน้าที่ ความรับผิดชอบ และการประสานงานที่ดี จะช่วยลดข้อผิดพลาดลงได้

6. **ระบบงาน** ความเสี่ยงที่เกิดจากระบบงานมักจะเกี่ยวข้องกับ Functions หรือ Transactions และ Data ของระบบงานนั้น เช่น บันทึกรายการไม่ถูกต้อง เป็นต้น ดังนั้นการป้องกันและการควบคุมในระบบงานนั้น ปกติมักจะรวมอยู่เป็นส่วนหนึ่งของระบบงาน (Computerized Application) อยู่แล้ว เพื่อให้สามารถป้องกันเหตุร้ายหรือค้นพบได้ในทันที โดยเฉพาะระบบงานที่เป็นลักษณะ Online

เมื่อกล่าวถึงระบบงานเราควรจะเข้าใจตรงกันว่า งานที่เริ่มตั้งแต่การพัฒนาระบบงานไปจนถึงขั้นการบำรุงรักษาและแก้ไขระบบงานเพื่อจัดงานนั้นออกใช้งานแล้ว

เมื่อทราบมูลเหตุความเสี่ยงแล้ว จะต้องพิจารณาว่าจะจัดการกับความเสี่ยงได้อย่างไร การจัดการกับความเสี่ยงมี 2 แบบ คือ

1. Risk Financing คือ การโอนความเสี่ยงไปให้บุคคลอื่น เช่น การประกันภัย เป็นต้น ปกติการประกันภัยมักจะถูกใช้ควบคู่ไปกับการควบคุมความเสี่ยงเสมอ ทั้งนี้เพราะการควบคุมแต่เพียงอย่างเดียวไม่อาจป้องกันหรือบรรเทาความเสียหายได้ร้อยเปอร์เซ็นต์ หรือได้ทุกกรณี เราไม่อาจเสี่ยงต่อความเสียหายได้แม้จะมีโอกาสเกิดน้อยก็ตาม เนื่องจากความเสียหายบางอย่างมีมูลค่าสูงเกินกว่าที่จะยอมรับได้ เช่น เครื่องคอมพิวเตอร์ถูกทำลายเสียหายจนใช้การไม่ได้ เป็นต้น

2. Risk control คือ การใช้มาตรการทางด้านการควบคุมเพื่อกำจัดหรือลดความเสี่ยงและความเสียหาย

การควบคุมมีความมุ่งหมายเพื่อขจัดหรือลดความเสี่ยงและความเสียหายที่อาจเกิดกับองค์กร อย่างน้อยที่สุดหากมีภัยและความเสียหายเกิดขึ้น ก็อยู่ในวิสัยที่จะรับได้ หรือทำให้กลับคืนสู่สภาวะปกติได้ สิ่งที่ควรพิจารณาเกี่ยวกับการควบคุมมีดังนี้

1. จุดที่ควบคุม เราไม่สามารถควบคุมตัวความเสี่ยงได้โดยตรง แต่ควบคุมจุดที่เกิดเหตุและความเสียหายได้ เพราะฉะนั้นจุดที่เกิดความเสี่ยงและจุดที่มีการควบคุม จึงเป็นจุดเดียวกัน การเลือกจุดที่ควรควบคุมมีอยู่ 2 แนวทาง ขึ้นอยู่กับความเสี่ยงว่าเป็นความเสี่ยงของระบบคอมพิวเตอร์ (EDP resource) หรือระบบงานคอมพิวเตอร์ (EDP applications)

ก. ความเสี่ยงของระบบคอมพิวเตอร์ ส่วนใหญ่จะเกิดกับ Hardware, Software, Data Files และ Operation เป็นต้น

ข. ความเสี่ยงของระบบงานคอมพิวเตอร์ ส่วนใหญ่จะเกิดกับ Transactions หรือ Functions ของระบบงาน อันเนื่องมาจากข้อมูลถูกเปลี่ยนแปลงแก้ไข รายการถูกดึงออกไปจากระบบงาน ข้อมูลบางส่วนหายไป เป็นต้น จุดที่ควรควบคุมก็คือจุดที่อาจทำให้ Transactions มีการเปลี่ยนแปลง

2. ลักษณะของการควบคุม การควบคุมโดยทั่วไปอาจแบ่งออกได้เป็น 2 ประเภท คือ การควบคุมทางด้านการเงิน (Financial controls) และการควบคุมการปฏิบัติงาน (Operation controls)

การควบคุมทางด้านการเงิน (Financial controls) หมายถึง การควบคุมเพื่อให้รายการทางการเงินถูกต้องสมบูรณ์ และเป็นไปตามหลักการบัญชีที่ยอมรับกันโดยทั่วไป

การควบคุมการปฏิบัติงาน (Operation controls) หมายถึง การควบคุมให้มีการปฏิบัติงานเป็นไปอย่างมีประสิทธิผลและประสิทธิภาพ

นอกจากนั้นการควบคุมอาจแบ่งออกได้เป็น 3 วิธี คือ

ก. การป้องกันหรือหลีกเลี่ยงมูลเหตุที่นำไปสู่ความเสียหาย (Prevention controls) ควรใช้กับความเสี่ยงที่ก่อให้เกิดความเสียหายและยากต่อการแก้ไข หรือเสียค่าใช้จ่ายมาก เช่น การป้องกันมิให้เข้าไปในห้องคอมพิวเตอร์และใช้เครื่องโดยไม่ได้รับอนุญาต เป็นต้น การป้องกันอาจทำได้โดยให้มียามรักษาการณ์และออก Password ให้แก่ผู้มีสิทธิใช้เครื่อง เป็นต้น

ข. การตรวจให้พบปัญหาที่อาจนำไปสู่ความเสียหาย (Detective controls) ควรใช้กับความเสี่ยงที่ยังไม่ได้เกิดความเสียหาย โดยทันที หรืออาจไม่เกิดความเสียหายร้ายแรง หรือถ้าจะคิดป้องกันก็คงทำได้ยากและเสียค่าใช้จ่ายมาก เช่น การป้อนข้อมูล การป้องกันมิให้มีการป้อนข้อมูลผิดพลาด ย่อมทำได้ยากกว่าตรวจสอบว่ามีข้อมูลผิดพลาดหรือไม่ เป็นต้น การควบคุมในลักษณะนี้มักใช้เพื่อเสริมให้การควบคุมในแบบแรกมีประสิทธิภาพมากยิ่งขึ้น ข้อที่ควรระวังก็คือ การควบคุมนี้เป็นเพียงเครื่องมือค้นพบปัญหา แต่หากปัญหานั้นไม่ได้รับการแก้ไขหรือแก้ไขไม่ถูกต้อง ความเสียหายก็ยังเกิดขึ้นได้อีก โดยเฉพาะกรณีที่มีเจตนาละเมิดหรือ Override การควบคุมนั้น

ค. การตรวจให้พบมูลเหตุหรือปัญหาที่นำไปสู่ความเสียหาย และพร้อมกับกำหนดวิธีการแก้ไขล่วงหน้า (Detective and corrective controls) การควบคุมวิธีนี้ดีกว่าวิธีที่สอง เพราะว่าปัญหาที่ตรวจพบจะได้รับการแก้ไขอย่างเหมาะสมและรวดเร็ว เช่น การควบคุมความเสี่ยงอันเกิดจากไฟไหม้ โดยการติดตั้งเครื่อง Fire alarm แต่เพียงอย่างเดียวยังไม่เพียงพอ ควรจัดติดตั้งเครื่องดับไฟอัตโนมัติควบคู่กันไปด้วย ซึ่งจะทำให้สามารถควบคุมความเสียหายได้ดีขึ้น

3. วิธีปฏิบัติในการควบคุม แบ่งออกได้เป็น 7 วิธี คือ

ก. Redundancy check หมายถึง การกระทำในสิ่งเดียวกันอย่างน้อย 2 ครั้ง แต่ต่างวิธีกัน แล้วเปรียบเทียบผลลัพธ์ที่ได้ เช่น การคำนวณตัวเลขต่าง ๆ เป็นต้น

ข. Verify หมายถึง การตรวจสอบกับหลักฐานที่เชื่อถือได้ เช่น ตรวจสอบเลขที่บัญชีกับ Data base เป็นต้น

ค. Confirmation หมายถึง การให้ยืนยันความถูกต้อง เช่น กำหนดให้ผู้ป้อนรายการข้อมูลในระบบ Online ยืนยันความถูกต้องของข้อมูลที่ปรากฏอยู่บนจอ Terminal ก่อนที่ข้อมูลจะเข้าสู่ระบบ

ง. Recalculation หมายถึง การคำนวณซ้ำในจุดที่มีการคำนวณ ปกติจะใช้คำนวณด้วยมือ (Manual) แล้วเทียบกับการคำนวณด้วยคอมพิวเตอร์ หรือสลับกันโดยสูตรในการคำนวณเหมือนกัน

จ. Limit หมายถึง การกำหนดขอบเขตของหน้าที่ การกระทำหรือรายการไว้แน่นอน ซึ่งสามารถทำได้ทั้งปริมาณและจำนวนเงิน เวลาและความถี่ เช่น การยินยอมให้ป้อนรหัสประจำตัว (Password) ผิดพลาดได้ไม่เกิน 3 ครั้ง ครั้งที่ 4 เครื่องจะยึดบัตร เป็นต้น

ฉ. Containment หมายถึง การสกัดกั้นมิให้ความเสียหายระบาดหรือลุกลามไปยังที่อื่น เช่น การมีเครื่องคอมพิวเตอร์ตั้งอยู่ใกล้กัน 2 เครื่อง ควรกั้นผนังทนไฟระหว่างเครื่องคอมพิวเตอร์ เพื่อป้องกันมิให้ไฟลุกลามจากเครื่องหนึ่งไปอีกเครื่องหนึ่ง เป็นต้น

ช. Fallback หมายถึง การกำหนดวิธีปฏิบัติหรือระบบสำรอง ในกรณีที่เกิดความเสียหายบางส่วนหรือทั้งหมด เพื่อให้สามารถดำเนินงานต่อไปได้ เช่น กรณี Data base ถูกทำลายหรือเสียหาย ให้ทำระบบสำรอง (Backup) มาทำการ Copy เพื่อจะได้ดำเนินงานต่อไป เป็นต้น

4. การควบคุมที่ดีควรมีหลักฐานที่แสดงให้เห็นว่าได้ควบคุมจริง และเป็นไปตามแผนงานที่วางไว้ตัวอย่างบางประการที่เกิดจากความเสี่ยงของการดำเนินงานด้านคอมพิวเตอร์ที่มีผลกระทบต่อการควบคุม (Control risk)

ตัวอย่างของการวิเคราะห์ความเสี่ยง/ความเสียหาย ของการประมวลข้อมูลด้วยระบบคอมพิวเตอร์ (จากจุดที่อาจก่อให้เกิดความเสียหาย)

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
	การจัดองค์การ	
1	Structure	- ไม่มีการมอบหมายอำนาจหน้าที่และความรับผิดชอบ - ไม่ได้มอบหมายอำนาจหน้าที่และความรับผิดชอบเป็นลายลักษณ์อักษร - ไม่ได้จัดทำ Job description และ Organization charts
2	Policies & Procedures	- ไม่มีแผนงานประจำปี หรือไม่ปฏิบัติตามแผนงาน - ไม่มีการจัดทำงบประมาณประจำปี หรือไม่ปฏิบัติตามงบประมาณ - ไม่มีนโยบายและระเบียบปฏิบัติงานประมวลข้อมูลด้วยคอมพิวเตอร์ - ไม่มีระเบียบปฏิบัติในการจ้างงานและระบบเงินเดือน - ไม่มีการวิเคราะห์ความเสี่ยงและการควบคุมทรัพย์สินแต่ละประเภท
	การพัฒนาระบบงาน	
3	System specification	- Syst. designer ไม่เข้าใจความต้องการของ User หรือเข้าใจคลาดเคลื่อน - Syst. designer ไม่ได้ใช้เครื่องฯ และคน ให้เป็นประโยชน์มากที่สุด
4	Programming	- Programmer เข้าใจคำขอแก้ไขโปรแกรมผิดพลาด - Programmer ทำการแก้ไข Object program โดยตรง - มีการแอบแก้ไขเพิ่มเติมโปรแกรม เป็นเหตุให้โปรแกรมขาด คุณสมบัติทางด้านการป้องกันความ

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
		ปลอดภัย เช่น แฟ้ม ข้อมูลที่สำคัญถูกลบล้างออกไปหมดทันทีที่มีการ Run งาน - Programmer มิได้จัดทำเอกสารประกอบโปรแกรมหรือการแก้ไขโปรแกรม หรือทำอย่างไม่เป็นทางการ
5	Testing	- ไม่ได้ทดสอบโปรแกรมอย่างเพียงพอก่อนนำออกใช้งาน - การแก้ไขโปรแกรมอาจก่อให้เกิดความผิดพลาดที่คาดไม่ถึง - ไม่ได้รวบรวมข้อมูลที่ใช้ในการทดสอบ ผลการทดสอบ และ เอกสารรับรองความถูกต้องของโปรแกรมไว้เป็นหลักฐาน
6	Documentation	- เอกสารสนับสนุนระบบงานไม่เพียงพอ เป็นเหตุให้การแก้ไขโปรแกรมไม่ถูกต้อง หรือไม่สามารถกระทำได้ - เอกสาร ฯ ไม่ชัดเจน
7	Conversion	- ไม่สามารถนำโปรแกรม/ระบบงานออกใช้ได้ทันความต้องการ - เกิดข้อมูลผิดพลาดระหว่างทำการ Conversion - สูญเสีย File integrity
	การปฏิบัติการคอมพิวเตอร์	
8	Hardware	- ทำการ Maintenance ในขณะที่ยัง Run งาน Online ตามปกติ และไม่ได้แยก Hardware ส่วนนั้นออกจากระบบ - ในขั้นตอนการทำงาน Tape ไม่ได้มีการบันทึกสถานะของ Tape ไว้ทั้งหมด - ตั้งใจหรือประมาท ให้ชื่อ Media ไม่ถูกต้อง เป็นเหตุให้ข้อมูลใน Media ถูกล้างออกไปหมด - ไม่มีการตรวจสอบความถูกต้องของ Internal label

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
		- Expiry date ใน File ไม่ถูกต้อง เป็นเหตุให้ข้อมูลถูกล้างออกไปหมด - มี Write rings ค้างอยู่ในม้วน Tape หรือ Mount เทปผิดพลาด เป็นเหตุให้การประมวลข้อมูลหรือ Update ข้อมูลผิดพลาด
9	Software (O/S)	- มีการใช้ File เดียวกันพร้อมกัน 2 งาน ทำให้ข้อมูลอาจสะดุด - ไม่ได้ใช้ Controls ที่มีอยู่ใน O/S ให้เป็นประโยชน์ - ไม่สามารถปรับปรุง O/S ให้เป็นไปตามที่ต้องการได้
10	Operations	- Restart ไม่ถูกต้องหรือโดยประมาท เป็นเหตุให้ไม่ทราบสถานะของการทำรายการที่ค้างอยู่ - Operator ป้อนข้อมูลผิดพลาดเข้าไปใน Console เช่น ยกเลิกงานผิด - ใช้โปรแกรมที่ไม่ใช่ชุดปัจจุบัน Run งาน - ใช้ข้อมูลไม่ถูกต้องกับโปรแกรม - Operator ข้ามหรือละเลยการควบคุมความปลอดภัย เช่น ไม่ยอมให้ Write rings บน Tape - Operator เรียนรู้งานอย่างไม่ถูกต้อง ทำให้ข้อมูลใน Master file คลาดเคลื่อน หรือถูกลบทิ้งไป - Mount เทปโดยไม่มี Write ring protection
11	Backup recovery	- O/S อาจเสียหายหรือผิดปกติจนไม่สามารถรักษา Audit trail ไว้ได้ครบถ้วน เช่น ไม่ได้บันทึกการออก Output จาก Spooled storage devices - เมื่อทำ Restart หลังจากระบบล้มเหลวแล้ว O/S ไม่ได้ตรวจสอบสภาพของ Terminal location - File อาจถูก Read หรือ Write โดยที่ไม่ได้ Open - File อาจถูกทำลายระหว่างทำ Reorganize หรือ

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
		Release ข้อมูล - Record อาจถูกดึงหายไปจาก File ที่สำคัญโดยไม่มีหลักประกันว่าจะสามารถสร้างขึ้นได้ใหม่ - Temporary file ที่เกิดระหว่างประมวลผล อาจถูกลบล้างหรือแก้ไข เนื่องจากขาดการควบคุม หรือระบบคอมพิวเตอร์หยุดอย่างผิดปกติ
12	การรักษาความปลอดภัย	- Data หรือโปรแกรมถูกขโมยจากห้องคอมพิวเตอร์หรือที่เก็บอื่น - เครื่องฯ ถูกทำลายเสียหายโดยผู้บุกรุกจากภายนอกหรือพนักงานลูกจ้าง - ไม่มีการตรวจสอบผู้ที่จะเข้าไปใน EDP area - ไม่มีการป้องกันการใช้ Remote terminal - ผู้ไม่ได้รับอนุญาตอาจเข้าถึงระบบคอมพิวเตอร์โดยทางสายโทรศัพท์และ Password ของพนักงาน - User อาจเปิดเผย Password ของตัวเองโดยไม่รู้ตัว เช่น จดทิ้งไว้ในสถานที่เห็นได้ง่าย ปรากฏอยู่บน Print out หรือถูกสังเกตขณะที่ใช้งาน - User เปิด Terminal ทิ้งคาไว้ เปิดโอกาสให้ผู้ที่ไม่ได้รับอนุญาตเข้าไปใช้งานได้ทันที - พนักงานที่ถูกพักงานหรือออกจากงานแล้วยังสามารถเข้าถึงระบบได้อยู่ เนื่องจากชื่อและ Password ยังไม่ได้ถูกลบล้างออกไปจาก Tables หรือ Control lists - ไม่มีการติดตามหรือตรวจสอบความพยายามที่จะเข้าถึงระบบหรือ File โดยไม่ได้รับอนุญาต - Console operator อาจละเลย Label check แต่ไม่ปรากฏหลักฐานใน Security log - ไม่ได้กำหนดขอบเขต User ในการเข้าถึงระบบงาน (โปรแกรมและ Data) - ไม่มีการทบทวนความถูกต้องของรายการที่เป็นจำนวน

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
		เงินมาก ๆ หรือที่ผิดปกติ - ไม่มีการทบทวนรายงานวิเคราะห์การปฏิบัติงาน เพื่อดูว่า มีการละเมิดความปลอดภัยหรือไม่ - เจ้าพนักงานควบคุมความปลอดภัย เมื่อได้รับรายงานการละเมิดระบบการรักษาความปลอดภัย อาจสั่งการที่ไม่เหมาะสม เพราะไม่มีระเบียบปฏิบัติที่เป็นแบบแผนกำหนดไว้ - Operator ประทุษร้ายต่อเครื่องฯ - พนักงานอาจขโมยโปรแกรมไปใช้ประโยชน์ส่วนตัว เช่น นำออกไปขายให้บุคคลภายนอก - เจ้าหน้าที่บริหารศูนย์ฯ ใช้อุบายหรืออำนาจ ทำให้การควบคุมการปฏิบัติงานไม่มีผล เพื่อแก้ไขหรือนำข้อมูลออกมาใช้ - ไม่ได้เก็บเอกสารประกอบโปรแกรมที่สำคัญไว้ในที่ปลอดภัย - Programmers เพิ่มเติมข้อความพิเศษเข้าไปใน Programe เพื่อเปลี่ยนแปลงข้อมูลที่เกี่ยวกับตนเอง เช่น บัญชีเงินเดือน - Encryption key อาจถูกขโมย - ข้อความแปลกปลอมอาจถูกส่งเข้ามาในระบบ - O/S อาจถูกแก้ไขโดยไม่ได้รับอนุญาต ให้เสมียนป้อนรายการสามารถป้อนโปรแกรมเข้าไปทำลายหรือล้มล้างระบบ - Line อาจถูกตรวจสอบหรือติดตามความเคลื่อนไหวจากบุคคลที่ไม่ได้รับอนุญาต - ข้อมูลหรือโปรแกรมอาจถูกขโมยทางสายโทรศัพท์ - ข้อมูลอาจถูกเปลี่ยนแปลงแก้ไขจากการ Tapping โดยไม่ได้รับอนุญาต - Media ประเภทสารแม่เหล็ก อาจถูกทำลายสภาพหรือสถานะของแม่เหล็ก

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
13	Communications	- User ที่สามารถเข้าถึงข้อมูลรายตัวใน File อาจ List ข้อมูลทั้งหมดโดยไม่ได้รับอนุญาต เพื่อประโยชน์ส่วนตัว เช่น เพื่อขายรายชื่อและที่อยู่พนักงานให้บุคคลภายนอก - ข้อมูลอาจถูกส่งไปผิด Terminal โดยไม่ได้ตั้งใจ - Protocal ล้มเหลวจนไม่สามารถตรวจสอบความถูกต้องของ Transmitter หรือ Receiver ได้ - ในระหว่างที่การประมวลผลหยุดชะงักงันโดยไม่คาดคิด Network-controller อาจทิ้งข้อมูลบางส่วนค้างไว้ใน Memory โดยไม่มีการป้องกันใด ๆ

ระบบงานที่ประมวลข้อมูลด้วยคอมพิวเตอร์

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
1	Origination	- ไม่มีการนับจำนวนเอกสารหรือวิธีการควบคุม Source data อื่น - Data หรือ Transaction สูญหายหรือเพิ่มเติมขึ้นมาโดยไม่สามารถตรวจสอบได้ - ไม่ได้ตรวจสอบรายการที่มีจำนวนเงินผิดปกติ
2	Authorization	- ไม่มีหรือไม่ได้ปฏิบัติตามระเบียบคำสั่งในการมอบหมายอำนาจหน้าที่ - ไม่ได้ลงลายมือชื่อรับรองของผู้รับมอบอำนาจ - ไม่ควบคุมหรือจำกัดขอบเขตการเข้าถึงระบบงาน - ไม่มีระเบียบคำสั่งเกี่ยวกับการ Authorize - ไม่ได้ใช้เอกสารที่มีหมายเลขกำกับ หรือแบบฟอร์มเฉพาะ - ไม่มีการแบ่งแยกหน้าที่เพื่อป้องกันมิให้บุคคลใดบุคคลหนึ่ง สามารถควบคุมความถูกต้องของรายการได้แต่เพียงผู้เดียว - ไม่มีการทบทวนความถูกต้องของรายการ (Transactions) ก่อนนำไปประมวลผล - Password ของเจ้าหน้าที่บริหาร ปรากฏบนจอภาพของ Operator
3	Data Entry	- ผ่านรายการสำคัญโดยไม่ต้องขออนุมัติหรือควบคุมจากพนักงานขั้นบริหาร - ตรวจไม่พบข้อผิดพลาดในขณะที่ทำการป้อนรายการ - ข้อมูลที่ไม่ครบถ้วนหรือไม่ตรงตาม Format ยังสามารถผ่านเข้าไปได้เสมือนหนึ่งถูกต้อง - Record ที่พบข้อผิดพลาด เมื่อได้รับการแก้ไขแล้วอาจไม่ผ่านการตรวจสอบทั้ง Record อีกครั้ง

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
4	Processing	- ความผิดพลาดของโปรแกรมเป็นเหตุให้การประมวลข้อมูลผิดพลาด - ตรวจไม่พบข้อผิดพลาดที่น่าจะพบ - ข้อมูลบางอย่างที่อยู่นอกเหนือการกำหนดไว้ เช่น Code อาจถูกประมวลผลในลักษณะที่คาดไม่ถึง
5	File storage	- ไม่ได้ให้ชื่อกำกับไว้ ในที่สุดสูญหาย - จำนวน Records ไม่ตรงกับ Control totals - เป็น File ที่ผิด Version
6	Output	- ส่งรายงานให้ผิดคนหรือผิด Terminal - รายงานสูญหาย - วัสดุเหลือใช้ เช่น รายงานชุดสำเนาที่ไม่ได้ใช้ประโยชน์กระดาษคาร์บอนที่ใช้แล้ว ฯลฯ อาจได้รับการทำลายหรือ จำหน่ายออกไปไม่เหมาะสม

ความเสี่ยงของการดำเนินงาน
ด้านคอมพิวเตอร์ที่มีผลกระทบต่อการตรวจสอบ (Audit Risks)

ความเสี่ยงในแง่ของการตรวจสอบ (Audit risks) มีอยู่ 2 ประเภทใหญ่ ๆ คือ

1. เหตุการณ์ต่าง ๆ ที่ไม่น่าพอใจหรือไม่อาจยอมรับได้ เกิดขึ้นอยู่ในระบบงาน ซึ่งวิธีการตรวจสอบ (Audit Procedure) ไม่อาจตรวจพบได้

2. เหตุการณ์ที่ไม่น่าพอใจหรือไม่อาจยอมรับได้ ที่อาจตรวจพบได้โดยวิธีการตรวจสอบ แต่ผู้ตรวจสอบอาจเข้าใจเหตุการณ์หรือเงื่อนไข (Condition) ผิดพลาดหรือไม่ถูกต้องอย่างแท้จริง

ความเสี่ยงของการตรวจสอบคอมพิวเตอร์ (Risk in auditing EDP) จุดประสงค์ของการควบคุมต่าง ๆ ที่ใช้กับระบบงานคอมพิวเตอร์ยังคงเหมือนกับจุดประสงค์ในการควบคุมที่ใช้ในระบบงานทั่วไป สิ่งที่เปลี่ยนแปลงไปก็คือ วิธีการควบคุม (Methods of Control) เพื่อให้เหมาะสมกับลักษณะการทำงานด้วยเครื่องคอมพิวเตอร์ ซึ่งประกอบด้วยเรื่องต่าง ๆ ดังนี้

1. หลักฐานมีรูปแบบและลักษณะแตกต่างจากระบบงานที่ปฏิบัติด้วยมือ (Manual) มาก
2. มีเอกสาร (Hard copy) น้อยลง
3. เปลี่ยนแปลงการมอบหมายหน้าที่ความรับผิดชอบมากขึ้น
4. มีการควบคุมโดยเครื่องคอมพิวเตอร์ (Automated control)
5. มีลักษณะการทำงานแบบสม่ำเสมอ (ไม่ว่าจะถูกหรือไม่ถูก)

ความเสี่ยงของการตรวจสอบคอมพิวเตอร์มีประเภทต่าง ๆ ดังนี้

1. ความเสี่ยงอันเนื่องจากการแปลงข้อมูล (Data conversion risk) หมายถึงว่า การแปลงข้อมูลจากข้อมูลในเอกสารต่าง ๆ เป็นข้อมูลที่เครื่องคอมพิวเตอร์สามารถอ่านได้ อาจมีการแปลงข้อมูลผิด

2. ความเสี่ยงอันเนื่องจากการผิดพลาดซ้ำ (Repetition of Errors Risk) ความผิดพลาดอันเกิดขึ้นซ้ำ ๆ กันได้ เนื่องจากระบบงานคอมพิวเตอร์จะทำงานเป็นรูปแบบสม่ำเสมอ

3. ความเสี่ยงอันเนื่องจากการผิดพลาดเป็นทอด ๆ (Cascading of Error risk) ความผิดพลาดที่เกิดขึ้นในระบบงาน อาจมีผลกระทบกระเทือนข้อมูลอื่นในระบบงานนั้นให้เกิดความผิดพลาดด้วย

4. ความเสี่ยงอันเกิดจากการประมวลผลขาดตอน (Discontinuity of Processing risk) ความเพียงพอของการจัดทำ Backup และ Documentation ของระบบงาน ย่อมมีผลอย่างยิ่งต่อการประมวลผล ถ้า Documentation และการ Backup ไม่เพียงพอ อาจทำให้การประมวลผลขาดตอนได้

5. ความเสี่ยงอันเกิดจากผลทางเทคโนโลยี (Technological Risk) อาจมีการใช้เทคโนโลยีแบบผิด ๆ ซึ่งจะทำให้ผลการปฏิบัติงานผิดพลาดหรือขาดประสิทธิภาพ

6. ความเสี่ยงอันเกิดจากประพฤติไม่ชอบโดยอาศัยคอมพิวเตอร์ (Computer Abuse risk) อาจมีผู้ใช้คอมพิวเตอร์ไปในทางที่ไม่ชอบ เพื่อหาประโยชน์ให้แก่ตนเอง หรือก่อการทุจริตด้วยคอมพิวเตอร์

ตารางวิเคราะห์ความเสี่ยงและการควบคุมระบบงานที่ประมวลผลด้วยคอมพิวเตอร์

ความเสี่ยง (Risks) / กิจกรรม (resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	เอกสารปลอมหรือไม่ผ่านการอนุมัติ	เอกสารไม่ครบถ้วนและสมบูรณ์	เอกสารผิดพลาด				ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
Source Documents			X	X					การบันทึกบัญชีและยอดคงเหลือตามบัญชี ไม่ถูกต้องและหรือการทุจริต	**AUTHORIZATION** - มีแบบฟอร์มเอกสารเฉพาะ หรือแบบฟอร์มมาตรฐานที่มีหมายเลขกำกับ - มีการควบคุมการเข้าถึงแบบฟอร์มเปล่า โดยเฉพาะตราสารการเงิน เช่น สมุดเช็ค ดราฟท์ และตั๋วแลกเงิน เป็นต้น - มีการอนุมัติด้วยลายมือชื่อในเอกสารสนับสนุนรายการทุกประเภท - ไม่ควรให้เจ้าหน้าที่คนหนึ่งสามารถอนุมัติรายการได้หลายประเภท เช่น การเปิดบัญชี การปิดบัญชี หรือการแก้ไขรายการ เป็นต้น - แยกหน้าที่จัดทำเอกสารสนับสนุนรายการออกจากหน้าที่อื่น หรือไม่ให้ทำหน้าที่อย่างอื่น เช่น การป้อนรายการ หรือตรวจสอบรายงาน เป็นต้น
	X	X		X	X					**COMPLETE & ACCURACY** - มีการตรวจสอบข้อมูลในเอกสารสนับสนุนรายการโดยบุคคล - มีการควบคุมความครบถ้วนแบบ Batch Controls ได้แก่ - Source Document Counts - Record Counts - Total Values หรือ Control Totals - มีทะเบียนบันทึกรายละเอียดของ Batches - มีการตรวจสอบความถูกต้องของ Batch Totals โดยเปรียบเทียบ Manual กับ Computer Totals - มีการเก็บรวบรวมเอกสารสนับสนุนรายการ หรือตัวสำเนาเอกสารไว้ให้ครบถ้วนและเป็นระเบียบ เพื่อไว้ใช้ในการตรวจสอบภายหลัง หรือสร้างข้อมูลขึ้นใหม่

ความเสี่ยง (Risks) / กิจกรรม (Resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	เอกสารปลอมหรือไม่ผ่านการอนุมัติ	เอกสารไม่ครบถ้วนและสมบูรณ์	เอกสารผิดพลาด				ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
				X	X					**ERROR CORRECTION** - มีรายงานข้อมูลที่ผิดพลาด ผิดปกติ และข้อมูลที่ถูก reject ให้ user ตรวจสอบหาสาเหตุและทำการแก้ไขต่อไป - มีทะเบียนบันทึกรายการผิดพลาด - มีบัญชีพัก (Suspense A/C) สำหรับบันทึกรายการที่ผิดพลาดและถูก reject สิ้นวัน สำหรับติดตามและควบคุมการแก้ไขในวันถัดไป (Manual หรือ Computer) - มีการควบคุมและตรวจสอบความถูกต้องเช่นเดียวกับรายการปกติประจำวัน

ความเสี่ยง (Risks) / กิจกรรม (resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	รายการไม่ครบถ้วนและสมบูรณ์	รายการลอง หรือไม่มีเอกสารสนับสนุน	รายการเกิดขึ้นเองจากโปรแกรมในเครื่อง	รายการผิดพลาด			ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
Data Entry				X					การบันทึกบัญชีและยอดคงเหลือตามบัญชีไม่ถูกต้องและหรือ การทุจริต	**AUTHORIZATION** - มีการแยกหน้าที่ระหว่างการจัดทำเอกสารสนับสนุนรายการ การอนุมัติรายการ และการป้อนข้อมูล - Terminal อยู่ในที่ปลอดภัย และมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต - ใส่กุญแจเครื่อง Terminal หลังเสร็จงานแล้ว - มีการ Sign-on หรือ initiate เครื่อง Terminal โดยเจ้าหน้าที่ระดับหัวหน้าปฏิบัติการ ก่อนที่ Operator จะสามารถใช้เครื่องได้ - มีการใช้ Password ควบคุมและป้องกันการใช้เครื่อง Terminal โดยไม่ได้รับอนุญาต หรือเกินกว่าขอบเขตที่กำหนด - มีรายงานให้ติดตามและตรวจสอบการพยายามใช้ Terminal โดยไม่ได้รับอนุญาต หรือเกินกว่าขอบเขตที่กำหนด
	X	X	X		X	X			การบันทึกบัญชีและยอดคงเหลือตามบัญชีไม่ถูกต้องและหรือ การทุจริต	**COMPLETE & ACCURACY** - มี Screen Format สำหรับใช้ในการป้อนรายการ เพื่อให้ Operator สามารถป้อนรายการได้สะดวกและตรวจสอบความถูกต้องได้ด้วยสายตา - มีการตรวจสอบข้อมูลทุก Field โดยโปรแกรมคอมพิวเตอร์ Field ที่ควรทำการตรวจสอบ ได้แก่ - Transaction ID (Check digit) - Transaction Code - Transaction Date

ความเสี่ยง (Risks) / กิจกรรม (Resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	เอกสารปลอมหรือไม่ผ่านการอนุมัติ	เอกสารไม่ครบถ้วนและสมบูรณ์	เอกสารผิดพลาด	รายการผิดพลาด			ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
										- Amounts - Limit - Range - Signs - Balance - มีการตรวจสอบความครบถ้วนของรายการโดยวิธี Sequence Check (Manual หรือ Computer) - มีการตรวจสอบความครบถ้วนของรายการ โดยการตรวจสอบ Batch Total และ Terminal log. - Record counts - Total Value หรือ Control totals - มีข้อห้ามในการ Override รายการที่ไม่ถูกต้อง หรือให้อยู่ในอำนาจของเจ้าหน้าที่ระดับบริหาร และมี Automatic log สำหรับบันทึกรายการที่ถูก Override เพื่อให้สามารถทบทวนความเหมาะสมได้ในภายหลัง
						X			การบันทึกบัญชีและยอดคงเหลือตามบัญชีไม่ถูกต้อง	**ERROR COLLECTION** - มีคำอธิบายข้อผิดพลาดในการป้อนข้อมูลและการแก้ไข - แสดงข้อผิดพลาด (Error Messages) บนจอ Terminal หรือมีรายงานทันทีเพื่อให้ Operator ทำการแก้ไขได้อย่างรวดเร็ว - มี Suspense File สำหรับบันทึกรายการที่ถูก reject ทั้งหมด (Manual หรือ computer) และออกรายงานให้ user เป็นผู้ทำการแก้ไขต่อไป

ความเสี่ยง (Risks) / กิจกรรม (resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	รายการไม่ครบถ้วนและสมบูรณ์	รายการล่อย หรือไม่มีเอกสารสนับสนุน	รายการเกิดขึ้นเองจากโปรแกรมคอมพิวเตอร์	รายการผิดพลาด			ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
										- มีเจ้าหน้าที่ระดับบริหารเป็นผู้ทำการตรวจสอบความถูกต้องของรายแก้ไขเช่นเดียวกับรายการปกติ - การแก้ไขรายการที่ค้างใน Suspense File ไม่ควรใช้วิธีล้างหรือลบรายการออกจาก File แต่ควรใช้เป็นรายการเดบิทหรือเครดิต เพื่อให้สามารถติดตามและตรวจสอบการแก้ไขได้ - มีรายงานรายการที่ค้างนานใน Suspense File

ความเสี่ยง (Risks) / กิจกรรม (Resources)	ประมวลผลโดยใช้ข้อมูลผิดพลาด	ประมวลผลโดยใช้โปรแกรมผิดพลาด	ประมวลผลไม่ครบถ้วน	ประมวลผลไม่ถูกต้อง	รายการเกิดขึ้นเองโดยไม่มีเงื่อนไข				ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
Data Processing	X	X	X	X	X				การบันทึกบัญชีและยอดคงเหลือทางบัญชีไม่ถูกต้องการประกอบธุรกิจหยุดชะงักสูญเสียรายได้ภาพพจน์เสียหายและอาจเกิดการทุจริต	**COMPLETENESS & ACCURACY** - มีการตรวจสอบความถูกต้องของ Transaction แต่ละรายการก่อนนำไปประมวลผลกับ Master File - Matching - Limit - Reasonableness - มีการตรวจสอบความถูกต้องของ File ก่อนประมวลผล (Header Label Check) - มีการตรวจสอบความถูกต้องของ File หลังประมวลผล (Trailer Label Check - Control record) - มี Run-to-Run control สำหรับงานที่มี intermediate run ก่อนถึงการประมวลผลขั้นสุดท้าย - มีการตรวจสอบความถูกต้องของผลลัพท์กับข้อมูล input โดยบุคคล - ตรวจสอบ Output control total กับ Input control total - ตรวจสอบรายงาน Update, Change, Add และ Delete - มีการทดสอบการคำนวณโดยบุคคล - เลือกทดสอบบางรายการ - ทดสอบผลรวม - มีการตรวจสอบ Master File เป็นครั้งคราว โดยการตรวจสอบกับเอกสารสนับสนุนรายการที่เกี่ยวข้อง

ความเสี่ยง (Risks) / กิจกรรม (resources)	รายงานผิดพลาด	รายงานล่าช้า	รายงานสิ้นเปลือง	รายงานไม่ครบถ้วน					ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)

DATA OUTPUT	X	X	X	X					การประกอบธุรกิจจะก่อเกิดความเสียหายทางการเงิน อันเนื่องจากการตัดสินใจและการปฏิบัติงานผิดพลาด และอาจเกิดการทุจริต	**COMPLETE & ACCURACY**
										- มีการตรวจสอบ Output โดยบุคคลของศูนย์ฯ และ Users
										การตรวจสอบของศูนย์ฯ
										- ตรวจสอบ Output Batch totals กับ Input Batch totals
										- ตรวจสอบ Output record counts กับ Input record counts
										- ตรวจสอบจำนวนฉบับรายงานเทียบกับโปรแกรมสั่งงาน
										- ตรวจสอบลำดับหน้าของรายงาน
										- ตรวจสอบหัวและท้ายของรายงาน
										  - ชื่อรายงาน
										  - โปรแกรมที่ใช้ในการประมวลผล
										  - วันและเวลาที่ออกรายงาน
										  - ระยะเวลาที่ออกรายงาน
										  - หน่วยงานผู้ใช้
										  - Record counts
										  - Control totals
										การตรวจสอบของ Users
										- ตรวจสอบรูปแบบของรายงาน
										- ตรวจสอบ Computer control total กับ Manual control total

ความเสี่ยง (Risks) / กิจกรรม (Resources)	รายงานผิดพลาด	รายงานล่าช้า	รายงานสูญหาย	รายงานไม่ครบถ้วน					ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
										- ตรวจสอบ Output record counts กับ Input record counts - ตรวจสอบรายการเปลี่ยนแปลงข้อมูลใน Master File (List of changes) - ตรวจสอบรายการที่เกิดจากเงื่อนไขในโปรแกรม (List of Computer generated Transactions) - ตรวจสอบรายการที่ป้อนเข้าระบบงานทั้งสิ้น (Transaction List) - มี Distribution List สำหรับควบคุมการจัดส่งรายงานให้ Users