การประเมินความเสี่ยงทางคอมพิวเตอร์

ดร.นิตยา วงศ์ภินันท์วัฒนา*

บทคัดย่อ

การประเมินความเสี่ยงนับเป็นเครื่องมือที่มีความสำคัญในการประเมินโอกาสที่สินทรัพย์ขององค์กรจะสูญหายหรือถูกทำลาย เนื่องจากการประเมินความเสี่ยงมีหลายด้านด้วยกัน บทความนี้เน้นการประเมินความเสี่ยงสองรูปแบบด้วยกันคือ การประเมินความเสี่ยงโดยพิจารณาจากต้นทุนและผลประโยชน์ และการประเมินความเสี่ยงแบบ Renaissance Approach ซึ่งคำนึงถึงความเสี่ยงทางคอมพิวเตอร์เป็นหลัก

บทนำ

ความเสี่ยงคือโอกาสที่การกระทำหรือเหตุการณ์หนึ่ง ๆ จะส่งผลกระทบในทางที่ไม่ดีต่อองค์กรและระบบสารสนเทศขององค์กร โดยความเสี่ยงเป็นการคุกคามที่มีแนวโน้มที่จะก่อให้เกิดอันตรายต่อทรัพย์สินหรือกลุ่มของทรัพย์สินทั้งในด้านการทำให้ทรัพย์สินสูญหายหรือถูกทำลาย ส่วนการประเมินความเสี่ยงนั้น เป็นคำที่มีการกล่าวถึงกันอย่างกว้างขวางโดยเฉพาะอย่างยิ่งในกลุ่มผู้สอบบัญชี ซึ่งให้ความสนใจกับการประเมินความเสี่ยงมากกว่าที่เคยเป็นมา (การเปรียบเทียบความแตกต่างระหว่างการตรวจสอบแบบเดิมและการตรวจสอบแบบประเมินความเสี่ยงแสดงในภาคผนวก) อนึ่ง การประเมินความเสี่ยงคือ กระบวนการในการตัดสินใจเกี่ยวกับความเสียหายที่จะเกิดขึ้นกับทรัพย์สินขององค์กร

ในการวิเคราะห์ความเสี่ยงนั้นส่วนใหญ่จะประเมินความเสี่ยงใน 5 ปัจจัยหลักด้วยกันคือ การประเมินความเสี่ยงด้านเครดิต ด้านตลาด ด้านกลยุทธ์ ด้านสภาพคล่อง และด้านการปฏิบัติงาน อย่างไรก็ตาม FDIC (Federal Deposit Insurance Corporation) ได้ให้ความสำคัญกับการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเพิ่มมากขึ้น เนื่องจากองค์กรต่าง ๆ โดยเฉพาะสถาบันการเงินนำระบบสารสนเทศมาใช้ในการดำเนินธุรกิจมากขึ้น เช่น ใช้ระบบสารสนเทศในการฝากและถอนเงิน สินเชื่อ และการให้บริการทางการเงินผ่านทางอินเทอร์เน็ต เป็นต้น นอกจากนี้สถาบันการเงินต่าง ๆ ยังนำเทคโนโลยีสารสนเทศมาเป็นกลยุทธ์ขององค์กรด้วย การประเมินความเสี่ยงของเทคโนโลยีสารสนเทศเหล่านี้มีความสำคัญเพราะความเสียหายหรือล้มเหลวของเทคโนโลยีสารสนเทศจะส่งผลต่อความเสียหายทางการเงินและเชื่อเสียงขององค์กรนอกเหนือจากปัจจัย 5 ประการดังกล่าวมาข้างต้นเช่นกัน

ในการประเมินความเสี่ยงนั้น คนส่วนใหญ่มักคิดว่าจะต้องพิจารณาทุกปัจจัยที่อาจก่อให้เกิดความเสียหายกับทรัพย์สินทางด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งในความเป็นจริงคงทำไม่ได้ เนื่องจากมีเหตุการณ์มากมายนับไม่ถ้วนที่เป็นเหตุการณ์ที่อาจก่อให้เกิดความเสียหายได้ และการที่จะพิจารณาให้ครอบคลุมความเสี่ยงทั้งหมดที่

* ผู้ช่วยศาสตราจารย์ประจำภาควิชาระบบสารสนเทศเพื่อการจัดการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

อาจเกิดขึ้นก็เป็นไปได้ยากเช่นกัน ดังนั้นในการพิจารณาถึงความเสียหายกับทรัพย์สินทางด้านเทคโนโลยีสารสนเทศจึงควรจำกัดเฉพาะเหตุการณ์ที่มีความเป็นไปได้ที่จะก่อให้เกิดความเสียหายเท่านั้น เหตุผลหลักที่ทำให้ผู้สอบบัญชีให้ความสนใจในการประเมินความเสี่ยงมีดังนี้

1. ก่อให้เกิดความตระหนักและความสนใจเกี่ยวกับการควบคุมและการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศขององค์กรที่มีความเสี่ยงค่อนข้างสูง
2. กำหนดทรัพย์สินทางด้านเทคโนโลยีสารสนเทศที่อาจได้รับความเสียหายและการควบคุมทรัพย์สินนั้น ๆ โดยการวิเคราะห์อย่างเป็นระบบจะช่วยให้สามารถวิเคราะห์ความเสี่ยงอย่างละเอียดได้
3. สามารถประเมินถึงความเหมาะสมของการควบคุมที่มีอยู่ต่อความปลอดภัยของทรัพย์สินทางด้านเทคโนโลยีสารสนเทศนั้น ๆ
4. กำหนดขั้นตอนการตรวจสอบที่สามารถพบข้อผิดพลาดหรือสิ่งผิดปกติอย่างมีสาระสำคัญของเทคโนโลยีสารสนเทศได้
5. กำหนดค่าใช้จ่ายสำหรับการรักษาความปลอดภัยที่เหมาะสม ค่าใช้จ่ายสำหรับระบบการรักษาความปลอดภัยบางประเภทค่อนข้างสูงเมื่อประโยชน์ที่ได้รับไม่เด่นชัด การวิเคราะห์ความเสี่ยงจะช่วยในการระบุประโยชน์ของการรักษาความปลอดภัยนั้น ๆ ว่าคุ้มกับค่าใช้จ่ายที่ลงทุนไปหรือไม่ อนึ่ง ผู้สอบบัญชีสามารถนำผลลัพธ์ที่ได้ในข้อนี้ไปเสนอแนะการรักษาความปลอดภัยที่เหมาะสมสำหรับองค์กรต่อไป

การเลือกเครื่องมือในการประเมินความเสี่ยง

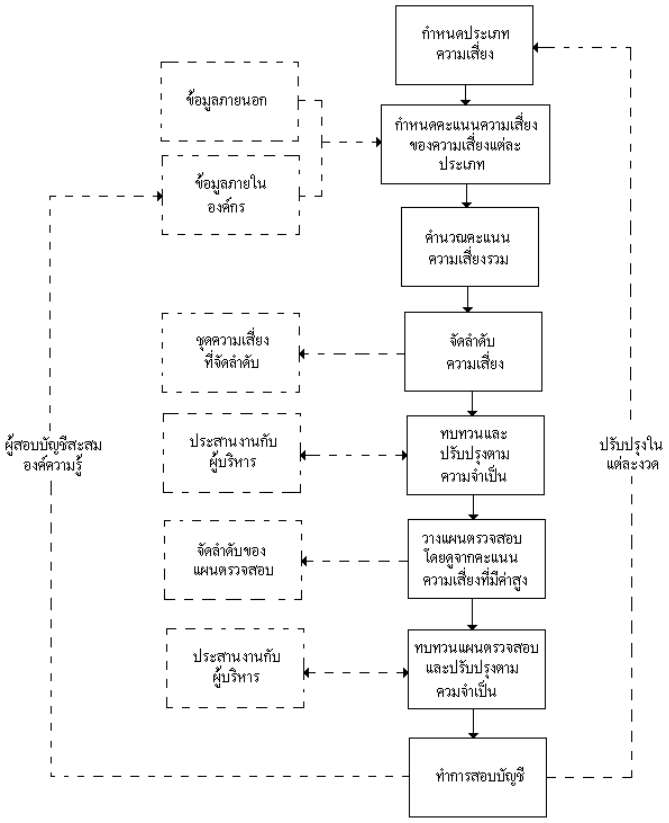
เนื่องจากวิธีการกำหนดความเสี่ยงในปัจจุบันมีเป็นจำนวนมาก ทั้งวิธีประเมินความเสี่ยงแบบง่าย ๆ ซึ่งจัดระดับความเสี่ยงเป็น สูง กลาง ต่ำ โดยใช้การตัดสินใจของผู้สอบบัญชีเป็นหลัก จนกระทั่งวิธีประเมินความเสี่ยงที่ค่อนข้างซับซ้อน ซึ่งใช้สูตรการคำนวณทางคณิตศาสตร์เพื่อหาตัวเลขความเสี่ยง ผู้สอบบัญชีทางคอมพิวเตอร์ควรเลือกวิธีการประเมินความเสี่ยงที่เหมาะสมกับความซับซ้อนและรายละเอียดของข้อมูลขององค์กรที่ตรวจสอบ เพื่อให้ได้ผลลัพธ์ของการประเมินความเสี่ยงที่ถูกต้อง อย่างไรก็ตามไม่ว่าจะเป็นวิธีประเมินความเสี่ยงใดก็ตาม มักต้องการการตัดสินใจของผู้สอบบัญชีเช่น การตัดสินใจเกี่ยวกับน้ำหนักของความเสี่ยง เป็นต้น แม้ว่าจะไม่มีวิธีการประเมินความเสี่ยงใดที่เหมาะสมกับทุกสถานการณ์ก็ตาม ผู้สอบบัญชีที่ต้องการใช้วิธีการตรวจสอบโดยเน้นการวิเคราะห์ความเสี่ยง (Risk-based audit approach) คงต้องเลือกวิธีการประเมินความเสี่ยงที่จะนำไปใช้ ในการเลือกวิธีการประเมินความเสี่ยงนั้น ผู้สอบบัญชีควรพิจารณาถึง

1. ประเภทของข้อมูลที่ต้องจัดหา เนื่องจากวิธีประเมินความเสี่ยงบางวิธีจะพิจารณาเฉพาะปัจจัยทางการเงินเท่านั้น ดังนั้นวิธีดังกล่าวอาจไม่เหมาะสมกับการสอบบัญชีทางคอมพิวเตอร์ได้
2. ค่าใช้จ่ายสำหรับโปรแกรมหรือค่าลิขสิทธิ์ที่จำเป็นในการใช้เครื่องมือประเมินความเสี่ยงนั้น ๆ
3. การมีอยู่ของข้อมูลที่ใช้ในเครื่องมือประเมินความเสี่ยงนั้น ๆ
4. จำนวนข้อมูลที่ต้องการเพิ่มเติมเพื่อใช้ในการประเมินความเสี่ยง และค่าใช้จ่ายในการจัดหาข้อมูลนั้น ๆ รวมถึงเวลาที่ใช้ในการจัดหาข้อมูลนั้น ๆ ด้วย
5. ความคิดเห็นของผู้ใช้คนอื่น ๆ ต่อเครื่องมือประเมินความเสี่ยงนั้น ๆ
6. ความเต็มใจของผู้บริหารในการยอมรับเครื่องมือดังกล่าวในการประเมินความเสี่ยงและนำไปวางแผนการสอบบัญชีต่อไป

ข้อมูลที่นำมาใช้ในการประเมินความเสี่ยงอาจได้มาจาก การสัมภาษณ์ผู้บริหารขององค์กรที่จะตรวจสอบ การจัดส่งแบบสอบถาม การทบทวนรายงานการตรวจสอบก่อนหน้า แผนกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศ งบประมาณขององค์กรสำหรับเทคโนโลยีสารสนเทศ และความรู้ด้านการตรวจสอบทางเทคโนโลยีสารสนเทศ อนึ่ง บทความนี้จะกล่าวถึงการประเมินความเสี่ยงสองรูปแบบด้วยกันคือ การประเมินความเสี่ยงโดยพิจารณาจากต้นทุนและผลประโยชน์ และการประเมินความเสี่ยงแบบ Renaissance Approach ซึ่งคำนึงถึงความเสี่ยงทางคอมพิวเตอร์เป็นหลักเท่านั้น (ผู้ที่สนใจสามารถหารายละเอียดเครื่องมือการประเมินความเสี่ยงทางด้านคอมพิวเตอร์จากอินเทอร์เน็ต เช่น การประเมินความเสี่ยงตามที่ Information Systems Audit and Control Association หรือ ISACA กำหนด เป็นต้น)

ขั้นตอนในการกำหนดความเสี่ยง

เนื่องจากผู้สอบบัญชีจำเป็นต้องประเมินความเสี่ยงของการดำเนินงานขององค์กรที่ตรวจสอบ และจากการที่องค์กรต่างๆ นำคอมพิวเตอร์มาช่วยในการดำเนินงานกันมากขึ้น บทความนี้จึงนำเสนอขั้นตอนในการประเมินความเสี่ยงทางคอมพิวเตอร์เป็นหลัก การประเมินความเสี่ยงที่นำเสนอในที่นี้เป็นความเสี่ยงที่ปรับปรุงมาจากการประเมินความเสี่ยงทางการบริหาร เนื่องจากระบบคอมพิวเตอร์มีความซับซ้อนและมีจุดเด่นเฉพาะที่แตกต่างออกไป ขั้นตอนในการประเมินความเสี่ยงโดยทั่วไปและแผนการตรวจสอบแสดงดังภาพที่ 1



ภาพที่ 1 ขั้นตอนในการประเมินความเสี่ยงและการวางแผนการตรวจสอบ

โดยปกติผู้สอบบัญชีทางคอมพิวเตอร์จะเก็บรวบรวมหลักฐานเพื่อประเมินการรักษาความปลอดภัยของทรัพย์สิน (Asset Safeguarding) ความเชื่อถือได้ของข้อมูล (Data Integrity) และความมีประสิทธิภาพและประสิทธิผลของระบบ (System Efectiveness and System Efficiency) ขององค์กร หรืออาจกล่าวอีกนัยหนึ่งว่าผู้สอบบัญชีทางคอมพิวเตอร์ประเมินความเสี่ยงทางคอมพิวเตอร์สองด้านคือ

1. ความเสี่ยงด้านเทคโนโลยี (IT Risk) เช่น ผลการปฏิบัติงานของโปรแกรม ความสามารถเข้าถึงและใช้ระบบได้ และภัยคุกคามระบบ
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk) เช่น ความมีประสิทธิภาพและประสิทธิผลของการประมวลผล และการปฏิบัติตามระเบียบที่กำหนด

แต่การสอบบัญชีในลักษณะของการสุ่มตัวอย่าง ผู้สอบบัญชีอาจไม่พบความสูญเสียหรือข้อผิดพลาดทางการบัญชีที่เป็นสาระสำคัญได้ ความเสี่ยงที่ผู้สอบบัญชีไม่สามารถตรวจพบข้อผิดพลาดดังกล่าวในการสรุปผลการสอบบัญชีเรียกว่า ความเสี่ยงของการสอบบัญชี (Audit Risk) อย่างไรก็ตามผู้สอบบัญชีจะใช้วิธีการและขั้นตอนในการสอบบัญชีเพื่อพยายามลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ระดับความเสี่ยงของการสอบบัญชีที่เป็นที่ยอมรับกันโดยทั่วไปสำหรับผู้สอบบัญชีภายนอกคือ

$$DAR = IR \times CR \times DR \qquad (1)$$

โดย

DAR (Desired audit risk) คือ ความเสี่ยงของการสอบบัญชีที่ต้องการ

IR (Inherent risk) คือ ความเสี่ยงที่มีอยู่โดยธรรมชาติในทรัพย์สินนั้น (Inherent Risk) กล่าวคือทรัพย์สินแต่ละประเภทมีแนวโน้มที่จะสูญหายหรือผิดพลาดบางส่วนซึ่งเป็นผลมาจากลักษณะของทรัพย์สินนั้น (โดยไม่คำนึงถึงความเชื่อถือได้ของการควบคุมภายใน) เช่น ความเสี่ยงที่มีอยู่ในโปรแกรมระบบ (Operating System) จะมีมากกว่าความเสี่ยงที่มีอยู่ในเครื่องไมโครคอมพิวเตอร์ที่ไม่ได้เชื่อมโยงกับเครื่องคอมพิวเตอร์อื่นๆ (Stand-Alone PC) เนื่องจากถ้าการรักษาความปลอดภัยของโปรแกรมระบบไม่เหมาะสมจะส่งผลให้สามารถเปลี่ยนแปลงและเปิดเผยข้อมูลในโปรแกรมอื่นๆ ได้ง่าย ส่งผลให้โปรแกรมระบบมีความเสี่ยงสูงกว่าเครื่องไมโครคอมพิวเตอร์ที่ไม่ได้ใช้งานที่สำคัญๆขององค์กร

CR (Control Risk) คือความเสี่ยงของการควบคุม ซึ่งแสดงให้เห็นแนวโน้มที่การควบคุมภายในบางส่วนไม่สามารถป้องกัน ตรวจจับ หรือแก้ไขสิ่งของจากการสูญหายหรือผิดพลาดในบางส่วนที่เกิดขึ้นได้ เช่น ความเสี่ยงจากการตรวจสอบ คอมพิวเตอร์ล็อกหรือการบันทึกการปฏิบัติการของคอมพิวเตอร์ (Computer Logs) ด้วยมือจะมีความเสี่ยงสูง เนื่องจากการสอบทานข้อมูลเป็นจำนวนมากในล็อก (Logs) อาจมีข้อมูลบางส่วนที่หลงไปได้ ดังนั้นความเสี่ยงของการควบคุมจะสูง ส่วนความเสี่ยงของการควบคุมของโปรแกรมสอบทานข้อมูลจะค่อนข้างต่ำ เนื่องจากการประมวลผลเป็นอัตโนมัติ

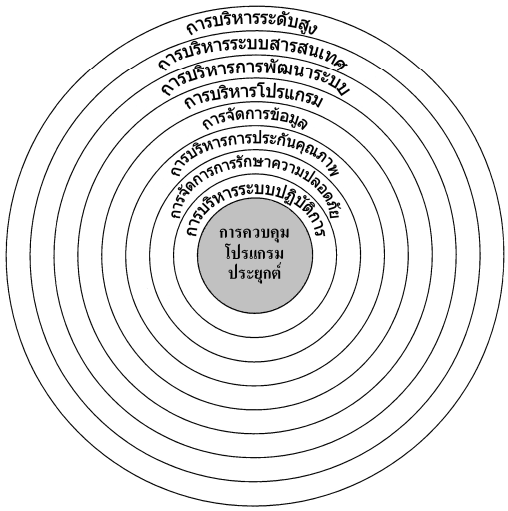
DR (Detection Risk) คือความเสี่ยงจากการตรวจจับ เป็นความเสี่ยงที่แสดงให้เห็นว่าวิธีการตรวจสอบบางอย่างไม่สามารถค้นพบการสูญหายหรือข้อผิดพลาดทางบัญชีอย่างมีสาระสำคัญได้ เช่น ความเสี่ยงจากการตรวจจับข้อบกพร่องของการรักษาความปลอดภัยของโปรแกรมประยุกต์ค่อนข้างสูง เนื่องจากล็อก (Log) ที่เก็บข้อมูลเกี่ยวกับการใช้งานระบบคอมพิวเตอร์ทั้งหมดยังไม่มีในช่วงที่ทำการตรวจสอบ แต่ความเสี่ยงจากการตรวจจับข้อบกพร่องของแผนฟื้นฟูระบบ (Disaster recovery plan) จะค่อนข้างต่ำ เนื่องจากมีเอกสารที่ผู้สอบบัญชีสามารถนำมาประเมินได้

ในการประเมินระดับความเสี่ยงที่มีอยู่ในทรัพย์สินเนื่องจากลักษณะของทรัพย์สินนั้น ผู้สอบบัญชีสามารถใช้เกณฑ์ที่แสดงในตารางที่ 1 ข้างล่างเพื่อประกอบการพิจารณา

ตารางที่ 1 แนวทางในการพิจารณาความสี่ยงของปัจจัยที่มีความเสี่ยง เนื่องจากลักษณะของทรัพย์สินขององค์กร

ปัจจัยที่เป็นความเสี่ยง เนื่องจากลักษณะของทรัพย์สิน	คำอธิบาย
ระบบการเงิน	เป็นระบบที่นำมาควบคุมทรัพย์สินที่สำคัญขององค์กร เช่น การรับเงินและการเบิกจ่ายเงิน เงินเดือน ลูกหนี้และเจ้าหนี้ ซึ่งส่วนมากจะมีความเสี่ยงเนื่องจากลักษณะของทรัพย์สินค่อนข้างสูง ระบบเหล่านี้เป็นระบบที่มีความถี่สูงต่อการเป็นเป้าหมายของการฉ้อโกงและการยักยอกเงินหรือทรัพย์สิน
ระบบกลยุทธ์	เป็นระบบที่ทำให้องค์กรมีความได้เปรียบในการแข่งขัน เช่น ระบบที่เกี่ยวข้องกับสิทธิบัตรหรือความลับทางการค้า มักเป็นระบบที่มีความเสี่ยงของตัวระบบเองค่อนข้างสูง ระบบดังกล่าวมักเป็นเป้าหมายของการทำจารกรรมหรือการตอบโต้จากคู่แข่ง
ระบบการปฏิบัติงานที่สำคัญ	ระบบที่สามารถทำให้องค์กรเสียหายถ้าระบบไม่ปฏิบัติงาน เช่น ระบบสั่งจองสำหรับลูกค้า หรือระบบควบคุมการผลิต ซึ่งมักเป็นระบบที่มีความเสี่ยงของตัวระบบเองค่อนข้างสูง
ระบบที่ใช้เทคโนโลยีที่มีความก้าวหน้า	ระบบที่ใช้เทคโนโลยีขั้นสูงมักเป็นระบบที่มีความเสี่ยงภายในตัวระบบเองค่อนข้างสูงเช่นกัน เนื่องจากระบบดังกล่าวมีความซับซ้อนและองค์กรขาดประสบการณ์ในการใช้เทคโนโลยีดังกล่าว

ในการประเมินระดับความเสี่ยงของการควบคุมที่สัมพันธ์กับส่วนของการสอบบัญชีนั้น ผู้สอบบัญชีจะพิจารณาถึงความเชื่อถือได้ของทั้งการควบคุมทางการบริหารและโปรแกรมประยุกต์ กล่าวคือผู้สอบบัญชีจะระบุและประเมินการควบคุมระบบย่อย ๆ ทางการบริหารก่อน เนื่องจากการควบคุมดังกล่าวเป็นการควบคุมเบื้องต้นซึ่งครอบคลุมโปรแกรมประยุกต์ทั้งหมด ดังนั้นผู้สอบบัญชีจะให้ความสำคัญต่อการขาดการควบคุมทางการบริหารอย่างมาก จากภาพที่ 2 ซึ่งแสดงให้เห็นถึงวงแหวนของหัวหอม (Onion Skins) โดยการควบคุมของผู้บริหารระดับสูงอยู่ที่วงแหวนนอกสุดและโปรแกรมประยุกต์อยู่ที่แกนกลางของหัวหอม จะเห็นได้ว่าถ้าการควบคุมรอบนอกไม่เสียหายแล้ว การควบคุมในสุดจะไม่เสียหายด้วย นอกจากนี้การประเมินการควบคุมจะมีประสิทธิภาพ ถ้าผู้สอบบัญชีประเมินการควบคุมทางการบริหารก่อนการควบคุมโปรแกรมประยุกต์ เนื่องจากภายหลังจากผู้สอบบัญชีประเมินการควบคุมทางการบริหารแล้ว ผู้สอบบัญชีไม่จำเป็นต้องประเมินการควบคุมดังกล่าวอีก เพราะการควบคุมดังกล่าวจะมีผลกับทุกโปรแกรมประยุกต์ ตัวอย่างเช่น ถ้าผู้สอบบัญชีพบว่าองค์กรกำหนดคุณภาพของการจัดทำมาตรฐานของเอกสารอย่างสูงแล้ว ผู้ตรวจสอบไม่จำเป็นที่จะต้องประเมินคุณภาพของเอกสารประกอบโปรแกรมประยุกต์ทุกโปรแกรม



ภาพที่ 2 การควบคุมทางการบริหารซึ่งล้อมรอบการควบคุมโปรแกรมประยุกต์

จะเห็นได้ว่าถ้าการประเมินความเสี่ยงที่มีอยู่ในลักษณะของทรัพย์สินและความเสี่ยงจากการควบคุมมีค่าสูงแล้ว ผู้สอบบัญชีควรสุ่มตัวอย่างเพื่อนำมาวิเคราะห์ในขั้นตอนการตรวจสอบสาระสำคัญ (Substantive Test) มากขึ้น นอกจากนี้ผู้สอบบัญชีมักกำหนดระดับความเสี่ยงของการสอบบัญชีที่ต้องการหรือยอมรับได้ โดยผู้สอบบัญชีภายนอกจะพิจารณาระดับของความเสี่ยงของปัจจัยดังกล่าวที่บุคคลภายนอกยังให้ความเชื่อถือต่อรายงานทางการเงินและระดับของความเป็นไปได้ที่องค์กรจะเผชิญกับปัญหาทางการเงินภายหลังการตรวจสอบ ส่วนผู้สอบบัญชีภายในนั้นมักจะพิจารณาผลกระทบต่อองค์กรทั้งระยะสั้นและระยะยาว ถ้าผู้สอบบัญชีไม่สามารถตรวจพบประสิทธิภาพและประสิทธิผลของการปฏิบัติงานอย่างมีสาระสำคัญ

วิธีการประเมินความเสี่ยงแบบต้นทุนและผลประโยชน์

การประเมินความเสี่ยงเชิงตัวเลขนี้มีขั้นตอนในการประเมิน 6 ขั้นตอนดังนี้

ขั้นตอนที่หนึ่ง คือการจัดหมวดหมู่ของทรัพย์สินทางคอมพิวเตอร์ ออกเป็นส่วนต่าง ๆ ดังนี้

1. กลุ่มฮาร์ดแวร์ ประกอบด้วย หน่วยประมวลผลกลาง เครื่องเทอร์มินอล เครื่องอ่านดิสก์ เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสาร เป็นต้น
2. กลุ่มซอฟต์แวร์ ประกอบด้วย ระบบปฏิบัติการ โปรแกรมอรรถประโยชน์ โปรแกรมประยุกต์ (ทั้งโปรแกรมต้นฉบับ โปรแกรมรหัส) และโปรแกรมการวิเคราะห์ต่าง ๆ เป็นต้น
3. กลุ่มข้อมูล ประกอบด้วย ข้อมูลที่ใช้ระหว่างการประมวลผล ข้อมูลที่จัดเก็บในสื่อจัดเก็บข้อมูลและกระดาษพิมพ์ และร่องรอยการตรวจสอบ เป็นต้น
4. กลุ่มเอกสาร ประกอบด้วย เอกสารเพื่ออธิบายลักษณะและการใช้งานเครื่องคอมพิวเตอร์ โปรแกรมและการบริหารจัดการคอมพิวเตอร์ เป็นต้น
5. กลุ่มวัสดุ ประกอบด้วย กระดาษ แบบฟอร์ม สื่อเก็บข้อมูล และหมึกพิมพ์ เป็นต้น
6. กลุ่มทรัพยากรบุคคล ประกอบด้วย คนที่ทำหน้าที่สั่งให้โปรแกรมประมวลผลหรือเขียนโปรแกรม เป็นต้น

ปกติแล้วข้อมูลดังกล่าวข้างต้นโดยเฉพาะเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ และโปรแกรมต่าง ๆ จะมีการบันทึกบัญชีและทำการตรวจนับทุกสิ้นปี แต่ข้อมูลอาจไม่ทันสมัย นอกจากนี้ข้อมูลที่จัดเก็บทางการบัญชียังไม่รวมถึงสินทรัพย์ที่จับต้องไม่ได้ เช่น ข้อมูลและทรัพยากรบุคคล

ขั้นตอนที่สอง คือประเมินความเป็นไปได้ที่ทรัพย์สินทางคอมพิวเตอร์ที่จัดหมวดหมู่ในขั้นตอนที่หนึ่งจะได้รับความเสียหาย โดยความเสียหายนั้นจะส่งผลกระทบต่อ การรักษาความปลอดภัยของทรัพย์สิน ความเชื่อถือได้ของข้อมูล และความมีประสิทธิภาพและประสิทธิผลของระบบ จะเห็นได้ว่าผู้สอบบัญชีภายนอกจะสนใจว่ามีข้อผิดพลาดหรือสิ่งผิดปกติที่จะก่อให้เกิดความสูญเสียต่อองค์กรหรือข้อผิดพลาดกับข้อมูลทางการเงินที่จัดทำโดยองค์กรอย่างมีสาระสำคัญ ในขณะที่ผู้สอบบัญชีภายในนั้นจะคำนึงถึงความสูญเสียที่เกิดขึ้นหรืออาจเกิดขึ้นเนื่องจากการปฏิบัติงานที่ไม่มีประสิทธิภาพหรือประสิทธิผลขององค์กร อย่างไรก็ตามผู้สอบบัญชี ภายนอกจะคำนึงถึงความไม่มีประสิทธิภาพหรือประสิทธิผลของการปฏิบัติงานที่คุกคามองค์กรด้วยเช่นกัน นอกจากนี้ผู้สอบบัญชีภายนอกยังรายงานปัญหาดังกล่าวโดยถือเป็นส่วนหนึ่งของบริการทางด้านวิชาชีพกับผู้บริหารองค์กรด้วย

นอกจากเกณฑ์ดังกล่าว ผู้สอบบัญชีสามารถพิจารณาถึงผลกระทบของความเสียหายโดยตั้งคำถามเหล่านี้

- อะไรคือผลกระทบของความผิดพลาดที่ไม่ได้ตั้งใจ กรณีนี้ให้ลองคิดถึงการป้อนคำสั่ง ข้อมูล และการทิ้งหรือการทำลายข้อมูลผิดพลาด
- อะไรคือผลกระทบของความผิดพลาดที่เกิดจากการมีเจตนาร้าย กรณีนี้ให้ลองคิดถึงพนักงานที่ไม่พอใจกิจการ
- อะไรคือผลกระทบของคนภายนอก กรณีนี้ให้ลองคิดถึงการเข้าถึงเครือข่าย และ Hackers
- อะไรคือผลกระทบของภัยทางธรรมชาติและทางกายภาพ กรณีนี้ให้ลองคิดถึงไฟ พายุ น้ำท่วม ไฟตก และองค์ประกอบทางคอมพิวเตอร์ล้มเหลว

ตารางที่ 2 แสดงให้เห็นถึงปัญหาทั่ว ๆไปที่ส่งผลกระทบต่อทรัพย์สินทางคอมพิวเตอร์ สิ่งที่จำเป็นในการพิจารณาคือจะเกิดอะไรขึ้นกับฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และความล้มเหลวขององค์ประกอบ

ตารางที่ 2 ทรัพย์สินและการรักษาความปลอดภัย

ทรัพย์สิน	การรักษาความปลอดภัย	ความเชื่อถือได้	การมีประสิทธิภาพและประสิทธิผล
ฮาร์ดแวร์	ถูกขโมย	ถูกใช้งานมากเกินไป ถูกทำลาย แทรกแซง	ล้มเหลว ถูกทำลาย **ไม่มีให้ใช้งาน**
ซอฟต์แวร์	ถูกขโมย ถูกจัดทำสำเนา ถูกละเมิดสิทธิ	โปรแกรมไวรัสม้าไม้แห่งทรอย ถูกปรับปรุง แทรกแซง	ถูกลบทิ้ง ถูกนำไปไว้ผิดที่ หมดอายุ
ข้อมูล	ถูกเปิดเผย ถูกเข้าถึงจากคนภายนอก ถูกอ้างถึง	ถูกทำลาย โปรแกรมทำงานผิดพลาด ฮาร์ดแวร์ทำงานผิดพลาด ผู้ใช้งานทำงานผิดพลาด	ถูกนำไปไว้ผิดที่ ถูกทำลาย
เอกสาร	สูญหาย		ถูกขโมย ถูกทำลาย
วัสดุ	สูญหาย		ถูกขโมย ถูกทำให้เสียหาย
ทรัพยากรบุคคล			ลาออก, ลาพัก ปลดออก, เกษียณอายุ

ขั้นตอนที่สาม คือการประมาณความเป็นไปได้ที่จะเกิดความเสียหายกับทรัพย์สินทางคอมพิวเตอร์ แม้ว่าอาจเป็นไปได้ยากที่จะทำนายความเป็นไปได้ของการเกิดเหตุการณ์ที่จะก่อให้เกิดความเสียหาย แต่มีวิธีการกะประมาณเหตุการณ์หนึ่ง ๆ ดังนี้

- สังเกตุจากข้อมูลของประชากรทั่วไป แม้ว่าคงเป็นไปไม่ได้ที่จะกำหนดว่าเมื่อไรจะเกิดเพลิงไหม้ศูนย์คอมพิวเตอร์ขององค์กรหนึ่ง ๆ แต่บริษัทประกันภัยจะเก็บรวบรวมข้อมูลจำนวนมากซึ่งสามารถนำมาใช้ทำนายว่าแต่ละปีจะมีเพลิงไหม้ศูนย์คอมพิวเตอร์จำนวนกี่แห่ง ซึ่งจะก่อให้เกิดความเสียหายเป็นจำนวนเท่าไร นอกจากนี้บริษัทประกันภัยยังมีข้อมูลที่สามารถประมาณการแนวโน้มที่พนักงานจะทุจริต เป็นขโมย และอื่น ๆ ด้วย
- สังเกตุข้อมูลจากระบบปฏิบัติการ (Operating System) ซึ่งทำให้สามารถติดตามข้อมูลเกี่ยวกับความล้มเหลวของฮาร์ดแวร์ และความล้มเหลวของความพยายามเข้าสู่ระบบได้
- ประมาณการจำนวนของการเกิดเหตุการณ์ภายในช่วงเวลาที่กำหนด เช่น ให้นักวิเคราะห์ระบบประมาณการจำนวนครั้งที่มีเหตุการณ์ที่ผู้สอบบัญชีต้องการทราบซึ่งเกิดขึ้นเมื่อปีที่แล้ว เป็นต้น แม้ว่าตัวเลขที่ได้จากการประมาณการของนักวิเคราะห์ระบบจะไม่ใช่ตัวเลขที่ถูกต้อง เนื่องจากมิได้จัดเก็บข้อมูลเอาไว้ แต่นักวิเคราะห์ระบบอาจสามารถประมาณการได้ค่อนข้างใกล้เคียง
- วิธีการ Delphi เป็นวิธีการที่ให้ผู้ประเมินแต่ละคนประมาณโอกาสที่จะเกิดเหตุการณ์หนึ่ง ๆ ต่อจากนั้นจะจัดเก็บ ทำสำเนา และแจกจ่ายการกะประมาณที่แต่ละคนจัดทำให้กับผู้ประเมินทุกคน พร้อมกับถามผู้ประเมินว่าต้องการปรับปรุงอัตราที่กำหนดขึ้นก่อนหน้านั้นหลังจากทราบประมาณการของผู้ประเมินคนอื่น ๆ หรือไม่ หลังจากการแก้ไขปรับปรุง จะทำการรวบรวมประมาณการเหล่านั้น ถ้าประมาณการที่เก็บมายังมีค่าเหมือนเดิมหรือไม่เปลี่ยนแปลงจะนำค่าที่ได้นี้เป็นค่าสุดท้ายที่จะนำมาใช้ต่อไป แต่ถ้าประมาณ

การที่เก็บมีการเปลี่ยนแปลง ผู้ประเมินจะมาประชุมกันเพื่อพูดคุยเกี่ยวกับเหตุผลที่ประมาณการไม่คงที่ พร้อมทั้งหาข้อสรุปสำหรับค่าสุดท้ายต่อไป

- ประมาณการแนวโน้มจากตาราง ในการวิเคราะห์ความเสี่ยงหลาย ๆ วิธีนั้น ผู้วิเคราะห์ความเสี่ยงจะเลือกอัตราความเป็นไปได้ที่เกิดความเสียหายต่อทรัพย์สินขององค์กรจากตารางซึ่งเป็นแนวทางในการเลือกแนวโน้มหรือความเป็นไปได้ (ดังแสดงในตารางที่ 3)

ตารางที่ 3 อัตราของความเป็นไปได้

ความถี่	อัตรา
มากกว่าหนึ่งครั้งต่อวัน	10
หนึ่งครั้งต่อวัน	9
หนึ่งครั้งต่อทุกสามวัน	8
หนึ่งครั้งต่อสัปดาห์	7
หนึ่งครั้งต่อสองสัปดาห์	6
หนึ่งครั้งต่อเดือน	5
หนึ่งครั้งต่อทุก ๆ สี่เดือน	4
หนึ่งครั้งต่อปี	3
หนึ่งครั้งต่อทุก ๆ สามปี	2
น้อยกว่าหนึ่งครั้งในสามปี	1

ขั้นตอนที่สี่ คือการกำหนดค่าความเสียหายต่อปีสำหรับความเสียหายที่อาจเกิดขึ้น เนื่องจากการกำหนดค่าความเสียหายของแต่ละทรัพย์สินทางคอมพิวเตอร์แต่ละประเภทจะแตกต่างกันออกไป เช่น ความเสียหายที่เกิดกับฮาร์ดแวร์จะกำหนดค่าความเสียหายเป็นตัวเงินได้ง่าย แต่การกำหนดค่าความเสียหายจากการที่เครื่องคอมพิวเตอร์ไม่สามารถประมวลผลได้ตามกำหนดเวลานั้นอาจคิดเป็นตัวเงินได้ยาก อย่างไรก็ตามสามารถใช้คำถามต่อไปนี้เพื่อเป็นแนวทางในการกำหนดค่าความเสียหาย

- สิ่งใดที่ควรกระทำเพื่อรักษาความลับหรือความเชื่อถือได้ของข้อมูล
- การเปิดเผยข้อมูลจะส่งผลกระทบต่อบุคคลหรือองค์กรหรือไม่ สามารถฟ้องร้องกันทางกฎหมายได้หรือไม่
- การเข้าถึงข้อมูลของผู้ที่ไม่รับอนุมัติจะก่อให้เกิดผลเสียต่อโอกาสอันดีของธุรกิจในอนาคตหรือไม่ การเข้าถึงข้อมูลดังกล่าวจะทำให้คู่แข่งมีความได้เปรียบหรือไม่ ประมาณการยอดขายที่สูญเสียไปเป็นจำนวนเท่าไร
- สภาพทางจิตวิทยาของผลกระทบของการไม่มีบริการทางคอมพิวเตอร์เป็นอย่างไร เกิดความละอายหรือไม่ สูญเสียความเชื่อถือ สูญเสียธุรกิจ จำนวนลูกค้าที่ถูกกระทบ
- มูลค่าของการเข้าถึงข้อมูลหรือโปรแกรมเป็นจำนวนเท่าไร สามารถเลื่อนการคำนวณออกไปได้หรือไม่ สามารถคำนวณจากที่อื่นได้หรือไม่ ถ้าให้บุคคลที่สามทำการคำนวณมูลค่าการเข้าถึงข้อมูลหรือโปรแกรมจะต้องเสียค่าใช้จ่ายจำนวนเท่าไร
- มูลค่าของการเข้าถึงข้อมูลหรือโปรแกรมของคนภายนอก จำนวนเงินที่คู่แข่งยอมจ่ายในการเข้าถึงข้อมูลดังกล่าว
- จะเกิดปัญหาอะไรจากการสูญเสียข้อมูล ข้อมูลถูกเปลี่ยนแปลงได้หรือไม่ สามารถจัดสร้างข้อมูลใหม่ได้หรือไม่ งานที่ต้องทำเป็นอย่างไร

ตามที่กล่าวมาแล้วว่าค่าความเสียหายดังกล่าวไม่สามารถหามาได้ง่ายนัก อย่างไรก็ตามควรประเมินมูลค่าความเสียหายเพื่อให้การวิเคราะห์กระทำได้อย่างทั่วถึงและเหมาะสม โดยมูลค่าความเสียหายของเหตุการณ์ที่อาจเกิดขึ้นจะได้มาจาก การคูณค่าความเสียหายที่เกิดขึ้นกับความถี่ของการเกิดเหตุการณ์นั้นๆ เช่น ประมาณการต้นทุนมีค่าเท่ากับ 10,000 บาท โดยความถี่ที่จะเกิดเหตุการณ์เท่ากับ 3 ครั้งต่อปี ดังนั้นมูลค่าความเสียหายที่อาจเกิดขึ้นต่อปี (Annual loss expectancy หรือ ALE) มีค่าเท่ากับ 30,000 บาท เป็นต้น

ขั้นตอนที่ห้า คือสำรวจการควบคุมที่เป็นไปได้และค่าใช้จ่ายสำหรับการควบคุมนั้นๆ การพิจารณาถึงจุดควบคุมที่เหมาะสมนั้น ให้พิจารณาถึงความเป็นไปได้ที่ทรัพย์สินทางคอมพิวเตอร์จะเสียหายต่อจากนั้นให้คิดถึงการควบคุมที่สามารถนำไปใช้ในการป้องกันความเสียหายต่อทรัพย์สินทางคอมพิวเตอร์ เช่น การควบคุมการพัฒนาโปรแกรม การแปลงข้อมูล และการควบคุมเครือข่าย เป็นต้น ในกรณีที่องค์กรที่ทำการตรวจสอบมีการควบคุมภายในอยู่แล้ว แต่ถ้าความสูญเสียมีค่าสูงจนยอมรับไม่ได้แล้ว ต้องพิจารณาการควบคุมใหม่ๆ ขึ้นมา

ขั้นตอนสุดท้าย คือแสดงสิ่งที่สามารถประหยัดได้ต่อปีจากการมีระบบการควบคุม โดยประสิทธิผลของการควบคุมคือสามารถลดมูลค่าความเสียหายที่อาจเกิดขึ้นต่อปี หรืออาจกล่าวอีกนัยหนึ่งคือ ค่าใช้จ่ายในการติดตั้งระบบควบคุมที่จ่ายไป น้อยกว่าความสามารถในการประหยัดค่าความเสียหายที่อาจเกิดขึ้น ตารางที่ 4 และ 5 แสดงให้เห็นถึงการคำนวณการประหยัดที่ได้จากการควบคุม อนึ่ง ในขั้นตอนนี้ผู้สอบบัญชีสามารถกำหนดวิธีการตรวจสอบที่เหมาะสมด้วยเช่นกัน

ตารางที่ 4 การพิสูจน์โปรแกรมการควบคุมการเข้าถึง

รายการ	จำนวนเงิน
ความเสี่ยง: การเปิดเผยข้อมูลที่เป็นความลับ	
ค่าใช้จ่ายในการจัดสร้างข้อมูลให้ถูกต้อง 1,000,000 โดยโอกาสที่จะเกิดเท่ากับ 10% ต่อปี	100,000
ความมีประสิทธิผลของโปรแกรมควบคุมการเข้าถึงข้อมูล 60%	-60,000
ค่าใช้จ่ายของโปรแกรมควบคุมการเข้าถึง	25,000
ประมาณการค่าใช้จ่ายต่อปีเนื่องจากการสูญหายและการควบคุม (100,000 – 60,000 + 25,000)	65,000
การประหยัด (100,000 – 65,000)	35,000

ตารางที่ 5 การวิเคราะห์ต้นทุนและผลประโยชน์ของการทดแทนการเข้าถึงเครือข่าย

รายการ	จำนวนเงิน
ความเสี่ยง	
การเข้าถึงข้อมูลและโปรแกรมที่ไม่ได้รับอนุมัติ: 100,000 โดยโอกาสที่จะเกิดเท่ากับ 2% ต่อปี	2,000
การใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุมัติ 10,000 โดยโอกาสที่จะเกิดเท่ากับ 40% ต่อปี	4,000
ประมาณการการสูญเสียต่อปี	6,000
ประสิทธิภาพของการควบคุมของเครือข่าย: 100%	-6,000
ค่าใช้จ่ายของการควบคุม	
ฮาร์ดแวร์ (50,000 ตัดค่าเสื่อม 5 ปี)	10,000
ซอฟต์แวร์ (20,000 ตัดค่าเสื่อม 5 ปี)	4,000
การสนับสนุนจากบุคลากร (รายปี)	40,000
ค่าใช้จ่ายรายปี	54,000
ประมาณการการสูญเสียรายปี 6,000-6,000+54,000	54,000
การประหยัด 6,000 – 54,000	-48,000

ข้อโต้แย้งต่อการวิเคราะห์ความเสี่ยง (Arguments Against Risk Analysis)

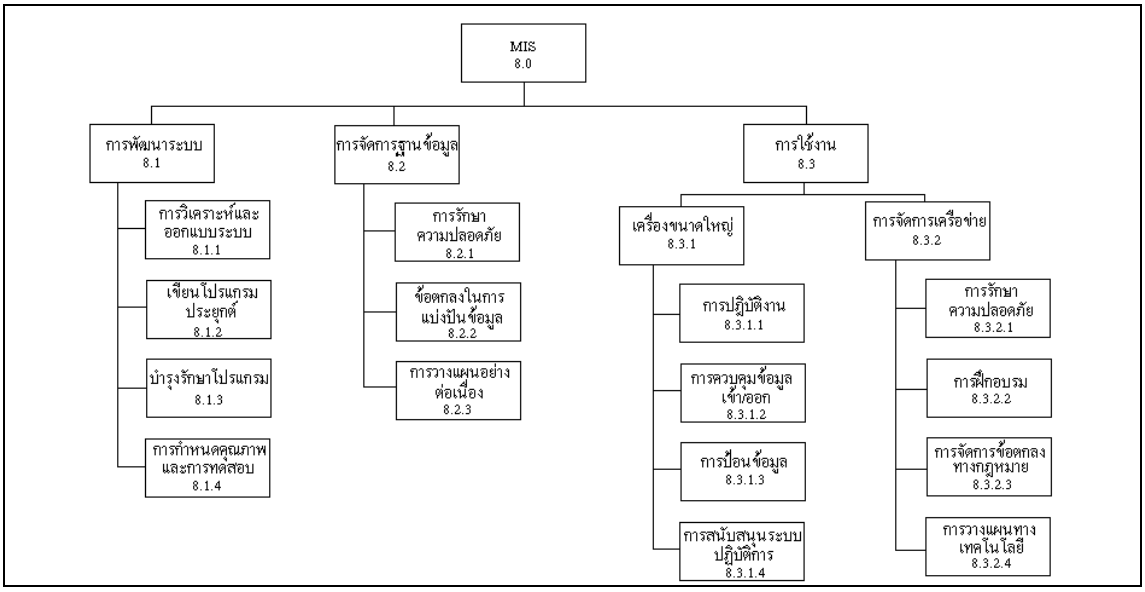
จะเห็นได้ว่าการวิเคราะห์ความเสี่ยงข้างต้นนี้ ผู้สอบบัญชีจำเป็นต้องกำหนดมูลค่าความเสียหายที่อาจเกิดขึ้นและประสิทธิภาพของการควบคุมที่จัดให้มีขึ้น โดยในการวิเคราะห์ความเสี่ยงในบางครั้งจะไม่มีการคำนวณมูลค่าดังกล่าว แต่จะกะประมาณโอกาสที่จะเกิดข้อผิดพลาดเท่านั้น ทำให้เกิดข้อโต้แย้งในการใช้การวิเคราะห์ความเสี่ยงโดยคำนึงถึงมูลค่าเป็นหลักดังกล่าวข้างล่าง

1. **ตัวเลขที่นำมาใช้ในการวิเคราะห์ความเสี่ยงเป็นตัวเลขที่ไม่ถูกต้อง** เป็นเพียงตัวเลขประมาณการเท่านั้น ซึ่งส่งผลให้ผู้ใช้บางคนอาจให้ความสำคัญกับตัวเลขมากจนเกินไป กล่าวคือเน้นการควบคุมกับจุดที่มีมูลค่าของความเสี่ยงสูง โดยละเลยจุดที่มีมูลค่าของความเสี่ยงต่ำ เป็นต้น
2. **ไม่มีการเปลี่ยนแปลง** ในทางอุดมคติแล้ว การวิเคราะห์ความเสี่ยงควรปรับปรุงทุกปี อย่างไรก็ตามในทางปฏิบัติมักจะใช้ตัวเลขของปีก่อนหน้าแทนที่จะวิเคราะห์และประเมินค่าใหม่ทุกปี
3. **ไม่อยู่บนพื้นฐานทางวิทยาศาสตร์** อย่างไรก็ตามการที่กล่าวว่าการวิเคราะห์ความเสี่ยงข้างต้นไม่ได้อยู่บนพื้นฐานทางวิทยาศาสตร์นั้นไม่เป็นความจริง เนื่องจากการวิเคราะห์ความเสี่ยงต้องนำทฤษฎีความเป็นไปได้และการวิเคราะห์ทางสถิติร่วมด้วย

วิธีการประเมินความเสี่ยงแบบ Renaissance Approach

การประเมินความเสี่ยงแบบ Renaissance Approach เป็นวิธีการที่ Gulf Canada Resources นำมาใช้ในการประเมินความเสี่ยงโดยให้ทั้งผู้สอบบัญชีและหน่วยงานผู้รับตรวจประเมินความเสี่ยงร่วมกัน ขั้นตอนในการประเมินความเสี่ยงมีดังนี้

1. กำหนดกลุ่มของหน้าที่งานที่จะตรวจสอบ ภาพที่ 3 แสดงหน้าที่งานของส่วนงานบริการด้านการจัดการระบบสารสนเทศ (เนื่องจากองค์กรที่ตรวจสอบจะมีหน้าที่งานเป็นจำนวนมาก จึงจัดกลุ่มงานออกเป็นส่วนย่อย ๆ ในที่นี้สมมุติว่า ส่วนงานบริการด้านการระบบสารสนเทศ เป็นกลุ่มงานที่ 8 ของโครงสร้างองค์กร)



ภาพที่ 3 หน้าที่งานของส่วนงานบริการด้านการจัดการระบบสารสนเทศ

2. เนื่องจากโอกาสที่จะเกิดความเสี่ยงในแต่ละสถานการณ์แตกต่างกันออกไป จึงต้องกำหนดอัตราสองอัตราด้วยกัน คือ อัตราแรกคือ
   - อัตราความเป็นไปได้ที่แต่ละปัจจัยความเสี่ยง (Risk factors) จะเกิดขึ้นกับแต่ละหน้าที่งาน โดย 0 = ไม่มีความเสี่ยง 1 = ความเสี่ยงน้อย 2 = ความเสี่ยงปานกลาง 3 = ความเสี่ยงสูง
   - ความเป็นไปได้ที่แต่ละปัจจัยความเสี่ยงจะเกิดขึ้น ซึ่งมีค่าอยู่ระหว่าง 0 และ 1

ตารางที่ 6 และ 7 แสดงถึงความเป็นไปได้ของปัจจัยความเสี่ยงและภัยของความเสี่ยงที่อาจจะเกิดขึ้น (Risk Eexposures) แยกตามปัจจัยความเสี่ยงและหน้าที่งานของส่วนงานที่จะตรวจสอบ โดยปัจจัยที่ก่อให้เกิดความเสี่ยงประกอบด้วย 10 ปัจจัยด้วยกันคือ ขนาดของงาน (Size of Unit) ความซับซ้อนของการปฏิบัติงาน (Complexity of Operations) สภาพคล่องของทรัพย์สิน (Liquidity of Assets) ความสนใจของผู้บริหาร (management interest) การเปลี่ยนแปลงบุคลากรหรือระบบที่สำคัญ (Change of Key Personnel or System) การปฏิบัติตามกฎข้อบังคับ (Compliance with Rregulations) ขอบเขตการใช้คอมพิวเตอร์ (Extent of Use of the Computer) สภาพที่เป็นความลับ (Confidentiality) ระยะเวลาการตรวจสอบครั้งก่อน (Time Ssince Llast Aaudit) จุดแข็งของการควบคุมระบบ (Strength of System of Controls)

ตารางที่ 6 ความเป็นไปได้ที่แต่ละปัจจัยความเสี่ยงจะเกิดขึ้น

	ปัจจัยเสี่ยง	ความเป็นไปได้
A	ขนาดของงาน	0.12
B	ความซับซ้อนของการปฏิบัติงาน	0.12
C	สภาพคล่องของทรัพย์สิน	0.10
D	ความสนใจของผู้บริหาร	0.06
E	การเปลี่ยนแปลงบุคลากรหรือระบบที่สำคัญ	0.10
F	การปฏิบัติตามกฎข้อบังคับ	0.10
G	ขอบเขตการใช้คอมพิวเตอร์	0.05
H	สภาพที่เป็นความลับ	0.05
I	ระยะเวลาการตรวจสอบครั้งก่อน	0.15
J	จุดแข็งของการควบคุมระบบ	0.15
	ยอดรวมค่าความเป็นไปได้	**1.00**

ตารางที่ 7 ภัยของความเสี่ยงที่อาจจะเกิดขึ้นแยกตามปัจจัยความเสี่ยง และหน้าที่งานของส่วนงานบริการด้านระบบสารสนเทศ

รหัส	หน้าที่งาน	A	B	C	D	E	F	G	H	I	J
8.1.1	การวิเคราะห์และออกแบบระบบ	3	2	3	1	1	0	2	0	3	3
8.1.2	เขียนโปรแกรมประยุกต์	1	2	3	1	0	1	1	0	3	3
8.1.3	บำรุงรักษาโปรแกรม	3	2	2	2	0	1	1	0	3	3
8.1.4	การกำหนดคุณภาพและทดสอบ	3	2	3	0	0	1	1	0	3	3
8.2.1	การรักษาความปลอดภัย	3	2	3	1	0	1	1	0	3	3
8.2.2	ข้อตกลงในการแบ่งปันข้อมูล	3	2	0	0	0	1	0	1	3	3
8.2.3	การวางแผนอย่างต่อเนื่อง	3	2	1	3	0	2	0	0	3	3
8.3.1.1	การปฏิบัติงาน	3	2	3	2	1	0	2	0	3	3
8.3.1.2	การควบคุมข้อมูลเข้า/ออก	3	1	3	1	0	2	2	0	3	3
8.3.1.3	การป้อนข้อมูล	3	1	3	1	0	2	2	0	3	3
8.3.1.4	การสนับสนุนระบบปฏิบัติการ	3	2	3	1	0	1	2	0	3	3
8.3.2.1	การรักษาความปลอดภัย	3	2	3	1	0	2	1	0	3	3
8.3.2.2	การฝึกอบรม	3	3	3	1	0	1	1	0	3	3
8.3.2.3	การจัดการข้อตกลงทางกฎหมาย	3	2	3	1	0	2	1	0	3	3
8.3.2.4	การวางแผนทางเทคโนโลยี	3	2	3	1	0	2	1	0	3	3

3. นำค่าที่กำหนดในตารางที่ 6 และ 7 มาคูณกันเพื่อหาค่าในตารางที่ 8

ตารางที่ 8 น้ำหนักของภัยของความเสี่ยงที่อาจจะเกิดขึ้นแยกตามปัจจัยความเสี่ยง และหน้าที่งานของส่วนงานบริการด้านระบบสารสนเทศ

หน้าที่งาน	A	B	C	D	E	F	G	H	I	J	รวม
การวิเคราะห์และออกแบบระบบ	0.36	0.24	0.30	0.06	0.10	0.00	0.10	0.00	0.45	0.45	2.06
เขียนโปรแกรมประยุกต์	0.12	0.24	0.30	0.06	0.00	0.10	0.05	0.00	0.45	0.45	1.77
บำรุงรักษาโปรแกรม	0.36	0.24	0.20	0.12	0.00	0.10	0.05	0.00	0.45	0.45	1.97
การกำหนดคุณภาพและทดสอบ	0.36	0.24	0.30	0.00	0.00	0.10	0.05	0.00	0.45	0.45	1.95
การรักษาความปลอดภัย	0.36	0.24	0.30	0.06	0.00	0.10	0.05	0.00	0.45	0.45	2.01
ข้อตกลงในการแบ่งปันข้อมูล	0.36	0.24	0.00	0.00	0.00	0.10	0.00	0.05	0.45	0.45	1.65
การวางแผนอย่างต่อเนื่อง	0.36	0.36	0.10	0.18	0.00	0.20	0.00	0.00	0.45	0.45	2.10
การปฏิบัติงาน	0.36	0.24	0.30	0.12	0.10	0.00	0.10	0.00	0.45	0.45	2.12
การควบคุมข้อมูลเข้า/ออก	0.36	0.12	0.30	0.06	0.00	0.20	0.10	0.00	0.45	0.45	2.04
การป้อนข้อมูล	0.36	0.12	0.30	0.06	0.00	0.20	0.10	0.00	0.45	0.45	2.04
การสนับสนุนระบบปฏิบัติการ	0.36	0.24	0.30	0.06	0.00	0.10	0.10	0.00	0.45	0.45	2.06
การรักษาความปลอดภัย	0.36	0.24	0.30	0.06	0.00	0.20	0.05	0.00	0.45	0.45	2.11
การฝึกอบรม	0.36	0.36	0.30	0.06	0.00	0.10	0.05	0.00	0.45	0.45	2.13
การจัดการข้อตกลงทางกฎหมาย	0.36	0.24	0.30	0.06	0.00	0.20	0.05	0.00	0.45	0.45	2.11
การวางแผนทางเทคโนโลยี	0.36	0.24	0.30	0.06	0.00	0.20	0.05	0.00	0.45	0.45	2.11

4. วางแผนการตรวจสอบ ในขั้นตอนนี้ผู้สอบบัญชีต้องกำหนดว่าหน้าที่งานใดของส่วนงานที่จะทำการตรวจสอบ (การกำหนดนี้จะจัดทำขึ้นในกรณีที่มีกำลังคนน้อยไม่สามารถตรวจสอบได้ทั้งหมด) อนึ่ง ในขั้นตอนนี้ผู้สอบบัญชีจะกำหนดว่า
   - หน้าที่งานใดเป็นหน้าที่งานที่ต้องตรวจสอบ (Mandatory) เนื่องจากงานที่ต้องตรวจสอบนั้นผู้สอบบัญชีต้องทำการตรวจสอบอย่างไม่มีทางเลือก
   - หน้าที่งานใดเป็นหน้าที่งานที่ต้องให้ความระมัดระวัง (Discretionary) กล่าวคือเป็นหน้าที่งานที่ผู้สอบบัญชีต้องคัดเลือกว่าจะตรวจสอบหน้าที่งานใดเป็นจำนวนเท่าไร ตารางที่ 9 เป็นตารางที่แสดงให้เห็นถึงจำนวนหน้าที่งานที่จะตรวจสอบ โดยหน้าที่งานที่มีความเสี่ยงสูง จะเลือกตรวจสอบทั้งหมดเท่ากับ 100% ถ้ามีความเสี่ยงปานกลาง จะสุ่มตรวจสอบหน้าที่งานเท่ากับ 50% ในขณะที่หน้าที่งานที่มีความเสี่ยงต่ำ จะสุ่มตรวจสอบ 25% และท้ายที่สุดหน้าที่งานที่ไม่มีความเสี่ยงจะสุ่มตรวจสอบ 10% ดังนั้นยอดรวมของจำนวนตัวอย่างที่สุ่มตรวจสอบมีค่าเท่ากับ 37% (=.10*100 + .30*50 + .40*25 + .2*10)

ตารางที่ 10 เป็นตารางแสดงจำนวนหน้าที่งานที่จะตรวจสอบโดยนำข้อมูลในตารางที่ 8 และ 9 มากำหนดจำนวนหน้าที่งานที่จะตรวจสอบ อนึ่ง การสุ่มจำนวนหน้าที่งานสามารถใช้วิธีการสุ่มตัวอย่างโดยทั่วไป

ตารางที่ 9 จำนวนหน้าที่งานที่จะตรวจสอบ

ระดับความเสี่ยง	ระดับชั้นของหน้าที่งาน	จำนวนส่วนงานที่จะตรวจสอบ
ความเสี่ยงสูง (3)	10%	100%
ความเสี่ยงปานกลาง (2)	30%	50% (สุ่มตัวอย่าง)
ความเสี่ยงต่ำ (1)	40%	25% (สุ่มตัวอย่าง)
ไม่มีความเสี่ยง (0)	20%	10% (สุ่มตัวอย่าง)
	100%	**37% (ยอดรวมจำนวนตัวอย่างที่จะตรวจสอบ)**

ตารางที่ 10 จำนวนหน้าที่งานที่จะตรวจสอบของส่วนงานบริการด้านระบบสารสนเทศ

ระดับความเสี่ยง	ระดับชั้นของหน้าที่งาน*	จำนวนส่วนงานที่จะตรวจสอบ
ความเสี่ยงสูง (3)	0%	100%(สุ่มตัวอย่าง)
ความเสี่ยงปานกลาง (2)	73.33% (=11/15)	50% (สุ่มตัวอย่าง)
ความเสี่ยงต่ำ (1)	26.67% (=4/15)	25%(สุ่มตัวอย่าง)
ไม่มีความเสี่ยง (0)	0%	10%(สุ่มตัวอย่าง)
	100%	**43.33%**

* ตัวเลขระดับชั้นของหน้าที่งานคำนวณจากการหารจำนวนรวมของระดับความเสี่ยงแต่ละระดับด้วยหน้าที่งานทั้งหมด (ดังแสดงในตารางที่ 8)

จะเห็นได้ว่าการประเมินความเสี่ยงแบบ Renaissance Approach เป็นการประเมินความเสี่ยงที่คำนึงถึงองค์ประกอบย่อย ๆ ของระบบคอมพิวเตอร์มากกว่าการประเมินต้นทุนและผลประโยชน์

บทสรุป

จากขั้นตอนการประเมินความเสี่ยงทางคอมพิวเตอร์ที่กล่าวข้างต้น พบว่าไม่ว่าการประเมินความเสี่ยงจะเป็นแบบใดก็ตาม (การประเมินความเสี่ยงโดยพิจารณาจากต้นทุนและผลประโยชน์ หรือการประเมินความเสี่ยงแบบ Renaissance Approach) การประเมินความเสี่ยงจะมีลักษณะที่เหมือนกันตรงที่ผู้ประเมินต้องกะประมาณอัตราความเป็นไปได้ที่จะเกิดความเสี่ยง ซึ่งความถูกต้องของการประมาณการตัวเลขดังกล่าวจะส่งผลต่อความถูกต้องหรือใกล้เคียงของการประเมินความเสี่ยง นอกจากนี้ผู้ประเมินความเสี่ยงควรมีความรู้และความเข้าใจเกี่ยวกับลักษณะของสิ่งที่จะประเมินความเสี่ยง เพื่อให้สามารถกะประมาณอัตราความเป็นไปได้ที่จะเกิดความเสี่ยงได้อย่างเหมาะสม ซึ่งการที่จะประมาณตัวเลขได้อย่างเหมาะสมนั้นมักขึ้นกับประสบการณ์ของผู้ประเมินเป็นหลัก อย่างไรก็ตามแนวทางการพิจารณาความเสี่ยงสามารถนำไปใช้ประกอบการวิเคราะห์ความเสี่ยงในเบื้องต้นได้เช่นกัน

บรรณานุกรม

Bjelke Sten. (2001), "Risk Assessment – Mission Impossible?", **ITAudit**, Vol 4, September, (http://itaudit.org).

Boccasam Prashanth V. (2003), "Continuous Monitoring of Enterprise Application Risks", **ITAudit**, Vol 6, May 15, (http://itaudit.org).

Hinson Gary. (2000), "A Practical Model for Risk Assessment and Prioritization", **ITAudit**, Vol 3, April 1, (http://itaudit.org).

Information Systems Audit and Control Association. (2003), "**Information system Risk Procedure**", July, (http://www.isaca.org).

Kanter Howard A. and Pitman Marshall K. (1997), "Audit Risk Assessment: A Renaissance Approach", **IS Audit and Control Journal**, Vol 1, p. 34-39.

Manello Carl and Rocholl William. (1997), "Security Evaluation a Methodology for Risk Assessment", **IS Audit and Control Journal**, Vol. 6, p. 42-46.

Marchany Randy. (2002), "Seven-step IT Risk Assessment", **ITAudit**, Vol 5, March 1, (http://itaudit.org).

McNamee David and Selim Georges. (1988), "**Changing the Paradigm**", October, (http://www.mc2consulting.com/riskart8.htm).

Ozier Will. (2003), "Risk Metrics Needed for IT Security", **ITAudit**, Vol 6, April 1, (http://itaudit.org).

Pfleeger Charles P. and Pfleeger Shari Lawrence. (2003), **Security in Computing**, third edition, Pearson Education, Inc, USA.

Virginia Tech, Information Resources and Technology Security. (2000), "**Business Impact Analysis/ Risk Assessment for Information Assets General Information & Process**", December, (http://state.vipnet.orq/cts/).

Weber Ron. (1999), **Information Systems Control and Audit**, Prentice Hall, USA.

ภาคผนวก

David McNamee แสดงให้เห็นความแตกต่างระหว่างการตรวจสอบในรูปแบบเดิมและการตรวจสอบในรูปแบบใหม่ที่เน้นการประเมินความเสี่ยงเป็นหลักตามตาราง ก ข้างล่าง

ตาราง ก ตารางการเปลี่ยนแปลงรูปแบบการตรวจสอบ

รายการ	รูปแบบเดิม	รูปแบบใหม่
ประเด็นที่สนใจ	การควบคุมภายใน	ความเสี่ยงของธุรกิจ
ลักษณะการตรวจสอบ	- เป็นการตรวจสอบภายหลังจากรายการเกิดขึ้นแล้ว - สังเกตการณ์แผนกลยุทธ์ในขั้นต้นเท่านั้น ไม่มีความต่อเนื่อง	- เป็นการตรวจสอบระหว่างการเกิดรายการ - ติดตามและมีส่วนร่วมในแผนกลยุทธ์อย่างต่อเนื่อง
การประเมินความเสี่ยง	ปัจจัยความเสี่ยง	ประเมินความเสี่ยงในระดับย่อยในเรื่องเกี่ยวกับ การฉ้อโกง การจัดการวิกฤตการณ์ และความหายนะ เพื่อให้สามารถสอบทานการฉ้อโกงก่อนที่จะเกิดขึ้น พร้อมทั้งเปลี่ยนแปลงการควบคุมหรือการออกแบบระบบให้เหมาะสมกับการฉ้อโกงที่อาจจะเกิดขึ้น
การตรวจสอบ	จุดควบคุมที่สำคัญ	ความเสี่ยงที่สำคัญ
วิธีการตรวจสอบ	เน้นการทดสอบการควบคุมในรายละเอียด	เน้นการควบคุมความเสี่ยงที่สำคัญขององค์กร
ข้อเสนอแนะการตรวจสอบ	จุดแข็ง ต้นทุนและผลประโยชน์ และความมีประสิทธิภาพและประสิทธิผลของการควบคุมภายใน	หลีกเลี่ยง โอน และควบคุมความเสี่ยง
รายงานการตรวจสอบ	กล่าวถึงการควบคุมหน้าที่งานต่าง ๆ	กล่าวถึงความเสี่ยง
บทบาทของผู้ตรวจสอบ	ประเมินหน้าที่งานโดยอิสระ	ผสมผสานการจัดการความเสี่ยงและ Corporate Governance

* คัดลอกจาก McNamee และ Selim (1988)