การตรวจสอบด้านเทคโนโลยีสารสนเทศ ตามแนวทางการประเมินความเสี่ยง

(IT – RBS)

(Information Technology – Risk Based Supervision)

คำนำ

การจัดทำคู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศของสายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย ในครั้งนี้เป็นการ**ปรับปรุงแนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศใหม่ตามมาตรฐานสากลที่องค์กรกำกับดูแลสถาบันการเงินประเทศต่าง ๆ ใช้เป็นแนวทางในการกำกับตรวจสอบสถาบันการเงิน (สง.)** ทั้งนี้ โดย**ได้รับการสนับสนุนจากธนาคารโลก (World Bank) ที่ได้ให้ผู้เชี่ยวชาญมาให้ความรู้ คำแนะนำ และแลกเปลี่ยนประสบการณ์เพื่อจัดทำแนวทางการตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Information Technology – Risk Based Supervision หรือ IT-RBS) เพื่อให้ผู้ตรวจสอบได้ใช้เป็นแนวทางในการประเมินและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนั้นยังเป็นประโยชน์กับสถาบันการเงินที่จะสามารถใช้แนวทางดังกล่าวในการบริหารจัดการและควบคุมติดตามความเสี่ยงด้าน IT ของสถาบันการเงินที่มีการดูแลความเสี่ยงในการทำธุรกรรมทางการเงินโดยใช้เทคโนโลยีสารสนเทศอีกด้วย**

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศหวังว่า คู่มือการตรวจสอบสถาบันการเงินด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยง (IT-RBS) ทั้งหมดนี้จะช่วยให้การปฏิบัติงานตรวจสอบและประเมินความเสี่ยงที่เกี่ยวข้องกับสถาบันการเงินของผู้ตรวจสอบเป็นตามมาตรฐานสากลและมีประสิทธิภาพมากยิ่งขึ้น อย่างไรก็ดีผู้ตรวจสอบจำเป็นต้องติดตามและพัฒนาเทคนิควิธีการตรวจสอบ ไปพร้อมกับการใช้คู่มือตรวจสอบด้านเทคโนโลยีสารสนเทศทุกฉบับที่ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศได้พัฒนาขึ้นมาก่อนหน้านี้และคู่มือที่จะพัฒนาเพิ่มขึ้นในภายหลัง เพื่อให้ทันกับพัฒนาการทางด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไปอย่างรวดเร็ว

อนึ่ง ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศขอกราบขอบพระคุณคณะผู้บริหารระดับสูงของสายกำกับสถาบันการเงินซึ่งประกอบด้วยท่าน ผู้ช่วยผู้ว่าการสายกำกับสถาบันการเงิน ผู้อำนวยการอาวุโส และผู้อำนวยการ ทุกท่านที่ได้กรุณาให้คำแนะนำอันเป็นประโยชน์ในการปรับปรุงเนื้อหาและแนวทางในการพัฒนาคู่มือตรวจสอบ และขอขอบคุณคณะทำงานในการพัฒนาคู่มือฯ ซึ่งประกอบไปด้วยผู้บริหารทีม และผู้ตรวจสอบอาวุโสในส่วนตรวจสอบเทคโนโลยีสารสนเทศ ที่ได้ทุ่มเทความพยายามในการเรียบเรียงคู่มือซึ่งมีเนื้อหาทางด้านเทคนิคที่ค่อนข้างยากที่จะเข้าใจให้กลายเป็นคู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศที่ง่ายต่อความเข้าใจและสามารถนำไปใช้ปฏิบัติงานได้จริง

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ

ธันวาคม 2551

สารบัญ

บทนำ

แนวทางการตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Information Technology – Risk Based Supervision หรือ IT-RBS) เป็นกรอบใหญ่ของกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ คู่มือแนวทางการตรวจสอบ ฯ ได้วางแนวทางในการตรวจสอบด้านเทคโนโลยีสารสนเทศออกเป็น 2 ส่วนใหญ่ๆ คือ ส่วนแรกเป็นกรอบในการพิจารณาประสิทธิภาพในการดำเนินงานของฝ่ายจัดการ ซึ่งครอบคลุมในหัวข้อที่เกี่ยวข้องกับกระบวนการบริหารการจัดการการตรวจสอบด้าน IT การบริหารระบบข้อมูลสารสนเทศเพื่อการบริหาร (MIS) และการบริการงาน IT Outsourcing ส่วนที่สองเป็นเรื่องการประเมินประสิทธิภาพของการดำเนินงานประจำวัน ซึ่งเกี่ยวข้องกับระบบการรักษาความปลอดภัย (Security) ความถูกต้องเชื่อถือได้ของข้อมูล (Integrity) และความพร้อมใช้งานของระบบงานและข้อมูล (Availability) ตามลำดับ

อย่างไรก็ดี คู่มือ IT-RBS ฉบับนี้เป็นเพียงกรอบแนวทางในการตรวจสอบ ส่วนรายละเอียดของเรื่องที่จะต้องตรวจสอบและวิธีการตรวจสอบจะถูกแยกออกไปเป็นคู่มือตรวจสอบด้าน IT เฉพาะเรื่องต่างๆ เช่น คู่มือตรวจสอบการการจัดการ คู่มือตรวจสอบ IT Governance และคู่มือตรวจสอบการตรวจสอบภายในและภายนอก เป็นต้น ดังนั้น ผู้ตรวจสอบหรือผู้บริหารสถาบันการเงินที่ประสงค์จะนำแนวทางการตรวจสอบ IT-RBS ไปใช้งานจะต้องศึกษาและทำความเข้าใจทั้งกรอบแนวทางในการตรวจสอบด้าน IT ตามคู่มือ IT-RBS และต้องศึกษาคู่มือตรวจสอบเฉพาะด้านต่างๆ ประกอบจึงจะสามารถดำเนินการได้ตามวัตถุประสงค์

อนึ่ง คู่มือการตรวจสอบ IT-RBS เป็นแนวทางในการตรวจสอบด้านเทคโนโลยีสารสนเทศใหม่ตามมาตรฐานสากลที่องค์กรกำกับดูแลสถาบันการเงินประเทศต่าง ๆ ใช้เป็นแนวทางในการกำกับตรวจสอบสถาบันการเงิน และมีความสอดคล้องกับแนวทางในการบริหารและตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ COBIT ทั้งนี้ ในขั้นตอนของการพัฒนาแนวทางการตรวจสอบตามคู่มือ IT-RBS ธปท.ได้รับการสนับสนุนจากธนาคารโลก (World Bank) ในการส่งผู้เชี่ยวชาญมาให้ความรู้ คำแนะนำ และแลกเปลี่ยนประสบการณ์เพื่อจัดทำแนวทางการตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Information Technology – Risk Based Supervision หรือ IT-RBS) เพื่อให้ผู้ตรวจสอบได้ใช้เป็นแนวทางในการประเมินและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนั้นยังเป็นประโยชน์กับสถาบันการเงินที่จะสามารถใช้แนวทางดังกล่าวในการบริหารจัดการและควบคุมติดตามความเสี่ยงด้าน IT ของสถาบันการเงินที่มีการดูแลความเสี่ยงในการทำธุรกรรมทางการเงินโดยใช้เทคโนโลยีสารสนเทศอีกด้วย

คู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศเล่มนี้ประกอบด้วยเนื้อหาหลัก 2 ส่วน คือ

ส่วนที่ 1 ความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศของสถาบันการเงิน

ส่วนที่ 2 การตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยง

ประเด็นสำคัญในคู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศเล่มนี้จะประกอบด้วยเรื่องต่าง ๆ ดังต่อไปนี้

1. ความเสี่ยงที่เกิดจากการใช้เทคโนโลยีในการดำเนินงาน ผลิตภัณฑ์การให้บริการ การบริหารช่องทาง การส่งมอบและกระบวนการพิจารณาความเสี่ยงในด้านต่าง ๆ โดยเฉพาะอย่างยิ่งความเสี่ยงด้านกลยุทธ์และความเสี่ยงด้านการปฏิบัติงาน

2. การประเมินการบริหารความเสี่ยงของสถาบันการเงินในการระบุ วัดผล ติดตามและควบคุมความเสี่ยงของตนเอง โดยความเสี่ยงที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศควรมีการสอบทานไปพร้อมกับความเสี่ยงด้านอื่น ๆ ของสถาบันการเงิน

3. เมื่อมีการพิจารณาและนำเทคโนโลยีมาใช้งานแล้ว ผู้บริหารของสถาบันการเงินจะต้องกำหนดกระบวนการวิเคราะห์ความเสี่ยงที่เข้มงวด เพื่อระบุถึงระดับความเสี่ยง ความเป็นไปได้และสามารถควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

4. กระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีจะมีองค์ประกอบที่สำคัญ 3 ประการคือ

4.1 แผนงานการใช้เทคโนโลยี

4.2 การตัดสินใจในการนำเทคโนโลยีมาใช้

4.3 การวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น

ทั้งสามประการดังกล่าวเป็นเรื่องสำคัญที่มีผลกระทบต่อกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยี เพื่อให้การนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจของสถาบันการเงินมีประสิทธิผลคุ้มค่ากับการลงทุนไม่ว่าสถาบันการเงินนั้นจะมีขนาดเพียงใดก็ตาม

ส่วนที่ 1 ความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีมาใช้โดยมีผลกระทบถึงระบบงานและการปฏิบัติงาน ซึ่งอาจก่อให้เกิดความเสียหายต่อเงินกองทุนและรายได้ของสถาบันการเงิน

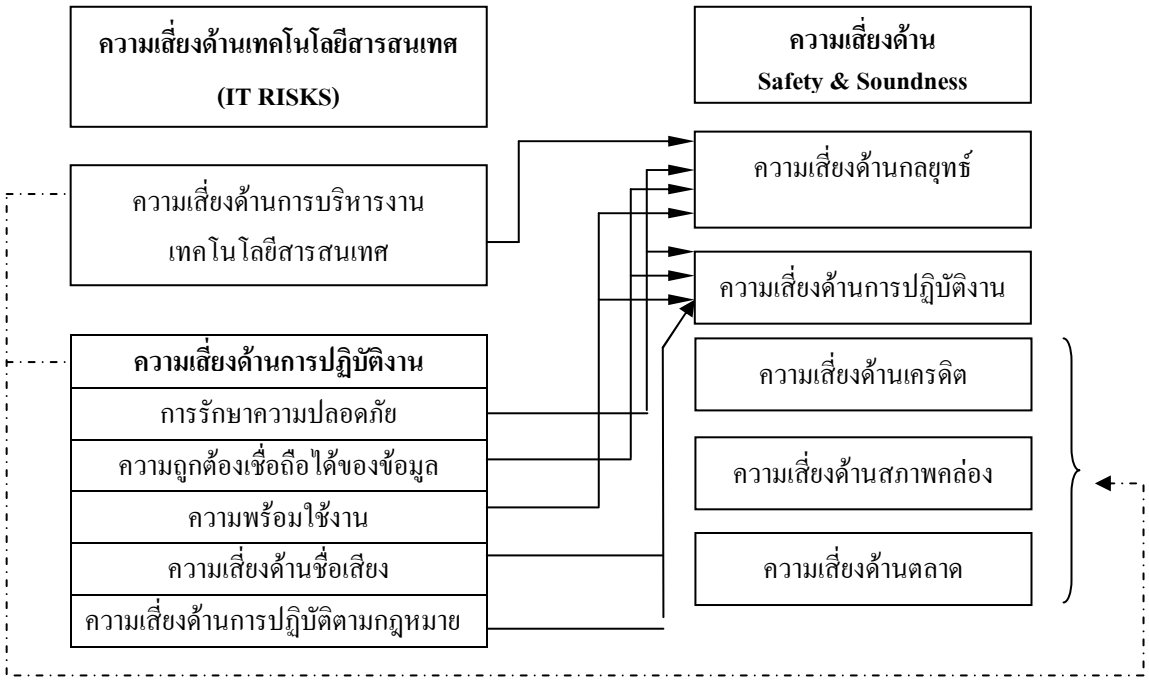
ความเสี่ยงที่มีอยู่มิใช่ว่าจะเป็นปัญหาเสมอไป แม้จะมีความเสี่ยงสูงในพื้นที่ใดพื้นที่หนึ่งก็มิใช่เป็นเรื่องที่ต้องกังวลเสมอไป ตราบใดที่การบริหารความเสี่ยงมีประสิทธิภาพในการจัดการกับระดับความเสี่ยงนั้น การมองความเสี่ยงไปข้างหน้าผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศควรพิจารณาว่า ความเสี่ยงที่สถาบันการเงินกำหนดขึ้นมีเหตุผลสมควรหรือไม่ โดยทั่ว ๆ ไปแล้วความเสี่ยงนั้นควรจะสามารถระบุได้ ทำความเข้าใจได้ วัดผลได้ ติดตามและควบคุมได้ สถาบันการเงินควรที่จะสามารถดำเนินการใด ๆ เพื่อควบคุมภัยพิบัติทางการเงินเมื่อเกิดความเสี่ยงเหล่านั้นได้อย่างทันท่วงที แต่**ถ้าพิจารณาแล้วเห็นว่าเป็นความเสี่ยงที่ไม่สามารถเข้าใจได้ วัดผลไม่ได้ ขาดการควบคุม ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องติดต่อผู้บริหารหรือคณะกรรมการบริหารเพื่อแจ้งให้ทราบถึงความจำเป็นที่จะต้องดำเนินการขจัดความเสี่ยงที่มากเกินความจำเป็นออกไป** ซึ่งการดำเนินการนั้นอาจหมายถึงการลดโอกาสที่จะเกิดความเสี่ยงการเพิ่มเงินกองทุน และ/หรือทำให้กระบวนการบริหารความเสี่ยงมีประสิทธิภาพมากขึ้น

ธนาคารแห่งประเทศไทยได้กำหนดความเสี่ยงด้านฐานะและการดำเนินงานของสถาบันการเงิน (Safety & Soundness) เป็น 5 ประเภท เพื่อความมุ่งหมายในการกำกับดูแลสถาบันการเงิน คือ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านเครดิต ความเสี่ยงด้านการตลาด ความเสี่ยงด้านสภาพคล่อง และความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงทั้ง 5 ประเภทนี้ ไม่สามารถแยกจากกันได้โดยเด็ดขาด บางผลิตภัณฑ์หรือบริการอาจทำให้สถาบันการเงินประสบกับความเสี่ยงหลาย ๆ ด้าน และความเสี่ยงอาจไม่เป็นอิสระต่อกัน ซึ่งความเสี่ยงประเภทหนึ่งเพิ่มขึ้นอาจไปเพิ่มความเสี่ยงประเภทอื่นด้วย ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศควรทราบถึงการมีผลกระทบระหว่างความเสี่ยงประเภทต่าง ๆ และประเมินผลกระทบในลักษณะที่ครอบคลุมความเสี่ยงโดยรวม และที่เกิดขึ้นอย่างสม่ำเสมอ

การดำเนินงานด้านเทคโนโลยีสารสนเทศสามารถก่อให้เกิดความเสี่ยงต่อสถาบันการเงินได้ด้วยเช่นกัน ดังนั้น ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศจำเป็นต้องปฏิบัติตามแนวทางการตรวจสอบเพื่อประเมิน**ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk)** โดย**จะพิจารณาความเสี่ยงออกเป็น 2 เรื่องใหญ่ ประกอบด้วย ความเสี่ยงด้านการบริหารงานด้านเทคโนโลยีสารสนเทศ และความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ**

ความเสี่ยงด้านเทคโนโลยีสารสนเทศมิได้แยกเป็นอิสระออกจากความเสี่ยงด้านฐานะและการดำเนินงาน (Safety & Soundness) ที่ประเมินโดยผู้ตรวจสอบ On-Site โดยสิ้นเชิง ในความเป็นจริงแล้วความเสี่ยงด้านเทคโนโลยีสารสนเทศจะส่งผลกระทบทั้งทางตรงและทางอ้อมต่อความเสี่ยงด้านฐานะและการดำเนินงาน ส่วนใหญ่ความเสี่ยงด้านฐานะและการดำเนินงานที่จะได้รับ**ผลกระทบโดยตรงจากการดำเนินงานด้านเทคโนโลยีสารสนเทศ คือความเสี่ยงด้านกลยุทธ์ และความเสี่ยงด้านการปฏิบัติงาน** สำหรับ**ความเสี่ยงด้านเครดิต ด้านสภาพคล่อง และด้านตลาดนั้นเป็นความเสี่ยงที่จะได้รับผลกระทบโดยอ้อม**ทั้งสิ้น ดังนั้น การพิจารณาเพื่อประเมินฐานะและความเสี่ยงของสถาบันการเงิน ผู้ตรวจสอบจำเป็นต้องนำแนวคิด Technology risk Integration ซึ่งเป็นการรวมความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (IT Risk) เข้ากับความเสี่ยงด้านฐานะและการดำเนินงาน โดยการพิจารณาว่า ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นกระทบกับความเสี่ยงที่เกี่ยวข้องกับฐานะและการดำเนินงานด้านใดบ้าง และผลการประเมินความเสี่ยงด้านฐานะและการดำเนินงานก็ควรจะสะท้อนถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วย

แผนผังแสดงความสัมพันธ์ระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงด้านฐานะและการดำเนินงาน (Safety & Soundness)



ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เนื่องจากการดำเนินงานด้านเทคโนโลยีสารสนเทศจะส่งผลกระทบโดยตรงต่อความเสี่ยงด้านฐานะและการดำเนินงานในส่วนที่เกี่ยวข้องกับความเสี่ยงด้านกลยุทธ์และความเสี่ยงด้านการปฏิบัติงาน ดังนั้น การพิจารณาความเสี่ยงด้านเทคโนโลยีสารสนเทศจะแบ่งออกเป็น 2 ประเภทหลัก ๆ คือ

1. ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ (IT Management Risk)
2. ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (Operational Risk)
   - 2.1 ความเสี่ยงที่เกี่ยวกับการรักษาความปลอดภัย (Security)
   - 2.2 ความเสี่ยงที่เกี่ยวกับความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)
   - 2.3 ความเสี่ยงที่เกี่ยวกับความพร้อมใช้งาน (Availability)
   - 2.4 ความเสี่ยงด้านชื่อเสียง (Reputation)
   - 2.5 ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Regulation)

1. ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ**เป็นความเสี่ยงซึ่งเกิดจากนโยบายและกลยุทธ์ขององค์กรที่ไม่เอื้ออำนวยต่อการดำเนินธุรกิจหรือกระบวนการตัดสินใจในการพัฒนาและนำระบบออกใช้งานจริงซึ่งส่งผลกระทบต่อรายได้และเงินกองทุน ความเสี่ยงที่เกิดจากความไม่สอดคล้องในเป้าหมายกลยุทธ์ขององค์กรและกลยุทธ์ทางธุรกิจ รวมทั้งคุณภาพในการนำกลยุทธ์ออกใช้งาน การนำทรัพยากรต่าง ๆ มาใช้ในการดำเนินกลยุทธ์ทางธุรกิจให้เหมาะสมและเกิดประโยชน์สูงสุด** ผู้บริหารองค์กรควรพิจารณาและยึดหลักธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance) ในการบริหารงานเพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพสูงสุด

ในการควบคุมความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศนั้น สถาบันการเงินควรพิจารณาถึงสภาพแวดล้อมโดยรวมทางธุรกิจ ความรู้และประสบการณ์ของผู้บริหารระดับสูงการนำเทคโนโลยีมาใช้ในผลิตภัณฑ์และการให้บริการที่เหมาะสมกับวงจรธุรกิจ รวมทั้งกำหนดนโยบายให้ครอบคลุมเรื่องการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ของข้อมูล และความพร้อมในการใช้งานของข้อมูล ตลอดจนมีระบบข้อมูลเพื่อการบริหาร (MIS) อย่างเพียงพอและตอบสนองผู้ใช้งานได้อย่างมีประสิทธิภาพ นอกจากนี้ สถาบันการเงินควรดำเนินการให้ฝ่ายตรวจสอบด้านเทคโนโลยีสารสนเทศสามารถตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศได้อย่างอิสระและมีขอบเขตการตรวจสอบครอบคลุมการปฏิบัติงานอย่างครบถ้วนสมบูรณ์

2. ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านการปฏิบัติงานเป็น**ความเสี่ยงที่เกิดขึ้นจากการที่สถาบันการเงินขาดการกำกับดูแลและการควบคุมภายในด้านเทคโนโลยีสารสนเทศอย่างเพียงพอ**ก่อให้เกิดปัญหาในการปฏิบัติงานซึ่งมีผลกระทบต่อรายได้และเงินกองทุน ความเสี่ยงประเภทนี้จะพิจารณาจากการควบคุมภายใน ระบบข้อมูลสารสนเทศ ความซื่อสัตย์ของพนักงาน และขั้นตอนการปฏิบัติงานในการให้บริการแก่ลูกค้า การพิจารณาความเสี่ยงด้านการปฏิบัติงานจะแบ่งออกได้ ดังนี้

2.1 **การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Security)**

การรักษาความปลอดภัยเป็นการพิจารณาสภาพแวดล้อมในการประมวลผลทั้งด้านกายภาพและตรรกะ (Physical & Logical) โดยจัดการป้องกันให้มีความเหมาะสมทั้งคุณค่าและความสำคัญของข้อมูล ซึ่งหลักเกณฑ์ในการมีระบบการรักษาความปลอดภัยที่ดีจะต้อง**สามารถป้องกันการเข้าถึง การเข้าไปแก้ไขเปลี่ยนแปลง การทำลาย หรือการเปิดเผยข้อมูล ทั้งระหว่างที่กำลังพัฒนาระบบงาน หรือในการจัดส่งข้อมูลการประมวลผลหรือจัดเก็บรักษาข้อมูลในระบบงาน**

2.2 **ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)**

การส่งมอบข้อมูลที่มีความสมบูรณ์ ถูกต้อง ครบถ้วนและน่าเชื่อได้ให้กับผู้ที่ต้องการใช้ข้อมูล (End User) จะทำให้การดำเนินงานและการบริหารงานขององค์กรมีประสิทธิภาพ หากผู้ที่ต้องการใช้ข้อมูลได้รับข้อมูลที่ขาดความน่าเชื่อถือย่อมก่อให้เกิดความเสี่ยงต่อองค์กร ทั้งนี้ การบริหารความเสี่ยงด้านนี้จะมีผลกระทบทั้งต่อโครงสร้างของการควบคุมองค์กรและต่อโครงสร้างของสายงานการให้บริการทั้งหมด

การพิจารณาความเสี่ยงในส่วนนี้จะครอบคลุมถึงความบกพร่องในกระบวนการออกแบบระบบ การนำออกใช้งานจริง หรือในระหว่างการบำรุงรักษาระบบและเครื่องมืออุปกรณ์ ตัวอย่าง เช่น การไม่สามารถทำงานร่วมกันได้ของระบบงานภายในและภายนอก หรือของอุปกรณ์และ Software ที่ทำให้สถาบันการเงินเกิดความเสี่ยงด้านการปฏิบัติงาน **ความเสี่ยงประเภทนี้จะมีเพิ่มขึ้นเมื่อสถาบันการเงินจ้างบุคคลภายนอกทำการออกแบบผลิตภัณฑ์** การให้บริการช่องทางการรับส่งข้อมูลและการประมวลผลที่ไม่เหมาะสมกับระบบงานของสถาบันการเงิน หรือความต้องการของลูกค้า ในทำนองเดียวกันเมื่อสถาบันการเงินให้ผู้ขายบริการเป็นผู้ปฏิบัติงานในการดำเนินธุรกิจหลักของสถาบันการเงิน เช่น เงินให้กู้ที่มีภาระผูกพัน และระบบการพิจารณาสินเชื่อ (Credit Scoring) เป็นต้น ถ้าสถาบันการเงินขาดการควบคุมที่เพียงพอในการติดตามการทำธุรกรรมของผู้ขายบริการเหล่านี้ความเสี่ยงด้านการปฏิบัติงานก็อาจจะมีเพิ่มขึ้น การควบรวมกิจการสถาบันการเงินเข้าด้วยกันหรือมีความต้องการทำธุรกรรมใหม่เพิ่มขึ้น การรวมระบบงานคอมพิวเตอร์ของสถาบันการเงินเข้าด้วยกันอาจทำให้เกิดความคลาดเคลื่อนหรือความไม่สมบูรณ์ของข้อมูลหรือการปฏิบัติงาน การวัด

ระบบการรักษาความปลอดภัย แผนฉุกเฉิน การทดสอบระบบ และมาตรฐานการตรวจสอบที่ไม่มีความเพียงพอมีส่วนทำให้ความเสี่ยงด้านการปฏิบัติงานเพิ่มขึ้นด้วย

2.3 **ความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (Availability)**

ความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศมี**ความเสี่ยงในเรื่องของการจัดส่งข้อมูลไปให้ผู้ที่ต้องการใช้ข้อมูลได้รวดเร็วทันเวลาและสามารถให้ข้อมูลได้อย่างต่อเนื่องในเวลาที่เหมาะสม** เพื่อให้สามารถสนับสนุนการดำเนินงานและการตัดสินใจของสถาบันการเงิน โดยอาศัยข้อมูลทั้งจากแหล่งภายในและภายนอก โดยต้องจัดให้มีแผนการเตรียมความพร้อมเพื่อรองรับเหตุการณ์ฉุกเฉินในการแก้ไขปัญหาหรือมีศูนย์ประมวลผลสำรอง รวมทั้งการจัดทำข้อมูลสำรอง **สถาบันการเงินจะต้องสามารถดำเนินการเพื่อให้บริการลูกค้าได้อีกครั้งภายในเวลา 24 ชั่วโมงหลังจากการดำเนินงานหยุดชะงักอันเนื่องมาจากเหตุการณ์ฉุกเฉินหรือภัยพิบัติ** ทั้งนี้ สถาบันการเงินที่มีความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ซึ่งเป็นแผนการดำเนินงานหลักของสถาบันการเงิน และมีแผนการกู้ระบบกลับคืน (Disaster Recovery Plan) แผนสำรองฉุกเฉิน (Contingency Plan) และแผนรองรับเหตุการณ์ที่ไม่คาดว่าจะเกิดขึ้น (Incident Response Plan) เป็นแผนงานรองประกอบแผนงานหลักดังกล่าว

แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan หรือ BCP) หมายถึง แผนการดำเนินงานหลักที่ทำให้การดำเนินธุรกิจของสถาบันการเงินสามารถกระทำได้อย่างต่อเนื่องไม่หยุดชะงัก เมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉินกับสถาบันการเงิน

แผนการกู้ระบบกลับคืน (Disaster Recovery Plan หรือ DRP) หมายถึง แผนการดำเนินงานทางด้านเทคโนโลยีสารสนเทศเพื่อให้ข้อมูลและระบบงานของระบบคอมพิวเตอร์สามารถกลับมาดำเนินการได้ภายใน 24 ชั่วโมง หลังจากสถาบันการเงินประสบภัยพิบัติหรือเหตุฉุกเฉิน

แผนสำรองฉุกเฉิน (Contingency Plan) หมายถึง แผนรองรับการดำเนินงานหรือการปฏิบัติงานของสถาบันการเงินให้ผู้ปฏิบัติงานสามารถดำเนินการให้มีการปฏิบัติงานได้อย่างรวดเร็วเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉิน

แผนรองรับเหตุการณ์ที่ไม่คาดว่าจะเกิดขึ้น (Incident Response Plan หรือ IRP) หมายถึง แผนรองรับเหตุการณ์ต่างๆ ที่เกิดขึ้นโดยไม่คาดว่าจะเกิดกับสถาบันการเงิน ซึ่งเป็นเหตุการณ์ที่นอกเหนือจากสิ่งที่คิดว่าจะเกิดขึ้น เช่น การขู่วางระเบิด ตึกถล่ม Hackerโจมตีระบบงาน หรือเหตุการณ์ 11 กันยายน 2545 ที่ผู้ก่อการร้ายถล่มตึกเวิลด์เทรด ประเทศสหรัฐอเมริกา เป็นต้น เพื่อให้สถาบันการเงินสามารถดำเนินงานภายหลังเกิดเหตุการณ์ที่ไม่คาดว่าจะเกิดขึ้นได้ในระยะเวลาที่รวดเร็วและเหมาะสม

2.4 **ความเสี่ยงด้านชื่อเสียง (Reputation)**

ความเสี่ยงด้านชื่อเสียงเป็นความเสี่ยงที่เกิดจากความคิดเห็นในเชิงลบของสาธารณชน ที่มีอิทธิพลต่อความสามารถของสถาบันการเงินที่จะทำให้เกิดการสร้างความสัมพันธ์ใหม่ ๆ หรือยังคงดำรงความสัมพันธ์ของการให้บริการแก่ลูกค้าคงอยู่ต่อไปซึ่งมีผลกระทบต่อรายได้และเงินกองทุนของสถาบันการเงิน ความเสี่ยงนี้เกิดจากการที่สถาบันการเงินถูกดำเนินคดี ความเสียหายทางการเงินหรือความเสียหายต่อชื่อเสียง โอกาสที่จะเกิดความเสี่ยงด้านชื่อเสียงอาจเกิดขึ้นทั่วทั้งองค์กร และเป็นคำถามว่าทำไมสถาบันการเงินต้องรับผิดชอบที่จะทำทุกอย่างด้วยความระมัดระวังในการติดต่อลูกค้าและประชาชน

ความเสี่ยงด้านชื่อเสียงเกิดขึ้นเมื่อใดก็ได้ที่สถาบันการเงินนำเทคโนโลยีที่เกี่ยวข้องกับผลิตภัณฑ์ การให้บริการ ช่องทางการรับส่งข้อมูล หรือการประมวลผลมาใช้ ซึ่งอาจตรงข้ามกับความคิดเห็นของสาธารณชนถึงขั้นส่งผลกระทบให้รายได้หรือเงินกองทุนของสถาบันการเงินลดลง ตัวอย่าง เช่น จุดอ่อนของระบบการรักษาความปลอดภัยซึ่งเป็นภัยอย่างสำคัญต่อความเป็นส่วนตัวของลูกค้า ความไม่เพียงพอของแผนฉุกเฉินและแผนรองรับการดำเนินธุรกิจที่มีอิทธิพลต่อความสามารถของสถาบันการเงินที่จะรักษาหรือเริ่มต้นการปฏิบัติงานใหม่ และ**เตรียมรองรับการให้บริการลูกค้าเมื่อระบบผิดพลาด การทุจริตซึ่งเป็นส่วนสำคัญในการทำลายความเชื่อถือของสาธารณชน และเกิดการฟ้องร้องมากขึ้นทำให้เห็นว่า สถาบันการเงินมีภาระหนี้สินที่สำคัญและเป็นผลให้เกิดความเสียหายอย่างรุนแรงต่อชื่อเสียงของสถาบันการเงิน** ความคิดเห็นที่ไปในทิศทางตรงข้ามกับสาธารณชนอาจทำให้เกิดภาพในทางลบที่ยาวนานต่อการดำเนินงานของสถาบันการเงินทั้งหมดและเป็นการลดคุณค่าของความสามารถของสถาบันการเงินในการรักษาความสัมพันธ์กับลูกค้าและธุรกิจไว้ได้

2.5 **ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Regulation)**

ความเสี่ยงด้านการปฏิบัติตามกฎหมายเป็นความเสี่ยงที่เกิดจากการปฏิบัติฝ่าฝืนหรือไม่ทำตามมาตรการผ่อนผันของกฎหมาย ระเบียบ คำสั่ง วิธีบัญญัติที่ถูกต้องตามมาตรฐานซึ่งมีผลกระทบต่อรายได้และเงินกองทุน ความเสี่ยงนี้เกิดขึ้นในสถานการณ์ที่กฎหมายและระเบียบของรัฐในการกำกับดูแลผลิตภัณฑ์หรือธุรกรรมของลูกค้าสถาบันการเงินอาจเคลือบแคลงไม่ชัดเจน ความเสี่ยงด้านการปฏิบัติตามกฎหมายนำมาซึ่งการเสื่อมเสียชื่อเสียง จำกัดโอกาสทางธุรกิจ ลดความเป็นไปได้ในการขยายตัว และขาดความสามารถในการบังคับให้เป็นไปตามสัญญา

ความเสี่ยงด้านการปฏิบัติตามกฎหมายอาจเกิดขึ้นในหลาย ๆ ทาง ได้แก่ เกิดจาก **สถาบันการเงินไม่สามารถที่จะทำตามความต้องการที่ให้ปฏิบัติอย่างเปิดเผยได้ หรือเมื่อทำการเปิดเผยข้อมูลไปให้กลุ่มบุคคลภายนอก ทั้ง ๆ ที่เป็นข้อมูลที่ต้องเก็บเป็นความลับ** เป็นต้น นอกจากนี้ การใช้เทคโนโลยีในการพิจารณาให้สินเชื่อแบบอัตโนมัติจะทำให้เกิดความเสี่ยงด้านการปฏิบัติตามกฎหมาย

ถ้าโปรแกรมนั้นไม่มีการทดสอบอย่างถูกต้องหรือไม่มีการตรวจสอบคุณภาพของข้อมูล เช่น การใช้ Credit Scoring Model เพื่อการพิจารณาให้สินเชื่อแบบอัตโนมัติสามารถทำให้สถาบันการเงินเกิดความเสี่ยงด้านการปฏิบัติตามกฎหมาย ถ้าข้อมูลนั้นอยู่ในโปรแกรมที่มีข้อบกพร่องหรือเกิดจากการออกแบบโปรแกรมมีช่องโหว่ก็จะส่งผลกระทบต่อรูปแบบการให้สินเชื่อที่เป็นการละเมิดกฎหมาย และระเบียบข้อบังคับ

หลายสถาบันการเงินเปลี่ยนแปลงการปฏิบัติงานที่ใช้กระดาษไปสู่การแลกเปลี่ยนข้อมูลโดยการใช้อิเล็กทรอนิกส์ สถาบันการเงินจำเป็นต้องพิจารณาถึงกฎหมายว่าได้กำหนดให้การปฏิบัติงานโดยใช้กระดาษไปสู่การปฏิบัติงานแลกเปลี่ยนข้อมูลโดยการใช้อิเล็กทรอนิกส์ไว้อย่างไร เทคโนโลยีใหม่ ๆ ที่เกิดขึ้นบางอย่างยังไม่ได้ออกกฎข้อบังคับ บ่อยครั้งที่สมาชิกสภาผู้แทนราษฎรและสภานิติบัญญัติจะปรับปรุงกฎข้อบังคับและกฎหมายไม่ทันตามเทคโนโลยีใหม่ ๆ เหล่านั้น ธุรกรรมผ่านทางอินเตอร์เน็ตอาจเกิดคำถามใหม่ ๆ จากศาล ดังนั้น สถาบันการเงินควรให้ความระมัดระวัง เฝ้าดูแลติดตาม และรับผิดชอบต่อการเปลี่ยนแปลงที่เกี่ยวข้องกับกฎหมายและข้อบังคับที่เกิดจากการพัฒนางานเหล่านี้

กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินในปัจจุบันได้เตรียมสนองต่อความต้องการทางเทคโนโลยีสารสนเทศในหลาย ๆ ทาง เช่น บางแห่งมีการวางแผนเทคโนโลยีสารสนเทศครอบคลุมแผนกลยุทธ์ในทุก ๆ ด้าน ขณะที่สถาบันการเงินแห่งอื่นอาจเจรจาที่จะนำเทคโนโลยีสารสนเทศมาใช้ทีละโครงการ ความซับซ้อนของกระบวนการบริหารความเสี่ยงควรกำหนดให้มีเพียงพอกับระดับความเสี่ยงที่เกิดขึ้น ซึ่งรวมถึงลักษณะของความเสี่ยง ความรุนแรงของความเสี่ยงด้านเทคโนโลยีสารสนเทศในเชิงเปรียบเทียบและมองในภาพรวมกับความเสี่ยงของสถาบันการเงินอื่นและความสามารถโดยรวมของสถาบันการเงินที่จะจัดการและควบคุมความเสี่ยงนั้น อย่างไรก็ตาม **สถาบันการเงินที่มีระบบการบริหารความเสี่ยงที่ดี**จะมีหลักเบื้องต้นเหมือนกันหลายอย่าง **คือ การระบุความเสี่ยง การวัดความเสี่ยง การควบคุมความเสี่ยงและการติดตามความเสี่ยง กระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศมีกระบวนการสำคัญ 3 ประการ**ที่สถาบันการเงินควรดำเนินการ คือ

1. การวางแผนการใช้เทคโนโลยีสารสนเทศ

เนื่องจากการนำเทคโนโลยีใหม่ ๆ มาใช้มีความจำเป็นต้องใช้ผู้ที่มีความสามารถพิเศษในการออกแบบ การนำระบบมาใช้และการให้บริการ ซึ่งสถาบันการเงินไม่มีผู้ที่มีความสามารถพิเศษดังกล่าวจึงอาจจะต้องหาบุคลากรที่มีความชำนาญพิเศษเฉพาะด้านจากผู้ให้บริการจากภายนอก ดังนั้น ในการวางแผนว่าจะทำสัญญาเกี่ยวกับความต้องการใช้เทคโนโลยีหรือไม่ อย่างไร สถาบัน

การเงินควรจะประเมินว่าจะบริหารความเสี่ยงที่เกี่ยวกับการใช้บริการจากบุคคลภายนอกอย่างไร หากไม่มีการควบคุมการใช้บริการจากบุคคลอื่นอย่างเพียงพอให้ทำการออกแบบหรือสนับสนุนระบบเทคโนโลยีสารสนเทศใหม่ของสถาบันการเงิน อาจเป็นการเพิ่มความเสี่ยงได้ ซึ่งผู้บริหารจะต้องรับผิดชอบต่อผลของการปฏิบัติการของบุคคลอื่นที่กระทำการแทนสถาบันการเงินนั้น ๆ

เมื่อพิจารณาว่าจะนำเทคโนโลยีใหม่ ๆ มาใช้หรือเพิ่มความสามารถของระบบเดิมที่มีอยู่ **สถาบันการเงินควรประเมินว่าจะใช้เทคโนโลยีภายใต้สิ่งแวดล้อมที่เป็นเป้าหมายทางกลยุทธ์ทั้งหมดของสถาบันการเงินนั้นได้อย่างไร ปัจจัยในการวางแผนมี ดังนี้**

(1) **ค่าใช้จ่ายในการพัฒนา การออกแบบ และการทดสอบของระบบ และการปฏิบัติงานในระบบ** ทั้งที่เป็นการปฏิบัติงานภายในและกระทำผ่านผู้ให้บริการภายนอก

(2) **ความสามารถของการกู้ระบบกลับมาอย่างรวดเร็ว** โดยที่ไม่เกิดความเสียหายต่อข้อมูลในกรณีที่ระบบล้มเหลว หรือมีผู้ไม่ได้รับอนุญาตมาบุกรุกระบบ

(3) **การควบคุมภายในที่เพียงพอ รวมถึงการควบคุมภายในของผู้ให้บริการภายนอก** (บุคคลที่สาม)

(4) **ความสามารถในการพิจารณาความเสี่ยงที่เกิดขึ้นเป็นการเฉพาะ**ซึ่งเกินความสามารถของสถาบันการเงินในการจัดการและควบคุมความเสี่ยงนั้น

จากการที่เทคโนโลยีสารสนเทศมีการพัฒนาและเปลี่ยนแปลงอย่างต่อเนื่อง ผู้บริหารของสถาบันการเงินควรจะพิจารณาและประเมินผลการใช้เทคโนโลยีให้เป็นส่วนหนึ่งของการวางแผนทางธุรกิจเพื่อให้มั่นใจว่า การดำเนินการพัฒนาโครงการเกี่ยวกับเทคโนโลยีสารสนเทศสอดคล้องกับแผนการดำเนินงานของสถาบันการเงิน **การวางแผนทางเทคโนโลยีสารสนเทศมักจะเกี่ยวข้องกับการวางแผนกลยุทธ์ การวางแผนทางธุรกิจ และการวางแผนของโครงการต่าง ๆ** ซึ่งการวางแผนกลยุทธ์เป็นการสร้างบทบาททางเทคโนโลยีสารสนเทศของสถาบันการเงิน เพราะเป็นเรื่องเกี่ยวข้องกับพันธกิจของสถาบันการเงินและประเมินชนิดของเทคโนโลยีสารสนเทศซึ่งสถาบันการเงินจำเป็นต้องแสดงบทบาทให้สมบูรณ์ การวางแผนทางธุรกิจจะรวมถึงความต้องการทางเทคโนโลยีสารสนเทศใหม่ในสายงานธุรกิจปัจจุบัน และพิจารณาประเภทของเทคโนโลยีสารสนเทศที่เหมาะสมสำหรับสายงานทางธุรกิจโดยเฉพาะ ส่วนการวางแผนโครงการจะเป็นการกำหนดทรัพยากรที่จำเป็น ตารางเวลา จุดวัดผล และข้อมูลอื่น ๆ ที่จำเป็นในการเปลี่ยนแผนงานทางธุรกิจไปสู่การปฏิบัติจริง การทบทวนและรอบระยะเวลาในการวางแผนอาจจะแตกต่างกันไปขึ้นอยู่กับประเภทของสถาบันการเงินและการใช้เทคโนโลยีที่แตกต่างกันออกไป การวางแผนอย่างเหมาะสมน่าจะลดความเสี่ยงที่อาจจะเกิดขึ้นจากการที่ Hardware และ Software ไม่สามารถทำงานร่วมกันได้ และทำให้การปรับปรุงความต้องการของสถาบันการเงินและลูกค้าในการใช้เทคโนโลยีในอนาคต

มีความคล่องตัวมากขึ้น

กระบวนการวางแผนสำหรับระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้มีประสิทธิผลนั้น สถาบันการเงินควรจะคำนึงถึงองค์ประกอบพื้นฐาน 3 ประการ ดังนี้

(1) **การตัดสินใจที่เกี่ยวข้องกับผู้บริหารระดับสูง และคณะกรรมการบริหาร**

ผู้บริหารระดับสูงมีความรู้และความสามารถเพียงพอในการบริหารการใช้เทคโนโลยีสารสนเทศหรือไม่ และประเมินว่าคณะกรรมการบริหารและผู้บริหารระดับสูง**ได้เกี่ยวข้องกับกระบวนการในการวางแผนจัดการกับความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของสถาบันการเงินเพียงพอหรือไม่**

การที่ผู้บริหารระดับสูงมีความรู้และเกี่ยวข้องในกระบวนการวางแผนเทคโนโลยีสารสนเทศซึ่งเป็นบทบาทที่สำคัญในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน **คณะกรรมการบริหารและผู้บริหารระดับสูงควรจะทบทวน อนุมัติ และติดตามความคืบหน้าของโครงการ**ทางด้านเทคโนโลยีสารสนเทศที่อาจมีผลกระทบที่สำคัญต่อผลการดำเนินงาน ผลประกอบการ และเงินทุนของสถาบันการเงิน นอกจากนั้น **ผู้บริหารระดับสูงควรที่จะมีความรู้ความสามารถในการประเมินผลและวิจารณ์การออกแบบ การดำเนินงานและสังเกตความผิดพลาด** ของโครงการเทคโนโลยีสารสนเทศต่าง ๆ **คณะกรรมการบริหารควรจะได้รับรายงานที่สมบูรณ์** จากผู้บริหารระดับสูงเป็นระยะ ๆ เกี่ยวกับความเสี่ยงของโครงการด้านเทคโนโลยีสารสนเทศซึ่งอาจมีผลกระทบต่อสถาบันการเงิน

สถาบันการเงินที่ใช้เทคโนโลยีในการดำเนินงานอย่างกว้างขวาง โดยเฉพาะอย่างยิ่ง สถาบันการเงินขนาดใหญ่ควรที่จะมีบุคลากรระดับผู้จัดการและพนักงานที่มีความสามารถในการทบทวนและสังเกตความผิดพลาดของโครงการด้านเทคโนโลยีสารสนเทศมีการควบคุมและบริหารความเสี่ยงที่เกี่ยวข้องให้เป็นไปตามมาตรฐาน นอกจากนี้ ผู้บริหารระดับสูงที่ได้รู้ถึงการริเริ่มใช้เทคโนโลยีของสถาบันการเงินควรรายงานให้คณะกรรมการบริหารได้รับทราบเกี่ยวกับการพัฒนาการใหม่ ๆ เป็นระยะ ๆ

(2) **การรวบรวมและวิเคราะห์ข้อมูล**

สถาบันการเงินมีความเข้าใจเกี่ยวกับระบบต่าง ๆ ที่มีอยู่อย่างไร ความคาดหวังของลูกค้าและภาวะการแข่งขันซึ่งทำให้ต้องมีการเพิ่มการใช้หรือการวางแผนการใช้เทคโนโลยีใหม่ในการรวบรวมและวิเคราะห์ข้อมูล สถาบันการเงินควรจะดำเนินการ ดังต่อไปนี้

- **รวบรวมข้อมูลเกี่ยวกับระบบและการดำเนินงานที่มีอยู่ในปัจจุบัน** สถาบันการเงินควรจะทบทวนระบบที่มีอยู่และพิจารณาว่า ระบบเป็นที่พอใจและเป็นโครงการที่สนองความต้องการของสถาบันการเงินหรือไม่ ในขณะเดียวกันสถาบันการเงินควรจะประเมินว่าเทคโนโลยี

สารสนเทศใหม่ ๆ จะปรับเข้ากับระบบต่าง ๆ ที่มีอยู่อย่างไร และจะต้องปรับปรุงเปลี่ยนแปลงระบบปัจจุบันอย่างไรหรือไม่ เพื่อให้เหมาะกับการที่จะนำเทคโนโลยีใหม่มาใช้

- **ทบทวนมาตรฐานที่ใช้ในธุรกิจสถาบันการเงิน ผู้บริหารสถาบันการเงินควรจะประเมินมาตรฐานที่ใช้ในปัจจุบันเพื่อพิจารณาว่าควรจะนำเทคโนโลยีอย่างใดอย่างหนึ่งโดยเฉพาะมาใช้งานหรือไม่** เทคนิคที่เป็นมาตรฐานจะช่วยให้มั่นใจว่า ระบบต่าง ๆ จะสอดคล้องและทำงานร่วมกันได้ดี

- **พิจารณาว่าเมื่อไรที่จะนำเทคโนโลยีใหม่มาใช้งาน** การกำหนดเวลาที่เหมาะสมเป็นเรื่องสำคัญ เพราะการนำเทคโนโลยีใหม่มาใช้เร็วไปหรือช้าไปอาจจะมีความเสี่ยงได้

(3) **การประเมินความต้องการและทบทวนทางเลือกต่าง ๆ**

ผู้บริหารของสถาบันการเงินได้กำหนดความต้องการใช้เทคโนโลยีอย่างระมัดระวังและทบทวนทางเลือกต่าง ๆ โดยอยู่ในขอบข่ายของแผนงานโดยรวมของสถาบันการเงินนั้น ๆ หรือไม่ ผู้บริหารควรพิจารณาอย่างรอบคอบว่ามีทรัพยากรที่จำเป็น มีเวลาและมีความชำนาญในการบริหารโครงการที่สามารถนำมาใช้ในการทำให้แผนการใช้เทคโนโลยีใหม่ประสบความสำเร็จ ซึ่งก่อนที่จะปรับปรุงนำเทคโนโลยีใหม่มาใช้ ผู้บริหารสถาบันการเงินควรระบุจุดอ่อนหรือข้อบกพร่องของความสามารถที่สถาบันการเงินจะนำเทคโนโลยีมาใช้ และควรจะพิจารณาว่าพนักงานของสถาบันการเงินนั้น ๆ จะสามารถปฏิบัติการภายใต้ระบบเก่าและระบบใหม่ควบคู่กันไปได้หรือไม่ การพิจารณาองค์ประกอบต่าง ๆ เหล่านี้ จะช่วยให้ผู้บริหารเลือกประเภทและระดับเทคโนโลยีสารสนเทศที่เหมาะสมที่สุดในการสนับสนุนวัตถุประสงค์และความต้องการของธุรกิจหลักของสถาบันการเงินนั้น ๆ

สถาบันการเงินควรกำหนดจุดประสงค์ของโครงการด้วยความระมัดระวังและควรแน่ใจว่าจุดประสงค์ดังกล่าวไม่คลุมเครือ และไม่ควรตั้งเป้าหมายไว้สูงเกินไป การวางแผนโครงการที่เป็นไปได้จะช่วยให้ผู้บริหารลดความเสี่ยงลงได้ การวางแผนนี้ควรรวมถึงการแบ่งโครงการออกเป็นส่วนย่อยเพื่อให้บริหารได้ง่ายขึ้น และควรจะสร้างจุดเพื่อให้มีการตัดสินใจเป็นการเฉพาะในการจะปรับปรุงหรือยกเลิกโครงการ นอกจากนี้ การวางแผนที่ดีจะต้องมีแผนรองรับในกรณีที่โครงการไม่สามารถดำเนินไปตามแผนที่วางไว้

เมื่อพิจารณาถึงทางเลือกต่าง ๆ **ผู้บริหารควรประมาณการต้นทุน และผลของการนำเทคโนโลยีใหม่มาใช้ ในขณะเดียวกันควรจะประเมินความเสี่ยงที่อาจจะเกิดขึ้นและผลกระทบทางด้านการเงิน**ซึ่งรวมถึงต้นทุนในการเริ่มโครงการ การปฏิบัติการ และที่สำคัญคือต้นทุนในการยกเลิกโครงการ

2. การนำเทคโนโลยีสารสนเทศมาใช้

การพิจารณาความสามารถของสถาบันการเงินในการบริหารโครงการ โดยเฉพาะในขั้นตอนการนำระบบออกใช้งานจริงว่าจะบรรลุผลตามวัตถุประสงค์ของโครงการเพื่อให้ได้ผลิตภัณฑ์ การให้บริการ ช่องทางการรับส่ง และมีกระบวนการปฏิบัติงานที่ดีนั้นจำเป็นอย่างยิ่งที่จะต้องมีขั้นตอนในการนำระบบงานมาใช้ปฏิบัติงานที่ดีและมีความคิดริเริ่มใหม่ ๆ นอกจากนี้ สถาบันการเงินควรจะต้องดำเนินการให้มีการควบคุมไม่ให้เกิดความล้มเหลวในการปฏิบัติงานและการบุกรุกโดยบุคคลที่ไม่ได้รับอนุญาต ซึ่งอาจทำให้เกิดความเสียหายหรือเสียชื่อเสียงได้ สถาบันการเงินจึงควรมีมาตรฐานในการใช้โครงสร้างหรือสถาปัตยกรรมของระบบเทคโนโลยีสารสนเทศต่าง ๆ เพื่อกำหนดทิศทางสำหรับสถาบันการเงิน

ผู้บริหารควรจะเรียงลำดับความสำคัญก่อนหลังของโครงการเพื่อให้เกิดความมั่นใจว่าโครงการจะมีการประสานงาน และการทำงานร่วมกันระหว่างหน่วยงานต่าง ๆ รวมถึงการกำหนดผู้ใช้งานและทรัพยากรที่ต้องการ ประมาณการต้นทุน จุดมาตรฐานของโครงการและประมาณการวันส่งมอบโครงการ และที่สำคัญการควบคุมโครงการต้องกระทำโดยบุคคลที่เกี่ยวข้องจากทุกฝ่ายงาน ผู้บริหารโครงการควรจะรายงานผู้บริหารระดับสูงถึงอุปสรรคที่เกิดขึ้นให้เร็วที่สุดเท่าที่จะเป็นไปได้ เพื่อให้มั่นใจว่ามีการควบคุมที่เหมาะสมและมีการดำเนินการแก้ไขข้อบกพร่องเพื่อจัดการความเสี่ยงที่เกิดขึ้นได้ทันเวลา ซึ่ง**การนำระบบออกใช้งานควรมีการพิจารณา ดังนี้**

(1) **ระบบการควบคุม**

สถาบันการเงินได้นำระบบการควบคุมมาใช้เพียงพอหรือไม่ โดยพิจารณาถึงระดับความเสี่ยงและประมาณการความเสียหายที่อาจจะเกิดขึ้นจากการนำเทคโนโลยีมาใช้ **ระบบการควบคุมควรจะชัดเจนและมีเป้าหมายการปฏิบัติงานที่สามารถวัดได้ มีการกระจายความรับผิดชอบเป็นการเฉพาะสำหรับการนำโครงการสำคัญมาใช้และมีกลไกอิสระในการวัดระดับความเสี่ยง ลดระดับความเสี่ยงที่มากเกินไป** ระบบการควบคุมเหล่านี้ควรจะมีการทบทวนถึงความเหมาะสมเป็นระยะ ๆ

ระบบการควบคุมความปลอดภัยของระบบเทคโนโลยีสารสนเทศของสถาบันการเงินมีความสำคัญอย่างยิ่ง มาตรการรักษาความปลอดภัยควรจะมีการกำหนดอย่างชัดเจน และมีมาตรฐานการปฏิบัติงานที่สามารถวัดค่าได้ **สถาบันการเงินควรแต่งตั้งบุคลากรเป็นการเฉพาะให้ทำหน้าที่รับผิดชอบเรื่องระบบรักษาความปลอดภัยเพื่อให้มั่นใจว่าระบบดังกล่าวครอบคลุมเนื้อหาสำคัญทั้งหมด** ผู้บริหารของสถาบันการเงินควรจะดำเนินการทุกขั้นตอนที่จำเป็นเพื่อเป็นการป้องกันการบุกรุกเข้าสู่ระบบที่สำคัญของผู้ที่ไม่ได้รับอนุญาต ระบบต่าง ๆ ควรได้รับการป้องกันมากที่สุดเท่าที่จะทำได้จากความเสี่ยงที่เกี่ยวข้องกับการทุจริต ความประมาทเลินเล่อ และการทำลายทรัพย์สินของสถาบันการเงิน จุดควบคุมควรจะรวมถึงอุปกรณ์ เครื่องมือ บุคลากร นโยบายและวิธีการปฏิบัติ การควบคุมเครือข่าย

การควบคุมระบบงาน และรวมไปถึงผู้ให้บริการภายนอก เช่น การจำกัดการเข้าสู่ระบบ การตรวจสอบภูมิหลังของพนักงาน การแบ่งแยกหน้าที่ของพนักงาน และการตรวจสอบร่องรอยก็มีความสำคัญต่อการป้องกันระบบรักษาความปลอดภัยทั้งจากภายในสถาบันการเงินและผู้ให้บริการภายนอก ระบบการควบคุมดังกล่าวอาจจะต้องมีการทบทวนและเปลี่ยนแปลงเป็นระยะ ๆ เมื่อเทคโนโลยีและระบบเปลี่ยนแปลงไป

(2) **การวางนโยบายและวิธีปฏิบัติ**

ผู้บริหารได้มีการวางนโยบายและวิธีปฏิบัติที่เข้มงวดเหมาะสมในการบริหารความเสี่ยงเกี่ยวกับการนำเทคโนโลยีใหม่ ๆ มาใช้ในสถาบันการเงินหรือไม่ นโยบายและวิธีปฏิบัติที่ดีซึ่งมีประสิทธิผลนั้นได้มีการนำไปปฏิบัติกับพนักงานของสถาบันการเงิน ผู้ให้บริการที่เป็นบุคคลที่สามหรือไม่ การทดสอบว่าได้มีการปฏิบัติตามนโยบายและวิธีปฏิบัติที่ดีจะช่วยให้สถาบันการเงินสามารถแก้ไขปัญหาก่อนที่จะกลายเป็นเรื่องร้ายแรงได้ การเขียนนโยบายอย่างชัดเจนและการประชาสัมพันธ์อย่างสม่ำเสมอจะก่อให้เกิดความเข้าใจในหน้าที่รับผิดชอบ การประสานงานและการปฏิบัติงานอย่างมีประสิทธิผลและมั่นคง รวมทั้งยังเป็นคู่มือที่ใช้ในการอบรมพนักงานใหม่ได้ด้วย ผู้บริหารควรแน่ใจว่าเนื้อหาของนโยบายและวิธีปฏิบัติได้มีการปรับปรุงแก้ไขให้ชัดเจนและทันสมัยอยู่เสมอ

(3) **ความรู้ความชำนาญ และการฝึกอบรม**

ผู้บริหารมีแผนการอบรมพนักงานที่มีความสำคัญกับงานโดยตรง ผู้ให้บริการมีความรู้ความสามารถในการปฏิบัติงานที่รับผิดชอบและได้รับการอบรมที่เหมาะสม **ผู้บริหารควรจะจัดสรรบุคลากรที่เพียงพอ และฝึกอบรมพนักงานเพื่อให้มั่นใจว่ามีพนักงานทดแทนเพียงพอ** ในกรณีที่พนักงานผู้รับผิดชอบไม่มาทำงาน การฝึกอบรมอาจจะรวมถึงอบรมทางด้านเทคนิค การเข้าร่วมประชุมกับกลุ่มธุรกิจการค้าทั่วไป การมีส่วนร่วมในคณะทำงานของกลุ่มธุรกิจการค้า และรวมถึงการจัดสรรให้พนักงานได้มีโอกาสติดตามวิวัฒนาการและการพัฒนาตลาดทางด้านเทคโนโลยีสารสนเทศใหม่ ๆ การอบรมควรรวมถึงการเข้าถึงลูกค้าด้วยเพื่อให้มั่นใจว่าลูกค้าของสถาบันการเงินมีความเข้าใจในวิธีการใช้งานหรือวิธีเข้าถึงเทคโนโลยีสารสนเทศของสถาบันการเงินในด้านผลิตภัณฑ์และการบริการ รวมทั้งสามารถใช้งานได้เป็นอย่างดี

(4) การทดสอบ

ผู้บริหารได้จัดให้มีการทดสอบระบบและผลิตภัณฑ์ที่ใช้เทคโนโลยีใหม่อย่างทั่วถึง การทดสอบเป็นการยืนยันว่า อุปกรณ์และระบบต่าง ๆ ทำงานได้อย่างถูกต้องและก่อให้เกิดผลงานตามที่ได้วางแผนไว้ ในส่วนหนึ่งของกระบวนการทดสอบควรจะทำการตรวจสอบว่า ระบบเทคโนโลยีสารสนเทศใหม่ที่นำมาใช้สามารถทำงานได้อย่างมีประสิทธิภาพร่วมกับระบบปัจจุบัน และสามารถทำงานร่วมกับระบบของบุคคลภายนอกตามที่กำหนดไว้หรือไม่ โปรแกรมนำร่องหรือโปรแกรม

ต้นแบบเป็นเครื่องมือที่ช่วยในการพัฒนาระบบงานเทคโนโลยีสารสนเทศใหม่ก่อนที่จะนำโปรแกรมไปใช้อย่างกว้างขวาง สถาบันการเงินควรทำการทดสอบเป็นระยะ ๆ เพื่อเป็นการลดความเสี่ยงที่อาจจะเกิดขึ้นได้

(5) **การจัดทำแผนฉุกเฉินและแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง**

ระบบเทคโนโลยีสารสนเทศของสถาบันการเงินได้มีการออกแบบเพื่อลดผลกระทบจากเหตุการณ์ต่าง ๆ ที่จะทำให้ระบบล้มเหลวมีการป้องกันการบุกรุกเข้าระบบและปัญหาอื่น ๆ หรือไม่ระบบสำรองได้รับการบำรุงรักษาและมีการทดสอบเป็นประจำเพื่อลดความเสี่ยงจากระบบล้มเหลวและการบุกรุกโดยไม่ได้รับอนุญาต ความเสี่ยงที่เกิดขึ้นจากระบบล้มเหลวหรือความผิดพลาดของผู้ปฏิบัติงานสามารถเกิดขึ้นกับทุกระบบของเทคโนโลยีสารสนเทศ ความเสี่ยงดังกล่าวนี้อาจเกิดจากทรัพยากรทั้งที่อยู่ภายในและที่อยู่นอกเหนือการควบคุมของสถาบันการเงิน เช่น การที่ระบบล้มเหลวและมีการบุกรุกเข้าระบบอาจเกิดจากการออกแบบที่ไม่ดี ระบบไม่มีความสามารถเพียงพอ และเกิดจากภัยธรรมชาติหรือไฟไหม้หรือเกิดจากการไม่ปฏิบัติตามระเบียบการรักษาความปลอดภัยหรือ บุคลากรไม่ได้รับการอบรมที่เพียงพอ หรือเกิดจากการที่สถาบันการเงินไม่ได้ควบคุมระบบเพราะไว้วางใจผู้ให้บริการจากภายนอก

สถาบันการเงินควรเตรียมแผนรองรับการดำเนินธุรกิจไว้ก่อนที่จะเริ่มนำเทคโนโลยีใหม่มาใช้ปฏิบัติจริง แผนงานดังกล่าวควรจะระบุถึงขั้นตอนการปฏิบัติในกรณีที่ระบบเกิดเหตุล้มเหลวหรือมีการบุกรุกโดยผู้ที่ไม่ได้รับอนุญาต และควรจะประสานกับแผนงานการดำเนินธุรกิจต่อเนื่องอื่นทั้งหมดที่เป็นกิจกรรมในการดำเนินงานและกิจกรรมทางธุรกิจของสถาบันการเงิน แผนงานควรจะระบุถึงการกู้ข้อมูลกลับคืนและระบบสำรองสำหรับการประมวลผลข้อมูล รวมถึงพนักงานที่กำหนดให้รับผิดชอบในกรณีฉุกเฉิน และหน่วยงานที่คอยให้บริการต่อลูกค้า ผู้บริหารจะต้องจัดทำแผนการสื่อสาร โดยกำหนดชื่อพนักงานหลักและโครงร่างของแผนการแจ้งพนักงานตามแผนฉุกเฉินดังกล่าว นอกจากนี้ ควรรวมถึงการประชาสัมพันธ์ การขยายกลยุทธ์ในการตอบสนองต่อลูกค้าและการใช้เครื่องมือโต้ตอบอย่างทันทีเมื่อระบบล้มเหลวหรือมีการบุกรุกโดยไม่ได้รับอนุญาต ในขณะเดียวกันผู้บริหารควรจะต้องวางแผนในการตอบสนองต่อเหตุการณ์ภายนอกซึ่งอาจจะมีผลต่อความมั่นใจของลูกค้า เช่น การที่คู่แข่งซึ่งใช้เทคโนโลยีเดียวกันประสบปัญหาจากการดำเนินงานล้มเหลว เป็นต้น

(6) **การใช้บริการจากบุคคลภายนอก**

การประเมินการบริหารความเสี่ยงที่เกี่ยวข้องกับการจ้างบุคคลภายนอกและพันธมิตรภายนอกของสถาบันการเงิน **เพื่อมั่นใจว่าผู้บริหารได้ควบคุมดูแลเกี่ยวกับความชำนาญ ประสบการณ์และความมั่นคงทางการเงินของผู้ให้บริการที่จะทำตามพันธะข้อตกลงอย่างเต็มที่** อีกทั้งต้องมั่นใจว่า

สิ่งที่คาดหมายและพันธะการตกลงของคู่ค้าแต่ละรายกำหนดขึ้นอย่างชัดเจน เข้าใจง่าย และสามารถควบคุมได้ เช่น ผู้บริหารควรกำหนดให้แน่นอนว่า สถาบันการเงินมีสิทธิที่จะตรวจสอบผู้ให้บริการ เพื่อที่สถาบันการเงินสามารถติดตามดูการปฏิบัติงานภายใต้สัญญากับผู้ให้บริการ

ปัจจัยสำคัญของการนำโครงการมาประยุกต์ใช้งานหรือเป็นการรวบรวมโครงการต่าง ๆ มาพัฒนา และนำออกใช้งาน สถาบันการเงินจำเป็นต้องอาศัยพนักงานหรือผู้ให้บริการ การไม่มีระบบการควบคุมที่จำเป็นอาจทำให้เกิดผลเสียต่อการรักษาความปลอดภัยซึ่งทำให้มีการบริการที่ต่ำกว่ามาตรฐานและการติดตั้งอุปกรณ์ที่เข้ากันไม่ได้ ระบบงานล้มเหลว ต้นทุนที่ควบคุมไม่ได้ และมีการเปิดเผยข้อมูลส่วนตัวของลูกค้า กรณีที่สถาบันการเงินร่วมมือหรือกลายเป็นพันธมิตรกับบริษัทหรือสถาบันการเงินอื่น ผู้บริหารต้องทำการตรวจสอบความพร้อมอย่างเพียงพอเพื่อจะมั่นใจได้ว่า ผู้ร่วมธุรกิจการค้ามีความสามารถและมีความมั่นคงทางการเงินที่จะทำตามพันธะข้อตกลง สถาบันการเงินจะต้องมีทรัพยากรเพียงพอในการติดตามและการวัดผลการปฏิบัติงานภายใต้เงื่อนไขข้อตกลงกับบุคคลที่สาม

3. การวัดและติดตามผลการปฏิบัติงาน

ผู้บริหารควรวัดและติดตามผลการปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของผลิตภัณฑ์ การให้บริการ ช่องทางรับส่งข้อมูล และกระบวนการป้องกันความล้มเหลวในการปฏิบัติงานและลดความเสียหายที่อาจเกิดขึ้น **ผู้ตรวจสอบจะประเมินว่า ผู้บริหารของสถาบันการเงินได้กำหนด การควบคุมที่สามารถระบุและบริหารความเสี่ยงได้** เพื่อที่สถาบันการเงินสามารถบริหารงานในความรับผิดชอบที่มีอยู่ได้อย่างเหมาะสมและมั่นใจ ผู้บริหารควรระบุผู้ที่จะได้รับมอบหมายให้รับผิดชอบเป้าหมายทางธุรกิจ วัตถุประสงค์และผลลัพธ์ของโครงการเฉพาะด้านเทคโนโลยีสารสนเทศ นอกจากนี้ ควรกำหนดการควบคุมโดยหน่วยงานที่เป็นอิสระเพื่อให้มั่นใจได้ว่า มีการจัดการความเสี่ยงอย่างเหมาะสม มีการสอบทานกระบวนการทางเทคโนโลยีสารสนเทศเป็นระยะ เพื่อการควบคุมดูแลคุณภาพที่ดี

<u>การตรวจสอบ</u>

ผู้ตรวจสอบจะประเมินความเพียงพอของการตรวจสอบที่จะระบุและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการประเมินว่าผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่รับผิดชอบในการตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศได้จัดให้มีกลไกในการควบคุมและค้นหาความบกพร่องของการบริหารความเสี่ยงในการนำเทคโนโลยีออกใช้งาน ทั้งนี้ ผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่รับผิดชอบงานดังกล่าวควรเป็นผู้มีคุณวุฒิเหมาะสมที่จะประเมินความเสี่ยงเฉพาะด้านที่เกิดจากการใช้เทคโนโลยีเป็นการเฉพาะ และผู้บริหารสถาบันการเงิน ควรจัดข้อมูลที่เพียงพอให้แก่ผู้สอบบัญชีเกี่ยวกับมาตรฐาน นโยบาย วิธีปฏิบัติ โปรแกรม และระบบงาน ผู้สอบบัญชี

ควรปรึกษาผู้บริหารสถาบันการเงินระหว่างกระบวนการวางแผนเพื่อมั่นใจว่าระบบงานที่เกี่ยวข้องกับเทคโนโลยีได้รับการตรวจสอบอย่างโปร่งใส และการบริหารต้นทุนมีประสิทธิผล

การรับรองคุณภาพ

ผู้ตรวจสอบจะสอบทานการบริหารงานของสถาบันการเงินว่ามีการกำหนดวิธีปฏิบัติให้เกิดการรับรองคุณภาพของการทำงานหรือไม่ ซึ่งวิธีการปฏิบัติอาจรวมถึงการวัดผลการปฏิบัติงานภายใน การสำรวจกลุ่มเป้าหมายและลูกค้า นอกจากนี้ ผู้ตรวจสอบจะประเมินว่า สถาบันการเงินได้ดำเนินการทบทวนการรับรองคุณภาพเมื่อมีการร่วมกันใช้เทคโนโลยีที่สำคัญกับสถาบันการเงินอื่นหรือการได้มาซึ่งอีกธุรกิจหนึ่งหรือไม่

ในส่วนของการวางแผน และการติดตามนั้น สถาบันการเงินต้องทำให้เกิดความชัดเจนในวัตถุประสงค์ของการวัดผล และทำการสอบทานเป็นระยะ ๆ เพื่อมั่นใจว่าเป้าหมายและมาตรฐานต่าง ๆ ที่กำหนดโดยผู้บริหารสถาบันการเงินเป็นไปตามเป้าหมายที่กำหนด มาตรฐานต่าง ๆ ควรรวมถึงการเน้นความถูกต้องเชื่อถือได้ของข้อมูลซึ่งเป็นส่วนประกอบสำคัญในการใช้เทคโนโลยีอย่างมีประสิทธิผล ข้อมูลที่ได้ควรมีความสมบูรณ์และถูกต้องทั้งก่อนและหลังการประมวลผล ควรมีการดูแลเอาใจใส่เป็นพิเศษในการใช้เทคโนโลยีที่สำคัญร่วมกับสถาบันการเงินอื่น หรือการได้มาซึ่งธุรกิจอื่น การควบคุมโครงการด้านเทคโนโลยีต่าง ๆ ที่มีความซับซ้อนยุ่งยากเนื่องจากการวัดความก้าวหน้าและการพิจารณาค่าใช้จ่ายจริงที่เกิดขึ้นกระทำได้ลำบาก เป็นเรื่องสำคัญที่ผู้บริหารสถาบันการเงินจะต้องกำหนดมาตรฐานที่มีความเหมาะสมสำหรับโปรแกรมระบบงานต่าง ๆ เป็นการเฉพาะ ความสำเร็จของการนำเทคโนโลยีมาใช้จะขึ้นอยู่กับผลลัพธ์ว่าได้สำเร็จตามที่มุ่งหวังหรือไม่

ส่วนที่ 2 การตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยง

วัตถุประสงค์การตรวจสอบ

คู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศฉบับปรับปรุงนี้ จัดทำขึ้นตามแนวทางการประเมินความเสี่ยง (IT-RBS) เพื่อให้การตรวจสอบสถาบันการเงินด้านเทคโนโลยีสารสนเทศสามารถปรับตัวเข้ากับการพัฒนากลยุทธ์ในการกำกับและตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม แนวทางการตรวจสอบในคู่มือฉบับนี้ สามารถนำคู่มือการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ FFIEC ปี 2003 – 2006 รวมทั้งคู่มือการตรวจสอบด้าน Electronic Banking ที่จัดทำขึ้นเมื่อปี 2544 มาประยุกต์ใช้ร่วมกันได้ โดยการตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยงนี้ มีวัตถุประสงค์เพื่อ

- **พิจารณาระดับและแนวโน้มความเสี่ยง**ที่เกี่ยวข้องกับธุรกรรมปัจจุบันและที่ได้วางแผนไว้

- **ประเมินนโยบายและการจัดการ**ตลอดจนระบบสารสนเทศเพื่อการบริหารให้มีการบริหารความเสี่ยงอย่างมีประสิทธิภาพ

- **ประเมินความเพียงพอของการดำเนินงาน**ด้านการตรวจสอบภายในของสถาบันการเงิน ในการช่วยลดความเสี่ยงของการดำเนินงานด้านเทคโนโลยีสารสนเทศ

- **ประเมินระบบการรักษาความปลอดภัย**ของสถาบันการเงิน ในการลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและผลกระทบที่อาจเกิดขึ้นต่อธุรกรรมของสถาบันการเงิน

- **ประเมินความถูกต้องเชื่อถือได้ของข้อมูล**ในเชิงปริมาณและเชิงคุณภาพในด้านการบริหารความเสี่ยงทั้งหมด โดยพิจารณาความเหมาะสมของการนำมาใช้งานให้เกิดประโยชน์ต่อการบริหารสูงสุด

- **ประเมินสภาพความพร้อมใช้งาน**ด้านเทคโนโลยีสารสนเทศของสถาบันการเงินตลอดจนความเหมาะสมของแผนสำรองฉุกเฉินต่าง ๆ ในการลดความเสี่ยงที่จะเกิดกับสถาบันการเงิน

- **พิจารณาการปฏิบัติตามกฎหมาย ประกาศของธนาคารแห่งประเทศไทย** และนโยบายของทางการที่กำหนดให้สถาบันการเงินนั้น ๆ ถือปฏิบัติ

ขอบเขตการตรวจสอบ

การตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยงมี**ขอบเขตของการตรวจสอบในแต่ละด้าน ดังนี้**

1. การบริหารงานเทคโนโลยีสารสนเทศ

1.1 การจัดการด้านเทคโนโลยีสารสนเทศ

1.1.1 โครงสร้างและทรัพยากรมีความคล่องตัว สอดคล้องกับโครงสร้างโดยรวมขององค์กร และมีการปรับปรุงทบทวนให้เกิดประสิทธิภาพในการดำเนินงานอยู่เสมอ

1.1.2 นโยบายที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศของสถาบันการเงินได้ครอบคลุมในเรื่องต่าง ๆ ภายในองค์กรอย่างเพียงพอ

1.1.3 แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศและโครงการด้านเทคโนโลยีสารสนเทศสามารถสนับสนุนแผนกลยุทธ์โดยรวม พร้อมทั้งการดำเนินธุรกิจของสถาบันการเงินให้ประสบความสำเร็จตามเป้าหมาย

1.1.4 การควบคุมและการกำกับดูแลมีความชัดเจน โปร่งใส โดยเน้นที่ความสามารถของคณะกรรมการ และ/หรือ ผู้บริหารระดับสูงในการตัดสินใจดำเนินการอย่างถูกต้องและในเวลาที่เหมาะสม

1.2 การตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ

1.2.1 นโยบายแผนงานและกระบวนการปฏิบัติควรเป็นไปตามแนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศครบถ้วนทุกธุรกรรมที่เกี่ยวข้อง รวมทั้ง การทบทวนจัดลำดับความสำคัญของการตรวจสอบความเสี่ยงที่เกิดขึ้นอย่างสม่ำเสมอ

1.2.2 ความเป็นอิสระในบทบาทหน้าที่ ความรับผิดชอบ และสายการบังคับบัญชาของสายงาน/หน่วยงานตรวจสอบ พร้อมทั้งการแสดงความเห็นได้อย่างเปิดเผยภายใต้กรอบของกฎหมายและคณะกรรมการสถาบันการเงินที่ยึดหลักธรรมาภิบาลที่ดี

1.3 ระบบข้อมูลเพื่อการบริหาร (MIS)

1.3.1 นโยบายด้านระบบสารสนเทศเพื่อการบริหารมีประสิทธิภาพเชื่อถือได้มีข้อมูลเพียงพอเพื่อประกอบการตัดสินใจ

1.3.2 การประมวลผลข้อมูลเพื่อการบริหารสามารถแสดงผลลัพธ์ได้ทันเวลาและสนองความต้องการของผู้ใช้งานได้อย่างแท้จริง

1.4 แผนสำรองฉุกเฉิน

1.4.1 ฝ่ายบริหารควรกำหนดนโยบายและการจัดการแผนสำรองฉุกเฉินให้ครอบคลุมการดำเนินงานทุกด้านเพื่อความต่อเนื่องของการให้บริการแก่องค์กรและลูกค้า

1.4.2 การติดตามดูแลการปฏิบัติตามแผนสำรองฉุกเฉินขององค์กรกระทำอย่างสม่ำเสมอ และปรับปรุงแผนให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลง

2. การปฏิบัติงานเทคโนโลยีสารสนเทศ

2.1 การรักษาความปลอดภัย (Security)

2.1.1 นโยบายการรักษาความปลอดภัย

2.1.2 ด้านกายภาพและตรรกะ (Physical & Logical)

2.1.3 ด้านข้อมูล

2.1.4 ด้านระบบเครือข่ายสื่อสาร

2.2 ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)

2.2.1 การบริหารโครงการ

2.2.2 การพัฒนาระบบงานและโปรแกรม รวมทั้งการจัดซื้อระบบงาน

2.2.3 การบำรุงรักษาระบบงานและการบริหารการเปลี่ยนแปลง

2.2.4 การบริหารการใช้บริการจากหน่วยงานภายนอก

2.3 ความพร้อมใช้งานของข้อมูล (Availability)

2.3.1 ความเพียงพอของแผนเตรียมความพร้อมต่อเหตุการณ์ฉุกเฉิน และแนวทางปฏิบัติงานในกรณีเกิดเหตุการณ์ฉุกเฉิน

2.3.2 ความถูกต้องของแผนสำรองฉุกเฉินรวมถึงการทดสอบแผนสำรองฉุกเฉินและการรายงานผลต่อระดับบริหาร

2.3.3 ประสิทธิภาพในการจัดการศูนย์สำรอง ความถูกต้องและครบถ้วนของการสำรองข้อมูลและระบบ

2.3.4 ความต่อเนื่องของการบำรุงรักษาและการประกันภัยอุปกรณ์คอมพิวเตอร์และระบบงาน

2.4 ความเสี่ยงด้านชื่อเสียง (Reputation)

2.4.1 การขาดความน่าเชื่อถือเนื่องจากระบบการรักษาความปลอดภัยมีจุดอ่อน

2.4.2 การถูกดำเนินคดีเนื่องจากการทุจริต

2.4.3 ความเสียหายทางการเงินอันเนื่องมาจากระบบการปฏิบัติงานบกพร่องและทุจริต

2.5 ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Regulation)

2.5.1 การไม่สามารถปฏิบัติตามกฎหมาย ระเบียบ คำสั่งที่ทางการกำหนด

2.5.2 การปรับปรุงกฎระเบียบ และกฎหมายให้ทันเทคโนโลยีสมัยใหม่อาจก่อให้เกิดความไม่เข้าใจและปฏิบัติไม่ถูกต้อง

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยงมีเป้าหมายให้ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศประเมินประสิทธิภาพของการบริหารและการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดย**จัดลำดับความเสี่ยงออกเป็น 2 ประเภท คือ ความเสี่ยงด้านการบริหารและความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ** ด้วยเหตุนี้ ในการประเมินความเสี่ยงของการดำเนินงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน **ผู้ตรวจสอบจะต้องสามารถระบุถึงปริมาณความเสี่ยง คุณภาพการบริหารความเสี่ยง ความเสี่ยงโดยรวม และแนวโน้มความเสี่ยง** โดยใช้ข้อสรุปที่ได้จากการตรวจสอบ ซึ่งการพิจารณาเพื่อประเมิน**ความเสี่ยงของสถาบันการเงินสามารถแบ่งออกเป็น 3 ด้าน ดังนี้**

1. **การประเมินความเสี่ยงเชิงปริมาณ**

การพิจารณาความเสี่ยงเชิงปริมาณ ก็คือ **การพิจารณาระดับหรือปริมาณความเสี่ยงที่เกิดขึ้นซึ่งสถาบันการเงินประสบอยู่และแสดงลักษณะของความเสี่ยงว่า ต่ำ ปานกลาง หรือสูง** ในลักษณะที่ว่าสถาบันการเงินมีการให้บริการทางการเงินต่อลูกค้าโดยอาศัยเทคโนโลยีสารสนเทศมากน้อยเพียงใด มีการนำเทคโนโลยีมาใช้กับงานสำคัญ ๆ ของสถาบันการเงินหรือไม่ และลักษณะโครงสร้างของระบบเทคโนโลยีสารสนเทศมีความซับซ้อนมากหรือไม่ เพราะยิ่งสถาบันการเงินมีการใช้เทคโนโลยีในการดำเนินธุรกิจมาก และระบบงานมีความซับซ้อนมาก สถาบันการเงินก็ยิ่งจะมีความเสี่ยงเกิดขึ้นมากเท่านั้น ทั้งนี้ มีปัจจัยในการพิจารณาดังต่อไปนี้

(1) ความสามารถของระบบเทคโนโลยีสารสนเทศ (Capacity)

(2) ความสลับซับซ้อนของโครงสร้างเทคโนโลยีสารสนเทศ (Complexity)

(3) ความสลับซับซ้อนของปัญหาทางด้านกฎหมาย (Litigation)

(4) ระดับของการให้บริการ (Services Levels)

2. **การประเมินความเสี่ยงเชิงคุณภาพ**

คุณภาพการบริหารความเสี่ยง คือ **การรู้จักความเสี่ยงดีเพียงใด ในการที่จะระบุได้ วัดผลได้ ควบคุมได้ และติดตามได้ และมีการแสดงลักษณะของความเสี่ยงว่า ดี พอใช้ หรืออ่อน** การพิจารณาความเสี่ยงเชิงคุณภาพ ก็คือ การพิจารณาในลักษณะที่ว่าสถาบันการเงินมีการดำเนินงานด้านเทคโนโลยีสารสนเทศในลักษณะใดบ้าง เพื่อให้ตนเองสามารถที่จะควบคุม หรือลดระดับของความเสี่ยงจากการดำเนินงานด้านเทคโนโลยีสารสนเทศนั้นให้เหลือในระดับที่สถาบันการเงินสามารถยอมรับความเสี่ยงนั้นๆ ในการดำเนินงานประจำวันได้ (ความเสี่ยงนั้นจะต้องไม่มีผลกระทบที่รุนแรงจนกระทบกับฐานะและการหารายได้ของสถาบันการเงิน) โดยปัจจัยที่ใช้ในการพิจารณา

เพื่อประเมินความเสี่ยงเชิงคุณภาพมีดังนี้

(1) เป้าหมายในการดำเนินธุรกิจของสถาบันการเงิน (Goals)

(2) ผลกระทบในการดำเนินธุรกิจของสถาบันการเงิน (Effect on Business)

(3) ผลการเปลี่ยนแปลงของสถาบันการเงินและความสามารถในการควบคุมการเปลี่ยนแปลง (Pace of Change)

(4) ประเภทของการให้บริการมีความสลับซับซ้อนหรือไม่ และสถาบันการเงินได้มีการเตรียมการรองรับอยู่ในระดับใด (Services)

(5) นโยบายของสถาบันการเงินในการดำเนินงานด้านเทคโนโลยีสารสนเทศมีความเป็นไปได้เพียงใด (Services Levels)

(6) ขั้นตอนในการดำเนินธุรกรรมของสถาบันการเงินว่ามีประสิทธิภาพหรือไม่ (Processes)

(7) ประสิทธิภาพของบุคลากรของสถาบันการเงิน (Human Resources)

(8) ประสิทธิภาพของเครื่องมือในการวัดผลการดำเนินงานของสถาบันการเงินว่ามีประสิทธิภาพหรือไม่ (Feedback Devices)

3. **การประเมินความเสี่ยงโดยรวม**

เป็นการตัดสินใจสรุปเกี่ยวกับระดับการกำกับดูแลที่ต้องเอาใจใส่ การตัดสินใจ**จะต้องสอดคล้องกับปริมาณความเสี่ยงและคุณภาพการบริหารความเสี่ยงของสถาบันการเงินนั้น** โดย**ผู้ตรวจสอบจะให้น้ำหนักที่สัมพันธ์กับความสำคัญของความเสี่ยงแต่ละด้าน ลักษณะความเสี่ยงโดยรวมจะแสดงเป็น ต่ำ ค่อนข้างต่ำ ปานกลาง ค่อนข้างสูง และสูง**

อนึ่ง ในการพิจารณาความเสี่ยงโดยรวม จะต้องนำแนวโน้มความเสี่ยงเข้ามาพิจารณาควบคู่กันด้วย เนื่องจากเป็นปัจจัยที่มีอิทธิพลต่อการกำหนดกลยุทธ์ในการกำกับดูแลสถาบันการเงิน แนวโน้มความเสี่ยงจะสะท้อนให้เห็นการเปลี่ยนแปลงของความเสี่ยง ซึ่ง**ทิศทางการเปลี่ยนแปลงของความเสี่ยงมี 3 แบบ คือ ลดลง คงที่ หรือเพิ่มขึ้น** ผู้ตรวจสอบสามารถนำแนวโน้มความเสี่ยงมาใช้วิเคราะห์สำหรับพิจารณาขอบเขตการตรวจสอบครั้งต่อไป

ขั้นตอนการตรวจสอบ

ในการปฏิบัติงานตรวจสอบของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ มีขั้นตอนปฏิบัติ 3 ขั้นตอนคือ ขั้นตอนเตรียมการก่อนออกตรวจสอบ (Pre-Examination) ขั้นตอนปฏิบัติงานตรวจสอบ (Onsite Examination) และขั้นตอนการสรุปผลและจัดทำรายงาน (Post-Examination) ซึ่งผู้ตรวจสอบสามารถอ่านรายละเอียดเกี่ยวกับวิธีปฏิบัติงานในแต่ละขั้นตอนได้ในคู่มือการปฏิบัติ

งานของส่วนตรวจสอบเทคโนโลยีสารสนเทศ ใน Public Folder ของสายกำกับสถาบันการเงิน

<u>ขั้นเตรียมการก่อนออกตรวจสอบ</u>

วัตถุประสงค์

กระบวนการเตรียมการก่อนออกตรวจสอบ มีวัตถุประสงค์หลัก ดังต่อไปนี้

- เพื่อลดเวลาที่ใช้ในการตรวจสอบสถาบันการเงินและลดภาระที่มีต่อผู้บริหารและเจ้าหน้าที่ของสถาบันการเงิน

- เพื่อให้เข้าใจสถาบันการเงินที่จะออกตรวจสอบในเบื้องต้น ในเรื่องโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบรักษาความปลอดภัย และงานบริการด้านเทคโนโลยีสารสนเทศ

- เพื่อประเมินระดับความเสี่ยงและพิจารณานโยบาย ขั้นตอน ระบบการติดตามที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ

- เพื่อให้ทราบถึงความเปลี่ยนแปลงต่างๆที่เกิดขึ้นของธุรกรรมและการบริการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของสถาบันการเงิน จากช่วงเวลาที่เข้าตรวจสอบครั้งล่าสุด

- เพื่อกำหนดขอบเขตการตรวจสอบโดยมุ่งเน้นประเด็นไปที่การดำเนินธุรกรรมหรือการบริการที่จะทำให้สถาบันการเงินมีความเสี่ยงเพิ่มขึ้น

วิธีการ

(1) รวบรวมข้อมูล

(2) วิเคราะห์และประเมินข้อมูลที่ได้รับ

(3) สรุปประเด็นและกำหนดขอบเขตการตรวจสอบ

(4) การจัดสรรกำลังคน ระยะเวลาที่ใช้ในการตรวจสอบ และจัดทำแผนการตรวจสอบ

(5) การขออนุมัติออกตรวจสอบ

(6) การเตรียมการเพื่อออกตรวจสอบ

รายละเอียดขั้นตอนการเตรียมการก่อนออกตรวจสอบ

1 รวบรวมข้อมูล

รวบรวมข้อมูลทั้งจากภายในและภายนอกเพื่อเป็นพื้นฐานการประเมินลักษณะการดำเนินงาน การบริการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเบื้องต้น และควรติดต่อขอข้อมูลจากส่วนงานอื่นในสายกำกับสถาบันการเงิน ได้แก่ ฝ่ายวิเคราะห์และติดตามฐานะ ฝ่ายกำกับสถาบันการเงิน และข้อมูลจากสายงานอื่น ได้แก่ สายนโยบายสถาบันการเงินและสายระบบชำระเงินเพื่อรวบรวมประเด็นที่ต้องติดตามและการสั่งการของทางการต่อสถาบันการเงิน นอกจากนี้ ควรติดตาม

ข่าวสารและความเคลื่อนไหวต่าง ๆ ด้านเทคโนโลยีสารสนเทศในวงการที่เกี่ยวข้องจากแหล่งข้อมูลต่าง ๆ ซึ่งข้อมูลเบื้องต้นที่ผู้ตรวจสอบควรศึกษาและรวบรวม คือ

(1) รายงานการตรวจสอบและกระดาษทำการของการตรวจสอบครั้งก่อนเพื่อติดตามประเด็นที่มีนัยสำคัญที่พบจากการตรวจสอบครั้งก่อน

(2) รายงานจากผู้ตรวจสอบภายในและภายนอก หรือรายงานการตรวจสอบของผู้ให้บริการแก่สถาบันการเงิน และรายงานตรวจสอบอื่น ๆ ที่เกี่ยวข้อง

(3) รายชื่อบริษัทตัวแทนจำหน่ายหรือผู้ให้บริการ

(4) รายละเอียดของผลิตภัณฑ์หรือบริการ และการวิเคราะห์ฐานะทางการเงินของบริษัทตัวแทนฯ หรือผู้ให้บริการ

(5) รายชื่อของระบบคอมพิวเตอร์และระบบเครือข่าย

(6) รายชื่อของ Software และโปรแกรมระบบงานที่สนับสนุนการประมวลผลข้อมูลทางการเงินหรือกระบวนการบริหารความเสี่ยง

(7) รายงานที่ใช้ติดตามกิจกรรมทางด้านคอมพิวเตอร์ การดำเนินงานระบบเครือข่ายความสามารถของระบบ การละเมิดระบบรักษาความปลอดภัย และการบุกรุกระบบเครือข่าย

(8) เรื่องที่สถาบันการเงินขออนุญาตหรือแจ้งให้ ธปท. ทราบทางด้านเทคโนโลยีสารสนเทศ

(9) ผังโครงสร้างองค์กร สายการบังคับบัญชา การบริหารดูแลและควบคุมกิจกรรมทางด้านเทคโนโลยีสารสนเทศของทั้งองค์กร

(10) แผนกลยุทธ์และทิศทางการดำเนินงานทางด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

(11) รายงานการประชุมของคณะกรรมการที่เกี่ยวข้องกับกิจกรรมทางด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

(12) นโยบายการรักษาความปลอดภัยของสถาบันการเงิน

(13) แผนการเตรียมความพร้อมรับสถานการณ์ฉุกเฉินของสถาบันการเงิน

(14) การออกแบบเพื่อพัฒนาระบบเทคโนโลยีสารสนเทศใหม่ และ/หรือปรับปรุงระบบเทคโนโลยีสารสนเทศเดิม

(15) การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากบุคคลภายนอก

2. วิเคราะห์และประเมินข้อมูลที่ได้รับ

นำข้อมูลที่รวบรวมมาวิเคราะห์และประเมินความเสี่ยงในเบื้องต้น โดยพิจารณาตามแนวทางการประเมินความเสี่ยงเพื่อกำหนดขอบเขตการตรวจสอบ และอาจซักถามประเด็น ข้อ

สงสัยกับองค์กรภายนอกที่เกี่ยวข้อง เช่น ผู้ประเมินระบบอิสระเพื่อให้เกิดความเข้าใจมากขึ้น และอาจขอข้อมูลเพิ่มเติม หากข้อมูลที่รวบรวมยังไม่มีความเพียงพอ ซึ่งการวิเคราะห์และประเมินข้อมูลควรดำเนินการ ดังนี้

(1) สอบทานข้อมูลจากรายงานการตรวจสอบจากครั้งก่อนเพื่อกำหนดประเด็นปัญหาที่ต้องติดตาม

(2) หากไม่มีข้อมูลจากการตรวจสอบครั้งก่อนให้ขอข้อมูลจากสถาบันการเงินและสอบทานข้อมูลที่มีอยู่เพื่อพิจารณาเกี่ยวกับลักษณะโครงสร้างความซับซ้อนของการประมวลผลและรายงานที่ผู้บริหารใช้ในการกำกับดูแลทางด้านเทคโนโลยีสารสนเทศ

(3) สอบทานข้อมูลและเอกสารจากฝ่ายกำกับสถาบันการเงินเพื่อใช้ในการติดตามประเด็นต่าง ๆ ที่เกี่ยวข้องทางด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและเรื่องที่สถาบันการเงินขออนุญาตหรือแจ้งให้ ธปท. ทราบ

(4) พิจารณาแผนงาน นโยบายการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ รายงานการประชุมคณะกรรมการที่เกี่ยวข้องทางด้านเทคโนโลยีสารสนเทศเพื่อวิเคราะห์ปัญหาและอุปสรรคในการดำเนินงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

3. สรุปประเด็นและกำหนดขอบเขตการตรวจสอบ

3.1 สรุปภาพรวมของการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ โครงสร้างระบบงาน ระบบเครือข่าย และระบบรักษาความปลอดภัย

3.2 ประเมินการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจและ ความเพียงพอของการบริหารจัดการด้านเทคโนโลยีสารสนเทศ

3.3 ระบุการบริหารหรือการดำเนินงานที่มีแนวโน้มความเสี่ยงสูง

3.4 กำหนดประเด็นสำคัญที่ต้องติดตาม โดยเรียงลำดับความสำคัญของประเด็นที่พบตามระดับความเสี่ยงจากสูงไปหาต่ำ โดยอาศัยผลการวิเคราะห์ข้อมูลและวิจารณญาณของทีมผู้ตรวจสอบ

3.5 ศึกษาปัจจัยภายนอกที่สำคัญที่อาจก่อให้เกิดความเสี่ยงใดๆ แก่สถาบันการเงิน เช่น การเปลี่ยนแปลงทางเทคโนโลยีที่ก้าวหน้าอย่างรวดเร็ว

3.6 เข้าร่วมประชุมหารือกับฝ่ายตรวจสอบ ฝ่ายกำกับสถาบันการเงิน และฝ่ายวิเคราะห์และติดตามฐานะ

3.7 กำหนดวัตถุประสงค์และขอบเขตการตรวจสอบ โดย

- สรุปผลการประเมินความเสี่ยงเบื้องต้น
- กำหนดขอบเขตธุรกรรมที่จะทำการทดสอบรายการ (ในกรณีที่จำเป็น)

- พิจารณาให้สอดคล้องกับนโยบายจากผู้บริหารระดับสูง (กรณีมีคำสั่งตรวจเฉพาะเรื่อง)

3.8 จัดทำบันทึกแสดงขอบเขตการตรวจสอบ โดยกำหนดหัวข้อขั้นต่ำ ดังนี้

- วัตถุประสงค์ของการตรวจสอบ
- เรื่องที่จะตรวจสอบ
- ขอบเขตธุรกรรมที่จะทำการทดสอบรายการ (ในกรณีที่จำเป็น)
- จำนวนผู้ตรวจสอบ
- ระยะเวลาการตรวจสอบ

4. การจัดสรรกำลังคน ระยะเวลาที่ใช้ในการตรวจสอบ และจัดทำแผนการตรวจสอบ

4.1 กำหนดแผนตรวจสอบจากผลการประเมินการดำเนินงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

4.2 ประมาณอัตรากำลังคนและเวลาที่จะใช้ในการตรวจสอบในแต่ละเรื่อง

4.3 จัดทำแผนการตรวจสอบ

5. การขออนุมัติออกตรวจสอบ

เสนอบันทึกขออนุมัติออกตรวจสอบสถาบันการเงิน พร้อมแนบแผนการตรวจสอบให้ผู้อำนวยการ ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ พิจารณาอนุมัติการออกตรวจสอบ

6. การเตรียมการเพื่อออกตรวจสอบ

6.1 จัดเตรียมรายการขอเอกสาร (โปรดดูภาคผนวก) เพื่อส่งให้สถาบันการเงินได้จัดเตรียมไว้ให้ในวันแรกของการออกตรวจสอบ

6.2 จัดเตรียมหนังสือถึงผู้บริหารสถาบันการเงินเพื่อแจ้งการเข้าตรวจสอบและส่งให้สถาบันการเงินลงนามรับทราบก่อนเข้าตรวจสอบ (ในกรณีที่เป็นการตรวจสอบร่วมกับทางฝ่ายตรวจสอบ 1 ฝ่ายตรวจสอบ 2 หรือฝ่ายตรวจสอบสถาบันเฉพาะกิจและ Non-bank EIC จะเป็นผู้จัดเตรียม)

6.3 ส่งบันทึกแสดงขอบเขตการตรวจสอบให้ผู้ตรวจสอบที่จะออกตรวจรับทราบ

6.4 ชี้แจงให้ทีมผู้ตรวจสอบเข้าใจขอบเขต แผนงาน และการจัดสรรกำลังคนในการตรวจสอบ

6.5 ยืนยันการนัดหมายกับผู้บริหารของสถาบันการเงิน เพื่อพบปะหารือใน

วันแรกของการตรวจสอบ

6.6 เตรียมเอกสาร กระดาษทำการ อุปกรณ์ และเครื่องเขียนต่างๆ ที่ใช้ในการตรวจสอบ

<u>ขั้นปฏิบัติงานตรวจสอบ</u>

วัตถุประสงค์

- เพื่อ**ประเมินระดับความเสี่ยง**โดยพิจารณาจากขนาด ปริมาณ และโครงสร้างความซับซ้อนของธุรกรรมและลักษณะการให้บริการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

- เพื่อ**ประเมินจุดอ่อนในโครงสร้างของระบบงาน** และ**ความรัดกุม**ของสภาพแวดล้อมของระบบรักษาความปลอดภัย

- เพื่อ**ประเมินระดับความเสี่ยงจากทิศทาง**ของแนวนโยบายของระดับ และแผนดำเนินธุรกิจต่าง ๆ ทางด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

- เพื่อ**ประเมินความเพียงพอ ความมีประสิทธิภาพของการกำหนด วัดติดตาม และควบคุมความเสี่ยง**

- เพื่อให้**ข้อเสนอแนะในการแก้ไขปัญหา**หรือลดความเสี่ยงในการดำเนินงานด้านเทคโนโลยีสารสนเทศ ก่อนที่จะเกิดความเสียหายแก่สถาบันการเงินเป็นสำคัญ

วิธีการ

(1) **นัดหมายผู้บริหารเพื่อให้นำเสนอข้อมูลของแต่ละฝ่ายงาน**ที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ

(2) ตรวจสอบตามแนวทางการประเมินความเสี่ยงซึ่งแบ่งเป็น 4 ด้าน ได้แก่ การบริหารงานเทคโนโลยีสารสนเทศ ความถูกต้องเชื่อถือได้ของข้อมูล การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ และความพร้อมใช้งานเทคโนโลยีสารสนเทศ นอกจากนั้น ผู้ตรวจสอบควรพิจารณาแนวทางการตรวจสอบในคู่มือการตรวจสอบเทคโนโลยีสารสนเทศ (FFIEC 2003-2006) และคู่มือการตรวจสอบ E-Banking มาประยุกต์ใช้ร่วมกันด้วย

(3) สรุปผลการตรวจสอบเบื้องต้นกับผู้บริหารของสถาบันการเงิน (Exit Meeting)

(4) สรุปผลการตรวจสอบอย่างเป็นทางการกับผู้บริหารระดับสูง

<u>ขั้นการสรุปผลและจัดทำรายงาน</u>

วัตถุประสงค์

เพื่อจัดทำรายงานการตรวจสอบด้านเทคโนโลยีสารสนเทศ และนำเสนอผู้บริหาร ธนาคารแห่งประเทศไทย เพื่อพิจารณาอนุมัติ

วิธีการ

(1) จัดทำบันทึกสรุปผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ

(2) จัดทำรายงานการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งรวมผลการตรวจสอบด้าน E-Banking เข้ามาด้วยแล้ว

(3) นำรายงานการตรวจสอบด้านเทคโนโลยีสารสนเทศเข้าพิจารณาในที่ประชุมคณะกลั่นกรองผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ เพื่อพิจารณาผลการตรวจสอบ

(4) ส่งรายงานการตรวจสอบด้านเทคโนโลยีสารสนเทศที่แก้ไขแล้วตามความเห็นในที่ประชุมคณะกลั่นกรองผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ ให้ฝ่ายตรวจสอบ 1 , 2 หรือฝ่ายตรวจสอบสถาบันเฉพาะกิจและ Non-bank เพื่อจัดทำรายงานการตรวจสอบของสถาบันการเงิน

(5) ประสานงานกับ EIC เพื่อจัดทำเอกสารการนำเสนอในที่ประชุมคณะอนุกรรมการพัฒนาการตรวจสอบสถาบันการเงิน (อพส.) ซึ่งเกี่ยวข้องกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ

การเขียนรายงานการตรวจสอบด้านเทคโนโลยีสารสนเทศ

การสรุปผลในรายงานการตรวจสอบด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบจะต้องเรียบเรียงและจัดกลุ่มประเด็นต่างๆ โดยแบ่งหัวข้อตามความเสี่ยงที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ ประกอบด้วยความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ และความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ จะว่าด้วยเรื่องที่เกี่ยวข้องกับนโยบาย การจัดการ บทบาทคณะกรรมการและฝ่ายบริหาร การพัฒนาบุคลากร ตรวจสอบภายในและภายนอก รายงานสำหรับผู้บริหาร การบริหารงานทั่วไปเกี่ยวกับงานด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารเฉพาะด้านของการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ ความถูกต้องและน่าเชื่อถือของข้อมูล และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ จะว่าด้วยเรื่องขั้นตอนและวิธีปฏิบัติ ทั้งที่เป็นกระบวนการทำงานประจำ (Daily Operation) และงานในลักษณะโครงการ ซึ่งเกี่ยวกับเรื่องการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ ความถูกต้องเชื่อถือได้ของข้อมูล และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ

หากผู้ตรวจสอบพบว่ามีประเด็นที่อาจส่งผลกระทบต่อความเสี่ยงด้านอื่น ได้แก่ ความเสี่ยงด้านเครดิต ความเสี่ยงด้านตลาด และความเสี่ยงด้านสภาพคล่อง ให้ดำเนินการรวบรวมประเด็นหรือข้อสังเกตที่พบ เพื่อประสานงาน/หรือส่งหลักฐานให้ทีมตรวจสอบที่รับผิดชอบตรวจสอบความเสี่ยงด้านนั้น ๆ ทราบ เพื่อดำเนินการต่อไป

วิธีการตรวจสอบ

การตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยง **ผู้ตรวจสอบ ต้องประเมินการดำเนินงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงินตามแนวทางการพิจารณาความเสี่ยงซึ่งเป็นมาตรฐานขั้นต่ำที่สถาบันการเงินพึงปฏิบัติ** โดยพิจารณาตามขอบเขตการตรวจสอบหลัก 2 เรื่อง คือ การบริหารงานและการปฏิบัติงานเทคโนโลยีสารสนเทศ ในสถานการณ์ที่สถาบันการเงินมีความเสี่ยงเพิ่มขึ้นและมีความซับซ้อนในการนำเทคโนโลยีมาใช้มากขึ้น ผู้ตรวจสอบอาจขยายการสอบทานด้านเทคโนโลยีสารสนเทศเพิ่มขึ้นโดยนำเอาวิธีการปฏิบัติจากคู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศของ FFIEC ปี 2003 – 2006 และคู่มือการตรวจสอบ E-Banking มาใช้ประกอบการตรวจสอบด้วย

ผู้ตรวจสอบจะต้องดำเนินการตรวจสอบเพื่อประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ**โดยพิจารณาใน 3 ประเด็นหลัก คือ**

1. **แนวทางการพิจารณาความเสี่ยง**
2. **การประเมินความเสี่ยง**
3. **ผลกระทบต่อความเสี่ยง**

แนวทางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยพิจารณาตามขอบเขตการตรวจสอบ มีดังนี้

ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ		
แนวทางการพิจารณาความเสี่ยง	**การประเมินความเสี่ยง**	**ผลกระทบต่อความเสี่ยง**
การบริหารงานเทคโนโลยีสารสนเทศ	การบริหารงานเทคโนโลยีสารสนเทศให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการจัดการ (Management)** ประกอบการตรวจสอบ	
1. โครงสร้างองค์กรและทรัพยากรด้านเทคโนโลยีสารสนเทศ	1.1 โครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศของสถาบันการเงินมีความเหมาะสมเพียงพอกับธุรกิจโดยพิจารณาจาก - ผังโครงสร้างองค์กรโดยรวม และโครงสร้างด้านเทคโนโลยีสารสนเทศ - โครงสร้างสายงานการบังคับบัญชาและอำนาจการบริหารงาน - ความชัดเจนในการแบ่งแยกอำนาจและหน้าที่ของสายงานเทคโนโลยีสารสนเทศ	โครงสร้างด้านเทคโนโลยีสารสนเทศและทรัพยากรที่ไม่เหมาะสมกับโครงสร้างองค์กรโดยรวม ระบบคอมพิวเตอร์ที่ไม่ได้รับการดูแลให้มีเสถียรภาพ หรือล้าสมัยจะลดความสามารถในการแข่งขัน ซึ่งจะมีผลกระทบถึงความเสี่ยงด้านกลยุทธ์และการดำเนินงานของสถาบันการเงิน
	1.2 จัดสรรทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างเหมาะสมเพียงพอกับขนาดความซับซ้อนของธุรกรรมสถาบันการเงินเพื่อให้การดำเนินธุรกิจเป็นไปอย่างต่อเนื่อง โดยพิจารณาถึง ฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย บุคลากร และระบบข้อมูล เป็นต้น	
	1.3 การคัดเลือก การพัฒนา การอบรมทรัพยากรบุคคล และการจัดสรรทรัพยากรให้มีประสิทธิภาพ	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
2. นโยบายด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน	2.1 กระบวนการในการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศควรมาจากฝ่ายบริหารของสถาบันการเงินโดยมีความเพียงพอเหมาะสมกับระดับและปริมาณของกิจกรรมทางด้านเทคโนโลยีสารสนเทศเพื่อรองรับความเสี่ยงที่เกิดจากธุรกรรมต่าง ๆ ของสถาบันการเงิน ดังนั้น นโยบายด้านเทคโนโลยีสารสนเทศควรมีความครอบคลุมในเรื่องสำคัญต่าง ๆ อย่างน้อย ดังต่อไปนี้	หากสถาบันการเงินขาดการบริหารจัดการที่เหมาะสมเพียงพอ ไม่ได้กำหนดนโยบายทางด้านเทคโนโลยีสารสนเทศที่สำคัญย่อมมีผลกระทบต่อความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านชื่อเสียง และความเสี่ยงด้านการปฏิบัติตามกฎหมาย
	- นโยบายด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ - นโยบายด้านความถูกต้องเชื่อถือได้ของข้อมูล - นโยบายด้านความพร้อมใช้งานเทคโนโลยีสารสนเทศซึ่งรวมถึงนโยบายเกี่ยวกับแผนฟื้นฟูธุรกิจและแผนสำรองฉุกเฉินของสถาบันการเงินเพื่อให้ธุรกิจของสถาบันการเงินไม่เกิดการหยุดชะงัก	
	2.2 นโยบายด้านการให้บริการและการใช้บริการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ช่วยในการจัดการด้านเทคโนโลยีสารสนเทศแก่สถาบันการเงิน	
	2.3 สถาบันการเงินควรกำหนดให้มีระบบสารสนเทศเพื่อการบริหารอย่างเพียงพอและมีประสิทธิภาพ	
	2.4 สถาบันการเงินควรจัดให้มีนโยบายการประกันความเสี่ยงและความเสียหายที่อาจจะเกิดขึ้นและมีผลกระทบต่อด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
3. แผนกลยุทธ์และแผนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	3.1 แผนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศควรสอดคล้องกับแผนกลยุทธ์และเป้าหมายหลักของสถาบันการเงิน	ผลกระทบจากการที่สถาบันการเงินไม่มีแผนกลยุทธ์และแผนปฏิบัติงานด้านเทคโนโลยีสารสนเทศ หรือมีแต่ไม่สนับสนุนแผนกลยุทธ์และเป้าหมายโดยรวม หรือไม่สามารถดำเนินการตามระยะเวลาที่กำหนดในแผน จัดเป็นความเสี่ยงด้านกลยุทธ์ของสถาบันการเงิน
	3.2 แผนกลยุทธ์และแผนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศควรจัดทำเป็นแผนระยะสั้น และแผนระยะยาว	
	3.3 การประเมินการควบคุม และการติดตามผลปฏิบัติงานตามแผนงานด้านเทคโนโลยีสารสนเทศที่สนับสนุนกับแผนกลยุทธ์โดยรวมของสถาบันการเงิน	
	3.4 การจัดสรรงบประมาณด้านเทคโนโลยีสารสนเทศควรสอดคล้องกับแผนกลยุทธ์และเป้าหมายหลักของสถาบันการเงิน	
	3.5 กำหนดให้มีระเบียบและขั้นตอนการปฏิบัติงานต่าง ๆ ให้ครอบคลุมทุกด้านที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	
	3.6 กำหนดให้มีสัญญาและเงื่อนไขต่าง ๆ ต่อบุคคลภายนอกที่ช่วยในการจัดการด้านเทคโนโลยีสารสนเทศ	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
4. บทบาทของคณะกรรมการ และ / หรือผู้บริหารในการกำกับงานด้านเทคโนโลยีสารสนเทศ	4.1 สอบทานรายงานการประชุมเพื่อประเมินบทบาทของคณะกรรมการว่า นำแผนไปกำหนดวิธีปฏิบัติงานอย่างเหมาะสมและเพียงพอต่อความต้องการขององค์กร ได้แก่ รายงานประชุมของคณะกรรมการ ดังนี้ - คณะกรรมการธนาคาร - คณะกรรมการบริหาร - คณะกรรมการตรวจสอบ - คณะกรรมการด้านเทคโนโลยีสารสนเทศ	บทบาท หน้าที่ ความรับผิดชอบและการตัดสินใจที่ไม่เหมาะสม ตลอดจนขาดการติดตามดูแลที่ดีจะก่อให้เกิดผลกระทบต่อความเสี่ยงด้านกลยุทธ์ และความเสี่ยงด้านปฏิบัติงาน
	4.2 คณะกรรมการสถาบันการเงินต้องตระหนักถึงการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และวิธีปฏิบัติในการบริหารความเสี่ยงเพื่อประเมินการควบคุม และติดตามความเสี่ยงที่เกิดจากงานด้านเทคโนโลยีสารสนเทศ	
	4.3 คณะกรรมการสถาบันการเงินควรกำหนดโครงสร้างการดำเนินงานด้านเทคโนโลยีสารสนเทศให้มีคณะกรรมการด้านเทคโนโลยีสารสนเทศทำหน้าที่ดูแลด้านเทคโนโลยีสารสนเทศ และติดตามดูแลการดำเนินงานตามแผนงานต่าง ๆ ในด้านเทคโนโลยีสารสนเทศ	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
การตรวจสอบภายใน **1. นโยบายแผนงาน และกระบวนการปฏิบัติงาน**	การตรวจสอบภายในให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการตรวจสอบภายในและภายนอก (Audit)** ประกอบการตรวจสอบ	
	1.1 นโยบายและแผนการตรวจสอบประจำปีควรมีความสอดคล้องกับแผนกลยุทธ์โดยรวมของสถาบันการเงิน	หากสถาบันการเงินขาดนโยบายและการวางแผนการปฏิบัติงานตรวจสอบที่ดีและขาดการจัดทำคู่มือการปฏิบัติงานตรวจสอบอาจทำให้เกิดความเสี่ยงด้านกลยุทธ์และส่งผลกระทบต่อความเสี่ยงด้านการปฏิบัติงาน
	1.2 แผนการตรวจสอบด้านเทคโนโลยีสารสนเทศควรมีขอบเขตและความถี่ในการตรวจสอบ โดยพิจารณาให้ครอบคลุมประเภทของธุรกรรมและลักษณะความเสี่ยงที่เกี่ยวข้องของสถาบันการเงิน	
	1.3 สถาบันการเงินควรมีบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านในการตรวจสอบเทคโนโลยีสารสนเทศ	
	1.4 สถาบันการเงินควรมีการจัดทำแผนการตรวจสอบและจัดสรรทรัพยากรด้านการตรวจสอบเพื่อให้บรรลุเป้าหมายที่กำหนด	
	1.5 สถาบันการเงินควรจัดทำคู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศเพื่อให้ผู้ตรวจสอบได้ใช้เป็นแนวทางในการปฏิบัติงาน	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
2. ความเป็นอิสระ และหน้าที่ความรับผิดชอบด้านการตรวจสอบเทคโนโลยีสารสนเทศ	2.1 พิจารณาโครงสร้างสายการบังคับบัญชา บทบาทหน้าที่และการกำกับดูแลสายงานตรวจสอบควรมีความเป็นอิสระจากฝ่ายบริหารจัดการของสถาบันการเงิน	หากการดำเนินงานของสายตรวจสอบภายในของสถาบันการเงินไม่เป็นอิสระจะทำให้การบริหารและควบคุมความเสี่ยงไม่มีประสิทธิภาพส่งผลกระทบต่อความเสี่ยงด้านกลยุทธ์ และด้านการปฏิบัติงานของสถาบันการเงิน
	2.2 การกำหนดแผนการตรวจสอบ และขอบเขตการตรวจสอบควรมีความเป็นอิสระและได้รับอนุมัติจากคณะกรรมการตรวจสอบ	
	2.3 รายงานการตรวจสอบที่จัดส่งให้ผู้บริหารระดับสูง และคณะกรรมการที่เกี่ยวข้องควรมีความครอบคลุมเพียงพอเพื่อให้ฝ่ายจัดการดำเนินการแก้ไขประเด็นข้อบกพร่องต่าง ๆ ที่ระบุไว้ในรายงานตรวจสอบอย่างเพียงพอและทันเวลา	
ระบบสารสนเทศเพื่อการบริหาร **1. นโยบายด้านระบบสารสนเทศเพื่อการบริหาร**	การตรวจสอบระบบสารสนเทศเพื่อการบริหารให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการจัดการ (Management)** ประกอบการตรวจสอบ	
	1.1 จัดให้มีระบบสารสนเทศเพื่อการบริหารที่ช่วยในการตัดสินใจอย่างมีประสิทธิภาพ และเชื่อถือได้เพื่อให้ผู้บริหารมีข้อมูลที่เพียงพอประกอบการตัดสินใจ	หากการจัดการระบบสารสนเทศเพื่อการบริหารไม่เพียงพอ ทำให้การตัดสินใจเชิงกลยุทธ์ต่าง ๆ ไม่มีประสิทธิภาพทันต่อเหตุการณ์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว ส่งผลให้เกิดความเสี่ยงด้านกลยุทธ์ และความเสี่ยงด้านการปฏิบัติงาน

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	1.2 สถาบันการเงินควรจัดให้มีทรัพยากรอย่างเหมาะสมเพียงพอเพื่อรองรับการจัดทำระบบสารสนเทศเพื่อการบริหารที่มีประสิทธิภาพ	
แผนสำรองฉุกเฉิน **1. นโยบายและการจัดการแผนสำรองฉุกเฉิน**	การตรวจสอบแผนสำรองฉุกเฉินให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning)** ประกอบการตรวจสอบ	
	1.1 การกำหนดนโยบายของแผนสำรองฉุกเฉินควรมีกระบวนการในการดำเนินการโดยฝ่ายบริหารของสถาบันการเงิน	หากสถาบันการเงินขาดนโยบาย การติดตาม ดูแลการปฏิบัติงานตามแผนสำรองฉุกเฉินอาจส่งผลให้ไม่สามารถกู้ระบบกลับคืนได้อย่างทันเวลา ส่งผลให้การดำเนินธุรกิจหยุดชะงักหรือขาดความต่อเนื่อง กระทบต่อความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน และความเสี่ยงด้านชื่อเสียงต่อสถาบันการเงินได้
	1.2 นโยบายทางด้านเทคโนโลยีสารสนเทศของสถาบันการเงินควรมีความครอบคลุมเรื่องต่อไปนี้ - Business Continuity Plan (BCP) - Disaster Recovery Plan (DRP) - Contingency Plan - Incident Response Plan (IRP)	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	1.3 การติดตามดูแลการปฏิบัติงานตามแผนสำรองฉุกเฉินต่าง ๆ ที่กำหนดไว้ในนโยบายหรือแผนงานของสถาบันการเงิน พร้อมทั้ง ปรับปรุงแผนให้ทันสมัยสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไปของสถาบันการเงิน	

ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ

การรักษาความปลอดภัย (security)

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
1. ด้านนโยบาย การรักษาความปลอดภัย (Security Policy)	นโยบายการรักษาความปลอดภัยให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล (Information Security)** ประกอบการตรวจสอบ	
	1.1 สถาบันการเงินควรมีนโยบายการรักษาความปลอดภัยที่มีความสัมพันธ์กับการใช้เทคโนโลยีสารสนเทศขององค์กร การกำหนดแผนการรักษาความปลอดภัยควรมีความสอดคล้องกับนโยบายการรักษาความปลอดภัยโดยรวมขององค์กร นโยบายและแผนงานดังกล่าวจะต้องผ่านการอนุมัติและติดตามดูแลโดยคณะกรรมการของ สถาบันการเงิน	หากสถาบันการเงินไม่มีนโยบาย ระเบียบวิธีปฏิบัติในด้านการรักษาความปลอดภัย รวมทั้งขาดการประชาสัมพันธ์ให้พนักงานตระหนักถึงการรักษาความปลอดภัยที่ดี และไม่มีหน่วยงานที่รับผิดชอบการรักษาความปลอดภัย ทำให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศไม่สนับสนุนแผนกลยุทธ์ขององค์กรก่อให้เกิดผลกระทบต่อความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน และความเสี่ยงด้านชื่อเสียงได้

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	1.2 สถาบันการเงินควรมีการกำหนดระเบียบวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัยให้เพียงพอเหมาะสมและสอดคล้องกับความเสี่ยงขององค์กรที่เปลี่ยนแปลงไป	
	1.3 สถาบันการเงินควรมีหน่วยงานที่รับผิดชอบในการรักษาความปลอดภัยเพื่อเป็นศูนย์กลางในการควบคุมดูแลการรักษาความปลอดภัยให้แก่องค์กร	
	1.4 ควรจัดให้มีมาตรการส่งเสริมให้พนักงานตระหนักถึงความสำคัญของการรักษาความปลอดภัยขององค์กร และต้องปฏิบัติตามระเบียบโดยเคร่งครัด จัดให้มีการประชาสัมพันธ์ภายในองค์กรให้พนักงานตระหนักถึงความสำคัญของการรักษาความปลอดภัย และการเปลี่ยนแปลงระเบียบวิธีปฏิบัติ	
2. การรักษาความปลอดภัยด้านกายภาพ (Physical security)	การรักษาความปลอดภัยด้านกายภาพให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล (Information Security)** ประกอบการตรวจสอบ	
	2.1 ตรวจสอบสภาพแวดล้อมทั่วไปภายในและภายนอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง ตลอดจนรวมถึงการจัดวางอุปกรณ์คอมพิวเตอร์ต่าง ๆ ให้คำนึงถึงความปลอดภัยในระดับมาตรฐานที่ยอมรับได้โดยทั่วไป	สถาบันการเงินที่ไม่มีระเบียบและวิธีการปฏิบัติหรือขาดการควบคุมดูแลในการรักษาความปลอดภัยด้านกายภาพ อาจส่งผลให้การปฏิบัติงานของเจ้าหน้าที่ในองค์กรขาดประสิทธิภาพ กระทบต่อความเสี่ยงในด้านการบริหารงานและการปฏิบัติงานเทคโนโลยีสารสนเทศ ทำให้สถาบันการเงินนั้นขาดความน่าเชื่อถือกระทบต่อชื่อเสียงของสถาบันการเงินได้

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	2.2 ให้มีระบบการติดตามดูแลการปฏิบัติงานภายในอาคารสถานที่พร้อมทั้งมีระบบเตือนภัยต่าง ๆ บริเวณที่มีความเสี่ยงสูง เช่น จัดให้มีการติดตั้งทีวีวงจรปิดและต้องมีสื่อเพื่อบันทึกรายละเอียดที่เกิดขึ้น เป็นต้น	
	2.3 กำหนดระเบียบและวิธีปฏิบัติในการเข้า – ออกเกี่ยวกับผู้ปฏิบัติงาน ผู้มาติดต่อทั้งจากบุคคลภายในและบุคคล ภายนอก ตลอดจนเครื่องมือเครื่องใช้ต่าง ๆ ที่เกี่ยวข้อง รวมทั้ง จัดให้มีการควบคุมการปฏิบัติดังกล่าวอย่างเคร่งครัด	
	2.4 จัดให้มีสถานที่เก็บสื่อบันทึกข้อมูลต่าง ๆ และระบบควบคุมการเก็บสื่อบันทึกข้อมูลต่าง ๆ อย่างเพียงพอ ปลอดภัย พร้อมทั้ง ติดตามดูแลปรับปรุงให้เป็นปัจจุบันเสมอ	
	2.5 สถาบันการเงินควรควบคุมดูแลการนำโปรแกรมที่ไม่ได้รับอนุญาตหรือโปรแกรมที่ละเมิดลิขสิทธิ์มาลงในระบบงาน	
3. การรักษาความปลอดภัยด้านตรรกะ (Logical security)	การรักษาความปลอดภัยด้านตรรกะให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล (Information Security)** ประกอบการตรวจสอบ	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	3.1 กำหนดให้มีระบบการควบคุมการนำข้อมูลเข้าและการแสดงผลจากเครื่องคอมพิวเตอร์ ตลอดจนกระบวนการพิสูจน์ถึงความถูกต้องของข้อมูลต่าง ๆ ที่ถูกบันทึกไว้ในระบบคอมพิวเตอร์	สถาบันการเงินที่ไม่มีระเบียบและวิธีการปฏิบัติหรือขาดการควบคุมดูแลในการรักษาความปลอดภัยด้านการเข้าใช้ระบบงานและข้อมูลที่ชัดเจนอาจทำให้การนำข้อมูลเข้า การนำข้อมูลออก รวมถึงการกำหนดสิทธิของเจ้าหน้าที่ผู้รับผิดชอบระบบงานต่าง ๆ ดำเนินการไปโดยขาดประสิทธิภาพ ก่อให้เกิดความเสียหายต่อองค์กรส่งผลกระทบต่อความเสี่ยงด้านการบริหารงานและการปฏิบัติงานเทคโนโลยีสารสนเทศของสถาบันการเงิน
	3.2 กำหนดสิทธิในการเข้าถึงระบบหรือข้อมูลควรมีการแบ่งแยกหน้าที่ตามความเหมาะสมกับประเภทของงานและความรับผิดชอบ	
	3.3 ควรกำหนดให้มีกระบวนการในการทบทวนและปรับปรุงสิทธิในการเข้าใช้ระบบงานต่าง ๆ ให้เป็นปัจจุบัน และการเปลี่ยนแปลงสิทธิจะต้องได้รับอนุมัติจากผู้บริหารระดับสูง	
	3.4 ในกรณีที่องค์กรมีระบบสื่อสารระยะไกล (Remote Access) ควรจัดให้มีมาตรการรักษาความปลอดภัยในระหว่างการรับ – ส่งข้อมูล เช่น การเข้ารหัส (Encryption) เป็นต้น	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	3.5 สถาบันการเงินควรกำหนดให้มีมาตรการและกระบวนการป้องกัน ตรวจจับ และแก้ไขภัยคุกคามต่าง ๆ เช่น การถูกโจมตีโดยไวรัส หรือการบุกรุกจากผู้ประสงค์ร้ายกับระบบของสถาบันการเงิน พร้อมทั้งมีระบบการรายงานพฤติกรรมที่ผิดปกติหรือน่าสงสัยให้ผู้บริหารทราบอย่างรวดเร็วและทันเหตุการณ์	
	3.6 สถาบันการเงินควรเลือกใช้เทคนิคการเข้ารหัสการรับ – ส่งข้อมูลทั้งภายในและภายนอกองค์กรให้ เหมาะสมกับธุรกรรมและความเสี่ยงของสถาบันการเงิน	
	3.7 สถาบันการเงินควรกำหนดมาตรการในการเก็บรักษาข้อมูลส่วนบุคคล โดยคำนึงถึงสิทธิหน้าที่ความรับผิดชอบตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล	
	3.8 สถาบันการเงินควรกำหนดวิธีการพิสูจน์ตัวตนที่เหมาะสมกับความเสี่ยงของธุรกรรม เช่น การใช้ User ID และ Password หรือการใช้ Two-Factor Password หรือ Biometric Devices เป็นต้น	
	3.9 สถาบันการเงินควรจัดให้มีการบันทึกประวัติการทำรายการในระบบสารสนเทศที่สำคัญ และมีการสำรองข้อมูลดังกล่าวอย่างครบถ้วนเพียงพอ เช่น Transaction Logs, Security Log และ System Log เป็นต้น เพื่อให้สามารถสืบค้นย้อนหลังและสามารถระบุตัวตนของผู้ทำรายการได้	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
4. ด้านระบบเครือข่ายสื่อสาร	ระบบเครือข่ายสื่อสารให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก **คู่มือตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล (Information Security)** ประกอบการตรวจสอบ	
	4.1 ให้ประเมินความเพียงพอของระบบรักษาความปลอดภัยบนเครือข่ายพร้อมทั้งจัดให้มีการทดสอบเพื่อการประเมินประสิทธิภาพของระบบรักษาความปลอดภัยบนเครือข่ายของสถาบันการเงินโดยพิจารณาให้เหมาะสมกับระดับความเสี่ยงของการให้บริการ และปรับปรุงให้ทันสมัย พร้อมทั้งจัดให้มีการสอบทานรายงานต่าง ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยบนระบบเครือข่ายสื่อสาร	สถาบันการเงินที่ไม่มีระเบียบและวิธีการปฏิบัติหรือขาดการควบคุมดูแลในการรักษาความปลอดภัยด้านระบบเครือข่ายสื่อสารที่ชัดเจน อาจทำให้บุคคลภายในและภายนอกสามารถเข้ามาเจาะระบบเครือข่ายสื่อสารขององค์กรและนำข้อมูลต่าง ๆ ไปใช้ในทางที่ผิดวัตถุประสงค์ส่งผลกระทบต่อความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศและชื่อเสียงขององค์กรได้
	4.2 สถาบันการเงินควรจัดให้มีระบบการตรวจจับการบุกรุกระบบเครือข่ายภายในและภายนอกให้เหมาะสมกับความเสี่ยงของสถาบันการเงินนั้น ๆ และสามารถแก้ไขปัญหาให้ทันต่อเหตุการณ์	
	4.3 สถาบันการเงินควรจัดให้มีการบันทึกประวัติการเข้าใช้งานระบบเครือข่ายที่สำคัญ และมีการสำรองข้อมูลดังกล่าวอย่างครบถ้วนเพียงพอ เช่น Firewall Log, Router Log และ IDS Log เป็นต้น เพื่อให้สามารถสืบค้นย้อนหลังและสามารถระบุตัวตนของผู้เข้าใช้งานเครือข่ายได้	

ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)		
แนวทางการพิจารณาความเสี่ยง	**การประเมินความเสี่ยง**	**ผลกระทบจากความเสี่ยง**
1. การบริหารโครงการพัฒนาระบบงานและโปรแกรม (Project Management)	การบริหารโครงการพัฒนาระบบงานและโปรแกรมให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการพัฒนาและการจัดหาระบบงานและโปรแกรม (Development Acquisition)** ประกอบการตรวจสอบ	
	1.1 การดำเนินงานและการบริหารงบประมาณโครงการของสถาบันการเงินควรสอดคล้องกับแผนกลยุทธ์เป้าหมายในการดำเนินธุรกิจ และทิศทางของภาคธุรกิจการเงิน รวมทั้งกฎระเบียบของทางการ	สถาบันการเงินที่มีการบริหารโครงการอย่างไม่มีประสิทธิภาพจะทำให้สถาบันการเงินใช้ทรัพยากรอย่างไม่คุ้มค่า โครงการไม่สามารถประสบผลสำเร็จหรือไม่สามารถสนับสนุนแผนกลยุทธ์ของสถาบันการเงินได้ ย่อมกระทบต่อความสามารถในการหารายได้และลดความสามารถในการแข่งขันลงไปกระทบต่อความเสี่ยงด้านกลยุทธ์และชื่อเสียงของสถาบันการเงิน
	1.2 สถาบันการเงินควรมีความเพียงพอหรือความพร้อมของระเบียบและขั้นตอนหรือเงื่อนไขต่าง ๆ ในการพิจารณาคัดเลือกโครงการใหม่ ๆ กระบวนการวิเคราะห์ความคืบหน้า / อุปสรรคของการดำเนินการเพื่อให้สถาบันการเงินรวบรวมข้อมูลได้อย่างรวดเร็ว และทันสมัย	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบจากความเสี่ยง
2. การพัฒนาระบบงานและโปรแกรม รวมทั้งการจัดซื้อระบบงาน (SDLC & Acquisition)	การพัฒนาระบบงานและโปรแกรมให้ ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการพัฒนาและการจัดหาระบบงานและโปรแกรม (Development Acquisition)** ประกอบการตรวจสอบ	
	2.1 การพัฒนาระบบงานของสถาบันการเงินควรมีความสอดคล้องและสัมพันธ์กับโครงสร้างของระบบงานเทคโนโลยีสารสนเทศพื้นฐาน อันประกอบไปด้วย เครือข่ายการสื่อสาร / เครื่องคอมพิวเตอร์ที่ใช้ / ระบบฐานข้อมูล และการเชื่อมโยงหรือส่งผ่านข้อมูลระหว่างกัน	การพัฒนาระบบงานและการเปลี่ยนแปลงระบบงานที่ขาดกระบวนการบริหารความเสี่ยงอย่างครอบคลุมทั่วถึงทั้งองค์กรอาจส่งผลกระทบต่อความถูกต้อง ความลับและความพร้อมใช้งานของข้อมูล ส่งผลกระทบต่อความเสี่ยงด้านการปฏิบัติงาน ด้านการปฏิบัติตามกฎหมาย และชื่อเสียงของสถาบันการเงิน
	2.2 สถาบันการเงินควรมีระเบียบวิธีปฏิบัติในการพิจารณาทางเลือกระหว่างการพัฒนาระบบงานเองภายใน หรือการจัดซื้อจัดหาระบบงานจากภายนอก	
	2.3 สถาบันการเงินควรมีระเบียบวิธีปฏิบัติและขั้นตอนในการควบคุมการพัฒนาระบบงาน (Systems Development Life Cycle) ซึ่งประกอบด้วยการคัดเลือกโครงการ การดำเนินงาน การ Implement การจัดทำเอกสาร คู่มือและการอบรมการใช้งานให้แก่พนักงาน	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	2.4 ระบบงานที่จะนำมาใช้งาน หรือที่ได้รับการปรับปรุงแก้ไขแล้ว ควรต้องผ่านการทดสอบประสิทธิภาพความถูกต้องและความปลอดภัยในการใช้งานอย่างเพียงพอจากหน่วยงานที่ทำหน้าที่ตรวจสอบคุณภาพระบบงานและโปรแกรม (Quality Assurance) แล้ว และต้องผ่านการอนุมัติจากผู้บริหารของสถาบันการเงิน	
	2.5 สถาบันการเงินควรมีการประเมินความเสี่ยงการควบคุมระบบรักษาความปลอดภัยของระบบงานที่พัฒนาใหม่ ซึ่งให้บริการบนเครือข่ายอินเตอร์เน็ตทั้งในขั้นตอนก่อนการพัฒนา และทบทวนหลังจากที่นำระบบงานมาใช้จริงแล้วเป็นระยะ ๆ	
3. การบำรุงรักษาระบบงานและการบริหารการเปลี่ยนแปลง (System Maintenance & Change Control)	การบำรุงรักษาระบบงานและการบริหารการเปลี่ยนแปลงให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก **คู่มือตรวจสอบการพัฒนาและการจัดหาระบบงานและโปรแกรม (Development Acquisition)** ประกอบการตรวจสอบ	
	3.1 สถาบันการเงินควรมีขั้นตอนปฏิบัติงานด้านการบำรุงรักษาระบบงานและโปรแกรม การขออนุมัติการเปลี่ยนแปลงระบบงานภายหลังจากที่ระบบงานได้ถูกนำไปใช้งานจริง ซึ่งรวมไปถึงระบบงานที่จัดซื้อจากภายนอกด้วย	การขาดกระบวนการบำรุงรักษาระบบงานและการดูแลการเปลี่ยนแปลงที่เพียงพออาจทำให้ระบบงานมีความล้าสมัย ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ หรือไม่สามารถทำงานได้อย่างต่อเนื่อง ทำให้เกิดความเสี่ยงด้านการปฏิบัติงาน ส่งผลกระทบต่อชื่อเสียงของสถาบันการเงิน

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	3.2 การจัดทำเอกสารประกอบระบบงาน การจัดทำสำเนาระบบงานและโปรแกรมของสถาบันการเงินควรมีความเหมาะสมและมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เมื่อมีการเปลี่ยนแปลงระบบงานและโปรแกรมเกิดขึ้นทุกครั้ง รวมทั้งควรจัดให้มีการเก็บสำเนาของระบบงานที่จำเป็นต้องใช้ไว้ที่ศูนย์ประมวลผลสำรองอย่างครบถ้วนและติดตามการปรับเปลี่ยนโปรแกรมระบบงานที่มีในศูนย์ประมวลผลสำรองให้เป็นรุ่นเดียวกัน (Same Version) กับระบบงานที่ใช้จริงในปัจจุบัน	
4. การบริหารการใช้บริการจากหน่วยงานภายนอก (Management of Outsourcing)	การบริหารการใช้บริการจากหน่วยงานภายนอกให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการให้บริการด้านเทคโนโลยีจากบุคคลภายนอก (Outsourcing Technology Services)** ประกอบการตรวจสอบ	
	4.1 นโยบายการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกควรมีการประเมินอย่างน้อยปีละครั้งเพื่อให้สอดคล้องกับแผนกลยุทธ์และเป้าหมายของสถาบันการเงิน	สถาบันการเงินที่กระบวนการบริหารติดตามดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศโดยบุคคลภายนอกไม่มีประสิทธิภาพและขาดความต่อเนื่องแล้วอาจทำให้สถาบันการเงินประสบปัญหาการปฏิบัติงานของผู้ให้บริการไม่มีประสิทธิภาพก่อให้เกิดความเสี่ยงทั้ง 5 ด้าน (กลยุทธ์ เครดิต ตลาด สภาพคล่องและปฏิบัติการ) รวมถึงความเสี่ยงด้านชื่อเสียงและการปฏิบัติตามกฎหมาย ซึ่งขึ้นอยู่กับประเภทของการใช้บริการ

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	4.2 สถาบันการเงินควรมีกระบวนการในการประเมินและหลักเกณฑ์ในการคัดเลือกผู้ให้บริการที่ชัดเจน รวมถึงกระบวนการตรวจสอบความพร้อมและความเหมาะสมของผู้ให้บริการจากภายนอก	
	4.3 สัญญาในการว่าจ้างการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากบุคคลอื่นต้องมีการจัดทำเป็นลายลักษณ์อักษร ซึ่งควรต้องครอบคลุมไปถึงการรับจ้างช่วง (Subcontract) ของผู้ให้บริการด้วย นอกจากนี้ สัญญาควรมีความเหมาะสมเพียงพอและยืดหยุ่นสามารถปรับเปลี่ยนได้ตามสถานการณ์	
	4.4 สถาบันการเงินควรให้ผู้ให้บริการจัดทำแผนสำรองฉุกเฉินให้สอดคล้องกับแผนสำรองฉุกเฉินของสถาบันการเงิน	
	4.5 สัญญาว่าจ้างการใช้บริการด้านงานเทคโนโลยีสารสนเทศของสถาบันการเงินควรกำหนดอำนาจหน้าที่ของผู้ตรวจสอบภายในและภายนอกของสถาบันการเงิน รวมทั้งหน่วยงานภาครัฐที่เกี่ยวข้องให้สามารถเข้าตรวจสอบการดำเนินงาน การควบคุมภายในและการรักษาความปลอดภัยของผู้ให้บริการ และผู้รับจ้างช่วงได้ รวมทั้งต้องมีการรักษาความปลอดภัยของข้อมูลและความเป็นส่วนตัวของข้อมูลลูกค้า	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	4.6 สถาบันการเงินควรจัดการติดตาม ดูแล ประสานงาน ประเมินผลและตรวจสอบการให้บริการของผู้ให้บริการและผู้รับจ้างช่วงอย่างสม่ำเสมอ และจัดทำรายงานการติดตามเสนอฝ่ายบริหารให้ทราบเป็นระยะ ๆ	
ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ **ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability)**		
แนวทางการพิจารณาความเสี่ยง	**การประเมินความเสี่ยง**	**ผลกระทบต่อความเสี่ยง**
1. แผนการเตรียมความพร้อมสำหรับเหตุการณ์ฉุกเฉินและภัยพิบัติ	การเตรียมความพร้อมสำหรับเหตุการณ์ฉุกเฉินและภัยพิบัติให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning)** ประกอบการตรวจสอบ	
	1.1 แผนสำรองฉุกเฉินควรมีความครอบคลุมทุกกิจกรรม หรือบริการที่สำคัญของสถาบันการเงิน ทั้งที่อยู่ภายใต้และนอกเหนือความรับผิดชอบของสายงานเทคโนโลยีสารสนเทศ	แผนสำรองฉุกเฉินของสถาบันการเงินที่ไม่ครอบคลุมทุกระบบงานสำคัญ หรือไม่ระบุขั้นตอนการปฏิบัติที่จำเป็นให้เพียงพอที่จะปฏิบัติตามได้ หรือแผนไม่สอดคล้องกับแนวทางปฏิบัติโดยรวมของสถาบันการเงิน และสูญเสียโอกาสการสร้างรายได้ อาจทำให้สถาบันการเงินไม่สามารถดำเนินธุรกิจได้อย่างต่อเนื่องและราบรื่นเกิดความล่าช้าในการดำเนินงาน ทำให้กระทบต่อชื่อเสียงของสถาบันการเงินอาจก่อให้เกิดความเสี่ยงด้านการปฏิบัติงาน ความน่าเชื่อถือและการยอมรับจากลูกค้าลดน้อยลง

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	1.2 สถาบันการเงินควรจัดลำดับความสำคัญของเหตุการณ์ฉุกเฉิน ขั้นตอนการดำเนินงาน ระบุมอบหมายหน้าที่ให้กับทีมบุคลากรหลักเพื่อปฏิบัติงานภายใต้สภาวะฉุกเฉินอย่างชัดเจน และวิธีการติดต่อบุคคลหรือองค์กรที่จำเป็นต่อการกู้สถานการณ์เป็นลายลักษณ์อักษรในแผนฯ รวมทั้งประเด็นความพร้อมของ Hardware, Software, อุปกรณ์ และบุคลากรที่จะปฏิบัติงานภายใต้สภาวะฉุกเฉิน	
	1.3 สถาบันการเงินควรมีกระบวนการทบทวนปรับปรุงแผนฯ อย่างสม่ำเสมอ เพื่อให้แผนฯ มีความสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป	
	1.4 การบริหารเหตุการณ์ฉุกเฉินของสถาบันการเงินควรกำหนดแผนงานและระเบียบให้มีความครอบคลุมในเรื่องขั้นตอนการปฏิบัติงานฉุกเฉินและแผนการโยกย้าย การโต้ตอบต่อการบุกรุกหรือการเจาะระบบเครือข่าย การรายงานที่ต้องเสนอผู้บริหารเพื่อการควบคุมเป็นการเฉพาะหรือเสนอต่อหน่วยงานของราชการ และการกู้ระบบ (Recovery)	
	1.5 แผนสำรองฉุกเฉินของสถาบันการเงินควรมีความสอดคล้องกับแผนสำรองฉุกเฉินของบริษัทผู้ให้บริการ	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	1.6 สถาบันการเงินควรจัดทำคู่มือปฏิบัติงานด้วย Manual และฝึกซ้อมให้พนักงานสามารถปฏิบัติงานในสภาวะฉุกเฉินได้	
2. การทดสอบแผนสำรองฉุกเฉินและการรายงานผลต่อระดับบริหาร	การทดสอบแผนสำรองฉุกเฉินให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning)** ประกอบการตรวจสอบ	
	2.1 สถาบันการเงินควรจัดทำแผนการทดสอบประจำปี และปฏิบัติตามแผนการทดสอบดังกล่าวอย่างเคร่งครัด รวมทั้งรายงานผลการทดสอบให้ผู้บริหารทราบ	สถาบันการเงินที่ไม่มีการวางแผน การทดสอบแผนสำรองฉุกเฉินที่ดีอาจทำให้สถาบันการเงินไม่สามารถประเมินปัญหาหรือข้อบกพร่องของแผนสำรองฉุกเฉินได้อย่างมีประสิทธิภาพซึ่งหากเกิดเหตุการณ์ฉุกเฉินขึ้นจะก่อให้เกิดความเสี่ยงที่พนักงานไม่สามารถปฏิบัติตามแผนสำรองฉุกเฉินได้ ทำให้เกิดความเสี่ยงด้านการปฏิบัติงานและกระทบต่อชื่อเสียงของสถาบันการเงิน
	2.2 การทดสอบแผนสำรองฉุกเฉินควรพิจารณาประเด็น ดังต่อไปนี้ (1) ทดสอบระบบงานอย่างน้อยปีละครั้ง (2) กำหนดขอบเขตของการทดสอบให้ครอบคลุมทุกระบบงานที่มีนัยสำคัญต่อการดำเนินธุรกิจ (3) จัดลำดับความสำคัญ (Priority) ของการกู้ระบบ (Recovery) ตามความสำคัญของระบบงาน	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	2.3 สถาบันการเงินควรมีกระบวนการติดตามการทดสอบแผนสำรองฉุกเฉินของบริษัทผู้ให้บริการภายนอก	
3. การจัดการศูนย์สำรอง การสำรองข้อมูลและโปรแกรมระบบงาน	การจัดการศูนย์สำรอง การสำรองข้อมูลและโปรแกรมระบบงานให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning)** ประกอบการตรวจสอบ	
	3.1 ศูนย์สำรองของสถาบันการเงินควรมีระยะห่างพอสมควรจากศูนย์คอมพิวเตอร์หลัก	สถาบันการเงินที่มีการสำรองข้อมูลและโปรแกรมระบบงานบกพร่อง ขาดความน่าเชื่อถืออาจส่งผลกระทบทำให้ธนาคารไม่สามารถดำเนินธุรกิจในสภาวะฉุกเฉินได้อย่างต่อเนื่อง เกิดความล่าช้าในการให้บริการแก่ลูกค้าก่อให้เกิดความเสี่ยงด้านการปฏิบัติงานและชื่อเสียงของสถาบันการเงิน
	3.2 ศูนย์สำรองควรมีระบบการควบคุมภายในและการรักษาความปลอดภัยที่รัดกุมเพียงพอ	
	3.3 สถาบันการเงินควรกำหนดระเบียบวิธีปฏิบัติเกี่ยวกับการสำรองข้อมูลและโปรแกรมระบบงานให้มีความครอบคลุม ปลอดภัย และถูกต้อง	
	3.4 สถาบันการเงินควรติดตามดูแลแฟ้มข้อมูลและระบบงานที่เก็บรักษาที่ศูนย์ประมวลผลสำรองให้มีความสมบูรณ์ครบถ้วนถูกต้อง และทันสมัยอยู่เสมอ และรายงานผลให้ผู้บริหารทราบ	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	3.5 การสำรองข้อมูลและโปรแกรมระบบงานโดยบริษัทภายนอก สถาบันการเงินควรมีการจัดทำสัญญาหรือข้อตกลงไว้อย่างชัดเจน และมีกระบวนการติดตามและตรวจสอบผลการดำเนินงานของบริษัทภายนอกอย่างต่อเนื่อง	
	3.6 ในกรณีที่บริษัทผู้ให้บริการภายนอกอยู่ที่ต่างประเทศ สถาบันการเงินควรจัดให้มีการสำรองข้อมูลหรือระบบคอมพิวเตอร์ในประเทศไทยอย่างเพียงพอ เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่องโดยไม่หยุดชะงัก	
4. การบำรุงรักษาและการประกันภัยอุปกรณ์คอมพิวเตอร์ และระบบงาน	การบำรุงรักษาและการประกันภัยอุปกรณ์คอมพิวเตอร์ และระบบงานให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการพัฒนาและการจัดหาระบบงานและโปรแกรม (Development Acquisition)** ประกอบการตรวจสอบ	
	4.1 สถาบันการเงินจัดให้มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และระบบงานอย่างสม่ำเสมอ	สถาบันการเงินที่มีการบำรุงรักษาและการประกันภัยอุปกรณ์คอมพิวเตอร์ ระบบงานบกพร่องขาดความต่อเนื่องอาจส่งผลให้อุปกรณ์ล้าสมัยหรือเสียหายง่าย ทำให้การปฏิบัติงานหยุดชะงักก่อให้เกิดความเสี่ยงด้านการปฏิบัติงานและชื่อเสียงของสถาบันการเงิน
	4.2 สถาบันการเงินควรจัดทำประกันภัยอุปกรณ์คอมพิวเตอร์ ระบบงาน และสิ่งอำนวยความสะดวกต่าง ๆ อย่างเพียงพอ และกำหนดขั้นตอนในการติดตามและการต่ออายุประกันภัย	

ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ ความเสี่ยงด้านชื่อเสียง (Reputation)		
แนวทางการพิจารณาความเสี่ยง	**การประเมินความเสี่ยง**	**ผลกระทบต่อความเสี่ยง**
1. การรักษาความลับและความเป็นส่วนตัวของลูกค้า (Privacy)	การรักษาความลับและความเป็นส่วนตัวของลูกค้า (Privacy) ให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล (Information Security)** ประกอบการตรวจสอบ	
	1.1 สถาบันการเงินควรมีการพิจารณาอย่างรอบคอบในการนำเทคโนโลยีสารสนเทศมาใช้กับผลิตภัณฑ์หรือช่องทางการให้บริการใหม่ๆ โดยควรคำนึงถึงความปลอดภัยของข้อมูลที่สำคัญ เช่น ข้อมูลส่วนตัวลูกค้า ข้อมูลประวัติการทำรายการของลูกค้า และข้อมูลทางการเงินต่างๆ	ความเสี่ยงด้านชื่อเสียงเป็นความเสี่ยงที่เกิดขึ้นจากการที่สถาบันการเงินไม่สามารถรักษาความปลอดภัยด้านต่าง ๆ ที่กล่าวมาข้างต้น จึงเกิดการหยุดชะงักล่าช้าหรือเกิดการทุจริต ต่าง ๆ ขึ้น และในที่สุดก็มีผลกระทบต่อความน่าเชื่อถือของระบบเทคโนโลยี ระบบการควบคุมภายในและความมั่นคงของสถาบันการเงิน
	1.2 สถาบันการเงินควรมีการปกป้องและควบคุมการเข้าถึงข้อมูลส่วนตัวของลูกค้าและข้อมูลประวัติการทำรายการของลูกค้าอย่างปลอดภัยและเหมาะสม โดยคำนึงถึงความเป็นส่วนตัวของลูกค้า	
	1.3 สถาบันการเงินควรมีการแบ่งแยกประเภทของข้อมูลตามระดับความสำคัญและตามความลับของข้อมูล (Data Classification) เพื่อให้มีการควบคุมการเข้าถึงข้อมูลในแต่ละประเภทอย่างเหมาะสม	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	1.4 สถาบันการเงินควรมีการจัดทำแผนการรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) แผนการกู้ระบบกลับคืน (Disaster Recovery Plan) แผนสำรองฉุกเฉิน (Contingency Plan) และแผนรองรับเหตุการณ์ที่ไม่คาดว่าจะเกิดขึ้น (Incident Response Plan) รวมทั้งมีการทดสอบการปฏิบัติตามแผนต่างๆอย่างสม่ำเสมอ และมีการปรับปรุงแผนให้มีสอดคล้องกับสภาวการณ์ และเทคโนโลยีที่เปลี่ยนแปลงไปอย่างสม่ำเสมอ	
ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ **ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Regulation)**		
แนวทางการพิจารณาความเสี่ยง	**การประเมินความเสี่ยง**	**ผลกระทบต่อความเสี่ยง**
1. การควบคุมและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้เป็นไปตามกฎหมายและกฎระเบียบของหน่วยงานราชการต่าง ๆ	การควบคุมและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้เป็นไปตามกฎหมายและกฎระเบียบของหน่วยงานราชการต่าง ๆให้ผู้ตรวจสอบดูหลักเกณฑ์และวิธีการตรวจสอบจาก**คู่มือตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล (Information Security)** ประกอบการตรวจสอบ	
	1.1 สถาบันการเงินควรมีการติดตามการเปลี่ยนแปลงของกฎหมายและกฎระเบียบที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และนำมาปรับปรุงในคู่มือการตรวจสอบอย่างสม่ำเสมอ	

แนวทางการพิจารณาความเสี่ยง	การประเมินความเสี่ยง	ผลกระทบต่อความเสี่ยง
	1.2 สถาบันการเงินควรมีการควบคุมและกำกับดูแลให้มีการปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่เป็นไปตามกฎหมายและกฎระเบียบของหน่วยงานราชการต่างๆที่เกี่ยวข้องอย่างสม่ำเสมอ	

การจัดอันดับผลการดำเนินงานด้านเทคโนโลยีสารสนเทศ

การจัดอันดับผลการดำเนินงานด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยง ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศจะพิจารณาจากข้อสังเกตการตรวจสอบด้านการบริหารงานเทคโนโลยีสารสนเทศและด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ เพื่อกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแต่ละด้าน (IT Risk Rating) ซึ่งระดับความเสี่ยงในแต่ละด้านจะนำมาประเมินผลการจัดอันดับความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยรวม (IT Aggregate Risk Rating) ของสถาบันการเงินต่อไป

ในการประเมินความเสี่ยงแต่ละด้าน ผู้ตรวจสอบจะต้องระบุระดับความเสี่ยง คุณภาพการบริหารความเสี่ยง และแนวโน้มระดับความเสี่ยงโดยนำระดับความเสี่ยงและคุณภาพการบริหารความเสี่ยงมาประกอบการพิจารณาจัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังตาราง

การจัดระดับความเสี่ยงรวมด้านเทคโนโลยีสารสนเทศ (IT Aggregate Risk Rating)

		ระดับความเสี่ยง		
		ต่ำ	ปานกลาง	สูง
คุณภาพการบริหารความเสี่ยง	อ่อน	ปานกลาง	ค่อนข้างสูง	สูง
	พอใช้	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง
	ดี	ต่ำ	ค่อนข้างต่ำ	ปานกลาง

การจัดอันดับผลการดำเนินงานด้านเทคโนโลยีสารสนเทศโดยรวม (IT Aggregate Risk Rating) จะพิจารณาจากผลการจัดระดับความเสี่ยงแต่ละด้าน ทั้งนี้ความเสี่ยงที่มีผลกระทบต่อเสถียรภาพและความมั่นคงในการดำเนินงาน ชื่อเสียง การปฏิบัติตามกฎหมายของสถาบันการเงินก็ควรจะให้น้ำหนักมากเป็นพิเศษ จากนั้นจึงจัดอันดับผลการดำเนินงานด้านเทคโนโลยีสารสนเทศโดยรวม ซึ่งมีทั้งหมด 5 ระดับ คือ ดี ค่อนข้างดี พอใช้ ค่อนข้างอ่อน อ่อน

แนวทางในการพิจารณาจัดอันดับผลการดำเนินงานด้านเทคโนโลยีสารสนเทศ

1. การจัดอันดับความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ

ระดับความเสี่ยง

ต่ำ

การเปลี่ยนแปลงโครงสร้างองค์กรหรือโครงสร้างทางด้านเทคโนโลยีสารสนเทศหลังการตรวจสอบครั้งก่อนมีผลกระทบต่อองค์กรเพียงเล็กน้อย

การวางแผนกลยุทธ์และการดำเนินงานด้านเทคโนโลยีสารสนเทศมีความชัดเจน มีระบบการจัดการ ระบบการบริหารความเสี่ยงและแผนการดำเนินงานที่ดีและมีประสิทธิภาพ เป้าหมายกลยุทธ์มีความชัดเจนและสอดคล้องกับทิศทางการดำเนินธุรกิจและสภาพแวดล้อมที่เปลี่ยนแปลงไป มีการสื่อสารทั่วทั้งองค์กรและนำไปปฏิบัติอย่างมีประสิทธิภาพและสม่ำเสมอ

การตัดสินใจทางด้านเทคโนโลยีสารสนเทศมีผลกระทบต่อฐานะการดำเนินงานและชื่อเสียงของสถาบันการเงินเพียงเล็กน้อย

ปานกลาง

การเปลี่ยนแปลงโครงสร้างองค์กรหรือโครงสร้างทางด้านเทคโนโลยีสารสนเทศหลังการตรวจสอบครั้งก่อนมีผลกระทบต่อองค์กรไม่มากนักและสามารถแก้ไขได้ในระยะเวลาอันสั้น

การวางแผนกลยุทธ์และการดำเนินงานด้านเทคโนโลยีสารสนเทศ มีระบบการจัดการ ระบบการบริหารความเสี่ยงและแผนการดำเนินงานที่เพียงพอและสอดคล้องกับทิศทางการดำเนินธุรกิจและสภาพแวดล้อมที่เปลี่ยนแปลงไป มีการสื่อสารอย่างเหมาะสมและนำไปปฏิบัติอย่างมีประสิทธิผลทั้งองค์กร การตัดสินใจทางด้านเทคโนโลยีสารสนเทศมีผลกระทบต่อฐานะการดำเนินงานและชื่อเสียงที่ไม่ได้ก่อให้เกิดความเสียหายต่อสถาบันการเงินอย่างมีนัยสำคัญ

สูง

การเปลี่ยนแปลงโครงสร้างองค์กรหรือโครงสร้างทางด้านเทคโนโลยีสารสนเทศหลังการตรวจสอบครั้งก่อนมีผลกระทบต่อองค์กรอย่างมีนัยสำคัญ

การวางแผนกลยุทธ์และการดำเนินงานด้านเทคโนโลยีสารสนเทศ ไม่มีระบบการจัดการ ระบบการบริหารความเสี่ยงและแผนการดำเนินงานที่มีความชัดเจนเพียงพอ เนื่องจากการขยายตัวหรือการลงทุนทางด้านเทคโนโลยีสารสนเทศที่เร็วเกินไป สะท้อนถึงเป้าหมายกลยุทธ์ในเชิงรุกมากเกินไปไม่สอดคล้องกับทิศทางการดำเนินธุรกิจและไม่สามารถตอบสนองต่อสภาพแวดล้อมที่เปลี่ยนแปลงไป ไม่มีการสื่อสารอย่างชัดเจนทั่วทั้งองค์กร และไม่ได้นำไปปฏิบัติหรือนำไปปฏิบัติแต่ไม่มีประสิทธิผล

การตัดสินใจทางด้านเทคโนโลยีสารสนเทศคาดว่าจะเกิดผลกระทบในทางลบก่อให้เกิดความเสียหายต่อสถาบันการเงินสูง

<u>การจัดการความเสี่ยง</u>

ดี

สถาบันการเงินมีการวางแผนกลยุทธ์ นโยบายและแผนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศได้สอดคล้องกับกลยุทธ์การดำเนินงานขององค์กรและสะท้อนให้เห็นถึงจุดแข็ง จุดอ่อน โอกาสและอุปสรรคในการดำเนินงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

เป็นอย่างดี และมีการติดตามดูแลการดำเนินงานอย่างใกล้ชิดทั่วถึง

การบริหารงานด้านเทคโนโลยีสารสนเทศตามหลักธรรมาภิบาลเป็นไปอย่างมีประสิทธิภาพและมีความโปร่งใสในการเปิดเผยข้อมูล สถาบันการเงินมีนโยบายและขั้นตอนการปฏิบัติสำหรับธุรกรรมด้านเทคโนโลยีสารสนเทศที่ชัดเจน เพื่อป้องกันปัญหาการขัดแย้งด้านผลประโยชน์ (Conflict of Interest) อย่างมีประสิทธิผล

คณะกรรมการหรือคณะทำงานด้านเทคโนโลยีสารสนเทศ มีคุณสมบัติครบถ้วนและมีประสบการณ์ที่หลากหลายเข้าร่วมประชุมอย่างสม่ำเสมอ ปฏิบัติหน้าที่อย่างอิสระและติดตามแก้ไขปัญหาอย่างต่อเนื่องและรวดเร็วทันเหตุการณ์

ฝ่ายบริหารด้านเทคโนโลยีสารสนเทศมีความสามารถในการพัฒนาทิศทางกลยุทธ์และเพิ่มประสิทธิภาพในการปฏิบัติตามกลยุทธ์และในการดำเนินงานขององค์กรให้ประสบความสำเร็จตามเป้าหมายที่วางไว้ ฝ่ายตรวจสอบภายในด้านเทคโนโลยีสารสนเทศสามารถตรวจสอบได้ครอบคลุมทุกจุดที่มีความเสี่ยงและมีความเป็นอิสระอย่างแท้จริง

ระบบสารสนเทศเพื่อการบริหารขององค์กรสามารถสนับสนุนแนวทางและการดำเนินงานตามกลยุทธ์ได้อย่างมีประสิทธิภาพ นโยบายและการจัดการแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง สามารถครอบคลุมและรองรับการดำเนินงานขององค์กรได้ทั้งหมด รวมทั้งมีการสื่อสารให้พนักงานได้รับทราบอย่างทั่วถึงทั้งองค์กร

พอใช้

สถาบันการเงินมีการวางแผนกลยุทธ์ นโยบายและแผนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศได้สอดคล้องกับกลยุทธ์การดำเนินงานขององค์กรและสะท้อนให้เห็นถึงจุดแข็ง จุดอ่อน โอกาสและอุปสรรคในการดำเนินงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงินได้อย่างเพียงพอและมีการติดตามดูแลการดำเนินงานอย่างใกล้ชิดพอสมควร

การบริหารงานด้านเทคโนโลยีสารสนเทศตามหลักธรรมาภิบาลมีเพียงพอและมีความโปร่งใสในการเปิดเผยข้อมูล สถาบันการเงินมีนโยบายและขั้นตอนการปฏิบัติสำหรับธุรกรรมด้านเทคโนโลยีสารสนเทศ เพื่อป้องกันปัญหาการขัดแย้งด้านผลประโยชน์ (Conflict of Interest) ที่ยอมรับได้

คณะกรรมการหรือคณะทำงานด้านเทคโนโลยีสารสนเทศมีคุณสมบัติและประสบการณ์เพียงพอที่สามารถปฏิบัติงานได้ อาจขาดการเข้าร่วมประชุมในบางครั้งแต่ไม่มีนัยสำคัญ ปฏิบัติหน้าที่อย่างเหมาะสมและติดตามแก้ไขปัญหาข้อบกพร่องได้รวดเร็วพอสมควร

ฝ่ายบริหารด้านเทคโนโลยีสารสนเทศสามารถพัฒนาทิศทางกลยุทธ์และเพิ่มประสิทธิภาพในการปฏิบัติตามกลยุทธ์และในการดำเนินงานขององค์กรให้สำเร็จตามเป้าหมายได้

พอสมควร ฝ่ายตรวจสอบภายในด้านเทคโนโลยีสารสนเทศสามารถตรวจสอบให้ครอบคลุมจุดที่มีความเสี่ยงได้เพียงพอและมีความเป็นอิสระพอสมควร

ระบบสารสนเทศเพื่อการบริหารขององค์กรสามารถสนับสนุนแนวทางและการดำเนินงานตามกลยุทธ์ได้เพียงพอในระดับที่ยอมรับได้ นโยบายและการจัดการแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง สามารถครอบคลุมและรองรับการดำเนินงานขององค์กร มีการสื่อสารให้พนักงานได้รับทราบอย่างเพียงพอ

อ่อน

การวางแผนกลยุทธ์ นโยบายและแผนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศไม่สอดคล้องกับกลยุทธ์การดำเนินงานขององค์กรและไม่สามารถสะท้อนให้เห็นถึงจุดแข็ง จุดอ่อน โอกาสและอุปสรรคในการดำเนินงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงินได้อย่างเพียงพอ ขาดการติดตามดูแลการดำเนินงานทำให้แผนงานมีความล่าช้า

การบริหารงานด้านเทคโนโลยีสารสนเทศตามหลักธรรมาภิบาลมีไม่เพียงพอและไม่มีความโปร่งใสในการเปิดเผยข้อมูล นโยบายและขั้นตอนการปฏิบัติสำหรับธุรกรรมด้านเทคโนโลยีสารสนเทศ เพื่อป้องกันปัญหาการขัดแย้งด้านผลประโยชน์ (Conflict of Interest) ยังไม่มีความชัดเจนและเป็นที่ยอมรับได้หรือไม่มีนโยบายดังกล่าวเลย

คณะกรรมการหรือคณะทำงานด้านเทคโนโลยีสารสนเทศมีคุณสมบัติไม่เหมาะสมและขาดประสบการณ์ที่จะสามารถปฏิบัติงานได้ ขาดการเข้าร่วมประชุมบ่อยครั้ง การปฏิบัติหน้าที่ยังไม่มีความเป็นอิสระ การติดตามแก้ไขปัญหาข้อบกพร่องยังมีความล่าช้าไม่ทันกับเหตุการณ์

ฝ่ายบริหารด้านเทคโนโลยีสารสนเทศไม่สามารถพัฒนาทิศทางกลยุทธ์และเพิ่มประสิทธิภาพในการปฏิบัติตามกลยุทธ์และในการดำเนินงานขององค์กรให้สำเร็จตามเป้าหมาย ฝ่ายตรวจสอบภายในด้านเทคโนโลยีสารสนเทศยังไม่สามารถตรวจสอบให้ครอบคลุมจุดที่มีความเสี่ยงได้เพียงพอและยังไม่มีความเป็นอิสระในการตัดสินใจและการดำเนินงานที่ยอมรับได้

ระบบสารสนเทศเพื่อการบริหารขององค์กรยังไม่สามารถสนับสนุนแนวทางและการดำเนินงานตามกลยุทธ์ได้อย่างเพียงพอ นโยบายและการจัดการแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องยังไม่ครอบคลุมและรองรับการดำเนินงานขององค์กร ไม่มีการสื่อสารให้พนักงานได้รับทราบอย่างเพียงพอ

2. สรุปการจัดระดับความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ

ระดับความเสี่ยง

ที่	ปัจจัยความเสี่ยง	ต่ำ	ปานกลาง	สูง
1	ผลกระทบจากการเปลี่ยนแปลงโครงสร้างองค์กรและทรัพยากรด้านเทคโนโลยีสารสนเทศ	- มีน้อยมาก	- มีไม่มากนักและสามารถแก้ไขได้ในระยะเวลาอันสั้น	- มีอย่างมีนัยสำคัญและต้องอาศัยเวลาในการแก้ไข
2	การวางแผนกลยุทธ์และการดำเนินงานด้านเทคโนโลยีสารสนเทศ มีระบบการจัดการการบริหารความเสี่ยงและแผนการดำเนินงานที่.....	- มีความชัดเจนเป็นอย่างดี	- มีความชัดเจนอย่างเพียงพอ	- ไม่มีความชัดเจนเพียงพอและขาดประสิทธิภาพ
3	ความเสี่ยงที่เกิดขึ้นสะท้อนให้เห็นลักษณะของเป้าหมายเชิงกลยุทธ์และการบริหารงานด้านเทคโนโลยีสารสนเทศที่.....	- มีความชัดเจนและปลอดภัยดี สอดคล้องกับการดำเนินธุรกิจและการเปลี่ยนแปลงของสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศ	- มีความชัดเจนและปลอดภัยเพียงพอ สอดคล้องกับการดำเนินธุรกิจและการเปลี่ยนแปลงของสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศ	- ไม่มีความชัดเจนและปลอดภัยเพียงพอ ไม่สอดคล้องกับการดำเนินธุรกิจและสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศ
4	การสื่อสารเป้าหมาย นโยบาย แผนการดำเนินงานและระเบียบปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศขององค์กรไปยังผู้ปฏิบัติงานทุกระดับและนำไปปฏิบัติ	- มีการสื่อสารที่ดีและนำไปปฏิบัติได้อย่างมีประสิทธิผลและสม่ำเสมอ	- มีการสื่อสารอย่างเหมาะสมและนำไปปฏิบัติอย่างมีประสิทธิผล	- การสื่อสารไม่ชัดเจนไม่ได้นำไปปฏิบัติหรือนำไปปฏิบัติแต่ไม่มีประสิทธิผล
5	การตัดสินใจทางด้านเทคโนโลยีสารสนเทศมีผลกระทบต่อฐานะการดำเนินงานและชื่อเสียงของสถาบันการเงิน	- มีผลกระทบน้อยมาก	- ผลกระทบไม่ได้ก่อให้เกิดความเสียหายอย่างมีนัยสำคัญ	- มีผลกระทบที่อาจก่อให้เกิดความเสียหายสูง

การจัดการความเสี่ยง

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
1	การวางแผนกลยุทธ์ นโยบายและแผนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	- มีอย่างชัดเจน สอดคล้องกับ กลยุทธ์ขององค์กรและการติดตามเป็นไปอย่างใกล้ชิด ทั่วถึง	- มีเพียงพอ สอดคล้องกับกลยุทธ์ขององค์กรและมีการติดตามในระดับเพียงพอ	- ไม่เพียงพอขาดความชัดเจนและไม่สอดคล้องกับกลยุทธ์ขององค์กร ขาดการติดตาม ทำให้แผนมีความล่าช้า
2	การบริหารด้านเทคโนโลยีสารสนเทศตามหลักธรรมาภิบาล (IT Governance)	- มีอย่างชัดเจนและโปร่งใสในการเปิดเผยข้อมูล	- มีเพียงพอและโปร่งใสในการเปิดเผยข้อมูล	- มีไม่เพียงพอขาดความชัดเจนและโปร่งใสในการเปิดเผยข้อมูล
3	คณะกรรมการหรือคณะทำงานด้านเทคโนโลยีสารสนเทศ	- มีคณะกรรมการหรือคณะทำงานที่สำคัญครบถ้วน - มีคุณสมบัติที่จะปฏิบัติงานได้อย่างมีประสิทธิภาพ - ให้ความสำคัญและดำเนินการให้มีผลในทางปฏิบัติอย่างจริงจัง - เข้าประชุมอย่างสม่ำเสมอ - สามารถปฏิบัติตามหน้าที่ที่ได้รับมอบหมายได้อย่างอิสระและมีประสิทธิภาพ และมีการติดตามงานและประเมินผล รวมทั้งติดตาม แก้ไขข้อบกพร่องต่างๆ อย่างใกล้ชิดและต่อเนื่อง	- มีอย่างเพียงพอ - มีคุณสมบัติเพียงพอที่จะปฏิบัติงานได้ - ให้ความสำคัญและดำเนินการให้มีผลในทางปฏิบัติพอสมควร - ขาดการประชุมแต่ไม่เป็นนัยสำคัญ - ปฏิบัติตามหน้าที่ที่ได้รับมอบหมายอย่างเหมาะสม และมีการติดตามงานและประเมินผล รวมทั้งติดตามแก้ไขข้อบกพร่องต่างๆ พอสมควร	- ไม่มีหรือมีไม่เพียงพอ - มีคุณสมบัติไม่เพียงพอสำหรับการปฏิบัติงาน - ให้ความสำคัญและดำเนินการให้มีผลในทางปฏิบัติไม่เพียงพอ - ไม่ให้ความสำคัญกับการประชุม - การปฏิบัติตามหน้าที่และการบริหารงานขาดความเป็นอิสระ ความรัดกุมและไม่มีการติดตามงานและประเมินผลรวมทั้งติดตามแก้ไขข้อบกพร่องต่างๆ อย่างเพียงพอ

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
4	ฝ่ายบริหารด้านเทคโนโลยีสารสนเทศ	- มีประสบการณ์ ความรู้ ความชำนาญ และมีศักยภาพสูงในการพัฒนากลยุทธ์ - สามารถปฏิบัติงานได้ตามแผนฯและเพิ่มประสิทธิภาพขององค์กร อย่างดี - มีการริเริ่มและเสนอแนวทางใหม่ มีการทบทวนนโยบายที่กำลังดำเนินอยู่ มีการติดตามงานและประเมินผล อย่างใกล้ชิดและต่อเนื่อง - สามารถปฏิบัติตามหน้าที่ที่ได้รับมอบหมายได้อย่างอิสระและมีประสิทธิภาพ และมีการติดตามงานและประเมินผล รวมทั้งติดตาม แก้ไขข้อบกพร่องต่าง ๆ อย่างใกล้ชิดและต่อเนื่อง	- มีประสบการณ์ ความรู้ ความชำนาญ และมีศักยภาพเพียงพอในการพัฒนากลยุทธ์ - สามารถปฏิบัติงานได้ตามแผนฯและเพิ่มประสิทธิภาพขององค์กรพอควร - มีการริเริ่มและเสนอแนวทางใหม่ มีการทบทวนนโยบายที่กำลังดำเนินอยู่ มีการ ติดตามงานและประเมินผลพอสมควร - ปฏิบัติตามหน้าที่ที่ได้รับมอบหมายอย่างเหมาะสม และมีการติดตามงานและประเมินผล รวมทั้งติดตามแก้ไขข้อบกพร่องต่าง ๆ พอสมควร	- มีประสบการณ์ ความรู้ ความชำนาญ และมีศักยภาพไม่เพียงพอในการพัฒนากลยุทธ์ - ไม่สามารถปฏิบัติงานได้ตามแผนฯและขาดประสิทธิภาพในการปฏิบัติงาน - ไม่มีการริเริ่มและเสนอแนวทางใหม่ ไม่มีการทบทวนนโยบายที่กำลังดำเนินอยู่ และไม่มีการติดตามงานและประเมินผล อย่างเพียงพอ - การปฏิบัติตามหน้าที่และการบริหารงานขาดความเป็นอิสระ ความรัดกุมและ ไม่มีการติดตามงานและประเมินผลรวมทั้งติดตามแก้ไขข้อบกพร่องต่าง ๆ อย่างเพียงพอ

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
5	การตรวจสอบภายใน	- แผนการตรวจสอบมีความชัดเจน ระบุประเด็นที่จะทำการตรวจสอบ ระยะเวลาและกำลังคนในการตรวจสอบแต่ละเรื่องมีความเหมาะสมและได้รับอนุมัติจากคณะกรรมการตรวจสอบหรือคณะกรรมการสง.	- มีการจัดทำแผนการตรวจสอบอย่างเหมาะสมและได้รับอนุมัติจากคณะกรรมการตรวจสอบหรือคณะกรรมการสง.	- ไม่มีการจัดทำแผนการตรวจสอบหรือมีแต่ไม่มีความชัดเจนและไม่ได้รับการอนุมัติจากคณะกรรมการตรวจสอบหรือคณะกรรมการสง.
		- การตรวจสอบครอบคลุมทุกจุดที่อาจเกิดความเสี่ยง	- การตรวจสอบครอบคลุมทุกจุดที่มีนัยสำคัญ	- การตรวจสอบไม่ครอบคลุมจุดที่อาจเกิดความเสี่ยงที่มีนัยสำคัญ
		- มีคู่มือและเครื่องมือในการตรวจสอบครบถ้วน เพียงพอ	- มีคู่มือและเครื่องมือในการตรวจสอบ ยังไม่ครบถ้วน แต่เพียงพอสำหรับระบบงานหลัก	- ยังไม่มีคู่มือและเครื่องมือในการตรวจสอบอย่างเพียงพอ
		- ผลการตรวจสอบและกระบวนการตรวจสอบมีความเหมาะสมเชื่อถือได้	- ผลการตรวจสอบและกระบวนการตรวจสอบยังมีจุดอ่อน แต่ไม่มีนัยสำคัญ	- ไม่สามารถใช้ผลการตรวจสอบได้อย่างมีประสิทธิผลและมีกระบวนการตรวจสอบที่ไม่เหมาะสม
		- มีความเป็นอิสระจากผู้ที่ก่อให้เกิดความเสี่ยง ไม่ได้ถูกครอบงำโดยผู้บริหารหรือคณะกรรมการ สง. ครบถ้วน	- มีความเป็นอิสระพอสมควร	- ไม่มีความเป็นอิสระจากผู้ที่ก่อให้เกิดความเสี่ยงมีความคลุมเครือไม่ชัดเจน

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
6	ระบบสารสนเทศเพื่อการบริหาร (MIS)	- สามารถรายงานข้อมูลเพื่อสนับสนุนการตัดสินใจของผู้บริหารได้อย่างถูกต้อง ครบถ้วน ทันเวลาและเชื่อถือได้	- ข้อมูลและรายงานมีความถูกต้อง ครบถ้วน ทันกาล และเชื่อถือได้อยู่ในระดับที่ยอมรับได้	- ข้อมูลและรายงานมีข้อผิดพลาดอย่างมีนัยสำคัญ ไม่ครบถ้วนเพียงพอและมีความล่าช้า
7	นโยบายและการจัดการแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง	- มีแผนครอบคลุมการกู้ระบบ การสำรองภัยฉุกเฉินและการวางแผนรองรับด้านการบริหารงานทั้งหมด - ทดสอบแผนอย่างสม่ำเสมอ - มีการสื่อสารให้พนักงานในองค์กรเข้าใจและตระหนักอย่างมีประสิทธิภาพ	- มีแผนครอบคลุมการกู้ระบบ การสำรองภัยฉุกเฉินและการวางแผนรองรับด้านการบริหารงานเพียงพอ - ทดสอบแผนเป็นระยะ - มีการสื่อสารให้พนักงานในองค์กรได้รับทราบเพียงพอ	- ไม่มีแผนหรือมีแต่ไม่ครอบคลุมการกู้ระบบ การสำรองภัยฉุกเฉินและการวางแผนรองรับด้านการบริหารงานอย่างเพียงพอ - ไม่มีการทดสอบแผน - ไม่มีการสื่อสารให้พนักงานในองค์กรเข้าใจอย่างมีประสิทธิภาพ

3. การจัดอันดับความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ

ระดับความเสี่ยง

ต่ำ

ด้านการรักษาความปลอดภัย

การนำเทคโนโลยีสมัยใหม่มาใช้สถาบันการเงินได้คำนึงถึงระบบการรักษาความปลอดภัยในการใช้เทคโนโลยีอย่างดี ปริมาณธุรกรรมและผลิตภัณฑ์ที่ต้องพึ่งพาเทคโนโลยีสารสนเทศไม่มีความซับซ้อนและไม่ส่งผลกระทบต่อการปฏิบัติงาน โครงสร้างระบบเทคโนโลยีสารสนเทศและเครือข่ายไม่มีความซับซ้อนตอบสนองการทำธุรกรรมและการให้บริการแก่ลูกค้าอย่างดี ความผิดพลาดและการทุจริตที่เกิดจากการปฏิบัติงานมีเพียงเล็กน้อย มีระบบการควบคุมภายในและการรักษาความปลอดภัยที่ดี

ด้านความถูกต้องเชื่อถือได้ของข้อมูล

การพัฒนาและปรับปรุงระบบงานที่เกิดความล่าช้าไม่ส่งผลกระทบต่อการดำเนินงานและการดำเนินกลยุทธ์ของสถาบันการเงิน ระบบงานที่พัฒนาสามารถตอบสนองความต้องการและเกิดประโยชน์แก่ผู้ใช้งานและองค์กรอย่างแท้จริง ความผิดพลาดของข้อมูลและรายงานที่เกิดจากการประมวลผลระบบงานไม่มีข้อผิดพลาดที่สำคัญ การเชื่อมโยงระบบงานต่างๆ เป็นไปอย่างสมบูรณ์ ข้อมูลที่ได้รับมีความถูกต้องเชื่อถือได้ ทำให้การดำเนินงานเกิดประสิทธิผลอย่างแท้จริง

ด้านความพร้อมใช้งาน

การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉินได้มีการจัดทำแผนครอบคลุมการปฏิบัติงานทุกด้านอย่างครบถ้วนและสามารถกู้ระบบกลับคืนเพื่อใช้งานได้อย่างรวดเร็วเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉิน

ปานกลาง

ด้านการรักษาความปลอดภัย

การนำเทคโนโลยีสมัยใหม่มาใช้สถาบันการเงินได้คำนึงถึงระบบการรักษาความปลอดภัยในการใช้เทคโนโลยีอย่างเพียงพอในระดับที่ยอมรับได้ ปริมาณธุรกรรมและผลิตภัณฑ์ที่ต้องพึ่งพาเทคโนโลยีสารสนเทศมีความซับซ้อนไม่มากนักและส่งผลกระทบต่อการปฏิบัติงานบ้างแต่ไม่มีนัยสำคัญ โครงสร้างระบบเทคโนโลยีสารสนเทศและเครือข่ายมีความซับซ้อนไม่มากนักสามารถตอบสนองการทำธุรกรรมและการให้บริการแก่ลูกค้าดีพอสมควร ความผิดพลาดและการทุจริตที่เกิดจากการปฏิบัติงานมีเป็นครั้งคราวแต่ไม่ส่งผลกระทบต่อการดำเนินงานอย่างมีนัยสำคัญ ระบบการควบคุมภายในและการรักษาความปลอดภัยมีจุดอ่อนในระดับที่ยอมรับได้

ด้านความถูกต้องเชื่อถือได้ของข้อมูล

การพัฒนาและปรับปรุงระบบงานที่เกิดความล่าช้าส่งผลกระทบต่อการดำเนินงานและการดำเนินกลยุทธ์ของสถาบันการเงินบ้างแต่ไม่มีนัยสำคัญ ระบบงานที่พัฒนาสามารถตอบสนองความต้องการและเกิดประโยชน์แก่ผู้ใช้งานและองค์กรได้เพียงพอ ความผิดพลาดของข้อมูลและรายงานที่เกิดจากการประมวลผลระบบงานมีข้อผิดพลาดที่สามารถยอมรับได้ การเชื่อมโยงระบบงานต่างๆ ยังไม่สมบูรณ์ แต่มีระบบรองรับการรวบรวมข้อมูลที่เชื่อถือได้

ด้านความพร้อมใช้งาน

การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉิน ได้มีการจัดทำแผนการปฏิบัติงานด้านต่างๆอย่างเพียงพอ และต้องใช้เวลาในการกู้ระบบกลับคืนเพื่อใช้งานเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉินไม่มากนัก และไม่กระทบต่อการดำเนินธุรกิจโดยรวมอย่างมีนัยสำคัญ

สูง

ด้านการรักษาความปลอดภัย

การนำเทคโนโลยีสมัยใหม่มาใช้สถาบันการเงินมิได้คำนึงถึงระบบการรักษาความปลอดภัยในการใช้เทคโนโลยีที่เพียงพอ มีจุดอ่อนที่ก่อให้เกิดความเสี่ยงสูง ปริมาณธุรกรรมและผลิตภัณฑ์ที่ต้องพึ่งพาเทคโนโลยีสารสนเทศมีความซับซ้อนมากและมีปริมาณมาก ส่งผลกระทบต่อการปฏิบัติงานอย่างมีนัยสำคัญ โครงสร้างระบบเทคโนโลยีสารสนเทศและเครือข่ายมีความซับซ้อนมากส่งผลกระทบต่อการทำธุรกรรมและการให้บริการแก่ลูกค้าอย่างมีนัยสำคัญ ความผิดพลาดและการทุจริตที่เกิดจากการปฏิบัติงานเกิดขึ้นบ่อยครั้งและส่งผลกระทบต่อการดำเนินงานอย่างมีนัยสำคัญ ระบบการควบคุมภายในและการรักษาความปลอดภัยมีจุดอ่อนอย่างมากจำเป็นต้องได้รับการแก้ไขอย่างเร่งด่วน

ด้านความถูกต้องเชื่อถือได้ของข้อมูล

การพัฒนาและปรับปรุงระบบงานที่เกิดความล่าช้าส่งผลกระทบต่อการดำเนินงานและการดำเนินกลยุทธ์ของสถาบันการเงินมากอย่างมีนัยสำคัญ ระบบงานที่พัฒนาไม่สามารถตอบสนองความต้องการและเกิดประโยชน์แก่ผู้ใช้งานและองค์กรได้จำเป็นต้องดำเนินการปรับปรุงแก้ไขทันที ความผิดพลาดของข้อมูลและรายงานที่เกิดจากการประมวลผลระบบงานมีข้อผิดพลาดมากกระทบต่อการดำเนินงานอย่างมีนัยสำคัญ ระบบงานต่างๆ ยังไม่สามารถเชื่อมโยงกันได้อย่างสมบูรณ์และไม่มีระบบรองรับการรวบรวมข้อมูลเพื่อนำมาใช้งานอย่างมีประสิทธิภาพ

ด้านความพร้อมใช้งาน

การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉิน ยังไม่มีการจัดทำให้ครอบคลุมการปฏิบัติงานด้านต่างๆ อย่างเพียงพอหรือไม่ได้มีการจัดทำแผนดังกล่าว ในการกู้ระบบกลับคืนเพื่อใช้งานเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉินต้องใช้เวลานานเกิน 24 ชั่วโมง กระทบต่อการดำเนินธุรกิจโดยรวมอย่างมีนัยสำคัญ

<u>การจัดการความเสี่ยง</u>

ดี

ด้านการรักษาความปลอดภัย

สถาบันการเงินมีนโยบายการรักษาความปลอดภัยที่เขียนเป็นลายลักษณ์อักษรชัดเจนครอบคลุมทั้งองค์กร มีการจัดตั้งหน่วยงานที่ดูแลและรับผิดชอบด้านการรักษาความปลอดภัยอย่างชัดเจน มีการสื่อสารนโยบายการรักษาความปลอดภัยให้พนักงานในองค์กรได้เข้าใจและปฏิบัติตามอย่างเคร่งครัดสม่ำเสมอ การรักษาความปลอดภัยทั้งด้านกายภาพและตรรกะมีการควบคุมที่ดีและกำหนดระเบียบปฏิบัติอย่างเหมาะสม ระบบเครือข่ายสื่อสารมีความเหมาะสมกับองค์กรและป้องกันการบุกรุกจากผู้ที่ไม่มีหน้าที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ

ด้านความถูกต้องเชื่อถือได้ของข้อมูล

การบริหารโครงการพัฒนาระบบงานและโปรแกรมสามารถดำเนินการได้ตามเป้าหมายที่กำหนดและสนับสนุนแผนกลยุทธ์ขององค์กรได้ดี ผลของการพัฒนาระบบงานและโปรแกรมมีความถูกต้องสมบูรณ์ ปฏิบัติตามหลักเกณฑ์และระเบียบที่กำหนดอย่างเคร่งครัด การติดตามดูแลบำรุงรักษาระบบงานและโปรแกรมมีการปฏิบัติอย่างสม่ำเสมอ การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกมีการบริหารงานที่ชัดเจนโปร่งใสและติดตามดูแลผู้ให้บริการอย่างใกล้ชิดสม่ำเสมอ

ด้านความพร้อมใช้งาน

แผนการเตรียมความพร้อมเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉินของสถาบันการเงินมีการจัดทำเป็นลายลักษณ์อักษรครอบคลุมทุกกิจกรรมอย่างชัดเจนและได้รับการอนุมัติจากฝ่ายบริหารอย่างถูกต้อง มีการทดสอบตามแผนที่กำหนดทุกครั้งอย่างสม่ำเสมอ ในกรณีที่มีการใช้บริการจากหน่วยงานภายนอก ได้จัดให้ผู้ให้บริการจัดทำแผนสำรองฉุกเฉินที่สอดคล้องกับแผนขององค์กร และติดตามดูแลการดำเนินงานของผู้ให้บริการอย่างใกล้ชิด สถานที่จัดตั้งศูนย์คอมพิวเตอร์สำรองมีความเหมาะสมและปลอดภัยอย่างดี มีการจัดทำการประกันภัยระบบงานรวมทั้งอุปกรณ์คอมพิวเตอร์อย่างครบถ้วนเพียงพอและต่ออายุสัญญาอย่างสม่ำเสมอ

พอใช้

ด้านการรักษาความปลอดภัย

สถาบันการเงินมีนโยบายการรักษาความปลอดภัยที่เขียนเป็นลายลักษณ์อักษรอย่างเพียงพอแต่ยังไม่ครอบคลุมทั้งองค์กร การดูแลและรับผิดชอบด้านการรักษาความปลอดภัยขององค์กรอยู่ในหน่วยงานอื่นมิได้มีการจัดตั้งขึ้นโดยเฉพาะแต่เป็นที่ยอมรับได้ การสื่อสารนโยบายการรักษาความปลอดภัยให้พนักงานในองค์กรได้เข้าใจอยู่ในระดับที่เพียงพอและมีการปฏิบัติตามอย่างเคร่งครัด การรักษาความปลอดภัยทั้งด้านกายภาพและตรรกะมีการควบคุมที่เพียงพอและกำหนดระเบียบปฏิบัติเป็นที่ยอมรับได้ ระบบเครือข่ายสื่อสารมีความเหมาะสมกับองค์กรและป้องกันการบุกรุกจากผู้ที่ไม่มีหน้าที่เกี่ยวข้องในระดับที่ยอมรับได้

ด้านความถูกต้องเชื่อถือได้ของข้อมูล

การบริหารโครงการพัฒนาระบบงานและโปรแกรมสามารถดำเนินการได้ตามเป้าหมายที่กำหนดไว้เป็นส่วนใหญ่และสนับสนุนแผนกลยุทธ์ขององค์กรได้ดี ผลของการพัฒนาระบบงานและโปรแกรมมีความถูกต้องเพียงพอตามหลักเกณฑ์และระเบียบที่กำหนด การติดตามดูแลบำรุงรักษาระบบงานและโปรแกรมมีการปฏิบัติตามคู่มือการปฏิบัติงานในระดับที่ยอมรับได้ การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกมีการบริหารงานที่โปร่งใสและติดตามดูแลผู้ให้บริการเพียงพอในระดับที่ยอมรับได้

ด้านความพร้อมใช้งาน

แผนการเตรียมความพร้อมเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉินของสถาบันการเงินมีการจัดทำเป็นลายลักษณ์อักษรอย่างเพียงพอและได้รับการอนุมัติจากฝ่ายบริหาร มีการทดสอบตามแผนที่กำหนดเป็นระยะในระดับที่ยอมรับได้ ในกรณีที่มีการใช้บริการจากหน่วยงานภายนอก ได้จัดให้ผู้ให้บริการจัดทำแผนสำรองฉุกเฉินและติดตามดูแลการดำเนินงานของผู้ให้บริการอย่างเพียงพอ สถานที่จัดตั้งศูนย์คอมพิวเตอร์สำรองมีความเหมาะสมและปลอดภัยในระดับที่ยอมรับได้ การจัดทำการประกันภัยระบบงานรวมทั้งอุปกรณ์คอมพิวเตอร์มีการประกันภัยความเสียหายในจุดที่มีสาระสำคัญอย่างเพียงพอและต่ออายุสัญญาอย่างสม่ำเสมอ

อ่อน

ด้านการรักษาความปลอดภัย

สถาบันการเงินยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยที่ชัดเจนครอบคลุมทั้งองค์กรหรือไม่ได้มีการกำหนดนโยบายไว้เลย รวมทั้งไม่มีการจัดตั้งหน่วยงานที่ดูแลและรับผิดชอบด้านการรักษาความปลอดภัยอย่างชัดเจน การสื่อสารนโยบายการรักษาความปลอดภัยให้พนักงานในองค์กรได้เข้าใจไม่มีความชัดเจนและไม่มีการนำไปปฏิบัติตามอย่างจริงจัง

การรักษาความปลอดภัยทั้งด้านกายภาพและตรรกะไม่มีการควบคุมที่ดีหรือมีแต่การควบคุมไม่เพียงพอ การกำหนดระเบียบปฏิบัติยังไม่เหมาะสม ระบบเครือข่ายสื่อสารไม่มีความเหมาะสมเพียงพอและไม่มีระบบป้องกันการบุกรุกจากผู้ที่ไม่มีหน้าที่เกี่ยวข้องก่อให้เกิดความเสี่ยงอย่างมีนัยสำคัญ

ด้านความถูกต้องเชื่อถือได้ของข้อมูล

การบริหารโครงการพัฒนาระบบงานและโปรแกรมไม่สามารถดำเนินการได้ตามเป้าหมายล่าช้ากว่าที่กำหนดเกือบทุกโครงการทำให้ไม่สามารถสนับสนุนแผนกลยุทธ์ขององค์กรได้ ผลของการพัฒนาระบบงานและโปรแกรมมีข้อผิดพลาดมากไม่ปฏิบัติตามหลักเกณฑ์และระเบียบที่กำหนด การติดตามดูแลบำรุงรักษาระบบงานและโปรแกรมมีไม่เพียงพอและไม่ปฏิบัติตามคู่มือการปฏิบัติงานอย่างมีนัยสำคัญ การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกมีการบริหารงานที่ยังไม่ชัดเจนโปร่งใส การติดตามดูแลผู้ให้บริการยังไม่เพียงพอจำเป็นต้องปรับปรุงแก้ไขอย่างมีนัยสำคัญ

ด้านความพร้อมใช้งาน

สถาบันการเงินไม่มีแผนการเตรียมความพร้อมเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉินหรือมีแผนแต่ไม่เพียงพอที่จะรองรับภัยพิบัติหรือเหตุฉุกเฉินได้และแผนดังกล่าวยังไม่ได้รับการอนุมัติจากฝ่ายบริหาร การทดสอบแผนไม่เป็นไปตามที่กำหนดหรือไม่มีการทดสอบเลย ในกรณีที่มีการใช้บริการจากหน่วยงานภายนอก ไม่ได้จัดให้ผู้ให้บริการจัดทำแผนสำรองฉุกเฉินหรือมีแผนสำรองฉุกเฉินแต่ไม่สอดคล้องกับแผนขององค์กร การติดตามดูแลการดำเนินงานของผู้ให้บริการยังไม่ให้ความสนใจอย่างเพียงพอ สถานที่จัดตั้งศูนย์คอมพิวเตอร์สำรองยังไม่มีความเหมาะสมและปลอดภัยหรือไม่มีศูนย์สำรองเลย รวมทั้งไม่มีการจัดทำการประกันภัยระบบงานรวมทั้งอุปกรณ์คอมพิวเตอร์อย่างครบถ้วนเพียงพอและไม่มีการติดตามการต่ออายุสัญญาที่ครบกำหนดอย่างสม่ำเสมอ

4. สรุปการจัดระดับความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ

<u>ด้านการรักษาความปลอดภัย</u>

ระดับความเสี่ยง

ที่	ปัจจัยความเสี่ยง	ต่ำ	ปานกลาง	สูง
1	การรักษาสมดุลในการนำเทคโนโลยีใหม่มาใช้กับระบบการรักษาความปลอดภัย	- มีการคำนึงถึงระบบการรักษาความปลอดภัยอย่างดี	- มีการคำนึงถึงระบบการรักษาความปลอดภัยพอสมควรและเป็นที่ยอมรับได้	- ไม่ได้คำนึงถึงระบบการรักษาความปลอดภัยเพียงพอและมีจุดอ่อนที่ก่อให้เกิดความเสี่ยงสูง
2	ปริมาณ ประเภท และความซับซ้อนของรายการ/ ธุรกรรมผลิตภัณฑ์และบริการทางการเงินทางอิเล็กทรอนิกส์หรือบริการที่ต้องพึ่งพาเทคโนโลยีสารสนเทศ	- เป็นธุรกรรมหรือผลิตภัณฑ์พื้นฐานทั่วไปที่ไม่มีความซับซ้อนและมีปริมาณน้อย เมื่อเทียบกับสง. อื่นที่มีขนาดใกล้เคียง และไม่ส่งผลกระทบต่อการปฏิบัติงาน	- เป็นธุรกรรมหรือผลิตภัณฑ์ทั้งประเภทพื้นฐานจนถึงประเภทที่มีความซับซ้อนไม่มากนัก และมีปริมาณใกล้เคียงกับสง. อื่นที่มีขนาดใกล้เคียงกัน และอาจส่งผลกระทบต่อการปฏิบัติงานบ้าง แต่ไม่มีนัยสำคัญ	- เป็นธุรกรรมหรือผลิตภัณฑ์ทั้งประเภทพื้นฐานจนถึงประเภทที่มีความซับซ้อนมากและมีปริมาณมากเมื่อเทียบกับสง. อื่นที่มีขนาดใกล้เคียงกัน และอาจส่งผลกระทบต่อการปฏิบัติงานอย่างมีนัยสำคัญ
3	ความเหมาะสมของโครงสร้างระบบเทคโนโลยีสารสนเทศและเครือข่ายสื่อสารเพื่อรองรับการให้บริการ	- ไม่มีความซับซ้อนเหมาะสมกับการทำธุรกรรมและการให้บริการอย่างดี	- มีความซับซ้อนไม่มากนักอาจส่งผลกระทบต่อการทำธุรกรรมและการให้บริการบ้าง แต่ไม่มีนัยสำคัญ	- มีความซับซ้อนมากอาจส่งผลกระทบต่อการทำธุรกรรมและการให้บริการอย่างมีนัยสำคัญ

ที่	ปัจจัยความเสี่ยง	ต่ำ	ปานกลาง	สูง
4	ความผิดพลาด ข้อบกพร่อง และการทุจริตที่เกิดจาก สภาพแวดล้อมความปลอดภัย และประสิทธิภาพของ ระบบงาน	- มีเพียงเล็กน้อย	- มีเกิดขึ้นบ้างเป็น ครั้งคราวแต่ไม่ ส่งผลกระทบต่อ การดำเนินงานอย่าง มีนัยสำคัญ	- มีเกิดขึ้นบ่อยครั้งและ ส่งผลกระทบต่อการ ดำเนินงานอย่างมี นัยสำคัญ
5	จุดอ่อนของระบบการควบคุม ภายในและการรักษาความ ปลอดภัย	- ระบบการควบคุม ภายในและการรักษา ความปลอดภัยมีความ รัดกุม เพียงพอ	- ระบบการควบคุม ภายในและการ รักษาความ ปลอดภัยมีจุดอ่อน แต่มีระบบหรือ วิธีการควบคุมอื่น มาสนับสนุน เพียงพอ	- ระบบการควบคุม ภายในและการรักษา ความปลอดภัยมี จุดอ่อนอย่างมาก จำเป็นต้องได้รับการ แก้ไขอย่างเร่งด่วน

การจัดการความเสี่ยง

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
1	นโยบายการรักษาความ ปลอดภัย	- มีอย่างชัดเจนและ ครอบคลุมทั้งองค์กร	- มีอย่างเพียงพอ แต่ยังไม่ ครอบคลุมทั้ง องค์กร	- มีไม่เพียงพอหรือไม่มี การกำหนดนโยบายไว้ เลย
2	ความชัดเจนของหน่วยงานที่ รับผิดชอบในการรักษาความ ปลอดภัยให้แก่องค์กร	- มีหน่วยงานที่ รับผิดชอบชัดเจน	- มีอยู่ใน หน่วยงานอื่นและ มีหน้าที่รับผิดชอบ ที่ยอมรับได้	- ไม่มีหน่วยงานที่ รับผิดชอบชัดเจนหรือมี แต่ไม่สามารถยอมรับ ได้
3	การสื่อสารนโยบายการรักษา ความปลอดภัยให้แก่พนักงาน ในองค์กร	- มีการสื่อสารที่ชัดเจน ทั้งองค์กรและปฏิบัติ ตามอย่างเคร่งครัด สม่ำเสมอ	- มีการสื่อสารที่ เพียงพอและ ปฏิบัติตามโดย เคร่งครัด	- การสื่อสารไม่ชัดเจน และไม่มีการนำไป ปฏิบัติอย่างจริงจัง หรือไม่มีการปฏิบัติเลย
4	คุณภาพของการรักษาความ ปลอดภัยด้านกายภาพ	- มีความเหมาะสมดี - มีการกำหนดระเบียบ ปฏิบัติและควบคุมอย่าง เคร่งครัดสม่ำเสมอ	- มีความเพียงพอ - มีการกำหนด ระเบียบปฏิบัติ และควบคุมใน ระดับที่ยอมรับได้	- ไม่มีความเหมาะสม เพียงพอ - มีระเบียบปฏิบัติที่ไม่ ชัดเจนและไม่มีการ ควบคุมดูแลที่ดี

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
5	คุณภาพของการรักษาความปลอดภัยทั้งด้านตรรกะ รวมทั้งความเป็นส่วนตัวของข้อมูล	- มีการควบคุมที่ดีและเหมาะสมในการเข้าใช้งาน - มีการกำหนดระเบียบปฏิบัติและป้องกันภัยคุกคามอย่างเหมาะสม	- มีการควบคุมที่เพียงพอในการเข้าใช้งาน - มีการกำหนดระเบียบและป้องกันภัยคุกคามในระดับที่ยอมรับได้	- ไม่มีการควบคุมการเข้าใช้งานหรือมีแต่ไม่เพียงพอ - ไม่มีการกำหนดระเบียบและป้องกันภัยคุกคามซึ่งก่อให้เกิดความเสี่ยงอย่างมีนัยสำคัญ
6	ระบบเครือข่ายสื่อสาร	- มีความเหมาะสมดีและมีระบบการป้องกันการบุกรุกที่มีประสิทธิภาพ	- มีความเหมาะสมเพียงพอและมีระบบการป้องกันการบุกรุกอยู่ในระดับที่ยอมรับได้	- ไม่มีความเหมาะสมเพียงพอและไม่มีระบบการป้องกันการบุกรุกก่อให้เกิดความเสี่ยงอย่างมีนัยสำคัญ

<u>ด้านความถูกต้อง เชื่อถือได้ของข้อมูล</u>

ระดับความเสี่ยง

ที่	ปัจจัยความเสี่ยง	ต่ำ	ปานกลาง	สูง
1	ผลกระทบจากความล่าช้าของการพัฒนาและปรับปรุงระบบงานเพื่อรองรับความต้องการใหม่	- ไม่มีผลกระทบหรือมีผลกระทบน้อยมาก	- มีผลกระทบบ้างพอสมควรแต่ไม่มีนัยสำคัญ	- มีผลกระทบมากอย่างมีนัยสำคัญ
2	ระบบที่พัฒนาและปรับปรุงสามารถตอบสนองความต้องการของผู้ใช้งานและการดำเนินธุรกิจได้อย่างแท้จริง	- ตรงตามความต้องการและเกิดประโยชน์อย่างแท้จริง	- สามารถตอบสนองความต้องการได้เพียงพออาจมีข้อบกพร่องบ้างแต่ไม่มีนัยสำคัญ	- ไม่สามารถตอบสนองความต้องการได้และต้องดำเนินการแก้ไขทันทีเนื่องจากมีผลกระทบต่อการดำเนินงานอย่างมีนัยสำคัญ
3	ข้อผิดพลาดของข้อมูลและรายงานที่ออกจากระบบงานต่างๆ	- ไม่มีข้อผิดพลาด หรือมีน้อยมาก	- มีข้อผิดพลาดบ้างแต่ไม่มีนัยสำคัญ	- มีข้อผิดพลาดมากอย่างมีนัยสำคัญ

ที่	ปัจจัยความเสี่ยง	ต่ำ	ปานกลาง	สูง
4	การเชื่อมโยง แก้ไข หรือเปลี่ยนแปลงระบบงาน ซึ่งอาจทำให้เกิดข้อผิดพลาด	- เป็นระบบที่มีการเชื่อมโยงกันอย่างสมบูรณ์ ไม่มีความยุ่งยากในการแก้ไขหรือเปลี่ยนแปลง และข้อมูลที่ได้มีความถูกต้องเชื่อถือได้	- เป็นระบบที่ยังไม่สามารถเชื่อมโยงกันได้อย่างสมบูรณ์ แต่มีระบบรองรับในการรวบรวมข้อมูลเพื่อนำมาใช้งานได้อย่างถูกต้อง แต่ก็อาจมีข้อผิดพลาดบางเล็กน้อยซึ่งไม่มีนัยสำคัญ	- เป็นระบบที่ยังไม่สามารถเชื่อมโยงกันได้อย่างสมบูรณ์ และไม่มีระบบรองรับในการรวบรวมข้อมูลเพื่อนำมาใช้งานหรือมีข้อผิดพลาดที่มีนัยสำคัญซึ่งจำเป็นต้องได้รับการแก้ไขอย่างเร่งด่วน

การจัดการความเสี่ยง

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
1	การบริหารโครงการพัฒนาระบบงานและโปรแกรม	- สามารถดำเนินการได้ตามเป้าหมายทุกโครงการและสนับสนุนแผนกลยุทธ์ได้ดี	- สามารถดำเนินการได้ตามเป้าหมาย เป็นส่วนใหญ่และสนับสนุนแผนกลยุทธ์ได้ดี	- โครงการไม่สามารถดำเนินการได้ตามเป้าหมายมีความล่าช้าเกือบทุกโครงการทำให้ไม่สามารถสนับสนุนแผนกลยุทธ์ได้
2	การพัฒนาระบบงานและโปรแกรม รวมทั้งการจัดซื้อจัดหาระบบ	- มีความถูกต้องสมบูรณ์ตามหลักเกณฑ์และระเบียบที่กำหนด	- มีความถูกต้องเพียงพอตามหลักเกณฑ์และระเบียบที่กำหนด โดยข้อผิดพลาดไม่มีนัยสำคัญ	- มีข้อผิดพลาดมากไม่ปฏิบัติตามหลักเกณฑ์และระเบียบที่กำหนดหรือไม่ได้กำหนดหลักเกณฑ์และระเบียบไว้
3	การบำรุงรักษาระบบงานและโปรแกรม	- มีการติดตามดูแลรักษาอย่างดีและปฏิบัติตามคู่มือการปฏิบัติงานอย่างสม่ำเสมอ	- มีการติดตามดูแลรักษาที่เพียงพอและปฏิบัติตามคู่มือการปฏิบัติงานในระดับที่ยอมรับได้	- ไม่มีการติดตามดูแลรักษาอย่างเพียงพอและไม่ปฏิบัติตามคู่มือการปฏิบัติงานอย่างมีนัยสำคัญ

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
4	การบริหารการใช้บริการจากหน่วยงานภายนอก	- มีความโปร่งใสในกระบวนการคัดเลือกและติดตามดูแลผู้ให้บริการอย่างสม่ำเสมอ	- มีความโปร่งใสในกระบวนการคัดเลือกพอสมควรและติดตามดูแลผู้ให้บริการเพียงพอในระดับที่ยอมรับได้	- กระบวนการคัดเลือกยังไม่มีความชัดเจนและโปร่งใส การติดตามดูแลผู้ให้บริการยังไม่เพียงพอจำเป็นต้องปรับปรุงแก้ไขอย่างมีนัยสำคัญ

<u>ด้านความพร้อมใช้งาน</u>

ระดับความเสี่ยง

ที่	ปัจจัยความเสี่ยง	ต่ำ	ปานกลาง	สูง
1	การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉิน	- มีการจัดทำแผนครอบคลุมการปฏิบัติงานด้านต่างๆ อย่างดีและครบถ้วน	- มีการจัดทำแผนเพื่อรองรับการปฏิบัติงานด้านต่างๆ อย่างเพียงพอ	- ไม่ได้จัดทำแผนเพื่อรองรับการปฏิบัติงานด้านต่างๆ หรือมีแผนแต่ไม่เพียงพอที่จะรองรับภัยพิบัติหรือเหตุฉุกเฉินได้
2	ความสามารถในการกู้ระบบกลับคืนเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉิน	- สามารถกู้ระบบกลับคืนเพื่อใช้งานได้ในทันทีหรือในระยะเวลาอันสั้น	- ต้องใช้เวลาในการกู้ระบบกลับคืนเพื่อใช้งานแต่ไม่มากนักและไม่กระทบการดำเนินธุรกิจโดยรวมอย่างมีนัยสำคัญ	- ไม่สามารถกู้ระบบกลับคืนเพื่อใช้งานได้หรือต้องใช้ระยะเวลานานเกิน 24 ชั่วโมง กระทบต่อการดำเนินธุรกิจโดยรวมอย่างมีนัยสำคัญ

การจัดการความเสี่ยง

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
1	แผนการเตรียมความพร้อมเมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉิน	- แผนมีความครอบคลุมทุกกิจกรรม และผ่านการอนุมัติจากผู้บริหาร - จัดทำเป็นลายลักษณ์อักษรชัดเจน ขั้นตอนการปฏิบัติมีความเข้าใจง่าย ละเอียด สามารถปฏิบัติตามได้ทันที	- แผนมีความเพียงพอ และได้รับการอนุมัติจากผู้บริหาร - จัดทำเป็นลายลักษณ์อักษรเฉพาะขั้นตอนของการปฏิบัติงานที่สำคัญ สามารถปฏิบัติตามแต่อาจต้องอาศัยความเข้าใจของพนักงานด้วย	- ไม่มีการจัดทำแผนหรือมีแผนแต่ไม่เหมาะสมเพียงพอกับธุรกรรมหรือไม่ได้รับอนุมัติจากผู้บริหาร - ไม่มีการจัดทำเป็นลายลักษณ์อักษรหรือจัดทำแต่ไม่สามารถนำไปปฏิบัติให้เกิดผลตามความต้องการได้
2	แผนสำรองฉุกเฉินของบริษัทผู้ให้บริการภายนอก	- มีความสอดคล้องกับแผนสำรองฉุกเฉินของสถาบันการเงิน รวมทั้งมีกระบวนการติดตามดูแลการดำเนินงานของผู้ให้บริการอย่างใกล้ชิด	- มีความสอดคล้องกับแผนสำรองฉุกเฉินของสถาบันการเงิน และกระบวนการติดตามดูแลการดำเนินงานของผู้ให้บริการอยู่ในระดับที่ยอมรับได้	ไม่มีแผนสำรองฉุกเฉินหรือมีแต่ไม่สอดคล้องกับแผนของสถาบันการเงินและไม่ให้ความสนใจในการติดตาม ดูแลการดำเนินงานของผู้ให้บริการอย่างเพียงพอ
3	การทดสอบแผนฉุกเฉินและการสอบทานรายงานที่เกี่ยวข้อง	- มีการทดสอบเป็นไปตามแผนครบถ้วนทุกระบบงาน อย่างน้อยปีละครั้ง - ผู้บริหารระดับสูงจัดให้มีการสอบทานผลการทดสอบและควบคุมดูแลให้มีการแก้ไขอย่างครบถ้วนและรวดเร็ว	- มีการทดสอบเพียงพอในระดับที่ยอมรับได้ - ผู้บริหารระดับสูงสอบทานผลการทดสอบและดำเนินการแก้ไขในจุดที่มีสาระสำคัญ	- ไม่มีการทดสอบหรือทดสอบไม่เป็นไปตามแผนอย่างมีนัยสำคัญ - ไม่มีการสอบทานโดยผู้บริหารระดับสูงหรือไม่มีการแก้ไขในจุดที่มีสาระสำคัญ

ที่	ปัจจัยความเสี่ยง	ดี	พอใช้	อ่อน
4	ศูนย์คอมพิวเตอร์สำรอง	- มีสถานที่ตั้งและสภาพแวดล้อมภายในที่ปลอดภัยและได้รับการดูแลอย่างดี	- มีสถานที่ตั้งและสภาพแวดล้อมภายในตลอดจนการดูแลรักษาความปลอดภัยอยู่ในระดับที่ยอมรับได้	- ไม่มีศูนย์สำรอง หรือมีแต่สภาพแวดล้อมและการดูแลรักษาความปลอดภัยอยู่ในระดับที่มีความเสี่ยงค่อนข้างสูง
5	การประกันภัยระบบงานหรืออุปกรณ์คอมพิวเตอร์เพื่อรองรับความเสียหาย	- มีการประกันภัยอย่างเพียงพอและครอบคลุมความเสียหายที่อาจเกิดขึ้น -มีการติดตามเพื่อต่ออายุสัญญาอย่างสม่ำเสมอ	- มีการประกันภัยความเสียหายที่อาจเกิดขึ้นในจุดที่มีสาระสำคัญอย่างเพียงพอ -มีการติดตามเพื่อต่ออายุสัญญาอย่างสม่ำเสมอ	-ไม่ได้จัดให้มีการประกันภัยความเสียหายที่อาจเกิดขึ้นหรือมีแต่ไม่เพียงพอและไม่ครอบคลุมในจุดที่มีสาระสำคัญ -ไม่มีการติดตามเพื่อต่ออายุสัญญา

5. ปัจจัยในการจัดอันดับโดยรวม

หัวข้อ	อันดับ 1	อันดับ 2	อันดับ 3	อันดับ 4	อันดับ 5
ส่วนใหญ่ของ IT Aggregate risk ของความเสี่ยง 2 ประเภท	อยู่ในระดับต่ำถึงค่อนข้างต่ำ	ต่ำถึงปานกลาง	ปานกลาง	ค่อนข้างสูง	สูง
การจัดการด้าน IT	ดี (อธิบาย : มีการปฏิบัติเป็นไปตามมาตรฐาน เพื่อความมั่นคงปลอดภัยในทุกด้าน การดำเนินงานสอดคล้องกับนโยบายและวิธีปฏิบัติของสถาบันการเงินและทางการ จุดอ่อนในการจัดการมีเพียงเล็กน้อย และไม่มีนัยสำคัญ สามารถจัดการได้โดยคณะกรรมการและผู้บริหาร)	ค่อนข้างดี (อธิบาย : จุดอ่อนในการจัดการมีบ้าง แต่ไม่มีนัยสำคัญ แต่สามารถจัดการได้โดยคณะกรรมการและผู้บริหาร)	พอใช้ (อธิบาย : อยู่ในเกณฑ์ที่ต้องให้ความเอาใจใส่ ข้อบกพร่องหรือจุดอ่อนต่างๆ ที่พบด้านการจัดการมีพอสมควร แต่ไม่รุนแรงเท่าอันดับ 4 และ 5)	ค่อนข้างอ่อน (อธิบาย : ไม่มั่นคงและไม่ปลอดภัย ผลการจัดการไม่เป็นที่น่าพอใจ เนื่องจากมีข้อบกพร่องหรือจุดอ่อนเกี่ยวกับการจัดการอย่างร้ายแรง)	อ่อน (อธิบาย : ไม่มั่นคงและปลอดภัยเป็นอย่างยิ่ง ผลการจัดการอ่อนมาก ปริมาณและความรุนแรงของปัญหาอยู่เหนือความสามารถในการควบคุมหรือแก้ไขของฝ่ายบริหาร)

หัวข้อ	อันดับ 1	อันดับ 2	อันดับ 3	อันดับ 4	อันดับ 5
การปฏิบัติงานด้าน IT - การรักษาความปลอดภัย - ความถูกต้องเชื่อถือได้ของข้อมูล - ความพร้อมใช้งาน	มีประสิทธิภาพดีทุกด้าน (อธิบาย: มีการไม่ปฏิบัติตามนโยบายและระเบียบขั้นตอนภายในที่กำหนดเพียงเล็กน้อยไม่มีนัยสำคัญ)	มีประสิทธิภาพดี (อธิบาย : มีข้อบกพร่องในการปฏิบัติตามนโยบายและระเบียบขั้นตอนภายในที่ไม่รุนแรงสามารถแก้ไขได้ในการดำเนินงานปกติ)	ประสิทธิภาพพอใช้ (อธิบาย: มีข้อบกพร่องในการปฏิบัติตามนโยบายและระเบียบขั้นตอนภายในที่ค่อนข้างมากและมีนัยสำคัญที่ฝ่ายบริหารต้องติดตามดูแลโดยใกล้ชิด)	ประสิทธิภาพค่อนข้างอ่อน (อธิบาย: มีข้อบกพร่องในการปฏิบัติงานจำนวนมากขาดระเบียบหลักเกณฑ์ในการปฏิบัติงานไม่มีการติดตามดูแลเอาใจใส่จากฝ่ายบริหารเท่าที่ควร)	ประสิทธิภาพอ่อน (อธิบาย: การปฏิบัติงานบกพร่องอย่างร้ายแรงมีผลกระทบต่อความมั่นคงและปลอดภัยขององค์กรฝ่ายบริหารมิได้สนใจดำเนินการแก้ไขปัญหาที่เกิดขึ้น)

6. ความหมายของอันดับความเสี่ยงโดยรวม

ความเสี่ยงรวม เท่ากับ 1

สถาบันการเงินและหรือหน่วยงานผู้ให้บริการภายนอกที่ได้รับการจัดอันดับเป็น "1" ต้องแสดงให้เห็นถึงความเข้มแข็งในด้านการปฏิบัติงานในทุกๆด้าน และโดยทั่วไปแล้วจะต้องมีส่วนประกอบเป็น 1 หรือ 2 การมีจุดอ่อนต่างๆในด้าน IT ต้องมีลักษณะเป็นเรื่องเล็กๆ ที่สามารถแก้ไขได้ง่าย ๆ ในระหว่างเวลาดำเนินธุรกิจตามปกติ กระบวนการในการบริหารความเสี่ยงที่จะช่วยให้เกิดแผนการดำเนินงานที่ครอบคลุมในการระบุและตรวจสอบความเสี่ยงที่มีความสัมพันธ์กับขนาด ความสลับซับซ้อน และประวัติของความเสี่ยงของหน่วยงาน และควรที่จะมีแผนกลยุทธ์ต่าง ๆ ที่ได้ระบุรายละเอียดไว้อย่างดีและมีความสัมพันธ์กันทั้งองค์กร ซึ่งจะช่วยให้ผู้บริหารสามารถปรับตัวเข้ากันได้อย่างรวดเร็วในการเปลี่ยนแปลงของตลาด การดำเนินธุรกิจและการใช้เทคโนโลยีสารสนเทศที่องค์กรมีความต้องการ นอกจากนี้ฝ่ายจัดการต้องสามารถที่จะระบุจุดอ่อนได้อย่างรวดเร็วและสามารถดำเนินมาตรการในการแก้ไขข้อผิดพลาดได้อย่างเหมาะสม เพื่อเป็นการแก้ไขประเด็นที่พบจากการตรวจสอบและการกำกับดูแลประกอบกับสถานะทางการเงินของผู้ให้บริการหรือหน่วยงานผู้ให้บริการภายนอกจะต้องเข้มแข็งและมีผลการปฏิบัติงานโดยรวมที่ไม่มีสัญญาณอะไรที่จะทำให้หน่วยงานผู้ทำหน้าที่กำกับดูแลต้องวิตกกังวล

ความเสี่ยงรวม เท่ากับ 2

สถาบันการเงินและหน่วยงานผู้ให้บริการภายนอกที่ได้รับการจัดอันดับเป็น "2" ต้องแสดงให้เห็นถึงความปลอดภัยและความสามารถในการดำเนินงานในระดับที่ดีแต่อาจจะมีความบกพร่องในระดับปานกลางในเรื่องการปฏิบัติงานประจำวัน การควบคุมความเสี่ยง และกระบวนการบริหารหรือการพัฒนาระบบงาน ทั้งนี้ ผู้บริหารระดับสูงของสถาบันการเงินต้องสามารถแก้ไขจุดอ่อนต่าง ๆ ได้ในระหว่างเวลาดำเนินธุรกิจตามปกติ และมีกระบวนการในการบริหารความเสี่ยงที่เพียงพอในการระบุและตรวจตราความเสี่ยงที่มีความสัมพันธ์กับขนาด ความสลับซับซ้อน และประวัติของความเสี่ยงของหน่วยงาน มีการกำหนดแผนกลยุทธ์ต่างๆ แต่อาจจะต้องการรายละเอียดเพิ่มเติม หรือต้องการความร่วมมือและการสื่อสารภายในองค์กรให้มากขึ้น ดังนั้น แม้ว่าผู้บริหารจะมีวิสัยทัศน์แต่การปรับตัวขององค์กรต่อการเปลี่ยนแปลงของตลาด การดำเนินธุรกิจ และการใช้เทคโนโลยีทำได้ไม่ค่อยรวดเร็วนัก แต่อย่างไรก็ตาม ฝ่ายจัดการก็สามารถที่จะระบุจุดอ่อนและดำเนินการแก้ไขข้อผิดพลาดได้อย่างเหมาะสม ถึงแม้ว่าการแก้ไขส่วนใหญ่จะเกิดจากผลการตรวจสอบและการกำกับดูแลที่ระบุประเด็นปัญหาและแนวทางในการแก้ไขก็ตาม ทั้งนี้ ฐานะทางการเงินของหน่วยงานผู้ให้บริการภายนอกต้องอยู่ในสถานะที่ยอมรับได้และแม้ว่าจะมีจุดอ่อนในเรื่องการควบคุมภายในบ้างแต่ต้องไม่เป็นปัญหาในประเด็นที่สำคัญ ๆ หน่วยงานผู้ทำหน้าที่กำกับดูแลสามารถกำกับดูแลอย่างไม่

เป็นทางการและอยู่ในวงจำกัด

ความเสี่ยงรวม เท่ากับ 3

สถาบันการเงินและหน่วยงานผู้ให้บริการภายนอกที่ได้รับการจัดอันดับเป็น "3" แสดงให้เห็นถึงความวิตกกังวลของธนาคารแห่งประเทศไทยเกี่ยวกับจุดอ่อนของสถาบันการเงินที่มีตั้งแต่ระดับกลางจนถึงระดับสูง และถ้าความอ่อนแอของสถาบันการเงินยังคงดำรงอยู่ก็จะมีความเป็นไปได้ที่สถานะภาพและการดำเนินงานของสถาบันการเงินหรือหน่วยงานผู้ให้บริการภายนอกจะเสื่อมลงได้ ประกอบกับมีกระบวนการบริหารความเสี่ยงที่ไม่ค่อยมีประสิทธิผลที่จะใช้ในการระบุความเสี่ยงของสถาบันการเงินและอาจจะไม่เหมาะสมกับขนาด ความสลับซับซ้อน และประวัติของความเสี่ยงของหน่วยงาน แผนกลยุทธ์ต่าง ๆ ขององค์กรกำหนดไว้อย่างคลุมเครือและไม่สามารถระบุทิศทางของการริเริ่มนำ IT มาใช้ได้อย่างเหมาะสม ดังนั้น ฝ่ายจัดการจึงพบกับความยุ่งยากในการปรับตัวกับการเปลี่ยนแปลงของธุรกิจ ตลาด และเกี่ยวข้องกับเทคโนโลยีที่จำเป็นต่อองค์กร นอกจากนี้การปฏิบัติการเพื่อการประเมินความเสี่ยงด้วยตนเองค่อนข้างอ่อนและโดยทั่วไปจะเป็นปฏิกิริยาแบบตอบสนองต่อผลการตรวจสอบและการกำกับดูแล และมักจะมีปัญหาแบบเดิมเกิดขึ้นซ้ำ ๆ ซึ่งแสดงให้เห็นว่าฝ่ายจัดการอาจจะขาดความสามารถหรือขาดความตั้งใจที่จะแก้ปัญหาดังกล่าว ประกอบกับที่สถานะทางการเงินของหน่วยงานผู้ให้บริการภายนอกอาจจะไม่ดีและหรือมีแนวโน้มที่จะเป็นลบขณะที่ความล้มเหลวในด้านการเงิน หรือการดำเนินการไม่แน่ว่าจะเกิดขึ้น จึงยังมีความจำเป็นที่หน่วยงานผู้ทำหน้าที่กำกับดูแล จะต้องเพิ่มการกำกับดูแลมากขึ้น โดยอาจจำเป็นต้องใช้การตรวจสอบทั้งแบบเป็นทางการและไม่เป็นทางการเพื่อให้เกิดความมั่นใจว่ามีการดำเนินการปรับปรุงแก้ไขอย่างมีประสิทธิภาพ

ความเสี่ยงรวม เท่ากับ 4

สถาบันการเงินและหน่วยงานผู้ให้บริการภายนอกที่ได้รับการจัดอันดับเป็น "4" แสดงให้เห็นถึงความไม่ปลอดภัยหรือความไม่เหมาะสมของสภาพแวดล้อมในการดำเนินงานซึ่งอาจจะมีผลกระทบกับความอยู่รอดขององค์กรในอนาคตได้ ทั้งนี้ความอ่อนแอของการดำเนินงานนี้เป็นการชี้บอกให้เห็นถึงความบกพร่องอย่างรุนแรงของฝ่ายจัดการ ประกอบกับการที่องค์กรมีกระบวนการบริหารความเสี่ยงที่ไม่เพียงพอในการระบุและควบคุมความเสี่ยงตลอดจนการมีขั้นตอนการปฏิบัติที่ไม่เหมาะสมกับขนาด ความสลับซับซ้อน และประวัติของความเสี่ยงของหน่วยงาน นอกจากนี้ การจัดทำแผนกลยุทธ์ต่าง ๆ ยังไม่ดีพอ และไม่มีการประสานงานหรือการติดต่อสื่อสารให้ทั่วถึงภายในองค์กร เป็นผลให้ฝ่ายจัดการและคณะกรรมการมิได้รับมอบหมายหรืออาจไม่มีความสามารถที่จะทำให้เกิดความมั่นใจได้ว่าความจำเป็นเกี่ยวกับการใช้เทคโนโลยีขององค์กรจะถูกต้อง นอกจากนี้ฝ่ายจัดการก็มิได้ทำการประเมินความเสี่ยงด้วยตนเองและได้แสดงให้เห็นว่า

ไม่มีความสามารถหรือแสดงให้เห็นว่ามิได้เป็นใจที่จะแก้ไขปัญหาหรือข้อวิตกกังวลที่พบจากการตรวจสอบและการกำกับดูแล ประกอบกับการที่หน่วยงานผู้ให้บริการภายนอกมีสถานะทางการเงินที่กำลังตกต่ำอย่างรุนแรงและหรือกำลังเสื่อมลง อีกทั้งมีความเป็นไปได้ที่สถาบันการเงินหรือหน่วยงานผู้ให้บริการภายนอกจะประสบกับความล้มเหลวในการให้บริการถ้าปัญหาในเรื่อง IT ยังไม่ได้รับการแก้ไข ดังนั้น หน่วยงานผู้ทำหน้าที่กำกับดูแลจะต้องให้ความสนใจให้มากขึ้นและโดยส่วนมากแล้วมักจะได้รับมอบอำนาจให้ดำเนินมาตรการเพื่อการบังคับให้สถาบันการเงินหรือหน่วยงานผู้ให้บริการภายนอกดำเนินการแก้ไขปัญหาต่าง ๆ อย่างเป็นทางการด้วย

ความเสี่ยงรวม เท่ากับ 5

สถาบันการเงินและหน่วยงานผู้ให้บริการภายนอกที่ได้รับการจัดอันดับเป็น “5” แสดงให้เห็นถึงความบกพร่องอย่างร้ายแรงของการดำเนินงานซึ่งจำเป็นที่จะต้องปรับปรุงแก้ไขอย่างเร่งด่วนต่อไป ปัญหาต่าง ๆ ในการดำเนินงานและจุดอ่อนสำคัญต่างๆมีอยู่ทั่วไปทั้งองค์กร นอกจากนี้ องค์กรยังมีกระบวนการบริหารความเสี่ยงมีไม่เพียงพออย่างร้ายแรงจนแทบจะไม่สามารถช่วยให้ฝ่ายจัดการได้เห็นภาพของความเสี่ยงที่มีความสัมพันธ์กับขนาด ความสลับซับซ้อน และประวัติของความเสี่ยงขององค์กรได้ และองค์กรก็ไม่มีการจัดทำแผนกลยุทธ์หรือมีแต่ไม่ได้ผล ประกอบกับการที่ฝ่ายจัดการและคณะกรรมการแทบจะไม่ได้กำหนดทิศทางของการริเริ่มใช้ IT จึงเป็นสาเหตุให้ฝ่ายจัดการมิได้ตระหนักหรือมิได้ให้ความสนใจต่อความจำเป็นเกี่ยวกับการใช้เทคโนโลยีภายในองค์กร อนึ่ง ฝ่ายจัดการไม่ได้เต็มใจหรือไม่สามารถที่จะแก้ไขปัญหาหรือข้อวิตกกังวลต่าง ๆ ที่พบจากการตรวจสอบ และจากการกำกับดูแล อีกทั้งสถานะทางการเงินของหน่วยงานผู้ให้บริการภายนอกก็ย่ำแย่หรือมีความเป็นไปได้ที่จะล้มเหลวอันเนื่องมาจากผลการปฏิบัติงานที่ไม่ดีหรือความไม่มีเสถียรภาพทางการเงิน ดังนั้น หน่วยงานผู้ทำหน้าที่กำกับดูแลจึงมีความจำเป็นที่จะต้องเข้าไปกำกับดูแลอย่างต่อเนื่อง

7. สรุปการจัดอันดับสถาบันการเงินด้านเทคโนโลยีสารสนเทศโดยรวม

การให้อันดับความเสี่ยงโดยรวม (Risk Rating)	**ความหมายของอันดับที่จัด (Risk Definition)**
1 ดี	➢ การดำเนินงานด้าน IT มีความสมบูรณ์ดีในทุกๆด้าน ➢ ปัญหามีเพียงเล็กน้อยสามารถจัดการได้ในลักษณะที่เป็นงานประจำ ➢ ไม่จำเป็นต้องพึ่งพาการควบคุมจากทางการ
2 ค่อนข้างดี	➢ การดำเนินงานด้าน IT มีโครงสร้างพื้นฐานสมบูรณ์ ➢ จุดอ่อนที่ก่อให้เกิดความเสี่ยงอยู่ในระดับที่ไม่รุนแรง ➢ ปัญหาสามารถจัดการได้ในช่วงเวลาการดำเนินธุรกิจปกติ ➢ ทางการจะต้องเข้ามาควบคุมดูแลในระดับที่จำกัด
3 พอใช้	➢ การดำเนินงานด้าน IT มีข้อบกพร่องค่อนข้างมาก ➢ การจัดการความเสี่ยงยังไม่มีประสิทธิผล ➢ ต้องควบคุมดูแลจากทางการใกล้ชิดขึ้น ➢ สถานะทางการเงินที่เข้มแข็ง IT ล้มเหลวเป็นไปได้ยาก
4 ค่อนข้างอ่อน	➢ การดำเนินงานด้าน ITไม่สามารถยอมรับได้ ➢ การบริหารความเสี่ยงยังไม่เพียงพอ ➢ ความล้มเหลวทั้งด้านการเงินและการดำเนินธุรกรรมเป็นไปได้สูงในปัจจุบัน ➢ ทางการจะต้องเข้ามาควบคุมและดำเนินมาตรการแก้ไขในทันที
5 อ่อน	➢ การดำเนินงานด้าน IT มีจุดอ่อนจำนวนมาก ➢ การบริหารความเสี่ยงมีไม่เพียงพออย่างร้ายแรง ➢ มีแนวโน้มถึงจุดที่จะกระทบกับการดำเนินงานพื้นฐาน ➢ ทางการต้องเข้ามาควบคุมและดำเนินมาตรการแก้ไขในทันที และกำกับควบคุมอย่างต่อเนื่อง

ภาคผนวก

การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ธนาคาร…….....

การบรรยายสรุปและรายการขอเอกสาร

1. การบรรยายสรุปการดำเนินงาน และการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ:

- นโยบายและการบริหารจัดการด้านเทคโนโลยีสารสนเทศ (IT Management)
- การตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ
- ระบบข้อมูลเพื่อการบริหาร (MIS)
- การพัฒนาโครงการและระบบงานด้านเทคโนโลยีสารสนเทศ
- การว่าจ้างบุคคลภายนอกดำเนินงานด้านเทคโนโลยีสารสนเทศ (IT Outsourcing)
- การปฏิบัติงานและการสนับสนุนงานด้านเทคโนโลยีสารสนเทศ (IT Operation and Supporting)
- การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและ Electronic Banking

ขอให้ธนาคาร จัดบรรยายสรุปตามหัวข้อดังกล่าวข้างต้น โดยโปรดแจ้งให้ผู้ประสานงานของ ธปท. ทราบภายในวันที่ จักขอบคุณยิ่ง

2. รายการขอเอกสารประกอบการตรวจสอบ

การจัดการด้านเทคโนโลยีสารสนเทศ

1. แผนแม่บทด้านเทคโนโลยีสารสนเทศ (IT Master Plan)
2. ผังโครงสร้างองค์กรที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ
3. นโยบายและแผนกลยุทธ์การดำเนินงานด้านเทคโนโลยีสารสนเทศ
4. แผนงาน รายละเอียดโครงการ และงบประมาณปี …… ด้านเทคโนโลยีสารสนเทศ
5. รายงานการประชุมของคณะกรรมการบริหาร คณะกรรมการเทคโนโลยีสารสนเทศ คณะทำงานด้านเทคโนโลยีสารสนเทศ ปี …….
6. รายงานสรุปผลการดำเนินงานของสายงานเทคโนโลยีสารสนเทศ ปี ……..
7. นโยบาย คำสั่ง ระเบียบและวิธีปฏิบัติด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับ
   - 7.1 การบริหารโครงการ
   - 7.2 การพัฒนาโครงการและระบบงาน
   - 7.3 การปฏิบัติงานและการประมวลผล

7.4 Job Description ของฝ่ายงานต่างๆ

7.5 MIS, CIF, คลังข้อมูล (Data Warehouse)

7.6 การรักษาความปลอดภัย (Security Policy)

7.7 แผนฉุกเฉินและระบบคอมพิวเตอร์สำรอง

8. คู่มือปฏิบัติงานของระบบเงินฝาก สินเชื่อ บัตรเครดิต ATMและบริหารเงิน

9. รายละเอียดการฝึกอบรมพนักงานสายงานเทคโนโลยี สารสนเทศ ปี …….

10. ทะเบียนการรับแจ้งปัญหาของหน่วยงาน Help office ปี ……

การตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ

1. นโยบายและแผนการตรวจสอบ ประจำปี …..….. ด้านเทคโนโลยีสารสนเทศ และด้าน Internet Banking

2. รายงานสรุปผลการปฏิบัติงานของฝ่ายตรวจสอบระบบสารสนเทศประจำปี.....

3. คู่มือระเบียบปฏิบัติงานด้านการตรวจสอบเทคโนโลยีสารสนเทศ ขอบเขตและเทคนิคที่ใช้ในการตรวจสอบ

4. รายงานการตรวจสอบและกระดาษทำการของการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ ประจำปี ……

5. รายละเอียดการฝึกอบรมผู้ตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ ประจำปี ……

6. เอกสารการตรวจสอบด้านเทคโนโลยีสารสนเทศ และด้าน Internet Banking ของผู้สอบบัญชี หรือผู้ตรวจสอบภายนอกฉบับหลังสุด ประกอบด้วย

- สัญญาการว่าจ้าง
- แผนการตรวจสอบ
- ขอบเขตการตรวจสอบ
- รายงานผลการตรวจสอบ

7. แผนและผลการทดสอบระบบรักษาความปลอดภัยโดยผู้ตรวจสอบภายใน หรือผู้เชี่ยวชาญภายนอก

การพัฒนาโครงการและระบบงานด้านเทคโนโลยีสารสนเทศ

1. ระเบียบปฏิบัติงานการพัฒนาระบบงาน

2. รายงานผลการพัฒนาโครงการ ระบบงานและโปรแกรมที่เสนอธนาคาร ปี.....

3. ทะเบียนคุมรายงานที่ออกจากระบบงานต่าง ๆ (อาจจะระบุชื่อเฉพาะระบบงานที่ต้องการตรวจสอบก็ได้)

4. เอกสารที่ใช้ในขั้นตอนงานการพัฒนาโครงการ และกระบวนการ Change control

- Request /Requirement form
- Change document
- QA document
- Testing
- Move production
- Implement document
- Load document

5. เอกสาร System environment, System diagram, Data and Process diagram, User and System manual ประกอบระบบงาน

- Retail Banking, Deposit, Credit, Customer Information
- Internet, Web banking, Mobile banking, Front office intranet
- Corporate cash management
- Payment system, Financial EDI
- MIS, Data warehouse
- Workflow system, Centralized operations

การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

1. คู่มือปฏิบัติงาน Operation, Backup, Rerun-Recovery
2. เอกสาร และ Flow การปฏิบัติงานด้าน Computer operation
   - Check list, Data preparation, Data input, Job processing
   - Load module, Backup, Report, Maintenance
3. รายละเอียดการประกันภัยด้านเทคโนโลยีสารสนเทศ
4. ทะเบียนคุมทรัพย์สินอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์
5. คำสั่ง ระเบียบ วิธีปฏิบัติงานการประมวลผลข้อมูล
   - การปฏิบัติงานภายในศูนย์คอมพิวเตอร์
   - การซ่อมบำรุงเครื่องคอมพิวเตอร์และอุปกรณ์
6. สัญญาซื้อ สัญญาเช่า สัญญาบริการ และสัญญาซ่อมบำรุงระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายสื่อสาร

7. IT Infrastructure diagram, Computer system, Network System, Configuration Interface

8. ทะเบียน Media ชุดที่ใช้ประมวลผลและชุดสำรอง

9. Job scheduling ของแต่ละระบบงาน (อาจจะระบุชื่อเฉพาะระบบงานที่ต้องการตรวจสอบก็ได้)

10. Activity report, Administration report ของ Production system ณ วันที่.....

11. Backup report, Activity log ของ Production system ณ วันที่ …….

12. ทะเบียนบันทึกปัญหา และการแก้ไขปัญหาด้าน Operation, Network

13. รายชื่อพนักงานฝ่ายงานที่เป็น Administrator ของ Application ต่าง ๆ รวมถึงระเบียบวิธีปฏิบัติและการจัดการด้าน user, password

แผนฉุกเฉินและระบบคอมพิวเตอร์สำรอง

1. ขั้นตอนการปฏิบัติงานในกรณีที่เกิดเหตุฉุกเฉิน หรือเกิดเหตุขัดข้องในการปฏิบัติงานศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และด้านอาคารอุปกรณ์สนับสนุน

2. รายงานผลการทดสอบแผนฉุกเฉิน ระบบคอมพิวเตอร์สำรอง อุปกรณ์สนับสนุน และเอกสารประกอบการทดสอบ

Internet Banking

การจัดการ

1. Job Description ของฝ่ายและส่วนงานที่เกี่ยวข้องกับการให้บริการทางด้าน Internet Banking

2. นโยบายและแผนกลยุทธ์ทางด้าน Internet Banking

3. รายงานการประชุมคณะกรรมการและคณะทำงานที่เกี่ยวข้องกับการให้บริการ Internet Banking

4. ผลการประเมินความเสี่ยงและผลการสอบทานการทำธุรกรรม Internet Banking

5. ระเบียบและขั้นตอนการปฏิบัติงานเกี่ยวกับการออกผลิตภัณฑ์และบริการใหม่ การเสนอช่องทางให้บริการใหม่ รวมถึงการพิจารณาจัดซื้อ/จัดจ้าง

6. เอกสารเกี่ยวกับการออกผลิตภัณฑ์และบริการใหม่ แผนงานเชิงกลยุทธ์ และผลการศึกษาความเป็นไปได้ การวิเคราะห์ต้นทุนและประโยชน์ที่จะได้รับ (cost / benefit analysis) แผนทดสอบระบบและผลการทดสอบ แผนใช้งานจริง และผลจากการนำระบบไปใช้งานจริง (deployment plans and reviews)

7. รายงานที่ใช้วัดและวิเคราะห์ผลการดำเนินงานจริงเทียบกับเป้าหมายที่คาดคะเนไว้

8. ข้อมูลเกี่ยวกับคดีความอันสืบเนื่องมาจากการทำธุรกรรม Internet Banking ที่กำลังอยู่ระหว่างการดำเนินการและ/หรือดำเนินการเรียบร้อยแล้ว

9. เอกสารการฝึกอบรมและ/หรือพัฒนาพนักงานทางด้าน Internet Banking

การปฏิบัติงาน

1. รายละเอียด Internet Banking Platforms ที่ใช้ และ System Topology Maps ซึ่งครอบคลุมถึง server, routers, firewalls และองค์ประกอบอื่นๆของระบบงาน

2. รายงานติดตามการทำงานของระบบ Internet Banking เช่น ปริมาณธุรกรรม แนวโน้มการบุกรุกระบบงาน เป็นต้น

3. รายชื่อของผู้ใช้ระบบที่ได้รับอนุญาตและระดับการเข้าถึงระบบ (User Profile) ได้แก่ พนักงานเจ้าหน้าที่ของบริษัทภายนอก, ลูกค้า และกลุ่มผู้ใช้งานอื่น

4. รายงานกิจกรรมที่ต้องให้ความสนใจเป็นพิเศษ (Exceptional reports), ผลสอบทาน logs และรายชื่อพนักงานผู้สอบทานรายงานและเวลา

5. สำเนารายงานการติดตามวิเคราะห์รูปแบบพฤติกรรมของลูกค้าในการเข้าใช้บริการ Internet Banking

6. แฟ้มแสดงรายละเอียดการจัดซื้อโปรแกรมระบบงาน และ/หรือการจัดจ้างบริษัทผู้ให้บริการภายนอก (ประกอบด้วย สัญญาหรือข้อตกลงในการจัดซื้อ/จัดจ้าง บันทึกการประชุมคณะทำงานเอกสารการทำ due diligence review บริษัทผู้ให้บริการ คู่สัญญา บริษัทผู้แทนจำหน่ายระบบงาน และเอกสารประกอบอื่นๆที่ใช้ในกระบวนการจัดซื้อ/จัดจ้าง)

7. สัญญาการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่เกี่ยวข้องกับระบบงาน Internet Banking

3. การขอเอกสารเพิ่มเติม

ผู้ตรวจสอบอาจจำเป็นต้องขอเอกสารบางอย่างเพิ่มเติมนอกเหนือจากรายการขอเอกสารข้างต้น โดยจะแจ้งให้ทราบในระหว่างทำการตรวจสอบต่อไป

4. ผู้ประสานงานของ ธปท.

1…….. โทร. ……..

2…….. โทร. ……..