คู่มือตรวจสอบ

การจัดการ

(Management)

คำนำ

คู่มือตรวจสอบการจัดการ เป็นคู่มือฉบับหนึ่งในบรรดาคู่มือที่เป็นส่วนประกอบของคู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT) โดยคู่มือฉบับนี้จะมาทดแทนบทที่ 9 การจัดการและบทที่ 11 การสอบทานระบบข้อมูลสารสนเทศเพื่อการบริหาร ของคู่มือการตรวจสอบระบบข้อมูลสารสนเทศ ปี 2539 ของ FFIEC คู่มือฉบับนี้ได้ให้แนวทางสำหรับผู้ตรวจสอบและฝ่ายจัดการของสถาบันการเงิน ในการประเมินกระบวนการบริหารความเสี่ยงของสถาบันการเงิน เพื่อให้เกิดความมั่นใจในประสิทธิภาพของการบริหารงานด้าน IT

การบริหารงานด้าน IT อย่างมีประสิทธิภาพจะช่วยให้สถาบันการเงินได้รับประโยชน์สูงสุดจาก IT และสนับสนุนเป้าหมายและวัตถุประสงค์หลักขององค์กรได้ โดยมีสายงานด้าน IT เป็นผู้ดำเนินงานด้านปฏิบัติการ (back office) การจัดการเครือข่าย การพัฒนาและจัดหาระบบงาน ทั้งนี้ผู้บริหารสายงาน IT ทำหน้าที่สองประการ คือ การคัดเลือกเทคโนโลยีและการควบคุมการปฏิบัติงานประจำวัน เพื่อสนับสนุนการดำเนินงานธุรกิจหลักต่าง ๆ เช่น ระบบการให้สินเชื่อและจัดการสินทรัพย์เป็นต้น และการดำเนินกิจกรรม IT ทั้งองค์กร เช่น การรักษาความปลอดภัยและการดำเนินงานตามแผนการดำเนินธุรกิจอย่างต่อเนื่อง เป็นต้น และด้วยบทบาทของฝ่ายจัดการข้างต้นและการที่องค์กรจำเป็นต้องขยายการใช้ IT มากยิ่งขึ้น จึงทำให้การบริหารงานด้าน IT เป็นเรื่องที่มีความสำคัญมากในการกำกับดูแลกิจการตามหลักธรรมาภิบาล (corporate governance)

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ หวังว่าแนวทางการตรวจสอบในคู่มือฉบับนี้จะเป็นประโยชน์และช่วยพัฒนาการตรวจสอบให้มีประสิทธิภาพต่อไปในอนาคต

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ

ธันวาคม 2551

สารบัญ

หน้าที่

<u>ส่วนที่ 1</u> บทนำ

การบริหารงานด้าน IT มีผลกระทบที่สำคัญต่อผลประกอบการและความสำเร็จของสถาบันการเงิน ครอบคลุมไปถึงเรื่องการควบคุมต้นทุน และความเสี่ยงด้านปฏิบัติการ ดังนั้นสถาบันการเงินที่สามารถจัดการให้ระบบงานด้าน IT ของตนเองมีความสอดคล้องและสนับสนุนกลยุทธ์ทางธุรกิจได้ดี ก็จะช่วยเพิ่มมูลค่าให้แก่องค์กรและเสริมสร้างความสำเร็จขององค์กรได้อย่างยั่งยืน ดังนั้นคณะกรรมการสถาบันการเงินและฝ่ายจัดการควรจะต้องเข้าใจและรับผิดชอบในการกำกับและติดตามดูแลการบริหารจัดการด้าน IT ในฐานะที่เป็นปัจจัยที่มีความสำคัญอย่างมากของความพยายามในการบริหารธรรมาภิบาลในองค์กรที่ดี

อนึ่ง องค์กรธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (ITGI = The IT Governance Institute) ได้ให้คำนิยาม “ธรรมาภิบาลด้าน IT” ก็คือ องค์ประกอบของการกำกับดูแลองค์กรที่ดี รวมกับสภาวะของการเป็นผู้นำ การจัดโครงสร้างองค์กรและกระบวนการที่ช่วยให้ระบบงานด้าน IT สามารถควบคุมและส่งเสริมกลยุทธ์และเป้าหมายที่องค์กรตั้งไว้ได้ เนื่องจากว่าองค์กรจำเป็นต้องพึ่งพิง IT มากขึ้น ทำให้การบริหารงานด้าน IT อย่างมีประสิทธิภาพ มีผลกระทบต่อการบรรลุเป้าหมายที่สำคัญขององค์กร นอกจากนี้ สถาบันการเงินไม่สามารถแยกการบริหารงานด้าน IT ซึ่งมีความสำคัญมากขึ้น ในปัจจุบันนี้ ออกมาดำเนินการตามลำพัง แต่สถาบันการเงินจำเป็นต้องประสานการดำเนินงานตามแผนกลยุทธ์ด้าน IT ให้สอดคล้องกับเป้าหมายทางธุรกิจทุกด้าน เพื่อสนับสนุนให้สถาบันการเงินสามารถต่อสู้กับสิ่งท้าทายใหม่ ๆ ที่เกิดขึ้นในตลาดได้อย่างทันท่วงที

- IT กลายเป็นสิ่งจำเป็นพื้นฐานที่ต้องใช้กันทุกที่สำหรับทุกหน่วยธุรกิจขององค์กร
- สถาบันการเงินได้เชื่อมต่อระบบงานของตนเข้ากับระบบงานของลูกค้า ธุรกิจต่าง ๆ บุคคลที่สาม และสาธารณะชนทั่วไป
- IT ได้ก่อให้เกิดการพึ่งพาอาศัยกันระหว่างโครงสร้างพื้นฐานระบบงานต่าง ๆ เนื้อหาของข้อมูลบนเว็บ และกระบวนการตัดสินใจเพื่อสนับสนุนการส่งมอบผลิตภัณฑ์และบริการใหม่ให้แก่ลูกค้า
- ข้อมูลสารสนเทศที่ถูกต้องและทันเวลา มีบทบาทสำคัญต่อการดำเนินธุรกิจขององค์กร
- ภาคธุรกิจต่าง ๆ ต้องเผชิญกับการเปลี่ยนแปลงอย่างรวดเร็วทางด้าน IT ทำให้เกิด

ความต้องการการลงทุนใหม่ ๆ อย่างทันทีทันใด ทั้งด้านโครงสร้างพื้นฐาน ระบบปฏิบัติการและโปรแกรมระบบงานต่าง ๆ

- เทคโนโลยีใหม่ ๆ ทำให้องค์กรมีความจำเป็นที่จะต้องแสวงหาบุคลากรที่มีความรู้ความสามารถเข้ามาช่วยงาน ซึ่งก่อให้เกิดการแข่งขันในการแสวงหาผู้ที่มีความรู้ ความสามารถ ความชำนาญและทักษะต่าง ๆ ที่มีความจำเป็น

การบริหารงานด้าน IT ที่มีประสิทธิภาพสามารถสนันสนุนให้องค์กรมีโอกาสมากขึ้นในการต่อสู้กับปัญหาและอุปสรรคต่าง ๆ และช่วยให้สถาบันการเงินสามารถบริหารความเสี่ยงต่าง ๆได้ดียิ่งขึ้น ช่วยให้สถาบันการเงินสามารถนำเสนอผลิตภัณฑ์และบริการใหม่ ๆ แก่ลูกค้าได้ ช่วยเพิ่มประสิทธิภาพในการปฏิบัติงานและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน รวมทั้งช่วยให้สถาบันการเงินมีความพร้อมสำหรับการแข่งขันในอนาคตข้างหน้า ดังนั้น คณะกรรมการสถาบันการเงินและฝ่ายจัดการจึงควรมีความเข้าใจว่าเทคโนโลยีใหม่ ๆ และการเปลี่ยนแปลงของ IT ช่วยเร่งให้ความเสี่ยงด้านปฏิบัติการเดิม ๆ เพิ่มมากขึ้น หรือก่อให้เกิดความเสี่ยงด้านปฏิบัติการใหม่ ๆ ได้แก่ ความเสี่ยงที่เกิดจากการเชื่อมต่อระบบงานของสถาบันการเงินเข้ากับระบบงานภายนอกองค์กร การใช้บริการจากบุคคลที่สาม การทำธุรกิจพาณิชย์อิเล็กทรอนิกส์ และการทำธุรกิจระบบการชำระเงินรูปแบบใหม่ ซึ่งเกี่ยวข้องกับความเสี่ยงในการรักษาความลับ ความถูกต้องเชื่อถือได้ และความพร้อมใช้งานของระบบและข้อมูล นอกจากนี้ การเปลี่ยนแปลงด้าน IT ยังก่อให้เกิดความเสี่ยงด้านชื่อเสียงและกฎหมายอีกด้วย เพราะฉะนั้น การบริหารงานด้าน IT ที่ดี จึงเป็นองค์ประกอบที่สำคัญของการมีธรรมาภิบาลที่ดีและการจัดการความเสี่ยงด้านปฏิบัติการที่ดีขององค์กรอีกด้วย

คู่มือฉบับนี้ประกอบด้วยสี่ส่วน ส่วนแรกเป็นเรื่องความสัมพันธ์ระหว่างการบริหารงานด้าน IT กับความเสี่ยงด้านปฏิบัติการและความเสี่ยงด้านอื่น ส่วนที่สองเป็นเรื่องปัญหาหลักในการกำกับดูแลด้าน IT ส่วนที่สามเป็นเรื่องกระบวนการจัดการ IT ที่เกี่ยวข้องกับความเสี่ยง ส่วนที่สี่เป็นเรื่องแนวทางเพิ่มเติมสำหรับผู้ให้บริการด้าน IT แก่สถาบันการเงิน

<u>ส่วนที่ 2</u> แนวทางที่พึงปฏิบัติ

2.1 ภาพรวมของความเสี่ยง

2.1.1 ความเสี่ยงด้านปฏิบัติการและความเสี่ยงจากการดำเนินธุรกรรม

แม้ว่าฝ่ายจัดการจำเป็นต้องตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นทุกรูปแบบ แต่ความเสี่ยงด้านปฏิบัติการ หรืออาจเรียกอีกชื่อหนึ่งว่าความเสี่ยงจากการทำรายการธุรกรรม ก็เป็นความเสี่ยงหลักที่เกี่ยวข้องโดยตรงกับการใช้ IT ความเสี่ยงด้านปฏิบัติการนี้เกิดขึ้นได้กับทุกสายงาน มีสาเหตุหลักมาจากกระบวนการปฏิบัติงาน บุคลากรหรือระบบงานที่ไม่เหมาะสมหรือการปฏิบัติงานผิดพลาด หรือการทุจริต รวมถึงเหตุการณ์หรือปัจจัยภายนอก จนทำให้เกิดความเสียหายทางการเงิน

ความเสี่ยงด้านปฏิบัติการเป็นความเสี่ยงที่เกิดจากการทุจริตหรือความผิดพลาด หรือความไม่เพียงพอของกระบวนการทำงาน พนักงาน ระบบงาน หรือระบบเทคโนโลยีสารสนเทศ และเหตุการณ์หรือปัจจัยภายนอก อาจมีสาเหตุมาจากการที่ฝ่ายจัดการไม่สามารถรักษาศักยภาพในการแข่งขัน การบริหารจัดการข้อมูลสารสนเทศ หรือการส่งมอบผลิตภัณฑ์และบริการ จนก่อให้เกิดความเสี่ยงด้านปฏิบัติการใหม่ๆ หรือผลรวมของความเสี่ยงที่สูงขึ้นได้ นอกจากนี้ การด้อยประสิทธิภาพในการบริหารความเสี่ยงด้านปฏิบัติการยังส่งผลให้เกิดผลขาดทุนจำนวนมากจากภัยคุกคามด้าน IT จากการหยุดชะงักของการให้บริการหรือจากการดำเนินงานตามแนวทางการดำเนินธุรกิจที่ไม่เหมาะสม

สถาบันการเงินควรจัดให้มีระบบการระบุประเภท ประเมิน เฝ้าติดตามดูแลควบคุม และรายงานความเสี่ยงด้านปฏิบัติการที่เหมาะสม อนึ่ง ฝ่ายจัดการควรจะต้องแยกแยะองค์ประกอบของความเสี่ยงด้านปฏิบัติการออกไปจากความเสี่ยงประเภทอื่น ๆให้ชัดเจน เพื่อให้สามารถมุ่งเน้นไปที่การลดความเสี่ยงด้านปฏิบัติการ และคณะกรรมการสถาบันการเงินควรจัดให้มีแผนงานในการจัดการและเฝ้าติดตามดูแลความเสี่ยงชนิดนี้ แต่ต้องเป็นแผนงานที่มีรายละเอียดที่ครอบคลุมไปถึงความสามารถในการรองรับความเสี่ยงของสถาบันการเงิน ประสิทธิภาพของการควบคุมภายใน หน้าที่และความรับผิดชอบของฝ่ายจัดการในการบรรเทาความเสี่ยง รวมทั้งกระบวนการที่จำเป็นเพื่อการบริหารจัดการงานด้าน IT อย่างมีประสิทธิภาพ

ความเสี่ยงด้านปฏิบัติการไม่ได้จำกัดเฉพาะในงานด้าน back office และการประมวลผลรายการธุรกรรมต่าง ๆ เท่านั้น แต่ยังรวมไปถึงงานการให้บริการลูกค้า การพัฒนาและการสนับสนุนระบบการควบคุมภายใน ขั้นตอนในการดำเนินงานและการวางแผนจัดการทรัพยากรและอัตรากำลัง

ความเสี่ยงด้านปฏิบัติการของระบบงานด้าน IT ยังมีผลกระทบไปถึงความเสี่ยงด้านการให้สินเชื่อ ด้านการปฏิบัติตามกฎระเบียบของทางการ ด้านกลยุทธ์ ด้านการรักษาชื่อเสียงและด้านตลาด ดังนั้น ฝ่ายจัดการพึงต้องตระหนักถึงความเกี่ยวข้องระหว่างความเสี่ยงด้านปฏิบัติการของระบบงาน IT กับความเสี่ยงประเภทอื่น ๆ ดังต่อไปนี้

- ความเสี่ยงด้านสภาพคล่อง อัตราดอกเบี้ยและราคา ความเสี่ยงด้านสินเชื่อและความเสี่ยงด้านตลาดที่ชัดเจน มักจะเกิดจากการเปลี่ยนแปลงปัจจัยภายนอกของตลาดอุตสาหกรรมหรือลูกค้าเฉพาะราย ดังนั้น ระบบการควบคุมภายในที่ต้องพึ่งพิงอย่างมากจากความพร้อมใช้งานและประสิทธิภาพของระบบเทคโนโลยีสารสนเทศอาจจะทำให้ความเสี่ยงด้านปฏิบัติการเพิ่มสูงขึ้น ตัวอย่างเช่น ถ้าไม่มีกระบวนการเปลี่ยนแปลงวิธีการดำเนินงานที่เหมาะสม สำหรับการเสนอขายหลักทรัพย์ การจัดการด้านบัญชี หรือการรับชำระหนี้ ทำให้องค์กรขาดทุนจำนวนมากและทำให้ต้นทุนในการให้สินเชื่อและการรับชำระหนี้สูงขึ้น

- ความเสี่ยงด้านชื่อเสียง เกิดจากความผิดพลาด ความล่าช้าหรือการละเลยในการเลือกใช้เทคโนโลยี ซึ่งใช้กันทั่วไป และมีผลกระทบโดยตรงต่อพันธมิตรทางธุรกิจ ลูกค้า และผู้บริโภค ในลักษณะของการสูญเสียของข้อมูลความลับ (เกิดจากการเปิดเผยข้อมูลลับของลูกค้าโดยไม่ได้รับอนุญาตหรือการบุกรุก หรือดัดแปลงแก้ไขข้อมูลบนเว็บไซต์ของสถาบันการเงิน) จนทำให้ลูกค้าถอนเงินลงทุนออกไป

- ความเสี่ยงด้านกลยุทธ์ เกิดจากข้อมูลหรือการวิเคราะห์ที่ไม่ถูกต้องทำให้ฝ่ายจัดการตัดสินใจผิดพลาด ตัวอย่างเช่น ผู้บริหารระดับสูงด้าน IT อาจประหยัดเงินงบประมาณโดยการชะลอโครงการปรับปรุงประสิทธิภาพโครงสร้างพื้นฐานในการรับส่งข้อมูลบนเครือข่าย จนส่งผลให้สายงานธุรกิจสูญเสียส่วนแบ่งของตลาดไปจากการสูญเสียความสามารถในการแข่งขัน

- ความเสี่ยงด้านกฎหมาย เกิดจากการที่สถาบันการเงินไม่สามารถปฏิบัติตามกฎระเบียบหรือข้อบังคับของทางการ ในส่วนที่เกี่ยวข้องกับผลิตภัณฑ์และบริการด้าน IT ซึ่งอาจนำไปสู่ความผิดทางแพ่งหรืออาญาได้ ถ้าสถาบันการเงินเปิดเผยข้อมูลลับหรือให้ข้อมูลของลูกค้าแก่ทางการโดยที่ข้อมูลนั้นไม่ถูกต้อง ไม่ทันกาลหรือไม่เป็นไปตามหลักเกณฑ์หรือข้อบังคับของกฎหมาย

ผู้บริหารของหน่วยงาน IT ควรมีมุมมองในการใช้ IT ที่ครอบคลุมทั้งองค์กร และควรมีบทบาทอย่างมากในการกำหนดแผนกลยุทธ์เพื่อผสมผสาน IT เข้ากับเป้าหมายและกลยุทธ์ขององค์กร นอกจากนั้น ควรควบคุมการใช้ IT อย่างมีประสิทธิภาพทั่วทั้งองค์กร โดยผ่านวิธีการกำกับดูแลโดยตรงหรือผ่านกลไกการควบคุม IT ที่ฝากให้สายงานธุรกิจต่าง ๆ ดำเนินการแทน นอกจากนั้น ฝ่ายจัดการควร

ประเมินความเสี่ยงและพิจารณาวิธีการควบคุมและการบรรเทาความเสี่ยงต่าง ๆ และควรดำเนินการอย่างต่อเนื่องในการเปรียบเทียบความเสียหายจากความเสี่ยงกับมูลค่าการทำรายการธุรกรรมของธุรกิจ เพื่อหาระดับความเสี่ยงที่ยอมรับได้

2.2 บทบาทและความรับผิดชอบ

2.2.1 บทบาทด้านเทคโนโลยีสารสนเทศ

สรุปแนวทางการปฏิบัติ

คณะกรรมการสถาบันการเงินและฝ่ายจัดการ ควรกำกับดูแลงาน IT เพื่อให้มั่นใจว่า

- คณะกรรมการฯ ให้ความสำคัญ โดยการเข้ามามีส่วนร่วมและตระหนักรู้ถึงกิจกรรมด้าน IT
- เผยแพร่และบังคับใช้นโยบายและกระบวนการทำงานที่เหมาะสม
- จัดให้มีกระบวนการบริหารความเสี่ยงและการปรับปรุงแก้ไขที่มีประสิทธิภาพ
- สนับสนุนให้มีบุคลากรที่มีความสามารถให้เพียงพอต่อการปฏิบัติงาน และพัฒนาความสามารถของบุคลากรเหล่านั้น
- จัดให้มีระบบข้อมูลสารสนเทศเพื่อการบริหาร (MIS) ที่มีประสิทธิภาพ
- จัดให้มีการดำเนินงานให้เป็นไปตามกระบวนการบริหารโครงการที่ดี

(1) คณะกรรมการสถาบันการเงินและคณะกรรมการเทคโนโลยีสารสนเทศ

คณะกรรมการสถาบันการเงินมีหน้าที่ให้ความเห็นชอบแผนงาน นโยบายและค่าใช้จ่ายรายการใหญ่ที่เกี่ยวข้องกับงาน IT คณะกรรมการสถาบันการเงิน จึงควรมีความคุ้นเคยกับ IT ภาพรวมของศูนย์ประมวลผลข้อมูล (data center) และกิจกรรมต่าง ๆ ทางด้าน IT

คณะกรรมการสถาบันการเงินส่วนใหญ่จะมอบหมายหน้าที่การเฝ้าติดตามดูแลกิจกรรมด้าน IT ให้แก่คณะกรรมการบริหาร (senior management committee) หรือคณะกรรมการเทคโนโลยีสารสนเทศ (IT steering committee) ซึ่งทำหน้าที่ในการกำกับดูแลกิจกรรมที่เกี่ยวกับ IT ทั้งหมด ซึ่งประกอบไปด้วยสมาชิกซึ่งเป็นผู้บริหารระดับสูงจากหน่วยงาน IT และหน่วยงานธุรกิจหลัก อย่างไรก็ดี กรรมการแต่ละท่านไม่จำเป็นต้องมีตำแหน่งระดับหัวหน้าฝ่ายงาน แต่ควรเป็นผู้ที่มีความรู้ในนโยบาย วิธีการปฏิบัติ และขั้นตอนการดำเนินงานของสายงาน IT และควรได้รับมอบอำนาจให้ตัดสินใจ

ได้ภายใต้ขอบเขตของหน่วยงานที่ตนสังกัดอยู่ นอกจากนี้ ควรมีบุคลากรของสายงานบริหารความเสี่ยงทำหน้าที่ให้คำปรึกษาด้วย (ดูหน้า 9 เพิ่มเติม เรื่องหน้าที่การบริหารความเสี่ยง)

IT Steering Committee ควรรายงานให้คณะกรรมการสถาบันการเงินได้รับทราบถึงความคืบหน้าโดยภาพรวมของโครงการและประเด็นสำคัญต่าง ๆ ด้าน IT นอกจากนี้จะต้องให้ข้อมูลแก่คณะกรรมการสถาบันการเงินอย่างเพียงพอในการตัดสินใจเรื่องการปฏิบัติงานด้าน IT ทั้งนี้ คณะกรรมการสถาบันการเงินควรกำหนดบทบาท หน้าที่และความรับผิดชอบของ IT Steering Committee ไว้ในกฎบัตร (charter) และไม่จำเป็นต้องไปเกี่ยวข้องกับการปฏิบัติงานประจำวันเอง นอกจากบทบาทดังกล่าวแล้ว IT Steering Committee สามารถดำเนินการในเรื่องต่าง ๆ เพิ่มเติมได้ดังต่อไปนี้

- ควบคุมดูแล การพัฒนาและปรับปรุงแผนกลยุทธ์ด้าน IT
- อนุมัติการว่าจ้างผู้จำหน่ายสินค้าหรือบริการ (vendors) และติดตามฐานะทางการเงินของ vendors
- อนุมัติและติดตามโครงการใหญ่ งบประมาณ การจัดลำดับความสำคัญของงาน มาตรฐานการปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และผลการดำเนินงานทั้งหมด ด้านเทคโนโลยีสารสนเทศ
- ประสานงานระหว่างฝ่ายงาน IT และฝ่ายงานผู้ใช้งานในการจัดลำดับความสำคัญ ของงานต่างๆ
- สอบทานความเหมาะสมและเพียงพอในการจัดสรรทรัพยากรด้าน IT ทั้งด้านเงินลงทุน บุคลากร อุปกรณ์ และระดับของการให้บริการIT Steering Committee ควรที่จะได้รับข้อมูลเพื่อการบริหารจัดการจากฝ่ายงานด้าน IT ฝ่ายงานสายธุรกิจและฝ่ายงานตรวจสอบภายใน เพื่อประสานงานและเฝ้าติดตามดูแลการใช้ทรัพยากรด้าน IT ได้อย่างมีประสิทธิภาพ ติดตามดูแลว่าองค์กรได้ใช้วิธีการที่เหมาะสมในการทำงานให้บรรลุเป้าหมาย และควรจัดการประชุมและบันทึกผลการประชุมเกี่ยวกับผลการตัดสินใจของ IT Steering Committee เพื่อรายงานให้คณะกรรมการสถาบันการเงินได้รับทราบกิจกรรมที่ IT Steering Committee ได้ดำเนินการไปแล้ว

(2) ผู้บริหารระดับสูงด้านสารสนเทศ (CIO) และด้านเทคโนโลยี (CTO)

ผู้บริหารระดับสูงควรให้ความมั่นใจว่าระบบ IT สามารถตอบสนองความต้องการขององค์กรได้ และองค์กรก็ได้ปฏิบัติงานในแนวทางที่สอดคล้องกับนโยบายและแผนกลยุทธ์ที่คณะกรรมการสถาบันการเงินกำหนดขึ้นโดยเฉพาะในเรื่องของการจัดหาหรือพัฒนาระบบงาน IT โดย

มอบหมายให้ผู้จัดการฝ่ายอาวุโสหรือผู้บริหารสูงสุดของสายงาน IT (CIO : Chief Information Officer) เป็นผู้รับผิดชอบริเริ่มงานด้าน IT ที่สำคัญ ๆ เน้นไปที่ประเด็นปัญหาทางด้านกลยุทธ์และประสิทธิภาพโดยรวมของสายงาน IT และรับผิดชอบในการจัดทำแผนงบประมาณ ผลการปฏิบัติงาน การจัดหาระบบงาน การพัฒนาคุณภาพและฝึกอบรมบุคลากรของสายงาน IT รวมไปถึงการวางสถาปัตยกรรมทาง IT ตลอดจนการวางแผนกลยุทธ์และการใช้เงินลงทุน ดังนั้น CIO จึงควรดำรงตำแหน่งเป็นประธาน IT Steering Committee และกรรมการในคณะกรรมการบริหารงาน ซึ่งทำงานขึ้นตรงต่อกรรมการผู้จัดการใหญ่ และมีบทบาทสำคัญในการวางแผนกลยุทธ์ในการใช้ IT ไปพร้อม ๆ กับการสนับสนุนกิจกรรมของสายงานธุรกิจและมีส่วนร่วมในการตัดสินใจเรื่องสำคัญของสถาบันการเงิน

สถาบันการเงินบางแห่งอาจจะจ้างผู้บริหารระดับสูงด้าน IT (CTO : Chief Technology Officer) ซึ่งมีหน้าที่รายงานตรงต่อ CIO มาช่วยทำงานในขอบเขตที่แคบแต่มีความสำคัญและมีผลกระทบกับประสิทธิผลของสายงาน IT เช่น การติดตามความก้าวหน้าของ IT และการแสวงหาประโยชน์จากการลงทุนด้าน IT ให้มากที่สุด อย่างไรก็ดี สถาบันการเงินหลายแห่งได้ผนวกบทบาทของ CIO และ CTO เข้าด้วยกัน

(3) ผู้บริหารงานหลักด้านเทคโนโลยีสารสนเทศ (IT Line Management)

ผู้บริหารหน่วยงานหลักด้าน IT (IT Line Manager) เป็นตำแหน่งงานที่ทำงานขึ้นตรงต่อผู้บริหารระดับสูงของสายงาน IT มีบทบาทหน้าที่ในการกำกับดูแลทรัพยากรและกิจกรรมต่าง ๆ ด้าน IT ได้แก่ การวางแผนงาน ความคืบหน้าของโครงการและผลการปฏิบัติงานของระบบงานเฉพาะหรือฝ่ายงานที่ตนรับผิดชอบอยู่ ในหน่วยงานที่ดูแลเรื่อง data center หน่วยงานบริการเครือข่ายสื่อสาร หน่วยงานพัฒนาโปรแกรมระบบงาน (applications) หน่วยงานจัดการระบบปฏิบัติการ (system administration) หน่วยงานระบบสื่อสารระยะไกล (telecommunications) หน่วยงานบริการลูกค้า (customer support) อนึ่ง ผู้บริหารระดับหัวหน้างานชั้นต้น (front line manager) เหล่านี้มีหน้าที่ประสานงานกิจกรรมประจำวัน เฝ้าติดตามดูแลระบบงานที่ใช้งานในปัจจุบัน (production) ควบคุมการปฏิบัติงานให้เป็นไปตามตารางกำหนดเวลา และบังคับใช้นโยบายและระบบการควบคุมขององค์กรในเขตที่เขาเหล่านั้นรับผิดชอบอยู่

(4) ผู้บริหารงานหลักด้านธุรกิจ

ผู้บริหารหน่วยงานหลักด้านธุรกิจจากทุก ๆ สายงานธุรกิจ ต่างก็มีหน้าที่ความรับผิดชอบทางด้าน IT ดังตัวอย่างต่อไปนี้

- จัดเตรียมกระบวนการติดต่อสื่อสารให้ทราบถึงความต้องการทางธุรกิจและการปรับเปลี่ยนแผนกลยุทธ์อย่างต่อเนื่องทันต่อเหตุการณ์

- ระบุความต้องการด้าน MIS และแผนการพัฒนาผลิตภัณฑ์ รวมทั้งสื่อสารให้สายงานสนับสนุนด้าน IT หรือผู้บริหารสายงานหลัก IT รับทราบ เช่น การมีส่วนร่วมใน IT Steering Committee และคณะกรรมการด้าน IT เพื่อจัดระดับความสำคัญของงาน IT ให้เป็นไปตามความจำเป็นทางธุรกิจ เป็นต้น

- กำหนดขั้นตอนในการทดสอบการปฏิบัติตามนโยบายการควบคุมดูแลด้าน IT ภายในหน่วยงานธุรกิจ

- ดำเนินการให้เกิดความมั่นใจว่าองค์กรได้ให้ความสำคัญและให้เงินทุนในการพัฒนาด้าน IT ซึ่งสอดคล้องกับการพัฒนาแผนการดำเนินธุรกิจอย่างต่อเนื่อง

- สร้างความมั่นใจว่ามีการสำรองทรัพยากรด้าน IT ที่จำเป็นไว้ครบถ้วนแล้ว

- สร้างความมั่นใจว่ามีการเข้าร่วมในขั้นตอนของการทดสอบอย่างต่อเนื่อง

บทบาทเฉพาะของผู้บริหารหน่วยงานหลักด้าน IT และผู้บริหารหน่วยงานหลักด้านธุรกิจมีความแตกต่างกันไปตามประเภทของ IT วิธีการบริหารความเสี่ยง และการบังคับใช้นโยบายที่เกี่ยวข้องกับการบริหารความเสี่ยงของสถาบันการเงิน ซึ่งอาจจะใช้วิธีการบริหารจัดการแบบรวมศูนย์ (centralized) หรือกระจายศูนย์ (decentralized) ก็ได้

วิธีการบริหารจัดการแบบรวมศูนย์นั้น ผู้บริหารสายงาน IT จะทำหน้าที่ในการจัดหา การติดตั้งและการบำรุงรักษาด้าน IT เพื่อใช้งานทั่วทั้งองค์กรและสามารถควบคุมและเฝ้าติดตามผลการลงทุนด้าน IT ขององค์กรได้ดี และมีประสิทธิภาพในการปฏิบัติงานได้ดีกว่าวิธีอื่น โดยมีผู้บริหารของหน่วยงานธุรกิจทำหน้าที่บังคับใช้ระบบการควบคุมภายในต่าง ๆ ที่อยู่ในความรับผิดชอบของตน

ส่วนวิธีการบริหารจัดการแบบกระจายศูนย์นั้น ผู้บริหารสายงาน IT มีบทบาทเป็นเพียงผู้ให้คำแนะนำในการจัดหา การติดตั้ง และการบำรุงรักษาด้าน IT เฉพาะกับบางฝ่ายงานในองค์กรเท่านั้น **กระบวนการบริหารแบบนี้มักจะใช้กันแพร่หลายกับสถาบันการเงินที่มีความสลับซับซ้อนโดยการมอบหมายให้ฝ่ายงานต่างๆ ที่มีความสำคัญทางกลยุทธ์ เป็นผู้ที่ทำหน้าที่ในการตัดสินใจเกี่ยวกับการเลือกใช้ IT เพื่อเร่งรัดขั้นตอนในการจัดหาระบบงาน IT** โดยมีผู้บริหารของหน่วยงานธุรกิจทำหน้าที่รับผิดชอบมากกว่าในการส่งเสริมความเชื่อมั่นการลงทุนด้าน IT ให้สัมพันธ์กับแผนกลยุทธ์ต่างๆ ขององค์กร อนึ่ง กระบวนการบริหารในรูปแบบนี้จะทำให้องค์กรประสบกับปัญหาสำคัญในการควบคุมให้ระบบงานด้าน IT ภายในองค์กรทั้งหมดให้สามารถทำงานและสื่อสารร่วมกันได้ และการบังคับใช้

นโยบายขององค์กร โดยมีผู้บริหารสายงาน IT ทำหน้าที่รับผิดชอบสารสนเทศข้อบังคับในการควบคุมต่างๆ ขององค์กร อย่างไรก็ดี **การบังคับใช้ข้อกำหนดต่าง ๆ ทำได้ยากมากเมื่อเปรียบเทียบกับวิธีการบริหารจัดการแบบรวมศูนย์**

2.2.2 ความรับผิดชอบและการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

สรุปแนวทางการปฏิบัติ

สถาบันการเงินควรดำเนินมาตรการต่างๆ เพื่อให้เกิดความมั่นใจว่าได้**มีการกำหนดหน้าที่ความรับผิดชอบและสิ่งที่คาดหวังไว้อย่างชัดเจนระหว่างภาระหน้าที่ด้านการบริหารความเสี่ยงและหน้าที่การปฏิบัติงานด้าน IT** ที่สำคัญ ดังนี้

- หน้าที่การบริหารความเสี่ยง ซึ่งประกอบไปด้วยงานการตรวจสอบด้านIT การรักษาความปลอดภัยด้านข้อมูลสารสนเทศ แผนการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) การจ้างบุคคลภายนอก (IT Outsourcing) และการปฏิบัติตามกฎหมายและกฎเกณฑ์ต่าง ๆ
- หน้าที่การปฏิบัติงานด้าน IT ซึ่งประกอบไปด้วยงานด้านการบริหารโครงการ ทรัพยากรบุคคล การปฏิบัติงานและระบบสารสนเทศเพื่อการบริหาร

(1) หน้าที่การบริหารความเสี่ยง

สถาบันการเงินควรกำหนดให้**มีโครงสร้างการบริหารความเสี่ยงที่เหมาะสมขึ้นภายในองค์กร** ทั้งนี้บางองค์กรได้มีการแยกจัดตั้งสายงานบริหารความเสี่ยงขึ้นมาโดยเฉพาะเพื่อทำหน้าที่กำกับดูแลการรักษาความปลอดภัยของข้อมูลสารสนเทศ แผนการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) การตรวจสอบภายใน การประกันภัย **และการปฏิบัติตามกฎระเบียบข้อบังคับของทางการ** อนึ่งเพราะว่าการปฏิบัติหน้าที่การบริหารความเสี่ยงเหล่านี้จะเป็นกุญแจสำคัญในการประเมินวัดผล เฝ้าติดตามดูแลและควบคุมความเสี่ยง องค์กรจึงควรกำหนดให้มีสายงานการบังคับบัญชาที่เอื้อต่อการบังคับใช้และติดตามมาตรการการควบคุมต่าง ๆ อย่างจริงจังโดยไม่ถูกจำกัดโดยรูปแบบโครงสร้างที่มีอยู่

(2) การรักษาความปลอดภัยของข้อมูลสารสนเทศ

คณะกรรมการสถาบันการเงินมีหน้าที่กำกับดูแลและให้ความเห็นชอบเรื่องโปรแกรมการรักษาความปลอดภัยของข้อมูลสารสนเทศที่กำหนดขึ้นเป็นลายลักษณ์อักษร รวมถึงการพัฒนา การนำไปใช้ปฏิบัติ และการบำรุงรักษาโปรแกรมดังกล่าว แผนงานการรักษาความปลอดภัยของข้อมูลสารสนเทศ ควรครอบคลุมไปถึงการบริหารและการจัดการที่เหมาะสม การจัดการเชิงเทคนิคและ

ทางกายภาพตามขนาดขององค์กร ความสลับซับซ้อน ลักษณะทั่วไปของสภาพแวดล้อม และขอบเขตของการปฏิบัติงานขององค์กร คณะกรรมการสถาบันการเงินอาจมอบหมายงานในการเฝ้าติดตามดูแลความปลอดภัยของข้อมูลให้กับหน่วยงานตรวจสอบอิสระและสามารถมอบหมายงานการบริหารความปลอดภัยของข้อมูลให้กับผู้บริหารระบบรักษาความปลอดภัยอิสระ **อนึ่ง ภาพในอุดมคติที่ควรเป็นก็คือ องค์กรควรแยกหน้าที่การบริหารความปลอดภัยของข้อมูลและการเฝ้าติดตามดูแลความปลอดภัยของข้อมูลออกจากหน้าที่ในการดูแลระบบรักษาความปลอดภัยในการปฏิบัติงานด้าน IT ประจำวัน** และ **ผู้จัดการฝ่ายอาวุโสด้านการรักษาความปลอดภัยของข้อมูล ควรทำหน้าที่รับผิดชอบการบริหารความเสี่ยงในภาพกว้างของทั้งองค์กร**มากกว่าการมุ่งดูแลความปลอดภัยของทรัพยากรที่ใช้สำหรับการปฏิบัติงานด้าน IT ประจำวันเท่านั้น และ**ควรทำงานอย่างอิสระขึ้นตรงต่อคณะกรรมการสถาบันการเงินหรือฝ่ายจัดการมากกว่าการรายงานขึ้นตรงต่อสายงาน IT** อนึ่ง **สายงาน IT เองก็มีความจำเป็นต้องมีบุคลากรที่ทำหน้าที่รับผิดชอบต่อการนำเอานโยบายการรักษาความปลอดภัยขององค์กรมาปฏิบัติแต่ต้องไม่มีอำนาจหน้าที่ในการเปลี่ยนแปลงนโยบายและไม่ควรมีสิทธิในการอนุมัติการปฏิบัติงานที่ไม่เป็นไปตามขั้นตอนการปฏิบัติงานตามปกติ (exceptions)** ควรศึกษารายละเอียดในการรักษาความปลอดภัยเพิ่มเติมจากคู่มือตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล

(3) การดำเนินธุรกิจอย่างต่อเนื่อง (business continuity)

เช่นเดียวกับการรักษาความปลอดภัยของข้อมูลสารสนเทศ **การจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ควรเป็นกลยุทธ์ระดับกว้างของทั้งองค์กร** และสถาบันการเงินควรกำหนดหน่วยงานที่รับผิดชอบ เช่น หน่วยงานบริหารความเสี่ยง เป็นต้น และสถาบันการเงินควรทำการประเมินแผนการดำเนินธุรกิจอย่างต่อเนื่องของทุก ๆ สายงานธุรกิจหลักไปพร้อม ๆ กัน โดยเฉพาะสายงาน IT ควรจัดให้มีคนรับผิดชอบในการการพัฒนาและปรับปรุงแผนการดำเนินธุรกิจอย่างต่อเนื่องของสายงานให้ทันสมัยอยู่เสมอ ควรอ่านรายละเอียดเพิ่มเติมในคู่มือตรวจสอบการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

(4) การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ผู้บริหารระดับสูงและคณะกรรมการสถาบันการเงินควรทำให้เกิดความมั่นใจได้ว่าจะมีการประสานงานกันระหว่างฝ่ายจัดการและฝ่ายตรวจสอบด้าน IT และมีการตอบสนองที่รวดเร็วและถูกต้องต่อปัญหาหรือประเด็นที่พบจากการตรวจสอบ นอกจากนี้ผู้บริหารฝ่ายตรวจสอบ IT ควรรายงานผลการตรวจสอบโดยตรงต่อคณะกรรมการสถาบันการเงิน (ซึ่งรับผิดชอบในการกำกับดูแลและพิจารณาค่าตอบแทนของฝ่ายตรวจสอบฯ) หรือคณะกรรมการชุดอื่นๆ ซึ่งมีสมาชิกประกอบไปด้วย

กรรมการอิสระจากภายนอกองค์กรก็ได้ สำหรับ**บทบาทหลักของฝ่ายตรวจสอบ คือ การสอบทานความเสี่ยงที่เกิดขึ้นในฝ่ายงานต่างๆ และสอบทานว่าฝ่ายจัดการได้กำหนดให้มีกระบวนการควบคุมที่มีประสิทธิภาพแต่จะต้องไม่มีบทบาทใดๆ ในการติดตั้งระบบการควบคุมหรือบทบาทหลักในการบังคับใช้ระบบควบคุมตามนโยบายขององค์กร**

ฝ่ายจัดการควรกำหนดให้มีกระบวนการติดตามและบังคับใช้นโยบาย ในขณะที่ฝ่ายตรวจสอบภายในควรตรวจสอบความมีประสิทธิภาพของกระบวนการควบคุมภายในและรายงานผลให้กับคณะกรรมการสถาบันการเงินทราบโดยตรง ทั้งนี้คณะกรรมการสถาบันการเงินหรือคณะกรรมการตรวจสอบควรดำเนินการให้มั่นใจว่าฝ่ายตรวจสอบภายในมีความเชี่ยวชาญตามความจำเป็น และขอบเขตของการตรวจสอบภายในมีความเหมาะสม ทันกาล และเป็นอิสระ ส่วนการตรวจสอบด้าน IT ควรครอบคลุมไปถึงการพัฒนาระบบและโครงการจัดหาทรัพยากรต่าง ๆ ควรอ่านรายละเอียดเพิ่มเติมในคู่มือตรวจสอบการตรวจสอบภายในและภายนอก

(5) การปฏิบัติตามกฎหมายระเบียบและข้อบังคับ

ผู้บริหารระดับสูงควร**สร้างความมั่นใจว่าพนักงานจากหน่วยงาน Compliance ได้เข้ามามีส่วนร่วมเสมอทุกครั้งที่มีการนำเอาระบบใหม่หรือซอฟต์แวร์ใหม่มาใช้** ทั้งนี้เพราะว่าการนำเอาระบบงานใหม่มาใช้หรือการเปลี่ยนแปลงระบบงานใด ๆ ก็ตามอาจจะนำไปสู่การปฏิบัติงานที่ไม่เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ เช่น การคำนวณอัตราดอกเบี้ยที่ผิดพลาด การเปิดเผยข้อมูลอย่างไม่เหมาะสมหรือข้อมูลไม่ถูกต้องแม่นยำ การควบคุมรักษาความปลอดภัยในการเก็บรักษาหรือส่งผ่านข้อมูลของลูกค้าที่หละหลวมไม่รัดกุม และกระบวนการพิสูจน์ตัวตนของลูกค้าที่ด้อยประสิทธิภาพ ดังนั้น หน่วยงาน Compliance จึงควรสอบทานการเปลี่ยนแปลงของระบบหรือการเปลี่ยนแปลงใด ๆ เพื่อให้มีเกิดความมั่นใจว่ามีการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับ

(6) การบริหารโครงการ

การบริหารโครงการเป็นการประยุกต์ความรู้ ทักษะ เครื่องมือ และเทคนิค มาใช้ในกิจกรรมที่หลากหลายเพื่อให้เป็นไปตามข้อกำหนดของโครงการต่างๆ ขององค์กร ทั้งนี้ ผู้บริหารสายงาน IT จะมีหน้าที่และความรับผิดชอบอย่างกว้างๆ 2 ประการ คือ การควบคุมการปฏิบัติงานและบริการด้าน IT ให้ทุก ๆ สายงานธุรกิจต่าง ๆ และการกำกับดูแลการเปลี่ยนแปลงของ IT ที่ใช้ในกระบวนการปฏิบัติงานและขั้นตอนการดำเนินธุรกิจโดยกระบวนการบริหารโครงการซึ่งเป็นกุญแจสำคัญของการปฏิบัติงาน IT ที่ดี

สถาบันการเงินที่มีโครงสร้างองค์กรที่ซับซ้อนก่อให้เกิดความจำเป็นที่จะต้องมีกระบวนการบริหารโครงการที่เป็นรูปแบบมาตรฐานที่ชัดเจน คือ กระบวนการเริ่มต้นโครงการ การวางแผน การปฏิบัติการ การควบคุม และการปิดโครงการ เพื่อควบคุมโครงการจัดหาและพัฒนาระบบงาน และกิจกรรมอื่นๆ เช่น การโยกย้ายปรับเปลี่ยนระบบงานและข้อมูล (system conversions) การขยายศักยภาพของผลิตภัณฑ์ การปรับปรุงโครงสร้างพื้นฐานให้ทันสมัย และการบำรุงรักษาระบบงานให้ทันสมัยเป็นปัจจุบัน ทั้งนี้ ความสามารถของสถาบันการเงินในการบริหารโครงการเป็นปัจจัยสำคัญในการปรับเปลี่ยนความจำเป็นทางธุรกิจและเป้าหมายเชิงกลยุทธ์ขององค์กร

คณะผู้บริหารโครงการควรถ่วงดุลระหว่างการลงทุนด้วยเวลา เงิน และความเชี่ยวชาญ กับลำดับของความสำคัญของโครงการ ความเสี่ยง และข้อจำกัดต่างๆ ของโครงการ และควรควบคุมต้นทุนและการปฏิบัติให้เป็นไปตามมาตรฐานและข้อกำหนดทางเทคนิคต่างๆ โดยการใช้เทคนิคการบริหารที่ผ่านการพิสูจน์แล้วว่ามีประสิทธิภาพมาใช้ในการบริหารโครงการทุกขั้นตอน ทั้งนี้ การบริหารโครงการจำนวนมากๆ จำเป็นจะต้องมีองค์ประกอบ ดังต่อไปนี้

- การกำหนดวันแล้วเสร็จตามเป้าหมาย (target completion dates) ฝ่ายจัดการควรกำหนดวันแล้วเสร็จของแต่ละโครงการหรือแต่ละขั้นตอนของโครงการโดยใช้ความระมัดระวังในการระบุและประเมินความเสี่ยงที่มีนัยสำคัญทั้งหมด ทั้งนี้ การกำหนดวันแล้วเสร็จของงานแต่ละขั้นตอนทำให้ระบบการควบคุมโครงการได้รับการปรับปรุงให้ดีขึ้น

- การปรับข้อมูลสถานะของโครงการให้เป็นปัจจุบัน (project status updates) ฝ่ายจัดการควรเปรียบเทียบวันที่โครงการเสร็จจริงกับวันที่ที่ได้กำหนดไว้ตามเป้าหมาย และความก้าวหน้าของโครงการจริงเปรียบเทียบกับเป้าหมายเดิมทั้งด้านเวลาและค่าใช้จ่ายส่วนเกินจากที่เคยกำหนดไว้ (time and cost overruns) แต่ถ้าค่าใช้จ่ายในการพัฒนาสูงเกินกว่าที่กำหนดไว้เป็นจำนวนสูงมาก ฝ่ายจัดการจำเป็นต้องประเมินความคุ้มค่าของโครงการใหม่ หรือขออนุมัติในการจ่ายเงินลงทุนเพิ่มเติมต่อไปอีก

ฝ่ายบริหารควรออกแบบระบบข้อมูลสารสนเทศให้มีคุณสมบัติ ต่อไปนี้

- อำนวยความสะดวกในการบริหารธุรกิจ
- ช่วยสนับสนุนฝ่ายบริหารมีระบบช่วยในการตัดสินใจที่เพียงพอโดยการเสนอข้อมูลที่ทันเวลา มีความถูกต้อง มีความสม่ำเสมอ มีความสมบูรณ์ และเกี่ยวข้อง
- ผู้บริหารระดับสูงสนับสนุนให้มีการปฏิบัติงานอย่างเคร่งครัดตามขั้นตอนการบริหารโครงการที่ดี

- ผู้มีส่วนได้ส่วนเสียทุกฝ่ายงานและเจ้าหน้าที่สายงาน IT ร่วมกันกำหนดเป้าหมายหรือข้อกำหนดต่างๆของโครงการและร่วมกันรับผิดชอบในทุกขั้นตอนของการพัฒนาโครงการ

- การติดตามและวัดประสิทธิภาพของโครงการ โดยเทียบกับผลตอบแทนเป้าหมาย หรือข้อกำหนดต่าง ๆ ของโครงการ

- การกำหนดความเสี่ยงและการเฝ้าติดตามดูแลกระบวนการในการประเมินความเสี่ยงที่ครอบคลุมความเสี่ยงของโครงการทั้งหมดขององค์กร

- กระบวนการส่งมอบความเป็นเจ้าของโครงการจากทีมงานเดิมที่รับผิดชอบในการพัฒนาโครงการไปให้ทีมงานที่รับผิดชอบการปฏิบัติงานปกติประจำวัน พร้อมทั้งกระบวนการทดสอบและฝึกอบรมที่เพียงพอ

ผู้ตรวจสอบควรศึกษาหัวข้อดังกล่าวเพิ่มเติมจากคู่มือตรวจสอบการพัฒนาและการจัดหาระบบงานและโปรแกรม

(7) การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและงานสนับสนุนอื่น ๆ

(7.1) ทรัพยากรบุคคล

เป้าหมายของการบริหารทรัพยากรบุคคล คือ การว่าจ้างและรักษาไว้ซึ่งบุคลากรที่มีศักยภาพและมีแรงจูงใจในการทำงาน ดังนั้น องค์กรจึงควรมีแผนการบริหารบุคลากรด้าน IT ที่มีประสิทธิภาพซึ่งสามารถสนับสนุนงานทั้งด้าน IT และหน่วยงานธุรกิจผู้ใช้บริการ และผู้บริหารสายงาน IT ควรผนวกแผนการบริหารจัดการบุคลากรเข้ากับการวางแผนงานด้าน IT เพื่อให้มีการพัฒนาและมีความพร้อมใช้งานด้าน IT อย่างดีที่สุด

องค์ประกอบของกระบวนการบริหารทรัพยากรบุคคลที่มีประสิทธิภาพประกอบไปด้วย การวางแผนผลตอบแทน/รายได้ การประเมินประสิทธิภาพในการปฏิบัติงาน การมีส่วนร่วมการแสดงความคิดเห็นด้านเทคโนโลยีฯ กลไกในการถ่ายทอดความรู้ (อาทิ การหมุนเวียนงาน) การฝึกอบรม และการเฝ้าติดตามดูแลให้คำปรึกษา ทั้งนี้ คณะกรรมการบริหารควรกำหนดให้มีแผนงานเพื่อให้รางวัลแก่ผู้บริหารที่สามารถบรรลุเป้าหมายต่าง ๆ ด้าน IT เช่นเดียวกับการกำหนดแผนรางวัลสำหรับผู้บริหารระดับสูงของสายงานอื่น ๆ

สถาบันการเงินควรมีแผนงานเพื่อให้เกิดความมั่นใจว่าพนักงานมีความชำนาญและเชี่ยวชาญที่จำเป็นในการปฏิบัติงานเพียงพอที่จะบรรลุเป้าหมายและวัตถุประสงค์ขององค์กร อย่างไรก็ตาม องค์กรอาจจะยังมีความจำเป็นต้องใช้ผู้เชี่ยวชาญจากภายนอกมาช่วยปฏิบัติงานเฉพาะด้านเป็นบางกรณี

ฝ่ายจัดการควรพัฒนาโครงการฝึกอบรมเพื่อรองรับการปฏิบัติงานตามมาตรฐาน IT ใหม่ๆ และผลิตภัณฑ์ทุกประเภทก่อนนำออกมาใช้งานจริงในองค์กร โดยอาจจัดให้มีการออกประกาศนียบัตรรับรองให้แก่พนักงานที่ผ่านการฝึกอบรม เพื่อให้เกิดความมั่นใจว่าพนักงานมีความเชี่ยวชาญในการทำงานตามความจำเป็นในการดำเนินธุรกิจ

คณะกรรมการบริหารและผู้บริหารระดับสูงควรพิจารณาแผนการสืบทอดตำแหน่งหรือแผนการเปลี่ยนแปลงผู้บริหารและบุคลากรที่ทำหน้าที่ทางกลยุทธ์ที่สำคัญๆ โดยผ่านการดำเนินงานในเรื่องสำคัญต่าง ๆ คือ การจัดทำสัญญาจ้างงาน การพัฒนาแผนการดำเนินงานอย่างมืออาชีพ และแผนสำรองฉุกเฉินในการจัดหาผู้บริหารงานสำคัญฯ ให้ครอบคลุมไปถึงวิธีการลดความเสี่ยงในการสรรหาบุคลากรสำรองในตำแหน่งงานที่สำคัญ การฝึกอบรมบุคลากรให้สามารถปฏิบัติงานข้ามหน่วยงานกันได้ และการจัดหาผลิตภัณฑ์ทางการประกันภัยให้แก่พนักงานในตำแหน่งงานหลักต่าง ๆ เพื่อให้บรรลุวัตถุประสงค์หลักให้มีการเปลี่ยนแปลงตัวผู้บริหารระดับสูงหรือพนักงานปฏิบัติการของหน่วยงานสำคัญในสายงาน IT อย่างราบรื่น

(7.2) ระบบสารสนเทศเพื่อการบริหารและการรายงาน

สายงานด้าน IT มักจะมีบทบาทสำคัญในการสนับสนุนระบบข้อมูลสารสนเทศเพื่อการบริหาร (MIS) ซึ่งเป็นกระบวนการในการนำเสนอข้อมูลที่จำเป็นต่อการบริหารองค์กรอย่างมีประสิทธิภาพ อนึ่ง ระบบการรายงานข้อมูลเพื่อการบริหารให้กับผู้บริหารหลายๆ ระดับชั้นได้ทราบและใช้งานอย่างถูกต้องและทันกาลเป็นองค์ประกอบที่สำคัญของการบริหารและการจัดการองค์กรอย่างมีประสิทธิภาพในการสนับสนุนเป้าหมายและแผนกลยุทธ์ระยะยาวขององค์กร ทั้งนี้ **ผู้บริหารสายงาน IT จะต้องทำหน้าที่ในการกำหนดนโยบาย กระบวนงาน และการควบคุมระบบฐานข้อมูลและการจัดสร้างรายงานเพื่อให้เกิดความมั่นใจว่าองค์กรมีระบบข้อมูลสารสนเทศที่มีประสิทธิภาพและเป็นประโยชน์ต่อองค์กร**

ฝ่ายจัดการควรกำหนดรูปแบบของระบบข้อมูลสารสนเทศเพื่อให้ระบบข้อมูลนั้น

- ช่วยอำนวยความสะดวกให้ฝ่ายจัดการในการบริหารธุรกิจ
- ช่วยให้ฝ่ายบริหารมีระบบช่วยสนับสนุนการตัดสินใจที่เพียงพอโดยการจัดให้มีข้อมูลที่ทันกาล ถูกต้องแม่นยำ มีความต่อเนื่องราบรื่น ครบถ้วน สมบูรณ์และเกี่ยวข้องกับการตัดสินใจ
- ช่วยนำเสนอข้อมูลที่เกี่ยวข้องสัมพันธ์กันไปทั่วทั้งองค์กร

- ช่วยสนับสนุนเป้าหมายและทิศทางเชิงกลยุทธ์ขององค์กร
- ช่วยให้องค์กรมั่นใจได้ว่าจะมีข้อมูลที่ถูกต้องเชื่อถือได้ที่พร้อมใช้งานได้
- ช่วยให้มีระบบที่ไม่เอนเอียงในการบันทึกและเก็บรวบรวมข้อมูลข่าวสาร
- ช่วยลดค่าใช้จ่ายที่เกิดจากการใช้แรงงานจำนวนมากในการทำกิจกรรมด้วยมือ
- ช่วยส่งเสริมการติดต่อสื่อสารระหว่างพนักงาน

ระบบข้อมูลสารสนเทศเพื่อการบริหาร (MIS) จะให้ข้อเท็จจริงแก่ผู้ที่ทำหน้าที่ตัดสินใจสนับสนุนกระบวนการตัดสินใจ และเสริมสร้างประสิทธิภาพของการปฏิบัติงานทั่วทั้งองค์กร ทั้งนี้ ระบบ MIS ในระดับสูงจะให้ทั้งข้อมูลและข่าวสารสนเทศแก่คณะกรรมการบริหารและฝ่ายจัดการในการตัดสินใจเชิงกลยุทธ์ ส่วนในระดับต่ำลงมา ระบบ MIS จะช่วยให้ผู้บริหารสายงานต่าง ๆ สามารถเฝ้าติดตามดูแลกิจกรรมขององค์กรและช่วยแจกจ่ายข้อมูลข่าวสารไปสู่พนักงาน ลูกค้า และคณะผู้บริหาร

ความก้าวหน้าทาง IT ได้ช่วยเพิ่มปริมาณของข้อมูลข่าวสารให้แก่ฝ่ายจัดการเพื่อใช้ในการวางแผนและการตัดสินใจ แต่ในขณะเดียวกันก็เกิดความเสี่ยงจากการรายงานข้อมูลที่ไม่ถูกต้องก่อให้เกิดความผิดพลาดในการตัดสินใจ ทั้งนี้เพราะระบบจัดทำรายงานนั้นจำเป็นต้องอาศัยข้อมูลที่นำเข้าสู่ระบบงานด้วยมือ หรือข้อมูลที่ดึงออกมาจากระบบข้อมูลทางการเงิน หรือรายการธุรกรรมจากหลายๆ ระบบงานซึ่งมีโครงสร้างรูปแบบด้าน IT ที่แตกต่างกัน ดังนั้น ฝ่ายจัดการจะต้องสร้างความเชื่อมั่นให้ได้ว่ามีระบบการควบคุมต่างๆในการรักษาความสมบรูณ์ถูกต้องครบถ้วนของข้อมูลและมีสภาพแวดล้อมในการประมวลผลที่เหมาะสมเพียงพอ เพื่อให้ระบบ MIS มีข้อมูลที่ถูกต้องและเกี่ยวข้องสัมพันธ์กัน

หลักการพื้นฐานที่ดีในการทบทวนระบบสารสนเทศเพื่อการบริหาร ประกอบไปด้วยระบบควบคุมภายในต่างๆ กระบวนการในการปฏิบัติการ การเก็บรักษาทรัพย์สิน และการตรวจสอบที่ครอบคลุม

ระบบ MIS ที่สามารถจะนำมาใช้เป็นเครื่องมือตอบสนองให้ฝ่ายจัดการและพนักงานสามารถนำมาใช้งานได้อย่างมีประสิทธิภาพนั้น ประกอบไปด้วยองค์ประกอบของกิจกรรม **การประมวลผลข้อมูลด้าน IT ที่สำคัญ 5 ประการ คือ ความรวดเร็วทันกาล ความถูกต้องแม่นยำ ความสม่ำเสมอต่อเนื่อง ความสมบูรณ์ และความสัมพันธ์กันของข้อมูล** (ถ้าหากองค์ประกอบใดบกพร่องก็จะมีผลกระทบกับประโยชน์ใช้สอยของระบบสารสนเทศเพื่อการบริหาร)

- ความรวดเร็วทันกาล (timeliness) เพื่อสนับสนุนให้เกิดการตัดสินใจได้อย่างรวดเร็ว ระบบ MIS ขององค์กร จึงควรมีความสามารถในการให้และแจกจ่ายข้อมูลสารสนเทศที่เป็นปัจจุบันให้แก่ผู้ใช้งานที่เหมาะสม ดังนั้น ผู้พัฒนาระบบ MIS จะต้องออกแบบให้ระบบฯ มีความพร้อมใช้ในการออกรายงานได้อย่างรวดเร็ว สามารถจัดเก็บข้อมูลและการปรับปรุงแก้ไขได้รวดเร็ว และสามารถออกรายงานสรุปผลที่มีความหมายสามารถนำไปใช้ประโยชน์ได้

- ความเที่ยงตรงแม่นยำ (accuracy) ข้อมูลควรมีระบบควบคุมภายในที่ดีทั้งที่กระทำด้วยมือหรือควบคุมด้วยระบบอัตโนมัติ และข้อมูลสารสนเทศทั้งหมดจะต้องผ่านการตรวจเช็คการปรับปรุงให้เท่าเทียมกัน และผ่านการควบคุมของระบบควบคุมภายใน ทั้งนี้ กรรมการบริหารควรดำเนินการให้มีการตรวจสอบโดยผู้ตรวจสอบทั้งภายในและภายนอกองค์กรเข้ามาประเมินความเพียงพอของระบบควบคุมภายในด้วย

- ความสม่ำเสมอต่อเนื่อง (consistency) ข้อมูลควรจะถูกประมวลผลและถูกแปลให้เป็นภาษาเครื่องคอมพิวเตอร์อย่างสม่ำเสมอในรูปแบบเดียวกันเพื่อให้ข้อมูลมีความน่าเชื่อถือ ทั้งนี้ เพราะว่าการเปลี่ยนแปลงวิธีรวบรวมข้อมูลและวิธีรายงานผลอาจจะทำให้ข้อมูลผลการวิเคราะห์บิดเบือนไปจากข้อเท็จจริงได้ ดังนั้น ฝ่ายจัดการจึงควรกำหนดกระบวนการควบคุมการเปลี่ยนแปลงแก้ไขไว้เป็นลายลักษณ์อักษร จัดทำเอกสารประกอบการเปลี่ยนแปลง และสื่อสารให้พนักงานที่เกี่ยวข้องได้รับทราบ พร้อมกับจัดให้มีการเฝ้าติดตามดูแลการดำเนินงานอย่างมีประสิทธิภาพด้วย

- ความสมบูรณ์ (completeness) ผู้ทำหน้าที่ตัดสินใจต้องการได้รับข้อมูลในลักษณะของข้อสรุปผลที่สมบูรณ์ จึงควรทำหน้าที่เป็นผู้ออกแบบรายงานเพื่อหลีกเลี่ยงการจัดกลุ่มและข้อมูลที่มีรายละเอียดมากเกินไป

- ความสัมพันธ์กันของข้อมูล (relevance) ข้อมูลสารสนเทศจะด้อยคุณค่าไปทันที ถ้าข้อมูลไม่มีความเหมาะสม ไม่มีความจำเป็น หรือมีรายละเอียดมากเกินไปจนไม่สามารถนำมาใช้ในการตัดสินใจที่มีประสิทธิภาพได้ และระบบ MIS ควรมีระดับ ความละเอียดของข้อมูลและความสัมพันธ์กันของข้อมูลสัมพันธ์โดยตรงกับความจำเป็นต้องใช้ข้อมูลเพื่อการบริหารและปฏิบัติงานของกรรมการบริหาร คณะผู้บริหารระดับสูง ฝ่ายงานต่างๆ หรือผู้จัดการหน่วยงานระดับต้น

2.3 กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กระบวนการประเมินความเสี่ยงที่มีประสิทธิภาพมีผลต่อการลดความเสี่ยงผ่านทางกระบวนการควบคุมต่างๆ ด้าน IT ดังนั้น **ฝ่ายจัดการระดับสูงจึงควรกำหนด/ระบุ ตรวจวัด ควบคุม และ**

เฝ้าติดตามดูแลทางด้าน IT เพื่อหลีกเลี่ยงความเสี่ยงที่เป็นภัยคุกคามต่อความปลอดภัยและน่าเชื่อถือขององค์กร ผ่านกระบวนการ 4 อย่าง คือ

(1) การวางแผนการใช้ IT

(2) ประเมินความเสี่ยงที่เกิดจากการใช้ IT

(3) การเลือกวิธีการนำ IT มาใช้

(4) การตั้งกระบวนการในการตรวจวัดและเฝ้าติดตามความเสี่ยงที่กำลังเกิดขึ้น

นอกจากนี้ องค์กรควรกำหนดให้มีสิ่งต่าง ๆ ต่อไปนี้

- กระบวนการวางแผนที่มีประสิทธิภาพซึ่งประสานวัตถุประสงค์ด้าน IT เข้ากับวัตถุประสงค์เชิงธุรกิจ

- กระบวนการประเมินความเสี่ยงที่เกิดขึ้นอย่างต่อเนื่องซึ่งคำนึงถึงสภาพแวดล้อมและการเปลี่ยนแปลงที่มีแนวโน้มจะเกิดขึ้น

- กระบวนการนำ IT มาใช้งานพร้อมกับระบบการควบคุมที่เหมาะสม

- ความพยายามในการตรวจวัดและเฝ้าติดตามดูแลเพื่อกำหนด/ระบุวิธีการในการบริหารความเสี่ยง

กระบวนการเหล่านี้ จะต้องถูกจัดการอย่างเป็นรูปแบบมาตรฐานสำหรับองค์กรที่มีความสลับซับซ้อนและมีการริเริ่มนำเอา IT มาใช้อย่างแพร่หลาย

กระบวนการกำหนด/ระบุ และบริหารความเสี่ยงที่เกี่ยวข้องกับ IT จะไม่มีความสมบูรณ์ครบถ้วน ถ้าละเลยการพิจารณาในเรื่องของความเสี่ยงที่เกี่ยวข้องกับสภาพแวดล้อมด้าน IT จาก 2 มุมมอง ต่อไปนี้

- ถ้าสายงาน IT มีลักษณะการดำเนินงานแบบรวมศูนย์ที่สนับสนุนสายงานธุรกิจโดยใช้โครงสร้างพื้นฐานร่วมกัน ฝ่ายจัดการก็ควรที่จะรวมการบริหารความเสี่ยงด้าน IT เข้าด้วยกัน

- ถ้าสายงาน IT มีลักษณะการดำเนินงานแบบกระจายงานด้าน IT และสายงานธุรกิจเป็นผู้บริหารความเสี่ยงเอง ฝ่ายจัดการก็ควรประสานงานการบริหารความเสี่ยงให้สอดคล้องกับเป้าหมายร่วมกันขององค์กรต่อไป

2.3.1 การวางแผนงานปฏิบัติการและการลงทุนในเทคโนโลยีสารสนเทศ

สรุปแนวทางการปฏิบัติ

คณะกรรมการสถาบันการเงินและฝ่ายจัดการควรนำกระบวนการวางแผนด้าน IT มาใช้ในทางปฏิบัติ ดังนี้

- ผสมผสานการใช้ IT เข้ากับแผนกลยุทธ์ขององค์กร
- ผสมผสานงาน IT เข้ากับหน่วยงานธุรกิจ ทั้งในเชิงกลยุทธ์และในเชิงปฏิบัติการ
- จัดให้มีโครงสร้างพื้นฐานทาง IT เพื่อสนับสนุนการปฏิบัติงานด้านธุรกิจ ทั้งที่มีอยู่ในปัจจุบันและที่วางแผนว่าจะดำเนินการในอนาคต
- ผนวกการใช้จ่ายในงาน IT เข้าไว้ในกระบวนการจัดทำงบประมาณและเปรียบเทียบผลประโยชน์ที่ได้รับทั้งทางตรงและทางอ้อมกับต้นทุนรวมของ IT ที่จัดหามา
- กำหนด/ระบุ และประเมินความเสี่ยงก่อนการเปลี่ยนแปลงหรือการลงทุนใหม่ด้าน IT

การวางแผนเป็นการเตรียมการสำหรับกิจกรรมในอนาคต โดยกำหนดเป้าหมายและกลยุทธ์ที่ใช้เพื่อบรรลุวัตถุประสงค์ดังกล่าว และการที่ IT เป็นส่วนหนึ่งของการปฏิบัติงานประจำวันของสถาบันการเงิน ดังนั้น สถาบันการเงินจึงควรผนวกทรัพยากรและการลงทุนใน IT ไว้ในกระบวนการวางแผนธุรกิจโดยรวมทั้งหมด อนึ่ง การลงทุนในทรัพยากรด้าน IT ที่สำคัญ ๆ จะมีผลผูกพันในระยะยาวในการส่งมอบหรือมีผลต่อประสิทธิภาพในการออกผลิตภัณฑ์และบริการของสถาบันการเงิน จึงควรมีการวางแผนอย่างมีประสิทธิภาพในการจัดให้มีศูนย์ประมวลผลข้อมูลที่เป็นอิสระเพื่อให้ศูนย์ดังกล่าวสามารถให้บริการที่มีคุณภาพและมีต้นทุนที่ต่ำแก่สถาบันการเงินที่เป็นลูกค้าได้ ดังนั้น ฝ่ายจัดการขององค์กรจะต้องเฝ้าติดตามการเปลี่ยนแปลงใด ๆ ที่กระทบกับแผนกลยุทธ์และแผนการสร้างศูนย์ประมวลผลอิสระเพื่อให้บริการดังกล่าว

แผนงานอาจแปรเปลี่ยนไปได้อย่างมาก ขึ้นอยู่กับขนาดและโครงสร้างขององค์กร องค์กรแต่ละแห่งควรจะพยายามให้ได้มาซึ่งกระบวนการวางแผนซึ่งสามารถปรับตัวอย่างต่อเนื่องเพื่อรองรับความเสี่ยงหรือโอกาสใหม่ ๆ และเพิ่มมูลค่าของ IT ให้สูงสุด ในขณะเดียวกัน **ฝ่ายจัดการควรจัดทำแผนงานให้เป็นลายลักษณ์อักษร** (แม้ว่าการกระทำดังกล่าวไม่สามารถรับประกันประสิทธิภาพของกระบวนการวางแผนได้ก็ตาม) **ควรตรวจวัดผลของแผนงานแต่ละแผนว่าเป็นไปตามความต้องการเชิงธุรกิจขององค์กรหรือไม่** (ผู้ตรวจสอบควรประเมินกระบวนการดังกล่าวและผลลัพธ์) อันที่จริงแล้ว

แผนงานที่ดีจะต้องมีคณะกรรมการบริหาร ผู้บริหารระดับสูงและผู้ใช้งานเข้าไปมีส่วนเกี่ยวข้องด้วย โดยมีคณะกรรมการบริหารทำหน้าที่ทบทวนและให้ความเห็นชอบแผน ส่วนผู้บริหารระดับสูงเข้าไปมีส่วนร่วมในการจัดทำแผนและการนำแผนไปใช้ในทางปฏิบัติ และสำหรับฝ่ายงานหรือหน่วยงานต่างๆ ทำหน้าที่ในการระบุความต้องการเชิงธุรกิจของหน่วยงานของตนและเป็นผู้นำแผนไปใช้ในทางปฏิบัติ

(1) <u>การวางแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ</u>

การวางแผนกลยุทธ์ด้าน IT มุ่งเน้นไปที่แผนระยะ 3 – 5 ปี เพื่อช่วยให้แผนงาน IT ขององค์กรสอดคล้องกันกับแผนงานธุรกิจ และแผนกลยุทธ์ที่มีประสิทธิภาพเพียงพอ ก็จะช่วยให้องค์กรได้มาซึ่งบริการด้าน IT ที่มีความสมดุลระหว่างประสิทธิภาพและต้นทุนในขณะเดียวกันก็สนับสนุนให้หน่วยงานธุรกิจสามารถสนองความต้องการของตลาดที่มีการแข่งขันกันอย่างสูงมากได้

การวางแผนกลยุทธ์ควรคำนึงถึงเป้าหมายระยะยาวและวิธีการจัดสรรทรัพยากร IT โดยมีรายละเอียดที่เกี่ยวข้องกับ แผนการงบประมาณ การรายงานผลต่อคณะกรรมการบริหารเป็นรายงวด และสถานภาพของการควบคุมและบริหารความเสี่ยง รวมทั้งจะต้องมีการกำหนดขั้นตอนการดำเนินการ กำหนดระยะเวลาในการดำเนินการ รวมไปถึงโครงสร้างทางสถาปัตยกรรมของเครื่องคอมพิวเตอร์และโปรแกรมระบบงาน เครื่องมือประมวลผลสำหรับผู้ใช้งาน และการว่าจ้างให้บุคคลภายนอกทำหน้าที่ประมวลผลข้อมูลแทน นอกจากนี้ คณะกรรมการบริหารและฝ่ายจัดการขององค์กรควรจะต้องคำนึงถึงปัจจัยต่าง ๆ เพิ่มเติม ดังต่อไปนี้

- สภาวะของตลาด
- ปัจจัยทางประชากรศาสตร์ของลูกค้า
- เป้าหมายในการขยายตัวทางธุรกิจขององค์กร
- มาตรฐานของ IT ต่างๆที่จะต้องนำมาใช้
- การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับของทางการ
- การควบคุมต้นทุน
- การปรับปรุงกระบวนการ และประสิทธิผลที่องค์กรได้รับ
- การให้บริการแก่ลูกค้า และคุณภาพของ IT ที่ใช้
- การเปรียบเทียบระหว่างผู้ให้บริการจากภายนอก กับผู้เชี่ยวชาญภายใน
- โครงสร้างพื้นฐานที่เหมาะสม สำหรับการใช้งานในอนาคต
- ความสามารถในการรับเอา IT ใหม่มาประยุกต์ใช้งาน

ปัจจัยดังกล่าวข้างต้นควรสอดคล้องกันกับแผนธุรกิจ และแผนการนำ IT มาใช้ในทางปฏิบัติที่กำหนดมาอย่างดีจะทำให้องค์กรมีศักยภาพในการสร้างมูลค่าทางธุรกิจในรูปของส่วนแบ่งทางการตลาด รายได้ และส่วนทุนที่เพิ่มขึ้น ดังนั้น คณะกรรมการ IT ซึ่งมีสมาชิกเป็นตัวแทนมาจากสายงานต่าง ๆ จะช่วยให้องค์กรสามารถถ่วงดุลหรือผสานการลงทุนใน IT เข้ากับวัตถุประสงค์เชิงกลยุทธ์หรือเชิงปฏิบัติการได้ และสำหรับองค์กรที่สามารถปรับเปลี่ยนระบบงาน IT ให้เข้ากับเป้าหมายและวัตถุประสงค์ทางธุรกิจที่เปลี่ยนแปลงไปได้ดีมากเท่าใด ก็จะทำให้องค์กรมีความสามารถในการแข่งขันได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

สถาบันการเงินบางแห่งอาจจะมีการลงทุนด้าน IT ที่มากเกินไปจนสายงานธุรกิจไม่สามารถใช้ประโยชน์ได้เต็มที่ นอกจากนี้สายงาน IT หรือสายงานธุรกิจต่างก็มีโอกาสที่จะลงทุนใน IT เฉพาะด้านมากเกินไปทำให้เกิดมูลค่าทางธุรกิจที่ไม่เหมาะสมภายในองค์กร ทำให้ระบบงานไม่สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ หรือก่อให้เกิดกำลังผลิตส่วนเกินที่ไม่มีความจำเป็น

ในทางตรงกันข้าม สถาบันการเงินหรือองค์กรอาจใช้จ่ายอย่างระมัดระวังมากเกินไป หรือชะลอการลงทุนในโครงสร้างพื้นฐานหรือการออกผลิตภัณฑ์ใหม่จนสายงานธุรกิจเสียโอกาสในการแข่งขันเพื่อให้ได้ส่วนแบ่งตลาดและผลกำไร นอกจากนี้สายงานธุรกิจที่ปราศจากความเข้าใจถึง IT ที่มีการใช้งานกันอยู่ก็ประสบกับความล้มเหลวในการปรับปรุงกระบวนการผลิตและผลิตภัณฑ์ของตนให้มีความได้เปรียบในการผลิตและเพิ่มรายรับมากขึ้น และเพิ่มความเสี่ยงด้านการรักษาความปลอดภัยเพิ่มขึ้นอีกด้วย ดังนั้น เพื่อให้เกิดความสมดุล สถาบันการเงินหรือองค์กรควรเชื่อมโยงแผนกลยุทธ์และแผนปฏิบัติการระหว่างสายงาน IT และสายงานธุรกิจเข้าด้วยกัน

องค์ประกอบหลัก 4 ประการในการวางแผนด้าน IT ที่ฝ่ายจัดการควรคำนึง ได้แก่

- <u>การมีส่วนร่วมอย่างจริงจังของผู้บริหารระดับสูง</u> (strong senior management participation) ผู้บริหารระดับสูงควรเข้าใจและสนับสนุนแผนกลยุทธ์ด้าน IT และควรจัดลำดับความสำคัญของแต่ละแผนงาน

- <u>บทบาทของเทคโนโลยีสารสนเทศ</u> (role of IT) องค์กรจำเป็นต้องอธิบายข้อมูลเกี่ยวกับบทบาททางด้าน IT ให้ชัดเจน และอธิบายให้ชัดเจนว่าการวางแผนงาน IT ในปัจจุบันมุ่งหมายที่จะช่วยให้บุคลากรสามารถทำงานแบบเชื่อมโยงกันครอบคลุมทั้งองค์กร

- <u>ผลกระทบของ IT</u> (impact of IT) คณะกรรมการ IT ควรเข้าใจถึงความสัมพันธ์ระหว่างโครงสร้างพื้นฐานทาง IT (ซึ่งควรสนับสนุนเป้าหมายและวัตถุประสงค์ของ

แผนงานด้าน IT โดยตรง) กับโปรแกรมระบบงานประยุกต์ แผนกลยุทธ์ทางธุรกิจและแผนการปฏิบัติการประจำวัน

- <u>การประเมินผลงานที่ผ่านมาอย่างถูกต้องแม่นยำ</u> (accurate scorecard on past performance) คณะกรรมการ IT ควรเฝ้าติดตามดูแลโครงการทาง IT ในอดีตที่ผ่านมาและการนำไปใช้ในทางปฏิบัติ เพื่อเปรียบเทียบต้นทุนที่ประมาณการไว้กับผลตอบแทนที่ได้รับและเปรียบเทียบผลงานด้านอื่น ๆ กับตัวเลขอ้างอิงตามเป้าหมายหรือวัตถุประสงค์อื่นๆ เพิ่มเติม

คณะกรรมการบริหารควรกำกับดูแลความพยายามของฝ่ายจัดการในการริเริ่มและดำรงไว้ซึ่งความสัมพันธ์ของแผนกลยุทธ์ด้านธุรกิจกับแผนงานด้าน IT โดยการดำเนินการดังต่อไปนี้

- การยืนยันว่าแผนกลยุทธ์ด้าน IT สัมพันธ์กับแผนกลยุทธ์ทางด้านธุรกิจ
- การตัดสินใจว่าการดำเนินงานด้าน IT สนับสนุนแผนกลยุทธ์ที่ได้กำหนดไว้
- การสร้างความมั่นใจว่าสายงาน IT สามารถส่งมอบงานได้ทันตามกำหนดเวลาและมีการใช้งบประมาณตามกำหนด และเป็นไปตามข้อกำหนดต่างๆ ที่กำหนดไว้
- การกำหนดทิศทางให้มีการลงทุนด้าน IT ที่สมดุลระหว่างการลงทุนในระบบงานต่างๆ ที่สนับสนุนการดำเนินงานในปัจจุบันกับการลงทุนในระบบงานอื่นๆ ที่จะเปลี่ยนแปลงการปฏิบัติงานประจำวันและสนับสนุนการดำเนินงานทางธุรกิจในขอบเขตการดำเนินธุรกิจใหม่ๆได้ดีขึ้น
- การตัดสินใจเพื่อใช้ทรัพยากรด้าน IT สำหรับวัตถุประสงค์พิเศษ เช่น การขยายตัว เข้าสู่ตลาดใหม่ ๆ การเสริมสร้างความสามารถในการแข่งขัน การเพิ่มขึ้นของรายได้ การสร้างความพึงพอใจให้ลูกค้า หรือการรักษากลุ่มลูกค้าเดิมไว้

(2) <u>การวางแผนปฏิบัติงานประจำวันด้านเทคโนโลยีสารสนเทศ</u>

แผนปฏิบัติงานประจำวัน ควรสอดคล้องและเป็นแผนย่อยที่เกิดมาจากแผนกลยุทธ์ โดยเป็นแผนระยะสั้นซึ่งใช้กระบวนการงบประมาณประจำปี ซึ่งฝ่ายจัดการควรทำการทบทวนแผนเป็นประจำอย่างน้อยปีละครั้ง ให้มีความสอดคล้องกับแผนกลยุทธ์และสอดคล้องกับการเปลี่ยนแปลงต่างๆ ตามที่สายงานธุรกิจมีความจำเป็นต้องใช้งาน ที่มุ่งเน้นไปที่ปัญหาในการดำเนินงานเร่งด่วนเฉพาะหน้า เช่น ความเพียงพอของทรัพยากรด้าน IT ความเพียงพอของงบประมาณ และการกำหนด / ระบุประเภทของความเสี่ยงที่เหมาะสม

(2.1) ทรัพยากรด้านเทคโนโลยีสารสนเทศ

ในการวางแผนปฏิบัติการ ฝ่ายจัดการควรดำเนินการให้มีทรัพยากรด้าน IT ที่เพียงพอสำหรับตอบสนองต่อความเปลี่ยนแปลงและความจำเป็นในการปฏิบัติงานประจำวันขององค์กร ทั้งนี้ การดำเนินงานทางธุรกิจจะครอบคลุมไปถึงเรื่องการผสมผสานระหว่างบุคลากร IT รวมไปถึงกระบวนการดำเนินงานทางธุรกิจและการทำรายการธุรกรรมให้แล้วเสร็จ อนึ่ง การเปลี่ยนแปลงกระบวนการดำเนินงานทางธุรกิจจำเป็นต้องอาศัยความร่วมมือและการรองรับของระบบงานด้าน IT ซึ่งฝ่ายจัดการจะต้องดำเนินการให้มีความสอดคล้องกัน ดังต่อไปนี้ คือ

- โครงสร้างพื้นฐาน (Infrastructure) ได้แก่ พลังงาน (เช่น ไฟฟ้า น้ำมัน ฯ) ความสามารถในการติดต่อสื่อสาร โครงสร้างพื้นฐานด้านเครือข่ายสื่อสาร และสิ่งอำนวยความสะดวกอื่น ๆ

- โปรแกรมระบบงานประยุกต์ (Application software) รวมไปถึงการเปลี่ยนแปลงโปรแกรมระบบงานประยุกต์ เพื่อให้บริการหรือผลิตภัณฑ์ทางการเงินอันเนื่องมาจากการแข่งขัน แรงผลักดันจากตลาด และกฎเกณฑ์หรือระเบียบของทางการที่เปลี่ยนแปลงไป จึงทำให้มีความจำเป็นต้องเสริมสร้างความสามารถในการดำเนินงานหรือเปลี่ยนทดแทนโปรแกรมระบบงานประยุกต์ที่ใช้ในระบบคอมพิวเตอร์ทุกระดับตั้งแต่ระดับ mainframe ลงไปจนถึงระดับเครื่องคอมพิวเตอร์ส่วนบุคคล

- โปรแกรมระบบปฏิบัติการ (operation software) ได้แก่ ระบบปฏิบัติการ โปรแกรมแปลงภาษาชั้นสูงเป็นภาษาเครื่อง (compiler) และโปรแกรมอรรถประโยชน์ต่างๆที่ถูกออกแบบไว้เพื่อช่วยให้อุปกรณ์คอมพิวเตอร์และโปรแกรมระบบงานประยุกต์ สามารถทำงานได้อย่างมีประสิทธิภาพ ดังนั้น การเปลี่ยนแปลงใด ๆ ในส่วนที่เกี่ยวข้องกับโปรแกรมระบบปฏิบัติการทั้งหมดอาจจะมีผลกระทบที่สำคัญกับคุณสมบัติเฉพาะของเครื่องคอมพิวเตอร์ อุปกรณ์ และโปรแกรมระบบงานต่างๆ

- เครื่องคอมพิวเตอร์และอุปกรณ์ (hardware) รวมไปถึงเครื่องคอมพิวเตอร์ mainframe คอมพิวเตอร์ server สำหรับระบบเครือข่ายสื่อสาร อุปกรณ์จัดเก็บและบันทึกข้อมูล และอุปกรณ์ประกอบอื่น ๆ ดังนั้น ในขั้นตอนของการวางแผนควรจะต้องทำการพิจารณาอย่างละเอียดถึงขีดความสามารถในการดำเนินงานของเครื่องคอมพิวเตอร์ทุกระดับตั้งแต่เครื่องคอมพิวเตอร์ mainframe ไปถึงเครื่องคอมพิวเตอร์ส่วนบุคคลว่ามีความสามารถในการดำเนินงานได้อย่างเพียงพอทั้งในปัจจุบันและอนาคต เพราะอาจไม่มีความคุ้มค่าทางเศรษฐกิจในการซื้อคอมพิวเตอร์ mainframe ชุดใหม่ แต่อาจจะ

เหมาะสมกว่าที่จะซื้อคอมพิวเตอร์ระดับกลางมาใช้ปฏิบัติงานเป็นการเฉพาะแยกต่างหากจากศูนย์ประมวลผลหลัก

- บุคลากร (personnel) รวมไปถึงการเปลี่ยนแปลงโยกย้ายพนักงาน กำหนดการปฏิบัติงาน การฝึกอบรม และการกำหนดค่าตอบแทน ซึ่งฝ่ายจัดการควรกำหนดอัตราเงินเดือนให้เหมาะสม หากต่ำเกินไปอาจทำให้พนักงานโยกย้ายหรือลาออกจนส่งผลให้ขาดแคลนพนักงานที่ชำนาญงาน แต่ถ้าอัตราเงินเดือนสูงเกินไปก็ทำให้รายได้รวมของกิจการลดลง

(2.2) งบประมาณ (budgeting)

คณะกรรมการบริหารควรประเมินแผนงานต่างๆที่ฝ่ายจัดการได้วางไว้ **และควรประเมินความสำเร็จของฝ่ายจัดการจากความสำเร็จในการจัดทำแผนงานงบประมาณ** (ซึ่งเป็นขั้นตอนหนึ่งในกระบวนการวางแผนปฏิบัติงานประจำวัน) และความสำเร็จในการดำเนินงานได้บรรลุผลตามเป้าหมายของแผนงานงบประมาณในฐานะของหนึ่งในตัวชี้วัดความสำเร็จของฝ่ายจัดการในการดำเนินงานศูนย์ประมวลผลข้อมูลและการบริหารการปฏิบัติงานประจำวัน ทั้งนี้ก็เพราะว่าการจัดทำงบประมาณนั้นเป็นแผนงานร่วมทางการเงินประเภทหนึ่งที่ฝ่ายจัดการทำการประมาณอัตราการเจริญเติบโตและสภาวะการณ์ทางเศรษฐกิจประกอบการจัดทำแผนปฏิบัติงานและบันทึกรายการแสดงความแตกต่างจากแผนงานไว้ในสมุดบัญชีงบดุลและงบกำไรขาดทุน ดังนั้นแผนงบประมาณจึงเป็นทั้งแผนงานที่ใช้ในการประเมินและควบคุมกิจกรรมขององค์กรว่าดำเนินการไปตามโครงการที่คาดการณ์ไว้หรือไม่และยังเป็นเครื่องมือที่ใช้ในการตรวจสอบฝ่ายจัดการที่สำคัญอีกวิธีหนึ่ง

อนึ่ง ในขั้นตอนของการพิจารณาโครงการด้าน IT ใหม่ๆ ฝ่ายจัดการควรคำนึงถึงทั้งต้นทุนครั้งแรกเพื่อการใช้เทคโนโลยีเหล่านั้นและต้นทุนส่วนเพิ่มที่เกิดหลังจากนำ IT ไปใช้ในทางปฏิบัติแล้ว ดังนั้น สถาบันการเงินและหน่วยงานผู้ให้บริการภายนอกต่างก็ต้องการข้อมูลเกี่ยวกับค่าใช้จ่ายทั้งหมดในการเป็นเจ้าของ IT (Total cost of ownership-TCO) ซึ่งมีจำนวนมากกว่าค่าใช้จ่ายเริ่มแรกในการจัดหา (initial entry costs) เพราะว่าค่าใช้จ่ายของโครงการด้าน IT ต่างๆมักจะไม่ได้มีการบันทึกเป็นหลักฐานเกี่ยวกับต้นทุนหลายประเภทไว้ เช่น ค่าใช้จ่ายในการเริ่มกำหนดค่าตัวแปรต่าง ๆ ของเครื่องคอมพิวเตอร์ (configure) ค่าบำรุงรักษา ค่าซ่อมแซม ค่าใช้จ่ายในการสนับสนุน ค่าใช้จ่ายในการปรับปรุงระบบให้ทันสมัย และค่าใช้จ่ายในการบริหารตลอดอายุการใช้งานของ IT นั้น ๆ ดังนั้นแบบจำลองต้นทุน TCO รวมทั้งข้อมูลในอดีตจะเป็นเครื่องมือที่ดีของฝ่ายจัดการในการจัดการกับต้นทุนที่แอบแฝงดังกล่าวเพื่อช่วยในการคัดเลือกและจัดทำงบประมาณของโครงการด้าน IT ที่ดีได้

นักวิเคราะห์ทางการเงินของสายงาน IT ควรเปรียบเทียบความมีประสิทธิภาพด้านต้นทุนระหว่างการปฏิบัติงานโดยหน่วยงานเองกับการใช้บริการจากผู้ให้บริการจากภายนอกรวมทั้งการเปรียบเทียบต้นทุนการปฏิบัติงานและสัดส่วนของค่าใช้จ่ายขององค์กร กับค่าใช้จ่ายและสัดส่วนของค่าใช้จ่ายขององค์กรอื่นที่อยู่ในธุรกิจเดียวกันและมีขนาดขององค์กรในระดับเดียวกัน (Peer group) อนึ่ง ในทางปฏิบัติองค์กรอาจจะแยกงบประมาณด้าน IT ออกมาต่างหากจากสายงานอื่นก็ได้ และสามารถเลือกได้ว่าจะจัดสรรค่าใช้จ่าย (charge back) ไปให้หน่วยงานผู้ใช้หรือไม่ก็ได้แต่เมื่อมีการจัดสรรค่าใช้จ่ายควรจะต้องดำเนินการอย่างเท่าเทียมกันโดยอาจจะคิดค่าใช้จ่ายกันตามผลการใช้งานจริงตามจำนวนรอบการประมวลผล (Central Processing Unit cycles) แต่ในบางกรณีซึ่งมีการใช้บริการจากบริษัทผู้ให้บริการที่อยู่ในเครือเดียวกัน อาจจะมีการคิดค่าใช้จ่ายระหว่างกันที่ต่ำกว่าความเป็นจริง ดังนั้น **เพื่อหลีกเลี่ยงการเอื้อประโยชน์กันระหว่างกิจการในเครือองค์กรจะต้องจัดทำสัญญาการใช้บริการที่มีเงื่อนไขต่างๆ เช่นเดียวกันกับการใช้บริการจากผู้ให้บริการรายอื่นๆ** (ผู้ตรวจสอบควรศึกษาเพิ่มเติมจากคู่มือตรวจสอบการให้บริการด้านเทคโนโลยีจากบุคคลภายนอก)

2.3.2 การระบุและการประเมินความเสี่ยง

สรุปแนวทางการปฏิบัติ

สถาบันการเงินควรจัดให้มีกระบวนการประเมินความเสี่ยงอย่างต่อเนื่อง ซึ่งจะมีผลให้เกิดการคัดเลือกและควบคุมการดำเนินงาน IT ที่ดี ทั้งนี้ กระบวนการประเมินความเสี่ยงควรครอบคลุมถึงหน้าที่ความรับผิดชอบที่สำคัญ เช่น การรักษาความปลอดภัย การดำเนินธุรกิจอย่างต่อเนื่องและการจัดการกับคู่ค้าและผู้ให้บริการจากภายนอก โดยมีขั้นตอนที่สำคัญ 4 ขั้นตอน ดังนี้

- การรวบรวมข้อมูลจากกิจกรรมที่องค์กรริเริ่มใหม่หรือที่ได้ดำเนินการไปแล้วอย่างต่อเนื่อง
- การวิเคราะห์ความเสี่ยง โดยพิจารณาจากผลกระทบที่อาจเกิดขึ้น
- การจัดลำดับความสำคัญของกิจกรรมต่างๆในการควบคุมและบรรเทาความเสี่ยง
- การเฝ้าติดตามดูแลกิจกรรมในการบรรเทาความเสี่ยงอย่างต่อเนื่อง

การวางแผนปฏิบัติการทาง IT ควรระบุและประเมินโอกาสที่จะเกิดความเสี่ยง (risk exposure) เพื่อให้เกิดความมั่นใจว่า แนวนโยบาย กระบวนการดำเนินงาน และกระบวนการควบคุมยังคง

มีประสิทธิภาพอยู่ (การประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลเป็นข้อกำหนดตามกฎหมาย GLBA ของประเทศสหรัฐอเมริกา) อนึ่ง ในขั้นตอนการควบคุมดูแลการปฏิบัติงานด้าน IT **ฝ่ายจัดการต้องพิจารณาผลลัพธ์จากการประเมินความเสี่ยงและกระบวนการควบคุมที่ครอบคลุมถึงกระบวนการระบุแหล่งที่ใช้จัดเก็บข้อมูลสำคัญของลูกค้าและขององค์กร รูปแบบของภัยคุกคามต่อข้อมูลทั้งจากภายนอกและภายในองค์กร และความเพียงพอของแนวนโยบายและกระบวนการในการบรรเทาภัยคุกคามดังกล่าว**

กระบวนการประเมินความเสี่ยงจะต้องมีขอบเขตที่ครอบคลุมไปถึงภาระหน้าที่ในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งหมด ด้านการรักษาความปลอดภัย การว่าจ้างบุคคลภายนอกมาดำเนินการและการดำเนินธุรกิจอย่างต่อเนื่อง ดังนั้น ผู้บริหารระดับสูงควรจะต้องสร้างความมั่นใจให้ได้ว่ากระบวนการระบุและประเมินความเสี่ยงด้าน IT มีความสัมพันธ์กันและสอดคล้องกันในภาพกว้างทั้งองค์กรและมีผลต่อการพัฒนาแนวนโยบายและการควบคุมที่มีประสิทธิภาพขององค์กร

ผู้บริหารระดับสูงสามารถนำเอาข้อมูลจากการประเมินความเสี่ยงและความเข้าใจเกี่ยวกับความเสี่ยงในการปฏิบัติงานประจำวันไปใช้ประกอบการตัดสินใจเพื่อใช้ในการบริหารความเสี่ยงที่ดีได้ อย่างไรก็ดี สำหรับสถาบันการเงินขนาดเล็กซึ่งมีระบบที่ไม่ซับซ้อนก็สามารถใช้กระบวนการประเมินความเสี่ยงที่เรียบง่ายได้ แต่สำหรับองค์กรที่มีความซับซ้อนการบริหารความเสี่ยงควรจะต้องมีกระบวนการบริหารความเสี่ยงที่เป็นรูปแบบที่ชัดเจนและสามารถปรับเปลี่ยนแปลงไปได้ตามสภาพแวดล้อมขององค์กรที่เปลี่ยนแปลงไปตลอดเวลา ดังนั้น ผู้ตรวจสอบควรทำการประเมินประสิทธิผลในการวัดประสิทธิภาพของกระบวนการโดยการประเมินว่าฝ่ายจัดการมีความเข้าใจและตระหนักถึงความเสี่ยง รวมทั้งมีวิธีการประเมินความเสี่ยงที่เหมาะสม และมีแนวนโยบายและกระบวนการควบคุมภายในองค์กรที่มีประสิทธิภาพ

(1) การรวบรวมข้อมูลที่เกิดขึ้นอย่างต่อเนื่อง

ความเข้าใจเกี่ยวกับสภาพแวดล้อมขององค์กรเป็นขั้นตอนแรกของกระบวนการประเมินความเสี่ยง ดังนั้น ผู้บริหารระดับสูงจึงควรนำเอาข้อมูลด้านเทคโนโลยีสารสนเทศต่าง ๆ อาทิ ข้อจำกัดด้านทรัพยากร ภัยคุกคาม การจัดลำดับความสำคัญของงานหรือกิจกรรมและระบบการควบคุมที่สำคัญต่างๆ มาประกอบการพัฒนากระบวนการประเมินความเสี่ยงที่เป็นมาตรฐาน และเก็บรวบรวมข้อมูลและตีความหมายของข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมด้านเทคโนโลยีฯขององค์กรจากแหล่งต่าง ๆ ได้แก่

- การจัดเก็บข้อมูลเกี่ยวกับระบบงาน IT ที่มีอยู่ทั้งหมด (IT systems inventories) เป็นสิ่งสำคัญต่อการทำความเข้าใจและการเฝ้าติดตามการปฏิบัติงานของสายงาน IT รวมไป**ถึงการกำหนด/ระบุแหล่งที่ใช้จัดเก็บรักษาข้อมูลลับของลูกค้าและองค์กร**

- แผนกลยุทธ์ด้าน IT จะให้ข้อมูลสำคัญในกระบวนการวางแผนขององค์กร ดังนั้น **การทบทวนและวิเคราะห์แผนกลยุทธ์ในขั้นตอนของการประเมินความเสี่ยงอาจจะชี้ให้เห็นถึงโอกาสที่จะเกิดความเสี่ยงต่างๆ** ที่กำลังก่อตัวขึ้น หรือแสดงให้เห็นข้อบกพร่องอื่น ๆ ซึ่งมีผลให้องค์กรไม่สามารถปฏิบัติตามลำดับของความสำคัญตามแผนกลยุทธ์ได้

- แผนฉุกเฉินด้านธุรกิจและแผนการดำเนินธุรกิจอย่างต่อเนื่องจะเป็นตัวจัดลำดับความพร้อมในการปฏิบัติงานของสายงานธุรกิจต่าง ๆ ให้แก่สถาบันการเงินและหน่วยงานภายนอก และบ่อยครั้งที่แผนดังกล่าวจะมีขอบเขตครอบคลุมถึงการกู้ระบบกลับมาใช้ และการจัดให้มีระบบการสำรองในการควบคุม การให้บริการลูกค้า และการสนับสนุนอื่นๆ ดังนั้นแผนดังกล่าวจึงช่วยแสดงให้เห็นถึงระบบการปฏิบัติงานประจำวันและสภาพแวดล้อมของระบบการควบคุมที่สำคัญๆ ขององค์กร**การสำรวจฐานะและการดำเนินงานของผู้ให้บริการภายนอกอย่างละเอียด และการเฝ้าติดตามดูแลผลการดำเนินงานของผู้ให้บริการภายนอกจะให้ข้อมูลที่สำคัญเกี่ยวกับสภาพแวดล้อมของระบบควบคุมของผู้ให้บริการเหล่านั้น** ซึ่งเป็นข้อมูลที่มีความจำเป็นต่อการประเมินความเสี่ยงที่สมบรูณ์ของสภาพแวดล้อมด้าน IT ขององค์กร

- รายงานติดตามผลการแก้ไขปัญหาจากศูนย์รับเรื่องร้องเรียน (Call center) สามารถแสดงให้เห็นศักยภาพในการให้บริการหรือประเด็นที่เกี่ยวข้องกับระบบการควบคุมถ้าได้มีการนำเอาข้อมูลเกี่ยวกับประเด็นปัญหาที่เกิดขึ้นบ่อยๆ หรือเกิดขึ้นเป็นปกติมาวิเคราะห์

- รายงานผลการประเมินตนเองในเรื่องความเพียงพอของระบบควบคุมด้าน IT ของแต่ละฝ่ายงานจะสามารถแสดงให้เห็นถึงข้อมูลเบื้องต้นเกี่ยวกับการไม่ปฏิบัติตามนโยบาย หรือจุดอ่อนในการควบคุมต่าง ๆ

- ผลการตรวจสอบด้าน IT จะสามารถให้ข้อมูลเชิงลึกในเรื่องความซื่อสัตย์และความรับผิดชอบต่อหน้าที่ของฝ่ายจัดการและพนักงานว่ามีการปฏิบัติงานตามแนวนโยบายและระบบการควบคุมภายในหรือไม่

(2) การวิเคราะห์ความเสี่ยง

ฝ่ายจัดการควรใช้ข้อมูลเกี่ยวกับทรัพยากรและความเสี่ยงด้าน IT มาใช้ในการวิเคราะห์ผลของความเสี่ยงที่อาจเกิดขึ้นกับองค์กร ทั้งนี้ การวิเคราะห์ควรแสดงเหตุการณ์หรือภัยคุกคาม

ต่าง ๆ ที่อาจส่งผลกระทบในทางลบต่อองค์กรทั้งในเชิงกลยุทธ์หรือเชิงการปฏิบัติงานประจำวัน ตามลำดับของความเป็นไปได้ที่จะเกิดเหตุการณ์และระดับของผลกระทบที่เป็นไปได้ ดังเช่นตัวอย่างดังต่อไปนี้

- **การล่วงละเมิดระบบการรักษาความปลอดภัย** ซึ่งอาจจะเกิดขึ้นได้ทั้งจากภายนอกและภายในองค์กร เช่น การทุจริตโดยการเขียนโปรแกรมระบบงาน ไวรัสคอมพิวเตอร์ หรือการโจมตีด้วยวิธีส่งคำสั่งซ้ำจนไม่สามารถให้บริการได้ (DOS: Denial of Service)

- **ความล้มเหลวหรือความผิดพลาดของระบบ** มีสาเหตุพื้นฐานมาจากการทำงานผิดพลาดของระบบการควบคุมเครือข่าย ความเสี่ยงที่เกิดจากการที่ระบบทำงานพึ่งพิงกับระบบงานอื่น ความล้มเหลวในการเชื่อมต่อกับระบบ ความล้มเหลวของระบบคอมพิวเตอร์และโปรแกรม และความล้มเหลวของระบบการสื่อสารภายในองค์กร

- **เหตุการณ์จากภายนอกองค์กร** องค์กรมีความเสี่ยงที่เกิดจากภัยคุกคามจากภายนอกองค์กร เช่น เหตุการณ์ที่เกี่ยวข้องกับสภาพของอากาศ แผ่นดินไหว การก่อการร้าย การโจมตีระบบผ่านเครือข่ายคอมพิวเตอร์ การทำลายระบบสาธารณูปโภค และไฟฟ้าดับซึ่งจะทำให้งานหรือระบบอำนวยความสะดวกที่เกี่ยวข้องล้มเหลวได้

- **ความผิดพลาดในการลงทุนด้าน IT** ซึ่งรวมไปถึงความผิดพลาดที่เกี่ยวข้องกับรูปแบบของแผนกลยุทธ์ ความเสี่ยงจากผู้ขายหรือให้บริการ การให้คำนิยามหรือ**การกำหนดความต้องการทางธุรกิจที่ไม่เหมาะสม** การที่ระบบงานไม่สามารถทำงานสัมพันธ์กันได้ (incompatibility) หรือโปรแกรมระบบงานที่ล้าสมัยจนกลายเป็นข้อจำกัดในการหาผลกำไรหรือการเพิ่มอัตราการเจริญเติบโตได้

- การพัฒนาระบบงานต่างๆ และปัญหาการนำระบบไปใช้งาน มีปัญหาร่วมกันที่สำคัญ คือ **การบริหารโครงการที่ไม่ดีเพียงพอ** การใช้ต้นทุนหรือเวลาที่มากเกินกำหนด การเขียนโปรแกรมระบบงานที่ผิดพลาด (ปัญหาทั้งจากภายในและภายนอกองค์กร) ความผิดพลาดในการเชื่อมโยงระบบงานเข้าด้วยกันหรือการย้ายระบบงานออกไป หรือความล้มเหลวของระบบในการตอบสนองความต้องการของสายงานธุรกิจได้

- **กำลังการผลิตที่ไม่เพียงพอ** ซึ่งเกิดจากการวางแผนกำลังการผลิตที่ไม่เหมาะสม รวมทั้งการพยากรณ์อัตราการเจริญเติบโตที่ไม่แม่นยำเมื่อองค์กรได้ระบุภาพรวมของความเสี่ยงที่จะเกิดขึ้นได้แล้ว ฝ่ายจัดการก็ควรประเมินโอกาสที่จะเกิดความเสียหายจากความเสี่ยงต่าง ๆ และควรประเมินผลกระทบต่อองค์กรทั้งด้านการเงิน ชื่อเสียง หรือผลกระทบอื่น ๆ เช่น การสูญเสียรายได้

การตัดสินใจด้านธุรกิจที่ผิดพลาด การกู้คืนระบบข้อมูลและค่าใช้จ่ายในการก่อสร้างระบบฉุกเฉิน ค่าใช้จ่ายทางด้านกฎหมาย การสูญเสียส่วนแบ่งของตลาดและการเพิ่มขึ้นของค่าเบี้ยประกันภัย หรือค่าใช้จ่ายในส่วนที่ไม่ได้รับความคุ้มครองจากบริษัทประกันภัย โดยปกติแล้วผลกระทบต่อองค์กรเป็นตัวเลขที่แปรผันและยากที่จะคำนวนเป็นตัวเลขที่ชัดเจนได้แต่ก็สามารถวิเคราะห์และเรียงลำดับได้ตามลำดับของความสัมพันธ์ระหว่างต้นทุนค่าใช้จ่ายและโอกาสที่จะเกิดขึ้น

(3) การจัดลำดับความสำคัญ

เมื่อฝ่ายจัดการได้เข้าใจถึงสภาพแวดล้อมด้าน IT ที่มีต่อองค์กรของตนแล้วก็**ควรเรียงลำดับของความเสี่ยงและจัดลำดับในการป้องกันปัญหาตามลำดับของความสำคัญ** โดยการประเมินผลรวมของโอกาสที่จะเกิดกับระดับความรุนแรงเป็นฐานในการลดความเสี่ยงหรือการกำหนดวิธีการควบคุมต่างๆในการรักษาความปลอดภัย สร้างความน่าเชื่อถือ และเสริมสร้างการดำเนินงานด้าน IT ที่เหมาะสมกับความสลับซับซ้อนขององค์กร ดังนั้น ผลของการประเมินภาพรวมของความเสี่ยงจึงเป็นปัจจัยหลักในการตัดสินใจของผู้บริหารด้าน IT ในเรื่องดังต่อไปนี้

- การจัดทำงบประมาณด้าน IT การลงทุนและนำเอาผลการตัดสินใจไปปฏิบัติ
- การวางแผนฉุกเฉิน
- การจัดทำนโยบายและขั้นตอนการปฏิบัติงาน
- การควบคุมภายใน
- การจัดหาบุคลากรและผู้เชี่ยวชาญ
- การประกันภัย
- การวัดผลการปฏิบัติงานด้าน IT
- การกำหนดระดับของการให้บริการด้าน IT ที่ดำเนินการภายในองค์กรและการใช้บริการจากหน่วยงานภายนอก
- การบังคับใช้นโยบาย และการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ

(4) การเฝ้าติดตาม

ฝ่ายจัดการและคณะกรรมการบริหารควรติดตามกิจกรรมในการบรรเทาความเสี่ยงเพื่อให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ ทั้งนี้ **การเฝ้าติดตามดูแลความเสี่ยงควรกระทำอย่างต่อเนื่องและทุกฝ่ายงานควรนำเสนอรายงานแสดงความคืบหน้าให้ฝ่ายจัดการเป็นระยะๆ อย่างสม่ำเสมอ** แทนที่จะรายงานแบบปีละครั้งเดียว โดยมีปัจจัยสำคัญในการเฝ้าติดตามดูแลที่มีประสิทธิภาพ ได้แก่

- แผนปฏิบัติการเพื่อบรรเทาหรือแก้ไขข้อผิดพลาด

- การกำหนดหน้าที่และความรับผิดชอบอย่างชัดเจน
- การรายงานผลต่อฝ่ายจัดการ

2.3.3 การควบคุมด้านเทคโนโลยีสารสนเทศในทางปฏิบัติ

สรุปแนวทางการปฏิบัติ

ฝ่ายจัดการของสถาบันการเงิน ควรนำแนวทางปฏิบัติในการควบคุมที่ดีมาใช้เป็นส่วนหนึ่งของแผนกลยุทธ์ในการบรรเทาความเสี่ยงด้าน IT ทั้งนี้ แนวทางปฏิบัติงานควบคุมที่ดีควรประกอบไปด้วยหัวข้อดังต่อไปนี้

- การควบคุมภายในซึ่งมีประสิทธิภาพสามารถลดความเสี่ยงที่ระบุไว้ในส่วนที่เกี่ยวข้องกับกระบวนการทางด้าน IT เช่น การบริหารการรักษาความปลอดภัย การพัฒนาระบบงานและโปรแกรม การปฏิบัติการด้าน IT ประจำวัน การใช้บริการจากบุคคลภายนอก การบริหารร้านค้า/คู่ค้า และความเสี่ยงด้านเทคโนโลยีสารสนเทศประเภทอื่น ๆ
- การควบคุมระบบ MIS ที่ให้ข้อมูลที่แม่นยำเที่ยงตรงและทันกาลให้ฝ่ายจัดการใช้ในการตัดสินใจ
- การจัดทำและบังคับใช้นโยบายและมาตรฐานด้าน IT
- มาตรฐานของการว่าจ้างงาน การเปลี่ยนแปลงลักษณะงาน และเลิกจ้างบุคลากรด้าน IT ซึ่งรวมถึงพนักงาน ที่ปรึกษา ลูกจ้างชั่วคราว และบุคคลภายนอก
- โปรแกรมการฝึกอบรมและการประเมินเพื่อดำรงไว้ ซึ่งระดับของความเชี่ยวชาญด้าน IT ของบุคลากร
- การทบทวนขอบเขตของการประกันภัยด้าน IT ประจำปี
- แผนการดำเนินธุรกิจอย่างต่อเนื่องของสายงานต่าง ๆ ที่มีความสำคัญ
- การกำกับดูแลความสัมพันธ์กับบุคคลภายนอกหรือผู้ให้บริการจากภายนอก

บทนี้จะกล่าวถึงระบบการควบคุมต่างๆ ซึ่งเมื่อนำมาใช้งานแล้วสามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพครอบคลุมไปถึงทั้งการใช้บริการจากผู้ให้บริการจากภายในหรือผู้ให้บริการจากภายนอกองค์กร อนึ่ง สถาบันการเงินควรทบทวนและประเมินแนวทางการปฏิบัติงานว่ามีความสม่ำเสมอคงที่หรือไม่ เพราะว่าความแตกต่างของแนวทางการปฏิบัติจากแนวทางของระบบการควบคุมที่

กำหนดไว้นี้จะทำให้เกิดความเสี่ยงที่สูงมากและฝ่ายจัดการควรหาทางบรรเทาความเสี่ยงก่อนที่จะดำเนินความสัมพันธ์กับบุคคลภายนอกอย่างเป็นทางการ

(1) แนวนโยบาย มาตรฐานและกระบวนการดำเนินงาน

ฝ่ายจัดการควรนำแนวนโยบาย กระบวนการดำเนินงาน และระบบงานต่างๆ ที่เหมาะสมมาใช้ในการบริหารความเสี่ยงด้าน IT และควบคุมให้มีการเก็บข้อมูลดังกล่าวไว้เป็นลายลักษณ์อักษร พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบที่ชัดเจนมีความทันสมัยอยู่เสมอ เพื่อใช้ฝึกอบรมพนักงานใหม่ สื่อสารให้พนักงานได้รับทราบอย่างสม่ำเสมอ ทั้งนี้เพราะว่าประสิทธิภาพของแนวนโยบายและกระบวนการดำเนินงานต่างๆ เหล่านี้จะขึ้นอยู่กับการยอมรับของทั้งพนักงานและบุคคลภายนอกที่เกี่ยวข้อง จึงจำเป็นที่จะต้องมีการทดสอบการปฏิบัติงานตามแนวนโยบายและกระบวนการดำเนินงานเพื่อจะได้รับทราบปัญหาและหาแนวทางแก้ไขปัญหาก่อนที่จะเกิดปัญหาสำคัญ

โดยทั่วไปแล้ว **แนวนโยบาย (policy) เป็นหลักการในการกำกับดูแล เป็นแนวทางพื้นฐานในการกำหนดมาตรฐานการปฏิบัติงาน และเป็นอำนาจสูงสุดในองค์กรที่แสดงให้เห็นปรัชญาหรือสิ่งที่สะท้อนถึงแนวทางปฏิบัติที่ดีของตลาด** ส่วน**มาตรฐานการปฏิบัติงาน (standard) เป็นกฎเกณฑ์หรือข้อกำหนดที่องค์กรจะต้องปฏิบัติตามแนวนโยบาย กฎระเบียบของทางการ และระดับของการควบคุมต่าง ๆ ซึ่งยอมรับได้** และ**ขั้นตอนการปฏิบัติงาน (procedure) ก็คือเป็นเอกสารที่มีคำอธิบายอย่างรายละเอียดเกี่ยวกับพฤติกรรมหรือกระบวนการทำงานที่เป็นไปตามมาตรฐานการปฏิบัติงาน**

สถาบันการเงินควรกำหนด บันทึกไว้เป็นลายลักษณ์อักษร บำรุงรักษา และยึดถือตามแนวนโยบายและมาตรฐานการปฏิบัติงานต่าง ๆ ในการบริหารและควบคุมสภาพแวดล้อมด้าน IT โดยมีแนวนโยบาย และมาตรฐานการปฏิบัติงานที่บันทึกไว้เป็นลายลักษณ์อักษรเป็นเครื่องชี้ให้เห็นถึงการปฏิบัติงานตามกฎข้อบังคับ ส่วนความละเอียดครบถ้วนของเอกสารย่อมขึ้นอยู่กับความสลับซับซ้อนขององค์กรแต่จะต้องมีขั้นต่ำที่เพียงพอสำหรับฝ่ายจัดการใช้ในการบริหารงาน

(2) การควบคุมภายใน

องค์กรควรจัดให้มีระบบการควบคุมภายในที่เหมาะสมกับระดับของโอกาสที่จะเกิดความเสี่ยงและความเสียหายทางการเงินที่อาจจะเกิดขึ้นจากการนำเทคโนโลยีมาใช้งาน ทั้งนี้ **ฝ่ายจัดการควรเริ่มต้นจัดให้มีระบบควบคุมภายในโดยการกำหนดเป้าหมายที่ชัดเจนเพื่อใช้ในการประเมินผลการปฏิบัติงาน จัดสรรหน้าที่และความรับผิดชอบเป็นการเฉพาะสำหรับผู้ที่รับผิดชอบในโครงการที่มีความสำคัญ ๆ สร้างกลไกอิสระมาใช้ในการวัดความเสี่ยงและช่วยลดการเกิดความเสี่ยงส่วนที่มากเกินไป และติดตามประเมินผลการดำเนินงานของระบบควบคุมต่าง ๆ เป็นระยะ**

ฝ่ายจัดการควรกำหนดให้มีระบบการควบคุมภายในที่มีประสิทธิภาพ ที่สามารถสนับสนุนความถูกต้องเชื่อถือได้และเหมาะสมกับสภาพแวดล้อมทางด้าน IT ทั้งนี้ ผู้บริหารระดับสูงมีหน้าที่ในการกำกับและเฝ้าติดตามดูแลระบบควบคุมภายในเพื่อให้ระบบควบคุมภายในดังกล่าวมีขอบเขตที่ครอบคลุมและมีคุณภาพและสามารถใช้เป็นองค์ประกอบหลักที่สำคัญของกระบวนการประเมินความเสี่ยงที่ครอบคลุมไปถึงเรื่องการบริหารจัดการและระเบียบวินัยในการดำเนินการทางเทคนิคได้

ฝ่ายจัดการควรกำหนด/ระบุเป้าหมายหลักของระบบการควบคุมภายในที่ต้องการไว้ในแนวนโยบาย มาตรฐานการปฏิบัติงาน และแนวทางในการปฏิบัติงานของสถาบันการเงินไว้เป็นบรรทัดฐานขั้นต่ำในการกำหนดขอบเขตการตรวจสอบ และบรรทัดฐานขั้นต่ำดังกล่าวก็จะแสดงให้เห็นถึงภาพทั่วไปของสภาพแวดล้อมในการควบคุมภายในขององค์กร โดยมีการกำหนดรายละเอียดของวิธีการหรือวินัยในการดำเนินงานเป็นเครื่องมือในการวัดผลการปฏิบัติงานตามแนวนโยบาย มาตรฐานการปฏิบัติงาน และแนวทางในการปฏิบัติงานของสถาบันการเงิน ทั้งนี้ แนวทางการปฏิบัติงานของฝ่ายบริหารที่เกี่ยวข้องกับระบบควบคุมภายในประกอบไปด้วย

- การรายงานต่อคณะกรรมการบริหารที่มีประสิทธิภาพ
- การทบทวนและปรับปรุงแนวนโยบาย มาตรฐานการปฏิบัติงาน และแนวทางการปฏิบัติงานให้ทันสมัยเป็นระยะ ๆ
- การทบทวนผลการตรวจสอบโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกอย่างสม่ำเสมอ
- การทบทวนข้อกำหนดเกี่ยวกับระดับของการให้บริการ
- การทบทวนระบบการควบคุมแบบ 2 มิติ ให้ครอบคลุมภาพรวมแบบตารางเมตริกระหว่างประเด็นของปัญหาต่าง ๆ กับแนวทางในการแก้ไขปัญหาดังกล่าว

ควรจัดให้มีโครงสร้างของระบบการควบคุมภายในต่างๆ ที่จะช่วยให้ฝ่ายจัดการเกิดความมั่นใจได้ ดังนี้

- บุคลากรได้สร้าง โอนย้าย และเก็บบันทึกรายการและธุรกรรมต่าง ๆ โดยวิธีการที่มีความปลอดภัยและเหมาะสม
- มีการแบ่งแยกหน้าที่การปฏิบัติงานอย่างเหมาะสม
- ข้อมูลที่อยู่ในระบบข้อมูลเพื่อการบริหาร MIS มีความถูกต้องน่าเชื่อถือได้และมีวงจรในการออกรายงานที่เหมาะสม

- มีกระบวนการปฏิบัติงานประจำวันที่มีประสิทธิภาพและประสิทธิผล

- กระบวนการปฏิบัติงานประจำวันต่างๆ ยังสามารถใช้การได้ดีและสามารถสนับสนุนให้องค์กรมีแผนการดำเนินธุรกิจอย่างต่อเนื่อง

- องค์กรสามารถกำหนด/ระบุและเฝ้าติดตามดูแลการปฏิบัติภาระหน้าที่งานและกิจกรรมที่มีความเสี่ยงสูง

- มีการปฏิบัติตามแนวนโยบาย มาตรฐานการปฏิบัติงาน กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง รวมทั้งแนวทางการปฏิบัติงานอื่นๆ ผู้ตรวจสอบอิสระสามารถตรวจสอบและยืนยันได้ว่าองค์กรมีระบบการควบคุมภายในที่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

(3) บุคลากร

สถาบันการเงินควรบรรเทาความเสี่ยงที่เกิดขึ้นจากพนักงานที่ปฏิบัติงานด้าน IT โดยการตรวจสอบประวัติความเป็นมาของพนักงาน การคัดกรองพนักงานใหม่ รวมถึงการดูแลบุคลากรของร้านค้า/คู่ค้า บริษัทที่ปรึกษา และลูกจ้างชั่วคราวที่ปฏิบัติงานสนับสนุนงานด้าน IT ที่เหมาะสม โดยมีหัวข้อที่ควรตรวจสอบขั้นต่ำดังต่อไปนี้

- ข้อมูลอ้างอิงเรื่องบุคลิกภาพ

- การตรวจสอบประวัติความเป็นมา โดยรวบรวมเอกสารต่างๆเพิ่มเติม เช่น หนังสือรับรองประสบการณ์การทำงานที่ผ่านมา ประวัติการศึกษา ใบรับรองคุณวุฒิจากสมาคมวิชาชีพและทะเบียนประวัติอาชญากรรม

- หนังสือรับรองหรือหลักฐานทางทะเบียนราษฎร์จากหน่วยงานราชการ

สถาบันการเงินควรปกป้องและรักษาความลับของข้อมูลของลูกค้าและองค์กร โดยการจัดทำข้อตกลงที่ครอบคลุมเรื่องการรักษาความลับ และสิทธิในการใช้ข้อมูล ทั้งนี้ **ฝ่ายจัดการควรดำเนินการเพื่อให้ได้รับหนังสือสัญญาในการรักษาความลับของข้อมูลจากพนักงานใหม่** ร้านค้า/คู่สัญญา และลูกจ้างชั่วคราว **ก่อนที่ยินยอมให้ผู้เกี่ยวข้องเหล่านั้นเข้าถึงข้อมูลด้าน IT** และหมั่นเผยแพร่แนวนโยบายและการขอรับการยืนยันจากผู้เกี่ยวข้องในการปฏิบัติตามแนวทางในการรักษาความลับของข้อมูลในการใช้เครือข่ายการสื่อสาร โปรแกรมระบบงานประยุกต์ อินเตอร์เน็ต ไปรษณีย์อิเล็กทรอนิกส์ และข้อมูลขององค์กร

สถาบันการเงินควรใช้เอกสารแสดงขอบเขตของงานในความรับผิดชอบ (Job description) เพื่อยืนยันสิทธิในการเข้าถึงระบบข้อมูล ใช้ข้อตกลงการจ้างงาน (โดยเฉพาะกับตำแหน่งงานระดับสูงๆ) เพื่อแสดงความคาดหวังต่อหน้าที่และข้อจำกัดของตำแหน่งงาน และใช้การฝึกอบรม

และส่งเสริมความรู้เพื่อส่งเสริมความเข้าใจและเพิ่มสำนึกต่อหน้าที่ของบุคลากร และการเผยแพร่แนวนโยบายอื่นๆ ของฝ่ายจัดการ

สถาบันการเงินควรกำหนดให้มีกระบวนการที่รวดเร็วในการยกเลิกหรือเปลี่ยนแปลงสิทธิในการเข้าถึงของพนักงานและผู้ที่เกี่ยวข้องอื่นๆ ถ้าองค์กรดูแลกระบวนการดังกล่าวไม่ดีจะก่อให้เกิดปัญหาเกี่ยวกับการปฏิบัติงานที่ไม่เหมาะสมหรือกระทำโดยมิได้รับอนุญาตโดยเฉพาะอย่างยิ่งจะเกิดความเสี่ยงที่มีความสำคัญมากขึ้นผันแปรไปกับระดับของสิทธิในการเข้าถึงระบบข้อมูลนั้นเอง

(4) การจัดทำสัญญาประกันภัย

ก่อนจัดทำสัญญาประกันภัย ฝ่ายจัดการควรพิจารณาโอกาสที่จะเกิดความเสียหาย วงเงินชดเชยความเสียหายที่จะได้รับจากบริษัทประกันภัย และต้นทุนของค่าใช้จ่ายในการจัดทำกรมธรรม์ประกันภัย (แตกต่างกันไปตามความซับซ้อนและความเสี่ยงขององค์กร) และพิจารณาระดับของความเสี่ยงที่องค์กรสามารถแบกรับได้ด้วยตนเองไปพร้อม ๆ กับการวิเคราะห์ผลกระทบต่อองค์กร บริษัทในเครือ หรือบริษัทแม่หากไม่ทำประกันภัย ในขณะเดียวกันถ้าองค์กรจะจ่ายค่ากรมธรรม์ประกันภัยให้บริษัทประกันภัยใด ๆ ก็ตาม **ฝ่ายจัดการควรประเมินฐานะทางการเงินและผลการจัดระดับของบริษัทประกันภัย จำนวนเงินเอาประกันที่เหมาะสมเหล่านั้นอย่างน้อยปีละหนึ่งครั้ง**

การจัดทำประกันภัยเป็นเครื่องมือช่วยเสริมให้ระบบควบคุมภายในดีขึ้นแต่ไม่ได้เป็นเครื่องมือที่ใช้ทดแทนระบบควบคุมภายใน ดังนั้น **การประเมินภาพรวมของระบบการควบคุมภายในจึงเป็นสิ่งที่มีความสำคัญมากต่อการพิจารณาความเพียงพอของการวางแผนการจัดทำประกันภัย** เพราะว่าการที่องค์กรมีระบบควบคุมภายในจะทำให้องค์กรเสียค่าเบี้ยประกันภัยที่น้อยลงได้ อนึ่ง ก่อนที่จะจัดซื้อกรมธรรม์ประกันภัย ฝ่ายจัดการควรที่จะประเมินต้นทุนต่างๆในการจัดทำประกันภัย ดังต่อไปนี้

- เครื่องมือและสิ่งอำนวยความสะดวกที่ใช้ในงานด้าน IT
- การสร้างสื่อใหม่/การกู้และจัดเก็บข้อมูลลงสื่อจัดเก็บข้อมูล
- การหยุดชะงักของธุรกิจ
- การสูญหายของข้อมูลระหว่างทาง
- ความซื่อสัตย์สุจริตของพนักงาน
- ค่าใช้จ่ายส่วนเพิ่ม
- การทำธุรกรรมการเงินทางธนาคารอิเล็กทรอนิกส์
- การปฏิบัติงานผิดพลาด และการละเว้น/ละเลยไม่ปฏิบัติหน้าที่

- ภาระที่มีต่อลูกค้า อันเนื่องมาจากให้บริการโอนเงินทางอิเล็กทรอนิกส์

ประมาณการค่าใช้จ่ายข้างต้นจะช่วยฝ่ายจัดการสามารถเลือกรูปแบบของการประกันภัยและวงเงินที่จะเอาประกัน รวมทั้งสามารถพิจารณาได้ว่าองค์กรควรที่จะทำการสะสมเงินในรูปแบบของการประกันภัยด้วยตนเองในวงเงินเท่าใดได้บ้าง

องค์กรหรือศูนย์ประมวลผลข้อมูลสามารถทำประกันในรูปแบบของกรมธรรม์ประกันภัยแบบมาตรฐานที่ใช้กันทั่วไปได้ แต่จะต้องมีความเข้าใจขอบเขตของการคุ้มครอง เช่น การทำประกันภัยที่คุ้มครองภัยพิบัติทางกายภาพจะไม่มีผลคุ้มครองไปถึงความเสียหายของเครื่องมือคอมพิวเตอร์ แต่ก็คุ้มครองไปถึงมูลค่าของสื่อจัดเก็บข้อมูลแบบทางกายภาพแต่ไม่คุ้มครองไปถึงค่าใช้จ่ายในการสร้างสื่อใหม่/การกู้และจัดเก็บข้อมูลลงสื่อจัดเก็บข้อมูลดังกล่าว ดังนั้น **ฝ่ายจัดการจะต้องเข้าใจอย่างถ่องแท้ถึงขอบเขตของความคุ้มครองและจะต้องจัดทำรายละเอียดของสิ่งที่กรมธรรม์ไม่คุ้มครองเพื่อหาทางปิดความเสี่ยงต่อไป** อย่างไรก็ดียังมีการจัดทำกรมธรรม์ประกันภัยที่เกี่ยวข้องกับระบบงานด้าน IT เป็นการเฉพาะ ซึ่งสามารถนำมาประยุกต์ใช้กับสภาพแวดล้อมเฉพาะตัวขององค์กร

กรมธรรม์ประกันภัยจะครอบคลุมถึงการคุ้มครองในส่วนที่เกี่ยวข้องกับงานด้าน IT โดยอาจมีการปรับแบบของกรมธรรม์ให้รองรับสภาพแวดล้อมทางด้าน IT ที่มีลักษณะเฉพาะของสถาบันการเงินและหน่วยงานภายนอกแต่ละแห่ง ตัวอย่างของการคุ้มครองตามกรมธรรม์ที่กำหนดขึ้นมาเป็นการเฉพาะและแนวทางในการประเมินค่าของการคุ้มครองดังกล่าวได้แก่

- อุปกรณ์และสิ่งอำนวยความสะดวกที่ใช้ในงานด้าน IT ฝ่ายจัดการควรเอาประกันภัยให้คุ้มครองความเสียหายทางกายภาพของศูนย์ข้อมูลและอุปกรณ์อัตโนมัติต่าง ๆ ทั้งหมด ความคุ้มครองตามกรมธรรม์ดังกล่าวควรรวมถึงอุปกรณ์ที่ได้เช่าซื้อมาด้วย หากผู้เช่าเป็นผู้รับผิดชอบในการทำประกันภัยคุ้มครองความเสียหาย

- การสร้างสื่อใหม่/ การกู้และจัดเก็บข้อมูลลงสื่อจัดเก็บข้อมูล องค์กรควรจัดทำกรมธรรม์ประกันภัยให้ครอบคลุมถึงความเสียหายของสื่อจัดเก็บข้อมูลด้าน IT เช่น แถบบันทึกแม่เหล็ก (tape) หรือแผ่นดิสก์ (disk) ซึ่งเป็นทรัพย์สินที่อยู่ในความรับผิดชอบของตนเอง ทั้งนี้จะต้องให้ความคุ้มครองทั้งสื่อที่อยู่ในอาคาร นอกอาคาร หรือที่อยู่ระหว่างการขนย้ายไปพร้อมๆ กันด้วย และควรคุ้มครองไปถึงต้นทุนหรือค่าใช้จ่ายที่เกิดขึ้นจริงในการกู้หรือสร้างระบบข้อมูลขึ้นมาใหม่บนสื่อชุดใหม่ (อย่างน้อยที่สุดก็ให้ครอบคลุมถึงค่าใช้จ่ายในการจัดซื้อจัดหาสื่อจัดเก็บข้อมูลเปล่า ๆ ชุดใหม่แทนชุดเดิมที่ชำรุดเสียหาย) รวมถึง ค่าใช้จ่ายในการพัฒนาโปรแกรมระบบงาน การเปลี่ยนแปลงทางกายภาพของอุปกรณ์ที่ชำรุดเสียหายและค่าใช้จ่ายในการสำรองข้อมูล

- ค่าใช้จ่ายส่วนเพิ่ม กรมธรรม์ประกันภัยควรคุ้มครองไปถึงค่าใช้จ่ายส่วนเพิ่มที่เกิดขึ้นจากการดำเนินการเพื่อให้สามารถเปิดดำเนินการและสามารถให้บริการได้อย่างต่อเนื่องในกรณีที่เกิดความเสียหายขึ้นกับศูนย์ประมวลผลข้อมูลหรือพื้นที่ปฏิบัติงานอื่น ๆ

- การทำธุรกรรมการเงินทางธนาคารอิเล็กทรอนิกส์ กรมธรรม์ประกันภัยควรคุ้มครองไปถึงความเสียหายหรือภาระหนี้สินอื่นๆ ที่เกิดขึ้นจากทำธุรกรรมทางการเงินบนเครือข่ายอิเล็กทรอนิกส์ เช่น ธุรกรรมการเงินบนเครือข่ายอินเตอร์เน็ต (internet banking)

- การหยุดชะงักของธุรกิจ ศูนย์ประมวลผลข้อมูล และองค์กรที่ให้บริการต่อผู้ใช้บริการจากภายนอกควรจะต้องได้เงินชดเชยคืนเมื่อเกิดความเสียหายทางการเงินจากการหยุดชะงักการปฏิบัติงานความเสียหายทางกายภาพของอุปกรณ์หรือสื่อเก็บข้อมูล

- เอกสารและบันทึกที่มีค่า ความคุ้มครองจากกรมธรรม์ควรครอบคลุมถึงมูลค่าที่เป็นตัวเงินของเอกสารและบันทึกข้อมูลที่อยู่ในรูปของกระดาษ (ไม่ใช่ตัวกลางหรือสื่ออิเล็กทรอนิกส์) หากเอกสารหรือบันทึกนั้นสูญหายหรือถูกทำลาย

- การปฏิบัติงานผิดพลาดและการละเว้น / ละเลยไม่ปฏิบัติหน้าที่ ฝ่ายจัดการควรจัดทำกรมธรรม์ประกันภัยให้คุ้มครองถึงความเสียหายที่เกิดขึ้นจากการละเลย ความผิดพลาด และการละเว้นใด/ละเลยไม่ปฏิบัติหน้าที่ในการให้บริการด้าน IT ต่อบุคคลอื่นด้วย (กรมธรรม์ส่วนใหญ่จะเขียนยกเว้นไม่คุ้มครองค่าใช้จ่ายอันเนื่องมาจากสาเหตุต่าง ๆ ดังต่อไปนี้)

- การทุจริตโดยพนักงาน
- การกระทำในลักษณะของการเผยแพร่ข้อมูล การดูหมิ่นหรือการทำให้เสียชื่อเสียง
- ภาระหนี้สินของบุคคลอื่นซึ่งอยู่ในความรับผิดชอบของผู้เอาประกันอันเนื่องมาจากสัญญาหรือข้อตกลง
- ภาระหนี้สินจากการขาดทุนหรือความเสียหายของทรัพย์สินของบุคคลอื่น
- การเจ็บป่วยหรืออาการบาดเจ็บทางร่างกายของบุคคล
- ภาระหนี้สินที่เกิดขึ้นเนื่องมาจากคำแนะนำของบุคคลที่สาม ไม่ว่าจะอยู่ในรูปของวิธีการ กระบวนงาน แนวทางปฏิบัติ ฯลฯ
- ภาระหนี้สินที่เกิดขึ้นเนื่องมาจากการเตรียมการเพื่อขอคืนภาษีเงินได้
- การสูญเสียซึ่งเกิดจากเจตนาหรือคำสั่งของผู้เอาประกัน

(5) การรักษาความปลอดภัยของข้อมูลสารสนเทศ

คณะกรรมการบริหารขององค์กรเป็นผู้รับผิดชอบโดยตรงต่อโปรแกรมการรักษาความปลอดภัยของข้อมูลสารสนเทศในภาพรวม เริ่มตั้งแต่การพัฒนา การนำไปใช้งาน และการบำรุงรักษา นอกจากนี้คณะกรรมการฯ ควรกำหนดแนวทางให้ฝ่ายจัดการดำเนินการ ควรทบทวนประสิทธิภาพในการปฏิบัติงานของฝ่ายจัดการ ควรกำหนดบุคคลผู้มีหน้าที่นำแนวทางดังกล่าวไปปฏิบัติ และควรให้ความเห็นชอบแนวนโยบายการรักษาความปลอดภัยและการดำเนินการตามนโยบายดังกล่าวอย่างน้อยปีละครั้ง แต่อย่างไรก็ดี คณะกรรมการบริหารควรกำหนดแนวทางให้ฝ่ายจัดการได้รับทราบความคาดหวังและข้อกำหนดต่างๆ ได้แก่

- การกำกับดูแลและการประสานงานจากส่วนกลาง
- ขอบเขตของหน้าที่และความรับผิดชอบ
- การวัดความเสี่ยง
- การเฝ้าติดตามดูแลและการทดสอบ
- การจัดทำรายงาน
- ระดับของความเสี่ยงที่เหลืออยู่ (residual risk) หลังจากการใช้มาตรการควบคุมภายในที่ยอมรับได้แล้ว

ข้อมูลสารสนเทศเป็นสินทรัพย์ที่มีความสำคัญมากที่สุดอย่างหนึ่ง ดังนั้น ฝ่ายจัดการและคณะกรรมการบริหารของสถาบันการเงินควรปกป้องข้อมูลสารสนเทศเพื่อสร้างความเชื่อมั่นระหว่างสถาบันการเงินและลูกค้าของตนเพราะว่าสถาบันการเงินอาจจะถูกกระทบกระเทือนอย่างรุนแรงจนกระทบกับความสามารถในการหารายได้หรือเงินกองทุน ถ้าเกิดเหตุการณ์ดังต่อไปนี้ คือ การสูญหาย การถูกทำลาย หรือการเปิดเผยข้อมูลที่สำคัญโดยไม่ได้รับความเห็นชอบ

ฝ่ายจัดการควรทำหน้าที่เป็นผู้พัฒนาโปรแกรมรักษาความปลอดภัยของข้อมูลสารสนเทศ ภายใต้การกำหนดแนวทางในการพัฒนาฯ การนำเอาระบบรักษาความปลอดภัยฯออกใช้งาน การให้ความเห็นชอบในการปรับปรุงแก้ไขรายละเอียดต่างๆ และการมอบหมายหน้าที่ความรับผิดชอบ และการทบทวนความเพียงพอของระบบรักษาความปลอดภัยเป็นประจำทุกปี (สอดคล้องกับข้อกำหนดตามกฎหมาย GLBA ของประเทศสหรัฐอเมริกา) อนึ่งโปรแกรมรักษาความปลอดภัยควรปกป้องข้อมูลสำคัญของลูกค้าจากการคุกคามความปลอดภัยหรือความถูกต้องเชื่อถือได้ของข้อมูลผู้ตรวจสอบควรศึกษารายละเอียดเพิ่มเติมจากคู่มือตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล

(6) การดำเนินธุรกิจอย่างต่อเนื่อง

คณะกรรมการบริหารและผู้บริหารระดับสูงมีหน้าที่รับผิดชอบในการจัดทำแนวนโยบาย กระบวนการปฏิบัติงาน และการมอบหมายหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการวางแผนการดำเนินธุรกิจอย่างต่อเนื่องขององค์กร อนึ่ง ฝ่ายจัดการควรจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่องเป็นลายลักษณ์อักษร ปรับปรุงแผนดังกล่าวให้เป็นปัจจุบันอยู่เสมอ ทดสอบแผนดังกล่าวไปพร้อมๆ กับความพร้อมของระบบสำรอง เพื่อลดความเสี่ยงจากระบบขัดข้องและการบุกรุกระบบโดยไม่ได้รับอนุญาตเป็นประจำทุกปี และรายงานผลการทดสอบแผนดังกล่าวพร้อมระบบสำรองอย่างน้อยปีละครั้งให้คณะกรรมการบริหาร ผู้ตรวจสอบควรศึกษาเพิ่มเติมจากคู่มือตรวจสอบการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

(7) การพัฒนาและจัดหาโปรแกรมระบบงาน

ผู้บริหารระดับสูงควรประเมินและลดความเสี่ยงจากการปฏิบัติงานหรือการทำรายการธุรกรรมที่เกี่ยวข้องกับการพัฒนาและจัดหาโปรแกรมระบบงาน โดยการ**พัฒนาแนวนโยบายและมาตรฐานการปฏิบัติงานและระบบการควบคุมต่างๆสำหรับกระบวนการพัฒนาและจัดหาโปรแกรมระบบงานขึ้นมาเป็นการเฉพาะ** เพราะว่าการพัฒนาและจัดหาโปรแกรมระบบงานที่ปราศจากการควบคุมอาจนำมาซึ่งความเสี่ยงในระดับที่ไม่สามารถยอมรับได้

ฝ่ายจัดการควรกำกับแนวทางการพัฒนาและจัดหาโปรแกรมระบบงาน ตามแนวความคิดในการเรื่องวงจรของการพัฒนาระบบงาน (System Development Life Cycle – SDLC) หรือใช้แนวทางอื่นๆ ที่คล้ายกันและเหมาะสมกับสภาพแวดล้อมทางด้าน IT ที่เป็นอยู่ อย่างไรก็ดี แม้ว่าSDLC จะช่วยในการกำหนด / ระบุความเสี่ยงในการพัฒนาระบบงานได้แต่ถ้ามีการจัดซื้อโปรแกรมระบบงานจากผู้พัฒนาระบบงานภายนอก สถาบันการเงินก็ควรที่จะพิจารณาไปถึงสภาวะแวดล้อมในการควบคุม ชื่อเสียง และความสามารถของผู้ผลิตก่อนการจัดซื้อจัดหาจากผู้ให้บริการรายดังกล่าว

สถาบันการเงินหรือองค์กรจึงควรจัดให้มีขั้นตอนในการพิสูจน์ทราบว่าระบบควบคุมต่างๆยังมีอยู่ครบถ้วนและสามารถป้องกันปัญหาที่เกี่ยวข้องกับความถูกต้องเชื่อถือได้ของข้อมูลและโปรแกรมได้ในทุกขั้นตอนของ SDLC และวิเคราะห์ผลกระทบที่จะเกิดขึ้นกับการปฏิบัติงานประจำวันในช่วงต้นก่อนการพัฒนาและการจัดหาโปรแกรมระบบงาน เพื่อให้ทราบถึงค่าใช้จ่ายส่วนเพิ่มและประเด็นปัญหาต่าง ๆ ที่ฝ่ายจัดการจะต้องเข้าไปให้การสนับสนุน นอกจากนี้ สายงานตรวจสอบภายในควรเข้ามามีส่วนร่วมให้เกิดความมั่นใจว่าฝ่ายจัดการได้นำระบบการรักษาความปลอดภัยที่ดีและเหมาะสมมาใช้ควบคุมในทุกขั้นตอนของการพัฒนาและการจัดหาโปรแกรมระบบงาน

ฝ่ายจัดการควรทดสอบด้าน IT โปรแกรมระบบงานและผลิตภัณฑ์ใหม่ ๆ อย่างถ่องแท้ก่อนที่จะนำมาใช้งานจริง เพื่อให้ทราบว่าเครื่องมือโปรแกรมระบบงานสามารถทำงานได้อย่างเหมาะสมและได้ผลลัพธ์ตามต้องการ รวมทั้งทำการทดสอบว่าโปรแกรมระบบงาน IT แบบใหม่สามารถทำงานร่วมกันกับระบบงาน IT เดิมที่มีอยู่และระบบงาน IT ของคู่ค้า/ผู้จัดได้อย่างมีประสิทธิภาพ ดังนั้น ฝ่ายจัดการควรนำเอาแนวทางการพัฒนาโปรแกรมนำร่อง (Pilot) หรือต้นแบบ (Prototype) มาทดลองใช้ก่อนที่จะนำเอาโปรแกรมระบบงานดังกล่าวมาใช้งานเป็นการทั่วไปภายในองค์กรและควรทำการทดสอบเป็นระยะเพื่อการหาแนวทางในการควบคุมความเสี่ยงได้อย่างต่อเนื่อง

(8) การปฏิบัติงานประจำวัน Operations ด้านเทคโนโลยีสารสนเทศ

ผู้บริหารระดับสูงควรตระหนักถึงความเสี่ยงที่เกิดจากการปฏิบัติงานประจำวันและการทำรายการธุรกรรมที่เกี่ยวข้องกับการปฏิบัติงานด้าน IT และควรหาทางบรรเทาหรือลดความเสี่ยงลงตามลำดับ เพราะว่าบางสถาบันการเงินและผู้ให้บริการจากภายนอกอาจจะมีกลุ่มของผู้ปฏิบัติงานประจำวันด้าน IT มากกว่าหนึ่งกลุ่มขึ้นไป ทำให้มีจำนวนของศูนย์ปฏิบัติงานประจำวันและชนิดของงานที่จะต้องทำแตกต่างกันไปตามประเภทขององค์กร ได้แก่ ศูนย์ประมวลผลข้อมูลแบบรวมศูนย์ ศูนย์ประมวลข้อมูลแบบกระจายศูนย์ (distributed computing) การประมวลผลด้วยคอมพิวเตอร์ส่วนบุคคล การจัดการการเปลี่ยนแปลงแก้ไขโปรแกรมระบบงานและการเปลี่ยนแปลงสิทธิ์ในการเข้าถึงระบบ ระบบการรักษาความปลอดภัย การบริหารทรัพยากรด้าน IT และการดำเนินการตามแผนฉุกเฉินด้าน IT

ภาระหน้าที่ในการปฏิบัติงานประจำวันมีปัจจัยความเสี่ยงสำคัญ ๆ ซึ่งต้องอาศัยการจัดการและควบคุมที่มีประสิทธิภาพ เช่น การที่ผู้จัดการระบบและผู้บริหารระบบรักษาความปลอดภัยซึ่งมีสิทธิในระดับที่สูงมากหลาย ๆ ระดับในการควบคุมระบบงานที่เขาปฏิบัติงานหรือบริหารอยู่ ดังนั้น **องค์กรจะต้องจัดให้มีการบันทึกข้อมูลและติดตามทบทวนข้อมูลผ่านรายงานติดตามผลการดำเนินงาน (audit trails) และบันทึกข้อมูลในการทำงานของระบบคอมพิวเตอร์ต่างๆ (logs) ของกิจกรรมที่ผู้จัดการระบบและผู้บริหารระบบรักษาความปลอดภัยได้ดำเนินการไป** เพื่อควบคุมโอกาสที่จะเกิดความเสี่ยง ซึ่งผู้ตรวจสอบควรศึกษาเพิ่มเติมจากคู่มือตรวจสอบการปฏิบัติการ

(9) การบริหารความเสี่ยงในการใช้บริการจากผู้ให้บริการภายนอก

สถาบันการเงินจำเป็นต้องพึ่งพาผู้ให้บริการจากภายนอก ผู้จัดจำหน่ายโปรแกรมระบบงานและบุคคลที่สามอื่น ๆ ดังนั้น สถาบันการเงินบางแห่งที่มีโครงสร้างซับซ้อนมักจะมีแนวทางการบริหารงานผู้จำหน่ายหรือผู้ให้บริการฯที่ครอบคลุมความสัมพันธ์ทุกลักษณะซึ่งทางสายงานเทคโนโลยีฯมักจะไปขอใช้บริการจากผู้ให้บริการฯในหลายๆรูปแบบ เช่น การประมวลผลข้อมูล การ

พัฒนาโปรแกรมระบบงาน การบำรุงรักษาเครื่องมือคอมพิวเตอร์ แผนการดำเนินธุรกิจอย่างต่อเนื่อง การจัดเก็บรักษาข้อมูล การใช้บริการเครือข่ายอินเตอร์เน็ต และการบริหารระบบรักษาความปลอดภัย

คณะกรรมการบริหารและผู้บริหารระดับสูงมีหน้าที่รับผิดชอบในการกำกับและควบคุมดูแลความสัมพันธ์กับผู้ให้บริการจากภายนอกอย่างมีประสิทธิภาพ ทั้งนี้เพราะว่าระบบงาน IT ที่ต้องใช้เพื่อสนับสนุนเป้าหมายทางธุรกิจนั้นมักจะเป็นปัจจัยสำคัญที่มีผลต่อการตัดสินใจเลือกใช้บริการจากผู้ให้บริการฯ ดังนั้น การจัดการในเรื่องของผู้ให้บริการฯจึงมิได้ครอบคลุมเฉพาะด้าน IT อย่างเดียว แต่เกี่ยวข้องกับประเด็นของการกำกับดูแลที่ดีภายในองค์กรทั้งหมด (ธรรมาภิบาล) และเพื่อช่วยให้ฝ่ายจัดการมีแนวทางในการกำกับดูแลองค์กรที่มีประสิทธิภาพ องค์กรจะต้องพัฒนาแนวทางในการกำกับดูแลผู้ให้บริการฯที่จะช่วยให้ฝ่ายจัดการสามารถเข้าใจ เฝ้าติดตามดูแล ตรวจวัด/ประเมิน และควบคุมความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับการใช้บริการจากผู้ให้บริการฯ ในขณะเดียวกัน**คณะกรรมการบริหารและผู้บริหารระดับสูงควรพัฒนานโยบายและกระบวนการเพื่อกำกับดูแลขั้นตอนในการใช้บริการจากผู้ให้บริการฯที่ครอบคลุมไปถึงเรื่อง การกำหนดเป้าหมายและกลยุทธ์ การคัดเลือกผู้ให้บริการฯ การเจรจาต่อรองและการจัดทำสัญญา และการเฝ้าติดตามดูแลความสัมพันธ์กับผู้ให้บริการฯ ให้ครอบคลุมปัจจัยต่างๆ ดังต่อไปนี้**

- การสร้างความมั่นใจว่าความสัมพันธ์กับผู้ให้บริการฯจะช่วยสนับสนุนให้องค์กรสามารถดำเนินการได้ตามเป้าหมายและแผนกลยุทธ์
- การประเมินคุณสมบัติของผู้ให้บริการฯที่สัมพันธ์กับขอบเขตและความสำคัญของบริการที่จะจัดหา
- การปรับปรุงแผนงานในการเฝ้าติดตามดูแลการดำเนินงานของผู้ให้บริการฯ ในทุกส่วนงานขององค์กรให้เหมาะสมกับภาพรวมของความเสี่ยงเริ่มต้นและความเสี่ยงอื่นๆ ที่เกิดขึ้นประจำต่อเนื่องให้เป็นปัจจุบัน
- เวลาและทรัพยากรที่จัดสรรให้แก่การบริหารจัดการผู้ให้บริการฯ อย่างมีประสิทธิภาพนั้นขึ้นอยู่กับปัจจัยต่าง ๆ เช่น ความสำคัญของกระบวนการทำงานที่จะมอบหมายให้ผู้ให้บริการฯเป็นผู้ดำเนินการแทน ความรู้ของพนักงาน และความซับซ้อนของระบบงาน ซึ่งผู้ตรวจสอบสามารถศึกษารายละเอียดเพิ่มเติมได้จากคู่มือตรวจสอบการให้บริการด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก

2.3.4 การประเมินประสิทธิภาพและการเฝ้าติดตาม

สรุปแนวทางการปฏิบัติ

ฝ่ายจัดการของสถาบันการเงินควรจัดให้มีการเฝ้าติดตามและการรายงานกิจกรรมและความเสี่ยงด้าน IT ที่น่าพอใจ ตามแนวทางปฏิบัติดังนี้

- การทบทวนเป้าหมายตามแผนธุรกิจและกลยุทธ์ที่เกี่ยวข้องกับระบบ IT
- การพัฒนาตัวอ้างอิงหรือตัวชี้วัด (Benchmarks) สำหรับใช้วัดผลงานหรือประสิทธิภาพ
- การกำหนดและทบทวนข้อตกลงเกี่ยวกับระดับของการให้บริการที่ทำไว้กับคู่ค้า/ ผู้จัดจำหน่ายและบุคคลที่สามในรายที่มีความสำคัญ
- การปฏิบัติตามแนวทางในการควบคุมคุณภาพหรือการรับประกันคุณภาพในการเฝ้าติดตามดูแลและทดสอบผลิตภัณฑ์และแนวทางในการปฏิบัติงาน

สถาบันการเงินควรวัดผลและเฝ้าติดตามรูปแบบของความเสี่ยงที่มีอยู่ในหน้าที่งานด้าน IT อย่างต่อเนื่อง และการวัดผลและติดตามความเสี่ยงไปพร้อมๆกันสามารถแสดงผลในรูปแบบตารางแสดงความสัมพันธ์ (metric) ส่วนรูปแบบเฉพาะในการรายงานผลและความถี่ที่จะต้องกระทำนั้นขึ้นอยู่กับสภาพแวดล้อมด้าน IT ของสถาบันการเงิน โดยมีตัวอย่างดังนี้

- จำนวนของประเด็นต่างๆด้านความเสี่ยงด้าน IT ที่สามารถกำหนด/ระบุได้ (ซึ่งถูกปรับปรุงให้เป็นปัจจุบันอยู่เสมอเพื่อสะท้อนให้เห็นประเด็นที่เกิดขึ้นใหม่หรือที่ได้ถูกแก้ไขแล้ว)
- จำนวนของประเด็นต่างๆด้านความเสี่ยงด้าน IT ที่ผู้บริหารระดับสูงได้ให้ความเห็นชอบว่าเป็นความเสี่ยงที่สามารถยอมรับได้ (ควรมีการจัดเก็บข้อมูลความเสี่ยงทั้งหมด แนวทางการลดความเสี่ยงแบบต่างๆ และเอกสารแสดงการยอมรับของฝ่ายจัดการ)
- จำนวนของเหตุการณ์หรือประเด็นความเสี่ยงทั้งในอดีตและปัจจุบัน (ทั้งที่เกิดจากภายนอกองค์กรและภายในองค์กรที่หลบเลี่ยงระบบการควบคุมมาตรฐานได้)
- จำนวนของประเด็นด้านความเสี่ยงจากผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอกหรือผู้ตรวจสอบจากหน่วยงานภาครัฐ

(1) การวางแผนจนถึงวัดผลการดำเนินงานที่เกิดขึ้นจริง (Outcome - based Measurement)

สถาบันการเงินควร**ทบทวนหน้าที่งานด้าน IT เป็นระยะ ๆ และพิจารณาว่าองค์กรได้ปฏิบัติตามแผน เป้าหมาย และความคาดหวังที่ได้กำหนดไว้แล้ว** ให้สอดคล้องกับต้นทุนที่จ่ายลงไป และไม่มีการปฏิบัติผิดพลาดที่จะก่อให้เกิดความเสี่ยงกับองค์กร และฝ่ายจัดการควรบริหารงานจากการใช้บริการของผู้ให้บริการจากภายนอกโดยอาศัยบทลงโทษและการให้ผลตอบแทนเพิ่มเติมตามที่กำหนดไว้ในสัญญาจ้างงาน

(2) เกณฑ์เปรียบเทียบผลการปฏิบัติงาน (Performance benchmark)

สถาบันการเงินควร**กำหนดตัวชี้วัดหรือมาตรฐานของผลงาน**หรือประสิทธิภาพสำหรับงานด้าน IT และมีการติดตามทบทวนข้อมูลดังกล่าวอย่างสม่ำเสมอ เพื่อให้องค์กรรับทราบถึงปัญหาได้ล่วงหน้าและรับประกันได้ว่าภาระหน้าที่ด้าน IT สามารถดำเนินการได้ตามวัตถุประสงค์ขององค์กร ประเด็นที่ควรพิจารณารวมถึงความพร้อมใช้ของระบบคอมพิวเตอร์หลักและระบบเครือข่าย ศูนย์คอมพิวเตอร์ การฟื้นคืนของระบบ เงื่อนไขของความไม่สมดุล เวลาการตอบสนอง อัตราความผิดพลาด ปริมาณการทำรายการ การขอแก้ไขระบบหรือโปรแกรมเป็นกรณีพิเศษ และการรายงานปัญหาที่เกิดขึ้น

(3) ระดับของการให้บริการ

สถาบันการเงินควร**ทำสัญญาอย่างเป็นทางการกับผู้ให้บริการด้าน IT** ทั้งที่เป็นงานพัฒนาภายในองค์กรเองและงานที่ว่าจ้างให้บุคคลภายนอกองค์กรดำเนินการให้ เพื่อกำหนดระดับของการให้บริการ (Service Level Agreements) ซึ่งควรมีเนื้อหาครอบคลุมถึงสภาพแวดล้อมด้าน IT ทั้งหมดขององค์กร เพื่อให้องค์กรได้รับการประกันตามแต่ละระดับของการให้บริการที่ดีที่สุด มาตรฐานในการวัดผลการปฏิบัติงานถือเป็นตัวอย่างประเด็นในการพิจารณาระดับของการให้บริการตามที่ได้กล่าวไว้ในหัวข้อ (2) เกณฑ์เปรียบเทียบผลการปฏิบัติงาน

(4) การค้ำประกันคุณภาพและการควบคุมคุณภาพ

ฝ่ายจัดการควรกำหนดให้มีกระบวนการในการรับประกันคุณภาพ การประเมินผลการดำเนินการเป็นระยะภายในองค์กรเองหรือมอบหมายให้องค์กรอื่นดำเนินการ และควรนำเอาผลของการดำเนินการตามแผนดังกล่าวไปปรับปรุงแผนงานรับประกันคุณภาพในอนาคตต่อไป อนึ่ง กระบวนการดังกล่าวควรจะต้องประกอบไปด้วยมาตรการวัดผลการปฏิบัติงานภายในองค์กร คณะทำงานเฉพาะกิจ และการสำรวจความพอใจของลูกค้า

เป้าหมายเริ่มแรกของกิจกรรมการรับประกันคุณภาพ คือ เพื่อให้ได้ผลิตภัณฑ์ที่มีคุณสมบัติเป็นไปตามข้อกำหนดเหมาะสมกับการใช้งาน และจะต้องตอบคำถามพื้นฐาน 3 ประการดังต่อไปนี้

1) การรับประกันคุณภาพทำได้ผลจริงหรือไม่

2) การรับประกันคุณภาพทำได้ตามที่ถูกกำหนดหรือไม่

3) การรับประกันคุณภาพทำได้มีความเหมาะสมกับการใช้งานหรือไม่

อนึ่ง เป้าหมายของกิจกรรมรับประกันคุณภาพ (QC : quality Control) คือ การระบุจุดอ่อนในขั้นตอนการผลิตเพื่อหลีกเลี่ยงการสูญเสียทรัพยากรและค่าใช้จ่ายในการปรับปรุงแก้ไขผลิตภัณฑ์ ในขณะเดียวกันสถาบันการเงินจะได้ประโยชน์เพิ่มเติมอื่นนอกจากการรับประกันคุณภาพแล้วยังได้รับประโยชน์ในการป้องปรามการทุจริตอีกด้วย นอกจากนี้ ฝ่ายจัดการควรทำการทดสอบคุณภาพของระบบงานใหม่ก่อนนำเอามาตรการดังกล่าวออกมาใช้งานจริง ทั้งนี้ การทดสอบควรเป็นอิสระจากผู้ที่ทำหน้าที่ด้านการพัฒนาโปรแกรมระบบ (หากเป็นโปรแกรมที่สถาบันการเงินพัฒนาขึ้นเอง) และควรมีการตรวจรับโปรแกรมโดยผู้ใช้งาน (User Acceptance Testing) สำหรับโปรแกรมที่พัฒนาโดยบุคคลภายนอก (Off - the - shelf) ทั้งนี้ การทดสอบระบบงานใหม่อย่างเต็มรูปแบบทุกแง่มุมจะช่วยชี้ให้เห็นว่ามีชุดสอดแทรกชุดคำสั่งที่ไม่ดีเป็นอันตรายกับองค์กรหรือไม่ และช่วยให้เห็นว่าระบบงานมีประสิทธิภาพหรือไม่ ซึ่งฝ่ายจัดการสามารถรับทราบข้อมูลดังกล่าวได้จากรายงานด้านการรับประกันคุณภาพอันประกอบไปด้วยข้อมูลเกี่ยวกับระบบการควบคุมและสำหรับสภาพแวดล้อมในการให้บริการกับลูกค้าจริง

(5) การปฏิบัติตามกฎระเบียบ ข้อบังคับของทางการ

สถาบันการเงินควรพัฒนากระบวนการในการพัฒนา การนำออกใช้งานจริงและการเฝ้าติดตามดูแลการวัดผลการปฏิบัติตามแนวนโยบาย มาตรฐานการปฏิบัติงาน และแนวทางการปฏิบัติงานจริงด้าน IT (IT compliance) ทั้งนี้ **สถาบันการเงินควรทำการประเมินตนเองเป็นประจำ** (เพื่อช่วยขยายมุมมองของฝ่ายจัดการโดยการรวบรวมความรู้ และการรับทราบผลการใช้งานโดยผู้ที่เกี่ยวข้องกับการประเมินตนเอง และยังช่วยระบุความจำเป็นในการเปลี่ยนแปลงหรือปรับปรุงนโยบายให้เป็นปัจจุบันอีกด้วย) นอกเหนือจากการใช้บริการตรวจสอบจากผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอกหรือผู้ตรวจสอบอิสระ

2.4 การพิจารณาเลือกผู้ให้บริการทางด้านเทคโนโลยีสารสนเทศ

สรุปแนวทางการปฏิบัติ

ผู้ให้บริการด้านเทคโนโลยี (Technology Service Provider- TSP) ควรสนับสนุนสถาบันการเงินและหน่วยงานภายนอกที่เป็นลูกค้า โดยการปฏิบัติดังต่อไปนี้

- การส่งมอบงบการเงินที่ผ่านการตรวจสอบแล้ว อย่างน้อยปีละหนึ่งครั้ง
- การจัดทำสัญญาที่มีความชัดเจนและใช้ภาษาที่เหมาะสม
- จัดให้มีการตรวจสอบผลการดำเนินการโดยผู้ตรวจสอบอิสระและรายงานผลการตรวจสอบดังกล่าวให้ลูกค้าทราบ
- การจัดให้มีหน่วยงานให้บริการและการสนับสนุนงานกับกลุ่มผู้ใช้งาน

สถาบันการเงินควรกำกับดูแลคุณภาพของการให้บริการ สถานะทางการเงิน และสภาพแวดล้อมในการควบคุมดูแลของผู้ให้บริการด้าน IT ควรศึกษาเพิ่มเติมจากคู่มือตรวจสอบการให้บริการด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก ซึ่งกล่าวถึงปัญหาในการบริหารความเสี่ยงของผู้รับบริการเป็นหลัก ส่วนผู้ให้บริการด้าน IT นั้นหมายถึงสถาบันการเงิน กิจการในเครือและบุคคลที่สามซึ่งมีความเป็นอิสระ ซึ่งมีหน้าที่ในการสนับสนุนการกำกับดูแลการให้บริการจากผู้รับบริการในระดับที่เหมาะสมกับระดับของความสำคัญของบริการนั้นที่มีต่อผู้รับบริการ แต่อย่างไรก็ตาม ขนาดและความสลับซับซ้อนของผู้ให้บริการฯ มิได้มีผลกระทบที่สำคัญ กับความพยายามในการบริหารความเสี่ยงของผู้รับบริการ ดังนั้น เนื้อหาในส่วนนี้จึงมุ่งเสนอแนวทางในการพิจารณาที่ผู้ให้บริการฯ จะต้องทำเพื่อให้การสนับสนุนผู้ใช้บริการที่เป็นสถาบันการเงินในการรักษาความปลอดภัย ความน่าเชื่อถือและการตอบสนองภาระในการให้บริการลูกค้าตามกฎ ระเบียบ และข้อบังคับของทางการ

2.4.1 สารสนเทศทางการเงิน

สถาบันการเงินควรได้รับข้อมูลสารสนเทศที่เป็นปัจจุบันและเพียงพอในการวิเคราะห์ฐานะและการดำเนินการทุกๆด้านของผู้ให้บริการด้าน IT เพื่อการสำรวจฐานะและผลการดำเนินงานทุกด้านอย่างละเอียด (due diligence) และการติดตามอย่างต่อเนื่อง ผู้ให้บริการด้าน IT ที่เป็นกิจการมหาชนจะมีพันธะที่ต้องส่งงบการเงิน ซึ่งจะเป็นแหล่งที่มาของข้อมูลทางการเงินแหล่งหนึ่ง สำหรับ**กรณีที่ผู้ให้บริการเป็นกิจการเอกชนที่ไม่ต้องเปิดเผยงบการเงินต่อสาธารณชนนั้น สถาบันการเงินและหน่วยงาน**

ภายนอกควรจะทำข้อตกลงไว้ว่า ผู้ให้บริการด้าน IT จะต้องส่งมอบงบการเงิน (ซึ่งควรผ่านการตรวจสอบโดยผู้ตรวจสอบที่มีความเป็นอิสระ) **อย่างน้อยปีละครั้ง**

เมื่อเกิดการล้มละลายทางการเงินของผู้ให้บริการด้าน IT เกิดขึ้น สถาบันการเงินของผู้ขอใช้บริการอาจทำให้เกิดผลเสียหายอย่างใหญ่หลวงเพราะบริการที่เคยได้รับอาจจะหยุดชะงักไปโดยที่ผู้ให้บริการอาจจะไม่สามารถส่งหนังสือแจ้งเหตุผลในการหยุดให้บริการล่วงหน้า 60-120 วัน ได้ตามสัญญา ซึ่งทำให้สถาบันการเงินจำเป็นต้องเร่งหาศูนย์ประมวลผลสำรองชดเชยโดยด่วน อนึ่งแม้ว่าสถาบันการเงินจะมีฐานะเป็นเจ้าของข้อมูล และสามารถขอไฟล์ข้อมูลปัจจุบันจากผู้ให้บริการของตน แต่**ผู้ให้บริการซึ่งเป็นเจ้าของโปรแกรมและเอกสารต่าง ๆ ที่จำเป็นต้องใช้ในการประมวลผลไฟล์ข้อมูลเหล่านั้นอาจจะไม่เต็มใจ จะส่งมอบโปรแกรมดังกล่าวให้แก่ลูกค้า หากไม่มีการระบุไว้ในข้อกำหนดพิเศษของสัญญา** ดังนั้น เจ้าหนี้ของผู้ให้บริการฯอาจจะพยายามเรียกชำระหนี้โดยอ้างบุริมสิทธิ์เหนือโปรแกรมระบบงานซึ่งเป็นทรัพย์สินที่สำคัญของผู้ให้บริการฯ ทำให้สถาบันการเงินผู้ใช้บริการจำเป็นที่จะต้องดำเนินการดังต่อไปนี้

(1) ชำระหนี้ให้แก่เจ้าหนี้แทนผู้ให้บริการฯ แล้วว่าจ้างผู้เชี่ยวชาญจากภายนอกมาดำเนินการศูนย์ประมวลผลต่อไป

(2) การแปลงรูปแบบของแฟ้มข้อมูลแล้วมอบหมายให้ผู้ให้บริการรายอื่นดำเนินการต่อไป

(3) การลงทุนจัดหาเครื่องมือและอุปกรณ์คอมพิวเตอร์และโปรแกรมระบบงานเพื่อดำเนินการเองภายในองค์กร แต่ไม่ว่าสถาบันการเงินผู้ใช้บริการจะเลือกใช้แนวทางใดก็ตาม สถาบันการเงินจะต้องลงทุนจำนวนสูงมากและใช้เวลาในการดำเนินการยาวนานมากเกินกว่าจะสามารถยอมรับได้

ผู้ให้บริการด้าน IT ที่กำลังมีปัญหาทางการเงินควรติดต่อให้ข้อมูลแก่ลูกค้าของตน ควรจัดหาแหล่งเงินทุนเพิ่มเติม หรือจัดทำแผนเพิ่มทุนเพื่อให้ลูกค้าของตนคลายความวิตกกังวลให้รวดเร็วที่สุดเท่าที่จะทำได้ และสถาบันการเงินควรประเมินความสำคัญของบริการด้าน IT ดังกล่าวและพิจารณาทบทวนการทำสัญญาหรือต่ออายุสัญญากับผู้ให้บริการฯที่ไม่สามารถให้ข้อมูลทางการเงินตามที่ควรจะเป็นได้

2.4.2 การทำสัญญา

ผู้ให้บริการฯ และสถาบันการเงินที่เป็นลูกค้าควรเจรจาต่อรองในการจัดทำสัญญาให้ครอบคลุมถึงประเด็นต่าง ๆ ตามคู่มือตรวจสอบการให้บริการด้านเทคโนโลยีจากบุคคลภายนอก ทั้งนี้

สถาบันการเงินควรจัดทำสัญญาที่มีความชัดเจนเป็นลายลักษณ์อักษร โดยมีรายละเอียดเพียงพอเพื่อเป็นหลักประกันสำหรับประสิทธิภาพ ความน่าเชื่อถือ การรักษาความปลอดภัย การรักษาความลับ และการรายงานผลการดำเนินงานเพราะว่าสัญญาที่ร่างไม่ดีหรือไม่ผ่านการสอบทานที่เหมาะสมอาจจะทำให้เกิดความเสี่ยงต่อทั้งสถาบันการเงินผู้ใช้บริการและผู้ให้บริการเพิ่มขึ้น ดังนั้น เพื่อหลีกเลี่ยงหรือลดปัญหาที่อาจเกิดขึ้นจากร่างสัญญาดังกล่าว จึงควรมอบหมายให้บริษัทที่ปรึกษาทางกฎหมายที่มีความคุ้นเคยกับคำศัพท์และข้อจำกัดต่างๆ ของสัญญาจ้างประมวลผลข้อมูลเป็นผู้ทำหน้าที่สอบทานร่างสัญญาดังกล่าวเพื่อปกป้องผลประโยชน์ของคู่สัญญาแต่ละฝ่าย อนึ่ง เนื่องจากสัญญาดังกล่าวครอบคลุมระยะเวลาในการดำเนินการจำนวนหลายปี จึงควรมีการจัดเก็บข้อมูลที่ได้ตกลงกันไว้ทั้งหมดในขั้นตอนการเจรจาต่อรองไว้ในสัญญาชุดที่ได้มีการลงนามกันไว้เรียบร้อยแล้วด้วย

สัญญาเป็นตัวกำหนดมาตรฐานขั้นต่ำในการให้บริการประมวลผลข้อมูลสารสนเทศและหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องสถาบันการเงินอาจเผชิญกับสถานการณ์ที่ผู้ให้บริการไม่สามารถหรือไม่เต็มใจที่จะยอมรับเงื่อนไขที่กำหนดให้ผู้ให้บริการต้องจัดให้มีกระบวนการบริหารความเสี่ยงที่มีประสิทธิภาพ หากเกิดสถานการณ์เช่นนี้ **มีแนวทางดำเนินการ 2 วิธี คือ**

(1) ไม่ควรทำสัญญากับผู้ให้บริการรายดังกล่าว

(2) ดำเนินมาตรการควบคุมภายในเพิ่มเติมจากข้อตกลงที่ผู้ให้บริการรับจะดำเนินการแล้ว และหากสถาบันการเงินยังมีปัญหาจากการจะต้องทบทวนข้อมูลตามที่ทางการกำหนด สถาบันการเงินก็ควรแจ้งให้ผู้ใช้งานและหน่วยงานภาครัฐทราบเพื่อขอรับการสนับสนุนต่อไป

2.4.3 รายงานผลการตรวจสอบ

ผู้ให้บริการด้าน IT ควรอำนวยความสะดวกให้แก่ผู้สอบบัญชีของสถาบันการเงินผู้ใช้บริการในการเข้าถึงศูนย์ประมวลข้อมูลของตน เพื่อให้ผู้ตรวจสอบภายนอกสามารถทำหน้าที่ในการตรวจสอบได้ตามที่สถาบันการเงินต้องการ หรือมิฉะนั้น ผู้ให้บริการเองก็สามารถจัดทำรายงานการตรวจสอบ รายงานความเพียงพอของระบบการควบคุมและการตรวจสอบอย่างอิสระอื่นๆ และจัดส่งให้แก่สถาบันการเงินผู้ใช้บริการโดยตรงแทนก็ได้ ซึ่งผู้ตรวจสอบควรศึกษาข้อมูลเพิ่มเติมจากคู่มือตรวจสอบการตรวจสอบภายในและภายนอก

2.4.4 การให้บริการแก่ลูกค้า

ผู้ให้บริการควรจัดทำแผนงานการให้บริการแก่ลูกค้าที่สามารถใช้ในการติดตามประสิทธิภาพ ติดตามการแก้ไขปัญหาหรือรับฟังความคิดเห็นของลูกค้าและแก้ไขปัญหาได้อย่างทันท่วงที ทั้งนี้ รูปแบบของแผนงานการให้บริการแก่ลูกค้าจะแตกต่างกันไปขึ้นกับขนาดของฐานลูกค้า

ถ้าเป็นผู้ให้บริการรายใหญ่อาจจัดตั้งศูนย์รับเรื่องร้องเรียนหรือ call center ซึ่งมีโปรแกรมระบบงานที่ช่วยติดตามและแก้ไขปัญหาให้กับลูกค้าได้อย่างรวดเร็ว ในขณะที่ผู้ให้บริการรายย่อยมีรูปแบบของบริการที่เป็นมาตรฐานน้อยกว่า อย่างไรก็ดี มีกิจกรรมที่ผู้ให้บริการควรร่วมมือกัน ดังต่อไปนี้

- กำหนดให้มีแนวนโยบายของแผนงานการให้บริการแก่ลูกค้าซึ่งครอบคลุมไปถึงเรื่อง วิธีการปฏิบัติงาน การกำหนดรูปแบบพื้นฐานของความรับผิดชอบ การกำหนดระยะเวลาที่ใช้ในการเริ่มต้นให้บริการ (response times) ที่น้อยที่สุด และการมอบอำนาจให้แก่พนักงานอาวุโส
- ติดตามปัญหาและแก้ไขให้สำเร็จลุล่วงจากรายงานบันทึกผลการปฏิบัติงานที่จัดเก็บไว้ภายในระบบ (logs) เพื่อประเมินระยะเวลาที่ใช้ให้บริการและระบุประเด็นของปัญหาร่วมกันของผู้ใช้งาน
- จัดให้มีการรายงานเป็นประจำ เพื่อติดตามสัญญาหรือข้อตกลงในการให้บริการ
- รับฟังความคิดเห็นจากการสัมภาษณ์กลุ่มผู้ใช้งาน หรือจากการสำรวจลูกค้า

ผู้ให้บริการควรสนับสนุนให้สถาบันการเงินที่เป็นลูกค้าของตนได้รวมตัวกันเป็นกลุ่มผู้ใช้งาน หากลูกค้ามีจำนวนมากพอ เพื่อประโยชน์ของทั้งผู้ให้บริการและสถาบันการเงินที่ใช้บริการเอง เพราะว่ากลุ่มผู้ใช้งานสามารถพูดคุยกันและหาแนวทางในการแก้ปัญหาหลักที่ต่างก็มีร่วมกันได้เป็นอย่างดี

<u>ส่วนที่ 3</u> แนวทางการตรวจสอบ

3.1 วัตถุประสงค์ของการตรวจสอบ

เพื่อพิจารณาคุณภาพและประสิทธิภาพของการบริหารงานด้าน IT และช่วยให้**ผู้ตรวจสอบสามารถประเมินความเพียงพอของกระบวนการบริหารความเสี่ยงด้าน IT ขององค์กรได้ อันประกอบไปด้วยการตระหนักรู้และการมีส่วนร่วมของฝ่ายจัดการ การประเมินความเสี่ยง นโยบายและขั้นตอนการปฏิบัติงาน การรายงานผล การเฝ้าติดตามดูแลอย่างต่อเนื่องและการติดตามผลหลังการตรวจสอบ**

แผนงานการตรวจสอบชุดนี้มีวัตถุประสงค์เพื่อช่วยผู้ตรวจสอบในการพิจารณาประสิทธิภาพของกระบวนการบริหารงานด้าน IT ของสถาบันการเงิน อย่างไรก็ดี ผู้ตรวจสอบสามารถเลือกใช้เฉพาะบางส่วนของแผนงานการตรวจสอบได้ ตามขนาด ความซับซ้อน และธรรมชาติของธุรกิจของสถาบันการเงินที่ตรวจสอบ

<u>วัตถุประสงค์ที่ 1</u>: เพื่อพิจารณาขอบเขตและเป้าหมายที่เหมาะสมในการตรวจสอบ

1. สอบทานรายงานเดิม เพื่อค้นหาประเด็นที่ค้างอยู่หรือปัญหาที่เกิดขึ้นแล้วในอดีต โดยตรวจสอบรายงานต่อไปนี้

- รายงานผลการตรวจสอบของหน่วยงานภาครัฐ
- รายงานผลการตรวจสอบของผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก
- การทดสอบระบบรักษาความปลอดภัยโดยผู้ตรวจสอบอิสระ
- รายงานผลการตรวจสอบผู้ให้บริการฯโดยทางการและผู้ตรวจสอบอื่น ๆ

2. การสอบทานข้อชี้แจงของฝ่ายจัดการที่มีต่อข้อสังเกตจากการตรวจสอบที่ยกขึ้นกล่าวถึง หรือข้อสังเกตจากการตรวจสอบครั้งก่อน โดยพิจารณาจากประเด็นต่อไปนี้

- ความเหมาะสมและทันเวลาในการแก้ไขปัญหาตามข้อสังเกตจากการตรวจสอบ
- การแก้ไขปัญหาตรงไปที่ต้นตอของปัญหามากกว่าการแก้ไขตามสถานการณ์เฉพาะหน้าที่ปรากฏให้เห็น
- การดำรงอยู่ของประเด็นปัญหาที่สำคัญต่าง ๆ
- ฝ่ายจัดการได้ดำเนินการประการใดบ้างเพื่อการแก้ไขข้อผิดพลาดในการ

ปฏิบัติงานที่ถูกตรวจพบและแสดงผลในรายงานผลการตรวจสอบ

3. สัมภาษณ์ฝ่ายจัดการและทบทวนคำตอบที่ฝ่ายจัดการตอบในขั้นตอนของการรวบรวมข้อมูลก่อนการตรวจสอบ (pre – exam) เพื่อระบุการเปลี่ยนแปลงในโครงสร้างพื้นฐานด้าน IT หรือผลิตภัณฑ์และบริการใหม่ที่อาจจะทำให้สถาบันการเงินมีความเสี่ยงสูงมากขึ้นโดยพิจารณาจาก

- ผลิตภัณฑ์หรือบริการที่ส่งมอบให้แก่ผู้ใช้ทั้งภายในและภายนอกองค์กร
- โครงสร้างของเครือข่าย (network topology) ซึ่งรวมความไปถึงการตั้งค่าตัวแปรสำหรับระบบงานหรือโปรแกรมและองค์ประกอบอื่น ๆ
- รายชื่อของอุปกรณ์คอมพิวเตอร์และโปรแกรมระบบงาน
- รายชื่อบุคลากรสำคัญที่ลาออกไปหรือรับเข้ามาใหม่
- รายชื่อของผู้ให้บริการทางด้าน IT และผู้จำหน่ายโปรแกรมระบบงาน
- ข้อมูลในการติดต่อสื่อสารกับหน่วยงานที่ทำหน้าที่กำกับควบคุมอื่น ๆ เช่น การสอบทานสินเชื่อ การบริหารความเสี่ยงด้านสินเชื่อ การรับประกันคุณภาพของสายงานธุรกิจ และการตรวจสอบภายใน เป็นต้น
- ข้อมูลความเสียหายทางการเงินที่เกิดจากการให้สินเชื่อ และการปฏิบัติงานประจำวันซึ่งคาดว่ามีสาเหตุมาจากหรืออาจจะมีสาเหตุมาจากระบบงานด้านIT เช่น ปัญหาของระบบงานต่างๆ ปัญหาการทุจริตจากการควบคุมที่ไม่ดีและปัญหาจากการเปลี่ยนแปลงแก้ไขโปรแกรมและการปฏิบัติงานที่ไม่ดีพอ เป็นต้น
- การเปลี่ยนแปลงขั้นตอนในการปฏิบัติงานธุรกิจภายในองค์กร
- การปรับปรุงเปลี่ยนแปลงโครงสร้างองค์กร

<u>วัตถุประสงค์ที่ 2:</u> เพื่อตรวจสอบว่าคณะกรรมการบริหารและผู้บริหารระดับสูงได้ตระหนักถึงความสำคัญของระบบงานด้าน IT ในฐานะที่เป็นส่วนหนึ่งที่มีความสำคัญในการส่งเสริมธรรมาภิบาลขององค์กรตั้งแต่การกำหนดแนวนโยบาย ขั้นตอนการปฏิบัติงานและการควบคุมด้าน IT

1. ทบทวนผังโครงสร้างองค์กรและสายงานด้าน IT เพื่อพิจารณาประเด็นต่าง ๆ ดังต่อไปนี้

- โครงสร้างขององค์กรเอื้ออำนวยให้ระบบงานด้าน IT สามารถให้การสนับสนุนการดำเนินงานของสายงานอื่น ๆ ทั้งองค์กรได้อย่างมีประสิทธิภาพ
- ผู้บริหารของสายงานด้าน IT รายงานผลขึ้นตรงต่อผู้บริหารระดับสูงขององค์กร

- ความรับผิดชอบของสายงานด้าน IT ได้ถูกแบ่งแยกออกมาจากกิจกรรมของการดำเนินธุรกิจ

- มีการแบ่งแยกหน้าที่การปฏิบัติงานอย่างเหมาะสม

- ได้มีการทบทวนข้อมูลของบุคลากรที่มีความสำคัญและพนักงานปฏิบัติงานเพื่อพิจารณาความเหมาะสมต่างๆ คือ ความรู้ความสามารถ ลำดับชั้นการบังคับบัญชา และแผนการสืบทอดตำแหน่งบริหาร

- ทบทวนและประเมินขอบเขตของงานในความรับผิดชอบของบุคลากรที่กำหนดเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่า มีการกำหนดนิยามของผู้มีอำนาจหน้าที่ ความรับผิดชอบและความชำนาญด้าน IT ที่จำเป็นไว้อย่างชัดเจน และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

- ระบุตำแหน่งงานหลักที่มีความสำคัญ เพื่อตรวจสอบว่าขอบเขตของงานในความรับผิดชอบที่กำหนดเป็นลายลักษณ์อักษรไว้นั้น มีบุคลากรที่จะทำหน้าที่แทนที่ได้ผ่านการฝึกอบรมมาแล้ว มีแผนการสืบทอดอำนาจที่ใช้เวลาไม่นานนักในกรณีที่เกิดการสูญเสียผู้บริหารหรือพนักงานที่สำคัญไป

- พิจารณาประสิทธิภาพของการติดต่อสื่อสารของฝ่ายจัดการและการเฝ้าติดตามดูแลการปฏิบัติงานทางด้าน IT ที่ดี

- หารือกับผู้ตรวจสอบเพื่อดูขอบเขตของการตรวจสอบว่าครอบคลุมเพียงพอหรือไม่และดูผลการตอบสนองของฝ่ายจัดการต่อจุดอ่อนที่ตรวจสอบพบ

<u>วัตถุประสงค์ที่ 3</u>: ตรวจสอบความเหมาะสมของการวางแผนงานและการประเมินความเสี่ยง IT

1. สอบทานรายชื่อของคณะกรรมการบริหาร คณะกรรมการด้าน IT และคณะกรรมการอื่น ๆ ที่ทำหน้าที่เกี่ยวข้องกับงานด้าน IT ว่าประกอบไปด้วยบุคลากรที่เหมาะสมและมีการประชุมอย่างสม่ำเสมอหรือไม่

2. สอบทานรายงานการประชุมคณะกรรมการบริหารและคณะกรรมการอื่น ๆ ที่เกี่ยวข้องเพื่อดูว่าผู้บริหารระดับสูงได้ให้การสนับสนุนและกำกับดูแลกิจกรรมด้าน IT

3. ตรวจสอบว่าคณะกรรมการต่าง ๆ ได้ทบทวน อนุมัติ/ให้ความเห็นชอบและรายงานผลต่อคณะกรรมการสถาบันการเงินในประเด็นต่าง ๆ ต่อไปนี้

- การประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลสารสนเทศ

- แผนกลยุทธ์ทั้งระยะสั้นและระยะยาวด้าน IT

- แผนงานและมาตรฐานการปฏิบัติงานประจำวันด้าน IT

- การจัดสรรทรัพยากร เช่น การจัดซื้อ/จัดหาเครื่องมือคอมพิวเตอร์และโปรแกรมระบบงาน และลำดับของโครงการต่างๆ ที่มีความสำคัญ เป็นต้น

- สถานภาพของโครงการที่มีความสำคัญ

- งบประมาณด้าน IT และค่าใช้จ่ายดำเนินงานในปัจจุบัน

- การศึกษาค้นคว้าและการพัฒนาด้าน IT

- การแก้ไขตามข้อสังเกตที่สำคัญๆตามรายงานของผู้ตรวจสอบภายในและผู้ตรวจสอบจากภายนอก

4. ตรวจสอบว่าคณะกรรมการบริหารและผู้บริหารระดับสูงได้ให้ความสำคัญอย่างเพียงพอในการพิจารณาปัญหาต่างๆ ด้าน IT ในขั้นตอนของการกำหนดแผนกลยุทธ์ด้านธุรกิจโดยรวมครอบคลุมประเด็นต่างๆ เหล่านี้ ได้แก่

- การประเมินความเสี่ยง

- แผนกลยุทธ์ด้าน IT

- สถานภาพปัจจุบันของโครงการหลักสำคัญฯ ทั้งที่อยู่ระหว่างการดำเนินการและที่อยู่ในแผนงาน

- ระดับของสายการบังคับบัญชาของพนักงานว่ามีให้เพียงพอต่อการปฏิบัติงานให้สำเร็จตามกำหนด

- ค่าใช้จ่ายในการปฏิบัติงานประจำวันด้าน IT แผนฉุกเฉินด้าน IT และแผนการกู้/ฟื้นฟูการดำเนินงานของสายงานธุรกิจ

5. ทบทวนแผนกลยุทธ์ด้าน IT เพื่อตรวจสอบว่าเป้าหมายและวัตถุประสงค์หลักของกิจกรรมด้าน IT สอดคล้องกันกับกลยุทธ์ด้านธุรกิจโดยรวมของสถาบันการเงิน พร้อมทั้งบันทึกเป็นลายลักษณ์อักษรสำหรับการเปลี่ยนแปลงที่สำคัญ ๆที่เกิดขึ้นหลังการตรวจสอบครั้งก่อนหรือการเปลี่ยนแปลงที่จะเกิดขึ้นในอนาคตซึ่งมีผลกระทบกับโครงสร้างขององค์กร การกำหนดค่าตัวแปรต่าง ๆ ของเครื่องคอมพิวเตอร์และโปรแกรมระบบงาน และเป้าหมายต่างๆ ในการประมวลผลข้อมูล โดยตรวจสอบตามประเด็นต่าง ๆ เหล่านี้ คือ

- ความจำเป็นหรือความต้องการทางธุรกิจมีความเป็นไปได้ในทางปฏิบัติหรือไม่

- ระบบงานด้าน IT มีความสามารถที่จะตอบสนองความต้องการของสายงาน

ธุรกิจหรือไม่

- แผนกลยุทธ์ได้ให้ข้อมูลเกี่ยวกับสภาพแวดล้อมด้าน IT ไว้หรือไม่
- แผนกลยุทธ์ได้กล่าวถึงรายชื่อของการริเริ่มโครงการต่างๆ เชิงกลยุทธ์หรือไม่
- แผนกลยุทธ์ได้กล่าวถึงแนวโน้มต่างๆ และประเด็นที่จะเกิดผลกระทบหรือไม่
- แผนกลยุทธ์ได้กำหนดเป้าหมายที่ชัดเจนและมีการแสดงข้อมูลเชิงเปรียบเทียบทางเมตริกหรือไม่

6. ทบทวนอัตราการหมุนเวียนของพนักงานสายงานด้าน IT และปรึกษาหารือกับผู้บริหารสายงานด้าน IT เกี่ยวกับการจัดหาและการรักษาพนักงาน เพื่อชี้ให้เห็นถึงรากเหง้าของการขาดแคลนพนักงานและผู้เชี่ยวชาญจากปัญหาการจ่ายเงินทดแทนหรือแนวทางการเก็บรักษาพนักงาน

7. ถ้าพนักงานสายงานด้าน IT มีหน้าที่ปฏิบัติงานในฝ่ายงานอื่นๆ ให้พิจารณาเพิ่มเติมว่า

- ฝ่ายจัดการได้ตระหนักถึงโอกาสที่จะเกิดความขัดแย้งอันเนื่องมาจากการที่พนักงานทำหน้าที่ในฝ่ายงานอื่น
- ภาระในการปฏิบัติงานที่ขัดแย้งกันอยู่นั้นได้อยู่ภายใต้การกำกับดูแลและการควบคุมผลตอบแทนที่เหมาะสม

8. สอบทานความเหมาะสมของการคุ้มครองตามกรมธรรม์ประกันภัยสำหรับกรณีต่อไปนี้ (หากมีเงื่อนไขให้กรมธรรม์ให้ความคุ้มครอง)

- ความซื่อสัตย์สุจริตของพนักงาน
- เครื่องมือและอุปกรณ์คอมพิวเตอร์ พร้อมทั้งเครื่องอำนวยความสะดวกด้าน IT
- การสร้างและจัดหาสื่อ/ตัวกลางเก็บข้อมูลแทนชุดที่สูญหายหรือถูกทำลาย
- บริการธนาคารอิเล็กทรอนิกส์
- บริการการโอนเงินทางอิเล็กทรอนิกส์ (EFT)
- ผลเสียหายอันเนื่องมาจากการหยุดชะงักของธุรกิจ
- ข้อผิดพลาด และการละเลย/ละเว้นไม่ปฏิบัติหน้าที่
- ค่าใช้จ่ายส่วนเพิ่มรวมถึงค่าใช้จ่ายสำหรับศูนย์ประมวลผลสำรอง
- วัสดุอุปกรณ์ที่อยู่ระหว่างการขนส่ง

- ความเสี่ยงอื่น ๆ (ความเสี่ยงเฉพาะพิเศษสำหรับองค์กรโดยเฉพาะ)

<u>วัตถุประสงค์ที่ 4</u>: ประเมินกระบวนการกำกับดูแลและควบคุมความเสี่ยงด้าน IT ของฝ่ายจัดการซึ่งครอบคลุมไปถึงเรื่องการวางแผนดำเนินธุรกิจอย่างต่อเนื่อง การรักษาความปลอดภัยของข้อมูล การใช้บริการจากภายนอก การพัฒนาและจัดหาโปรแกรมระบบงาน และการปฏิบัติงานประจำวัน

1. สอบทานแผนการกำกับดูแลด้าน IT ของคณะกรรมการบริหารและฝ่ายจัดการ โดยพิจารณาว่าคณะกรรมการสถาบันการเงินได้ดำเนินการดังต่อไปนี้

- เข้าไปมีส่วนเกี่ยวข้องโดยตรงในการกำหนดแนวทางหรือเข้าไปบริหารการกำกับดูแลด้าน IT
- มีการแต่งตั้งคณะกรรมการด้าน IT (IT steering committee)
- จัดให้มีกระบวนการและขั้นตอนการดำเนินงานซึ่งสนับสนุนแผนงานและเป้าหมายในการกำกับดูแลงานด้าน IT
- ให้ความเห็นชอบนโยบายการกำกับดูแลด้านการรักษาความปลอดภัยของข้อมูลสารสนเทศที่ได้จัดทำขึ้นอย่างเหมาะสม
- จัดให้มีแนวนโยบาย กระบวนการ และขั้นตอนการปฏิบัติงานที่สนับสนุนแนวทางในการกำกับดูแลตามข้อกำหนดของกฎหมายของทางการ
- จัดให้มีกำหนด/ระบุความเสี่ยงในขั้นตอนของการพัฒนาและจัดหาระบบงาน
- จัดให้มีการกำหนด/ระบุความเสี่ยงในขั้นตอนของการพัฒนาแผนการดำเนินธุรกิจอย่างต่อเนื่อง

2. สอบทานแนวทางปฏิบัติเกี่ยวกับธรรมาภิบาลด้าน IT ที่ดำเนินการโดยฝ่ายจัดการ

3. สอบทานการจัดหาเครื่องคอมพิวเตอร์และโปรแกรมระบบงานสำคัญๆ ว่าอยู่ในขอบเขตของการอนุมัติของคณะกรรมการสถาบันการเงิน

4. สอบทานโครงสร้างของการบริหารองค์กรด้าน IT เพื่อพิจารณาว่าคณะกรรมการสถาบันการเงินได้ดำเนินการดังต่อไปนี้

- การกำหนดบทบาทหน้าที่ที่ชัดเจนของผู้บริหารระดับสูงด้านสารสนเทศ (CIO) และผู้บริหารระดับสูงด้านเทคโนโลยี (CTO)
- การเข้ามามีส่วนร่วมของผู้บริหารสายงานธุรกิจในกระบวนการบริหารงาน

ด้าน IT

- การเข้ามามีส่วนร่วมของผู้บริหารชั้นต้นในสายงานธุรกิจในกระบวนการบริหารงานด้าน IT

วัตถุประสงค์ที่ 5: พิจารณาว่าคณะกรรมการสถาบันการเงินและฝ่ายจัดการได้ดำเนินการ ให้มีระบบการรายงานและการเฝ้าติดตามดูแลความเสี่ยงที่เกี่ยวข้องกับด้าน IT

1. ตรวจสอบว่าฝ่ายจัดการและคณะกรรมการสถาบันการเงินได้ปฏิบัติดังต่อไปนี้

- ทบทวนและให้ความเห็นชอบแผนงานการรักษาความปลอดภัยของข้อมูลสารสนเทศที่มีรูปแบบเป็นทางการและเป็นลายลักษณ์อักษร โดยกระทำปีละครั้ง
- ให้ความเห็นชอบและเฝ้าติดตามดูแลกระบวนการประเมินความเสี่ยง
- ให้ความเห็นชอบและเฝ้าติดตามดูแลโครงการด้าน IT ที่สำคัญๆ
- ให้ความเห็นชอบมาตรฐานการปฏิบัติงานและขั้นตอนการดำเนินงาน
- ติดตามผลการปฏิบัติงานโดยรวมด้าน IT
- รักษาความสัมพันธ์อย่างต่อเนื่องระหว่างสายงานด้าน IT และสายงานธุรกิจ
- ทบทวนและให้ความเห็นชอบโครงสร้างพื้นฐาน ผู้จำหน่าย หรือค่าใช้จ่ายลงทุนด้าน IT ที่สำคัญๆ ที่อยู่ในอำนาจอนุมัติของคณะกรรมการสถาบันการเงิน
- ทบทวนและเฝ้าติดตามดูแลสถานะของแผนงานและงบประมาณด้าน IT ประจำปี
- ทบทวนรายงานของฝ่ายจัดการ และเปรียบเทียบผลการปฏิบัติงานของโครงการสำคัญๆ กับแผนงานที่กำหนดไว้เดิม (และพิจารณาหาเหตุผลที่เกิดข้อบกพร่อง – ถ้ามี)
- ทบทวนความเพียงพอและการจัดสรรทรัพยากรด้าน IT (รวมถึงพนักงานและเทคโนโลยีสารสนเทศ)

2. ทบทวนกระบวนการประเมินความเสี่ยงเพื่อพิจารณาว่าสถาบันการเงินได้วางรูปแบบของระบบอย่างเหมาะสมและประเมินความเสี่ยงที่มีต่อสินทรัพย์ที่เป็นข้อมูลสารสนเทศ โดยพิจารณาว่าองค์กรได้ปฏิบัติดังต่อไปนี้หรือไม่

- ระบุและจัดอันดับความสำคัญของสินทรัพย์ข้อมูลสารสนเทศให้เป็นไปตามวิธีการที่เหมาะสม โดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นกับลูกค้า ข้อมูลสารสนเทศที่ไม่พึงเปิดเผยและองค์กร ระบุประเภทของภัยคุกคามที่มีความสมเหตุสมผลที่จะเกิดขึ้นกับสถาบันการเงิน
- วิเคราะห์จุดอ่อนทางเทคนิคและโครงสร้างขององค์กร

3. สอบทานว่าสถาบันการเงินได้ปรับปรุงกระบวนการประเมินความเสี่ยงให้เป็นปัจจุบันและมีประสิทธิภาพก่อนที่จะดำเนินการ ปรับปรุงหรือเปลี่ยนแปลงแก้ไขระบบงาน นำผลิตภัณฑ์หรือบริการใหม่มาใช้งานจริง และสอดคล้องกับสถานการณ์ใหม่ ๆ จากภายนอกองค์กร

4. พิจารณาประสิทธิภาพของรายงานสำหรับผู้บริหารระดับสูงหรือคณะกรรมการที่เกี่ยวข้องเพื่อใช้ในการกำกับดูแลและเฝ้าติดตามดูแลกิจกรรมด้าน IT ได้แก่

- รายงานของฝ่ายจัดการที่ให้ข้อมูลเกี่ยวกับสถานะในการพัฒนาและบำรุงรักษาโปรแกรมระบบงาน
- รายงานผลการปฏิบัติงานและปัญหาที่เกิดขึ้นโดยกลุ่มผู้ใช้งานภายในองค์กร
- รายงานแสดงการเปรียบเทียบระหว่างการใช้งานจากระบบงานจริงกับข้อมูลตามแผนงานที่จัดทำโดยผู้บริหารงานปฏิบัติงานประจำวัน
- รายงานผลการตรวจสอบด้าน IT ของผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก

<u>วัตถุประสงค์ที่ 6</u>: พิจารณาความเหมาะสมของแนวนโยบาย ขั้นตอนการปฏิบัติงานและระบบการควบคุมด้าน IT โดยคำนึงถึงลักษณะทางธรรมชาติและความสลับซับซ้อนของการปฏิบัติงานประจำวัน

1. สอบทานว่าผู้บริหารสายงานด้าน IT ได้จัดให้มีมาตรฐานการปฏิบัติงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมไปถึงกระบวนงานที่เหมาะสม โดยใช้การตรวจสอบหรือการสนทนาในประเด็นต่าง ๆ กับผู้ตรวจสอบ ตามประเด็นดังต่อไปนี้

- การประเมินความเสี่ยง
- การบริหารงานบุคคล
- การพัฒนาและการจัดซื้อ/จัดหาโปรแกรมระบบงาน
- การปฏิบัติงานประจำวันด้าน IT
- การบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก
- การรักษาความปลอดภัยของคอมพิวเตอร์และข้อมูลสารสนเทศ
- แผนการดำเนินธุรกิจอย่างต่อเนื่อง
- การตรวจสอบ

วัตถุประสงค์ที่ 7 : พิจารณาคุณภาพของการให้บริการและสนับสนุนลูกค้าในกรณีที่สถาบันการเงินให้บริการด้าน IT แก่สถาบันการเงินอื่น

1.วิเคราะห์สถานะทางการเงินของผู้ให้บริการด้าน IT (TSP) และให้บันทึกข้อมูลเกี่ยวกับจุดแข็งและจุดอ่อน (ในกรณีที่ TSP ไม่ใช่สถาบันการเงิน)

2. ตรวจสอบว่าผู้ให้บริการฯได้กำหนดวิธีการให้ลูกค้าจะเข้าถึงข้อมูลทางการเงินอย่างเหมาะสม โดยพิจารณาจากปัจจัยต่อไปนี้

- วิธีการสื่อสารกับสถาบันการเงินที่เป็นลูกค้า
- กำหนดเวลาที่ชัดเจนในการรายงานผล
- คุณภาพของข้อมูลทางการเงินตามความคิดเห็นของผู้ตรวจสอบภายในหรือผู้ตรวจสอบจากภายนอก

3. พิจารณาความเหมาะสมของรายงานผลการตรวจสอบผู้ให้บริการในเรื่องของขอบเขตของการตรวจสอบ ความเป็นอิสระ ความชำนาญ และมาตรการปรับปรุงแก้ไขตามข้อสังเกตที่อยู่ในรายงาน

4. พิจารณาคุณภาพของการให้บริการแก่ลูกค้าสถาบันผู้ใช้บริการ ดังต่อไปนี้

- สอบทานรายงานของฝ่ายจัดการที่ใช้ในการเฝ้าติดตามดูแลการให้บริการลูกค้าและปัญหาที่เกิดขึ้น
- สอบทานแฟ้มคำร้องเรียน และวิธีจัดการกับคำร้องเรียนเหล่านั้น
- ประเมินขอบเขตของกิจกรรมของกลุ่มผู้ใช้งาน และรายงานการประชุม
- สัมภาษณ์ตัวอย่างของลูกค้าประเมินความพึงพอใจของลูกค้า

5. พิจารณาสมรรถภาพของฝ่ายจัดการในการติดตามและแก้ไขตามข้อสังเกตของลูกค้าและปัญหาอื่น ๆ โดยการวิเคราะห์ข้อมูลข้างต้น

วัตถุประสงค์ที่ 8: ถ้าหากขอบเขตของการตรวจสอบครอบคลุมไปถึงระบบสารสนเทศเพื่อการจัดการ ให้ดำเนินการตามขั้นตอนในการดำเนินการดังต่อไปนี้

1. สอบทานประเด็นเกี่ยวกับระบบสารสนเทศเพื่อการจัดการที่พบในการตรวจสอบครั้งก่อน ว่าฝ่ายจัดการได้ดำเนินการอย่างไรกับประเด็นดังกล่าวนั้น

- ปรึกษาหารือกับผู้ตรวจสอบถึงเรื่องประโยชน์ใช้สอยและการใช้งานของระบบสารสนเทศเพื่อการบริหาร
- ขอสำเนารายงานใดๆที่กล่าวถึงจุดเด่นหรือปัญหาของระบบสารสนเทศเพื่อ

การบริหาร

- ตรวจสอบความมีนัยสำคัญของจุดอ่อนต่างๆเพื่อนำผลลัพธ์ดังกล่าวมาจัดลำดับในการติดตามผลตรวจสอบ

- ขอตัวอย่างรายงานและทบทวนรายงานการตรวจสอบชุดปัจจุบันของผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกที่เกี่ยวข้องกับระบบข้อมูลสารสนเทศเพื่อการบริหารและพิจารณาว่า มีการเปิดเผยปัญหาสำคัญของระบบสารสนเทศเพื่อการบริหาร มีการให้คำแนะนำเพื่อแก้ไขปรับปรุงปัญหา ฝ่ายจัดการได้เริ่มดำเนินการแก้ไขหรือแก้ไขเสร็จเรียบร้อยแล้ว ฝ่ายตรวจสอบได้ทำการตรวจสอบติดตามผลการแก้ไขตามข้อสังเกต

2. สอบทานรายงานการตรวจสอบระบบสารสนเทศเพื่อการบริหาร (สายงานธุรกิจเป็นผู้ดำเนินการ) และพิจารณาว่า มีการเปลี่ยนแปลงใดที่สำคัญ ซึ่งเกี่ยวข้องกับประโยชน์ในการใช้ข้อมูลจากระบบ MIS ในประเด็นต่างๆดังต่อไปนี้

- ข้อมูลที่ได้รับตรงเวลาและทันกาล
- มีความถูกต้องแม่นยำ
- ข้อมูลที่ได้รับมีความต่อเนื่อง ไม่ขาดตอนหรือหยุดชะงัก
- ข้อมูลที่ได้รับมีความสมบูรณ์ครบถ้วน
- ข้อมูลที่ได้รับมีความสัมพันธ์เกี่ยวข้องกัน

<u>วัตถุประสงค์ที่ 9</u>: ปรึกษาหารือเกี่ยวกับมาตรการแก้ไขและสื่อสารให้ทราบถึงสิ่งที่พบ

1. สอบทานข้อสรุปเบื้องต้นกับหัวหน้าทีมผู้ตรวจสอบ (EIC) ในประเด็น ต่อไปนี้

- การปฏิบัติผิดกฎหมาย กฎเกณฑ์ และระเบียบข้อบังคับของทางการ
- ประเด็นสำคัญที่ยกขึ้นสรุปผล เช่น ประเด็นที่ผู้บริหารสถาบันการเงินควรเอาใจใส่หรือเขียนเป็นข้อสังเกตใด ๆ ในรายงานการตรวจสอบ
- ผลการจัดอันดับภาพรวมของการดำเนินงานด้าน IT ตามแนวทางการจัดอันดับผลการดำเนินงานด้าน IT (URSIT = Uniform Rating System for Information Technology) ซึ่งปรากฏอยู่ในคู่มือ IT-RBS และผลกระทบจากข้อสรุปในการตรวจสอบองค์ประกอบย่อยแต่ละหัวข้อด้าน IT
- ผลกระทบจากการสรุปผลการตรวจสอบที่คาดว่าจะมีผลกระทบต่อวิธีการประเมินความเสี่ยงขององค์กร

2. ปรึกษาหารือกับฝ่ายจัดการและขอรับทราบแนวทางในการปรับปรุงแก้ไข

ข้อบกพร่องที่สำคัญ ๆ

3. จัดทำข้อสรุปเป็นบันทึกนำเสนอให้หัวหน้าทีมผู้ตรวจสอบ เพื่อจัดทำรายงานผลการตรวจสอบในหัวข้อที่เกี่ยวข้องและเป็นแนวทางในการตรวจสอบของผู้ตรวจสอบชุดใหม่ในอนาคตต่อไป

4. จัดทำกระดาษทำการให้สามารถสนับสนุนผลการตรวจสอบได้อย่างชัดเจนตามวัตถุประสงค์ในการตรวจสอบ