คู่มือตรวจสอบ

การตรวจสอบ

ภายในและภายนอก

(Audit)

คำนำ

คู่มือตรวจสอบการตรวจสอบภายในและภายนอก เป็นส่วนหนึ่งของการปรับปรุงคู่มือการตรวจสอบระบบเทคโนโลยีสารสนเทศ ฉบับเดือนพฤศจิกายน 2543 ของส่วนตรวจสอบเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ ซึ่งเป็นการยกเลิกบทที่ 6 การตรวจสอบภายในและภายนอก และใช้คู่มือฉบับนี้แทน โดยปรับปรุงตามแนวทางของ Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) ประเทศสหรัฐอเมริกา และคู่มือนี้เป็นแนวทางสำหรับการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT) ที่ผู้ตรวจสอบสามารถนำไปใช้ในงานตรวจสอบ โดยกล่าวถึงบทบาทหน้าที่และความผิดชอบของคณะกรรมการสถาบันการเงิน ผู้บริหารระดับสูง ผู้บริหารสายงานตรวจสอบภายใน ผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก ซึ่งให้แนวทางปฏิบัติสำหรับจัดทำโปรแกรมการตรวจสอบ IT มีรายละเอียดของวัตถุประสงค์และกระบวนการตรวจสอบ โปรแกรมการตรวจสอบสถาบันการเงินและผู้ให้บริการด้าน IT จากภายนอก ซึ่งมุ่งเน้นไปที่การตรวจสอบด้าน IT

การวางแผนอย่างดีมีความจำเป็นอย่างมากในขั้นตอนของการออกแบบโครงสร้างโปรแกรมการตรวจสอบที่เหมาะสมเพื่อใช้ประเมินกระบวนการบริหารความเสี่ยง การออกแบบระบบการควบคุมภายในที่ดี และการปฏิบัติงานให้สอดคล้องกับนโยบายการบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศสำหรับองค์กรทุก ๆ ขนาดและทุก ๆ ระดับความซับซ้อนขององค์กร อนึ่ง โปรแกรมการตรวจสอบที่มีประสิทธิภาพจะต้องมีคุณสมบัติดังต่อไปนี้ คือ มีการจัดทำแผนการตรวจสอบที่เน้นไปที่ความเสี่ยงหลักๆ ก่อน มีการสนับสนุนให้เกิดระบบการควบคุมภายในด้าน IT ที่ดี มีการปรับปรุงข้อบกพร่องที่ตรวจสอบพบในเวลาที่เหมาะสม และมีการนำเสนอให้คณะกรรมการสถาบันการเงินรับทราบถึงประสิทธิภาพของระบบการบริหารและการจัดการกับความเสี่ยงด้าน IT นอกจากนี้ กระบวนการตรวจสอบด้านIT ที่มีประสิทธิภาพก็เป็นปัจจัยสำคัญที่จะช่วยลดระยะเวลาในการตรวจสอบลงไปได้ ในขณะเดียวกันก็ควรจัดให้มีการตรวจสอบแบบเต็มเวลาและต่อเนื่องระหว่างการตรวจสอบภายในกับการตรวจสอบภายนอกที่ได้จัดทำแผนการตรวจสอบมาอย่างดีและสอดคล้องกันกับโปรแกรมการตรวจสอบจากภายใน

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ หวังว่าแนวทางการตรวจสอบในคู่มือฉบับนี้จะเป็นประโยชน์และช่วยพัฒนาการตรวจสอบให้มีประสิทธิภาพต่อไปในอนาคต

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ

ธันวาคม 2551

สารบัญ

หน้าที่

ส่วนที่ 1 บทนำ 1

ส่วนที่ 2 แนวทางที่พึงปฏิบัติ 3

2.1 บทบาทและความรับผิดชอบของการตรวจสอบด้านเทคโนโลยีสารสนเทศ 3

2.1.1 คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง 3

2.1.2 การบริหารงานตรวจสอบ 5

2.1.3 สายงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ 6

2.1.4 การบริหารงานด้านปฏิบัติการ 7

2.1.5 ผู้ตรวจสอบภายนอก 7

2.2 ความเป็นอิสระและสายงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ 8

2.2.1 ความเป็นอิสระ 8

2.2.2 การจัดการด้านบุคลากร 10

2.3 โปรแกรมการตรวจสอบภายใน 11

2.4 การประเมินความเสี่ยงและการตรวจสอบตามแนวความเสี่ยง 15

2.4.1 รายละเอียดของโปรแกรมการตรวจสอบ 15

2.4.2 ระบบการจัดลำดับความเสี่ยง 16

2.5 การมีส่วนร่วมของผู้ตรวจสอบภายในสำหรับ การพัฒนาระบบงาน การจัดหาระบบงาน การโอนย้ายระบบงาน และการทดสอบ 19

2.6 การใช้บริการตรวจสอบภายในจากหน่วยงานภายนอก 21

2.6.1 ความเป็นอิสระของผู้ตรวจสอบภายนอกที่ให้บริการด้านตรวจสอบภายใน 22

2.6.2 รูปแบบการใช้บริการงานตรวจสอบภายในจากหน่วยงานภายนอก 22

2.6.3 การใช้ผลการตรวจสอบภายในจากหน่วยงานภายนอกทดแทนการเข้าไปตรวจสอบการดำเนินงานของผู้ให้บริการภายนอก 26

ส่วนที่ 3 แนวทางการตรวจสอบ 28

3.1 วัตถุประสงค์ของการตรวจสอบ 28

3.2 วัตถุประสงค์และกระบวนการตรวจสอบทั่วไป (Tier 1) 28

3.3 วัตถุประสงค์และกระบวนการตรวจสอบเชิงลึก (Tier 2) 39

<u>ส่วนที่ 1</u> บทนำ

สถาบันการเงินต้องวางแผนงาน บริหารจัดการ และติดตามดูแลการเปลี่ยนแปลงทางด้านเทคโนโลยี เพื่อให้สามารถนำเสนอและสนับสนุนผลิตภัณฑ์ใหม่ๆ บริการชนิดใหม่ และช่องทางการให้บริการชนิดใหม่ เพราะว่าอัตราเร่งในการเปลี่ยนแปลงและความจำเป็นที่จะต้องพึ่งพาระบบเทคโนโลยีจึงทำให้การตรวจสอบที่ครอบคลุมด้าน IT มีความสำคัญอย่างยิ่งต่อการจัดทำโปรแกรมการตรวจสอบที่มีประสิทธิภาพโดยรวม ทั้งนี้โปรแกรมการตรวจสอบควรที่จะกล่าวถึงความเสี่ยงด้าน IT ขององค์กรโดยรวม รวมถึงเรื่องการบริหารงานและแผนกลยุทธ์ด้าน IT การปฏิบัติงานในศูนย์คอมพิวเตอร์ โครงสร้างพื้นฐานของระบบคอมพิวเตอร์แบบ Client -Server ระบบเครือข่ายแบบ Local and Wide-Area Networks ระบบการสื่อสารระยะไกล การรักษาความปลอดภัยทางด้านกายภาพและความปลอดภัยของข้อมูล ระบบ Electronic Banking การพัฒนาระบบงาน และแผนการดำเนินธุรกิจอย่างต่อเนื่อง อนึ่ง การตรวจสอบทางด้าน IT จะต้องมุ่งเน้นไปที่ฝ่ายจัดการว่าได้พิจารณาและตัดสินใจอย่างไรเกี่ยวกับความเสี่ยงด้าน IT รวมถึงกระบวนการควบคุมต่างๆ และการลดความเสี่ยงเหล่านั้นเป็นหลัก

ในการประเมินความเสี่ยงที่มีอยู่ขององค์กร ฝ่ายบริหารควรจัดให้มีการประเมินความเสี่ยงขององค์กรไปพร้อมๆกับ การประเมินคุณภาพของระบบควบคุมภายในในส่วนที่เกี่ยวข้องกับขั้นตอนในการพัฒนาระบบงาน การจัดซื้อจัดหา การติดตั้งระบบงาน และการใช้งานเทคโนโลยีด้านข้อมูลข่าวสารอย่างเป็นอิสระ ทั้งนี้ การประเมินความเสี่ยง สามารถดำเนินการได้โดยผู้ตรวจสอบภายในด้านIT ผู้ตรวจสอบภายนอกหรือผู้ประเมินอิสระภายนอก ขึ้นอยู่กับสภาพแวดล้อมและความซับซ้อนขององค์กรหรือความเชี่ยวชาญของผู้ตรวจสอบภายใน การตรวจสอบภายในที่เข้มแข็ง และการตรวจสอบภายนอกที่ผ่านการวางแผนมาเป็นอย่างดีแล้วนั้น จะช่วยเพิ่มความเป็นไปได้อย่างมีนัยสำคัญที่จะทำให้องค์กรสามารถตรวจพบปัญหาหรือความเสี่ยงด้านเทคโนโลยีต่าง ๆ ที่สำคัญๆได้ และโปรแกรมการตรวจสอบที่ดีควรมีลักษณะ ดังนี้

- ระบุขอบเขตที่มีความเสี่ยงด้าน IT มากที่สุดภายในองค์กรเพื่อใช้ในการกำหนดแนวทางการใช้ทรัพยากรสำหรับการตรวจสอบ
- ช่วยสนับสนุนให้ระบบงาน IT สามารถรักษาความลับของข้อมูล มีความถูกต้องน่าเชื่อถือได้ และมีความพร้อมใช้งานของระบบและข้อมูล
- ช่วยให้ทราบถึงประสิทธิภาพของฝ่ายจัดการในการวางแผน และการควบคุมดูแลกิจกรรมด้าน IT

- ช่วยประเมินถึงความเพียงพอของขั้นตอนการปฏิบัติงานและระบบการควบคุมภายใน

- ช่วยพิจารณาความเพียงพอของความพยายามของทุกหน่วยงานภายในองค์กรในการปฏิบัติงานให้สอดคล้องกับนโยบายด้าน IT และขั้นตอนของระบบการควบคุมภายใน

- ต้องมีมาตรการในการแก้ไขปัญหาอย่างเหมาะสม เพื่อชี้ให้เห็นถึงจุดอ่อนและข้อบกพร่องของการควบคุมภายใน พร้อมทั้งมีกระบวนการติดตาม เพื่อให้มั่นใจว่าฝ่ายบริหารได้มีการดำเนินการอย่างรวดเร็วและมีประสิทธิภาพเพื่อแก้ไขจุดอ่อนและข้อบกพร่องที่พบ

ผู้ตรวจสอบมีความรับผิดชอบในการประเมินประสิทธิภาพของการตรวจสอบด้าน IT ว่าสามารถดำเนินงานได้บรรลุตามวัตถุประสงค์ที่ตั้งไว้หรือไม่ และควรพิจารณาถึงความสามารถขององค์กรในการตรวจสอบและรายงานผลการตรวจสอบเมื่อตรวจพบความเสี่ยงที่สำคัญต่อคณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง อนึ่ง ในขั้นตอนของการประเมิน ผู้ตรวจสอบควรพิจารณาให้ครอบคลุมในเรื่องขนาด ความซับซ้อนขององค์กร และภาพรวมของความเสี่ยงทั้งหมดขององค์กรและความสามารถในการรองรับความเสี่ยงแต่ละประเภท นอกจากนี้ผู้ตรวจสอบควรที่จะพิจารณาถึงขอบเขตของงานตรวจสอบด้าน IT ในส่วนที่เกี่ยวข้องกับประเด็นต่าง ๆ ดังต่อไปนี้

- ความเป็นอิสระของการตรวจสอบและความสัมพันธ์ของระบบการรายงานผลการตรวจสอบต่อคณะกรรมการสถาบันการเงิน และคณะกรรมการตรวจสอบ

- ความเชี่ยวชาญและจำนวนของผู้ตรวจสอบที่มีความสัมพันธ์กับสภาพแวดล้อมด้าน IT

- การรวบรวมรายละเอียดของความเสี่ยงด้าน IT ทั้งหมดที่จะต้องตรวจสอบการประเมินความเสี่ยง ขอบเขต และความถี่ของการตรวจสอบด้าน IT ทั้งหมด

- กระบวนการติดตามและปรับปรุงแก้ไขจุดอ่อนตามรายงานการตรวจสอบอยู่ภายในระยะเวลาที่เหมาะสม

- กระบวนการจัดเก็บเอกสารประกอบการตรวจสอบด้าน IT เช่น กระดาษทำการรายงานผลตรวจสอบและรายงานการติดตามผล เป็นต้น

<u>ส่วนที่ 2</u> แนวทางที่พึงปฏิบัติ

2.1 บทบาทและความรับผิดชอบของการตรวจสอบด้านเทคโนโลยีสารสนเทศ

<u>สรุปแนวทางการปฏิบัติ</u>

คณะกรรมการสถาบันการเงิน คณะผู้บริหารระดับสูง ผู้บริหารงานตรวจสอบ ทีมงานตรวจสอบ และผู้บริหารงานปฏิบัติการ มีบทบาทหน้าที่และความรับผิดชอบที่สัมพันธ์กับการตรวจสอบด้าน IT

- **คณะกรรมการสถาบันการเงิน มีความรับผิดชอบในการจัดให้มีขอบเขตของการตรวจสอบด้าน IT ที่มีประสิทธิภาพ**
- คณะกรรมการสถาบันการเงิน ผู้บริหารระดับสูง มีความรับผิดชอบในการจัดให้มีการตรวจสอบด้าน IT โดยใช้ทรัพยากรอย่างเหมาะสม **เพื่อให้มั่นใจว่าการตรวจสอบงานด้าน IT ครอบคลุมทั้งองค์กรและมีความเป็นอิสระ**
- ผู้บริหารระดับสูง มีความรับผิดชอบและสนับสนุนการตรวจสอบด้าน IT โดยการระบุและกำหนดแผนการตรวจสอบที่สอดคล้องกับกระบวนการวางแผนงานด้าน IT นโยบายในการปฏิบัติงาน และระบบการควบคุมภายใน
- ผู้บริหารสายงานตรวจสอบภายใน มีความรับผิดชอบในการนำแนวทางการตรวจสอบที่คณะกรรมการสถาบันการเงินพิจารณาอนุมัติ มาดำเนินการเพื่อให้เกิดผลในทางปฏิบัติ
- ทีมงานตรวจสอบภายในด้าน IT รับผิดชอบในการประเมินการดำเนินงานด้าน IT ให้เป็นไปตามวัตถุประสงค์ที่กำหนด ด้วยความเป็นอิสระ เพื่อปรับปรุงประสิทธิภาพและประสิทธิผลของการบริหารจัดการความเสี่ยง การควบคุมภายใน และการดำเนินงานตามแนวทางของหลักธรรมาภิบาล (corporate governance)
- ผู้บริหารสายงานปฏิบัติการมีหน้าที่รับผิดชอบในการดำเนินการตามข้อแนะนำของการตรวจสอบด้าน IT อย่างรวดเร็วและมีประสิทธิผล

2.1.1 คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง

คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูงมีความรับผิดชอบดำเนินการให้สถาบันการเงินมีระบบการควบคุมภายในที่มีประสิทธิภาพ และครอบคลุมไปถึงการตรวจสอบด้าน IT

ทั้งนี้ การตรวจสอบจะต้องมีความเป็นอิสระและมีการใช้ทรัพยากรอย่างเหมาะสม ซึ่งคณะกรรมการสถาบันการเงินและคณะกรรมการตรวจสอบ ควรดำเนินการ ดังต่อไปนี้ คือ

- จัดให้มีการตรวจสอบภายในที่สามารถประเมินการควบคุมทางด้าน IT
- จัดให้มีที่ปรึกษา ผู้เชี่ยวชาญ หรือผู้ตรวจสอบจากภายนอกมาทำหน้าที่งานด้านการตรวจสอบภายใน หรือ
- ดำเนินการทั้งสองวิธีข้างต้น เพื่อให้มั่นใจว่าองค์กรจะได้รับการตรวจสอบที่ครอบคลุมการดำเนินงานด้าน IT อย่างเพียงพอ

คณะกรรมการสถาบันการเงิน อาจจะจัดตั้ง “คณะกรรมการตรวจสอบ” เพื่อกำกับดูแลภาระหน้าที่ของการตรวจสอบและรายงานผลการตรวจสอบให้คณะกรรมการสถาบันการเงินเป็นประจำเมื่อตรวจพบเรื่องที่มีนัยสำคัญเกิดขึ้น อนึ่งในคู่มือเล่มนี้ “คณะกรรมการตรวจสอบ” หมายถึงคณะกรรมการที่ทำหน้าที่ตรวจสอบสถาบันการเงินทุกประเภท และคณะกรรมการตรวจสอบจะต้องประกอบไปด้วยสมาชิกที่มีความเข้าใจอย่างชัดแจ้งเกี่ยวกับความสำคัญและความจำเป็นของภาระหน้าที่การตรวจสอบที่จะต้องมีความเป็นอิสระ ทั้งนี้ คณะกรรมการสถาบันการเงินควรจัดให้มีแนวทางในการตรวจสอบด้าน IT เป็นลายลักษณ์อักษรและต้องดูแลให้แน่ใจว่าแนวทางดังกล่าวได้ถูกนำไปใช้ในการปฏิบัติงานจริง อนึ่ง คณะกรรมการสถาบันการเงิน หรือคณะกรรมการตรวจสอบควรมอบหมายความรับผิดชอบในการทำหน้าที่ตรวจสอบให้กับพนักงานระดับบริหาร (ในที่นี้จะเรียกว่าผู้จัดการฝ่ายตรวจสอบภายใน) ซึ่งมีประสบการณ์เกี่ยวกับการตรวจสอบและมีความเป็นอิสระจากการปฏิบัติงานทางด้านธุรกิจประจำวัน และพนักงานสามารถปฏิบัติงานได้อย่างเป็นกลางไม่ถูกครอบงำโดยผู้บริหารระดับสูงหรือผู้จัดการฝ่ายงานอื่นๆที่ดูแลงานประจำวัน และฝ่ายตรวจสอบควรจะต้องมีโครงสร้างของการบังคับบัญชาที่ขึ้นตรงต่อคณะกรรมการสถาบันการเงิน และคณะกรรมการตรวจสอบโดยตรง อนึ่ง คณะกรรมการสถาบันการเงิน หรือคณะกรรมการตรวจสอบมีความรับผิดชอบในการทบทวนและอนุมัติแผนกลยุทธ์ในการตรวจสอบ (รวมไปถึงนโยบายและรายละเอียดของการตรวจสอบ) และต้องคอยติดตามความมีประสิทธิภาพของการตรวจสอบ (ผู้ตรวจสอบควรทบทวนบทบาทของกรรมการสถาบันการเงินตามแนวทางที่กำหนดในหนังสือ “คู่มือกรรมการของสถาบันการเงิน” ซึ่ง ธปท.ได้รับการสนับสนุนจากธนาคารโลก และความร่วมมือจากสมาคมธนาคารไทย สมาคมเงินทุน สมาคมธนาคารต่างชาติ และบริษัทที่ปรึกษา ไว้ท์ แอนด์ เคส (ประเทศไทย) จำกัด ในการยกร่างคู่มือฉบับดังกล่าวต่อไปด้วย)

คณะกรรมการสถาบันการเงิน ควรตระหนักและเข้าใจถึงความเสี่ยงที่สำคัญและระบบการควบคุมต่างๆ ที่เกี่ยวข้องกับการปฏิบัติงานประจำวัน รวมไปถึง ความเสี่ยงจากการออกผลิตภัณฑ์ใหม่ เทคโนโลยีชนิดใหม่ ระบบข้อมูลสารสนเทศ และระบบการให้บริการทางการเงินผ่าน

เครือข่ายอิเล็กทรอนิกส์ ทั้งนี้ มีข้อสังเกตเกี่ยวกับระบบการควบคุมต่างๆ ที่สัมพันธ์กับระบบงาน IT ดังต่อไปนี้ คือ

- การเข้าถึงระบบงานโดยผู้ไม่มีสิทธ์ในการเข้าถึงระบบงาน
- การเปิดเผยข้อมูลสำคัญโดยมิได้รับอนุญาต
- ค่าใช้จ่ายในการติดตั้งระบบงานที่สูงมากและไม่สามารถเชื่อถือได้
- การที่ระบบงาน IT ที่มีอยู่ไม่สอดคล้องและไม่สนับสนุนเป้าหมายทางธุรกิจอย่างเพียงพอ
- การจัดการฝึกอบรมการใช้โปรแกรมระบบงานสำหรับผู้ใช้งานและพนักงานที่มีหน้าที่ในการดูแลระบบงานไม่มีประสิทธิภาพ
- การประเมินความเหมาะสม (Due diligent) ของผู้ให้บริการด้าน IT ที่ไม่เพียงพอ
- การแบ่งแยกหน้าที่ความรับผิดชอบที่ไม่เหมาะสม
- การจัดเก็บร่องรอย (Audit trail) ที่ไม่เหมาะสมหรือไม่เพียงพอ
- การขาดมาตรฐานและระบบการควบคุมสำหรับผู้ใช้งานระบบงาน
- แผนงานระบบงาน และการประเมินแผนงาน BCP ที่ไม่มีประสิทธิภาพหรือไม่เพียงพอ
- ความเสียหายทางการเงินหรือชื่อเสียงอันเนื่องมาจากระบบงาน

คณะกรรมการสถาบันการเงิน หรือคณะกรรมการตรวจสอบควรเข้ารับการฝึกอบรมเพื่อเพิ่มเติมความรู้ความเข้าใจที่เกี่ยวข้องกับความเสี่ยงและระบบการควบคุมด้าน IT และควรพบกับผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกเป็นประจำเพื่อปรึกษาหารือเกี่ยวกับผลการตรวจสอบและข้อสังเกตจากการตรวจสอบในส่วนที่เกี่ยวข้องกับความเสี่ยงและระบบการควบคุมด้าน IT

2.1.2 การบริหารงานตรวจสอบ

ผู้บริหารสายงานตรวจสอบภายใน รับผิดชอบในการดำเนินการตรวจสอบให้เป็นไปตามทิศทางที่ได้รับอนุมัติจากคณะกรรมการตรวจสอบ การกำกับดูแลขอบเขตของการปฏิบัติงานและกำหนดทิศทางของการกำกับดูแลและการสื่อสารให้ครอบคลุมไปถึงเรื่อง นโยบายในการตรวจสอบ การปฏิบัติงานตรวจสอบ โปรแกรมการตรวจสอบ วิธีการในการดำเนินงาน การจัดสายการบังคับบัญชา การกำหนดบทบาทหน้าที่ความรับผิดชอบของบุคลากรและทีมงานในแต่ละระดับไว้อย่างชัดเจนเพื่อช่วยให้มีความรู้ ประสบการณ์ ทรัพยากรและเครื่องมือที่จะใช้ในการประเมินความเสี่ยงในการประเมินประสิทธิภาพของระบบความคุมภายในที่มีอยู่ในการปฏิบัติงานด้าน IT ขององค์กร ได้ตามเป้าหมาย

2.1.3 สายงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ

ผู้ตรวจสอบภายในด้าน IT ควรมีบทบาทในการประเมินอย่างเป็นอิสระ และตรงไปตรงมา เกี่ยวกับความเพียงพอ ของระบบการควบคุมต่างๆ รวมไปถึงความถูกต้องครบถ้วนของข้อมูล และความน่าเชื่อถือได้ของสภาพแวดล้อมด้าน IT ของสถาบันการเงิน ทั้งนี้ กระบวนการประเมินดังกล่าวจะช่วยเสริมสร้างหรือดำรงรักษาไว้ซึ่งความมีประสิทธิภาพและประสิทธิผลในการบริหารความเสี่ยงด้าน IT การควบคุมภายใน และการดำเนินงานตามแนวทางหลักธรรมาภิบาล (Corporate Governance) (โปรดอ่านคู่มือ กรรมการสถาบันการเงิน เพื่อให้ทราบคุณสมบัติ บทบาท และ หน้าที่ของกรรมการของสถาบันการเงิน ประกอบการพิจารณาหลักธรรมาภิบาลขององค์กรของหน่วยงานต่าง ๆ เช่น ประกาศธนาคารแห่งประเทศไทยที่ สนส. 60/2551 ลงวันที่ 3 สิงหาคม 2551 เรื่อง ธรรมาภิบาลของสถาบันการเงิน หรือประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) ในส่วนของการกำหนดคุณสมบัติของกรรมการ เป็นต้น)

บทบาทของผู้ตรวจสอบภายในด้าน IT

ผู้ตรวจสอบภายในด้าน IT ควรดำเนินงานให้ครอบคลุมไปถึงการดำเนินการในเรื่องต่างๆ ดังต่อไปนี้ คือ

- ประเมินแผนงานด้าน IT แผนกลยุทธ์ นโยบาย และขั้นตอนดำเนินงานเพื่อให้เกิดความมั่นใจว่าจะมีการกำกับดูแลอย่างเพียงพอจากฝ่ายจัดการ
- ประเมินระบบการควบคุมต่างๆในการปฏิบัติงานประจำวันด้าน IT เพื่อให้มั่นใจว่าระบบการประมวลผลและการบันทึกรายการธุรกรรมเป็นไปตามมาตรฐานและวิธีการทางบัญชี และสอดคล้องกับนโยบายและแนวทางการดำเนินงานที่คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูงอนุมัติไว้
- ปฏิบัติงานตรวจสอบให้ครอบคลุมเรื่อง การปฏิบัติงานประจำวัน และการพัฒนาระบบงาน เพื่อสร้างความมั่นใจว่าได้มีการจัดเตรียมระบบการควบคุมภายในไว้เรียบร้อยแล้ว และได้มีการกำหนดนโยบายและวิธีการปฏิบัติงานอย่างมีประสิทธิภาพ และ พนักงานได้ปฏิบัติงานตามแนวนโยบายที่ได้กำหนดไว้
- ตรวจสอบหาจุดอ่อน และทบทวนแผนงานของฝ่ายจัดการในการแก้ไข และติดตามผลการแก้ไขปัญหา/หรือจุดอ่อนเหล่านั้น และรายงานให้คณะกรรมการสถาบันการเงินรับทราบในเรื่องของปัญหา/หรือจุดอ่อนที่มีนัยสำคัญ

นอกจากนี้ ผู้ตรวจสอบควรตั้งข้อสังเกตเกี่ยวกับขั้นตอนการปฏิบัติงานที่มีผลกระทบกับระบบควบคุมด้าน IT ให้ฝ่ายจัดการได้รับทราบ และในกรณีที่มีการพัฒนาระบบงานใหม่ที่มี

ความสำคัญ คณะกรรมการสถาบันการเงินและผู้บริหารควรพัฒนาแนวทาง เงื่อนไข และ วิธีการประกอบการตัดสินใจว่าโครงการใดควรที่จะให้ฝ่ายตรวจสอบเข้ามาเกี่ยวข้องบ้าง โดยมีภาระหน้าที่ที่เกี่ยวข้องพอสังเขปของผู้ตรวจสอบ ดังต่อไปนี้ คือ การทบทวนภาพรวมของระบบการควบคุมภายในของระบบงาน ผลิตภัณฑ์และบริการ การปรับเปลี่ยนและโอนย้ายระบบข้อมูลสารสนเทศจากระบบงานเดิมไปสู่ระบบงานใหม่ รวมไปถึงงานการให้บริการตั้งแต่ขั้นตอนการพัฒนาจนถึงขั้นตอนการนำไปใช้และโดยเฉพาะหากผู้ตรวจสอบสามารถเข้าไปเกี่ยวข้องกับงานโครงการได้เร็วเท่าใดก็จะทำให้เกิดความมั่นใจได้ว่าโครงการเหล่านั้นจะมีระบบการควบคุมต่างๆ ที่เหมาะสมตั้งแต่ในช่วงแรกของการออกแบบระบบงาน แต่อย่างไรก็ดี ผู้ตรวจสอบจะต้องรักษาความเป็นอิสระในการดำเนินงานอยู่เสมอแม้ว่าตนเองจะต้องเข้าไปมีส่วนร่วมในการพัฒนาโครงการใดๆ ก็ตาม

2.1.4 การบริหารงานด้านปฏิบัติการ

ผู้บริหารสายงานด้านปฏิบัติการ ควรดำเนินการปรับปรุงแก้ไขการดำเนินงานตามข้อสังเกตของผู้ตรวจสอบด้าน IT อย่างเหมาะสมและมีประสิทธิภาพ ในขณะที่ทางสายงานตรวจสอบก็ควรมีความชัดเจนเกี่ยวกับแนวทาง หรือวิธีการที่จะดูแลติดตามจุดอ่อน ข้อบกพร่องของการควบคุมตามที่ผู้ตรวจสอบได้แจ้งเป็นข้อสังเกตไว้

อนึ่ง ผู้บริหารสายงานปฏิบัติการมีหน้าที่ความรับผิดชอบ ในการปรับปรุงแก้ไขที่ต้นเหตุของปัญหา ไม่ใช่การแก้ไขปัญหาเฉพาะหน้าเท่านั้น โดยจะต้องใช้ระยะเวลาในการปรับปรุงแก้ไขปัญหาอย่างสมเหตุสมผล และสอดคล้องกับความสลับซับซ้อนในการแก้ไขปัญหา และความเสี่ยงที่เกิดขึ้นจากการไม่แก้ไขปัญหาดังกล่าว ดังนั้น ผู้ตรวจสอบควรจะจัดเก็บเอกสาร จัดทำรายงานผลการตรวจสอบ และติดตามผลการปรับปรุงแก้ไขตามข้อสังเกต และข้อบกพร่องที่ยังไม่ได้รับการแก้ไข รวมทั้งการติดตามพิสูจน์ความมีประสิทธิภาพของฝ่ายบริหารในการปรับปรุงแก้ไขข้อสังเกตที่มีนัยสำคัญๆ

2.1.5 ผู้ตรวจสอบภายนอก

ผู้ตรวจสอบภายนอกจะทำการทบทวนกระบวนการควบคุมภายในด้าน IT และใช้เป็นส่วนหนึ่งของการประเมิน และการให้ความเห็นเกี่ยวกับความเพียงพอของระบบการควบคุมภายในในขั้นตอนของการจัดทำรายงานทางการเงินของสถาบันการเงิน และโดยปกติผู้ตรวจสอบภายนอกจะทำหน้าที่ทบทวนระบบการควบคุม 2 ด้าน คือ

- ระบบการควบคุมด้านทั่วไป (General control) ประกอบไปด้วยแผนงานขององค์การและการดำเนินงาน ขั้นตอนในการจัดทำเอกสารประกอบ กระบวนการดำเนินงาน การควบคุมการเข้าถึงอุปกรณ์และแฟ้มข้อมูล และระบบการควบคุมอื่นๆ ที่มีผลกระทบต่อการดำเนินงานของระบบการรวบรวมและจัดเก็บข้อมูลสารสนเทศ

- ระบบการควบคุมด้านระบบงาน (Application control) ประกอบไปด้วยระบบการควบคุมที่เกี่ยวข้องกับงานเฉพาะด้านต่างๆ ภายในระบบการรวบรวมและจัดเก็บข้อมูลสารสนเทศ ซึ่งจะช่วยให้การรับรองได้อย่างมีเหตุผลว่าระบบการเก็บบันทึกข้อมูล การประมวลผล และการรายงานผลของข้อมูลได้ถูกดำเนินการอย่างถูกต้องและเหมาะสม

ผู้ตรวจสอบภายนอก อาจจะสอบทานกระบวนการควบคุมภายในด้าน IT เพื่อใช้ประกอบการจัดทำแผนการตรวจสอบในกรณีที่จะต้องตรวจสอบการดำเนินงานเกี่ยวกับ IT Outsourcing ซึ่งผู้ตรวจสอบภายนอก อาจจะต้องเข้าไปทำงานในส่วนที่เป็นภาระหน้าที่ของผู้ตรวจสอบภายในทั้งหมดหรือบางส่วนก็ตาม (ผู้ตรวจสอบควรศึกษารายละเอียดดังกล่าวนี้เพิ่มเติมในคู่มือ Outsourcing Internal IT Audit) อนึ่ง ควรมีการกำหนด/ขยายขอบเขตการตรวจสอบของผู้ตรวจสอบภายนอกให้ครอบคลุมถึงการตรวจสอบระบบข้อมูลสารสนเทศ (information systems) และควรกำหนดรายละเอียดการว่าจ้างผู้ตรวจสอบภายนอกเป็นลายลักษณ์อักษรไว้อย่างชัดเจน ครอบคลุมรายละเอียดที่เกี่ยวข้องกับขอบเขตของการตรวจสอบ วัตถุประสงค์ การใช้ทรัพยากรต่าง ๆ ในงานตรวจสอบ ระยะเวลาในการตรวจสอบ และการรายงานผลการตรวจสอบ ดังนั้น ผู้ตรวจสอบสามารถที่จะทบทวนกระบวนการทำงานดังกล่าวแล้วนำมาประกอบการพิจารณาว่าจะสามารถใช้ผลการตรวจสอบของผู้ตรวจสอบภายนอกมาประกอบเพื่อช่วยลดขอบเขตของการตรวจสอบที่ตนเองจะต้องดำเนินการได้มากน้อยเพียงใดต่อไป

2.2 ความเป็นอิสระและสายงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ

สรุปแนวทางการปฏิบัติ

การที่จะดำเนินการตรวจสอบสภาพแวดล้อมทางด้าน IT ของสถาบันการเงินให้ได้อย่างมีประสิทธิภาพนั้น ผู้ตรวจสอบภายในจะต้องมีการปฏิบัติงานดังต่อไปนี้ คือ

1. ต้องมีความเป็นอิสระจากงานด้านปฏิบัติการ
2. ต้องมีระดับของความรู้และความชำนาญในระดับที่สอดคล้องกับขอบเขตของการตรวจสอบและความสลับซับซ้อนของสภาพแวดล้อมของสถาบันการเงินด้าน IT

2.2.1 ความเป็นอิสระ

ความเป็นอิสระของบุคลากรผู้ตรวจสอบภายในเป็นสิ่งสำคัญที่จะทำให้หน่วยงานตรวจสอบภายในสามารถบรรลุวัตถุประสงค์การดำเนินงานที่ตั้งไว้ โดยปกติแล้วการพิจารณาถึงความเป็นอิสระสามารถพิจารณาได้จากโครงสร้างขององค์กรและการจัดเรียงลำดับของฝ่ายตรวจสอบ

ภายใน ระดับของผู้มีอำนาจหน้าที่ในการรายงานผลการตรวจสอบ และความรับผิดชอบของผู้ตรวจสอบจะชี้ให้เห็นระดับของความเป็นอิสระได้เป็นอย่างดี ดังนั้น คณะกรรมการสถาบันการเงินจึงควรดำเนินการให้เกิดความมั่นใจให้ได้ว่าฝ่ายตรวจสอบมิได้เข้าไปร่วมในกิจกรรมใดๆ ที่จะทำให้สูญเสียความเป็นอิสระหรือทำให้มองเห็นได้ว่าจะขาดความเป็นอิสระ เช่น การจัดเตรียมรายงานหรือการบันทึกข้อมูล กระบวนการพัฒนาขั้นตอนการปฏิบัติงาน หรือการปฏิบัติงานประจำวันอื่นใดซึ่งตามปกติจะต้องถูกตรวจสอบโดยฝ่ายตรวจสอบ

นอกจากนี้ การตรวจสอบความเป็นอิสระสามารถพิจารณาได้จากการวิเคราะห์ขั้นตอนการจัดทำรายงานผลการตรวจสอบและการพิสูจน์ทราบว่าฝ่ายจัดการไม่ได้เข้ามาเกี่ยวข้องกับการรายงานหรือตั้งข้อสังเกตอย่างตรงไปตรงมาของฝ่ายตรวจสอบ นอกจากนี้คณะกรรมการสถาบันการเงินจะต้องยินยอมให้ผู้ตรวจสอบมีสิทธิเข้าถึงข้อมูลและพนักงานที่มีความสำคัญต่อกระบวนการตรวจสอบ และ กำหนดให้ฝ่ายจัดการต้องตอบสนองต่อข้อสังเกตที่มีความสำคัญของฝ่ายตรวจสอบ ทั้งนี้ ผู้ตรวจสอบภายในจะต้องประชุมหารือกับคณะกรรมการตรวจสอบหรือคณะกรรมการสถาบันการเงินเป็นครั้งคราวเพื่อทราบถึงข้อเท็จจริงที่ตรวจพบและข้อสังเกตที่เกี่ยวข้อง

ผู้บริหารงานตรวจสอบภายใน ควรรายงานโดยตรงต่อคณะกรรมการสถาบันการเงินหรือคณะกรรมการตรวจสอบทั้งประเด็นที่เกี่ยวข้องกับด้านตรวจสอบและประเด็นที่เกี่ยวข้องกับการบริหารและการจัดการ หรืออาจจะดำเนินการในแนวทางของการรายงานแบบสองทางพร้อมกัน โดยที่ผู้จัดการฝ่ายตรวจสอบจะรายงานผลเกี่ยวกับข้อสังเกตต่อคณะกรรมการสถาบันการเงินหรือคณะกรรมการตรวจสอบ ในขณะเดียวกันก็รายงานประเด็นที่เกี่ยวกับการบริหารและการจัดการให้กับผู้บริหารระดับสูง (CEO) ในลักษณะของการรายงานผลแบบคู่ขนานกันไป (dual reporting) อนึ่ง การดำเนินการแบบคู่ขนานนี้จะมีผลดีที่สุดก็ต่อเมื่อผู้จัดการฝ่ายตรวจสอบรายงานผลที่เกี่ยวข้องกับการบริหารจัดการให้กับผู้บริหารสูงสุดขององค์กร (CEO) โดยไม่ต้องแจ้งตรงไปที่ผู้บริหารทางการเงินสูงสุด (CFO) หรือผู้บริหารอื่นๆ ที่มีหน้าที่รับผิดชอบโดยตรงกับระบบงานที่ถูกตรวจสอบ และคณะกรรมการสถาบันการเงิน หรือคณะกรรมการตรวจสอบควรเป็นผู้ประเมินศักยภาพและพิจารณาผลตอบแทนให้กับผู้บริหารงานตรวจสอบภายใน

ตามปกติแล้วขอบเขตของงานด้านตรวจสอบภายใน ควรขึ้นอยู่กับขนาด ความซับซ้อน ขอบเขตการดำเนินงาน และความเสี่ยงที่มีขององค์กร และคณะกรรมการตรวจสอบและผู้บริหารงานตรวจสอบภายในมีหน้าที่และความรับผิดชอบในการพิจารณากำหนดขอบเขตของการตรวจสอบภายในที่จะสามารถติดตามดูแลระบบการควบคุมภายในอย่างมีประสิทธิภาพบนพื้นฐานของต้นทุนและประโยชน์จากการตรวจสอบภายใน ดังนั้น สถาบันการเงินที่มีขนาดใหญ่หรือมีการดำเนินงานที่ซับซ้อนจะได้รับประโยชน์จากการปฏิบัติงานที่เต็มเวลาของผู้บริหารและทีมงาน

ตรวจสอบที่มากกว่าต้นทุนค่าใช้จ่ายในด้านดังกล่าว ส่วนสถาบันการเงินขนาดเล็กที่มีพนักงานจำนวนน้อยหรือมีการปฏิบัติงานที่ไม่ซับซ้อนสถาบันการเงินอาจจะมีต้นทุนที่สูงกว่าประโยชน์ที่จะได้รับ อย่างไรก็ดี สำหรับสถาบันการเงินที่ไม่มีผู้ตรวจสอบภายใน สถาบันการเงินก็ยังสามารถที่จะดำเนินงานให้บรรลุวัตถุประสงค์ และสามารถจัดให้มีกระบวนการตรวจสอบภายในที่ตรงไปตรงมาและเป็นอิสระได้ โดยการจัดให้มีการสอบทานระบบการควบคุมภายในอย่างละเอียด โดยผู้ที่จะควบคุมและทำการสอบทานระบบการควบคุมภายในจะต้องไม่ใช้บุคคลที่ทำหน้าที่เป็นฝ่ายจัดการหรือผู้ที่ปฏิบัติงานที่เกี่ยวข้องกับระบบการควบคุมภายในเหล่านั้น

2.2.2 การจัดการด้านบุคลากร

บุคลากรที่จะทำหน้าที่เป็นผู้ตรวจสอบด้าน IT ควรมีความรู้ความสามารถเกี่ยวกับระบบ IT ที่เหมาะสมกับขอบเขตและความสลับซับซ้อนด้าน IT และควรจะต้องมีความชำนาญในเรื่องการวิเคราะห์และการจัดทำรายงานเกี่ยวกับต้นเหตุของความบกพร่องหรือไม่มีประสิทธิภาพ อนึ่ง ถ้าบุคลากรภายในองค์กรมีความชำนาญไม่เพียงพอ คณะกรรมการสถาบันการเงิน อาจพิจารณาใช้บริการจากภายนอกได้ เช่น ที่ปรึกษาด้านการบริหาร ผู้ตรวจสอบอิสระหรือผู้เชี่ยวชาญด้านอื่น ๆ เพื่อที่จะทำหน้าที่เสริมหรือทำหน้าที่ทดแทนฝ่ายตรวจสอบภายในด้าน IT ขององค์กร ซึ่งเราสามารถจัดประเภทของการตรวจสอบได้เป็น 2 ประเภท ดังต่อไปนี้ คือ

1. สถาบันการเงินบางแห่งอาจจะใช้บุคลากร หรือกลุ่มบุคลากรที่มาจากสายงานอื่นๆ นอกสายงานตรวจสอบด้าน IT ให้มาทำหน้าที่จัดการตรวจสอบในรูปแบบรวมศูนย์การตรวจสอบด้าน IT (centralize IT audit) และมอบหมายให้ผู้เชี่ยวชาญจำนวนหนึ่งคน หรือหลายๆ คน ไปทบทวนระบบควบคุมภายในสำหรับโปรแกรมระบบงานต่างๆ ในระดับที่ใช้กับผู้ใช้งาน (end-user) และการไปตรวจสอบระบบงาน IT ทางด้านเทคนิค ซึ่งช่วยให้สถาบันการเงินสามารถมั่นใจได้ว่าองค์กรจะมีจำนวนผู้เชี่ยวชาญด้าน IT อย่างเพียงพอ แต่การดำเนินการแบบนี้จะก่อให้เกิดความกดดันกับบุคลากรด้านเทคนิคมากและสถาบันการเงินก็จะต้องจัดให้มีการตรวจสอบหลายๆ แบบ(multiple audit) โดยฝ่ายงานของผู้ใช้งานนั้นๆ จึงมีความจำเป็นอย่างมากที่จะต้องใช้ผู้ตรวจสอบด้าน IT ที่มีความรู้เกี่ยวกับระบบการเงินและสายงานธุรกิจอย่างดีมาก

2. สถาบันการเงินบางแห่งอาจจะใช้วิธีการตรวจสอบแบบเดิมที่มีการทดสอบรายละเอียดประกอบการตรวจสอบ (integrated audit approach) โดยการมอบหมายให้ผู้ตรวจสอบที่มีความเชี่ยวชาญเฉพาะทางด้าน IT ตรวจสอบในส่วนของระบบ IT และสอบทานด้านเทคนิคอื่น ๆ และให้ผู้ตรวจสอบด้านทั่วไป ช่วยสอบทานการควบคุมตามระบบงานของผู้ใช้งาน ซึ่งการดำเนินการวิธีนี้สถาบันการเงินจะต้องเลือกใช้งานให้เหมาะสมกับผู้ตรวจสอบโดยการมอบหมายให้เฉพาะผู้ตรวจสอบที่มีความรู้และเชี่ยวชาญด้านเทคนิคได้ทำงานเฉพาะในส่วนที่เหมาะสมเท่านั้น และเพื่อให้

กระบวนการจ้างงานและการฝึกอบรมสามารถช่วยรับประกันว่าสถาบันการเงินมีผู้ตรวจสอบด้าน IT ที่มีคุณสมบัติเหมาะสม สถาบันการเงินจะต้องกำหนดเรื่องการศึกษาและประสบการณ์ให้สัมพันธ์กับความรับผิดชอบในการปฏิบัติหน้าที่ด้วย นอกจากนี้ ผู้จัดการฝ่ายตรวจสอบควรจะต้องจัดให้มีแผนการศึกษาและพัฒนาแบบต่อเนื่องที่มีประสิทธิภาพ เนื่องจากระบบข้อมูลสารสนเทศขององค์กรมีความซับซ้อนและมีพัฒนาการทางด้านเทคโนโลยีที่ซับซ้อน ผู้ตรวจสอบจึงจำเป็นต้องได้รับการพัฒนาอย่างสม่ำเสมอ

2.3 โปรแกรมการตรวจสอบภายใน

สรุปแนวทางการปฏิบัติ

ผู้บริหารงานตรวจสอบ ควรจัดให้มีการพัฒนาโปรแกรมการตรวจสอบภายใน (Internal audit program) ที่มีความสอดคล้องกับนโยบายและกระบวนการปฏิบัติงานตรวจสอบภายในและงานตรวจสอบ IT

โปรแกรมการตรวจสอบภายในของสถาบันการเงินประกอบไปด้วยแนวนโยบาย และขั้นตอนการปฏิบัติงานซึ่งครอบคลุมงานตรวจสอบภายใน รวมไปถึงการจัดทำโปรแกรมการตรวจสอบโดยเน้นไปที่ความเสี่ยงเป็นหลัก และการใช้บริการจากภายนอก ทั้งนี้ สำหรับสถาบันการเงินขนาดเล็กอาจจัดทำโปรแกรมการตรวจสอบในลักษณะรูปแบบไม่เป็นทางการเหมือนสถาบันการเงินขนาดใหญ่ที่มีความซับซ้อนกว่า แต่อย่างน้อยที่สุดโปรแกรมการตรวจสอบของสถาบันการเงินทุกขนาดจะต้องประกอบไปด้วยลักษณะ ดังต่อไปนี้

- ประกาศเรื่องพันธะกิจ วัตถุประสงค์ บทบาทอำนาจหน้าที่และภาระความรับผิดชอบของผู้ตรวจสอบภายใน พนักงานที่เกี่ยวข้อง ผู้บริหารงานตรวจสอบ และคณะกรรมการตรวจสอบ

- กระบวนการประเมินความเสี่ยงที่สามารถอธิบายและวิเคราะห์ลักษณะของความเสี่ยงตามธรรมชาติของความเสี่ยงในการดำเนินธุรกิจ และผู้ตรวจสอบควรทบทวนกระบวนการประเมินความเสี่ยงอย่างน้อยปีละครั้งหรือมากกว่านั้น หากจำเป็นเพื่อให้สามารถสะท้อนถึงความเสี่ยงที่เกิดจากการเปลี่ยนแปลงการควบคุมภายใน กระบวนการทำงานและการเปลี่ยนแปลงจากการเพิ่มประเภทธุรกิจใหม่ ทั้งนี้ ผู้ตรวจสอบควรจะใช้เกณฑ์การพิจารณาความถี่ในการตรวจสอบจากระดับของความเสี่ยงเป็นหลัก

- แผนการตรวจสอบที่มีรายละเอียดของงบประมาณและกระบวนการวางแผน เป้าหมายในการตรวจสอบ ตารางเวลา ทีมงาน และการรายงานผลการตรวจสอบ อนึ่ง แผนควรครอบคลุมการปฏิบัติงานอย่างน้อย 12 เดือน โดยควรกำหนดจากผลรวมขององค์ประกอบหลัก 2 ประการคือ การประเมินความเสี่ยงและทรัพยากรที่จะต้องใช้ในการตรวจสอบเพื่อให้ได้รับผลการตรวจสอบตามระยะเวลาและความถี่ที่กำหนดไว้ในการตรวจสอบ และคณะกรรมการตรวจสอบควรอนุมัติแผนการตรวจสอบอย่างเป็นทางการทุกปี หรือทบทวนเป็นประจำทุกปีในกรณีที่เป็นแผนการตรวจสอบระยะยาว ทั้งนี้ ผู้ตรวจสอบภายในควรรายงานผลการดำเนินงานจริงเปรียบเทียบกับแผนงานที่กำหนด และรายงานรายละเอียดของการปรับเปลี่ยนแผนการตรวจสอบให้คณะกรรมการตรวจสอบอนุมัติเป็นประจำด้วย

- วัฏจักรและวงจรงานตรวจสอบจะช่วยชี้ให้เห็นความถี่ของงานตรวจสอบซึ่งปกติแล้วผู้ตรวจสอบจะกำหนดความถี่และเรื่องที่จะตรวจสอบได้จากการประเมินความเสี่ยง ซึ่งอาจถูกจำกัดด้วยจำนวนบุคลากรและระยะเวลาที่มี อย่างไรก็ดี ไม่ควรลดความถี่ในการตรวจสอบเรื่องที่มีความเสี่ยงสูง

- โปรแกรมการทำงานตรวจสอบแต่ละเรื่องจะต้องมีการกำหนดขอบเขตและทรัพยากรที่จะต้องใช้ในการตรวจสอบรวมไปถึงกระบวนการตรวจสอบ การทดสอบ และมาตรฐานการตรวจสอบ ทั้งนี้ การวางแผนงานที่ดี มีโครงสร้างของโปรแกรมการตรวจสอบที่เหมาะสม เป็นสิ่งที่จำเป็นอย่างยิ่งสำหรับการบริหารจัดการความเสี่ยงที่มีประสิทธิภาพ และการพัฒนาระบบการควบคุมภายในแบบครบถ้วน

- การรายงานผลการตรวจสอบควรจัดทำเป็นเอกสารส่งตรงถึงคณะกรรมการสถาบันการเงิน และผู้บริหารของแต่ละฝ่าย/สายงาน เกี่ยวกับความสอดคล้องของการปฏิบัติตามนโยบาย และขั้นตอนการทำงาน นอกจากนี้ควรรายงานถึงประสิทธิภาพ จุดอ่อนและแนวทางในการแก้ไขระบบการควบคุมภายใน นอกจากนี้ผู้บริหารสายงานตรวจสอบควรนำระบบการจัดระดับผลการตรวจสอบแจ้งให้คณะกรรมการตรวจสอบพิจารณาและอนุมัติก่อนนำไปใช้งาน เพื่อให้ระบบจัดระดับการตรวจสอบมีความถูกต้องและมีระดับการประเมินที่สม่ำเสมอตามมาตรฐาน เดียวกันทุกครั้งเพื่อสะท้อนให้เห็นถึงความเสี่ยงสุทธิที่มีต่อเรื่องต่างๆ ที่กำลังตรวจสอบอยู่

- การกำหนดเกี่ยวกับรายละเอียดของกระดาษทำการด้านตรวจสอบ เพื่อให้มีการจัดเก็บเอกสารหลักฐานข้อเท็จจริงและผลการปฏิบัติงานของผู้ตรวจสอบรวมถึงการกำหนดระยะเวลาการจัดเก็บเอกสารต่างๆ ด้วย

- กระบวนการติดตามผลการแก้ไขข้อบกพร่องที่มีนัยสำคัญที่ผู้รับการตรวจสอบยอมรับที่จะแก้ไขแล้วซึ่งผู้ตรวจสอบจะต้องตัดสินใจว่าจะยุติการติดตามเรื่องเมื่อใด

- โครงการพัฒนาความรู้และเสริมสร้างวิทยฐานะสำหรับพนักงานตรวจสอบเพื่อช่วยให้พนักงานมีความรู้ความชำนาญที่จำเป็นอย่างเพียงพอในการทำงาน

ทั้งนี้ สถาบันการเงินทุกแห่งควรนำเอาแนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางความเสี่ยงที่ใช้ และควรใช้แนวทางในการประเมินความเสี่ยงที่มีรูปแบบที่ชัดเจนมาช่วยในการกำหนดความถี่ในการตรวจสอบรวมไปถึงขอบเขตของการตรวจสอบด้วย (ผู้ตรวจสอบควรศึกษาในหัวข้อเรื่องการประเมินความเสี่ยงและการตรวจสอบตามแนวทางความเสี่ยงในหน้าที่ 15 ของคู่มือฉบับนี้เพิ่มเติม)

กระบวนการตรวจสอบด้าน IT จะแปรผันไปตามปรัชญา ความชำนาญทางด้านเทคนิคของสายงานตรวจสอบ และสภาพแวดล้อมที่ศูนย์คอมพิวเตอร์และระบบงานด้านผู้ใช้งาน แต่อย่างไรก็ดี การตรวจสอบที่ครบถ้วนและมีประสิทธิภาพนั้นจะต้องประกอบไปด้วยโปรแกรมการตรวจสอบที่ดีและมีพนักงานที่มีความชำนาญงานสัมพันธ์กับระดับของความสลับซับซ้อนของกิจกรรมของศูนย์ประมวลผลนั้นๆ อนึ่ง ขั้นตอนของการตรวจสอบอาจจะประกอบไปด้วยขั้นตอนการทดสอบด้วยมือหรือการใช้โปรแกรมคอมพิวเตอร์ช่วยในการตรวจสอบ (Computer Assisted Audit Techniques : CAATs) ก็ได้ (โปรดศึกษารายละเอียดเกี่ยวกับ CAATs ในบทต่อไป)

สายงานตรวจสอบ ควรกำหนดให้มีนโยบายในส่วนที่เกี่ยวข้องกับมาตรฐานของกระดาษทำการ การติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้อง และการจัดเก็บเอกสารและกระดาษทำการ ทั้งนี้ ผู้ตรวจสอบควรจัดหมวดหมู่ของกระดาษทำการให้ดี มีการเขียนข้อความที่ชัดเจน และมีรายละเอียดที่ครอบคลุมทุกเรื่องที่ดำเนินการตรวจสอบ รวมทั้งมีหลักฐานที่เพียงพอที่จะสนับสนุนการปฏิบัติงานและข้อสังเกตที่ได้จากการตรวจสอบ นอกจากนี้ จะต้องมีขั้นตอนการปฏิบัติงานที่เป็นมาตรฐานในการสร้างความมั่นใจว่าผู้บริหารและคณะกรรมการตรวจสอบได้รับทราบรายงานผลการตรวจสอบและสิ่งที่ตรวจสอบพบได้อย่างมีประสิทธิภาพ และจะต้องมีรายงานผลการตรวจสอบฉบับสมบูรณ์ให้กับคณะกรรมการตรวจสอบ อนึ่ง สถาบันการเงินควรจัดให้มีนโยบายเกี่ยวกับระยะเวลาในการจัดเก็บกระดาษทำการ และควรพิจารณากำหนดให้มีการปฏิบัติงานตรวจสอบภายในที่สอดคล้องกับมาตรฐานในการปฏิบัติงานสากล เช่น Standards for the Professional practice of Internal Auditing โดยหน่วยงาน Institute for Internal Auditor (IIA) และหน่วยงาน Standards Board of the Information Systems Audit and Control Association (ISACA) เป็นต้น อนึ่ง มาตรฐานสากลดังกล่าวนี้ จะต้องให้ความสำคัญเกี่ยวกับความเป็นอิสระ การดำเนินงานในลักษณะมืออาชีพ ขอบเขตการตรวจสอบ ประสิทธิภาพของงานตรวจสอบ การบริหารงานตรวจสอบและการสอบทานการรับประกันคุณภาพ (quality assurance reviews)

ผู้ตรวจสอบด้าน IT จำนวนมากใช้เทคนิคการตรวจสอบโดยอาศัยคอมพิวเตอร์ช่วยในการตรวจสอบ (CAATs) เพื่อช่วยเพิ่มขอบเขตของการตรวจสอบและลดต้นทุนในขั้นตอนการทดสอบและสุ่มตัวอย่างซึ่งเดิมทำด้วยมือ โดยเทคนิคการตรวจสอบโดยอาศัยคอมพิวเตอร์ช่วยในการตรวจสอบ (CAATs)นั้น จะต้องอาศัยเครื่องมือและเทคนิคต่างๆ หลายอย่างประกอบกัน เช่น การใช้ซอฟต์แวร์ด้านการตรวจสอบทั่วไป (generalized audit software) ซอฟต์แวร์อรรถประโยชน์ (utility software) ข้อมูลทดสอบ (test data) ซอฟต์แวร์ที่ทำหน้าที่วิเคราะห์และติดตามการไหลเวียนของข้อมูลผ่านโปรแกรมระบบงานพร้อมทั้งบันทึกผลลัพธ์ที่เกิดขึ้นทั้งหมด (application software tracking and mapping) และระบบตรวจสอบอัจฉริยะ (audit expert systems) อนึ่ง สำหรับขั้นตอนในการจัดหา CAATs มาใช้งานนั้น มีวิธีการดังต่อไปนี้

- พัฒนาโดยทีมโปรแกรมเมอร์ภายในองค์กร หรือโดยโปรแกรมเมอร์จากภายนอกองค์กรภายใต้การกำกับดูแลของสายงานตรวจสอบภายใน
- จัดซื้อซอฟต์แวร์ด้านการตรวจสอบทั่วไป เช่น โปรแกรมตรวจสอบสำเร็จรูปที่จำหน่ายโดยบริษัทตรวจสอบบัญชี หรือบริษัทผู้จำหน่าย
- พัฒนาโดยผู้ตรวจสอบด้าน IT
- จัดหาจากบริษัทผู้ผลิตอุปกรณ์คอมพิวเตอร์หรือบริษัทผลิตซอฟต์แวร์ เพื่อนำมาใช้ในการวิเคราะห์การทำงานของเครื่องมือ โปรแกรมเมอร์และการปฏิบัติการทางคอมพิวเตอร์อย่างมีประสิทธิภาพ

อย่างไรก็ดี ไม่ว่าสถาบันการเงินจะจัดหา CAATs มาจากที่ไหนก็ตาม สถาบันการเงินจะต้องควบคุมการใช้ CAATs อย่างรัดกุมภายใต้การดูแลของสายงานตรวจสอบ รวมไปถึงการควบคุมเอกสารที่เกี่ยวข้องทั้งหมด ข้อมูลเกี่ยวกับการทดสอบ รายละเอียดของโปรแกรมและข้อกำหนดต่างๆที่พิมพ์ออกมาแล้ว (Source listings) โปรแกรมต้นฉบับ (Source code) และโปรแกรมภาษาเครื่อง(Object code) รวมทั้งการเปลี่ยนแปลงแก้ไขต่าง ๆ อย่างเข้มงวดด้วยเช่นกัน อนึ่ง ถ้ามีการติดตั้ง CAATs โดยการใช้โปรแกรมควบคุมการเข้าถึงสถานที่จัดเก็บโปรแกรมเป็นเครื่องมือรักษาความปลอดภัยจะต้องควบคุมให้มีการใช้ password ในการป้องกันการเข้าถึงโปรแกรม CAATs ด้วย นอกจากนี้จะต้องควบคุมให้ผู้ตรวจสอบเป็นผู้มีสิทธิ์ ในการควบคุมทั้งเอกสารและการเขียนคำสั่งเรียกใช้โปรแกรม CAATs จากสถานที่จัดเก็บโปรแกรมได้เอง ในกรณีที่ทำไม่ได้ผู้ตรวจสอบจะต้องแยกจัดเก็บโปรแกรมระบบงาน CAATs ไว้ที่อื่นไม่จัดเก็บรวมไว้ในสถานที่จัดเก็บโปรแกรมระบบงานอื่นๆ อนึ่งโปรแกรมสำหรับใช้ในการตรวจสอบควรจะต้องมีการจัดทำเอกสารสารประกอบอย่างระมัดระวังเพื่อแสดงวัตถุประสงค์ที่ชัดเจนและสร้างความมั่นใจในการใช้งานได้อย่างดีและต่อเนื่อง โดยมีตัวอย่างในการนำโปรแกรม CAATs มาใช้งาน ดังต่อไปนี้คือ

- การทดสอบรายการและยอดคงเหลือ เช่น การคำนวณดอกเบี้ย

- กระบวนการวิเคราะห์และสอบทาน เช่น รายการที่ไม่สัมพันธ์สอดคล้องกัน หรือมีผลกระทบที่มีนัยสำคัญ

- การทดสอบการปฏิบัติงานตามข้อกำหนดของระบบควบคุมทั่วไป เช่น ทดสอบการกำหนดค่าต่าง ๆ ในโปรแกรมระบบปฏิบัติการ หรือขั้นตอนในการเข้าถึงโปรแกรมที่จัดเก็บไว้ใน libraries

- โปรแกรมเลือกและสุ่มตัวอย่างข้อมูล เพื่อดึงข้อมูลมาตรวจสอบ

- การทดสอบการปฏิบัติงานตามข้อกำหนดในการควบคุมโปรแกรมระบบงาน เช่น ระบบควบคุมต่างๆของโปรแกรมระบบงาน

- การทดสอบความถูกต้องของการทำรายการผ่านระบบบัญชีอัตโนมัติต่างๆ

- การทดสอบเจาะระบบ

เครื่องมือและเทคนิคต่าง ๆ เหล่านี้ สามารถใช้ในการตรวจสอบความถูกต้องและน่าเชื่อถือของข้อมูล โดยการทดสอบตรรกะของการประมวลผลข้อมูลในระบบมากกว่าที่จะพึ่งพิงเฉพาะระบบการยืนยันความถูกต้องของระบบการนำข้อมูลเข้าและระบบการนำข้อมูลออกเท่านั้น

2.4 การประเมินความเสี่ยงและการตรวจสอบตามแนวความเสี่ยง

สรุปแนวทางการปฏิบัติ

คณะกรรมการสถาบันการเงินควรจัดให้มีการตรวจสอบตามแนวทางความเสี่ยงที่มีประสิทธิภาพ

โปรแกรมการตรวจสอบตามแนวทางความเสี่ยงที่มีประสิทธิภาพจะต้องครอบคลุมไปถึงการดำเนินกิจกรรมหลักที่สำคัญๆ ของสถาบันการเงินอย่างทั่วถึง สำหรับความถี่และความลึกของแต่ละเรื่องที่ตรวจสอบควรมีความสอดคล้องกับการประเมินความเสี่ยงในเรื่องนั้นด้วย และผู้ตรวจสอบควรจะต้องพิจารณาและกำหนดแนวทางการตรวจสอบให้เหมาะสมและสอดคล้องกับขนาดและความซับซ้อนของสถาบันการเงินด้วย

2.4.1 รายละเอียดของโปรแกรมการตรวจสอบ

การออกแบบโปรแกรมการตรวจสอบตามแนวความเสี่ยงที่เหมาะสมจะช่วยเพิ่มประสิทธิภาพและประสิทธิผลของการตรวจสอบ ดังนั้น ผู้บริหารงานตรวจสอบจึงต้องจัดรูปแบบและระดับความลึกในการตรวจสอบตามแนวความเสี่ยงให้สัมพันธ์กับขนาดและความซับซ้อนขององค์กรและจะต้องจัดให้มีกระบวนการในการประเมินความเสี่ยงที่มีประสิทธิภาพเพื่อช่วยกำหนดขอบเขต

ของการตรวจสอบให้มีความเหมาะสมให้ครอบคลุมสภาพแวดล้อมทางด้าน IT ขององค์กร อนึ่ง กระบวนการประเมินความเสี่ยงนั้นจะต้องช่วยให้คณะกรรมการสถาบันการเงินและผู้ตรวจสอบได้รับข้อมูลที่เป็นรูปธรรมในการจัดระดับความสำคัญและการจัดสรรทรัพยากรในการตรวจสอบได้อย่างเหมาะสม และโปรแกรมการตรวจสอบตามแนวทางความเสี่ยงควรมีลักษณะ ดังต่อไปนี้ คือ

- กำหนด/ระบุ ข้อมูล โปรแกรมระบบงาน และระบบปฏิบัติการ เทคโนโลยี องค์ประกอบสนับสนุนต่าง ๆ และบุคลากร

- กำหนด/ระบุ รายละเอียดของกิจกรรมทางธุรกิจ และขั้นตอนการปฏิบัติงานต่าง ๆ

- การสำแดงรายละเอียดของหน่วยงานด้านธุรกิจ ฝ่ายงาน สายการผลิต หรือระบบงานหลัก รวมไปถึงความเสี่ยงและลักษณะของการควบคุมพร้อมทั้งจัดทำเป็นเอกสารแสดงให้เห็นโครงสร้างของความเสี่ยงและระบบควบคุมทั้งหมดขององค์กร

- การนำเอาระบบการวัดผลหรือการให้คะแนนมาใช้ในการประเมินและการจัดลำดับความเสี่ยงและระบบการควบคุมต่างๆสำหรับหน่วยงาน ฝ่ายงาน หรือผลิตภัณฑ์ทางธุรกิจที่สำคัญอย่างทั่วถึงทั้งองค์กร

- ข้อมูลที่คณะกรรมการตรวจสอบได้อนุมัติแผนการประเมินความเสี่ยงและแผนการตรวจสอบตามแนวทางความเสี่ยงประจำปี รวมไปถึงกำหนดเวลาการตรวจสอบ ความถี่ในการตรวจสอบ ขอบเขตของการตรวจสอบ และการใช้ทรัพยากรในการตรวจสอบ

- การปฏิบัติงานตามแผนการตรวจสอบทุกขั้นตอน คือ การวางแผน การปฏิบัติงานจริง การรายงานผลการตรวจสอบ และการติดตามผลการแก้ไขตามข้อสังเกต

- การจัดเตรียมกระบวนการเฝ้าติดตามดูแล และปรับปรุงระบบการประเมินความเสี่ยงให้ทันสมัยอย่างน้อยปีละครั้ง สำหรับหน่วยงาน ฝ่ายงาน หรือผลิตภัณฑ์ทางธุรกิจ และระบบงานที่สำคัญ

2.4.2 ระบบการจัดลำดับความเสี่ยง

โปรแกรมการตรวจสอบตามแนวความเสี่ยงที่มีประสิทธิภาพ จะเกิดขึ้นได้ก็จะต้องอาศัยระบบการจัดลำดับความเสี่ยง (Risk scoring system) ที่มีประสิทธิภาพ ดังนั้น คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูงจะต้องดำเนินการให้เกิดความมั่นใจว่าการจัดลำดับความเสี่ยงเป็นระบบงานที่สามารถเข้าใจได้ง่าย และได้รวมเอาปัจจัยความเสี่ยงที่เกี่ยวข้องทั้งหมดเข้ามาไว้ด้วยกันแล้ว และจะต้องหลีกเลี่ยงการใช้ความคิดเห็นส่วนบุคคลให้มากที่สุดเท่าที่จะเป็นไปได้ โดยมีตัวอย่างของปัจจัยความเสี่ยงที่สำคัญๆ ที่จำเป็นต้องใช้ในการสร้างระบบการจัดลำดับความเสี่ยงที่ใช้กันอย่างแพร่หลายทั่วไป ดังต่อไปนี้ คือ

- ความเพียงพอของระบบการควบคุมภายใน

- ลักษณะของรายการธุรกรรมต่าง ๆ ที่เกิดขึ้น เช่น ลำดับที่ มูลค่าของรายการ ความซับซ้อนของธุรกรรม เป็นต้น

- อายุของระบบปฏิบัติการ และโปรแกรมระบบงาน

- ลักษณะของสภาพแวดล้อมในการปฏิบัติงานประจำ เช่น การเปลี่ยนแปลงของจำนวนธุรกรรม ระดับของความเข้มข้นในการควบคุมระบบงานและการรายงานผลจากส่วนกลาง ระดับความสำคัญของข้อมูลที่ประมวลผล ผลกระทบที่มีต่อกระบวนการทางธุรกิจที่สำคัญ ผลกระทบที่มีนัยสำคัญทางการเงิน แผนการเปลี่ยนแปลงโครงสร้างของข้อมูล สภาพแวดล้อมทางธุรกิจ และสภาพแวดล้อมในการการกำกับดูแลของทางการ เป็นต้น

- การรักษาความปลอดภัยทั้งด้านกายภาพและด้านตรรกะของข้อมูล อุปกรณ์ และอาคารสถานที่

- ความเพียงพอของการกำกับดูแลและการเฝ้าติดตามดูแล การบริหารงานที่เกี่ยวข้องกับการปฏิบัติงานประจำวัน

- ผลการตรวจสอบครั้งก่อนของเจ้าหน้าที่ตรวจสอบหรือเจ้าหน้าที่ทางการและการดำเนินการของผู้บริหารต่อข้อบกพร่องที่พบจากการตรวจสอบดังกล่าว

- การบริหารงานด้านทรัพยากรบุคคล รวมถึงประสบการณ์ของฝ่ายจัดการและพนักงาน อัตราการหมุนเวียนเข้า/ออกของพนักงาน ความชำนาญทางด้านเทคนิค ความรู้ความสามารถ แผนการจัดหาบุคลากรทดแทน และระดับความเข้มข้นในการกระจายอำนาจ

- การกำกับดูแลโดยผู้บริหารระดับสูง

ผู้ตรวจสอบควรพัฒนาแนวทางการดำเนินงานที่ชัดเจนเป็นลายลักษณ์อักษรและนำเสนอให้คณะกรรมการตรวจสอบและคณะกรรมการธนาคารพิจารณาในส่วนที่เกี่ยวข้องกับเครื่องมือและปัจจัยที่ใช้ในการประเมินความเสี่ยง ทั้งนี้ รูปแบบของแนวทางการดำเนินงานดังกล่าว (guidelines) ควรปรับเปลี่ยนให้สอดคล้องกับแต่ละองค์กร ตามขนาด ความซับซ้อน ขอบเขตของการดำเนินธุรกรรม สภาพแวดล้อมทางภูมิศาสตร์ และความหลากหลายของระบบเทคโนโลยีสารสนเทศของสถาบันการเงินที่ใช้งานอยู่ ทั้งนี้ สถาบันการเงินสามารถที่จะใช้มาตรฐานในการดำเนินงานทั่วไปตามประเภทของธุรกิจ หรือประสบการณ์ของตนเองในการจัดลำดับความเสี่ยง risk scoring ก็ได้ และผู้ตรวจสอบควรที่จะนำเอาแนวทางการประเมินความเสี่ยงมาใช้ในการวัดหรือประเมินความเสี่ยงและกำหนดช่วงของระดับหรือการประเมินผล (เช่น การจัดกลุ่มของความเสี่ยงเป็นกลุ่มความเสี่ยงระดับสูง กลาง ต่ำ หรือ กำหนดเป็นระดับของตัวเลข เช่น 1 ถึง 5 เป็นต้น) นอกจากนี้ แนวทางการประเมินความเสี่ยงดังกล่าวควรจะต้องมีรายละเอียดอื่นๆ ประกอบ ดังต่อไปนี้ คือ

- รอบระยะเวลาในการตรวจสอบ (audit cycles) ที่สอดคล้องกับการจัดลำดับความเสี่ยง ตัวอย่างเช่น บางสถาบันการเงินจะกำหนดให้มีการตรวจสอบ 1 ครั้งภายในระยะเวลา 12 เดือน หรือระยะเวลาที่น้อยกว่านั้น สำหรับความเสี่ยงที่อยู่ในระดับสูง หรือทุก 24 เดือน หรือน้อยกว่าสำหรับความเสี่ยงที่อยู่ในระดับปานกลาง และทุก 36 เดือนสำหรับความเสี่ยงที่อยู่ในระดับต่ำ ทั้งนี้ รอบระยะเวลาในการตรวจสอบจะต้องกำหนดเป็นตัวเลขที่ชัดเจน

- ช่วงระยะเวลาที่ใช้ในการประเมินความเสี่ยงของแต่ละฝ่ายงานหรือกิจกรรมทางธุรกิจ (โดยปกติจะต้องประเมินความเสี่ยงเป็นประจำทุกปี แต่สถาบันการเงินจะต้องทำการประเมินความเสี่ยงบ่อยมากขึ้นกว่าปกติถ้ามีการเติบโตอย่างเร่งด่วน หรือการเปลี่ยนแปลงการปฏิบัติงานประจำวัน หรือมีการเปลี่ยนแปลงกิจกรรมที่ดำเนินงานอยู่ให้แตกต่างไปจากเดิม)

- ข้อกำหนดต่างๆ ในการจัดทำเอกสารประกอบการพิจารณาเรื่องการจัดลำดับความเสี่ยง

- แนวทางการประเมินความเสี่ยงจะต้องมีข้อกำหนดสำหรับกรณีพิเศษที่จะต้องมีการยกเว้นหรือไม่ปฏิบัติตามผลการประเมินความเสี่ยงต่างๆ และมีรายละเอียดว่าใครบ้างที่มีอำนาจดำเนินการได้ และกระบวนการในการขออนุญาตไม่ปฏิบัติตามผลการประเมินความเสี่ยง รวมถึงการจัดทำรายงานและเอกสารประกอบ

กลุ่มธุรกิจในอุตสาหกรรมหลายๆ ประเภทได้จัดเตรียมอำนวยความสะดวกให้สถาบันการเงินสามารถที่จะนำเอาโครงสร้างแบบ matrix รูปของแบบจำลอง หรือข้อมูลเพิ่มเติมอื่นๆ มาใช้ในการประเมินความเสี่ยง เช่น ISACA สมาคมนายธนาคารของสหรัฐอเมริกา (ABA) สมาคมผู้สอบบัญชีรับอนุญาตของสหรัฐอเมริกา (AICPA) และสมาคมผู้ตรวจสอบภายใน (IIA) เป็นต้น อนึ่ง หน้าที่ในการบริหารโปรแกรมการตรวจสอบตามแนวความเสี่ยงประจำวัน เป็นหน้าที่ของผู้จัดการฝ่ายตรวจสอบภายใน ซึ่งจะต้องคอยเฝ้าติดตามดูแลขอบเขตของการตรวจสอบและกระบวนการประเมินความเสี่ยงเพื่อให้เกิดความมั่นใจว่าขอบเขตของการตรวจสอบนั้นยังมีความเหมาะสม นอกจากนี้ ผู้จัดการฝ่ายตรวจสอบภายในยังมีหน้าที่ในการจัดเตรียมรายงานแสดงการจัดระดับของความเสี่ยง ขอบเขตของการตรวจสอบตามแผนงาน รอบระยะเวลาในการตรวจสอบในแต่ละเรื่องและจะต้องสอบทานความถูกต้องน่าเชื่อถือได้ของระบบประเมินความเสี่ยงอย่างน้อยปีละครั้ง หรือเร็วกว่านั้นถ้ามีการเปลี่ยนแปลงที่มีนัยสำคัญในฝ่ายงานต่าง ๆ หรือหน้าที่งานนั้นๆ ส่วนผู้จัดการฝ่ายปฏิบัติการและผู้ตรวจสอบนั้น ควรที่จะร่วมกันทำงานในการประเมินความเสี่ยงของทุกๆฝ่ายงานเพื่อให้แน่ใจว่าการประเมินความเสี่ยงได้กระทำไว้อย่างถูกต้องและสมเหตุผลแล้ว

ผู้ตรวจสอบควรสอบทานกระบวนการควบคุมภายใน และการวิเคราะห์ข้อมูลทางการเงิน หรือการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล ว่ามีปัจจัยใดบ้างที่จะไปมีผลกระทบกับผลการ

ประเมินความเสี่ยงหรือการจัดลำดับความเสี่ยง ในขณะเดียวกัน ผู้จัดการฝ่ายปฏิบัติการมีหน้าที่จะต้องให้ข้อมูลที่เป็นปัจจุบันกับผู้ตรวจสอบว่ามีการเปลี่ยนแปลงที่สำคัญอะไรบ้างในฝ่ายงานหรือหน้าที่งานที่สำคัญต่าง ๆ เช่น การออกผลิตภัณฑ์ใหม่ การติดตั้งระบบงานใหม่ การโอนย้ายข้อมูลจากระบบงานเก่าสู่ระบบงานใหม่ หรือการเปลี่ยนแปลงบุคลากรในองค์กร เป็นต้น

2.5 การมีส่วนร่วมของผู้ตรวจสอบภายในสำหรับการพัฒนาระบบงาน การจัดหาระบบงาน การโอนย้ายระบบงาน และการทดสอบ

สรุปแนวทางการปฏิบัติ

ผู้บริหารระดับสูงควรมอบหมายให้เข้าไปมีส่วนเกี่ยวข้องในงานตรวจสอบด้าน IT ที่สำคัญๆ เช่น การพัฒนาระบบงาน การจัดซื้อ/จัดหาระบบงาน การโอนย้ายข้อมูลเดิมเข้าสู่ระบบงานใหม่ และการทดสอบ

การพัฒนาระบบงาน การจัดซื้อ/จัดหาระบบงาน การโอนย้ายข้อมูลเดิมเข้าสู่ระบบงานใหม่ และการทดสอบ เป็นการดำเนินงานที่ซับซ้อนและใช้ระยะเวลายาวนาน จะต้องอาศัยความร่วมมืออย่างเต็มที่จากโปรแกรมเมอร์ ผู้ใช้งาน และผู้ตรวจสอบภายใน ทั้งนี้ กระบวนการดำเนินงานทั้งหมดนี้รู้จักกันในชื่อว่า กระบวนการพัฒนาระบบงานและโปรแกรม (system development life cycle or system development methodology) ซึ่งเป็นกระบวนการสำคัญกำหนดให้มีการจัดเก็บข้อมูลในขั้นตอนการดำเนินงานต่างๆ ให้ครบถ้วนเพื่อช่วยให้เกิดความมั่นใจว่าโปรแกรมระบบงานจะสามารถทำงานได้ตรงตามความต้องการของสถาบันการเงิน ดังนั้น เมื่อการดำเนินงานได้พัฒนามาถึงขั้นตอนที่สำคัญๆ เหล่านี้ ผู้ตรวจสอบภายในจะต้องทำการทบทวนระบบการควบคุมภายใน ระบบการทดสอบ และระบบการสร้างร่องรอยเพื่อติดตามและตรวจสอบที่ถูกจัดเก็บไว้ในโปรแกรมระบบงาน อนึ่ง เนื่องจากการติดตามผลการดำเนินงานของระบบควบคุมภายในของโปรแกรมระบบงานที่ถูกติดตั้งและใช้งานจริงแล้วเป็นเรื่องที่ยุ่งยากและเสียค่าใช้จ่ายสูงมาก ดังนั้น สถาบันการเงินควรที่จะพัฒนาแนวทางการประเมินความเสี่ยงที่เน้นไปที่การทบทวนระบบงานใหม่ตั้งแต่ขั้นตอนแรกของการออกแบบระบบงานเพื่อให้ผู้ตรวจสอบภายในสามารถทบทวนความเพียงพอของระบบการควบคุมภายในได้อย่างเป็นอิสระตั้งแต่ช่วงต้นของกระบวนการพัฒนาโปรแกรมระบบงาน

นอกจากนี้ นโยบายด้านตรวจสอบของสถาบันการเงินที่ผ่านการอนุมัติจากคณะกรรมการสถาบันการเงินแล้ว จะต้องมีการกำหนดแนวทางและวิธีการดำเนินงานว่าผู้ตรวจสอบ

ภายในจะสามารถเข้าไปเกี่ยวข้องกับการพัฒนาระบบงาน การจัดซื้อ/จัดหาระบบงาน การโอนย้ายข้อมูลเดิมเข้าสู่ระบบงานใหม่ และการทดสอบได้อย่างไรบ้าง รวมถึงการติดตามดูแล การรายงานผล หรือการรายงานผู้บริหารระดับสูงเพื่อพิจารณาดำเนินการ (กรณีที่ตรวจพบว่าระบบการควบคุมภายในที่มีอยู่ไม่เพียงพอในการรองรับความเสี่ยง หรือกระบวนการทดสอบยังไม่เพียงพอ) ส่วนในขั้นตอนของการจัดซื้อ/จัดหาระบบงานนั้นก็จะต้องมีการกำหนดว่าจะให้ผู้ตรวจสอบเข้าไปมีส่วนเกี่ยวข้องในขั้นตอนใดของกระบวนการพัฒนาระบบงานและโปรแกรม (system development life cycle) และถ้าเป็นการจัดซื้อ/จัดหา ระบบงานที่มีความผลกระทบที่สำคัญต่อระบบงาน IT ผู้ตรวจสอบภายในควรจะต้องเข้าไปมีส่วนร่วมตั้งแต่ขั้นตอนแรกในการตรวจสอบความเป็นไปได้ในการเลือกใช้โปรแกรมระบบงานจากผู้จัดจำหน่ายและผลกระทบในการดำเนินการดังกล่าว (Due diligence)

อนึ่ง สิ่งที่มีความสำคัญมากในการที่ผู้ตรวจสอบภายในจะเข้าไปมีส่วนเกี่ยวข้องในกระบวนการพัฒนาระบบงานและโปรแกรม ก็คือ ความเป็นอิสระและการให้ความเห็นที่ตรงไปตรงมา ซึ่งผู้ตรวจสอบควรพิจารณาและให้คำแนะนำเกี่ยวกับระบบการควบคุมต่างๆ ที่เหมาะสมแก่ผู้บริหารโครงการ (Project management) แต่อย่างไรก็ดี คำแนะนำดังกล่าวมิได้เป็นการรับประกันล่วงหน้าว่าระบบการควบคุมต่างๆนั้นจะมีความเหมาะสมแล้ว ทั้งนี้ก็เพราะว่าผู้ตรวจสอบภายในมีฐานะที่เป็นมากกว่าผู้เชี่ยวชาญ/ที่ปรึกษา ผู้ตรวจสอบภายในจึงไม่ควรเข้าไปมีส่วนเกี่ยวข้องโดยตรงกับการตัดสินใจของฝ่ายบริหาร แต่ควรจะเป็นผู้ที่ยกประเด็นขึ้นคัดค้านถ้าผู้ตรวจสอบภายในเชื่อว่าระบบการควบคุมภายในที่มีอยู่ไม่มีความเพียงพอ

เมื่อมีการพัฒนาระบบงานใหม่ มีการโอนย้ายข้อมูลเดิมเข้าสู่ระบบงานใหม่หรือมีการปรับปรุงระบบงานเดิมจนแล้วเสร็จและนำออกใช้งานจริง ผู้ตรวจสอบภายในด้าน IT ควรจะต้องทำการตรวจสอบระบบงานภายหลังการติดตั้งและใช้งานจริง (post-implementation review) โดยไม่ชักช้าและควรตรวจสอบให้ครอบคลุมไปถึงเรื่อง ตรรกะของโปรแกรม การคำนวณ เงื่อนไขของข้อผิดพลาดต่าง ๆ การแก้ไข และระบบการควบคุมต่างๆเพื่อให้เกิดความมั่นใจว่าระบบงานสามารถดำเนินการได้ตามที่คาดหมายไว้ อนึ่ง การสอบทานหลังจากที่ระบบนำออกใช้งานจริงโดยเร็วจะช่วยให้ผู้ตรวจสอบสามารถตรวจสอบกระบวนการดำเนินงานที่ผิดพลาดหรือเงื่อนไขที่ไม่เหมาะสมได้อย่างรวดเร็ว ซึ่งจะช่วยลดความเสียหายจากการประมวลผลผิดพลาด หรือความไม่มีประสิทธิภาพของโปรแกรมระบบงานและระบบควบคุม หรือความเสียหายทางด้านชื่อเสียงจากการที่ระบบงานแสดงข้อมูลของลูกค้าผิดพลาดหรือไม่ถูกต้อง

สำหรับสถาบันการเงินที่มีระบบงานและสิ่งอำนวยความสะดวกด้าน IT ที่มีขนาดใหญ่ มักจะมีทีมงานตรวจสอบคุณภาพของงาน (Quality assurance) หรือกลุ่มบริหารงานด้านการเปลี่ยนแปลง (Change management groups) เป็นผู้รับผิดชอบในการตรวจสอบระบบงานภายหลังการ

ติดตั้งและใช้งานจริง (post-implementation) เพราะฉะนั้นผู้ตรวจสอบด้าน IT ก็ไม่จำเป็นต้องทำการตรวจสอบด้วยตัวเอง แต่ควรเข้าไปมีส่วนร่วมในการกำหนดเงื่อนไขและทำการวิเคราะห์ผลลัพธ์อื่นๆ อย่างเป็นอิสระแทน

2.6 การใช้บริการตรวจสอบภายในจากหน่วยงานภายนอก

สรุปแนวทางการปฏิบัติ

คณะกรรมการสถาบันการเงินที่ใช้บริการตรวจสอบภายในด้าน IT จากหน่วยงานภายนอก ควรพิจารณาถึงโครงสร้าง ขอบเขต และการบริหารงานบริการของผู้ให้บริการภายนอกว่าจะสามารถประเมินความเพียงพอของระบบควบคุมภายในได้อย่างเหมาะสมเพียงพอ

เพื่อแก้ไขปัญหาเกี่ยวกับคุณภาพและจำนวนของผู้ตรวจสอบ สถาบันการเงินจำนวนมากได้เปลี่ยนไปใช้บริการจากบริษัทสอบบัญชีที่มิได้ให้บริการจัดทำบัญชีให้กับองค์กร (Independence public accounting firms) หรือผู้เชี่ยวชาญสาขาวิชาชีพอื่นๆ จากภายนอกองค์กรให้เข้ามาทำงานแทนผู้ตรวจสอบภายในซึ่งการดำเนินการในรูปแบบดังกล่าวมีชื่อเรียกหลายแบบ ดังนี้ คือ “Internal audit outsourcing” “Internal audit assistance” “audit co-sourcing” หรือ “extended audit service”

การใช้บริการจากผู้ให้บริการภายนอกดังกล่าว อาจจะเป็นประโยชน์กับสถาบันการเงินก็ได้ ถ้าสถาบันการเงินได้มีการออกแบบโครงสร้าง ดำเนินการอย่างระมัดระวัง และบริหารงานอย่างมีวิจารณญาณ และฝ่ายบริหารของสถาบันการเงินจะต้องสร้างให้เกิดความมั่นใจว่าการใช้บริการดังกล่าวจะไม่ก่อเกิดปัญหาเกี่ยวกับผลประโยชน์ที่ทับซ้อนหรือขัดกัน (Conflicts of interest) และจะไม่ทำให้การตรวจสอบภายในขาดความเป็นอิสระ เช่น การว่าจ้างให้บริษัทสอบบัญชีตรวจสอบระบบงานด้าน IT ในขณะเดียวกันก็ว่าจ้างบริษัทดังกล่าวในการจัดทำงบการเงิน หรือให้บริการงานด้าน IT หรือทำหน้าที่เป็นที่ปรึกษาให้กับฝ่ายจัดการ ในเวลาเดียวกัน ทั้งนี้ เพราะว่าคณะกรรมการสถาบันการเงินยังคงมีความรับผิดชอบที่จะต้องสร้างความมั่นใจว่าหน้าที่ในการตรวจสอบภายในที่ได้มอบหมายให้ผู้ให้บริการจากภายนอกไปดำเนินการนั้นจะสามารถดำเนินการไปได้อย่างมีประสิทธิภาพและสอดคล้องกับแนวทางและการปฏิบัติงานที่ทางการกำหนดไว้

ผู้ตรวจสอบภายในของสถาบันการเงินควรพิจารณาว่าโครงสร้าง ขอบเขต และการบริหารงานบริการของผู้ให้บริการภายนอกมีความเหมาะสมพียงพอที่จะประเมินความเพียงพอของระบบควบคุมภายในหรือไม่ นอกจากนี้ ควรจะต้องประเมินว่ากรรมการและผู้บริหารระดับสูงของ

สถาบันการเงินได้ทำหน้าที่ตามความรับผิดชอบของตนเองได้อย่างสมบรูณ์ในการจัดให้มีระบบการควบคุมภายในที่มีประสิทธิภาพ และได้กำกับดูแลหน้าที่ในการตรวจสอบภายในที่ได้ว่าจ้างให้ผู้ให้บริการจากภายนอกดำเนินการไปแล้วอย่างมีประสิทธิภาพด้วย สำหรับแนวทางโดยละเอียดเกี่ยวกับโครงสร้าง ความเป็นอิสระ และแนวทางปฏิบัติที่ดีในการใช้บริการในตรวจสอบภายในจากผู้ให้บริการจากภายนอก ขอให้ผู้ตรวจสอบศึกษาเพิ่มเติมได้จากคู่มือ Interagency Policy Statement on the Internal Audit Functions and Its Outsourcing

2.6.1 ความเป็นอิสระของผู้ตรวจสอบภายนอกที่ให้บริการด้านตรวจสอบภายใน

ผู้ตรวจสอบภายในควรทบทวนว่าฝ่ายบริหารได้ออกแบบและดำเนินการในส่วนที่เกี่ยวข้องกับการใช้บริการจากผู้ให้บริการจากภายนอกองค์กรและดำเนินการให้ผู้ตรวจสอบจากภายนอกสามารถทำงานได้อย่างอิสระ เนื่องจากบริษัทผู้สอบบัญชีที่รับจ้างและทำหน้าที่เป็นผู้ตรวจสอบภายในแทนผู้ตรวจสอบภายในขององค์กร อาจจะมีความเสี่ยงที่จะปฏิบัติงานอย่างไม่เป็นอิสระเมื่อบริษัทผู้สอบบัญชีดังกล่าว ได้รับจ้างบริษัทในการทำหน้าที่เป็นผู้ตรวจสอบบัญชีของบริษัทไปพร้อมๆกันด้วย

ทั้งนี้ เพราะว่าบริษัทผู้สอบบัญชีที่รับจ้างทำหน้าที่เป็นผู้ตรวจสอบภายในแทนผู้ตรวจสอบภายในขององค์กรอาจจะไม่สามารถทำหน้าที่ได้อย่างเป็นอิสระ จะต้องพบกับปัญหาที่จะต้องประเมินผลงานของตนเองในการทำหน้าที่ผู้ตรวจสอบภายใน เนื่องจากหน้าที่ของผู้ตรวจสอบภายนอกส่วนหนึ่ง ก็คือ การประเมินขอบเขตของงานที่จะต้องตรวจสอบและความน่าเชื่อถือของผลการตรวจสอบภายในประกอบด้วย (กฎหมาย SOX ของสหรัฐอเมริกาก็ไม่ยินยอมให้บริษัทผู้สอบบัญชีรับทำหน้าที่ให้บริการตรวจสอบภายในกับบริษัทที่ตนเองเป็นผู้สอบบัญชีรับอนุญาตอยู่ด้วย)

2.6.2 รูปแบบการใช้บริการงานตรวจสอบภายในจากหน่วยงานภายนอก

ข้อตกลงในการใช้บริการจากผู้ให้บริการภายนอก ก็คือ การจัดทำสัญญาในการใช้บริการตรวจสอบภายในของสถาบันการเงินจากบริษัทผู้ให้บริการจากภายนอก โดยมีรูปแบบของการให้บริการที่แตกต่างกันไปตามขนาดของสถาบันการเงิน ตัวอย่างเช่น การจัดทำสัญญาว่าจ้างให้บริษัทผู้สอบบัญชีให้เข้ามาช่วยเหลือผู้ตรวจสอบภายในเพื่อตรวจสอบระบบงานที่ผู้ตรวจสอบภายในไม่มีความรู้ความชำนาญ ซึ่งในกรณีนี้ผู้ให้บริการตรวจสอบจะต้องอยู่ภายใต้การดูแลของผู้บริหารของสถาบันการเงิน โดยอาจจะจำกัดเพียงเพื่อช่วยผู้ตรวจสอบภายใน ในด้านที่ขาดความเชี่ยวชาญในการตรวจสอบภายใน และผู้ตรวจสอบภายในมีหน้าที่ กรณีดังกล่าวผู้จัดการสายงานตรวจสอบและผู้ตรวจสอบจะต้องกำกับดูแลการปฏิบัติงานของผู้ให้บริการภายนอกอย่างเพียงพอ

อีกรูปแบบหนึ่ง เป็นการว่าจ้างผู้ให้บริการตรวจสอบจากภายนอก เข้ามาช่วยตรวจสอบงานตรวจสอบภายในทั้งหมดหรือบางส่วน ดังนั้น ถ้าสถาบันการเงินเลือกที่จะใช้บริการจาก

ผู้ให้บริการจากภายนอกในลักษณะนี้แล้ว สถาบันการเงินจะต้องจัดให้มีทั้งผู้จัดการฝ่ายตรวจสอบภายใน และพนักงานตรวจสอบภายในที่เหมาะสมและเพียงพอที่จะกำกับดูแลการดำเนินงานของผู้ให้บริการจากภายนอก ตามปกติแล้วบริษัทผู้ให้บริการในการตรวจสอบจากภายนอกจะเข้ามาช่วยเหลือผู้ตรวจสอบภายในเพื่อกำหนด หรือประเมินขอบเขตการดำเนินงานที่มีความเสี่ยงและระดับของความเสี่ยงที่จะต้องเข้าไปตรวจสอบพร้อมกับเข้าไปดำเนินการตรวจสอบและตั้งข้อสังเกตตามที่ผู้จัดการฝ่ายตรวจสอบได้อนุมัติเรียบร้อยแล้ว และควรที่จะร่วมมือกับผู้จัดการฝ่ายตรวจสอบภายในในการรายงานผลการตรวจสอบที่มีนัยสำคัญให้คณะกรรมการตรวจสอบและคณะกรรมการสถาบันการเงินรับทราบด้วย

อนึ่ง ก่อนที่สถาบันการเงินจะทำสัญญาการใช้บริการดังกล่าว ฝ่ายบริหารของสถาบันการเงินจะต้องศึกษาความเป็นไปได้ในการเลือกใช้บริการจากผู้ให้บริการและผลกระทบในการดำเนินการดังกล่าว (Due diligence) เพื่อให้เกิดความมั่นใจว่าผู้ให้บริการจากภายนอกมีจำนวนของพนักงานที่มีคุณภาพอย่างเพียงพอในการให้บริการดังกล่าวได้ และต้องดำรงรักษาความเชี่ยวชาญในการทำงานไว้อย่างมีประสิทธิภาพในการทำหน้าที่ที่ได้รับมอบหมาย และควบคุมให้ผู้ให้บริการจากภายนอกยืนยันกับผู้จัดการฝ่ายตรวจสอบภายในรับทราบและมั่นใจในความรู้ความสามารถของบุคลากรที่จะมาช่วยทำงาน และจะต้องแจ้งให้ผู้จัดการฝ่ายตรวจสอบภายในรับทราบอย่างทันท่วงทีเมื่อผู้ให้บริการจะเปลี่ยนแปลงตัวบุคลากรในการทำงานซึ่งมีผลกระทบที่มีความสำคัญ

เมื่อสถาบันการเงินตัดสินใจเลือกใช้บริการจากผู้ให้บริการจากภายนอก หรือมีการเปลี่ยนแปลงสัดส่วนของทรัพยากรสำหรับการตรวจสอบภายในและการตรวจสอบภายนอกอย่างมีนัยสำคัญ สิ่งเหล่านี้ก็จะก่อให้เกิดความเสี่ยงด้านปฏิบัติการเพิ่มสูงขึ้น และสัญญาการใช้บริการอาจจะถูกยกเลิกได้อย่างกะทันหัน สถาบันการเงินจึงควรต้องจัดให้มีแผนฉุกเฉินเพื่อป้องกันความเสี่ยง โดยเฉพาะสำหรับขอบเขตในการตรวจสอบที่เกี่ยวข้องกับความเสี่ยงที่มีระดับความเสี่ยงสูงๆ โดยการพิจารณาแผนทางเลือกเพื่อรองรับในกรณีที่ผู้ตรวจสอบที่มีความชำนาญไม่สามารถทำงานตรวจสอบที่มีความเสี่ยงได้สำเร็จ หรือต้องมีการยกเลิกสัญญาว่าจ้างโดยการจัดเก็บข้อมูลเกี่ยวกับการให้บริการและความเชี่ยวชาญของผู้ให้บริการภายนอกรายอื่น ๆที่สามารถที่จะให้บริการในลักษณะเดียวกันหรือที่สามารถให้บริการได้มากกว่า

ในขั้นตอนของการจัดทำข้อตกลงกันระหว่างสถาบันการเงินกับผู้ให้บริการภายนอก สถาบันการเงินควรจะต้องพิจารณาอย่างรอบคอบเกี่ยวกับความเสี่ยงในปัจจุบันและความเสี่ยงที่คาดหวังไว้ว่าจะมีผลกระทบต่อการดำเนินธุรกิจด้วย เพื่อใช้ประกอบการกำหนดขอบเขตของการตรวจสอบภายในที่สถาบันการเงินและผู้ให้บริการจากภายนอกจะต้องรับผิดชอบและเพื่อให้เกิดความ

ชัดเจนเกี่ยวกับความรับผิดชอบดังกล่าว สถาบันการเงินควรจัดทำสัญญาเป็นลายลักษณ์อักษร เรียกว่า (Engagement letter) โดยมีรายละเอียดของสัญญาดังต่อไปนี้คือ

- กำหนดหน้าที่ความรับผิดชอบของทั้งสองฝ่าย ทั้งสถาบันการเงินและผู้ให้บริการ

- กำหนดขอบเขต ความถี่ และต้นทุนของงานที่ดำเนินการโดยผู้ให้บริการภายนอก

- กำหนดความรับผิดชอบในการรับส่งข้อมูลข่าวสาร เช่น วิธีการ ความถี่ของการเสนอรายงานต่อผู้บริหารระดับสูงและคณะกรรมการสถาบันการเงิน เกี่ยวกับสถานะของการดำเนินงานตามสัญญา

- กำหนดแนวทางปฏิบัติเมื่อจะทำการเปลี่ยนแปลงเงื่อนไขต่างๆ ของสัญญา เช่น การขยายขอบเขตของงานตรวจสอบในกรณีที่ตรวจพบสิ่งที่เป็นสาระสำคัญ หรือการกระทำผิดสัญญาและการยกเลิกสัญญาการให้บริการ

- ข้อกำหนดเรื่องการเก็บรักษาข้อมูลของสถาบันการเงินเป็นความลับ

- การกำหนดสถานที่จัดเก็บรายงานและกระดาษทำการตรวจสอบภายใน

- กำหนดรอบระยะเวลาที่ผู้ให้บริการจากภายนอกจะต้องเก็บรักษากระดาษทำการเพื่อการตรวจสอบไว้ หรือจะต้องกำหนดสิทธิให้สถาบันการเงินและผู้ตรวจสอบสามารถเข้าถึงกระดาษทำการอิเล็กทรอนิกส์ ถ้าจัดเก็บกระดาษทำการในรูปอิเล็กทรอนิกส์

- ข้อกำหนดว่าผู้ให้บริการตรวจสอบจากภายนอกจะต้องปฏิบัติตามข้อกำหนดของหน่วยงานภาครัฐที่เกี่ยวข้อง และจะต้องยินยอมให้ผู้ตรวจสอบของสถาบันเข้าถึงรายงานผลการตรวจสอบภายในและกระดาษทำการที่ผู้ให้บริการเป็นผู้จัดทำได้ทันทีเมื่อมีความจำเป็น

- กำหนดว่ารายผลการตรวจสอบภายในต่างๆ เป็นสมบัติของสถาบันการเงินและสถาบันการเงินมีสิทธิจะขอสำเนากระดาษทำการที่เกี่ยวข้องถ้าสถาบันการเงินเห็นว่ามีความจำเป็นและพนักงานของสถาบันการเงินที่ได้รับมอบหมายจะต้องสามารถเข้าถึงกระดาษทำการที่ผู้ให้บริการจากภายนอกเป็นผู้ดำเนินการได้ในเวลาที่รวดเร็วและสมเหตุผล

- กำหนดให้มีกระบวนการในการแก้ปัญหา (การใช้คนกลาง-arbitration หรือ การไกล่เกลี่ย-mediation และวิธีการอื่นๆ) และการตัดสินใจว่าใครจะเป็นผู้แบกรับค่าใช้จ่ายอันเป็นผลต่อเนื่องมาจากความเสียหายจากความผิดพลาด การละเลย และการไม่รับรู้

- กำหนดว่าผู้ให้บริการจากภายนอกจะไม่เข้าไปทำหน้าที่แทนฝ่ายจัดการ หรือทำการตัดสินใจแทนฝ่ายจัดการ หรือกระทำหรือแสดงให้ปรากฏต่อผู้อื่นว่าตนเองเป็นพนักงานหรือเป็นฝ่ายจัดการของสถาบันการเงิน นอกจากนี้จะต้องปฏิบัติตามแนวทางและข้อกำหนดทางวิชาชีพ และ

ข้อกำหนดของหน่วยงานภาครัฐได้โดยไม่ก่อเกิดให้เกิดปัญหาเกี่ยวกับผลประโยชน์ที่ทับซ้อนหรือขัดกัน (Conflicts of Interest)

กรรมการหรือผู้บริหารระดับสูงของสถาบันการเงินจะต้องทำให้เกิดความมั่นใจให้ได้ว่าสถาบันการเงินสามารถที่จะบริหารและจัดการเกี่ยวกับการใช้บริการตรวจสอบภายในจากผู้ให้บริการจากบุคคลภายนอกได้อย่างเหมาะสม เช่น สถาบันการเงินขนาดใหญ่ควรที่จะต้องว่าจ้างพนักงานที่มีความสามารถในจำนวนที่มากพอที่จะช่วยดำเนินงานของฝ่ายตรวจสอบภายในและช่วยเหลือผู้จัดการฝ่ายตรวจสอบภายใน เพื่อการกำกับดูแลการดำเนินงานของผู้ให้บริการจากภายนอก แต่สำหรับสถาบันการเงินขนาดเล็กที่ไม่มีผู้จัดการฝ่ายตรวจสอบภายในทำงานแบบเต็มเวลา สถาบันการเงินก็ควรแต่งตั้งพนักงานภายในองค์กรที่มีความเหมาะสมให้ไปกำกับดูแลการดำเนินงานของผู้ให้บริการจากภายนอกให้เป็นไปตามข้อกำหนดของสัญญา อนึ่ง บุคคลดังกล่าวจะต้องไม่มีหน้าที่รับผิดชอบในการบริหารงานใดๆ ที่ผู้ให้บริการจากภายนอกกำลังตรวจสอบอยู่ และมีหน้าที่โดยตรงเฉพาะการรายงานผลการดำเนินงานตรวจสอบและประเด็นปัญหาต่างๆ ที่ได้รับทราบจากการตรวจสอบโดยตรงต่อคณะกรรมการตรวจสอบเท่านั้น

อนึ่ง การที่สถาบันการเงินว่าจ้างผู้ให้บริการจากภายนอกเข้ามาทำหน้าที่รับผิดชอบงานตรวจสอบภายใน จะต้องไม่มีผลกระทบหรือทำให้ระดับของการสื่อสารระหว่างผู้จัดการฝ่ายตรวจสอบภายใน กับคณะกรรมการตรวจสอบ และผู้บริหารระดับสูงลดลงไปจากเดิม นอกจากนี้ ผู้จัดการฝ่ายตรวจสอบภายในจะต้องเข้าไปร่วมกับผู้ให้บริการภายนอกในการกำหนดกรอบโดยรวมของการตรวจสอบ (Risk Universe) และกำหนดแผนการตรวจสอบตามแนวทางความเสี่ยง (Risk-based IT Audit Schedule) และผู้ให้บริการภายนอกจะต้องจัดทำเอกสารประกอบการดำเนินงานทั้งหมดอย่างเหมาะสม และรายงานจุดอ่อนในการควบคุมทั้งหมดที่ตรวจพบต่อผู้บริหารสายงานตรวจสอบโดยเร็ว

ผู้ให้บริการภายนอกควรปฏิบัติงานร่วมกับผู้จัดการฝ่ายตรวจสอบภายในและช่วยกันพิจารณาว่ามีข้อสังเกตที่ตรวจพบจากการตรวจสอบใดบ้างที่มีสาระสำคัญและควรนำเสนอให้คณะกรรมการสถาบันการเงิน และคณะกรรมการตรวจสอบ แต่อย่างไรก็ดี แนวทางการกำหนดความหมายของคำว่ามีสาระสำคัญ (Materiality) ในส่วนที่เกี่ยวข้องกับการจัดทำรายงานทางการเงินนั้น ไม่ได้เป็นสิ่งที่จำเป็นหรือมิใช่ตัวชี้วัดจุดอ่อนของระบบการควบคุมภายในที่ดี เช่น การตรวจสอบอาจจะพบจุดอ่อนที่จะมีผลกระทบต่อชื่อเสียงหรือการปฏิบัติตามกฎหมาย แต่กลับไม่มีผลกระทบโดยตรงต่อการจัดทำรายงานทางการเงิน

2.6.3 การใช้ผลการตรวจสอบภายในจากหน่วยงานภายนอกทดแทนการเข้าไปตรวจสอบการดำเนินงานของผู้ให้บริการภายนอก (Third-Party Service Providers)

ตามปกติ ผู้ให้บริการภายนอก (Third-Party Service Providers) มักจะให้บริการกับสถาบันการเงินต่างๆ ไปพร้อมๆกันจำนวนหลายแห่งในขณะเดียวกัน ดังนั้น ถ้าสถาบันการเงินแต่ละแห่งต่างก็จัดส่งผู้ตรวจสอบภายในของตนเองเข้ามาประเมินความเพียงพอของระบบการควบคุมภายในของผู้ให้บริการจากภายนอกแล้ว ก็จะก่อให้เกิดผลกระทบอย่างมากต่อการบริหารและการดำเนินงานของผู้ให้บริการภายนอกได้

ดังนั้น เพื่อหลีกเลี่ยงปัญหาดังกล่าว ผู้ให้บริการภายนอกควรที่จะไปว่าจ้างผู้ให้บริการด้านการตรวจสอบจากภายนอกรายใดรายหนึ่งเพื่อให้เข้ามาทำการตรวจสอบสถานภาพและความน่าเชื่อถือของระบบการควบคุมภายในเพื่อทดแทนการอนุญาตให้ผู้ตรวจสอบภายในของสถาบันการเงินแต่ละแห่งเข้ามาดำเนินการด้วยตนเอง

อนึ่ง การตรวจสอบโดยผู้ให้บริการตรวจสอบจากภายนอก (Third Party Audit) หมายถึงการตรวจสอบผลการปฏิบัติงานของผู้ให้บริการภายนอก โดยผู้ตรวจสอบอิสระซึ่งไม่ได้เป็นพนักงานของผู้ให้บริการภายนอก หรือของสถาบันการเงิน โดยที่ผู้ที่เกี่ยวข้องทั้งหมด คือ ผู้ให้บริการภายนอก และผู้ตรวจสอบภายในของผู้ให้บริการจากภายนอก รวมทั้งสถาบันการเงินที่ใช้บริการจากผู้ให้บริการจากภายนอกต่างควรที่จะเข้ามาเกี่ยวข้องและมีบทบาทในการกำหนดบทบาทหน้าที่ของผู้ให้บริการตรวจสอบจากภายนอกพร้อมๆ กัน และผู้ตรวจสอบภายในของสถาบันการเงินก็สามารถที่จะนำเอาผลการตรวจสอบโดยผู้ให้บริการตรวจสอบจากภายนอกมาใช้ในการประเมินสถานะภาพและความเพียงพอของระบบการควบคุมภายในของผู้ให้บริการจากภายนอกได้ และผู้ตรวจการสถาบันการเงินก็สามารถนำผลการตรวจสอบดังกล่าวมาใช้ในการกำหนดขอบเขตในการตรวจสอบได้ด้วย

นอกจากนี้ สถาบันการเงินควรจะต้องจัดการบริหารความสัมพันธ์ระหว่างสถาบันการเงินกับผู้ให้บริการจากภายนอกที่สำคัญๆ อย่างมีประสิทธิภาพโดยมีขั้นตอนที่คณะผู้บริหารของสถาบันการเงินควรดำเนินการ ดังต่อไปนี้ คือ:

1. การดำเนินการในการส่งผู้ตรวจสอบเข้าไปตรวจสอบการปฏิบัติงานและการควบคุมของผู้ให้บริการด้านเทคโนโลยีสารสนเทศโดยตรง

2. การว่าจ้างผู้ให้บริการด้านการตรวจสอบจากภายนอกเข้าไปตรวจสอบการปฏิบัติงานและการควบคุมของผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือ

3. การขอรับรายงานและทบทวนข้อมูลที่มีรายละเอียดอย่างเพียงพอจากผู้ให้บริการตรวจสอบที่มีความเป็นอิสระซึ่งได้ให้ความเห็นเกี่ยวกับผู้ให้บริการด้านเทคโนโลยีสารสนเทศไว้

สถาบันการเงินที่ใช้รายงานของผู้ตรวจสอบภายนอกแทนการตรวจสอบเอง จะต้องมั่นใจว่าผู้ตรวจสอบดังกล่าวมีความเป็นอิสระและไม่มีผลประโยชน์ที่ทับซ้อน(Independent Auditor) และมีคุณสมบัติเพียงพอที่จะทำหน้าที่ตรวจสอบ นอกจากนี้ขอบเขตการตรวจสอบดังกล่าวจะต้องครอบคลุมไปถึงวัตถุประสงค์ในการตรวจสอบของสถาบันการเงินด้วย อนึ่ง ถ้าผลการตรวจสอบรายงานว่าได้พบความบกพร่องที่มีนัยสำคัญ ก็จะต้องมีรายละเอียดของความคืบหน้าในการแก้ไขปัญหาดังกล่าวด้วย

ทั้งนี้ สิ่งที่สำคัญอย่างยิ่ง คือ ผู้ตรวจการสถาบันการเงิน และสถาบันการเงินจะต้องเข้าใจขอบเขตของการว่าจ้าง (Engagement) การตรวจสอบ และระดับของความน่าเชื่อถือของผลการตรวจสอบของรายงานผลการตรวจสอบของสำนักงานสอบบัญชี (Accounting firm) ซึ่งเป็นผู้ให้บริการด้านการตรวจสอบจากภายนอกว่าอยู่ในระดับใด อนึ่ง ผู้ใช้รายงานการตรวจสอบไม่ควรจะอิงข้อมูลที่ได้รับในรายงานผลการตรวจสอบเพียงประการเดียวในการตรวจสอบความถูกต้องของระบบการควบคุมภายในของผู้ให้บริการด้านเทคโนโลยีสารสนเทศ แต่ควรที่จะใช้กระบวนการตรวจสอบความถูกต้อง และสามารถติดตามข้อมูลเพิ่มเติมตามรายละเอียดที่ปรากฏในคู่มือการตรวจสอบการให้บริการด้านเทคโนโลยีจากผู้ให้บริการจากภายนอก และประกาศหนังสือเวียนของ ธปท.ที่สนส.29/2551 เรื่อง การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ลงวันที่ 3 สิงหาคม 2551

<u>ส่วนที่ 3</u> แนวทางการตรวจสอบ

3.1 วัตถุประสงค์ของการตรวจสอบ

วัตถุประสงค์ของการตรวจสอบจะช่วยให้ผู้ตรวจการสามารถพิจารณาได้ถึงคุณภาพและประสิทธิผลของการตรวจสอบภายในด้านที่เกี่ยวข้องกับระบบการควบคุมภายในด้าน IT ขององค์กรได้ อนึ่ง กระบวนการในการตรวจสอบเหล่านี้จะแสดงให้ผู้ตรวจการได้รับทราบว่าขอบเขตของการตรวจสอบภายในมีความเหมาะสมเพียงพอหรือไม่ และผู้ตรวจการจะสามารถอาศัยผลการดำเนินงานของผู้ตรวจสอบภายใน มาใช้ประกอบการกำหนดขอบเขตการตรวจสอบด้าน IT ได้เพียงใด

- <u>ขั้นที่ 1</u> วัตถุประสงค์และกระบวนการตรวจสอบเพื่อพิสูจน์ทราบว่าสถาบันการเงินได้นำเอาวิธีการตรวจสอบที่มีประสิทธิภาพมาใช้หรือไม่ และผู้ตรวจการจะสามารถนำเอาผลมาใช้ในการระบุหรือบริหารความเสี่ยงได้หรือไม่

- <u>ขั้นที่ 2</u> วัตถุประสงค์และกระบวนการตรวจสอบในระดับนี้ เป็นไปเพื่อจะช่วยยืนยันว่ากระบวนการตรวจสอบภายในของสถาบันการเงินตามแนวทางความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ อนึ่ง คำถามในชุดนี้จะช่วยตอบสนองโดยตรงเกี่ยวกับการพิจารณาการจัดระดับ URSIT (Uniform Rating System for Information Technology) ตามระดับความเสี่ยงของสถาบันการเงิน ซึ่งผู้ตรวจการสามารถนำเอาผลมาใช้กำหนดขอบเขตการตรวจสอบด้าน IT ในเรื่องต่างๆ ต่อไป

3.2 วัตถุประสงค์และกระบวนการตรวจสอบทั่วไป (Tier 1)

<u>วัตถุประสงค์ที่ 1</u>**: ประเมินขอบเขตและวัตถุประสงค์ในการตรวจสอบทางด้าน IT และประสานงานกับผู้ตรวจการในการทบทวนแผนการตรวจสอบทางด้านทั่วไป** คือ

1. สอบทานรายงานการตรวจสอบครั้งก่อน สำหรับปัญหาที่สำคัญๆปัญหาที่เคยเกิดขึ้นก่อนหน้านี้ หรือประเภทของธุรกิจที่มีความเสี่ยงสูงและยังไม่ได้อยู่ในขอบเขตการตรวจสอบด้าน IT โดยพิจารณาในเรื่องต่อไปนี้

- รายงานการตรวจสอบของหน่วยงานภาครัฐ
- รายงานการตรวจสอบของผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก รวมไปถึงรายละเอียดของการติดต่อสื่อสารและการโต้ตอบกันระหว่างสถาบันการเงินกับผู้ตรวจสอบทั้ง 2 ประเภท
- รายงานผลของหน่วยงานภาครัฐ รายงานการตรวจสอบ รายงานผลการตรวจสอบระบบการรักษาความปลอดภัยของผู้ให้บริการจากภายนอกที่สำคัญๆ ของสถาบันการเงิน

- ข้อมูลผลการตรวจสอบและเอกสารสรุปผลการตรวจสอบชุดที่นำเสนอคณะกรรมการสถาบันการเงิน หรือคณะกรรมการตรวจสอบ

- แผนการตรวจสอบและขอบเขตการตรวจสอบ ของทั้งผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และผู้ให้บริการตรวจสอบจากภายนอก รวมทั้งการประเมินความเสี่ยงในภาพรวมขององค์กร

2. สอบทานผลการตรวจสอบทางด้าน IT ทั้งของผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก ชุดหลังสุดเพื่อพิจารณาเรื่องต่างๆต่อไปนี้

- บทบาทของฝ่ายจัดการในการตรวจสอบด้าน IT

- การเปลี่ยนแปลงกลยุทธ์ของธุรกิจ กิจกรรมทางธุรกิจ หรือเทคโนโลยีซึ่งอาจจะมีผลกระทบกับการตรวจสอบด้าน IT

- การเปลี่ยนแปลงโปรแกรมการตรวจสอบ ขอบเขต กำหนดการ หรือพนักงานที่มีผลกระทบต่อการตรวจสอบภายในและการตรวจสอบภายนอก

- ปัจจัยทั้งภายในและภายนอกที่จะมีผลกระทบต่อการทำงานตรวจสอบ

3. สอบทานผลการตอบชี้แจงของฝ่ายจัดการต่อข้อสังเกตต่างๆ ที่ยกขึ้นสอบถามจากการตรวจสอบครั้งก่อน

- ความเหมาะสมของระยะเวลาและกิจกรรมในการแก้ไขปัญหา/จุดอ่อน

- การแก้ไขปัญหาที่ต้นเหตุมากกว่าการแก้ไขปัญหาเฉพาะเรื่อง

- ข้อบกพร่องสำคัญๆ ที่ยังไม่ได้รับการแก้ไข

4. ประเมินคุณภาพของการตรวจสอบทางด้าน IT โดยพิจารณาจาก

- คุณสมบัติและคุณวุฒิของผู้ตรวจสอบทางด้านทั่วไปและด้าน IT

- นโยบาย ขั้นตอน และวิธีการตรวจสอบ

ผู้ตรวจสอบด้าน IT ควรจะนำผลลัพธ์ที่ได้จากขั้นตอนการตรวจสอบข้างต้นนี้มาประกอบการหารือกับ หัวหน้าผู้ตรวจสอบ (EIC) และเลือกขั้นตอนการตรวจสอบข้างท้ายนี้ที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์ในการตรวจสอบ (ไม่จำเป็นต้องตรวจสอบตามขั้นตอนการตรวจสอบทุกขั้นตอน)

<u>วัตถุประสงค์ที่ 2</u>: ประเมินคุณภาพของการกำกับดูแลและการให้การสนับสนุนในการตรวจสอบด้าน IT ของคณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง

1. สอบทานมติที่ประชุมของคณะกรรมการสถาบันการเงิน (Board Resolutions) และขอบเขต หน้าที่และความรับผิดชอบของการตรวจสอบ (Audit Charter) ที่ผ่านความเห็นชอบจากคณะกรรมการตรวจสอบ เพื่อพิจารณาอำนาจหน้าที่และภารกิจของงานตรวจสอบด้าน IT

2. สอบทานและสรุปมติที่ประชุมของคณะกรรมการสถาบันการเงินและคณะกรรมการตรวจสอบเกี่ยวกับการเข้าร่วมประชุมของสมาชิกในคณะกรรมการตรวจสอบ และกิจกรรมในการกำกับดูแลงานตรวจสอบด้าน IT

3. พิจารณาว่าคณะกรรมการสถาบันการเงินได้ทบทวนและได้ให้ความเห็นชอบเกี่ยวกับนโยบาย ขั้นตอนการตรวจสอบ และวิธีการตรวจสอบทางด้าน IT

4. พิจารณาว่าคณะกรรมการสถาบันการเงินได้อนุมัติแผนการตรวจสอบและกำหนดเวลาการตรวจสอบหรือไม่ นอกจากนี้ คณะกรรมการสถาบันการเงินได้ทบทวนผลการปฏิบัติงานจริงเปรียบเทียบกับแผนหรือไม่ นอกจากนี้ ควรพิจารณาว่าคณะกรรมการสถาบันการเงินได้ให้ความเห็นชอบกับการปฏิบัติงานที่เปลี่ยนแปลงไปจากแผนหรือไม่

5. พิจารณาว่าเนื้อหาและกำหนดเวลาในการนำเสนอรายงานผลการตรวจสอบและข้อสังเกตที่สำคัญที่ถูกเสนอและทบทวนโดยคณะกรรมการสถาบันการเงินและคณะกรรมการตรวจสอบมีความเหมาะสมหรือไม่

6. พิจารณาว่าผู้จัดการฝ่ายตรวจสอบภายในและผู้ตรวจสอบภายนอกได้รายงานผลการตรวจสอบโดยตรงให้คณะกรรมการสถาบันการเงินและคณะกรรมการตรวจสอบ รวมทั้งมีโอกาสรายงานผลเพิ่มเติมทั้งในเวลาปกติและนอกเวลาเพิ่มเติมได้ ถ้ามีเรื่องที่จำเป็นต้องรายงานเพิ่มเติม

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

1. พิจารณาดูว่ากรรมการที่รับผิดชอบในการกำกับดูแลงานตรวจสอบมีความสามารถในการกำกับดูแลงานดังกล่าวอย่างเพียงพอหรือไม่ ผู้ตรวจการสามารถดำเนินการดังต่อไปนี้ คือ

- พิจารณาดูว่ากรรมการที่มีหน้าที่กำกับดูแลงานตรวจสอบมีระดับของความรู้และความชำนาญด้าน IT และความเสี่ยงที่เกี่ยวข้องเป็นอย่างไรบ้าง
- ถ้ากรรมการไม่มีคุณสมบัติเกี่ยวกับการบริหารความเสี่ยงด้าน IT ควรพิจารณาดูว่าได้มีการนำผู้เชี่ยวชาญที่มีความเป็นอิสระจากภายนอกเข้ามากำกับดูแลผ่านทางวิธีการให้ความรู้และการฝึกอบรมหรือไม่

2. พิจารณาดูว่าองค์ประกอบของสมาชิกในคณะกรรมการตรวจสอบมีความเหมาะสมหรือไม่ และสอดคล้องกับการปฏิบัติตามข้อกฎหมายและการกำกับดูแลของหน่วยงานภาครัฐหรือไม่

วัตถุประสงค์ที่ 4**:** พิจารณาคุณสมบัติของผู้ตรวจสอบด้าน IT และแผนการพัฒนาอย่างต่อเนื่อง

1. พิจารณาดูว่ามีจำนวนผู้ตรวจสอบทางด้าน IT ที่เพียงพอ และผู้ตรวจสอบมีความรู้ทางเทคนิคที่จะทำงานได้หรือไม่

- เปรียบเทียบคุณสมบัติของผู้ตรวจสอบด้าน IT กับขอบเขตของงานที่ต้องรับผิดชอบตามตำแหน่งงานนั้นๆ

- ความรู้ศักยภาพของพนักงานสอดคล้องกับเทคโนโลยีที่มีใช้ในองค์กรหรือไม่

- พิจารณาดูว่าแนวโน้มของการจัดหาพนักงาน IT มีปัจจัยอะไรที่แสดงให้เห็นแนวโน้มด้านลบหรือไม่

วัตถุประสงค์ที่ 5 : พิจารณาระดับของความเป็นอิสระในการตรวจสอบ ดังนี้

1. พิจารณาดูว่ากระบวนการจัดทำรายงานผลการตรวจสอบด้าน IT มีความเป็นอิสระทั้งจากข้อเท็จจริงหรือจากภาพที่ปรากฏหรือไม่ โดยการสังเกตดูจากระดับของการควบคุมของบุคคลภายนอกที่จะมีผลกระทบต่อการจัดทำรายงานเสนอคณะกรรมการสถาบันการเงิน หรือคณะกรรมการตรวจสอบ

2. ทบทวนโครงสร้างของสายงานตรวจสอบภายในถึงความเป็นอิสระและความชัดเจนในกระบวนการจัดทำรายงานผลการตรวจสอบ ในแง่ความเป็นอิสระในการตรวจสอบและกระบวนการรายงานโดยพิจารณาว่าความเป็นอิสระสูญเสียไปหรือไม่ ดังนี้

- ผู้จัดการฝ่ายตรวจสอบภายในต้องรายงานผลการตรวจสอบให้ผู้บริหารระดับสูงในตำแหน่งดังต่อไปนี้ คือ ผู้จัดการฝ่ายการเงินหรือผู้ควบคุมแผนกบัญชี หรือผู้รับผิดชอบอื่นที่คล้ายกัน

- การพิจารณาเงินเดือนและการประเมินผลการปฏิบัติงานของผู้จัดการฝ่ายตรวจสอบภายในไม่ได้ขึ้นตรงต่อคณะกรรมการสถาบันการเงินหรือคณะกรรมการตรวจสอบแต่ขึ้นอยู่กับบุคคลอื่น

- ผู้ตรวจสอบต้องรับผิดชอบต่อระบบการควบคุมภายในหรือรับผิดชอบในการปฏิบัติการประจำวันด้านใดด้านหนึ่ง

หมายเหตุ ผู้บริหารด้านการตรวจสอบภายในควรรายงานข้อสังเกตให้คณะกรรมการตรวจสอบโดยตรงและควรที่จะรายงานเรื่องที่เกี่ยวข้องกับประเด็นเรื่องการบริหารการจัดการให้กับผู้บริหารระดับสูงได้รับทราบไปพร้อมๆกัน

วัตถุประสงค์ที่ 6**:** พิจารณาระยะเวลา รูปแบบในการติดตามผล และการรายงานผลการปรับปรุงแก้ไขจุดอ่อนหรือปัญหาด้าน IT ที่เป็นอยู่

1. พิจารณาว่าฝ่ายจัดการได้มีปฏิกิริยาตอบสนอง ต่อข้อสังเกตอย่างเหมาะสมและกระทำภายในระยะเวลาที่เหมาะสมหรือไม่ นอกจากนี้สายงานตรวจสอบหรือฝ่ายจัดการได้จัดทำรายงานเสนอคณะกรรมการสถาบันการเงินและคณะกรรมการตรวจสอบถึงสิ่งที่ได้ดำเนินการไปแล้วหรือไม่ และในที่สุดฝ่ายตรวจสอบได้ทำการทบทวนและตรวจสอบสิ่งที่ฝ่ายจัดการได้ชี้แจงเกี่ยวกับการแก้ไขปัญหาตามข้อสังเกตของฝ่ายตรวจสอบหรือไม่

2. เปรียบเทียบรายงานผลการตรวจสอบทั้งหมดที่มีอยู่กับทะเบียนคุมงานตรวจสอบทั้งหมดที่มีอยู่เพื่อให้ทราบว่าได้ดำเนินการครบถ้วนหรือไม่

3. พิจารณาว่าฝ่ายจัดการได้แก้ไขปัญหาที่ต้นเหตุของปัญหาหรือไม่ และถ้าเห็นว่ายังไม่ตรงประเด็น ให้พิจารณาเพิ่มเติมว่าทำไมมาตรการแก้ไขเหล่านั้น จึงยังไม่เพียงพอ

วัตถุประสงค์ที่ 7: พิจารณาความพอเพียงของแผนการตรวจสอบโดยรวมว่ามีความเหมาะสมและครอบคลุมถึงความเสี่ยงทางด้าน IT ทั้งหมดหรือไม่

1. สัมภาษณ์ฝ่ายจัดการและทบทวนข้อมูลจากการตรวจสอบเพื่อที่จะค้นหาความเปลี่ยนแปลงต่างๆที่มีผลกระทบต่อความเสี่ยงโดยรวมของสถาบันการเงินซึ่งจะมีผลกระทบโดยตรงต่อขอบเขตของการตรวจสอบโดยการพิจารณาดังต่อไปนี้

- กระบวนการประเมินความเสี่ยงของสถาบันการเงิน
- ผลิตภัณฑ์และบริการที่ให้บริการแก่ผู้ใช้งานทั้งภายในและภายนอกองค์กร
- การเพิ่มหรือลดของบุคลากรที่มีผลกระทบที่สำคัญ
- ข้อมูลและรายชื่อทั้งหมดของผู้ให้บริการด้านเทคโนโลยี หรือตัวแทนจำหน่ายซอฟท์แวร์

2. สอบทานคู่มือตรวจสอบด้าน IT หรือเนื้อหาในส่วนที่เกี่ยวข้องกับIT ในคู่มือตรวจสอบทั่วไป นอกจากนี้ควรประเมินความพียงพอของนโยบาย แนวทางการปฏิบัติ และขั้นตอนการทำงานที่เกี่ยวข้องกับรูปแบบและเนื้อหาของรายงานประเภทต่างๆ วิธีในการแจกจ่ายรายงาน แนวทางการแก้ไขปัญหาตามข้อสังเกต รูปแบบและเนื้อหาของกระดาษทำการ และการรักษาความปลอดภัยของข้อมูลการตรวจสอบ

วัตถุประสงค์ที่ 8: พิจารณาความเหมาะสมของวิธีการในการประเมินความเสี่ยงและการจัดสรรทรัพยากรในการตรวจสอบและการจัดทำตารางกำหนดเวลาตรวจสอบด้าน IT

1. ประเมินปัจจัยสำคัญที่มีผลกระทบต่อการวางแผนและการจัดกำหนดเวลาต่างๆ รวมไปถึงการวิเคราะห์ความเสี่ยง การคัดเลือก และการกำหนดขอบเขตในการตรวจสอบ และความถี่ในการตรวจสอบ เพื่อพิจารณาว่า

- การกำหนดกรอบรวมในการตรวจสอบทั้งหมด (Audit Universe) ได้ทำไว้ดีเพียงใด

- แผนการตรวจสอบและรอบระยะเวลาในการตรวจสอบสนับสนุนกรอบรวมในการตรวจสอบทั้งหมด อย่างสมเหตุผลและสามารถปฏิบัติได้จริง

2. พิจารณาว่าสถาบันการเงินมีมาตรฐานและกระบวนการตรวจสอบตามแนวทางความเสี่ยงและวิธีการประเมินความเสี่ยงภายในสถาบันการเงินอย่างเหมาะสม

- มีการจัดทำแฟ้มรวมเรื่องความเสี่ยง (risk profile) ที่ระบุและให้นิยามเกี่ยวกับความเสี่ยงและปัจจัยที่ใช้ในการประเมินและการบริหารความเสี่ยงและโครงสร้างของระบบควบคุมสำหรับผลิตภัณฑ์ บริการ และ ภาระหน้าที่ในการดำเนินงานด้าน IT

- มีการอธิบายวิธีการประเมินและการจัดทำเอกสารเกี่ยวกับความเสี่ยงและปัจจัยที่ใช้ในการควบคุมและการนำข้อมูลดังกล่าวไปใช้ในการจัดทำแผนการตรวจสอบ การจัดสรรทรัพยากร การกำหนดขอบเขตการตรวจสอบ และรอบความถี่ในการตรวจสอบ

<u>วัตถุประสงค์ที่ 9:</u> พิจารณาความเหมาะสมของขอบเขต ความถี่ ความถูกต้อง และความรวดเร็วในการจัดทำรายงานผลการตรวจสอบด้าน IT

1. สอบทานตัวอย่างของรายงานผลการตรวจสอบด้าน IT และกระดาษทำการเพื่อหาว่ามีการจัดระดับผลการตรวจสอบ ความสมบูรณ์ครบถ้วน และมีความสอดคล้องกับมาตรฐานการตรวจสอบที่คณะกรรมการสถาบันการเงินและคณะกรรมการตรวจสอบกำหนดไว้หรือไม่

2. วิเคราะห์และเปรียบเทียบผลการประเมินความเพียงพอของระบบการควบคุมภายในด้าน IT ซึ่งผู้ตรวจสอบภายในเป็นผู้ดำเนินการเปรียบเทียบกับผลการประเมินโดยผู้ตรวจการ

3. ประเมินขอบเขตการทำงานของผู้ตรวจสอบภายในว่าสัมพันธ์กับ ขนาดของสถาบันการเงิน ลักษณะเฉพาะและกิจกรรมทางธุรกิจ และภาพรวมของความเสี่ยงของสถาบันการเงินหรือไม่

4. พิจารณาว่ากระดาษทำการได้เปิดเผยให้เห็นขั้นตอนในการตรวจสอบ การคำนวณ หรือหลักฐานอื่นที่สนับสนุนขั้นตอนการดำเนินงานหรือข้อสรุปที่กำหนดไว้ในรายงานหรือไม่

5. พิจารณาจากรายงานการตรวจสอบ และกระดาษทำการว่าผู้ตรวจสอบ สามารถระบุความเสี่ยงได้อย่างถูกต้อง และได้รายงานให้เห็นถึงจุดอ่อนและความเสี่ยงอย่างสม่ำเสมอ

6. พิจารณาว่ารายงานผลการตรวจสอบมีองค์ประกอบดังนี้หรือไม่

- รวดเร็วและเป็นปัจจุบัน
- มีลักษณะสร้างสรรค์
- มีความถูกต้อง
- มีความครบถ้วน

วัตถุประสงค์ที่ 10: พิจารณาขอบเขตของการเข้าไปมีส่วนร่วมในการพัฒนาและการจัดหาระบบงานและโปรแกรม ของฝ่ายตรวจสอบเพื่อให้เกิดความมั่นใจว่าสถาบันการเงินจะมีระบบควบคุมภายในที่มีประสิทธิภาพ

1. หารือกับผู้บริหารงานตรวจสอบเพื่อทบทวนแนวนโยบายการตรวจสอบในส่วนที่เกี่ยวข้องกับการเข้าไปมีส่วนร่วมในการพัฒนาและการจัดหาระบบงานและโปรแกรม และการทดสอบระบบของฝ่ายตรวจสอบ

2. สอบทานกระบวนการที่ฝ่ายจัดการนำมาใช้เพื่อแจ้งให้ผู้ตรวจสอบด้าน IT ถึงการจัดหาโปรแกรมระบบงานใหม่ การเปลี่ยนแปลงโปรแกรมระบบงานเดิม การปรับปรุงหรือเพิ่มเติมระบบปฏิบัติการ (Operating System) หรือการเปลี่ยนแปลงสภาพแวดล้อมอื่นๆในการประมวลผลข้อมูล

3. พิจารณาความเหมาะสมและความเป็นอิสระของผู้ตรวจสอบ ดังนี้

- การมีส่วนร่วมในทุกขั้นตอนของการพัฒนาระบบงานและโปรแกรม
- การทบทวนการเปลี่ยนแปลงที่สำคัญๆของโปรแกรมระบบงานและระบบปฏิบัติการ
- ปรับปรุงขั้นตอนการตรวจสอบ โปรแกรมระบบงาน และเอกสารระบบงานสำหรับการเปลี่ยนแปลงของระบบงานและสภาพแวดล้อม
- การให้คำแนะนำให้มีการเปลี่ยนแปลงระบบงานใหม่หรือระบบงานเดิมที่มีอยู่ในส่วนที่เกี่ยวข้องกับการตรวจสอบและการควบคุม

วัตถุประสงค์ที่ 11**:** ในกรณีที่สถาบันการเงินได้ใช้บริการตรวจสอบภายในด้าน IT ทั้งหมดหรือบางส่วนจากผู้ให้บริการตรวจสอบจากภายนอก (IT outsourced) ผู้ตรวจการควรประเมินประสิทธิภาพว่าสถาบันการเงินสามารถที่จะเชื่อถือบริการดังกล่าวได้หรือไม่

1. การขอสำนาเอกสารเกี่ยวกับ

- สัญญาการจ้างบุคคลภายนอกและเอกสารกำหนดรายละเอียดของการใช้บริการและการประเมินผลต่างๆ
- รายงานผลการตรวจสอบภายในโดยผู้ให้บริการภายนอก

- นโยบายที่ใช้ในการตรวจสอบ

2. สอบทานสัญญาว่าจ้างผู้ให้บริการภายนอกและนโยบายต่างๆ เพื่อพิจารณาถึงความเพียงพอของสัญญาว่าจ้างดังกล่าว

- การกำหนดความต้องการและความรับผิดชอบของสถาบันการเงินและผู้ให้บริการจากภายนอก

- การกำหนดขอบเขต ความถี่ และค่าใช้จ่ายในการดำเนินงานที่ผู้ให้บริการจากภายนอกต้องดำเนินการแทนสถาบันการเงิน

- การกำหนดความรับผิดชอบในการให้และการได้รับข้อมูล เช่น รูปแบบและความถี่ในการจัดส่งรายงานเสนอผู้บริหารระดับสูงและกรรมการสถาบันการเงินเกี่ยวกับสถานะภาพของการทำงานจากผู้ให้บริการจากภายนอก

- การกำหนดข้อตกลงเกี่ยวกับการเปลี่ยนแปลงเงื่อนไขในการให้บริการโดยเฉพาะเมื่อมีการขยายขอบเขตของการตรวจสอบ เนื่องจากการตรวจพบประเด็นที่สำคัญและเงื่อนไขที่กำหนดเกี่ยวกับการทำงานผิดพลาดและการบอกเลิกสัญญา

- การกำหนดให้รายงานการตรวจสอบภายในของสถาบันการเงินเป็นทรัพย์สินของสถาบันการเงิน และสถาบันการเงินจะต้องได้รับสำเนาของกระดาษทำการเท่าที่เห็นว่าจำเป็น รวมทั้งพนักงานที่ได้รับมอบหมายจากสถาบันการเงินต้องสามารถเข้าถึงกระดาษทำการของผู้ให้บริการภายนอกได้ในระยะเวลาที่รวดเร็วสมเหตุผล

- การกำหนดว่าข้อมูลใดๆที่เป็นของสถาบันการเงินจะต้องถูกเก็บรักษาเป็นความลับ

- การกำหนดสถานที่จัดเก็บรายงานผลการตรวจสอบภายในและกระดาษทำการ

- ระบุระยะเวลาที่ผู้ให้บริการภายนอกจะต้องเก็บรักษากระดาษทำการและในกรณีที่กระดาษทำการถูกจัดเก็บอยู่ในรูปแบบอิเล็กทรอนิกส์ ผู้ให้บริการจากภายนอกจะต้องดำเนินการให้สถาบันการเงินและผู้ตรวจการได้รับสิทธิในการเข้าถึงกระดาษทำการอิเล็กทรอนิกส์ได้ในระหว่างช่วงระยะเวลาที่กำหนดไว้

- การกำหนดว่าผู้ให้บริการตรวจสอบจากภายนอกจะต้องยินยอมให้หน่วยงานภาครัฐและผู้ตรวจการมีสิทธิในการเข้าถึงรายงานผลการ ตรวจสอบภายใน กระดาษทำการ และเอกสารสำคัญอื่นๆ ที่ผู้ให้บริการจากภายนอกได้จัดทำขึ้นเพิ่มเติม

- การกำหนดกระบวนการในการแก้ไขปัญหา (โดยการใช้คนกลาง หรือวิธีการอื่นใด) โดยพิจารณาว่าใครจะต้องเป็นผู้รับผิดชอบต้นทุนของความเสียหายที่เกิดจากความผิดพลาดและการไม่ได้ปฏิบัติหน้าที่ และการละเลย

- การกำหนดไม่ให้ผู้ให้บริการภายนอกไปทำหน้าที่แทนฝ่ายจัดการ หรือกระทำให้รู้สึกได้ว่าเป็นผู้ทำหน้าที่แทนฝ่ายจัดการหรือพนักงานของสถาบันการเงิน แต่ควรกำหนดให้ผู้ให้บริการจากภายนอกให้ปฏิบัติตามแนวทางการปฏิบัติงานตามสายวิชาชีพ หรือแนวทางในการปฏิบัติงานอย่างเป็นอิสระซึ่งกำหนดโดยหน่วยงานภาครัฐ

3. พิจารณาจัดการประชุมร่วมกับผู้ตรวจสอบด้าน IT จากภายนอกเพื่อหารือเกี่ยวกับโปรแกรมการตรวจสอบและพิจารณาคุณสมบัติของผู้ตรวจสอบจากภายนอก

4. ควรพิจารณาว่าการใช้บริการจากผู้ให้บริการภายนอกสามารถดำรงรักษา หรือพัฒนาคุณภาพของการตรวจสอบภายในและระบบการควบคุมภายในหรือไม่ ผู้ตรวจสอบควรจะดำเนินการ ดังนี้ คือ

- ทบทวนผลการปฏิบัติงานและการปฏิบัติตามเงื่อนไขของสัญญา และวิธีการประเมินผลการดำเนินงานของผู้ให้บริการจากภายนอกแบบอื่นๆ ที่สถาบันการเงินกำหนดขึ้นภายใน

- ทบทวนรายงานผลการตรวจสอบและตัวอย่างกระดาษทำการ ของผู้ให้บริการตรวจสอบจากภายนอกว่ามีความเหมาะสมเพียงพอตามข้อกำหนดของสัญญาว่าจ้างหรือไม่

- พิจารณาว่ากระดาษทำการได้แสดงให้เห็นถึงรายละเอียดของขั้นตอนการทำงาน การคำนวณ หรือมีเอกสารสนับสนุนอื่นใดเกี่ยวกับขั้นตอนของการตรวจสอบและข้อสรุปที่จะปรากฏในรายงานผลการตรวจสอบหรือไม่

- พิจารณาขั้นตอนในการกำหนดขอบเขตของงานที่จะใช้บริการจากผู้ให้บริการจากภายนอกว่ามีความเหมาะสมหรือไม่

5. พิจารณาว่าพนักงานที่รับหน้าที่หลักของสถาบันการเงินและผู้ให้บริการจากภายนอกมีความเข้าใจที่ตรงกันเกี่ยวกับช่องทางการติดต่อสื่อสารระหว่างผู้รับผิดชอบหลักของสถาบันการเงินและผู้ให้บริการตรวจสอบจากภายนอกและรับทราบวิธีจัดการกับปัญหาของระบบการควบคุมภายในเมื่อผู้ให้บริการจากภายนอกตรวจสอบพบปัญหาดังกล่าวขึ้นมา

6. พิจารณาว่าฝ่ายจัดการและผู้ให้บริการตรวจสอบจากภายนอกได้ทบทวนขอบเขตของการตรวจสอบภายในอย่างเหมาะสมกับสภาวะแวดล้อม กิจกรรม ความเสี่ยง หรือการเปลี่ยนแปลงระบบปฏิบัติงานที่มีความสำคัญ หรือไม่

7. พิจารณาว่าคณะกรรมการสถาบันการเงินสามารถให้ความมั่นใจได้ว่าสถาบันการเงินสามารถบริหารงานตรวจสอบที่ใช้บริการจากผู้ให้บริการจากภายนอกได้อย่างมีประสิทธิภาพ

8. พิจารณาว่าคณะกรรมการสถาบันการเงินได้ทำการศึกษาอย่างละเอียดแล้วว่าผู้ให้บริการตรวจสอบจากภายนอกมีความสามารถในการให้บริการและจะช่วยให้สถาบันการเงินบรรลุวัตถุประสงค์ในการตรวจสอบความเสี่ยงภายในองค์กรได้ตามเป้าหมายก่อนการทำสัญญาจ้างงาน

9. พิจารณาว่าผู้ให้บริการตรวจสอบภายในที่สถาบันการเงินว่าจ้างมาได้ทำหน้าที่เป็นผู้ตรวจสอบภายนอกหรือเป็นที่ปรึกษาให้กับสถาบันการเงินในด้านอื่นๆ ไปพร้อมๆกับการทำหน้าที่เป็นผู้ตรวจสอบภายในหรือไม่ ผู้ตรวจการจะต้องตรวจสอบดูว่าสถาบันการเงินและผู้ให้บริการได้ร่วมกันปรึกษาหารือ ตัดสินใจ และจัดทำเอกสารให้สอดคล้องกับข้อกำหนดมาตรฐานของหน่วยงานภาครัฐในเรื่องความเป็นอิสระและไม่มีผลประโยชน์ทับซ้อนเรียบร้อยแล้ว

10. พิจารณาว่าสถาบันการเงินได้จัดเตรียมแผนรองรับอย่างเพียงพอหรือไม่เพื่อลดผลกระทบจากการที่ต้องเลิกว่าจ้างผู้ให้บริการตรวจสอบจากภายนอกอย่างกะทันหันในขณะที่ผู้ให้บริการจากภายนอกยังไม่ได้ตรวจสอบเรื่องหรือแผนกที่มีความเสี่ยงระดับสูงเลย

วัตถุประสงค์ที่ 12: **พิจารณาขอบเขตของการตรวจสอบภายนอกในส่วนที่เกี่ยวข้องกับการควบคุมด้าน IT**

1. สอบทานจากหนังสือสัญญาจ้างและสัมภาษณ์ผู้บริหารระดับสูงของสถาบันการเงินว่าผู้ตรวจสอบภายนอกได้เข้ามามีส่วนเกี่ยวข้องกับกระบวนการประเมินระบบควบคุมด้าน IT หรือไม่

2. ถ้าผู้ตรวจการจะอาศัยผลการตรวจสอบของผู้ตรวจสอบจากภายนอกมาใช้ในการจำกัดขอบเขตการตรวจสอบแล้ว ผู้ตรวจการควรที่จะสร้างความมั่นใจโดยการหารือและตรวจสอบกระดาษทำการของผู้ตรวจสอบภายนอกก่อน

วัตถุประสงค์ที่ 13: **พิจารณาว่าฝ่ายจัดการได้กำกับดูแล และเฝ้าระมัดระวังดูแลการประมวลผลที่มีความสำคัญซึ่งดำเนินการโดยผู้ให้บริการด้านเทคโนโลยีสารสนเทศจากภายนอกหรือไม่**

1. พิจารณาว่าฝ่ายจัดการได้ตรวจสอบการปฏิบัติงานและระบบการควบคุมของผู้ให้บริการจากภายนอกโดยตรง หรือว่าจ้างผู้ตรวจสอบภายนอกในการประเมินระบบการควบคุมภายในของผู้ให้บริการจากภายนอก หรือได้รับสำเนาผลการตรวจสอบที่มีข้อมูลอย่างเพียงพอจากผู้ให้บริการจากภายนอกเอง

2. พิจารณาว่าฝ่ายจัดการได้ขอรายงานผลการตรวจสอบด้าน IT จากหน่วยงานที่ทำหน้าที่กำกับดูแลที่เกี่ยวข้องหรือไม่

3. พิจารณาว่าฝ่ายจัดการได้สอบทานรายงานทั้งหมดอย่างเพียงพอเพื่อให้เกิดความมั่นใจว่าได้มีการกำหนดขอบเขตการตรวจสอบไว้อย่างเพียงพอ และได้มีการเตรียมการแก้ไขปัญหาสำหรับจุดอ่อนต่างๆ ได้อย่างเหมาะสม

สรุปผลการตรวจสอบ

<u>วัตถุประสงค์ที่ 14 :</u> การหาหรือเกี่ยวกับข้อเท็จจริงที่พบจากการตรวจสอบและแนวทางในการแก้ไขปัญหาเหล่านั้น

1. พิจารณาว่าจำเป็นต้องทำการตรวจสอบตามกระบวนการตรวจสอบเชิงลึก (Tier 2) เพิ่มเติมเพื่อช่วยยืนยันความถูกต้องและสนับสนุนข้อสรุปที่ได้จากกระบวนการตรวจสอบแบบทั่วไป (Tier 1)

2. ควรใช้ผลการตรวจสอบตามวัตถุประสงค์ในการตรวจสอบข้างต้น ร่วมกับผลการจัดระดับจากการตรวจสอบภายใน หรือขอบเขตของการตรวจสอบมาประกอบการพิจารณาว่ายังมีความจำเป็นที่จะต้องยืนยันความถูกต้องสำหรับเรื่องที่ตรวจสอบเป็นการเฉพาะหรือไม่

- ควรส่งรายงานผลการตรวจสอบให้กับผู้ตรวจสอบที่ทำงานเกี่ยวข้องกับเรื่องที่กำลังตรวจสอบจะไปตรวจสอบ

- แนะนำให้ผู้ตรวจสอบหรือสถาบันการเงินทำการยืนยันความถูกต้องตามขั้นตอนการตรวจสอบเชิงลึกเพิ่มเติมทุกครั้งที่สามารถทำได้

3. การใช้ผลจากการสอบทานหน้าที่การตรวจสอบ IT รวมถึงกระบวนการตรวจสอบเชิงลึก (Tier 2) ที่จำเป็น

- จัดทำข้อสรุปเป็นลายลักษณ์อักษรเกี่ยวกับคุณภาพและประสิทธิภาพของการตรวจสอบที่เกี่ยวข้องกับระบบควบคุมภายในด้าน IT

- พิจารณาและจัดทำข้อสรุปเป็นลายลักษณ์อักษรว่าผู้ตรวจการจะอาศัยผลการตรวจสอบของผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกมาใช้ในการกำหนดขอบเขตการตรวจสอบด้าน IT หรือไม่ และมากน้อยเพียงใด

4. ควรทบทวนข้อสรุปเกี่ยวกับผลการตรวจสอบชั้นต้นกับหัวหน้าผู้ตรวจการที่ควบคุมการตรวจสอบ (EIC) ในเรื่องต่างๆ ดังต่อไปนี้

- การปฏิบัติที่ไม่ชอบด้วยกฎหมาย กฎเกณฑ์ และข้อกำหนดของหน่วยงานภาครัฐ

- ประเด็นที่ตรวจสอบพบว่ามีนัยสำคัญที่จะต้องแจ้งให้คณะกรรมการสถาบันการเงินได้รับทราบ หรือจะต้องมีการเขียนเป็นข้อสังเกตในรายงานผลการตรวจสอบ

- ผลกระทบ (ที่อาจจะเกิดขึ้น) จากข้อสังเกตที่จะมีต่อผลการจัดระดับของสถาบันการเงินตามลำดับของความเสี่ยงและการควบคุมภายในทั้งในระดับของภาพรวม และในระดับย่อย (URSIT)

5. หารือกับฝ่ายจัดการเกี่ยวกับข้อสังเกตและกำหนดเวลาในการแก้ไขระบบการควบคุมภายในที่สำคัญๆ ที่ตรวจพบว่าไม่มีประสิทธิภาพ

6. จัดทำข้อสรุปเป็นลายลักษณ์อักษรซึ่งประกอบไปด้วยผลการจัดอันดับต่อผู้บริหารทีม และข้อสังเกตที่จัดเตรียมในรูปแบบของรายงานผลการตรวจสอบชุดที่พร้อมนำเสนอผู้ที่เกี่ยวข้องได้เลย

7. ควรจัดทำข้อสรุปเป็นลายลักษณ์อักษรเกี่ยวกับแนวทางในการตรวจสอบด้าน IT ในรอบหน้า

8. ควรจัดเรียงลำดับของกระดาษทำการในการตรวจสอบเพื่อใช้ในการสนับสนุนข้อสังเกต และผลสรุปที่สำคัญ

3.3 วัตถุประสงค์และกระบวนการตรวจสอบเชิงลึก (Tier 2)

กระบวนการตรวจสอบเชิงลึก (Tier 2) เป็นการตรวจสอบด้าน IT เพิ่มเติมเพื่อช่วยในการพิสูจน์และประเมินประสิทธิภาพของงานตรวจสอบด้าน IT อนึ่ง กระบวนการตรวจสอบชุดนี้ได้ถูกออกแบบมาเพื่อช่วยให้ผู้ตรวจการบรรลุทั้งวัตถุประสงค์ในการตรวจสอบและกรอบของขอบเขตการตรวจสอบที่กำหนดไว้ ทั้งนี้ ผู้ตรวจการสามารถที่จะเลือกใช้กระบวนการตรวจสอบทั้งหมดหรือบางส่วนก็ได้

อนึ่ง การตั้งคำถามในกระบวนการตรวจสอบเชิงลึกนี้จะสอดคล้องกับ URSIT ซึ่งผู้ตรวจการสามารถจะนำผลการตรวจสอบมาใช้ประกอบการตัดสินใจในการกำหนดขอบเขตการตรวจสอบด้าน IT ได้ เพราะฉะนั้น ผู้ตรวจการด้าน IT จึงควรประสานงานกับผู้ตรวจการด้านอื่นๆ เกี่ยวกับขอบเขตของการตรวจสอบที่ได้รับมอบหมาย เพื่อหลีกเลี่ยงการทำงานที่ซ้ำซ้อนกันในเรื่องเดียวกัน (สามารถศึกษาได้จากคู่มือตรวจสอบด้าน IT เล่มอื่นๆ)

ก. การจัดการ (Management)

1.พิจารณาว่ากระบวนการตรวจสอบด้านการจัดการได้มีการพิจารณาอย่างเหมาะสมแล้ว โดยพิจารณา ดังนี้ คือ

- ฝ่ายจัดการมีความสามารถในการวางแผนและการริเริ่มกิจกรรมหรือผลิตภัณฑ์เพื่อตอบสนองต่อความต้องการข้อมูลสารสนเทศและได้เตรียมความพร้อมไว้แล้วสำหรับความเสี่ยงที่เกิดจากการเปลี่ยนแปลงเงื่อนไขทางธุรกิจ

- ฝ่ายจัดการมีความสามารถในการนำเสนอรายงานต่างๆที่มีความจำเป็นต่อการจัดทำแผนงานและการตัดสินใจทางธุรกิจอย่างมีประสิทธิภาพและประสิทธิผล

- ความเพียงพอและสอดคล้องกันของนโยบายและระบบการควบคุมภายในที่สามารถรองรับกับการดำเนินงานด้าน IT และความเสี่ยงต่างๆที่เกิดขึ้นจากการดำเนินกิจกรรมทางธุรกิจที่มีความสำคัญ

- ประสิทธิภาพของระบบงานต่างๆในการควบคุมดูแลความเสี่ยง

- ระดับของการตระหนักรู้และการยอมรับในการปฏิบัติงานตามกฎหมายและข้อกำหนดของหน่วยงานภาครัฐ

- ระดับของการวางแผนเพื่อจัดเตรียมพนักงานที่จะเลื่อนตำแหน่งขึ้นมาทดแทนฝ่ายจัดการ

- ความสามารถของฝ่ายจัดการในการเฝ้าติดตามดูแลการส่งมอบบริการให้กับลูกค้าและการวัดผลความก้าวหน้าของสถาบันการเงินในการมุ่งไปสู่เป้าหมายทางธุรกิจที่กำหนดไว้อย่างมีประสิทธิภาพและประสิทธิผล

- ความเหมาะสมเพียงพอของสัญญาและความสามารถของฝ่ายจัดการในการเฝ้าติดตามดูแลความสัมพันธ์ระหว่างสถาบันการเงินและผู้ให้บริการด้านเทคโนโลยีสารสนเทศจากภายนอกองค์กรทุกแห่ง

- ความเหมาะสมเพียงพอของแผนกลยุทธ์ และแนวทางปฏิบัติในการระบุประเภท การวัดระดับ การเฝ้าติดตามดูแล และการควบคุมความเสี่ยงต่างๆ รวมไปถึงความสามารถของฝ่ายจัดการในการประเมินผลการปฏิบัติงานของตนเอง

- ความสามารถของฝ่ายจัดการในการระบุประเภท การวัดระดับ การเฝ้าติดตามดูแล และการควบคุมความเสี่ยงต่างๆ รวมไปถึงการเตรียมพร้อมรับเทคโนโลยี และแนวทางใหม่ๆ สำหรับควบคุมดูแลพัฒนาการด้าน IT ที่จำเป็น

ข. การพัฒนาและการจัดหาระบบงานและโปรแกรม

1.พิจารณาว่ากระบวนการตรวจสอบเกี่ยวกับการพัฒนาและการจัดหาระบบงานและโปรแกรมระบบงาน และ การบริหารความเสี่ยงมีความเหมาะสมเพียงพอหรือไม่ โดยพิจารณาดังนี้ คือ

- ระดับของการกำกับดูแลคุณภาพ และการสนับสนุนของผู้บริหารระดับสูงและคณะกรรมการสถาบันการเงินเกี่ยวกับการพัฒนาและการจัดหาระบบงานและโปรแกรม

- ความเหมาะสมของโครงสร้างของสถาบันการเงินและฝ่ายจัดการในการมอบหมายผู้รับผิดชอบและดูแลให้ระบบงาน IT และเทคโนโลยีใหม่ๆมีความน่าเชื่อถือได้

- จำนวน ลักษณะ และขอบเขตของความเสี่ยงที่เกี่ยวข้องกับการพัฒนาและการจัดหาระบบงานและโปรแกรมของสถาบันการเงิน

- มีมาตรฐานของกระบวนการในการพัฒนาและการจัดหาระบบงานและโปรแกรม และมาตรฐานในการเขียนโปรแกรมอย่างเหมาะสมเพียงพอ

- คุณภาพของโปรแกรมการบริหารโครงการและการปฏิบัติงานซึ่งได้รับการยอมรับและปฏิบัติตามโดยผู้พัฒนาระบบงาน พนักงานปฏิบัติงานด้านคอมพิวเตอร์ ผู้บริหารและเจ้าของ ผู้ให้บริการจากภายนอก บริษัทในเครือ และผู้ใช้งาน

- ความเป็นอิสระของหน่วยงานที่รับประกันคุณภาพและความเพียงพอของระบบควบคุมภายในเมื่อมีการเปลี่ยนแปลงต่างๆ เช่น การตรวจสอบว่ามีการเปลี่ยนแปลงของ Source Code และ Object Code หรือไม่ มีการทบทวนการเปลี่ยนแปลงโปรแกรมอย่างอิสระ มีการทบทวนผลการทดสอบอย่างละเอียด ได้รับการอนุมัติจากฝ่ายจัดการก่อนการย้ายโปรแกรมเข้า Production มีการปรับปรุงเอกสารให้ถูกต้องเป็นปัจจุบันอย่างรวดเร็ว

- มีเอกสารประกอบระบบงานที่มีคุณภาพและครบถ้วน

- มีความถูกต้องเชื่อถือได้และมีระบบการรักษาความปลอดภัยสำหรับเครือข่าย ระบบงาน และโปรแกรมระบบงานในขั้นตอนของการพัฒนาระบบงานและโปรแกรม

- มีการพัฒนาระบบงานด้าน IT ที่ตรงตามความต้องการของผู้ใช้งาน

- ระดับของการเข้าไปมีส่วนร่วมของผู้ใช้งานต้องอยู่ในขั้นตอนของการพัฒนาระบบงานและโปรแกรม

ค. การปฏิบัติงานประจำวัน

ควรพิจารณาว่ากระบวนการตรวจสอบได้พิจารณาครอบคลุมไปถึงเรื่องการปฏิบัติงานประจำวัน ดังนี้ คือ

- ความเพียงพอของนโยบายการรักษาความปลอดภัย (security policies) กระบวนการ และวิธีปฏิบัติในทุกหน่วยงานและทุกระดับของสถาบันการเงินและผู้ให้บริการจากภายนอก

- ความเพียงพอของระบบการควบคุมข้อมูลตั้งแต่ขั้นตอนการจัดเตรียม การป้อนข้อมูล การประมวลผลและการแสดงผลข้อมูล

- ความเพียงพอของแผนฉุกเฉินและแผนการดำเนินธุรกิจอย่างต่อเนื่องครอบคลุมเรื่องศูนย์ประมวลผล เครือข่ายสื่อสาร ผู้ให้บริการจากภายนอก และหน่วยงานธุรกิจ และควรพิจารณาความเพียงพอของโปรแกรมและข้อมูลที่จัดเก็บนอกศูนย์คอมพิวเตอร์หลัก และความเพียงพอของการทดสอบแผนการดำเนินธุรกิจอย่างต่อเนื่อง

- คุณภาพของขั้นตอนการดำเนินงานหรือโปรแกรมระบบงานในการเฝ้าติดตามความสามารถในการให้บริการเปรียบเทียบกับผลการดำเนินงานจริง

- ความเพียงพอของสัญญาว่าจ้างและความสามารถในการเฝ้าติดตามความสัมพันธ์กับผู้ให้บริการจากภายนอก ผลการทำงานอย่างเพียงพอ

- คุณภาพของการให้บริการ ความช่วยเหลือกับผู้ให้งาน รวมทั้งความสามารถในการจัดการกับปัญหาต่างๆ

- ความเพียงพอของนโยบาย ขั้นตอนการทำงาน และมีคู่มือปฏิบัติงานต่างๆที่จำเป็นสำหรับการปฏิบัติงานประจำวัน

- คุณภาพของการรักษาความปลอดภัย รวมถึงการรักษาความลับของข้อมูลทั้งด้านกายภาพและด้านตรรกะ

- ความเพียงพอของโครงสร้างทางสถาปัตยกรรมของ Firewall เพื่อรักษาความปลอดภัยในการเชื่อมโยงเครือข่ายการสื่อสารกับเครือข่ายสาธารณะ

ง. การรักษาความปลอดภัยของข้อมูลและข่าวสาร

1. พิจารณาว่ากระบวนการตรวจสอบเรื่องการรักษาความปลอดภัยของข้อมูลและข่าวสารได้ครอบคลุมไปถึงความเสี่ยงของการรักษาความปลอดภัยของข้อมูลข่าวสาร และการทำธุรกรรมทางอิเล็กทรอนิกส์ (e-banking) อย่างเพียงพอ โดยการพิจารณา ดังนี้ คือ

- มีการจัดทำนโยบายการรักษาความปลอดภัยเป็นลายลักษณ์อักษรเพียงพอและมีผลในทางปฏิบัติจริงครอบคลุมไปถึงระบบปฏิบัติการ ระบบฐานข้อมูล และโปรแกรมระบบงานที่สำคัญๆ

- ระบบการควบคุมภายในที่มีอยู่ในปัจจุบันมีความสอดคล้องกับนโยบายการรักษาความปลอดภัยทางด้านข้อมูลและข่าวสาร แนวทางปฏิบัติที่เป็นสากล หรือข้อกำหนดของหน่วยงานภาครัฐหรือไม่

- กิจกรรมหรือมาตรการรักษาความปลอดภัยของข้อมูลจะต้องเป็นมีความเป็นอิสระจากระบบปฏิบัติการ การเขียนโปรแกรม การปฏิบัติการประจำวัน การนำข้อมูลเข้า-ออก และการตรวจสอบโปรแกรมเมอร์หรือเจ้าหน้าที่ระบบ ผู้ทำหน้าที่โอเปอเรเตอร์ เจ้าหน้าที่ป้อนข้อมูลและผู้ตรวจสอบจะต้องไม่สามารถเข้าถึงข้อมูลได้

- มีขั้นตอนการพิสูจน์ตัวตน เช่น User ID และ Password ซึ่งควบคุมการเข้าถึงระบบงาน

- มีกระบวนการในการจัดเก็บรหัสผ่านเพื่อการเข้าถึงระบบงานอย่างเหมาะสมและมีการบังคับให้เปลี่ยนรหัสผ่านเป็นระยะอย่างเหมาะสม

- ต้องมีการบันทึกเกี่ยวกับการปรับปรุงข้อมูลทั้งของ operator และเจ้าหน้าที่ระบบงาน รวมทั้งการใช้คำสั่งพิเศษต่างๆ บนเครื่องคอมพิวเตอร์ส่วนบุคคล

- มีการจัดเก็บบันทึกรายการธุรกรรมทั้งหมดที่เกิดขึ้นทั้งในระบบปฏิบัติการและโปรแกรมระบบงานรวมไปถึงข้อมูลเกี่ยวกับคำสั่งงานต่างๆที่ผู้ใช้งาน หรือ พนักงานปฏิบัติการคอมพิวเตอร์ พิมพ์เข้าสู่ระบบผ่านทางจอ Terminal หรือ คอมพิวเตอร์ PC

- ความพยายามในการเข้าสู่ระบบปฏิบัติการและโปรแกรมระบบงานโดยไม่ได้รับอนุญาตจะต้องถูกบันทึกไว้ ต้องมีการติดตามผล และมีการตอบสนองโดยหน่วยงานที่มีความเป็นอิสระ

- คู่มือผู้ใช้งานหรือฟังก์ชั่นการช่วยเหลือจะต้องให้ข้อมูลที่อธิบายให้เห็นข้อกำหนดในการประมวลผลและการใช้งานโปรแกรม

- ต้องมีระบบการควบคุมต่างๆของระบบการสื่อสาร รวมไปถึงการเข้าถึงระบบจากระยะไกลของผู้ใช้งาน โปรแกรมเมอร์ หรือผู้จัดจำหน่ายโปรแกรมระบบงาน และต้องมีการควบคุมทั้งที่ Firewall และ Router เพื่อควบคุมการเข้าถึงองค์ประกอบต่างๆ ของโครงสร้างด้าน Hardware และ Software และระบบปฏิบัติการและโปรแกรมระบบงาน

- มีระบบการควบคุมการเข้าถึงอาคารสถานที่ ศูนย์คอมพิวเตอร์และอุปกรณ์ที่มีความสำคัญอย่างเพียงพอ

- มีกระบวนการทำงานเป็นลายลักษณ์อักษรซึ่งครอบคลุมในเรื่องกิจกรรมต่างๆที่เป็นหน้าที่ของบุคคลที่มีหน้าที่บำรุงรักษาเครือข่ายและระบบการสื่อสาร

- มีการจัดเก็บเอกสารเกี่ยวกับระบบสื่อสารที่ครบถ้วนถึงเรื่องการเข้าถึงระบบจากระยะไกลและการสื่อสารผ่านระบบสื่อสาร สาธารณะ และควบคุมให้เฉพาะผู้ที่มีอำนาจเท่านั้นในการเข้าถึงเอกสารดังกล่าว

- มีระบบการควบคุมทางตรรกะเพื่อควบคุมให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นในการเข้าสู่ระบบปฏิบัติการ Software ระบบสื่อสารFirewall และ Router

- มีกระบวนการปรับปรุงและทดสอบระบบเครือข่ายการสื่อสารซึ่งครอบคลุมไปถึงเรื่อง การกำหนดค่าตัวแปร (Configuring) การควบคุม และการเฝ้าติดตามดูแล Firewall และ Router

- มีกระบวนการในการอนุญาตที่เหมาะสม เมื่อพนักงาน คู่ค้า หรือบุคคลที่ต้องการเข้าถึงระบบงานจากระยะไกล Internet หรือ VPN

- มีการจัดเตรียมแผนฉุกเฉินที่มีรายละเอียดเกี่ยวกับกระบวนการในการใช้ระบบการสื่อสารชุดสำรอง หรือชุดทางเลือกอื่น

- มีระบบการพิสูจน์ตัวตนที่เหมาะสมในการควบคุมการเข้าถึงระบบสื่อสาร
- มีระบบเฝ้าติดตามดูแลการพยายามเข้าถึงระบบงานโดยไม่ได้รับอนุญาต

2. พิจารณาว่ากระบวนการตรวจสอบสัมพันธ์สอดคล้องกับมาตรฐานในการการรักษาความปลอดภัยสำหรับการส่งข้อมูลลูกค้าระหว่างองค์กรตามกฎหมาย Gramm-Leach-Bliley ของ USA หรือไม่ โดยการพิจารณา ดังนี้ คือ

- มีการกำหนด/ระบุ และประเมินความเสี่ยงที่จะมีต่อข้อมูลของลูกค้า
- มีการออกแบบและติดตั้งโปรแกรมที่ใช้ในการควบคุมความเสี่ยง
- มีการทดสอบระบบการควบคุมต่าง ๆ ที่สำคัญอย่างน้อยปีละครั้ง
- มีการอบรมและฝึกซ้อมพนักงาน
- มีการปรับปรุงแผนการปฏิบัติงานตามกฎหมายและข้อบังคับของหน่วยงานภาครัฐอย่างสม่ำเสมอ และทำให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี ระดับความสำคัญของข้อมูลของลูกค้า รวมถึงภัยคุกคามจากภายนอกและภายในองค์กรที่มีผลต่อการรักษาความปลอดภัยของข้อมูล

จ. ระบบชำระเงิน

1. พิจารณาว่ากระบวนการตรวจสอบได้พิจารณาถึงความเสี่ยงของระบบชำระเงินอย่างเหมาะสม และครอบคลุมไปถึงความเสี่ยงจากระบบชำระเงินรายใหญ่ (Wholesale electronic fund transfer-EFT เช่น Smart และ BahtNet ซึ่งโอนเงินขั้นต่ำรายการละ 5 แสนบาท และ 1 ล้านบาท ตามลำดับ) โดยการพิจารณา ดังนี้ คือ

- มีนโยบายและกระบวนการทำงานที่เหมาะสมครอบคลุมไปถึงกิจกรรมของฝ่ายงานที่ทำหน้าที่โอนเงิน และฝ่ายงานธุรกิจต้นเรื่อง (ตั้งแต่การอนุมัติ การพิสูจน์ความถูกต้อง และข้อกำหนดในการแจ้งผลการทำรายการธุรกรรม)
- มีสัญญาเป็นลายลักษณ์อักษรกับหน่วยงานที่เกี่ยวข้องกับการให้บริการโอนเงิน (ธปท. ITMX และสถาบันการเงินอื่นๆ)
- มีการแบ่งแยกหน้าที่เพื่อป้องกันมิให้บุคคลเพียงคนเดียวสามารถทำหน้าที่ทั้งหมดตั้งแต่การสร้างรายการธุรกรรมเริ่มต้น การตรวจสอบความถูกต้อง และการสั่งคำสั่งโอนเงิน
- มีการกำหนดนโยบายและแนวทางปฏิบัติงานสำหรับพนักงานที่ใช้งานได้จริง
- มีการกำหนดนโยบายในการรักษาความปลอดภัยในการป้องกันอุปกรณ์ที่ใช้สำหรับการทำรายการโอนเงิน Software สายสื่อสาร คำสั่งในการจ่ายเงินทั้งขาเข้าและขาออก และการตรวจสอบรหัสการโอนเงินอย่างเหมาะสมเพียงพอ

- มีนโยบายการให้สินเชื่อและการอนุมัติจากฝ่ายจัดการที่เหมาะสม ครอบคลุมเรื่องการอนุมัติการเบิกเงินเกินบัญชี

- มีการจัดพิมพ์รายการธุรกรรม การเฝ้าติดตามดูแล และการกระทบยอด (Reconcilement) อย่างน้อยวันละครั้ง หรือมากกว่าตามประเภทของธุรกรรม

- มีการประกันภัยตามความเสียหายที่เหมาะสม

- มีการจัดทำแผนฉุกเฉินที่มีความเหมาะสมกับขนาดและความสลับซับซ้อนของระบบโอนเงิน

- มีการใช้ระบบรักษาความปลอดภัยที่บังคับให้ผู้ใช้งานที่จะทำการโอนเงินผ่าน Terminal ต้องใช้รหัสผ่านที่เหมาะสมในการทำรายการธุรกรรม

2. พิจารณาว่ากระบวนการตรวจสอบได้พิจารณาถึงความเสี่ยงของระบบชำระเงินอย่างเหมาะสม และครอบคลุมไปถึงความเสี่ยงจากระบบชำระเงินรายย่อยทางอิเล็กทรอนิกส์ (Retail Payment Systems เช่น ATM, POS, Debit Card, Home Banking, Credit and Charge Card โดยการพิจารณา ดังนี้ คือ

- มีการกำหนดเป็นลายลักษณ์อักษรเกี่ยวกับกระบวนการโอนเงินรายย่อยแต่ละประเภทอย่างครบถ้วน

- มีการจัดเก็บเอกสารเกี่ยวกับการโอนเงินทุกประเภทอย่างเหมาะสม

- มีระบบการควบคุมทางด้านกายภาพในการป้องกันบัตรเครดิต ข้อมูลของรหัสผ่าน (PIN) อุปกรณ์ที่ใช้ในการโอนเงิน และระบบการสื่อสาร

- มีการแบ่งแยกหน้าที่และการควบคุมทางด้านตรรกะเพื่อป้องกันการเข้าถึง Software บัญชีของลูกค้า และข้อมูลของรหัสผ่าน

- มีการบันทึกรายการธุรกรรมอย่างเหมาะสมรวมถึงรายการที่ผิดปกติและจัดให้มีการจัดเก็บร่องรอยเพื่อการตรวจสอบสำหรับกิจกรรมแต่ละประเภท

- มีการกระทบยอดและพิสูจน์ความถูกต้องทุกวันโดยบุคคลที่ไม่มีผลประโยชน์ทับซ้อน

- มีการจัดทำแผนฉุกเฉินที่เพียงพอ

- มีการจัดทำกรมธรรม์ประกันภัยในวงเงินที่เหมาะสม

- มีการทำประกันความเสียหายของการทำรายการ

- การทำรายการโอนเงินต้องเป็นไปตามข้อกำหนดของหน่วยงานภาครัฐ

3. พิจารณาว่ากระบวนการตรวจสอบได้พิจารณาถึงความเสี่ยงของระบบ

ชำระเงินอย่างเหมาะสม และครอบคลุมไปถึงความเสี่ยงจากสำนักหักบัญชีอัตโนมัติ (ACH) โดยพิจารณา ดังนี้ คือ

- มีนโยบายและกระบวนการที่ครอบคลุมการทำงานของสำนักหักบัญชีอัตโนมัติ

- มีการตรวจสอบความถูกต้องของยอดรวมทั้งด้านรายรับและรายจ่ายอย่างเพียงพอ และมีการตรวจนับจำนวนรายการก่อนที่จะทำการบันทึกบัญชีของลูกค้า

- มีระบบการควบคุมอย่างเหมาะสมเพียงพอสำหรับรายการธุรกรรมประเภทที่ถูกปฏิเสธการชำระเงินแบบทันที (Reject) รายการที่ลูกค้าปฏิเสธการชำระเงินในภายหลังที่ได้ทำสำเร็จแล้วและสถาบันการเงินจำเป็นต้องล้างรายการกลับคืน (Charge back) รายการที่ลงบันทึกไว้แต่ยังไม่ได้ผ่านบัญชี และรายการคงค้างอื่นๆ

- มีระบบการควบคุมต่างๆ ที่สามารถป้องกันการเปลี่ยนแปลงข้อมูลที่ได้รับมา รวมถึงข้อมูลที่จะบันทึกเข้าระบบบัญชีด้วย

- มีระบบการควบคุมที่เหมาะสมเพื่อใช้ในการป้องกันการทำรายการเริ่มต้นเข้าสู่ระบบ รวมไปถึงการแบ่งแยกหน้าที่ในการเตรียมข้อมูลนำเข้า การนำข้อมูลเข้าสู่ระบบ การส่งผ่านข้อมูล และการกระทบยอดความถูกต้องของรายการธุรกรรม

- มีระบบการรักษาความปลอดภัยและระบบควบคุมภายในเพื่อจัดเก็บข้อมูลที่รับมาจาก ACH และการดูแลอุปกรณ์ที่ใช้ในการโอนเงิน

- มีการปฏิบัติงานตามข้อกำหนดของ ITMX สำนักหักบัญชี และข้อกำหนดของ ธปท.

ฉ. การใช้บริการจากภายนอก

1. พิจารณาว่ากระบวนการตรวจสอบได้พิจารณาถึงความเสี่ยงของการใช้บริการจากผู้ให้บริการภายนอกในกรณีที่จะต้องให้บริการด้าน IT ไปถึงผู้ใช้งานที่เป็นบุคคลภายนอก โดยพิจารณา ดังนี้ คือ

- มีกระบวนการทำงานที่เป็นลายลักษณ์อักษรและมีการมอบหมายให้พนักงานเพื่อการประสานงานกับผู้ใช้งานและลูกค้าในเรื่องที่เกี่ยวข้องกับศูนย์คอมพิวเตอร์ประมวลผล ได้แก่ เรื่องคำขอในการเปลี่ยนแปลงโปรแกรม การบันทึกข้อมูลที่ไม่ตรงกัน และระดับของคุณภาพในการให้บริการ

- มีการจัดทำสัญญากับลูกค้าครบถ้วน ทั้งกับบริษัทในเครือและบริษัทอื่นๆ ด้วย นอกจากนี้เอกสารสัญญาจะต้องผ่านการอนุมัติจากฝ่ายกฎหมายด้วย

- มีระบบการควบคุมต่างๆครอบคลุมไปถึงเรื่องการส่งใบเรียกเก็บและการรับชำระเงิน

- มีการจัดทำแผนฉุกเฉินที่ครอบคลุมไปถึงศูนย์คอมพิวเตอร์ ลูกค้า และผู้ใช้งาน

- มีระบบการควบคุม Terminal ที่ลูกค้าและผู้ใช้งานใช้ทำธุรกรรมแบบ Online

- มีคู่มือการทำงานที่ครบถ้วนและได้มีการแจกจ่ายออกไปใช้งานจริง

- มีการจัดให้มีกระบวนการและวิธีการในการติดต่อสื่อสารกับผู้ใช้บริการเมื่อเกิดเหตุการณ์ไม่ปกติในรูปแบบต่างๆเกิดขึ้น

2. พิจารณาว่ากระบวนการตรวจสอบเรื่องการใช้บริการจากผู้ให้บริการภายนอกเพียงพอหรือไม่ โดยพิจารณา ดังนี้ คือ

- มีการจัดทำสัญญาการใช้บริการที่ผ่านการตรวจสอบความถูกต้องจากฝ่ายกฎหมายของสถาบันการเงินเรียบร้อยแล้ว

- มีการเฝ้าติดตามดูแลผลการให้บริการ และฐานะทางการเงินของให้บริการจากภายนอก

- มีแผนฉุกเฉินและแผนการกู้คืนระบบที่สามารถใช้งานได้จริง

- มีระบบการควบคุมTerminal ที่สถาบันการเงินจะใช้ในการเข้าถึงแฟ้มข้อมูลที่จัดเก็บอยู่กับผู้ให้บริการซึ่งตั้งอยู่ภายนอกสถาบันการเงิน

- มีระบบการควบคุมภายในที่สม่ำเสมอและสอดคล้องกันสำหรับระบบงานที่สำคัญ ๆ ทั้งหมดโดยเฉพาะระบบงานที่พัฒนาเองภายในสถาบันการเงิน

- ฝ่ายจัดการต้องประเมินผลกระทบจากแนวโน้มและปัจจัยต่างๆทั้งภายนอกและภายในที่จะมีผลต่อความสามารถของผู้ให้บริการจากภายนอกในการให้บริการต่อลูกค้าของสถาบันการเงิน

- ผู้ให้บริการจากภายนอกจะต้องสามารถดำรงรักษาระดับของการให้บริการให้ตรงกับความต้องการของลูกค้าของสถาบันการเงิน

- ฝ่ายจัดการต้องเฝ้าติดตามดูแลคุณภาพและควบคุมคุณภาพของโปรแกรมระบบงาน เอกสารและคู่มือการใช้งาน และการฝึกอบรมให้ความรู้ ซึ่งผู้ให้บริการจากภายนอกเป็นผู้ดำเนินการ