คู่มือตรวจสอบความเสี่ยง ด้านปฏิบัติการ

สารบัญ

บทสรุปผู้บริหาร 1
แผนผังกระบวนการตรวจสอบความเสี่ยงด้านปฏิบัติการ 3
ส่วนที่ 1 ลักษณะและที่มาของความเสี่ยงด้านปฏิบัติการ 7
1.1 คำจำกัดความของความเสี่ยงด้านปฏิบัติการ 7
1.2 ที่มาของความเสี่ยงด้านปฏิบัติการ 9
1.3 ประเภทของความเสี่ยงด้านปฏิบัติการ 11
ส่วนที่ 2 แนวทางการบริหารความเสี่ยงด้านปฏิบัติการที่พึงปฏิบัติ 15
2.1 บทบาทคณะกรรมการ ผู้บริหารระดับสูง และการจัดองค์กรด้านปฏิบัติการ 16
2.1.1 บทบาทหน้าที่ 16
- คณะกรรมการสถาบันการเงิน 16
- ผู้บริหารระดับสูง 17
- คณะกรรมการตรวจสอบ 18
- คณะกรรมการบริหารความเสี่ยง 19
- หน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการ 20

2.1.2 การจัดองค์กร 29
2.2 นโยบายการบริหารความเสี่ยงด้านปฏิบัติการ 32
2.2.1 นโยบายและขอบเขตการบริหารความเสี่ยงด้านปฏิบัติการ 32
2.2.2 กลยุทธ์ในการบริหารความเสี่ยงด้านปฏิบัติการ 33
2.2.3 วัฒนธรรมองค์กร การสื่อสารและการควบคุม 33
2.3 การบริหารความเสี่ยงด้านปฏิบัติการ 33
2.3.1 การระบุความเสี่ยง 34
2.3.2 การประเมินความเสี่ยง 35
- การวัดความเสี่ยง 36
- การคำนวณเงินกองทุนรองรับความเสี่ยงด้านปฏิบัติการ 37

2.3.3 การติดตามและการรายงานความเสี่ยง 40
- การติดตามความเสี่ยง 40
- การรายงานความเสี่ยง 43

- ระบบข้อมูลสารสนเทศเพื่อการบริหารความเสี่ยงด้านปฏิบัติการ 45
- การเปิดเผยข้อมูล 46

2.3.4 การควบคุมและลดความเสี่ยง 47

- บุคลากรและการฝึกอบรม 55
- กระบวนการปฏิบัติงานและระบบงาน 55
- การบริหารความต่อเนื่องทางธุรกิจ 58

ภาคผนวก **63**

ประกาศ / หนังสือเวียน / แนวปฏิบัติที่เกี่ยวข้อง 63

บทสรุปผู้บริหาร

คู่มือการตรวจสอบความเสี่ยงด้านปฏิบัติการมีวัตถุประสงค์เพื่อให้ผู้ตรวจสอบใช้เป็นแนวทางในการตรวจสอบและมีมาตรฐานเดียวกัน โดยให้มีความเข้าใจถึง

1.ลักษณะและที่มาของความเสี่ยงด้านปฏิบัติการว่า ความเสี่ยงอาจพบในทุกผลิตภัณฑ์ กระบวนการ และหน่วยงาน รวมถึงระบบเทคโนโลยีสารสนเทศ ซึ่งอาจก่อให้เกิดความเสียหายต่อสถาบันการเงินได้

2. แนวทางการบริหารความเสี่ยงที่พึงปฏิบัติ (Best Practice) ที่สอดคล้องกับกฎเกณฑ์การกำกับที่เป็นสากลและตามประกาศ ธปท. ที่ออกใหม่ และ

3. แนวทางการตรวจสอบ ทั้งในการประเมินระดับความเสี่ยงและการจัดการความเสี่ยง

เนื้อหาของคู่มือตรวจสอบความเสี่ยงด้านปฏิบัติการ สามารถสรุปได้ดังนี้

I. ลักษณะและที่มาของความเสี่ยงด้านปฏิบัติการ

ความเสี่ยงด้านปฏิบัติการถือเป็นความเสี่ยงที่เกิดจากความผิดพลาด หรือความไม่เพียงพอของกระบวนการทำงาน พนักงาน ระบบงาน หรือระบบเทคโนโลยีสารสนเทศ และเหตุการณ์หรือปัจจัยภายนอก ซึ่งทำให้ได้รับความเสียหายต่อรายได้หรือเงินกองทุนของสถาบันการเงิน ทั้งทางตรงและทางอ้อม โดยมีปัจจัยที่มีผลกระทบต่อการดำเนินงาน 4 ปัจจัย ได้แก่ ปัจจัยด้านบุคลากร ปัจจัยด้านระบบงาน ปัจจัยด้านกระบวนการทำงาน และปัจจัยจากภายนอก

II. แนวทางการบริหารความเสี่ยงด้านปฏิบัติการที่พึงปฏิบัติ (Best Practice)

ระบบการบริหารความเสี่ยงด้านปฏิบัติการที่ดี ควรประกอบด้วย 3 องค์ประกอบหลัก ได้แก่

☏ บทบาทคณะกรรมการ ผู้บริหาร และการจัดองค์กรด้านปฏิบัติการ เป็นปัจจัยที่สำคัญอย่างหนึ่งในการบริหารความเสี่ยงของสถาบันการเงิน โดยคณะกรรมการ ผู้บริหารสถาบันการเงินทุกท่านต้องตระหนักและให้ความสำคัญกับนโยบาย แผนงานการปฏิบัติงานและธุรกิจของสถาบันการเงิน โดยการกำหนดกรอบนโยบาย กลยุทธ์ คำจำกัดความของความเสี่ยงด้านปฏิบัติการที่เหมาะสมกับองค์กร ระดับความเสี่ยงที่ยอมรับได้และแผนงานการบริหารความเสี่ยง รวมถึงการนำกรอบที่กำหนดไปปฏิบัติ สื่อสารให้ผู้ปฏิบัติงานรับทราบและควบคุมเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ ทั้งนี้ คณะกรรมการ และผู้บริหารของสถาบันการเงินต้องทบทวนนโยบาย ขอบเขตและแผนเป็นระยะ ๆ อย่างสม่ำเสมอ

☏ นโยบายการบริหารความเสี่ยงด้านปฏิบัติการ ประกอบด้วย

(1) นโยบายและขอบเขตการบริหารความเสี่ยงด้านปฏิบัติการ จะพิจารณาถึงเนื้อหาให้ครอบคลุมนโยบาย ขอบเขต และแนวทางปฏิบัติในการบริหารความเสี่ยงในเรื่องการระบุ การประเมิน การติดตาม การรายงาน การควบคุมและการลดความเสี่ยง รวมถึงการกำหนดระดับความเสี่ยงที่ยอมรับได้ เพื่อใช้เป็นเกณฑ์ในการกำหนดเงินกองทุนเพื่อรองรับความเสี่ยง โดยอ้างอิงหลักเกณฑ์การดำรงเงินกองทุนที่ธนาคารแห่งประเทศไทยกำหนด

(2) กลยุทธ์ในการบริหารความเสี่ยงด้านปฏิบัติการ จะพิจารณาถึงการกำหนดและทบทวนแผนกลยุทธ์อย่างสม่ำเสมอ เพื่อจัดทำแผนปฏิบัติการ (Action Plan) ในการพัฒนาระบบงานที่เกี่ยวเนื่องกับการบริหารความเสี่ยงด้านปฏิบัติการในระดับองค์กร และระดับหน่วยธุรกิจต่าง ๆ โดยแผนกลยุทธ์ที่จัดทำขึ้น ควรกำหนดรายละเอียดของวัตถุประสงค์ ขอบเขตงาน ผู้มีหน้าที่รับผิดชอบ งบประมาณ หรือทรัพยากรที่ต้องการ รวมถึงระยะเวลาของแผนที่ชัดเจน เพื่อประโยชน์ในการบริหาร และติดตามการดำเนินการตามแผนกลยุทธ์ในการบริหารความเสี่ยงที่กำหนดไว้

(3) วัฒนธรรมองค์กร การสื่อสารและการควบคุม เป็นจุดสำคัญที่จะเน้นการปลูกฝังจิตสำนึกในการสร้างระบบการควบคุมให้เป็นวัฒนธรรมขององค์กร เพื่อให้ผู้ที่เกี่ยวข้องทุกระดับตระหนักว่ากิจกรรมการควบคุมเป็นหน้าที่ของทุกคนในสถาบันการเงินไม่ใช่เป็นหน้าที่เฉพาะของหน่วยธุรกิจใดหน่วยธุรกิจหนึ่ง โดยเฉพาะคณะกรรมและผู้บริหารระดับสูงควรต้องมีความรับผิดชอบและเป็นผู้นำในการสร้างวัฒนธรรมองค์กร เพื่อสร้างให้เกิดการดำเนินงานและการมีระบบควบคุมที่ดีเป็นไปตามหลักการกำกับดูแลกิจการที่ดีภายในองค์กร

☏ การบริหารความเสี่ยงด้านปฏิบัติการ ถือเป็นสิ่งสำคัญของการบริหารความเสี่ยงด้านปฏิบัติการที่ผู้ตรวจสอบพึงรู้ ได้แก่ ปัจจัยความเสี่ยงด้านปฏิบัติการที่ประกอบด้วย ด้านบุคลากร ด้านระบบงาน ด้านกระบวนการทำงาน และด้านปัจจัยภายนอก รวมทั้งยังต้องทราบถึงระบบการบริหารความเสี่ยงด้านปฏิบัติการที่จะทำให้สถาบันการเงินได้ปฏิบัติให้อยู่ในกรอบของความเสี่ยงที่ยอมรับได้ โดยมีกระบวนการที่เกี่ยวกับ การระบุ การวัด การติดตาม การรายงาน การควบคุมและการลดความเสี่ยง

แผนผังกระบวนการตรวจสอบความเสี่ยงด้านปฏิบัติการ

แผนผังนี้แสดงถึงปัจจัยที่ก่อให้เกิดความเสี่ยงและแนวทางในการตรวจสอบ โดยเริ่มจากการกำหนดวัตถุประสงค์ในการตรวจสอบ พิจารณาขั้นตอนการบริหารความเสี่ยง ซึ่งกล่าวถึงการระบุ ประเมิน ติดตาม/รายงานและการควบคุม เพื่อนำไปสู่ขั้นตอนการตรวจสอบด้านระดับและการจัดการ ตลอดจนแนวโน้มความเสี่ยง

แนวทางการตรวจสอบความเสี่ยงด้านปฏิบัติการ

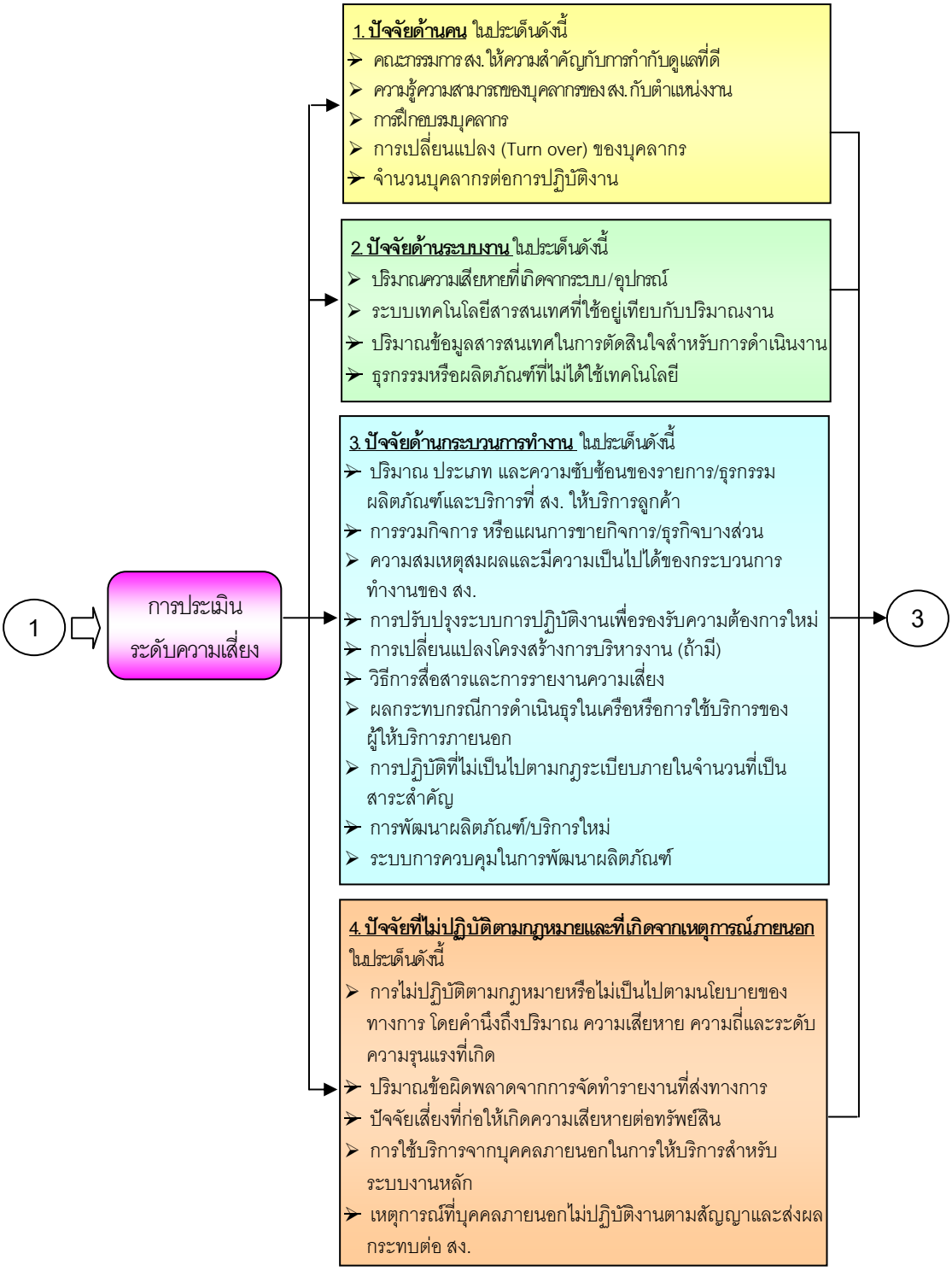
กำหนดวัตถุประสงค์การตรวจสอบ

- ให้มีการตระหนักถึงความเสี่ยงที่สำคัญและเกี่ยวข้อง เช่น โครงสร้างองค์กร การพัฒนาและสนับสนุน เป็นต้น
- มีการควบคุมดูแลอย่างถูกต้องเหมาะสมและทันกาล เช่น บทบาทหน้าที่ของคณะกรรมการและผู้บริหาร
- พิจารณาถึงระดับและคุณภาพการจัดการความเสี่ยง เช่น หน่วยธุรกิจและหน่วยงานสนับสนุน

การบริหารความเสี่ยง

- การระบุความเสี่ยง สง. ควรดำเนินการให้มีการระบุความเสี่ยง ประเภทความเสี่ยงและปัจจัยความเสี่ยงในแต่ละผลิตภัณฑ์ บริการทางการเงิน ระบบงาน หรือในแต่ละหน่วยงานของ สง. โดยจัดทำอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่เปลี่ยนแปลง
- การประเมินความเสี่ยง สง.ควรกำหนดหรือทบทวนแนวทางและวิธีการในการประเมินความเสี่ยงให้เหมาะสมกับการดำเนินธุรกิจอยู่เสมอ เพื่อให้ผู้บริหารทุกระดับสามารถประเมินความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงานที่ตนรับผิดชอบได้
- การติดตามและรายงานความเสี่ยง สง. ควรมีระบบการติดตามและการรายงานข้อมูลปัจจัยเสี่ยงรวมทั้งข้อมูลสถานะความเสี่ยงในภาพรวมให้ผู้บริหารรับทราบอย่างต่อเนื่องและสม่ำเสมอ โดยมีความถี่ในการติดตามที่เหมาะสม
- การควบคุมและลดความเสี่ยง สง. ควรประเมินการควบคุมว่าในแต่ละประเภทหรือหน่วยธุรกิจ ได้ดำเนินการไปตามวัตถุประสงค์หลักของการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งง่ายต่อการปฏิบัติและมีต้นทุนที่ไม่สูงเกินไป

1 2


1
การประเมิน
ระดับความเสี่ยง
1. ปัจจัยด้านคน ในประเด็นดังนี้
➢ คณะกรรมการ สง. ให้ความสำคัญกับการกำกับดูแลที่ดี
➢ ความรู้ความสามารถของบุคลากรของ สง. กับตำแหน่งงาน
➢ การฝึกอบรมบุคลากร
➢ การเปลี่ยนแปลง (Turn over) ของบุคลากร
➢ จำนวนบุคลากรต่อการปฏิบัติงาน
2. ปัจจัยด้านระบบงาน ในประเด็นดังนี้
➢ ปริมาณความเสียหายที่เกิดจากระบบ/อุปกรณ์
➢ ระบบเทคโนโลยีสารสนเทศที่ใช้อยู่เทียบกับปริมาณงาน
➢ ปริมาณข้อมูลสารสนเทศในการตัดสินใจสำหรับการดำเนินงาน
➢ ธุรกรรมหรือผลิตภัณฑ์ที่ไม่ได้ใช้เทคโนโลยี
3. ปัจจัยด้านกระบวนการทำงาน ในประเด็นดังนี้
➢ ปริมาณ ประเภท และความซับซ้อนของรายการ/ธุรกรรม ผลิตภัณฑ์และบริการที่ สง. ให้บริการลูกค้า
➢ การรวมกิจการ หรือแผนการขายกิจการ/ธุรกิจบางส่วน
➢ ความสมเหตุสมผลและมีความเป็นไปได้ของกระบวนการทำงานของ สง.
➢ การปรับปรุงระบบการปฏิบัติงานเพื่อรองรับความต้องการใหม่
➢ การเปลี่ยนแปลงโครงสร้างการบริหารงาน (ถ้ามี)
➢ วิธีการสื่อสารและการรายงานความเสี่ยง
➢ ผลกระทบกรณีการดำเนินธุรในเครือหรือการใช้บริการของผู้ให้บริการภายนอก
➢ การปฏิบัติที่ไม่เป็นไปตามกฎระเบียบภายในจำนวนที่เป็นสาระสำคัญ
➢ การพัฒนาผลิตภัณฑ์/บริการใหม่
➢ ระบบการควบคุมในการพัฒนาผลิตภัณฑ์
4. ปัจจัยที่ไม่ปฏิบัติตามกฎหมายและที่เกิดจากเหตุการณ์ภายนอก ในประเด็นดังนี้
➢ การไม่ปฏิบัติตามกฎหมายหรือไม่เป็นไปตามนโยบายของทางการ โดยคำนึงถึงปริมาณ ความเสียหาย ความถี่และระดับความรุนแรงที่เกิด
➢ ปริมาณข้อผิดพลาดจากการจัดทำรายงานที่ส่งทางการ
➢ ปัจจัยเสี่ยงที่ก่อให้เกิดความเสียหายต่อทรัพย์สิน
➢ การใช้บริการจากบุคคลภายนอกในการให้บริการสำหรับระบบงานหลัก
➢ เหตุการณ์ที่บุคคลภายนอกไม่ปฏิบัติงานตามสัญญาและส่งผลกระทบต่อ สง.
3

2 → การประเมินการจัดการความเสี่ยง

1. คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง ในประเด็นดังนี้
- บทบาทหน้าที่ของคณะกรรมการสถาบันการเงิน
- บทบาทหน้าที่ของผู้บริหารระดับสูง
- วิธีการสื่อสารและการรายงานความเสี่ยง
- บทบาทหน้าที่ของคณะกรรมการตรวจสอบ
- บทบาทหน้าที่ของคณะกรรมการบริหารความเสี่ยง

2. นโยบายและกลยุทธ์การบริหารความเสี่ยงด้านปฏิบัติการ ในประเด็นดังนี้
- กระบวนการกำหนดกลยุทธ์และภาพรวมในระดับความเสี่ยงของสถาบันการเงิน
- การทบทวนนโยบายและแผนกลยุทธ์
- วิธีการสื่อสารและการรายงานความเสี่ยง
- กฎระเบียบ วิธีปฏิบัติและคู่มือที่ชัดเจน และเป็นปัจจุบัน
- กระบวนการกำหนดเครื่องมือในการประเมินและติดตาม

3. โครงสร้างองค์กรและการบริหารงาน ในประเด็นดังนี้
- การจัดโครงสร้างองค์กรและการบริหารงาน
- กระบวนการปฏิบัติงานของหน่วยงานบริหารความเสี่ยง
- กระบวนการปฏิบัติงานของหน่วยงานตรวจสอบภายใน
- กระบวนการปฏิบัติงานของหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์
- ระบบการติดตาม
- การกำหนดเพดานความเสี่ยง

4. การควบคุมภายใน ในประเด็นดังนี้
- การ ติดตามการปฏิบัติงานตามวัตถุประสงค์และการควบคุมภายในขององค์กร
- กระบวนการกำหนดธุรกรรมและผลิตภัณฑ์ในการบริหารความเสี่ยง
- การวางระบบการบริหารความเสี่ยงเกี่ยวกับการประเมินความเสี่ยง
- การควบคุมการปฏิบัติงาน
- กระบวนการ วิธีการการควบคุมการปฏิบัติงานในแต่ละส่วนงาน
- การกำหนดโครงสร้างการควบคุมภายใน
- การมอบอำนาจการอนุมัติ
- การกำหนดการสอบทานความถูกต้องของการปฏิบัติงาน
- การควบคุมทรัพย์สินที่มีตัวตน
- การกำหนดนโยบายการปฏิบัติงาน โดยการแบ่งแยกหน้าที่ในองค์กรอย่างเหมาะสมและกำหนดนโยบายด้านการพนักงาน
- วิธีการลดความเสียหายที่อาจเกิดขึ้น

5. การติดตามและรายงานระบบข้อมูล ในประเด็นดังนี้
- ระบบการควบคุมหรือการตรวจสอบความถูกต้องของข้อมูลก่อนนำมาใช้ หาก สง. มีการเปลี่ยนแปลงระบบข้อมูล
- การจัดเก็บและรายงานข้อมูลความเสียหายที่เกิดขึ้น
- คณะกรรมการ สง. และผู้บริหารระดับสูงได้รับข้อมูลที่เชื่อถือได้และทันกาล สำหรับการบริหารและควบคุมความเสี่ยง
- พนักงานทราบถึงกฎระเบียบและวิธีปฏิบัติงานที่ผู้บริหารกำหนด
- คณะกรรมการและผู้บริหารระดับสูงได้ให้ความสนใจเกี่ยวกับการรักษาความปลอดภัยของข้อมูล
- การได้รับข้อมูลของคณะกรรมการตรวจสอบเพื่อการตัดสินใจ
- การเปิดเผยข้อมูลเกี่ยวกับการบริหารความเสี่ยงต่อสาธารณชน
- การคำนวณเงินกองทุนเพื่อรองรับความเสี่ยงด้านปฏิบัติการ

→ 3

2 การประเมินการจัดการความเสี่ยง

6. การตรวจสอบภายใน ในประเด็นดังนี้

- โครงสร้างของหน่วยงาน
  - หน้าที่และความรับผิดชอบของฝ่ายบริหาร
  - สถานภาพในองค์กร
  - ความเป็นอิสระ
  - ความรอบรู้ในวิชาชีพ
  - ความสัมพันธ์และการติดต่อสื่อสาร
  - การกำกับดูแลการตรวจสอบ
  - การ Outsource หน้าที่การตรวจสอบภายใน
- หน้าที่และความรับผิดชอบ
  - ความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน
  - การปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎหมายและข้อบังคับ
  - การตรวจสอบการทุจริต ข้อผิดพลาด การละเลยและรายการผิดปกติ
  - การตรวจสอบการบริหาร
  - การประเมินระบบงานสารสนเทศ
  - บทบาทในการให้คำปรึกษา
- ขอบเขตของงานตรวจสอบ
  - การประเมินความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน
  - การปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎหมายและข้อบังคับ
  - ความเพียงพอและประสิทธิผลของระบบการบริหารความเสี่ยง
  - การใช้ทรัพยากรอย่างมีประสิทธิภาพ ประสิทธิผลและประหยัด
  - การบรรลุวัตถุประสงค์และเป้าหมายที่วางไว้
- การรายงานและการจัดทำเอกสาร
  - รายงานผลการตรวจสอบ
  - การปฏิบัติตามข้อเสนอแนะและการติดตาม
  - การรายงานสิ่งที่ตรวจพบที่สำคัญและการทุจริต
  - การควบคุมและการจัดเก็บรายงานผลการตรวจสอบและกระดาษทำการ
  - การเก็บรักษารายงานผลการตรวจสอบและกระดาษทำการ

7. การกำกับการปฏิบัติงาน (Compliance unit) ในประเด็นดังนี้

- ความมีอิสระของหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์

8. การบริหารความต่อเนื่องทางธุรกิจ ในประเด็นดังนี้

- แผนรองรับการดำเนินธุรกิจต่อเนื่อง
- การกำหนดแผนฉุกเฉิน

9. การปฏิบัติตามกฎหมาย ระเบียบและกฎเกณฑ์อื่นที่เกี่ยวข้อง ในประเด็นดังนี้

- การไม่ปฏิบัติตามกฎหมาย ระเบียบและกฎเกณฑ์ที่กำหนด
- การดำเนินการในด้าน AML/CFT

3

การประเมินแนวโน้มความเสี่ยง ในประเด็นดังนี้

- ปัจจัยภายใน ประกอบด้วย
  - เทคโนโลยี
  - ระบบการควบคุมภายใน/การตรวจสอบภายใน
  - การรวมกิจการ
  - ความปลอดภัยและความถูกต้องของข้อมูล
  - ข้อผิดพลาด/คดีความที่จะถูกฟ้องร้อง/การทุจริตภายในและภายนอก
- ปัจจัยภายนอก ประกอบด้วย
  - การเปลี่ยนแปลงกฎหมาย ประกาศ ระเบียบข้อบังคับของทางการ
  - ภัยพิบัติ

ส่วนที่ 1 ลักษณะและที่มาของความเสี่ยงด้านปฏิบัติการ

1.1 คำจำกัดความของความเสี่ยงด้านปฏิบัติการ[1,2]

ความเสี่ยงด้านปฏิบัติการ (Operational risk) หมายถึง ความเสี่ยงจากการขาดการกำกับดูแลกิจการที่ดีหรือขาดธรรมาภิบาลในองค์กรที่เกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน บุคลากร ระบบงาน หรือเหตุการณ์ภายนอก และส่งผลกระทบต่อรายได้จากการดำเนินงานและเงินกองทุนของสถาบันการเงิน (สง.) รวมถึงความเสี่ยงด้านกฎหมาย เช่น ความเสี่ยงต่อการถูกฟ้องร้องหรือดำเนินคดีตามกฎหมาย ถูกทางการเปรียบเทียบปรับ รวมทั้งความเสียหายที่ได้รับจากการตกลงกันนอกชั้นศาล เป็นต้น ซึ่งความเสี่ยงด้านปฏิบัติการจะมีผลกระทบต่อความเสี่ยงด้านอื่นโดยเฉพาะความเสี่ยงด้านกลยุทธ์ (Strategic risk) และด้านชื่อเสียง[3] (Reputation risk)

ในการพิจารณาความเสี่ยงด้านปฏิบัติการจะประเมินในลักษณะภาพรวมของกลุ่ม ซึ่งถือว่ามีผลกระทบต่อการดำเนินงาน โดยความเสี่ยงด้านปฏิบัติการของกลุ่มจะหมายถึงกลุ่มธุรกิจทางการเงินตามคำนิยามในพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ที่กำหนดให้บริษัทแม่ต้องรับผิดชอบในลักษณะภาพรวม ในการกำหนดนโยบายการบริหารความเสี่ยงด้านปฏิบัติการ นโยบายการจัดเก็บข้อมูลความเสียหายที่เกิดจากความเสี่ยงด้านปฏิบัติการ นโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) นโยบายการใช้บริการจากผู้ให้บริการรายอื่น (Outsourcing) และมาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย (Anti-Money Laundering and Combating the Financing of Terrorism: AML/CFT)

---

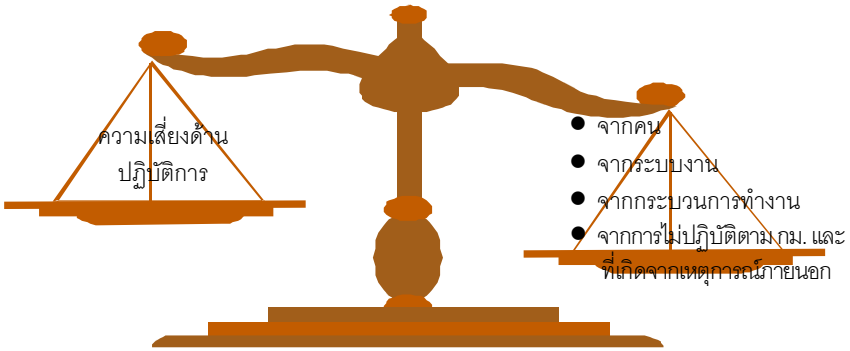
[1] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการ ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510385.pdf

[2] ประกาศธนาคารแห่งประเทศไทยที่ สนส.95/2551 เรื่อง หลักเกณฑ์การดำรงเงินกองทุนขั้นต่ำสำหรับความเสี่ยงด้านปฏิบัติการ ลงวันที่ 27 พฤศจิกายน 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510555.pdf

[3] ความเสี่ยงด้านชื่อเสียง ถือเป็นความเสี่ยงที่ส่งผลกระทบต่อสถาบันการเงิน ซึ่งจะถูกนำไปรวมไว้กับความเสี่ยงด้านกลยุทธ์

ทั้งนี้ บริษัทใดในกลุ่มธุรกิจทางการเงินที่ต้องปฏิบัติตามหลักเกณฑ์ของสำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน ให้ถือว่าบริษัทนั้นต้องปฏิบัติตามหลักเกณฑ์ AML/CFT ด้วย[4]

นอกจากนี้ ความเสี่ยงด้านปฏิบัติการอาจเป็นสาเหตุของความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านเครดิต ความเสี่ยงด้านตลาด และความเสี่ยงด้านสภาพคล่องได้ เช่น การทุจริต ความไม่เพียงพอหรือความไม่ถูกต้องของข้อมูลในการการตัดสินใจ การหยุดชะงักหรือการขัดข้องของระบบคอมพิวเตอร์ การก่อวินาศภัย หรือภัยธรรมชาติ เป็นต้น และอาจก่อให้เกิดความเสียหายต่อการดำเนินงาน และเงินกองทุนของ สง. ได้

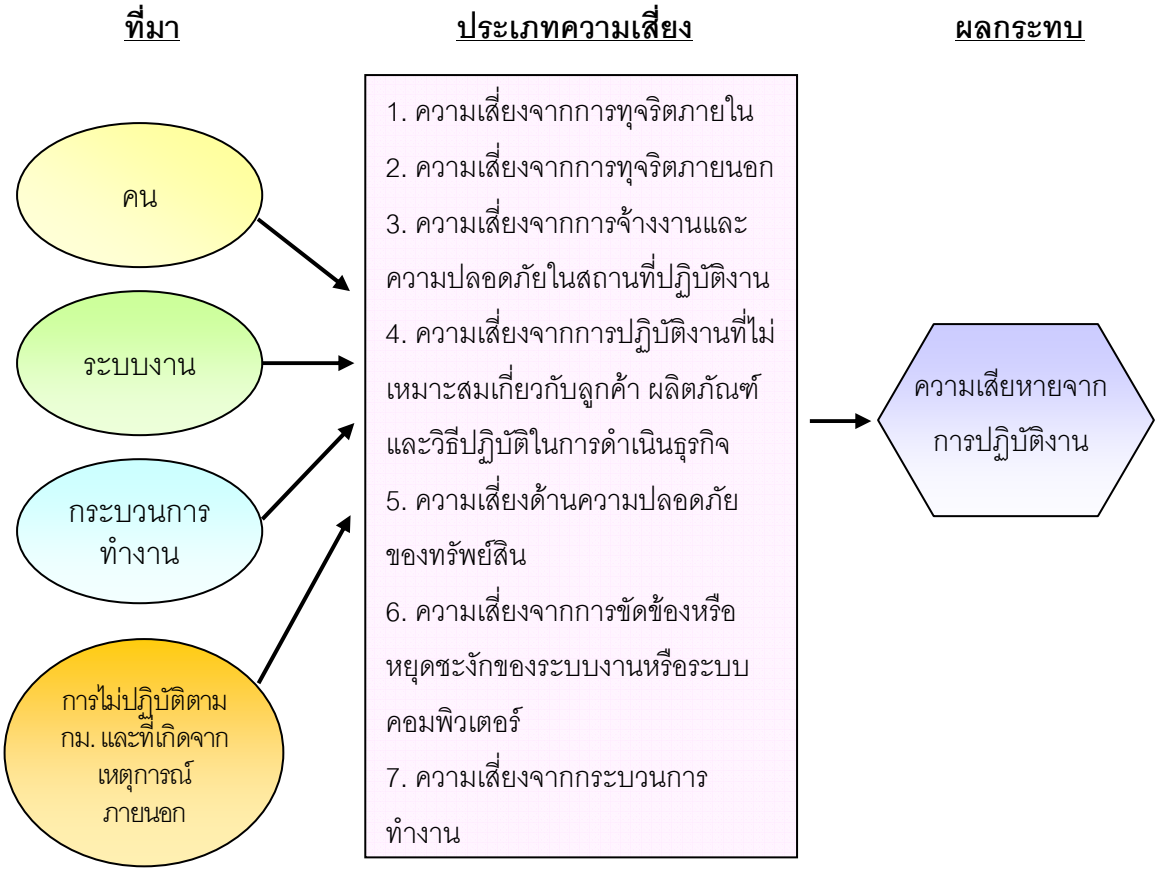


คำจำกัดความของความเสี่ยงด้านปฏิบัติการข้างต้น เป็นคำจำกัดความที่เป็นที่ยอมรับโดยทั่วไป อย่างไรก็ตาม คำจำกัดความ ประเภทของความเสี่ยง และแนวทางในการบริหารความเสี่ยงด้านปฏิบัติการ อาจกว้างกว่าคำจำกัดความที่กำหนดนี้ได้ เพื่อให้เข้าใจถึงการบริหารความเสี่ยงด้านปฏิบัติการในภาพรวมและสามารถนำข้อมูลไปประกอบการตัดสินใจเชิงนโยบาย ปรับปรุงระบบการควบคุมเพื่อลดความเสี่ยง และเพิ่มประสิทธิภาพในการดำเนินงาน รวมถึงช่วยในการจัดเก็บข้อมูลภายในเพื่อติดตามความเสี่ยงในภาพรวมของ สง. และพนักงานทุกระดับมีความเข้าใจและสามารถนำไปถือปฏิบัติได้

ทั้งนี้ คำจำกัดความ และประเภทของความเสี่ยงที่ สง.กำหนดขึ้น จะครอบคลุมความเสี่ยงที่เกิดขึ้นมากน้อยเพียงใดนั้น ขึ้นอยู่กับขอบเขตการดำเนินงาน ลักษณะ และสภาวะแวดล้อมทางธุรกิจของ สง. นั้น ๆ โดยจะต้องครอบคลุมความเสี่ยงที่สำคัญทุกด้านที่อาจจะเกิดขึ้นและจะส่งผลกระทบต่อการดำเนินงานของ สง.

---

[4] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 66/2551 เรื่อง หลักเกณฑ์การกำกับแบบรวมกลุ่ม ลงวันที่ 3 สิงหาคม 2551 หน้า 51 ข้อ 104 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510356.pdf



1.2 ที่มาของความเสี่ยงด้านปฏิบัติการ

ในปัจจุบัน สง. จะดำเนินธุรกิจในลักษณะกลุ่มธุรกิจทางการเงิน ประกอบด้วยบริษัทแม่ บริษัทลูก หรือบริษัทร่วมที่ประกอบธุรกิจทางการเงินหรือธุรกิจสนับสนุนเพื่อสามารถให้บริการทางการเงินได้หลายรูปแบบและครบวงจร โดย **สง. จะคำนึงถึงความเสี่ยงที่เกิดจากการประกอบธุรกิจและปัจจัยต่างๆ ที่มากระทบต่อการดำเนินงาน ซึ่งปัจจัยที่มีผลกระทบต่อการดำเนินงานประกอบด้วย 4 ปัจจัย ได้แก่**

(1) **ปัจจัยด้านคน** ถือเป็นปัจจัยที่มีผลต่อการปฏิบัติงานซึ่งเกิดจากกระบวนการทำงานผิดพลาด หรือการควบคุมภายในไม่เพียงพออันอาจนำไปสู่การทุจริตทั้งภายในและภายนอก ดังนั้น การให้ความสำคัญในการคัดเลือกพนักงาน การอบรม และการพัฒนา จะทำให้องค์กรได้พนักงานที่มีคุณสมบัติ ประสบการณ์ และความสามารถที่เหมาะสมต่อการปฏิบัติงาน รวมทั้ง การส่งเสริมและสร้างจริยธรรมให้พนักงานตระหนักถึงหน้าที่ความ

รับผิดชอบต่อการปฏิบัติงาน อย่างไรก็ดี ในการปฏิบัติงานก็ควรพัฒนาระบบให้มีการป้องกันความผิดพลาดที่เกิดจากความพลั้งเผลอของบุคลากร เช่น ข้อมูลมีการสอบยันกัน

ตัวอย่างความผิดพลาดที่เกิดจากคน

ธนาคารได้นำระบบ Core Banking มาใช้แทนระบบเดิม ขณะที่ธนาคารยังไม่มีการอบรมการใช้ระบบดังกล่าวให้แก่พนักงาน ทำให้พนักงานยังไม่เข้าใจขั้นตอนการทำงานของระบบและกระบวนการทำงานที่ชัดเจน จึงทำให้เกิดข้อผิดพลาด

(2) **ปัจจัยด้านระบบงาน** หากระบบงานเกิดความเสียหาย ขัดข้อง หรือหยุดชะงัก รวมถึงความถูกต้องเชื่อถือได้ของระบบข้อมูลและระบบการสื่อสารภายในองค์กร การควบคุมการเข้าถึงระบบ การรักษาความปลอดภัยของระบบและข้อมูล ตลอดจนความสามารถในการนำระบบให้กลับมาทำงานได้ตามปกติหลังจากที่เกิดเหตุการณ์ฉุกเฉิน อันอาจมีผลกระทบต่อการปฏิบัติงานได้ ดังนั้น การที่มีระบบงานที่ดี จะช่วยสนับสนุนการปฏิบัติงานของ สง. ให้สะดวกรวดเร็วและมีประสิทธิภาพเพิ่มขึ้น โดยระบบงานที่ใช้อยู่ ควรมีความเหมาะสมกับขนาดและความซับซ้อนของ สง.

ตัวอย่างความผิดพลาดที่เกิดจากระบบงาน

ธนาคารได้เปลี่ยนระบบ Core Banking โดยเชื่อมโยงระบบการทำงานของธนาคาร ทั้งระบบภายใน (Back office) และระบบบริการลูกค้า (Front office) แต่ระบบยังไม่สมบูรณ์ จึงส่งผลให้เกิดความผิดพลาด เช่น โปรแกรมคำนวณดอกเบี้ยไม่ถูกต้อง หรือระบบสินเชื่อที่อยู่อาศัยไม่ตัดบัญชีการชำระหนี้ของลูกค้า เป็นต้น

(3) **ปัจจัยด้านกระบวนการทำงาน** หาก สง. ไม่มีกระบวนการ / ขั้นตอนการทำงานหรือจุดควบคุมในแต่ละธุรกรรมที่อาจก่อให้เกิดความเสี่ยงให้เป็นรูปธรรมและสามารถนำไปปฏิบัติงานได้ อาจก่อให้เกิดความเสียหายทั้งในรูปของตัวเงิน เช่น การเปรียบเทียบปรับหรือการถูกฟ้องร้องจากการไม่ปฏิบัติตามกฎหมาย กฎระเบียบ หรือข้อบังคับที่เกี่ยวข้อง เป็นต้น หรือที่ไม่ใช่ตัวเงิน เช่น ด้านชื่อเสียง เป็นต้น ดังนั้น หน่วยงานควรกำหนดกระบวนการ / ขั้นตอนการทำงานตามนโยบาย กฎเกณฑ์ ระเบียบและข้อบังคับในการปฏิบัติงาน เช่น การมีระเบียบและคู่มือการปฏิบัติงาน เป็นต้น ให้ชัดเจนและง่ายต่อการปฏิบัติ และสอดคล้องกับปริมาณและความซับซ้อนของธุรกรรม เพื่อให้เกิดความมั่นใจว่า กระบวนการทำงานมีประสิทธิภาพ เหมาะสมและ

สามารถบรรลุเป้าหมายตามกลยุทธ์ของ สง.

ตัวอย่างความผิดพลาดที่เกิดจากกระบวนการทำงาน

ธนาคารได้มีการออกระเบียบปฏิบัติการทำธุรกรรมนอกสถานที่ทำการของธนาคาร แต่ยังไม่มีคู่มือการปฏิบัติงานที่ชัดเจน ทำให้พนักงานปฏิบัติงานไม่ครบถ้วนตามที่กำหนด และอาจก่อให้เกิดความเสียหายต่อธนาคาร

(4) **ปัจจัยที่ไม่ปฏิบัติตามกฎหมายและที่เกิดจากเหตุการณ์ภายนอก** ถือเป็นอีกหนึ่งปัจจัยที่ส่งผลกระทบต่อการปฏิบัติงาน เนื่องจากเป็นปัจจัยที่อยู่เหนือความคาดหมาย หรือการควบคุมของ สง. เช่น ด้านการเมือง ด้านภัยธรรมชาติ การเปลี่ยนแปลงหลักเกณฑ์ของกฎหมาย หรือกฎเกณฑ์ข้อบังคับของทางการ เป็นต้น ดังนั้น จึงมีความจำเป็นต้องมีการวิเคราะห์และระบุความเสี่ยง รวมทั้งกำหนดมาตรการรองรับเพื่อลดความสูญเสียให้อยู่ในระดับที่ยอมรับได้

ตัวอย่างความไม่สงบของบ้านเมืองจากการประท้วงซึ่งเกิดจากเหตุการณ์ภายนอก

เกิดเกตุการณ์ประท้วงของประชาชนในบริเวณใกล้เคียงกับสาขาของธนาคาร ซึ่งทำให้ไม่สามารถให้บริการแก่ลูกค้าได้ตามปกติ ทำให้ธุรกรรมของสาขาต้องหยุดชะงักหรือเสียหายได้ โดยเฉพาะอย่างยิ่ง หากธนาคารไม่มีแผนฉุกเฉินรองรับเหตุการณ์ดังกล่าว

1.3 ประเภทของความเสี่ยงด้านปฏิบัติการ

ประเภทความเสี่ยงด้านปฏิบัติการ **จำแนกออกได้ 7 ประเภท** ดังนี้

(1) **ความเสี่ยงจากการทุจริตภายใน** (Internal fraud) เป็นความเสี่ยงที่เกิดขึ้นจากการทุจริตของบุคคลภายในองค์กรที่กระทำหรือละเว้นการกระทำโดยเจตนา เพื่อให้ผลประโยชน์ที่เกิดขึ้นจากการทุจริตดังกล่าวตกแก่ตนเองและพวกพ้อง เช่น การทำธุรกรรมโดยไม่ได้รับอนุญาต การปลอมแปลงเอกสาร การยักยอก หรือ การรับสินบน เป็นต้น

ตัวอย่างการทุจริตภายใน

ธนาคารขาดทุนจากการเก็งกำไรในตลาดตราสารอนุพันธ์ เนื่องจากเจ้าหน้าที่ค้าเงินมีอำนาจทำรายการ Trading และควบคุมงาน Back office ซึ่งเป็นการเปิดโอกาสให้สามารถปกปิดหรือแก้ไขรายการทุจริตได้ โดยสามารถบันทึกบัญชี กระทบยอดบัญชี จัดทำรายงานทางการเงิน และสร้างบัญชีลับพิเศษเพื่อบันทึกการปกปิดรายการความเสียหายจากการเก็งกำไร ซึ่งสาเหตุของปัญหา สรุปได้ดังนี้:

- ขาดการควบคุมภายในที่ดี เช่น การแบ่งแยกหน้าที่
- ผู้บังคับบัญชาขาดการตรวจตราดูแลอย่างทั่วถึง
- ไม่มีการตรวจสอบภายใน

(2) **ความเสี่ยงจากการทุจริตภายนอก** (External fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายนอกองค์กรที่กระทำการโดยมิชอบด้วยกฎหมาย ซึ่งก่อให้เกิดความเสียหายโดยตรงต่อ สง. เช่น การปลอมแปลงเช็ค การปลอมแปลงเอกสารทางการเงิน การฉ้อโกง การโจรกรรม และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Hacking) เป็นต้น

(3) **ความเสี่ยงจากการจ้างงาน และความปลอดภัยในสถานที่ปฏิบัติงาน** (Employment practices and workplace safety) เป็นความเสี่ยงที่เกิดขึ้นจากกระบวนการจ้างงาน (Contract out) ที่ไม่เหมาะสม การจ่ายค่าตอบแทน หรือการปฏิบัติต่อพนักงานอย่างไม่เป็นธรรม รวมถึงการกำหนดมาตรการรักษาความปลอดภัยในการปฏิบัติงาน และการควบคุมสภาพแวดล้อมในการปฏิบัติงานที่ไม่เพียงพอ จนส่งผลกระทบต่อสุขภาพของพนักงาน อันเนื่องมาจากโรคภัยหรือได้รับบาดเจ็บจากอุบัติเหตุอันเนื่องมาจากการปฏิบัติงานได้ ซึ่งอาจก่อให้เกิดการถูกฟ้องร้อง การลาออก หรือการหยุดงานประท้วงได้

(4) **ความเสี่ยงจากการปฏิบัติงานที่ไม่เหมาะสมเกี่ยวกับลูกค้า ผลิตภัณฑ์และวิธีปฏิบัติในการดำเนินธุรกิจ** (Clients, products and business practices) เป็นความเสี่ยงที่เกิดขึ้นจากวิธีปฏิบัติในการดำเนินธุรกิจ กระบวนการออกผลิตภัณฑ์ และการเข้าถึงข้อมูลลูกค้าที่ไม่เหมาะสม ไม่เป็นไปตามกฎหมาย ระเบียบและกฎเกณฑ์อื่นที่เกี่ยวข้อง เช่น การทำธุรกรรมที่ละเมิดกฎหมาย การดำเนินธุรกรรมที่ไม่ได้รับอนุญาต การทำธุรกรรมที่เกี่ยวข้องกับการฟอกเงิน และการที่ สง. นำข้อมูลความลับของลูกค้าไปหาผลประโยชน์ เป็นต้น

ตัวอย่างการปฏิบัติงานไม่เหมาะสมของธนาคารต่อลูกค้า

ธนาคารขาดทุนจากตราสารหนี้ ซึ่งผู้บริหารของธนาคารได้ทำการซื้อขายตราสารหนี้ที่ผิดกฎหมาย โดยการขายตราสารหนี้ในบัญชี Bankers Trust เพื่อนำไปชดเชยความเสียหายที่เกิดขึ้น พร้อมทั้งปลอมแปลง Statement ของบัญชีดังกล่าว เพื่อไม่ให้แสดงรายการตราสารหนี้ที่ขาย รวมทั้งปลอมแปลงสลิปรายการซื้อขายตราสารหนี้และเอกสารอื่นที่เกี่ยวข้อง เมื่อลูกค้าต้องการได้รับดอกเบี้ยจากตราสารหนี้ที่ขาย โดยการ Settle บัญชีลูกค้าเหล่านั้น

(5) **ความเสี่ยงด้านความปลอดภัยของทรัพย์สิน** (Damage to physical assets) เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ทรัพย์สินของ สง. อันเนื่องมาจากอุบัติภัยต่างๆ เช่น อุบัติเหตุ อัคคีภัย ภัยธรรมชาติ การทำลายทรัพย์สิน การจลาจล การก่อความไม่สงบทางการเมือง การก่อวินาศภัย เป็นต้น

(6) **ความเสี่ยงจากการขัดข้องหรือหยุดชะงักของระบบงานหรือระบบคอมพิวเตอร์** (Business disruption and system failures) เป็นความเสี่ยงที่เกิดขึ้นจากระบบงานที่ผิดปกติ หรือการหยุดทำงานของระบบคอมพิวเตอร์ หรือการเปลี่ยนแปลงระบบงาน เช่น การหยุดให้บริการ ความเสียหายจากความไม่สอดคล้องกัน หรือความแตกต่างของระบบงานที่เกิดจากการควบรวมกิจการ ความล้มเหลว หรือความบกพร่องของระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย รวมถึงการใช้เครื่องมือและเทคโนโลยีที่ไม่เหมาะสม ล้าสมัย และไม่มีประสิทธิภาพ เป็นต้น

(7) **ความเสี่ยงจากกระบวนการทำงาน** (Execution, delivery and process management) เป็นความเสี่ยงที่เกิดขึ้นจากความผิดพลาดในวิธีปฏิบัติงาน (Methodology) ความผิดพลาดของระบบการปฏิบัติงาน (Procedure) หรือความผิดพลาดจากการปฏิบัติงานของพนักงานภายใน และการจ้างพนักงานภายนอก (Outsourcing) เช่น การนำเข้าข้อมูลผิดพลาด การประเมินมูลค่าหลักประกันไม่ถูกต้อง การไม่ปฏิบัติตามสัญญาของผู้รับจ้าง การขาดความรู้ความเข้าใจในการปฏิบัติงานและการใช้งานระบบคอมพิวเตอร์ของพนักงาน การปรับปรุงกระบวนการทำงานที่ไม่เหมาะสม รวมถึงการจัดทำนิติกรรมสัญญา และเอกสารทางกฎหมายที่ไม่สมบูรณ์ ทำให้ไม่สามารถใช้บังคับได้ตามกฎหมาย เป็นต้น

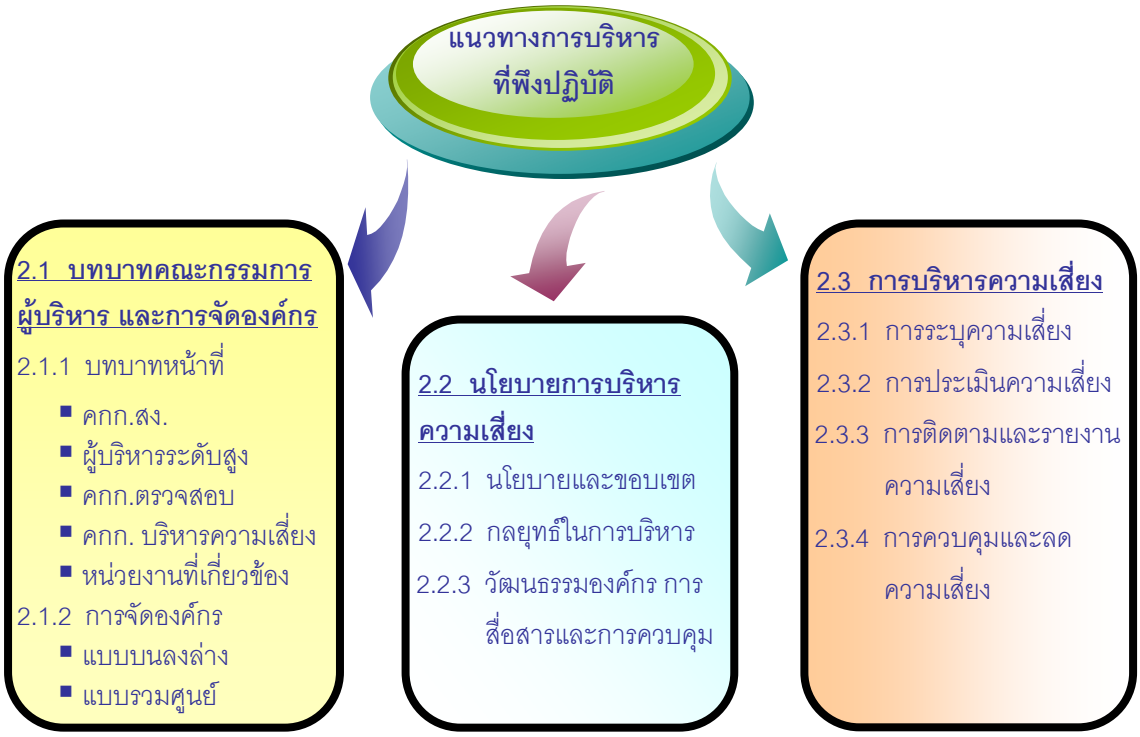
ตัวอย่างกระบวนการทำงานที่ไม่เหมาะสม

ธนาคารขาดทุนจากการทำธุรกรรมสัญญาซื้อขายล่วงหน้าและสัญญาสิทธิทองคำ โดยหัวหน้าเทรดเดอร์ที่ดูแลด้านการซื้อขายทองคำ เป็นบุคคลที่ "มุ่งแต่งาน" จึงได้รับความไว้วางใจ พร้อมทั้งมีการละเว้นการตรวจสอบ จึงทำให้หัวหน้าเทรดเดอร์ ฯ สามารถสร้างบัญชีเท็จ โดยบัญชีหนึ่งแสดงผลกำไรจากการซื้อขายทองคำเป็นจำนวนมาก รวมทั้งสัญญาล่วงหน้าและสัญญาสิทธิทองคำ แต่อีกบัญชีหนึ่งแสดงผลขาดทุนเป็นจำนวนหลายพันล้านดอลลาร์ สาเหตุของการทุจริต เนื่องจากการไม่ปฏิบัติตามกฎระเบียบข้อบังคับของธนาคาร และ

1. ขาดการแบ่งแยกหน้าที่ที่ดี
2. มอบหมายอำนาจให้กับบุคคลใดบุคคลหนึ่งมากเกินไป
3. รายงานทางการเงินไม่สามารถเชื่อถือได้ รวมทั้งการตรวจสอบไม่เพียงพอ
4. ขาดการตรวจสอบภายในที่มีประสิทธิภาพ
5. ขาดการบริหารการลงทุนเพื่อให้เกิดการกระจายความเสี่ยง

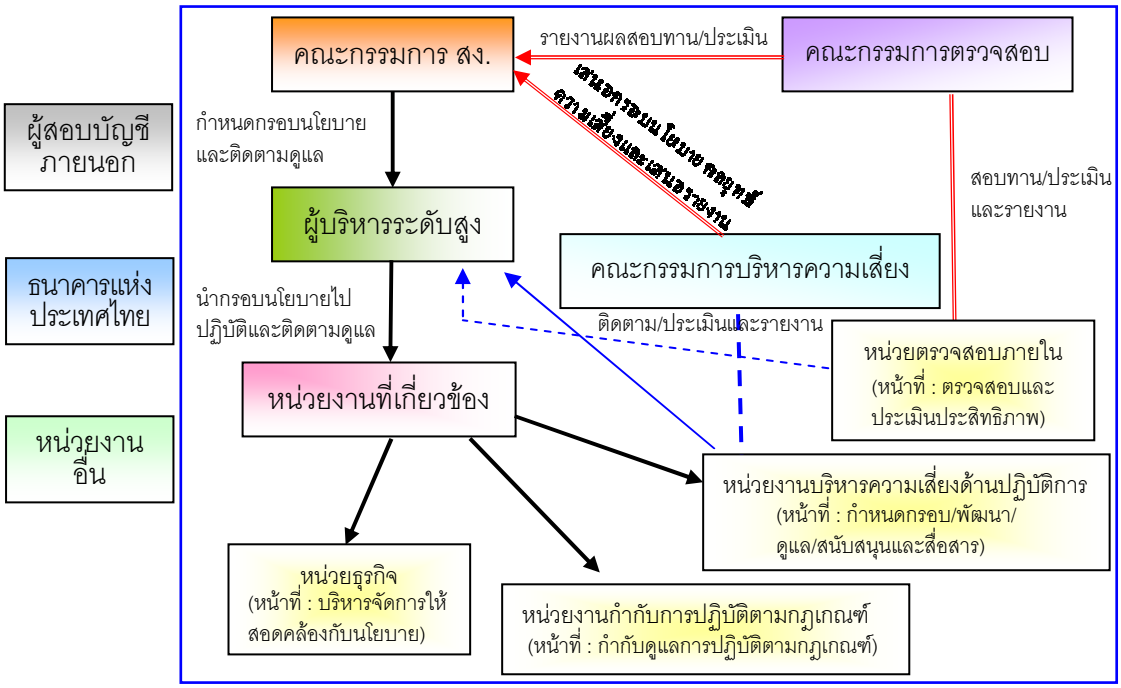
ส่วนที่ 2 แนวทางการบริหารความเสี่ยงด้านปฏิบัติการที่พึงปฏิบัติ

ความเสี่ยงด้านปฏิบัติการครอบคลุมถึงเหตุการณ์ความเสียหาย (Loss incidents) ที่อาจเกิดจากการดำเนินงานผิดพลาดของหน่วยธุรกิจ (Business unit) และอาจเกิดได้กับทุกระดับของการบริหารงาน (Management) นอกจากนี้ ความเสี่ยงด้านปฏิบัติการที่เกิดขึ้นกับหน่วยธุรกิจหนึ่ง อาจส่งผลกระทบและก่อให้เกิดความเสียหายให้กับหน่วยธุรกิจอื่นอย่างต่อเนื่องกันได้ ดังนั้น สง. จำเป็น ต้องมีระบบการบริหารความเสี่ยงด้านปฏิบัติการที่มีประสิทธิภาพ และเหมาะสมกับสภาวะแวดล้อมในการดำเนินธุรกิจ เพื่อให้ สง. มีความมั่นใจว่าสามารถจัดการกับความเสี่ยงด้านปฏิบัติการได้ โดยไม่ส่งผลกระทบต่อผู้ที่เกี่ยวข้องหรือผู้มีส่วนได้เสีย (Stakeholders) ในการดำเนินธุรกิจ ซึ่ง**ระบบการบริหารความเสี่ยงด้านปฏิบัติการที่ดีนั้น ควรประกอบด้วย 3 องค์ประกอบหลัก** ได้แก่



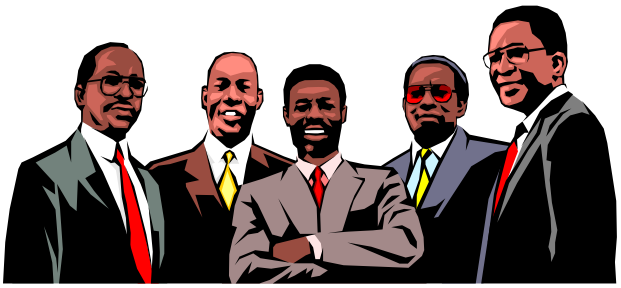
2.1 บทบาทคณะกรรมการ ผู้บริหารระดับสูง และการจัดองค์กรด้านปฏิบัติการ [5]

สรุปภาพรวมบทบาทและหน้าที่ของคณะกรรมการ ผู้บริหารระดับสูง และการจัดองค์กรด้านปฏิบัติการ ดังนี้



2.1.1 บทบาทหน้าที่

- **คณะกรรมการสถาบันการเงิน**



(1) ให้ความสำคัญกับความเสี่ยงด้านปฏิบัติการในฐานะที่เป็นความเสี่ยงหลัก โดยในวาระการประชุมคณะกรรมการและผู้บริหารระดับสูง จะต้องบรรจุเรื่องความเสี่ยงด้านปฏิบัติการไว้อย่างสม่ำเสมอ

[5] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการ ลงวันที่ 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510385.pdf

(2) กำหนดกรอบนโยบาย กลยุทธ์ คำจำกัดความของความเสี่ยงด้านปฏิบัติการที่เหมาะสมกับองค์กร ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และแผนงานการบริหารความเสี่ยงด้านปฏิบัติการ โดยจะต้องมีการทบทวนกรอบนโยบายอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงกรอบนโยบายอย่างมีนัยสำคัญ

(3) จัดให้มีหน่วยงานบริหารความเสี่ยงด้านปฏิบัติการแยกจากหน่วยงานอื่นและหน่วยงานตรวจสอบภายในอย่างชัดเจน โดยมีหน้าที่นำเสนอนโยบาย แผนงานและกระบวนการบริหารความเสี่ยงต่อคณะกรรมการ สง. เพื่อพิจารณาอนุมัติ

(4) พิจารณาอนุมัตินโยบาย แผนงานและกระบวนการบริหารความเสี่ยงด้านปฏิบัติการตามที่หน่วยงานบริหารความเสี่ยงด้านปฏิบัติการนำเสนอ

(5) จัดให้มีโครงสร้างการบริหารขององค์กรอย่างเหมาะสมและเอื้อต่อการบริหารความเสี่ยงด้านปฏิบัติการให้สอดคล้องกับหลักการควบคุมภายในที่ดี

(6) ส่งเสริมให้เกิดธรรมาภิบาลในองค์กรเพื่อสร้างความโปร่งใสและเป็นธรรม

(7) จัดให้มีผู้สอบบัญชีภายนอกที่มีคุณสมบัติเหมาะสม ทำหน้าที่ตรวจสอบรับรองงบการเงิน

(8) ดูแลให้ สง. มีการปฏิบัติตามกฎหมาย กฎระเบียบและกฎเกณฑ์อื่นที่เกี่ยวข้อง เช่น พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ประกาศหรือหนังสือเวียนของธนาคารแห่งประเทศไทย ข้อกำหนดของตลาดหลักทรัพย์แห่งประเทศไทยและสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ระเบียบข้อบังคับที่เกี่ยวข้องกับมาตรการป้องกันการฟอกเงินและการก่อการร้าย เป็นต้น

- **ผู้บริหารระดับสูง**

(1) นำกรอบนโยบายความเสี่ยงด้านปฏิบัติการมาจัดทำเป็นระเบียบ กฎเกณฑ์ หรือขั้นตอนการปฏิบัติงานในองค์กร และสื่อสารให้พนักงานทุกคนในองค์กรเข้าใจและตระหนักถึงความสำคัญและหน้าที่ความรับผิดชอบเกี่ยวกับความเสี่ยงด้านปฏิบัติการ

(2) ควบคุมดูแลให้มีการปฏิบัติตามนโยบาย ระเบียบ กฎเกณฑ์ และกระบวนการปฏิบัติงานที่กำหนดขึ้นอย่างเคร่งครัด

(3) กำหนดหน้าที่ความรับผิดชอบ สายการบังคับบัญชาหรือสายการรายงานในแต่ละ

หน่วยงานอย่างชัดเจน โดยหัวหน้าหน่วยงานควรเป็นผู้รับผิดชอบต่อความเสี่ยงด้านปฏิบัติการในหน่วยงานนั้น เนื่องจากเป็นผู้รู้และเข้าใจความเสี่ยงที่มีอยู่ในหน่วยงานดีที่สุด

- **คณะกรรมการตรวจสอบ** [6]

สง. จะต้องจัดตั้งคณะกรรมการตรวจสอบซึ่งประกอบด้วยกรรมการอิสระอย่างน้อย 3 คน โดยอย่างน้อยหนึ่งคนต้องมีความรู้และประสบการณ์เพียงพอที่จะสามารถทำหน้าที่ในการสอบทานความน่าเชื่อถือของงบการเงินได้

คณะกรรมการตรวจสอบมีบทบาทหน้าที่ความรับผิดชอบที่สำคัญ คือ

(1) สอบทานให้ สง. มีการรายงานทางการเงินอย่างถูกต้องและเพียงพอ

(2) สอบทานและประเมินผลให้ สง. มีระบบควบคุมภายในและการตรวจสอบภายในที่เหมาะสมและมีประสิทธิผล

(3) สอบทานให้ สง. ปฏิบัติตาม พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 กฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ ข้อกำหนดของตลาดหลักทรัพย์ ข้อกำหนดของธนาคารแห่งประเทศไทย หรือกฎหมายที่เกี่ยวข้องกับธุรกิจของสถาบันการเงิน เช่น พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต เป็นต้น

(4) พิจารณา คัดเลือก เสนอแต่งตั้งและกำหนดค่าตอบแทนผู้สอบบัญชีของ สง.

(5) พิจารณาการเปิดเผยข้อมูลของ สง. โดยเฉพาะในกรณีที่เกิดรายการที่เกี่ยวโยงกันหรือรายการที่อาจมีความขัดแย้งทางผลประโยชน์ให้มีความถูกต้องและครบถ้วน

(6) จัดทำรายงานการกำกับดูแลกิจการของคณะกรรมการตรวจสอบโดยเปิดเผยไว้ในรายงานประจำปี

(7) กำหนดหน้าที่ของคณะกรรมการตรวจสอบตลอดจนการเปลี่ยนแปลงในองค์ประกอบรวมทั้งการเปลี่ยนแปลงที่มีนัยสำคัญต่อการปฏิบัติงานของคณะกรรมการตรวจสอบไว้อย่างชัดเจนเป็นลายลักษณ์อักษรตามที่ได้รับอนุมัติจากคณะกรรมการ สง. และต้องเปิดเผยให้ผู้ถือหุ้นทราบในรายงานประจำปี

---

[6] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 60/2551 เรื่อง ธรรมาภิบาลของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510350.pdf

(8) รายงานต่อคณะกรรมการของ สง. เพื่อดำเนินการปรับปรุงแก้ไขภายในเวลาที่คณะกรรมการตรวจสอบเห็นสมควรหากคณะกรรมการตรวจสอบได้ตรวจพบหรือมีข้อสงสัยในรายการหรือการกระทำ ดังต่อไปนี้

- รายการที่เกิดความขัดแย้งทางผลประโยชน์
- การทุจริต หรือพบรายการที่ผิดปกติหรือข้อบกพร่องที่สำคัญในระบบควบคุมภายใน
- หากมีการฝ่าฝืนกฎหมาย หรือกฎเกณฑ์ข้อบังคับของทางการ และคณะกรรมการของ สง. หรือผู้บริหารไม่ได้ดำเนินการให้มีการปรับปรุงแก้ไขภายในระยะเวลาที่คณะกรรมการตรวจสอบกำหนด คณะกรรมการตรวจสอบจะต้องเปิดเผยการกระทำดังกล่าวไว้ในรายงานประจำปีและรายงานต่อ ธนาคารแห่งประเทศไทย

(9) ปฏิบัติการอื่นใดตามที่คณะกรรมการของ สง. มอบหมาย ด้วยความเห็นชอบของคณะกรรมการตรวจสอบ

นอกจากนี้ คณะกรรมการตรวจสอบควรมีการสอบทานบทบาทหน้าที่และกำหนดวาระการดำรงตำแหน่งของกรรมการในคณะกรรมการตรวจสอบด้วย

- **คณะกรรมการบริหารความเสี่ยง** [7]

(1) กำหนดกรอบนโยบาย และแนวทางการปฏิบัติเกี่ยวกับความเสี่ยงให้สอดคล้องกับกลยุทธ์ของ สง. เพื่อเสนอคณะกรรมการ สง. พิจารณาในเรื่องของการบริหารความเสี่ยงโดยรวม ซึ่งต้องครอบคลุมความเสี่ยงด้านต่าง ๆ ที่สำคัญ เช่น ความเสี่ยงด้านเครดิต ด้านตลาด ด้านสภาพคล่อง และด้านปฏิบัติการ เป็นต้น

(2) กำหนดกลยุทธ์ให้สอดคล้องกับนโยบายการบริหารความเสี่ยง โดยสามารถ ระบุ วัด ติดตาม รายงาน และควบคุมความเสี่ยงของ สง. ให้อยู่ในระดับที่เหมาะสม

(3) ทบทวนความเพียงพอของนโยบายและระบบการบริหารความเสี่ยง รวมถึงความมีประสิทธิผลของระบบการปฏิบัติงานและการปฏิบัติตามนโยบายที่กำหนด โดยพิจารณา

[7] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 60/2551 เรื่อง ธรรมาภิบาลของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510350.pdf

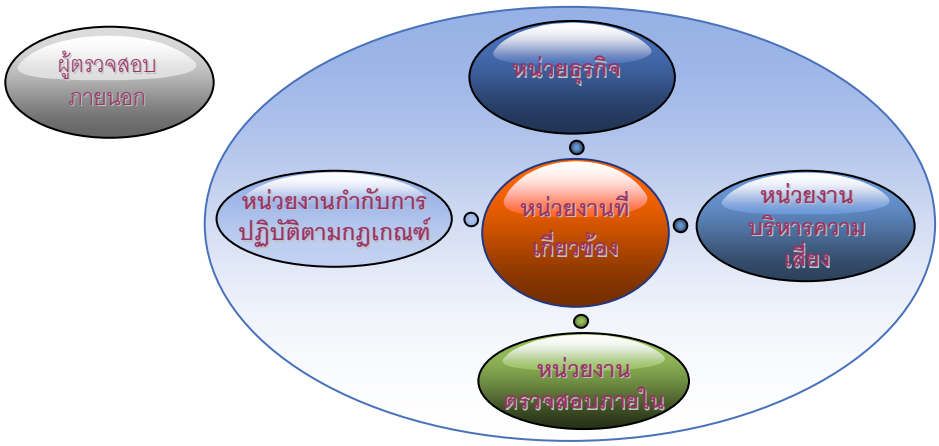
อนุมัติการจัดระดับความเสี่ยง กระบวนการติดตามความเสี่ยง และจัดให้มีมาตรการป้องกันแก้ไขและควบคุมความเสี่ยงอย่างเหมาะสม กำกับให้มีการปฏิบัติตามนโยบายการบริหารความเสี่ยง พิจารณาเห็นชอบ และอนุมัติกรอบการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan)

(4) รายงานต่อคณะกรรมการตรวจสอบอย่างสม่ำเสมอในเรื่องที่ต้องดำเนินการปรับปรุงแก้ไขเพื่อให้สอดคล้องกับนโยบายและกลยุทธ์ที่กำหนด รวมถึงการปฏิบัติหน้าที่อื่นๆ ตามที่ได้รับมอบหมายจากคณะกรรมการตรวจสอบ

(5) ดูแลทรัพยากรที่ใช้ในการบริหารความเสี่ยงด้านปฏิบัติการให้เพียงพอ เช่น ให้มีบุคลากรทั้งของหน่วยงานบริหารความเสี่ยงและหน่วยงานที่ทำหน้าที่ควบคุมความเสี่ยงเพียงพอ และปรับปรุงระบบงานให้ทันสมัย เพื่อรองรับการบริหารความเสี่ยง เป็นต้น

ทั้งนี้ ประธานคณะกรรมการบริหารความเสี่ยงควรเป็นผู้ที่มีตำแหน่งเป็นประธานเจ้าหน้าที่บริหาร หรือผู้ซึ่งดำรงตำแหน่งเทียบเท่าที่กำหนดชื่อเป็นอย่างอื่น

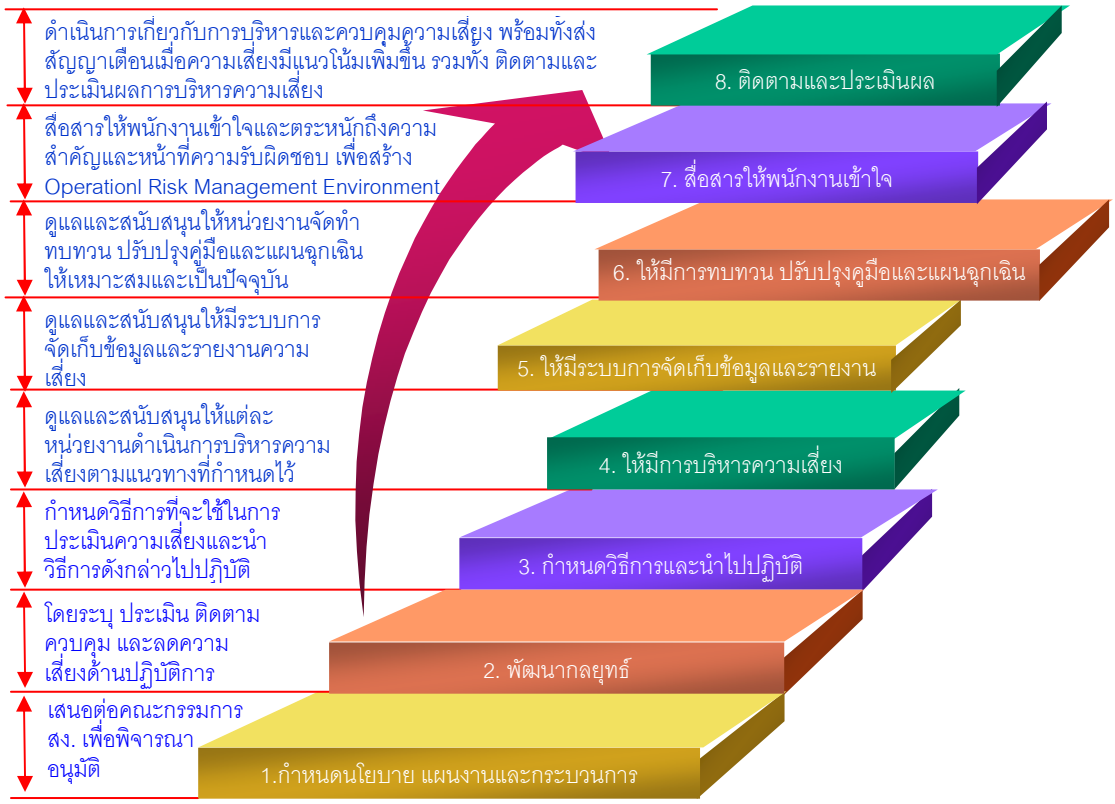
- **หน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการ**



(1) หน่วยธุรกิจ (Business Unit) มีบทบาท หน้าที่ และความรับผิดชอบในการบริหารจัดการความเสี่ยงด้านปฏิบัติการให้สอดคล้องกับนโยบาย รวมทั้งการจัดเก็บและรายงานข้อมูลความเสียหายที่เกิดขึ้น (Loss data) ของแต่ละผลิตภัณฑ์ บริการทางการเงิน หรือระบบงานที่อยู่ในความรับผิดชอบของหน่วยงาน รวมถึงการประเมินโอกาสหรือความถี่ (Likelihood/Frequency) และระดับความเสียหาย (Severity) ของเหตุการณ์ที่อาจเกิดขึ้นประกอบกัน

ซึ่งอาจจะทำในรูปแบบของการประเมินตนเอง เช่น Risk and Control Self Assessment, Risk Mapping และ Risk Indicators เป็นต้น

(2) หน่วยงานบริหารความเสี่ยงด้านปฏิบัติการมีบทบาท หน้าที่ และความรับผิดชอบ ดังนี้



(3) หน่วยงานตรวจสอบภายใน [8]

ระบบการควบคุมภายใน (Internal Control Systems) และการตรวจสอบภายใน (Internal Audit) เป็นส่วนสำคัญอย่างยิ่งของกระบวนการกำกับดูแลกิจการที่ดี โดยผู้ตรวจสอบภายในมีบทบาทสำคัญในการประเมินประสิทธิผล และยกระดับมาตรฐานของระบบการควบคุมของ สง. ซึ่งเป็นสิ่งจำเป็นอย่างยิ่งในการเสริมสร้างความมั่นคงของระบบการเงินโดยรวม และความเหมาะสมของโครงสร้างการตรวจสอบภายในก็เป็นสิ่งสำคัญ ดังนั้น สง. ควรจัดให้มีหน่วยงานตรวจสอบภายในที่เป็นอิสระ เหมาะสมกับขนาด ลักษณะ และขอบเขตของธุรกรรมของ สง. เพื่อทำหน้าที่สอบทาน

[8] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง แนวปฏิบัติงานตรวจสอบภายในของสถาบันการเงิน ลงวันที่. 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510388.pdf

และทดสอบระบบการควบคุมและระบบการบริหารความเสี่ยง โดยมีองค์ประกอบการตรวจสอบภายในดังต่อไปนี้

ก. หน้าที่และความรับผิดชอบของฝ่ายบริหาร มีการดำเนินการที่เกี่ยวกับ

1. จัดตั้งหน่วยงานตรวจสอบภายในที่เหมาะสม รวมทั้ง กำหนดวัตถุประสงค์ อำนาจหน้าที่ ความรับผิดชอบของหน่วยงาน และนโยบายการตรวจสอบที่ชัดเจน
2. ถ่ายทอดให้องค์กรทราบและส่งเสริมความเป็นอิสระและสถานภาพของผู้ตรวจสอบ
3. จัดสรรบุคลากรอย่างพอเพียงและเหมาะสมแก่หน่วยงานตรวจสอบภายใน

ข. ความเป็นอิสระและความมีใจเป็นอิสระ โดยผู้ตรวจสอบภายในสามารถใช้วิจารณญาณที่เป็นกลางและปราศจากอคติ ซึ่งอาจพิจารณาได้จาก

- สถานภาพในองค์กร

1. อยู่ในระดับที่สูงพอ และเป็นอิสระจากหน่วยงานอื่น เพื่อให้ผู้ตรวจสอบสามารถปฏิบัติหน้าที่ได้ตามวัตถุประสงค์ นอกจากนี้ ตำแหน่งหัวหน้าหน่วยงานตรวจสอบภายในต้องมีสถานภาพเทียบเท่ากับหัวหน้าหน่วยงานสำคัญอื่นๆ ในองค์กร

2. คณะกรรมการตรวจสอบหรือคณะกรรมการ สง.แต่งตั้ง โยกย้าย กำหนดค่าตอบแทน ประเมินผลงาน และถอดถอนหัวหน้าหน่วยงานตรวจสอบภายในได้
3. หัวหน้าหน่วยงานตรวจสอบภายในขึ้นตรงต่อคณะกรรมการตรวจสอบตามสายบังคับบัญชา และสามารถเข้าพบเพื่อรายงานผลการตรวจสอบได้ตลอดเวลา
4. หัวหน้าหน่วยงานตรวจสอบภายในกำหนดหน้าที่ความรับผิดชอบของบุคลากรหรือส่วนงานในหน่วยงานตรวจสอบภายใน พร้อมทั้งนำเสนอต่อผู้บริหาร และคณะกรรมการตรวจสอบหรือคณะกรรมการ สง. เพื่อขอความเห็นชอบ
5. ผู้ตรวจสอบภายในต้องไม่มีหน้าที่รับผิดชอบในการปฏิบัติงานหรือระบบงานใดๆ นอกเหนือจากงานตรวจสอบ
6. ผู้ตรวจสอบภายในสามารถเข้าถึงข้อมูล ทรัพย์สิน บุคลากร และสถานที่ทำการเพื่อปฏิบัติงานตรวจสอบได้โดยไม่มีข้อจำกัด หากมี ผู้ตรวจสอบภายในต้องรายงานคณะกรรมการตรวจสอบเป็นลายลักษณ์อักษรทันที เพื่อคณะกรรมการตรวจสอบจะได้ประสานงานกับฝ่ายบริหารต่อไป
7. หน่วยงานตรวจสอบภายในต้องได้รับข้อมูล เอกสารที่จำเป็นในการตรวจสอบ นอกจากนี้ หากหน่วยงานใดตรวจพบข้อบกพร่องร้ายแรง หรือเกิดความสูญเสียอย่างมาก หรือมีเหตุอันควรสงสัยว่าจะเกิดความสูญเสียอย่างมากในหน่วยงานของตน หน่วยงานนั้นจะต้องรายงานหน่วยงานตรวจสอบภายในทันที
8. ผู้ตรวจสอบภายในต้องมีความรู้และประสบการณ์ในขอบเขตและระดับความรับผิดชอบของงาน รวมทั้ง ควรเข้าใจในเรื่องที่ตรวจสอบ ระเบียบปฏิบัติ โครงสร้างองค์กร การดำเนินธุรกิจทั่วไป และความเสี่ยงของ สง. รวมถึงมีการติดตามและปรับใช้มาตรฐานบัญชี หลักเกณฑ์ที่เกี่ยวข้องให้เป็นปัจจุบัน

- <u>ความมีใจเป็นอิสระ</u>

1. หลีกเลี่ยงเหตุการณ์ขัดแย้งทางผลประโยชน์ที่เกิดจากความสัมพันธ์ทั้งเรื่องงานและเรื่องส่วนตัวหรือกิจกรรมที่ตรวจสอบ
2. ไม่ควรได้รับมอบหมายให้ตรวจสอบงานที่เคยเกี่ยวข้องก่อนเป็นผู้ตรวจสอบจนกว่ามีการตรวจสอบคั่นก่อนหน้า หรือเวลาล่วงมาไม่ต่ำกว่า 1 ปี

ค. ความรอบรู้ในวิชาชีพ โดยผู้ตรวจสอบภายในควรมีคุณสมบัติที่เหมาะสมและได้รับการฝึกอบรมที่จำเป็น รวมทั้งการศึกษาในวิชาชีพอย่างต่อเนื่อง เพื่อให้สามารถปรับตัวได้ทันกับพัฒนาการในภาคการเงิน รวมทั้งครอบคลุมในเรื่องต่อไปนี้

1. ทรัพยากร ควรประมาณการทรัพยากรตามขนาดและความซับซ้อนในการดำเนินงาน นอกจากนี้ ควรจัดทำเกณฑ์ที่เหมาะสมในการคัดเลือกเจ้าหน้าที่ตรวจสอบภายใน
2. คุณสมบัติ ความรู้ ประสบการณ์ และความชำนาญ ควรพิจารณาจากประวัติการศึกษา ความรู้เกี่ยวกับธุรกิจ องค์กร และการปรับใช้มาตรฐานวิชาชีพการตรวจสอบภายในที่เป็นปัจจุบัน
3. การกำกับดูแล ควรจัดทำตารางเวลาที่เหมาะสมสำหรับงานตรวจสอบแต่ละงาน ซึ่งพิจารณาจากความซับซ้อนของงาน
4. จรรยาบรรณ ควรจัดทำเป็นลายลักษณ์อักษรโดยผู้ตรวจสอบภายในต้องระมัดระวังในการปฏิบัติหน้าที่และความรับผิดชอบเยี่ยงผู้ประกอบวิชาชีพ
5. การฝึกอบรม ควรจัดทำแผนการฝึกอบรมอย่างต่อเนื่องแก่ผู้ตรวจสอบภายในเพื่อยกระดับมาตรฐานการตรวจสอบและความชำนาญทางเทคนิค

ง. ความสัมพันธ์และการติดต่อสื่อสาร ถือเป็นอีกปัจจัยหนึ่งที่ผู้ตรวจสอบภายในควรคำนึงถึง และควรมีการติดต่อประสานงานกับผู้ที่เกี่ยวข้อง ดังนี้

1. ผู้บริหาร ควรร่วมมือระหว่างผู้บริหารกับผู้ตรวจสอบภายใน โดยการปรึกษาหารือกับผู้บริหารอาจนำไปสู่การค้นพบจุดที่น่าเป็นห่วง และควรใช้ความชำนาญพิเศษให้คำปรึกษาที่เพิ่มคุณค่าแก่ผู้บริหาร
2. ผู้รับการตรวจ ควรสร้างความสัมพันธ์ที่ดีระหว่างผู้ตรวจสอบภายในกับผู้รับการตรวจสอบ เพื่อให้ได้รับความร่วมมือในการตรวจสอบ
3. ผู้สอบบัญชีภายนอก ควรมีการประชุมร่วมกันเป็นระยะๆ เช่น แผนการตรวจสอบ การจัดลำดับก่อนหลังในการตรวจสอบ เพื่อหลีกเลี่ยงการทำงานที่ซ้ำซ้อนกัน
4. ธนาคารแห่งประเทศไทยและหน่วยงานกำกับดูแลของรัฐ ผู้ตรวจสอบภายในต้องรายงานเรื่องที่ส่งผลกระทบ/ผลเสียต่อการดำเนินงานและฐานะการเงินของ

สถาบันการเงินต่อคณะกรรมการตรวจสอบ คณะกรรมการ สง. ประธานเจ้าหน้าที่บริหาร และ ธนาคารแห่งประเทศไทย ตามลำดับขั้นที่องค์กรกำหนดทันที รวมทั้งให้ความร่วมมือกับหน่วยงานกำกับดูแลของรัฐอื่น ๆ ที่เกี่ยวข้อง

จ. การกำกับดูแลการตรวจสอบ ควรจัดให้มีกฎบัตร แผนการตรวจสอบ คู่มือการปฏิบัติงานตรวจสอบภายใน แนวการตรวจสอบและการสอบถามการควบคุมภายใน และการรับรองคุณภาพ เพื่อให้มั่นใจว่าการปฏิบัติงานของหน่วยงานตรวจสอบภายในสอดคล้องกับมาตรฐานการตรวจสอบภายในที่ดี

ฉ. การใช้บริการจากบุคคลภายนอกในการตรวจสอบภายใน สง. อาจใช้บริการจากบุคคลภายนอกทำหน้าที่การตรวจสอบภายในบางส่วนหรือทั้งหมดไปบริษัทที่ให้บริการตรวจสอบภายใน เนื่องจากมีต้นทุนที่ต่ำกว่า หรือให้บริการที่ดีกว่า หากบริษัทนั้นมีโครงสร้างการดำเนินงานและการบริหารที่ดี

ลำดับต่อไปจะกล่าวถึงหน้าที่และความรับผิดชอบของหน่วยงานตรวจสอบภายใน ซึ่งถือว่าเป็นแนวทางปฏิบัติที่ดี ดังนี้

1. ความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน ผู้ตรวจสอบภายในควรสอบทานระเบียบปฏิบัติของ สง. เพื่อให้มั่นใจว่ามีการควบคุมอย่างเพียงพอ และพิจารณาว่าระบบควบคุมภายในที่มีอยู่มีประสิทธิผล ปฏิบัติได้ และมีการปฏิบัติตามหรือไม่ โดยสอบทานอย่างต่อเนื่องและสม่ำเสมอ ตลอดจนเครื่องมือที่ใช้ในการระบุ วัด จัดประเภท และรายงาน ควรมีการประเมินว่า ระบบการบริหารข้อมูลสารสนเทศโดยใช้คอมพิวเตอร์(MIS) มีประสิทธิภาพ
2. การปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎหมายและข้อบังคับ ผู้ตรวจสอบภายในควรประเมินว่า สง. มีการปฏิบัติตามกฎหมาย ข้อบังคับ ประกาศ คำสั่ง และหนังสือเวียน รวมถึงความสอดคล้องของการปฏิบัติงานกับนโยบายและระเบียบปฏิบัติภายในของ สง.
3. การตรวจสอบการทุจริต ข้อผิดพลาด การละเลย และรายการผิดปกติอื่นๆ ผู้ตรวจสอบภายในควรมีความตื่นตัว โดยเฉพาะในเวลาที่มีการเปลี่ยนแปลงสภาวะแวดล้อมทางการเงินที่การควบคุมภายในไม่มีประสิทธิภาพเท่าที่ควร และมีความเสี่ยงที่เกิดจากการทุจริตหรือข้อผิดพลาดสูง นอกจากนี้ ควรเข้าร่วมการพิจารณาความผิดจากการปฏิบัติงาน หรือการทุจริต หรือเป็นกรรมการในการพิจารณาวินัย
4. การตรวจสอบการบริหาร ผู้ตรวจสอบภายในควรสอบทานการใช้ทรัพยากรที่มีอยู่ให้เกิดประโยชน์สูงสุดเพื่อให้บรรลุวัตถุประสงค์และเป้าหมายขององค์กร รวมถึงการสอบทานระบบงานและระบบการบริหารทั่วไป
5. การประเมินระบบเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในควรประเมินระบบงานสารสนเทศ เพื่อให้แน่ใจว่ามีการควบคุมภายในที่เพียงพอ มีประสิทธิภาพ และครอบคลุมทุกกิจกรรมที่ใช้คอมพิวเตอร์ อันจะทำให้ข้อมูลมีความน่าเชื่อถือ ระบบข้อมูลมีความปลอดภัย รวมถึงการบริหารความเสี่ยงด้านการบริหารระบบงานสารสนเทศด้วย
6. บทบาทในการให้คำปรึกษา ผู้ตรวจสอบภายในอาจถูกร้องขอให้มีส่วนร่วมในการให้คำปรึกษาในเรื่องการออกผลิตภัณฑ์ ระบบงานใหม่ๆ และความเสี่ยงที่เกี่ยวเนื่องกับเรื่องนั้นๆ เพื่อให้แน่ใจว่ามีการนำเอาการควบคุมที่จำเป็นมาใช้ อย่างไรก็ดี การ

ทำหน้าที่ให้คำปรึกษาของผู้ตรวจสอบภายในควรแจ้งให้ฝ่ายบริหารทราบก่อน เพื่อไม่ให้ถูกมองว่ายอมลดความเป็นอิสระลง

การปฏิบัติหน้าที่ของหน่วยงานตรวจสอบภายในนั้น จะเป็นส่วนสำคัญที่ทำให้ผู้บริหารของ สง. มั่นใจได้ว่า รายการต่างๆ ที่เกิดขึ้นมีความถูกต้องครบถ้วนได้รับการอนุมัติตามอำนาจที่กำหนด มีการรายงานทั้งทางด้านการเงินและการควบคุมที่น่าเชื่อถือ มีการติดตามและแก้ไขปัญหาในกรณีมีการละเมิดกฎหมาย กฎระเบียบ และข้อบังคับต่างๆ ที่เกี่ยวข้อง มีการปฏิบัติที่ไม่เป็นไปตามนโยบาย และระบบการป้องกันทรัพย์สินที่ดีเพียงพอเพียงใด ซึ่งในการปฏิบัติงานให้ได้ตามเป้าหมายและบรรลุวัตถุประสงค์ของหน่วยงาน จะต้องมีแนวทางหรือคู่มือการใช้ปฏิบัติการตรวจสอบ รวมถึงมีการกำหนดขอบเขตการตรวจสอบ โปรแกรมการตรวจสอบ เกณฑ์ในการประเมิน รายงานการตรวจสอบ การติดตามและข้อสรุปที่เสนอต่อคณะกรรมการตรวจสอบ และแนวทางแก้ไขปัญหาที่ตรวจพบ ดังนั้น สิ่งสำคัญในการปฏิบัติงานของหน่วยงานตรวจสอบภายในก็คือ ความเป็นอิสระในการทำงาน และการนำเสนอรายการที่ตรวจพบที่สำคัญและแนวทางแก้ไขหรือ ข้อเสนอแนะที่เป็นประโยชน์ต่อฝ่ายบริหารได้ทันกาล

(4) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance Unit) [9]

สง. ควรกำหนดให้มีหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎเกณฑ์ โดยคณะกรรมการและผู้บริหารระดับสูง ให้ความสำคัญในการให้พนักงานทุกคนมีการปฏิบัติตามกฎเกณฑ์ที่กำหนด เพื่อหลีกเลี่ยงการดำเนินธุรกิจที่อาจก่อให้เกิดความเสี่ยง หรือความเสียหายทั้งในแง่ของความเสียหายทางการเงิน (Financial Loss) และความเสียหายด้านชื่อเสียง (Reputation loss) ซึ่งหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์มีหลักการของงาน ดังนี้

[9] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การกำกับการปฏิบัติตามกฎเกณฑ์ของสถาบันการเงิน (Compliance) ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510389.pdf

(5) ผู้สอบบัญชีภายนอก

ผู้สอบบัญชีภายนอก ผู้สอบบัญชีอิสระ หรือผู้สอบบัญชีรับอนุญาต หมายถึงบุคคลผู้ได้รับการแต่งตั้งโดยมติที่ประชุมผู้ถือหุ้นเสียงข้างมากให้ทำหน้าที่ตรวจสอบบัญชีของ สง. และได้รับความเห็นชอบจากธนาคารแห่งประเทศไทย

โดยปกติแล้ว ผู้สอบบัญชีจะต้องมีคุณสมบัติและปฏิบัติงานให้เป็นไปตามกฎหมายและมาตรฐานการสอบบัญชีที่กำหนดโดยองค์กรที่กำกับดูแล อย่างไรก็ตาม สง. ควรให้ความสำคัญในประเด็นเหล่านี้ว่า ผู้สอบบัญชีควร

1. มีความเป็นอิสระ และทราบถึงวัตถุประสงค์ของ สง.

2. มีการประเมินระบบการควบคุมภายในของ สง. เพื่อใช้วางแผนในการตรวจสอบ และเพื่อประเมินความเสี่ยงจากระบบการควบคุม

3. มีกระบวนต่างๆ ที่สามารถประเมินรายงานทางการเงินที่เพียงพอและเหมาะสมกับสภาพธุรกิจและสภาพแวดล้อมในการปฏิบัติงาน

4. มีการให้ข้อมูลสำคัญที่เป็นประโยชน์ต่อผู้ถือหุ้น คณะกรรมการ และผู้บริหารของ สง.

ขอบเขตการปฏิบัติงานของผู้สอบบัญชีภายนอก ประกอบด้วย [10]

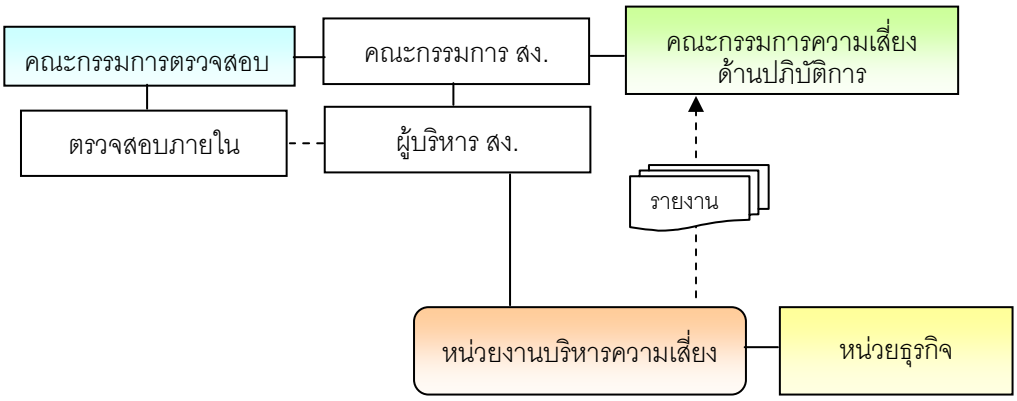
1. จัดส่งแนวการตรวจสอบบัญชี (Audit Program) ทุกด้านที่จะใช้ปฏิบัติงานสำหรับรอบปีการบัญชีที่ได้รับความเห็นชอบ โดยแสดงให้เห็นถึงขอบเขตและวิธีการตรวจสอบอย่างละเอียด และปริมาณการทดสอบ รวมทั้ง ประมาณการจำนวนชั่วโมงทำการในการตรวจสอบแต่ละเรื่องให้ธนาคารแห่งประเทศไทย ตลอดจนยินยอมให้ผู้สอบบัญชีจัดส่งแนวการตรวจสอบที่ใช้ปฏิบัติงานจริง กระดาษทำการ และเอกสารหลักฐานอื่นที่ได้จากการตรวจสอบเมื่อธนาคารแห่งประเทศไทยร้องขอ

2. จัดส่งหนังสือแจ้งการไม่ปฏิบัติตามกฎหมายและข้อบังคับ และหนังสือแจ้งจุดอ่อนของระบบการควบคุมภายในด้านบัญชีที่มีสาระสำคัญ รวมทั้ง หนังสือแจ้งข้อสังเกตหรือข้อแนะนำเกี่ยวกับฐานะการดำเนินงานหรือการบริหาร ที่ผู้สอบบัญชีส่งให้ สง. (ถ้ามี) ให้ธนาคารแห่งประเทศไทยด้วย

3. จัดทำรายงานพิเศษตามแนวการจัดทำรายงานที่กำหนด และให้ สง. จัดส่งรายงานดังกล่าวให้ธนาคารแห่งประเทศไทยด้วย

4. ตรวจสอบในเรื่องที่ธนาคารแห่งประเทศไทยสงสัยหรือมีข้อสังเกตเป็นพิเศษตามที่ธนาคารแห่งประเทศไทยร้องขอ

2.1.2 การจัดองค์กร



[10] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 62/2551 เรื่อง หลักเกณฑ์การให้ความเห็นชอบผู้สอบบัญชีของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510352.pdf

คณะกรรมการ สง. หรือคณะกรรมการที่ได้รับมอบหมาย และผู้บริหารระดับสูงควรร่วมกันกำหนดรูปแบบองค์กรที่เหมาะสม และเอื้อต่อการบริหารความเสี่ยงด้านปฏิบัติการ มีการแบ่งแยกหน้าที่ความรับผิดชอบและสายการรายงานอย่างชัดเจน สอดคล้องกับหลักการควบคุมภายในที่ดี โดยการจัดตั้งหน่วยงานที่ทำหน้าที่รับผิดชอบในการสนับสนุนงานด้านการบริหารความเสี่ยงด้านปฏิบัติการ (Risk management function) ซึ่งอาจจัดตั้งในรูปของคณะกรรมการ คณะอนุกรรมการ หรือหน่วยธุรกิจ และการวางระบบการควบคุม (Control Function) ทั้งในระดับนโยบาย และระดับปฏิบัติการที่ชัดเจน

อย่างไรก็ตาม การกำหนดรูปแบบองค์กรที่เหมาะสมไม่มีรูปแบบที่ตายตัวสำหรับแต่ละ สง. แต่หลักการที่สำคัญ คือ คณะกรรมการ คณะอนุกรรมการ หรือหน่วยธุรกิจที่ทำหน้าที่รับผิดชอบในการบริหารความเสี่ยงด้านปฏิบัติการ และวางระบบการควบคุมควรจะแยกออกจากหน่วยงานอื่นและหน่วยงานตรวจสอบภายในอย่างชัดเจน โดยให้รายงานคณะกรรมการบริหารความเสี่ยงของ สง. ซึ่ง สง. จะต้องพิจารณาปัจจัยแวดล้อมในการบริหารความเสี่ยงของตนเอง เพื่อการจัดโครงสร้างองค์กรที่เหมาะสม เช่น ระดับความเสี่ยงที่แต่ละองค์กรยอมรับได้ ขนาดขององค์กร แนวนโยบายด้านการบริหารความเสี่ยง ขีดความสามารถในการบริหารความเสี่ยงของผู้บริหาร และพนักงานที่เกี่ยวข้องในแต่ละระดับ รวมถึงประสิทธิภาพในการประสานงานระหว่างหน่วยงานที่เกี่ยวข้องโดยตรงกับการกำกับดูแล และบริหารจัดการความเสี่ยงด้านปฏิบัติการ เช่น คณะกรรมการ สง. คณะกรรมการตรวจสอบ คณะกรรมการบริหารความเสี่ยง ผู้บริหารระดับสูง หน่วยงานตรวจสอบภายใน ผู้สอบบัญชีภายนอก รวมถึงผู้กำกับดูแลของทางการ เป็นต้น

ภายใต้แนวความคิดในการจัดองค์กรที่เป็นไปตามมาตรฐานสากลนั้น สง. ต้องคำนึงถึงความเป็นอิสระและการถ่วงดุลอำนาจของฝ่ายจัดการและฝ่ายที่กำกับดูแลหรือหน่วยงานด้านการบริหารความเสี่ยง รวมถึงความซ้ำซ้อนของงาน และการละเลยงานด้วย สำหรับแนวความคิดในการจัดรูปแบบองค์กรที่ปฏิบัติกันโดยทั่วไปจะมีการผสมผสานรูปแบบการจัดองค์กรใน 2 ลักษณะ คือ

(1) การบริหารความเสี่ยงแบบบนลงล่าง (Top-Down Approach) และแบบล่างขึ้นบน (Bottom-Up Approach)

การผสมผสานระหว่างแนวคิดในการจัดองค์กรทั้งแบบบนลงล่าง และแบบล่างขึ้นบนนั้น จะก่อให้เกิดมุมมองในการบริหารความเสี่ยงด้านปฏิบัติการที่หลากหลาย ทั้งในระดับ

นโยบาย และระดับปฏิบัติการ คณะกรรมการ สง. หรือคณะกรรมการที่ได้รับมอบหมาย และผู้บริหารระดับสูงจะเป็นผู้กำหนดแนวนโยบาย และแผนกลยุทธ์ในการบริหารความเสี่ยงด้านปฏิบัติการ เพื่อให้ผู้บริหารระดับรองลงมาใช้เป็นแนวทางในการจัดทำแผนปฏิบัติการเพื่อรองรับการบริหารความเสี่ยงในระดับของหน่วยธุรกิจ และแตกย่อยลงมาจนถึงระดับปฏิบัติการ ในขณะเดียวกัน ผู้บริหาร และพนักงานในระดับปฏิบัติการจะเป็นผู้ที่นำแผนปฏิบัติการไปดำเนินการ รวมทั้ง รายงานข้อมูล หรือรายงานสรุปเกี่ยวกับความเสี่ยงด้านปฏิบัติการเสนอต่อผู้บริหารเพื่อใช้ในการตัดสินใจและกำหนดนโยบายในการบริหารความเสี่ยงในภาพรวมระดับองค์กรต่อไป อย่างไรก็ตาม สง. ควรคำนึงถึงการสร้างความสามารถในการประสานงาน และติดต่อสื่อสารระหว่างผู้บริหารในระดับชั้นต่างๆ เพื่อให้เกิดการสื่อสารที่มีประสิทธิภาพ โดยพิจารณานำระบบการรายงาน และติดตามความเสี่ยงที่เหมาะสมมาผนวกกับรูปแบบการบริหารความเสี่ยงที่ดีด้วย

(2) การบริหารความเสี่ยงแบบรวมศูนย์ (Centralized Approach) และแบบไม่รวมศูนย์ (Decentralized Approach)

การพิจารณาจัดรูปแบบองค์กรแบบรวมศูนย์ หรือแบบไม่รวมศูนย์ หรือการผสมผสานรูปแบบทั้งสองเข้าด้วยกัน สง. ต้องพิจารณาความสามารถขององค์กรในด้านการประสานงานระหว่างหน่วยธุรกิจต่างๆ ที่มีระดับชั้นการบริหารเดียวกัน รวมถึงความเป็นอิสระในการบริหารงานของแต่ละหน่วยธุรกิจ ความสามารถของบุคลากรในการบริหารความเสี่ยงของแต่ละหน่วยธุรกิจ และระดับความสามารถของ สง. ในการยอมรับความเสี่ยง โดยหลักการทั่วไปมีแนวทางกว้างๆ ในการพิจารณาเลือกรูปแบบองค์กรสรุปได้ ดังนี้

ปัจจัยในการพิจารณา	รูปแบบการจัดองค์กร	
	รวมศูนย์	ไม่รวมศูนย์
ระดับการยอมรับความเสี่ยงขององค์กร	ต่ำ	สูง
ระดับการยอมรับความเสี่ยงของแต่ละหน่วยธุรกิจ	เท่ากัน	ไม่เท่ากัน
ความเป็นอิสระของหน่วยธุรกิจในการดำเนินงาน	ต่ำ	สูง
ความสามารถของบุคลากรในการบริหารความเสี่ยงในหน่วยธุรกิจต่างๆ	ไม่เชี่ยวชาญ	เชี่ยวชาญ
ประสิทธิภาพด้านการประสานงานระหว่างหน่วยธุรกิจ	ต่ำ	สูง

อย่างไรก็ตาม สง. อาจพิจารณารูปแบบการจัดองค์กรให้มีความเหมาะสม โดยใช้ลักษณะของนโยบายการบริหารความเสี่ยงเป็นตัวกำหนดรูปแบบองค์กร กล่าวคือ ใช้รูปแบบการบริหารความเสี่ยงแบบรวมศูนย์เฉพาะกับนโยบายความเสี่ยงในระดับองค์กร (Enterprise-Wide Risk Policy) เพื่อให้เกิดมาตรฐานที่เท่าเทียมกันในแต่ละหน่วยธุรกิจ เช่น นโยบายความเสี่ยงด้านทรัพยากรบุคคล ด้านความปลอดภัย เป็นต้น ส่วนนโยบายการบริหารความเสี่ยงที่มีลักษณะเฉพาะของแต่ละหน่วยธุรกิจ เช่น การกำหนดเพดานการลงทุน การควบคุมเงินสด อาจเน้นที่การบริหารความเสี่ยงแบบไม่รวมศูนย์ กล่าวคือ ให้หน่วยธุรกิจบริหารความเสี่ยงของตนเองตามที่เห็นว่าเหมาะสม ซึ่งในกรณีนี้ หน่วยงานด้านการบริหารความเสี่ยงกลาง จะทำหน้าที่เพียงกำกับดูแลและให้คำปรึกษาแก่หน่วยธุรกิจในการกำหนดนโยบายการบริหารความเสี่ยงเท่านั้น

2.2 นโยบายการบริหารความเสี่ยงด้านปฏิบัติการ

2.2.1 นโยบายและขอบเขตการบริหารความเสี่ยงด้านปฏิบัติการ

คณะกรรมการ สง. หรือคณะกรรมการที่ได้รับมอบหมาย ทำหน้าที่กำหนดและอนุมัตินโยบาย แผนงานและกระบวนการบริหารความเสี่ยงด้านปฏิบัติการที่หน่วยงานบริหารความเสี่ยงด้านปฏิบัติการนำเสนอ โดยมีเนื้อหาครอบคลุมนโยบาย ขอบเขต และแนวทางปฏิบัติในการบริหารความเสี่ยงด้านปฏิบัติการ ซึ่งรวมถึง การกำหนดระดับความเสี่ยงที่ยอมรับได้ เพื่อใช้เป็นเกณฑ์ในการกำหนดเงินกองทุนเพื่อรองรับความเสี่ยง โดยอ้างอิงหลักเกณฑ์การดำรงเงินกองทุนที่ธนาคารแห่งประเทศไทย กำหนด การกำหนดหลักเกณฑ์ในการระบุความเสี่ยง การประเมินความเสี่ยง การติดตามและการรายงานความเสี่ยง การควบคุมและลดความเสี่ยง

ทั้งนี้ สง. ควรทบทวนความเหมาะสมของ นโยบาย ขอบเขต และแนวทางปฏิบัติในการบริหารความเสี่ยงด้านปฏิบัติการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงของปัจจัยเสี่ยงต่างๆ ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของ สง. อย่างมีนัยสำคัญ เช่น การออกผลิตภัณฑ์ใหม่ การเปลี่ยนแปลงระบบการทำงาน การเปลี่ยนแปลงหลักเกณฑ์หรือข้อกำหนดของทางการ การเปลี่ยนแปลงของภาวะเศรษฐกิจ หรือสภาพแวดล้อมในการดำเนินธุรกิจ เป็นต้น

2.2.2 กลยุทธ์ในการบริหารความเสี่ยงด้านปฏิบัติการ

เมื่อคณะกรรมการ สง. หรือคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงได้กำหนดนโยบายการบริหารความเสี่ยงด้านปฏิบัติการแล้ว ผู้บริหารและหน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการควรร่วมกันกำหนด และทบทวนแผนกลยุทธ์อย่างสม่ำเสมอ เพื่อจัดทำแผนปฏิบัติการ (Action Plan) ในการพัฒนาระบบงานที่เกี่ยวเนื่องกับการบริหารความเสี่ยงด้านปฏิบัติการในระดับองค์กร และระดับหน่วยธุรกิจต่างๆ โดยแผนกลยุทธ์ที่จัดทำขึ้น ควรกำหนดรายละเอียดของวัตถุประสงค์ ขอบเขตงาน ผู้มีหน้าที่รับผิดชอบ งบประมาณหรือทรัพยากรที่ต้องการ รวมถึงระยะเวลาของแผนที่ชัดเจน เพื่อประโยชน์ในการบริหาร และติดตามการดำเนินการตามแผนกลยุทธ์ในการบริหารความเสี่ยงที่กำหนดไว้

2.2.3 วัฒนธรรมองค์กร การสื่อสารและการควบคุม

สง. ควรปลูกฝังจิตสำนึกในการสร้างระบบการควบคุมให้เป็นวัฒนธรรมขององค์กร เพื่อให้ผู้ที่เกี่ยวข้องทุกระดับตระหนักว่ากิจกรรมการควบคุมเป็นหน้าที่ของทุกคนใน สง. ไม่ใช่เป็นหน้าที่เฉพาะของหน่วยธุรกิจใดหน่วยธุรกิจหนึ่ง อย่างไรก็ดี คณะกรรมการ สง. หรือคณะกรรมการที่ได้รับมอบหมาย และผู้บริหารระดับสูงต้องมีความรับผิดชอบ และเป็นผู้นำในการสร้างวัฒนธรรมองค์กร โดยการสื่อสาร แนะนำแนวทาง และเน้นถึงความสำคัญของการควบคุมเพื่อเป็นแบบอย่างที่ดีให้แก่พนักงานของ สง. ซึ่งรวมถึงการมีจริยธรรมในการบริหารงานด้วย เพื่อสร้างให้เกิดการดำเนินงาน และการมีระบบควบคุมที่ดีเป็นไปตามหลักการกำกับดูแลกิจการที่ดีภายในองค์กร นอกจากนี้ สง. ต้องมีระบบการตรวจสอบเพื่อให้แน่ใจว่าหน่วยธุรกิจต่างๆ ได้นำหลักการควบคุมไปใช้ในการปฏิบัติงานอย่างเหมาะสม รวมถึงต้องมีระบบการประเมินประสิทธิภาพ ความเพียงพอ และความเหมาะสมของระบบการควบคุมของทั้งภายใน สง. และบุคคลหรือองค์กรภายนอกอย่างเป็นทางการ และมีการรายงานผลให้ผู้บริหารในระดับต่างๆ รับทราบอย่างสม่ำเสมอด้วย

2.3 การบริหารความเสี่ยงด้านปฏิบัติการ

สิ่งสำคัญของการบริหารความเสี่ยงด้านปฏิบัติการที่ผู้ตรวจสอบพึงรู้ ได้แก่ ปัจจัยความเสี่ยงด้านปฏิบัติการที่ประกอบด้วย ด้านบุคลากร ด้านระบบงาน ด้านกระบวนการทำงาน และด้านปัจจัยภายนอก รวมทั้งยังต้องทราบถึงระบบการบริหารความเสี่ยงด้านปฏิบัติการที่จะทำให้ สง. ได้ปฏิบัติให้อยู่ในกรอบของความเสี่ยงที่ยอมรับได้ โดยมีกระบวนการที่เกี่ยวกับ การระบุ การวัด การติดตาม การรายงาน การควบคุมและการลดความเสี่ยง

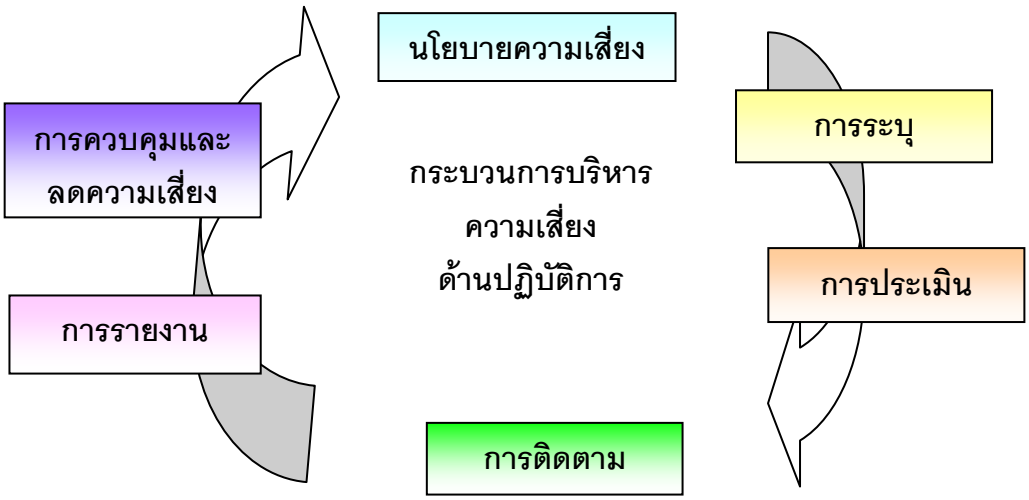
การบริหารความเสี่ยงด้านปฏิบัติการ [11] ของ สง. ควรสอดคล้องกับนโยบาย และรูปแบบองค์กรที่ สง. กำหนดขึ้น เพื่อสร้างขีดความสามารถในการบริหารจัดการความเสี่ยงด้านปฏิบัติการได้อย่างเหมาะสม และเกิดประสิทธิภาพสูงสุด ซึ่ง สง. ควรพิจารณาวางระบบการบริหารความเสี่ยงตามหลักมาตรฐานสากล ให้ครอบคลุมการปฏิบัติงานในทุกระดับชั้นของทุกหน่วยธุรกิจของ สง. ด้วย ซึ่งระบบการดำเนินงานเพื่อการบริหารความเสี่ยงนั้น ควรจะมีกระบวนการ ดังนี้

2.3.1 การระบุความเสี่ยง

2.3.2 การประเมินความเสี่ยง

2.3.3 การติดตามและรายงานความเสี่ยง

2.3.4 การควบคุมและลดความเสี่ยง



2.3.1 การระบุความเสี่ยง

สง. ควรดำเนินการให้มีการระบุความเสี่ยง ประเภทความเสี่ยงและปัจจัยความเสี่ยงในแต่ละผลิตภัณฑ์ บริการทางการเงิน ระบบงาน หรือในแต่ละหน่วยงานของ สง. โดยควรจัดทำอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงของปัจจัยความเสี่ยงต่างๆ ที่ส่งผลกระทบต่อกระบวนการปฏิบัติงานอย่างมีนัยสำคัญ เช่น การออกผลิตภัณฑ์ใหม่ การออกกฎระเบียบของทางการ การปรับโครงสร้างการทำงาน เป็นต้น โดยการระบุความเสี่ยง ควรจะดำเนินการในทุกระดับ

[11] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการ ลงวันที่ 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510385.pdf

ตั้งแต่ระดับปฏิบัติการขึ้นไปจนถึงระดับบริหาร และให้ครอบคลุมทุกหน่วยธุรกิจ ด้วย ซึ่งการระบุความเสี่ยงจะต้องอยู่ภายใต้เกณฑ์และมาตรฐานตามที่คณะกรรมการ สง. หรือคณะกรรมการที่ได้รับมอบหมาย และผู้บริหารระดับสูงของ สง. กำหนดขึ้น นอกจากนี้ หน่วยงานในฐานะผู้รู้และเข้าใจกระบวนการทำงานและความเสี่ยงที่มีอยู่ได้ดีที่สุด ควรมีส่วนร่วมในกระบวนการระบุความเสี่ยง โดยพิจารณาปัจจัยต่างๆ เช่น

- ประสิทธิภาพของระบบการควบคุมภายใน วัฒนธรรมองค์กรในการบริหารความเสี่ยงด้านปฏิบัติการ ความพร้อมของบุคลากร และทรัพยากรที่ใช้ในการปฏิบัติงาน
- ปริมาณ ความซับซ้อนและประเภทของธุรกรรม ซึ่งรวมถึงระบบที่เกี่ยวข้องในการให้บริการลูกค้า (End to End Operating Cycle) กลไกการกระจายผลิตภัณฑ์และบริการสู่ลูกค้าของ สง. (Distribution Mechanism)
- แผนผังกระบวนการทำงาน หรือขั้นตอนการปฏิบัติงาน (Work Process Mapping)
- เหตุการณ์ความเสียหายที่เกิดขึ้นในอดีต หรือเหตุการณ์ที่เกิดขึ้น แต่ สง. สามารถป้องกันความเสียหายไว้ได้ (Near-Misses)
- เหตุการณ์ความเสียหายที่เกิดขึ้นกับ สง. แห่งอื่น
- การเปลี่ยนแปลงของเทคโนโลยี การออกผลิตภัณฑ์ใหม่ การเปลี่ยนแปลงทางกฎหมาย สังคม การเมืองและเศรษฐกิจ เป็นต้น
- ดัชนีชี้วัดความเสี่ยง (Risk Indicators) ซึ่งรายละเอียดจะกล่าวไว้ในหัวข้อที่ 2.3.3 เรื่องการติดตามและการรายงานความเสี่ยง ซึ่งจะช่วยให้ สง. ทราบถึงระดับความเสี่ยงที่มีอยู่ในช่วงเวลาหนึ่งๆ โดยอาศัยการชี้วัดจากปัจจัยเสี่ยงต่างๆ ที่ สง. กำหนดขึ้น

2.3.2 การประเมินความเสี่ยง

สง. ควรกำหนดหรือทบทวนแนวทาง และวิธีการในการประเมินความเสี่ยงด้านปฏิบัติการให้มีความเหมาะสมกับการดำเนินธุรกิจอยู่เสมอ เพื่อให้ผู้บริหารทุกระดับของแต่ละหน่วยธุรกิจสามารถประเมินความเสี่ยงด้านปฏิบัติการที่อาจเกิดขึ้นจากการดำเนินงานของหน่วย

ธุรกิจที่ตนรับผิดชอบได้อย่างเหมาะสม โดยหลักมาตรฐานทั่วไป สง. ควรมีการประเมินระดับความเสี่ยงด้านปฏิบัติการโดยอ้างอิงมาตรฐานภายใน (Internal Standard Risk Rating) ที่กำหนดขึ้นเอง โดยอาจกำหนดในรูปแบบของระดับตัวเลข สัญลักษณ์ สี หรือคำบรรยายระดับสูงต่ำก็ได้ รวมทั้งมีคำอธิบายที่ชัดเจน เพื่อให้สามารถแบ่งระดับหรือจัดลำดับความสำคัญของการดำเนินการปรับปรุง ควบคุมและลดความเสี่ยงต่อไป นอกจากนี้ สง. ควรมีเครื่องมือเพื่อช่วยในการระบุและประเมินความเสี่ยงด้านปฏิบัติการ เช่น Risk and Control Self Assessment, Risk Mapping และ Risk Indicators เป็นต้น ซึ่งการระบุและประเมินความเสี่ยงควรดำเนินการอย่างต่อเนื่องและมีการทบทวนความเหมาะสมเป็นระยะๆ โดย

- **การวัดความเสี่ยง**

สง. อาจจัดทำเป็นตารางการวัดระดับความเสี่ยง (Risk Matrix) โดย คำนวณผลเปรียบเทียบระหว่างโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Severity of Impact) ที่อาจเกิดขึ้นจากความเสี่ยงนั้นๆ ดังตัวอย่างตามตาราง

โอกาสที่จะเกิด	**ระดับผลกระทบ**		
	ต่ำ	**ปานกลาง**	**สูง**
สูง	ปานกลาง	ค่อนข้างสูง	สูง
ปานกลาง	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง
ต่ำ	ต่ำ	ค่อนข้างต่ำ	ปานกลาง

ทั้งนี้ สง. อาจกำหนดรูปแบบ และเงื่อนไขในการประเมินความเสี่ยงด้านปฏิบัติการตามแนวทางที่เห็นสมควรนอกเหนือจากที่กล่าวไว้ข้างต้น โดยใช้วิธีการคำนวณเฉพาะตามหลักทางคณิตศาสตร์ และค่าความสัมพันธ์ทางสถิติต่างๆ หรือใช้โปรแกรมคอมพิวเตอร์สำเร็จรูป หรือโปรแกรมคอมพิวเตอร์ที่ สง. พัฒนาขึ้น แต่แนวทางและวิธีการคำนวณดังกล่าวจะต้องสอดคล้องกับลักษณะ ขอบเขตการดำเนินธุรกิจ และความสามารถในการยอมรับความเสี่ยงของ สง. และความเป็นจริงเป็นหลักสำคัญด้วย สำหรับการประเมินความเสี่ยงนั้น สามารถดำเนินการโดยพนักงานผู้ปฏิบัติงานในหน่วยธุรกิจนั้นๆ เอง โดยอาศัยหลักการของการประเมินการควบคุมด้วยตนเอง (Control Self- Assessment) หรือ สง. อาจกำหนดให้หน่วยงานบริหารความเสี่ยงส่วนกลางหรือบุคคลภายนอกเป็นผู้ประเมินความเสี่ยงให้ก็ได้ ขึ้นอยู่กับแนวนโยบายของแต่ละ สง.

- **การคำนวณเงินกองทุนรองรับความเสี่ยงด้านปฏิบัติการ** [12]

สง. สามารถเลือกวิธีการคำนวณเงินกองทุนรองรับความเสี่ยงด้านปฏิบัติการได้ 3 วิธี

(1) วิธี Basic Indicator Approach (BIA) คือวิธีการที่ให้ สง. ดำรงเงินกองทุนสำหรับความเสี่ยงด้านปฏิบัติการ โดยการนำค่าเฉลี่ยย้อนหลัง 3 ปีของรายได้จากการดำเนินงาน (Gross Income) คูณด้วยร้อยละ 15

(2) วิธี Standardised Approach (SA-OR) คือวิธีการที่ให้ สง. ดำรงเงินกองทุนสำหรับความเสี่ยงด้านปฏิบัติการ โดยการนำค่าเฉลี่ยย้อนหลัง 3 ปีของผลรวมของรายได้จากการดำเนินงานแต่ละสายธุรกิจหลัก 8 สายคูณกับค่าคงที่ (ตามตารางที่ ธนาคารแห่งประเทศกำหนด) ดังนี้

สายธุรกิจ (Business Lines)	ค่าคงที่ความเสี่ยงต่อรายได้จากการดำเนินงาน
1. Corporate finance	18%
2. Trading and sales	18%
3. Retail banking	12%
4. Commercial banking	15%
5. Payment and settlement	18%
6. Agency services	15%
7. Asset management	12%
8. Retail brokerage	12%

นอกจากนี้ สง. อาจใช้วิธี Alternative Standardised Approach (ASA) ซึ่งมีหลักการคำนวณเช่นเดียวกับวิธี SA-OR แต่ใช้ยอดคงค้างของเงินให้สินเชื่อเป็นฐานในการคำนวณเงินกองทุนสำหรับความเสี่ยงในสายธุรกิจ Retail banking และสายธุรกิจ Commercial banking

[12] ประกาศธนาคารแห่งประเทศไทยที่ สนส.95/2551 เรื่อง หลักเกณฑ์การดำรงเงินกองทุนขั้นต่ำสำหรับความเสี่ยงด้านปฏิบัติการ ลงวันที่ 27 พฤศจิกายน 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510555.pdf

แทนรายได้จากการดำเนินงานของสายธุรกิจ ทั้งนี้ สง. ที่เลือกใช้วิธี SA-OR หรือวิธี ASA จะต้องได้รับความเห็นชอบจากธนาคารแห่งประเทศไทย และผ่านเกณฑ์มาตรฐานขั้นต่ำตามที่ธนาคารแห่งประเทศไทย.กำหนด ดังนี้

1. คณะกรรมการและผู้บริหารระดับสูงของ สง. ต้องมีส่วนร่วมในการกำหนดกรอบนโยบายและการติดตามดูแลการบริหารความเสี่ยงด้านปฏิบัติการ

2. สง. ต้องมีระบบการบริหารความเสี่ยงด้านปฏิบัติการที่ดีและมีการนำระบบดังกล่าวไปใช้ในการบริหารความเสี่ยงอย่างรัดกุม

3. สง. ต้องมีทรัพยากรเพียงพอสำหรับการบังคับใช้วิธี SA-OR หรือวิธี ASA ในแต่ละสายธุรกิจและในสายงานควบคุมและตรวจสอบภายใน

4. สง. ต้องมีนโยบายและหลักเกณฑ์ในการเชื่อมโยงรายได้จากการดำเนินงานสำหรับแต่ละสายธุรกิจตามวิธี SA-OR (หรือยอดคงค้างเงินให้สินเชื่อสำหรับสายธุรกิจ Retail Banking และ Commercial Banking ตามวิธี ASA) เป็นลายลักษณ์อักษร รวมทั้งมีการทบทวนอย่างสม่ำเสมอและปรับปรุงหลักเกณฑ์ดังกล่าวเมื่อมีการเปลี่ยนแปลงธุรกิจหรือมีการทำธุรกิจใหม่

5. สง. ต้องมีระบบการจัดเก็บข้อมูลเกี่ยวกับความเสียหายที่เกิดขึ้นในแต่ละสายธุรกิจ ซึ่งต้องเป็นส่วนหนึ่งของระบบประเมินความเสี่ยงด้านปฏิบัติงานที่ สง. ใช้ภายในและต้องสามารถรวมเข้ากับกระบวนการบริหารความเสี่ยงของ สง. ได้เป็นอย่างดี เช่น ข้อมูลผลลัพธ์ที่ได้จากการประเมินความเสี่ยงต้องเป็นส่วนสำคัญในรายงานความเสี่ยงรายงานที่ส่งให้ผู้บริหาร และถูกนำไปใช้ในการวิเคราะห์ติดตามและควบคุมความเสี่ยง เป็นต้น

6. สง. ต้องมีการจัดทำรายงานความเสี่ยงและข้อมูลความเสียหายที่เกิดขึ้นเป็นประจำ

7. สง. ต้องจัดทำระบบบริหารความเสี่ยงเป็นลายลักษณ์อักษร และมีการติดตามการปฏิบัติตามนโยบายที่กำหนดไว้ การควบคุม และกระบวนการที่เกี่ยวกับระบบบริหารความเสี่ยงซึ่งรวมถึงการดำเนินการเมื่อเกิดกรณีที่ไม่ได้ปฏิบัติตามนโยบายที่กำหนดไว้

8. สง. ต้องมีการสอบทานกระบวนการบริหารความเสี่ยงและระบบประเมินความเสี่ยงที่เป็นอิสระเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในการทำธุรกรรม กระบวนการ หรือระบบบริหารความเสี่ยง

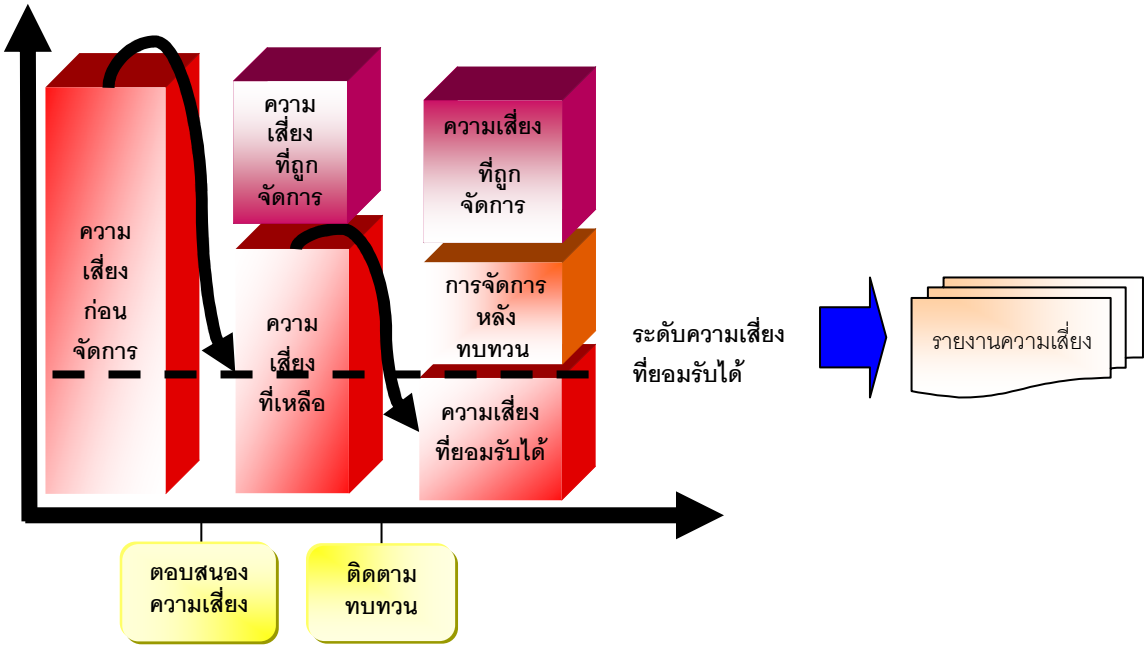
9. ระบบการบริหารความเสี่ยงด้านปฏิบัติการของ สง. ต้องมีการสอบทานโดยผู้ตรวจสอบภายนอกเมื่อ ธปท. เห็นสมควร

(3) วิธี Advanced Measurement Approach (AMA) ให้ สง. ใช้แบบจำลองที่ได้รับอนุญาตจากทางการในการคำนวณเงินกองทุนสำหรับความเสี่ยงด้านปฏิบัติการได้ ทั้งนี้ ข้อมูลในแบบจำลองต้องประกอบด้วย ข้อมูลเชิงปริมาณและเชิงคุณภาพ ได้แก่ ข้อมูลความเสียหายที่เกิดขึ้นภายใน สง. ร่วมกับข้อมูลความเสียหายใน สง. อื่นที่เกี่ยวข้อง ข้อมูลสถานการณ์สมมุติฐาน (Scenario analysis) และข้อมูลอื่นที่สะท้อนถึงสภาพแวดล้อมทางธุรกิจและระบบการควบคุมภายในที่เปลี่ยนแปลงไป (ปัจจุบันธนาคารแห่งประเทศไทย ยังไม่ได้อนุญาตให้ใช้วิธีนี้)

ทั้งนี้ การที่ สง. เลือกใช้วิธีการคำนวณเงินกองทุนแบบใดนั้น ควรขึ้นอยู่กับลักษณะและความซับซ้อนของการดำเนินธุรกิจของแต่ละ สง. อย่างไรก็ดี หาก สง. รายใดเลือกใช้วิธี Internal Rating-Based Approach (IRB) สำหรับความเสี่ยงด้านเครดิต ให้ สง. ใช้วิธี SA-OR สำหรับความเสี่ยงด้านปฏิบัติการเป็นมาตรฐานขั้นต่ำ ทั้งนี้ สำหรับ สง. ที่เลือกใช้วิธีที่ซับซ้อนกว่าแล้ว จะไม่สามารถกลับมาใช้วิธีที่ซับซ้อนน้อยกว่าได้ เว้นแต่จะได้รับอนุญาตจากธนาคารแห่งประเทศไทยก่อน

ผู้ตรวจสอบสามารถศึกษาแนวทางหรือขั้นตอนการตรวจสอบการคำนวณความเสี่ยงต่อเงินกองทุนสำหรับความเสี่ยงด้านปฏิบัติการเพิ่มเติมได้จาก “แนวทางการตรวจสอบการดำรงเงินกองทุนขั้นต่ำสำหรับความเสี่ยงด้านปฏิบัติการ”

2.3.3 การติดตามและการรายงานความเสี่ยง



- **การติดตามความเสี่ยง**

สง. ควรมีระบบการติดตามความเสี่ยง รวมถึงการรายงานข้อมูลปัจจัยเสี่ยง (Risk Factor) และข้อมูลสถานะความเสี่ยง (Risk Profile) ในภาพรวม ให้ผู้บริหารระดับสูงของ สง. รับทราบอย่างต่อเนื่องและสม่ำเสมอ โดยความถี่ในการติดตามสถานะความเสี่ยงที่เหมาะสมขึ้นอยู่กับวิธีการและข้อมูลปัจจัยเสี่ยงที่ สง. เลือกใช้ หากข้อมูลปัจจัยเสี่ยงมีการเปลี่ยนแปลงรวดเร็วและตลอดเวลา สง. ควรกำหนดความถี่ในการติดตามให้มากขึ้น เช่น มีการติดตามรายวัน รายสัปดาห์ เป็นต้น แต่หากข้อมูลปัจจัยเสี่ยงมีการเปลี่ยนแปลงน้อย และเปลี่ยนแปลงค่อนข้างช้า สง. อาจดำเนินการติดตามเพียงไตรมาสละครั้ง ปีละสองครั้ง หรือเป็นปีละครั้ง ทั้งนี้ เพื่อให้ผู้บริหารของ สง. สามารถติดตามสถานะความเสี่ยงที่มีอยู่ในแต่ละช่วงเวลา และสามารถวางแผนเพื่อบริหารจัดการความเสี่ยงด้านปฏิบัติการได้อย่างเหมาะสม นอกจากนี้ การติดตามความเสี่ยงยังเป็นเครื่องมือที่ช่วยให้ผู้บริหาร สง. ใช้ประเมินความสามารถของระบบการควบคุมว่ามีประสิทธิภาพมากน้อยเพียงใดได้อีกทางหนึ่งด้วย เพราะหากระบบการควบคุมมีประสิทธิภาพเพียงพอ สถานะความเสี่ยงของ สง. ก็ควรจะลดลงตามไปด้วยนั่นเอง ซึ่งโดยทั่วไปข้อมูลที่ สง. ใช้ในการติดตามความเสี่ยง จะประกอบด้วย

(1) ดัชนีชี้วัดความเสี่ยง (Key Risk Indicators) เป็นเครื่องมือที่ทำหน้าที่เตือนภัยล่วงหน้า ที่บอกให้ผู้บริหาร สง. ทราบถึงระดับความรุนแรงของปัจจัยเสี่ยง ณ ช่วงเวลาใดเวลาหนึ่ง โดยจะแสดงผลเป็นตัวเลข หรือค่าสัญลักษณ์อื่นใด เช่น ระดับสี มาตรวัดความรุนแรง เป็นต้น ขึ้นอยู่กับวิธีการที่ สง. เลือกใช้ ซึ่งตัวชี้วัดความเสี่ยงที่ดี นอกจากจะสะท้อนให้ สง. เห็นถึงความเสี่ยงที่เกิดขึ้นในอดีตที่ผ่านมา (Lacking Indicators) แล้ว ยังควรสามารถบ่งชี้ หรือพยากรณ์ให้ผู้บริหาร สง. สามารถคาดคะเนถึงความเสี่ยงที่อาจจะเกิดขึ้นในอนาคต (Forward Looking Indicators) จากระดับความรุนแรงของปัจจัยเสี่ยงที่ชี้วัดได้อีกด้วย ซึ่งจะช่วยให้ สง. สามารถปรับตัว และป้องกันความเสี่ยงได้ก่อนที่ความเสี่ยงเหล่านั้นจะเกิดขึ้นจริง และส่งผลเสียหายต่อ สง.

สง. ควรกำหนดระดับความเสี่ยงที่ยอมรับได้ (Tolerance level) ของดัชนีชี้วัดความเสี่ยงแต่ละตัว และให้มีการรายงานการเปลี่ยนแปลงของดัชนีชี้วัดความเสี่ยงอย่างครบถ้วนและเป็นระบบ ตลอดจนสื่อสารให้ทุกหน่วยงานทราบอย่างชัดเจน เพื่อเพิ่มความโปร่งใสให้กับการบริหารความเสี่ยงด้านปฏิบัติการขององค์กรด้วย

(2) ข้อมูลเหตุการณ์ความเสียหาย (Loss Incidents) เป็นข้อมูลแสดงรายละเอียดความเสียหายที่เกิดขึ้นในอดีต ซึ่งการจัดเก็บข้อมูลเหตุการณ์ความเสียหายที่มีประสิทธิภาพจะช่วยให้ สง. สามารถวิเคราะห์ และติดตามความเสี่ยงได้อย่างมีประสิทธิภาพมากขึ้น โดยการจัดเก็บข้อมูลเหตุการณ์ความเสียหายนั้น ควรมีรายละเอียดเบื้องต้นครอบคลุมประเด็นสำคัญดังนี้ [13]

- วันที่เกิด และตรวจพบความเสียหาย
- หน่วยงานที่เกิดความเสียหาย
- ประเภทของเหตุการณ์ความเสียหาย
- ความเสียหายที่เกิดขึ้น
- เงินชดเชยหรือค่าเสียหายที่เรียกคืนได้ ระยะเวลาที่ใช้ในการเรียกคืน และค่าใช้จ่ายในการดำเนินการ
- รายละเอียด และสาเหตุของเหตุการณ์ความเสียหาย
- การดำเนินการเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต

[13] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการ ลงวันที่ 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510385.pdf

ตารางตัวอย่างการเก็บข้อมูลความเสียหายที่เกิดจากความเสี่ยงด้านปฏิบัติการ

ลำดับที่ (1)	หน่วยงาน (2)	สายธุรกิจ (3)	วันที่เกิด (4)	วันที่ตรวจพบ (5)	รายละเอียด (6)	สาเหตุ (7)	ประเภทเหตุการณ์ (8)	จำนวนความเสียหาย (9)	จำนวนที่เรียกคืนได้ (10)	วันที่รับเงินคืน (11)	ค่าใช้จ่ายในการดำเนินการ (12)	การดำเนินการเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต (13)
1.	Branch -Teller บางขุนพรหม	BL 3 (RB)	18/02/47	29/05/47	พนักงานเบิกเงินจากบัญชีของลูกค้า โดยทุจริต (Teller Fraud)	พนักงานธนาคารได้รับความไว้วางใจจากลูกค้าธนาคารที่อยู่ใกล้สาขา ให้เบิกเงินแทนเจ้าของบัญชี	LET 1 (internal-fraud)	50,000	50,000	06/06/47	500	1. ผจก. สาขากำชับพนักงาน teller ให้ปฏิบัติตามกฎระเบียบเรื่อง บช เงินฝากอย่างเคร่งครัด พร้อมแจ้งลูกค้าทราบภายใน 1 เดือน 2. ตรวจสอบและกำชับสาขาอื่น ๆ ภายใน 1 เดือน

(1) ลำดับที่

(2) หน่วยงาน / ส่วนงาน / สายงานที่เกิดเหตุการณ์ความเสียหาย

(3) สายธุรกิจ (Business Line) ตามที่ BCBS กำหนดไว้ มีทั้งหมด 8 สายธุรกิจ

(4) วันที่เกิดเหตุการณ์ความเสียหาย

(5) วันที่ตรวจพบเหตุการณ์ความเสียหาย

(6) รายละเอียดของเหตุการณ์ความเสียหายที่เกิดขึ้น

(7) สาเหตุของเหตุการณ์ความเสียหายที่หน่วยงานทราบหรือที่ตรวจสอบได้ เพื่อประโยชน์ในการกำหนดมาตรการป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต

(8) ประเภทเหตุการณ์ (Loss Event Type) ตามที่ BCBS กำหนดไว้ มีทั้งหมด 7 ประเภทเหตุการณ์

(9) ความเสียหายที่เป็นตัวเงินที่เกิดขึ้น ซึ่งรวมถึง ความสูญเสียหรือเสียหายต่อทรัพย์สิน(Loss or damage to assets) จำนวนเงินที่ต้องรับผิดชอบชดใช้ (Legal liability) ค่าใช้จ่ายเพื่อดำเนินการให้กลับสู่สภาพเดิม (Loss of recourse) และความเสียหายที่ไม่สามารถเรียกคืนได้ (Write-down) เป็นต้น แต่ไม่รวมค่าเสียโอกาส (Opportunity cost) รายได้ที่พลาดโอกาสได้รับ (Foregone revenue) และเงินลงทุนเพื่อพัฒนาระบบและป้องกันความเสียหายในอนาคต (cost related to investment programs to prevent subsequent losses)

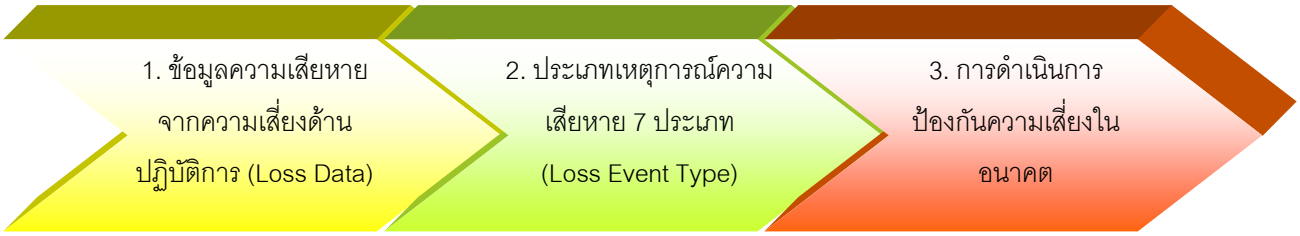
(10) จำนวนที่เรียกคืนได้จากผู้กระทำความผิดหรือบริษัทประกันภัย เป็นต้น

(11) วันที่ได้รับเงินคืน

(12) ค่าใช้จ่ายในการดำเนินการเรียกคืน เช่น ค่าใช้จ่ายในการดำเนินคดี เป็นต้น

(13) การดำเนินการเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต เช่น ปรับปรุงระบบควบคุมการภายในดูแลให้มีการปฏิบัติตามกฎระเบียบที่กำหนด หรือพัฒนาระบบรักษาความปลอดภัยให้เข้มงวดขึ้น เป็นต้น ซึ่งควรกำหนดกรอบเวลาและผู้รับผิดชอบอย่างชัดเจน พร้อมทั้งติดตามการดำเนินการอย่างใกล้ชิด

* ข้อมูลประกอบแนวทางการเก็บข้อมูลความเสียหายอาจศึกษาเพิ่มเติมได้จากแหล่งต่าง ๆ เช่น British Bankers' Association (BBA) (www.bba.org.uk) และ Operational Risk data eXchange Association (ORX) (www.orx.org)



- เพื่อประเมินจำนวนความเสียหายของ สง. ว่ามีมากน้อยเท่าใด (จากข้อ (9) – (12))

- เพื่อประเมินประเภทความเสียหายของ สง. ว่ามีสาเหตุเกิดจากอะไร (Root Cause) (จากข้อ (6) – (8))

- เพื่อประเมินการดำเนินของสง. ว่ามีอย่างไรบ้าง ในการป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต (จากข้อ (13)
- ประเมินว่ามีการปฏิบัติตามสิ่งที่กำหนดไว้อย่างสม่ำเสมอหรือไม่

นอกเหนือจากการจัดเก็บและรายงานข้อมูลความเสียหายที่เกิดขึ้นแล้ว สง. ควรเก็บข้อมูลเหตุการณ์ที่เกิดขึ้น แต่ สง. สามารถป้องกันความเสียหายไว้ได้ (Near-misses) เพื่อประโยชน์ในการศึกษาและพัฒนาระบบบริหารความเสี่ยงขององค์กรต่อไป

ทั้งนี้ สง. ควรกำหนดบทบาท หน้าที่ และความรับผิดชอบในการติดตามความเสี่ยงให้ชัดเจนว่าหน่วยงาน หรือหน่วยธุรกิจใด ทำหน้าที่ในการติดตามความเสี่ยง รวมถึงการกำหนดนโยบาย และพัฒนาระบบข้อมูลสารสนเทศ หรือกำหนดแบบรายงานที่ใช้ในการติดตามความเสี่ยงควบคู่กันไปด้วย

- **การรายงานความเสี่ยง**

คณะกรรมการ สง. หรือคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงจะต้องจัดให้มีการรายงานในส่วนที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการอย่างชัดเจน และสม่ำเสมอ เพื่อให้มั่นใจได้ว่าหน่วยธุรกิจที่เกี่ยวข้องได้รับข้อมูลความเสี่ยงด้านปฏิบัติการอย่างถูกต้อง ทันเวลา และทำให้คณะกรรมการและผู้บริหารระดับสูงได้ทราบถึงผลการดำเนินงาน และปัญหาที่เกิดขึ้น เพื่อใช้ประกอบการกำหนดนโยบาย จัดทำระบบการบริหารความเสี่ยง และวางระบบการควบคุมได้อย่างเหมาะสม และมีประสิทธิภาพ โดยการรายงานดังกล่าวควรประกอบด้วย

การนำเสนอและสรุปเหตุการณ์ความเสียหาย หรือปัญหาที่เกิดขึ้นในการดำเนินงาน ข้อสังเกตที่ตรวจพบ ตลอดจนแนวทางการแก้ไข เพื่อป้องกัน ควบคุม และลดความเสี่ยงด้านปฏิบัติการ ซึ่งลักษณะ ประเภท และลำดับชั้นของการรายงานนั้น ขึ้นอยู่กับสถานการณ์ เหตุการณ์ และระดับความรุนแรงของผลกระทบที่เกิดขึ้น ซึ่งการรายงานที่เกี่ยวข้องกับความเสี่ยงด้านปฏิบัติการใน

เบื้องต้นที่ สง. ควรจัดทำขึ้น มีดังนี้

(1) การรายงานต่อคณะกรรมการ สง.

เมื่อคณะกรรมการบริหารความเสี่ยงมีการกำหนดนโยบาย หรือระเบียบข้อบังคับใดๆ เพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้น คณะกรรมการบริหารความเสี่ยงควรรายงานข้อมูลที่เกี่ยวข้องต่อคณะกรรมการ สง. โดยสม่ำเสมอ และในกรณีที่ความเสี่ยงดังกล่าวทำให้เกิดความเสียหายต่อ สง. หรือส่งผลกระทบต่อผลการดำเนินงาน คณะกรรมการบริหารความเสี่ยงจะต้องรายงานต่อคณะกรรมการ สง. ให้ทราบทันที เพื่อให้คณะกรรมการ สง. ใช้ข้อมูลดังกล่าวประกอบการตัดสินใจเพื่อแก้ไขปัญหาได้อย่างเหมาะสม และทันท่วงที

(2) การรายงานต่อคณะกรรมการตรวจสอบ

หน่วยงานตรวจสอบภายใน ต้องรายงานสรุปผลการตรวจสอบในแต่ละงวด ซึ่งรวมถึงรายงานที่เกี่ยวข้องกับผู้สอบบัญชีภายนอก เช่น รายงานผู้สอบบัญชีรับอนุญาตต่องบการเงินในแต่ละงวด รายงานการตรวจสอบระหว่างกาลหรือรายงานการตรวจสอบในกรณีพิเศษ และรายงานการตรวจสอบความเสี่ยงและระบบการควบคุมภายใน เป็นต้น ต่อคณะกรรมการตรวจสอบเป็นระยะๆ และสม่ำเสมอ เพื่อให้มั่นใจว่าระบบการควบคุมต่างๆ ที่หน่วยธุรกิจจัดทำขึ้น สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ และเหมาะสมกับลักษณะการดำเนินงานและขอบเขตธุรกิจของ สง.

(3) การรายงานต่อคณะกรรมการบริหารความเสี่ยง

คณะกรรมการบริหารความเสี่ยงมีบทบาทโดยตรงในการกำหนดนโยบายและแนวทางการบริหารความเสี่ยงโดยรวมของ สง. ดังนั้น คณะกรรมการบริหารความเสี่ยงจะต้องมีการประชุมเป็นระยะๆ ตามความเหมาะสม เพื่อกำหนดหรือทบทวนนโยบาย ตลอดจนให้ข้อเสนอแนะเพื่อเป็นแนวทางในการวางระบบควบคุมอย่างเพียงพอ และมีประสิทธิภาพ รวมทั้ง จัดเตรียมรายงานที่เกี่ยวข้อง เช่น รายงานข้อผิดพลาด ข้อมูลความเสียหายที่เกิดขึ้นในแต่ละหน่วยธุรกิจ และรายงานการปฏิบัติที่ไม่เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ เป็นต้น เพื่อรายงานต่อคณะกรรมการ สง. หรือคณะกรรมการตรวจสอบตามความเหมาะสม ทั้งนี้ สง. ต้องจัดให้หน่วยงานด้านการบริหารความเสี่ยง หรือหน่วยธุรกิจอื่น มีกระบวนการในการรายงานข้อมูลความเสี่ยงอันเป็นประโยชน์ต่อการตัดสินใจในเชิงนโยบายต่อคณะกรรมการบริหารความเสี่ยงอย่างสม่ำเสมอด้วย โดย สง. อาจกำหนดในการรายงานให้หน่วยงานตรวจสอบภายในเข้าร่วม

สังเกตการณ์ และให้ความเห็นในการปรับปรุงระบบและวางกฎระเบียบเพื่อป้องกันและลดความเสี่ยงที่เกิดขึ้นได้อย่างเป็นอิสระ

(4) การรายงานต่อผู้บริหารของ สง.

หน่วยธุรกิจจะต้องรายงานความเสียหายที่เกิดขึ้นจากการดำเนินงาน ตลอดจนแนวทางการแก้ไขปัญหาให้ผู้บริหารของ สง. ทราบ ควบคู่ไปกับรายงานต่อหน่วยงานการบริหารความเสี่ยง เพื่อให้ผู้บริหารได้รับทราบถึงปัญหาที่เกิดขึ้น พร้อมทั้งกำหนดแนวทางในการแก้ไขปัญหาได้อย่างทันท่วงที และจำกัดความเสียหายหรือลดผลกระทบที่อาจจะเกิดขึ้นต่อการดำเนินงานได้

(5) การรายงานต่อหน่วยงานด้านการบริหารความเสี่ยงด้านปฏิบัติการ

หน่วยธุรกิจของ สง. ต้องรวบรวมผลการประเมินความเสี่ยง ข้อมูลเหตุการณ์ความเสียหาย ข้อมูลตัวชี้วัดความเสี่ยง และข้อมูลความเสี่ยงที่เกิดขึ้นจากการดำเนินงาน ให้หน่วยงานการบริหารความเสี่ยงด้านปฏิบัติการทราบอย่างสม่ำเสมอตามที่หน่วยงานการบริหารความเสี่ยงกำหนด เพื่อให้หน่วยงานการบริหารความเสี่ยงสามารถนำข้อมูลต่างๆ ไปวิเคราะห์ในภาพรวม และเสนอแนวทางในการป้องกัน ควบคุม และลดความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงต่อไป โดย สง. อาจพัฒนาการรายงานข้อมูลต่าง ๆ ผ่านระบบสารสนเทศในรูปแบบ Real Time หรือกำหนดเวลาการรายงานตามความเหมาะสมได้

- **ระบบข้อมูลสารสนเทศเพื่อการบริหารความเสี่ยงด้านปฏิบัติการ**

ระบบข้อมูลสารสนเทศเป็นองค์ประกอบสำคัญที่จะช่วยให้การบริหารติดตาม ควบคุม และลดความเสี่ยงด้านปฏิบัติการเป็นไปอย่างมีประสิทธิภาพมากขึ้น โดย สง. อาจพัฒนาระบบเองหรือให้ผู้บริการภายนอกเป็นผู้ดำเนินการ ซึ่งการจัดทำระบบข้อมูลสารสนเทศเพื่อรองรับระบบการบริหารความเสี่ยงด้านปฏิบัติการ มีข้อควรพิจารณาในเบื้องต้น ดังนี้

(1) ระบบข้อมูลสารสนเทศควรจะช่วยในการจัดเก็บข้อมูลที่เกี่ยวข้อง และจำเป็นต่อการบริหารจัดการความเสี่ยงด้านปฏิบัติการได้อย่างครบถ้วน ถูกต้องและทันเหตุการณ์ เช่น ข้อมูลเหตุการณ์ความเสียหายที่เกิดขึ้นในอดีต ข้อมูลดัชนีชี้วัดความเสี่ยง ข้อมูลประกอบการคำนวณโอกาสที่จะเกิดความเสี่ยง และข้อมูลความเสียหาย เป็นต้น

(2) ระบบข้อมูลสารสนเทศสามารถใช้สนับสนุนการปฏิบัติงานและการบริหารงาน

ของผู้บริหารในทุกระดับ เพื่อใช้ในการติดตาม ประเมิน ควบคุมและลดความเสี่ยง รวมถึงการตัดสินใจในเชิงนโยบายที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านปฏิบัติการได้

(3) ระบบข้อมูลสารสนเทศสามารถใช้สนับสนุนการคำนวณเงินกองทุน หรือรองรับความต้องการที่ใช้ในการบริหารความเสี่ยงด้านปฏิบัติการตามกฎเกณฑ์ ข้อบังคับของทางการ รวมทั้งมีข้อมูลที่สามารถนำไปใช้ในการพัฒนา หรือการสร้างแบบจำลองเพื่อบริหารความเสี่ยงด้านปฏิบัติการ (Operational Risk Model) ได้ด้วย

(4) ระบบข้อมูลสารสนเทศที่ สง. จัดทำขึ้น ต้องมีข้อมูลเพียงพอสำหรับจัดทำรายงานความเสี่ยง มีการจัดเก็บข้อมูลให้ถูกต้องเป็นปัจจุบัน และสอดคล้องกับการปฏิบัติงาน รวมทั้งมีการควบคุมการใช้งานระบบข้อมูลสารสนเทศอย่างเหมาะสม

- **การเปิดเผยข้อมูล**

สง. ควรเปิดเผยข้อมูลเกี่ยวกับการบริหารความเสี่ยงอย่างเพียงพอต่อสาธารณชนและผู้มีส่วนได้เสีย ทั้งนี้ ความเพียงพอของการเปิดเผยข้อมูลจะขึ้นอยู่กับขนาด ความซับซ้อนและความเสี่ยงของการดำเนินธุรกิจของ สง. แต่ละแห่ง นอกจากนี้ สง. ควรเปิดเผยวิธีการดำรงเงินกองทุนขั้นต่ำสำหรับความเสี่ยงด้านปฏิบัติการที่ สง. เลือกใช้ด้วย (ผู้ตรวจสอบสามารถศึกษารายละเอียดการเปิดเผยข้อมูลได้จากแนวทาง Pillar 3 Market Discipline ของ Basel Committee on Banking Supervision (BCBS) [14]

นอกจากการเปิดเผยข้อมูลให้แก่สาธารณชนและผู้มีส่วนได้เสียแล้ว สง. ควรเปิดเผยข้อมูลระหว่างบริษัทในกลุ่มธุรกิจทางการเงินด้วย เพื่อให้สามารถบริหารความเสี่ยงของกลุ่มธุรกิจทางการเงินได้อย่างมีประสิทธิภาพ และสามารถกำกับดูแลกลุ่มธุรกิจทางการเงินให้สอดคล้องกับเกณฑ์ที่ธนาคารแห่งประเทศไทยประกาศกำหนด โดยข้อมูลที่ควรเปิดเผยระหว่างบริษัทในกลุ่มธุรกิจทางการเงินมี ดังนี้ [15]

(1) ข้อมูลที่บริษัทแม่สามารถเปิดเผยให้แก่บริษัทลูกในกลุ่มธุรกิจทางการเงิน ได้แก่ข้อมูลยอดคงค้างของรายการต่างๆ ที่บริษัทลูกดังกล่าวจำเป็นต้องทราบ เพื่อปฏิบัติตามเกณฑ์

---

[14] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 96/2551 เรื่อง การเปิดเผยข้อมูลเกี่ยวกับการดำรงเงินกองทุนสำหรับธนาคารพาณิชย์ ลงวันที่ 27 พฤศจิกายน 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510557.pdf

[15] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 66/2551 เรื่อง หลักเกณฑ์การกำกับแบบรวมกลุ่ม ลงวันที่ 3 สิงหาคม 2551 หน้า 53 ข้อ 112
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510356.pdf

กำกับดูแลเชิงปริมาณตามหลักเกณฑ์การกำกับแบบรวมกลุ่ม ทั้งนี้ บริษัทลูกจะต้องไม่ทำการใดอันอาจเข้าข่ายเป็นการประกอบธุรกิจข้อมูลเครดิตตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

(2) ข้อมูลที่บริษัทลูกในกลุ่มธุรกิจทางการเงินสามารถเปิดเผยให้แก่บริษัทแม่ ได้แก่ ข้อมูลต่างๆ ที่บริษัทแม่จำเป็นต้องใช้ในการบริหารและกำกับดูแลความเสี่ยงของกลุ่มธุรกิจทางการเงินให้เป็นไปตามกลยุทธ์ของกลุ่มธุรกิจทางการเงิน หรือเกณฑ์กำกับดูแลเชิงปริมาณตามหลักเกณฑ์การกำกับแบบรวมกลุ่ม หรือข้อมูลต่างๆ ที่ใช้ในการจัดทำรายงานเพื่อส่งให้แก่ธนาคารแห่งประเทศไทย เช่น ข้อมูลเกี่ยวกับความเสี่ยงด้านเครดิต ตลาด สภาพคล่อง การปฏิบัติการ และข้อมูลยอดคงค้างของรายการต่างๆ เป็นต้น ทั้งนี้ บริษัทแม่จะต้องไม่กระทำการใดอันอาจเข้าข่ายเป็นการประกอบธุรกิจข้อมูลเครดิตตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

2.3.4 การควบคุมและลดความเสี่ยง

ระบบการควบคุมภายในที่มีประสิทธิภาพเป็นกลไกสำคัญในการควบคุมและป้องกันความเสียหายที่อาจเกิดขึ้นได้ นอกจากการใช้ระบบควบคุมภายในแล้ว สง. ควรจัดให้มีนโยบายและกระบวนการเพื่อลดความเสี่ยงอย่างชัดเจน พร้อมแนวทางในการดำเนินการที่เหมาะสม เช่น กรณีที่ความเสี่ยงสูงเกินระดับที่กำหนดไว้ หน่วยงานต้องจัดให้มีการลดความเสี่ยง ด้วยการเพิ่มการควบคุม หรือลดปริมาณธุรกรรมที่ทำลง ถ้าความเสี่ยงสูงเกินกว่าระดับที่ยอมรับได้ สง. อาจตัดสินใจหยุดการทำธุรกรรมนั้น หรืออาจลดความเสียหายที่อาจเกิดขึ้นด้วยการทำประกันภัย เป็นต้น

วัตถุประสงค์หลักของระบบการควบคุมภายในเพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ หลังจากที่ได้ดำเนินการประเมินความเสี่ยงแล้ว สง. ควรจัดอันดับความเสี่ยง โดยเรียงตามลำดับความสำคัญ เพื่อวางระบบการควบคุมความเสี่ยงในแต่ละประเภทของหน่วยธุรกิจนั้นๆ ซึ่งระบบการควบคุมที่ดีจะต้องง่ายต่อการนำไปปฏิบัติ โดยมีต้นทุนที่ไม่สูงมากจนเกินไป และเมื่อนำระบบการควบคุมมาใช้ปฏิบัติจริง ต้องไม่ส่งผลกระทบเชิงลบต่อกระบวนการทำงานและคุณภาพของงาน และระบบการควบคุมต้องสามารถลดความเสี่ยงได้อย่างชัดเจนด้วย สำหรับหลักเกณฑ์การวางระบบการควบคุมภายใน คือ การพิจารณาผลการประเมินความเสี่ยง โดยวิเคราะห์โอกาสที่จะเกิดความเสี่ยงและระดับความรุนแรงของความเสียหายที่อาจเกิดขึ้น กล่าวคือ

(1) ธุรกรรมใดที่มีโอกาสจะเกิดความเสี่ยงสูง แต่ผลกระทบต่ำ (High Frequency / Low Severity) สง. อาจใช้มาตรการควบคุมที่ช่วยลดโอกาสที่จะเกิดความเสี่ยงนั้น เช่น การเพิ่ม

กระบวนการในการสอบยัน (Check and Balance) หรือจัดทำคู่มือการปฏิบัติงาน เป็นต้น

(2) ธุรกรรมใดที่มีโอกาสจะเกิดความเสี่ยงต่ำ แต่ผลกระทบมีความรุนแรงสูง (Low Frequency/High Severity) การควบคุมความเสี่ยงกระทำโดยหามาตรการในการลดหรือจำกัดผลกระทบที่อาจจะเกิดขึ้น เช่น การกำหนดเพดานการทำธุรกรรม การทำประกันภัย และการใช้เครื่องมือในการกระจายความเสี่ยง เป็นต้น

(3) ธุรกรรมใดที่มีโอกาสจะเกิดความเสี่ยงสูง และผลกระทบมีความรุนแรงสูง (High Frequency/High Severity) สง. ควรหลีกเลี่ยง หรือยกเลิกการดำเนินงานนั้นๆ ไป หรืออาจพิจารณาจ้างบุคคลภายนอกมาดำเนินการแทน (Outsourcing) เพื่อเป็นการลด หรือขจัดความเสี่ยงนั้นๆ ออกไปจากการดำเนินงานของ สง.

ดังนั้น เพื่อสร้างระบบการควบคุมภายในที่ดี มีการบริหารงานที่โปร่งใส เป็นธรรม และมีจริยธรรมเพียงพอ รวมทั้ง มีการวางระบบควบคุมเพื่อป้องกัน และลดความเสี่ยงด้านปฏิบัติการที่อาจจะเกิดขึ้นในการดำเนินงานได้อย่างเหมาะสม คณะกรรมการ สง. หรือคณะกรรมการที่ได้รับมอบหมาย และผู้บริหารระดับสูงควรกำหนดนโยบาย และแนวทางการพัฒนาระบบการควบคุมของหน่วยธุรกิจต่างๆ โดยสามารถอ้างอิงหลักการควบคุมที่ดี ได้ดังนี้

ก) การมีส่วนร่วมของผู้บริหาร สง.

ผู้บริหารของ สง. ควรมีส่วนร่วมในการจัดทำ ทบทวนและประเมินระบบการควบคุมกระบวนการทำงานของหน่วยธุรกิจต่างๆ ในทุกระดับชั้น รวมถึงมีส่วนร่วมในการพิจารณารายงานต่างๆ ที่เกี่ยวข้องกับการควบคุม หรือการรายงานสถานะความเสี่ยงของหน่วยธุรกิจที่ตนดูแลรับผิดชอบอย่างสม่ำเสมอด้วย เช่น รายงานสถานะของการดำเนินงาน รายงานข้อมูลดัชนีชี้วัดความเสี่ยง รายงานข้อมูลเหตุการณ์ความเสียหาย รายงานการตรวจสอบภายใน เป็นต้น เพื่อให้สามารถติดตามการเปลี่ยนแปลง และเป็นข้อมูลประกอบการตัดสินใจเชิงนโยบาย เพื่อตอบสนองต่อการเปลี่ยนแปลงของปัจจัยเสี่ยงได้อย่างทันท่วงที รวมทั้ง เป็นการกระตุ้นให้ผู้บริหารในระดับชั้นต่างๆ สามารถประเมินความเหมาะสมของระบบการควบคุม เพื่อปรับปรุง และพัฒนาประสิทธิภาพการทำงานและลดความเสี่ยงให้อยู่ในระดับที่เหมาะสมที่ สง. ยอมรับได้อีกด้วย

ข) การควบคุมการปฏิบัติงานในแต่ละหน่วยธุรกิจ

ระบบการควบคุมของแต่ละหน่วยธุรกิจที่ สง. เลือกใช้อาจมีความเหมือนหรือความแตกต่างกันก็ได้ ขึ้นอยู่กับลักษณะการดำเนินงาน และระดับความเสี่ยงของหน่วยธุรกิจนั้นๆ เช่น การวางระบบการควบคุมกระบวนการทำงานที่เกี่ยวข้องกับเงินสดควรเน้นการป้องกันการทุจริต และความปลอดภัยของเงินสด โดยการวางระบบการสอบยัน การกำหนดเพดาน รวมถึงมีการกระทบยอดเงินสดอย่างรัดกุม หรือสำหรับหน่วยงานที่ทำหน้าที่วิเคราะห์ ควรมุ่งเน้นที่ความถูกต้องของข้อมูล ประสิทธิภาพของระบบการจัดเก็บและประมวลผลข้อมูล การรักษาความลับลูกค้า และคุณภาพการวิเคราะห์ข้อมูล เป็นต้น ซึ่งผู้ที่เกี่ยวข้องโดยตรงที่มีความชำนาญของแต่ละหน่วยธุรกิจนั้นๆ ควรมีส่วนร่วมในการวางระบบการควบคุม หรือ มีบุคคลหรือหน่วยงานที่เป็นอิสระ ทำหน้าที่ตรวจสอบ หรือทบทวนประสิทธิภาพของระบบการควบคุมและสม่ำเสมอด้วย เช่น หน่วยงานตรวจสอบภายใน หน่วยงานบริหารความเสี่ยง หน่วยงานด้านการควบคุม หรือ ผู้ตรวจสอบภายนอก เป็นต้น

ค) การอนุมัติและอำนาจการอนุมัติ

สง. ควรมีการกำหนดขอบเขตอำนาจ หน้าที่ และความรับผิดชอบของบุคคล หรือตำแหน่งงานใดๆ ให้ชัดเจน รวมทั้ง มีการกำหนดเพดานอำนาจการอนุมัติไว้ เพื่อให้เกิดระบบการกลั่นกรองงานที่ดี มีความเหมาะสม

สอดคล้องกับขนาดของธุรกรรม และขอบเขตอำนาจความรับผิดชอบของผู้บริหารในระดับชั้นการบังคับบัญชาต่างๆ

ง) การสอบทานความถูกต้อง

การสอบทานความถูกต้องของการทำธุรกรรมต่างๆ ของ สง. เป็นเครื่องมือที่ สง. สามารถใช้ เพื่อตรวจสอบว่าการปฏิบัติงานของพนักงาน หรือการทำงานของระบบงานต่างๆ สามารถดำเนินงานได้อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งเมื่อมีการดำเนินงานที่เกี่ยวข้องกับสินทรัพย์ที่มีตัวตน หรืองานประมวลผลที่ต้องการความถูกต้องสูง เช่น ระบบบัญชีต่างๆ รวมถึงการใช้แบบจำลองเพื่อการวิเคราะห์และการวางแผนในการดำเนินธุรกิจ เป็นต้น ดังนั้น สง. ควรมีระบบการตรวจสอบเพื่อยืนยันความถูกต้องอย่างสม่ำเสมอ เพื่อให้สามารถดำเนินการแก้ไขได้ทันท่วงที หากเกิดการทุจริต การผิดพลาดในการดำเนินงาน หรือประมวลผลข้อมูลขึ้น ซึ่งโดยทั่วไปแล้ว การสอบทานความถูกต้องหรือการตรวจสอบรายการกระทบยอดต่างๆ ควรดำเนินการโดยบุคคล หรือหน่วยงานอิสระอื่นที่ไม่ได้ทำรายการ หรือไม่ได้รับผิดชอบโดยตรงในการทำรายการนั้นๆ

จ) การแบ่งแยกหน้าที่

ระบบการควบคุมที่ดีจะต้องมีการแบ่งแยกหน้าที่และความรับผิดชอบแก่บุคคล อย่างเหมาะสม และไม่ซ้ำซ้อน โดยมีการกำหนดโครงสร้างองค์กร และการมอบหมายงานที่ไม่ก่อ ให้เกิดจุดอ่อนในการควบคุมภายใน นอกจากนี้ เพื่อให้มีการปฏิบัติหน้าที่โดยคำนึงถึงผลประโยชน์ของ สง. เป็นหลัก การกำหนดการแบ่งแยกหน้าที่นั้นควรพิจารณาประเด็นของการตรวจสอบ และการถ่วงดุลอำนาจด้วย โดยการกำหนดขอบเขตหน้าที่ และช่วยลดความเสี่ยงจากการแก้ไข เปลี่ยนแปลง หรือปกปิดข้อมูลจากการปฏิบัติหน้าที่โดยมิชอบ หรือทุจริต หรือไม่ควรมอบหมายให้บุคคล หรือตำแหน่งงานใดๆ มีอำนาจในการอนุมัติรายการตั้งแต่ต้นจนจบ เช่น การอนุมัติรายการ การจ่ายเงิน การตรวจสอบธุรกรรม และการกระทบยอดรายการ หรือมีอำนาจอนุมัติธุรกรรมการดำเนินธุรกิจทั้งในบัญชีเพื่อการค้าและบัญชีเพื่อการธนาคาร เนื่องจากจะเปิดโอกาสให้มีการปกปิดรายการขาดทุนจากการลงทุนโดยการโอนย้ายรายการระหว่างบัญชีทั้ง 2 บัญชีได้ เป็นต้น

ฉ) การใช้บริการจากบุคคลภายนอก (Outsourcing) [16]

การใช้บริการจากบุคคลภายนอกของ สง. สามารถแบ่งกลุ่มงานในการใช้บริการได้ ดังนี้

- กลุ่มที่ 1 กลุ่มงานหลักที่มีความสำคัญต่อธุรกิจสถาบันการเงิน
- กลุ่มที่ 2 กลุ่มงานสนับสนุนธุรกิจสถาบันการเงิน
- กลุ่มที่ 3 กลุ่มงานที่ไม่ถือว่าเป็นการใช้บริการจากบุคคลภายนอก

กลุ่มที่ 1 กลุ่มงานหลักที่มีความสำคัญต่อธุรกิจสถาบันการเงิน	กลุ่มที่ 2 กลุ่มงานสนับสนุนธุรกิจสถาบันการเงิน	กลุ่มที่ 3 กลุ่มงานที่ไม่ถือว่าเป็นการใช้บริการจากบุคคลภายนอก
กลุ่มงานที่มีความสำคัญและมีผลกระทบโดยตรงต่อทิศทางการดำเนินธุรกิจหากงานดังกล่าวมีการหยุดชะงักลงหรือไม่สามารถใช้บริการได้อย่างต่อเนื่องจะเกิดผลกระทบรุนแรงต่อการดำเนินธุรกิจของสถาบันการเงิน	กลุ่มงานที่ปฏิบัติการสนับสนุนธุรกิจหลักของสถาบันการเงินหรือเอื้ออำนวยต่อการดำเนินงานปกติของสถาบันการเงิน เช่น งานลูกค้าสัมพันธ์ งานบริหารบุคลากร	กลุ่มงานที่โดยปกติบุคคลภายนอกเป็นผู้ดำเนินการให้อยู่แล้ว ซึ่งไม่เข้าข่ายเป็นการใช้บริการจากบุคคลภายนอก รวมไปถึงกลุ่มงานบริการอำนวยความสะดวกทั่วไปที่มีความเสี่ยงต่ำ
สง. ต้องขออนุญาตมายังธนาคารแห่งประเทศไทยก่อนการใช้บริการบุคคลภายนอก	อนุญาตเป็นการทั่วไปให้ใช้บริการจากบุคคลภายนอกได้ โดยต้องปฏิบัติตามหลักเกณฑ์กำกับดูแลผู้ให้บริการฯ	อนุญาตเป็นการทั่วไปให้ใช้บริการจากบุคคลภายนอกได้ โดย สง. ต้องกำหนดหลักเกณฑ์ในการกำกับดูแลผู้ให้บริการเอง

ในกรณีที่ สง. ใช้บริการจากผู้ให้บริการภายนอกรายอื่น (Service Provider) หรือการแต่งตั้งตัวแทนปฏิบัติงานแทน (Authorised agents) เพื่อเพิ่มประสิทธิภาพและลดค่าใช้จ่ายในการดำเนินการ สง. ควรให้ความสนใจเป็นพิเศษ เนื่องจากปัจจัยความเสี่ยงอยู่นอกเหนือการควบคุม

[16] ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 43/2551 เรื่อง หลักเกณฑ์เกี่ยวกับการใช้บริการจากบุคคลภายนอก (Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510333.pdf

ของ สง. ดังนั้น สง. จึงควรจัดทำนโยบายการบริหารความเสี่ยงที่เกิดจากการใช้บริการดังกล่าว โดยพิจารณาดังต่อไปนี้

(1) คณะกรรมการหรือผู้บริหารระดับสูงของ สง. ควรจัดทำและอนุมัตินโยบายการกำกับดูแลกระบวนการใช้บริการจากภายนอกตามแนวความเสี่ยง ซึ่งนโยบายควรครอบคลุมความเสี่ยงที่เกิดจากการใช้บริการภายนอกและมีความเหมาะสมกับขนาดและความซับซ้อนของ สง.

(2) ควรมีการระบุความเสี่ยงของการใช้บริการจากภายนอก โดยการกำหนดความต้องการเป็นลายลักษณ์อักษรเพื่อใช้ในการควบคุมการดำเนินการของผู้ให้บริการ ซึ่งจะเป็นแนวทางในการบริหารงานและควบคุมความเสี่ยง เช่น กำหนดขอบเขตและลักษณะงานที่จะใช้บริการจากบุคคลภายนอก เป็นต้น

(3) ควรจัดทำแผนฉุกเฉินการสำรองข้อมูลที่พร้อมใช้งาน ขั้นตอนและวิธีการดำเนินการเพื่อแก้ไขปัญหาหรือฟื้นฟูความเสียหาย หากต้องเลิกใช้บริการจากผู้ให้บริการนั้น เพื่อรองรับกรณีเกิดปัญหาจากการใช้บริการจากผู้ให้บริการรายอื่นไว้อย่างชัดเจน

(4) ควรประเมินนโยบายการใช้บริการจากผู้ให้บริการรายอื่นเป็นระยะๆ หรืออย่างน้อยปีละ 1 ครั้ง เพื่อพิจารณาความมีประสิทธิภาพ ความเหมาะสม และสอดคล้องกับเป้าหมายที่กำหนด

ช) การปฏิบัติงานให้เป็นไปตามกฎระเบียบที่กำหนด

สง. ควรกำหนดให้มีหน่วยงานกำกับดูแลการปฏิบัติงานแยกเป็นอิสระจากหน่วยงานที่ทำธุรกรรม เพื่อทำหน้าที่ดูแลการดำเนินการของ สง. ให้เป็นไปตามนโยบายและวิธีการ เพื่อให้มั่นใจว่า หน่วยธุรกิจต่างๆ ดำเนินงานสอดคล้องภายใต้ขอบเขตของกฎระเบียบ ข้อบังคับต่างๆ ที่ สง. หน่วยงานของรัฐ หรือองค์กรที่เกี่ยวข้องได้กำหนดไว้ เพื่อหลีกเลี่ยงการดำเนินธุรกิจที่อาจก่อให้เกิดความเสี่ยง หรือความเสียหายทั้งในแง่ของความเสียหายทางการเงิน (Financial loss) และความเสียหายด้านชื่อเสียง (Reputation loss) ทั้งนี้ สง. ควรมีระบบการรายงาน และการติดตามความคืบหน้าในกรณีที่หน่วยงานไม่ปฏิบัติตาม หรือมีการละเว้นการไม่ปฏิบัติตามกฎระเบียบ ข้อบังคับ เพื่อให้ผู้บริหารรับทราบและสามารถติดตาม หรือแก้ไขได้ทันก่อนที่จะเกิดความเสียหายต่อการดำเนินงานของ สง. ในภาพรวมได้

ซ) กฎเกณฑ์การรู้จักลูกค้า (Know Your Customer) [17]

หนึ่งในมาตรฐานสากลของ Basel Committee (BIS Core Principle (CP)) ได้กำหนดกฎเกณฑ์การรู้จักลูกค้า(Know Your Customer) โดยการที่ผู้กำกับดูแลจะต้องกำหนดให้ สง. มีนโยบาย ระเบียบปฏิบัติและขั้นตอนการปฏิบัติที่เพียงพอต่อการรู้จักลูกค้า รวมถึงมีกฎเกณฑ์การตรวจสอบเพื่อทราบข้อเท็จจริงลูกค้า (Customer Due Diligence for Banks) เพื่อป้องกันมิให้ สง. ถูกใช้เป็นเครื่องมือในการประกอบอาชญากรรม หรือฟอกเงิน หรือการสนับสนุนทางการเงินแก่การก่อการร้ายทั้งตั้งใจหรือไม่ตั้งใจ เนื่องจาก การฟอกเงิน (Money Laundering) เป็นการกระทำที่ทำให้เงินหรือทรัพย์สินที่ได้มา โดยการกระทำความผิดมูลฐาน แปรสภาพเป็นเงินหรือทรัพย์สินที่ได้มาโดยเสมือนหนึ่งถูกต้องตามกฎหมาย หรืออีกนัยหนึ่งคือ การเปลี่ยนสภาพทรัพย์สินที่ได้มาโดยไม่ชอบด้วยกฎหมายหรือไม่สุจริตให้กลายสภาพเป็นทรัพย์สินที่ดูเหมือนได้มาโดยถูกต้องตามกฎหมายหรือพิสูจน์ไม่ได้ว่าทุจริต เป้าหมายสำคัญของการฟอกเงินคือ การใช้ สง. เป็นเครื่องมือในการเปลี่ยนสภาพเงินที่มีแหล่งที่มาต่างๆ ที่ไม่ถูกต้องตามกฎหมาย มาเป็นเงินที่แสดงถึงที่มาอย่างถูกต้องตามกฎหมายสามารถสอบทานแหล่งที่มาได้ เพราะว่าเงินที่หมุนเวียนหรือถ่ายโอนต่างๆ จะต้องใช้บริการจาก สง.

ดังนั้น สง. ควรกำหนดนโยบาย หลักเกณฑ์และระเบียบปฏิบัติเกี่ยวกับธุรกรรมต่างๆ ที่ สง. ให้บริการแก่ลูกค้า เพื่อเป็นการป้องกันการฟอกเงิน และการสนับสนุนทางการเงินแก่การก่อการร้ายของ สง. (AML/CFT) รวมทั้งจัดให้มีการปฏิบัติและการควบคุมให้เป็นไปตามประกาศ ข้อกำหนด หรือหลักเกณฑ์ที่กำหนดโดยสำนักงานป้องกันและปราบปรามการฟอกเงินและธนาคารแห่งประเทศไทย เช่น พ.ร.บ.ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และแนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง มาตรการป้องกันปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้ายของ สง. ลงวันที่ 3 สิงหาคม 2551 ซึ่งมีขอบเขตครอบคลุม ดังนี้

- การกำหนดนโยบายด้าน AML/CFT

[17] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อ มาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย (Anti-Money Laundering and Combating the Financing of Terrorism : AML/CFT) ของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510390.pdf

- แนวทางการปฏิบัติตามนโยบายด้าน AML/CFT
- ขั้นตอนการปฏิบัติตามนโยบายด้าน AML/CFT
- โครงสร้างองค์กร โดยมีการจัดตั้งหน่วยงานที่เป็นอิสระเพื่อทำหน้าที่ดูแล
- ระเบียบปฏิบัติ และการจัดทำคู่มือ/ขั้นตอนการปฏิบัติงานของหน่วยงานที่รับลูกค้า
- การฝึกอบรมพนักงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ในการรับลูกค้า
- ระบบการควบคุมภายใน โดยมีระบบการควบคุม และติดตามการปฏิบัติ / การตรวจสอบที่ดีและมีประสิทธิภาพ
- ระบบเทคโนโลยีสารสนเทศที่สามารถรองรับระบบคอมพิวเตอร์ของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ตลอดจนระบบการรักษาความปลอดภัยในระหว่างการรับ-ส่งข้อมูล
- ระบบรายงานการทำธุรกรรมที่รายงานต่อ ปปง. และการเก็บรักษาข้อมูล

ทั้งนี้ รายละเอียดเกี่ยวกับวิธีการหรือขั้นตอนการปฏิบัติงาน ผู้ตรวจสอบสามารถศึกษาเพิ่มเติมได้จากคู่มือการตรวจสอบการป้องกันการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้ายในภาคผนวก 4.1 ข้อ 1

นอกจากหลักเกณฑ์ระบบการควบคุมภายในที่ดี ที่กล่าวข้างต้นแล้วนั้น ประเด็นที่ควรพิจารณาในการจัดทำระบบการควบคุมความเสี่ยงมี ดังนี้

- **บุคลากรและการฝึกอบรม**

พนักงานถือเป็นบุคลากรที่มีความสำคัญต่อการปฏิบัติงาน ดังนั้น สง. ควรพิจารณาในเรื่องต่อไปนี้ เพื่อลดความเสี่ยงด้านปฏิบัติงาน

- คัดเลือก อบรมและพัฒนาพนักงานให้มีคุณสมบัติ ประสบการณ์และความสามารถเหมาะสมต่อการปฏิบัติงาน รวมถึงการจัดให้มีทรัพยากรในการปฏิบัติงานต่างๆ อย่างเพียงพอ

- ส่งเสริมให้พนักงานตระหนักถึงหน้าที่ความรับผิดชอบต่อการบริหารความเสี่ยงด้านปฏิบัติการขององค์กร รวมทั้งจริยธรรมในการปฏิบัติงาน

- นำหลักการควบคุมภายในที่ดีมาใช้ เช่น การแบ่งแยกหน้าที่ การสอบยันการปฏิบัติงาน ระบบการปฏิบัติงานโดย 2 ฝ่าย การยืนยันกระทบยอดอย่างสม่ำเสมอ และดูแลให้ความขัดแย้งด้านผลประโยชน์น้อยที่สุด เป็นต้น

- ดูแลนโยบายการกำหนดค่าตอบแทนให้เหมาะสม เช่น หากกำหนดนโยบายการจ่ายเงินค่าตอบแทนโดยพิจารณาผลกำไรจากการดำเนินงานเพียงอย่างเดียว อาจทำให้เกิดการละเว้นการปฏิบัติงานตามกฎระเบียบได้ เป็นต้น

- จัดให้มีคู่มือและเอกสารการปฏิบัติงานที่ชัดเจน โดยเฉพาะในส่วนที่เกี่ยวกับการปฏิบัติการที่ใช้ระบบเทคโนโลยีที่ซับซ้อน มีธุรกรรมจำนวนมาก หรือในส่วนที่จำเป็นต้องปฏิบัติตามกฎหมายหรือกฎเกณฑ์ข้อบังคับ รวมทั้งควรระบุจุดที่มีความเสี่ยงไว้ในคู่มือการปฏิบัติงานด้วย

- ดูแลให้พนักงานปฏิบัติตามระเบียบ กฎเกณฑ์ข้อบังคับและวิธีปฏิบัติงานอย่างเคร่งครัด รวมทั้งควรกำหนดมาตรการลงโทษพนักงานที่ไม่ปฏิบัติตามระเบียบ กฎเกณฑ์อย่างชัดเจน

- **กระบวนการปฏิบัติงานและระบบงาน**

การกำหนดกระบวนการปฏิบัติงานที่ชัดเจนและมีระบบงานที่เพียงพอ จะช่วยให้ สง. ปฏิบัติงานได้ตามวัตถุประสงค์ที่กำหนดและช่วยเพิ่มประสิทธิภาพการปฏิบัติงาน โดย สง. ควรพิจารณาในเรื่องต่อไปนี้

(1) <u>ระบบเทคโนโลยีสารสนเทศ</u> ผู้บริหารระดับสูงควรจัดให้มีระบบที่มีความเหมาะสมกับขนาดและความซับซ้อนของ สง. โดยการพัฒนาปรับปรุง ควบคุมและตรวจสอบระบบอย่างสม่ำเสมอ ตลอดจนให้มีการเตรียมความพร้อมในเรื่องศูนย์สำรองข้อมูลและแผนฉุกเฉิน

(2) <u>คู่มือการปฏิบัติงาน</u> ผู้บริหารระดับสูงควรดำเนินการให้มีคู่มือเกี่ยวกับขั้นตอนและกระบวนการปฏิบัติงานภายในของแต่ละส่วนงาน และระหว่างส่วนงานต่างๆ ที่ชัดเจนและเข้าใจง่ายต่อการปฏิบัติงาน เพื่อให้ทุกส่วนงานสามารถปฏิบัติงานได้อย่างต่อเนื่องและลดความผิดพลาดที่อาจเกิดขึ้นได้ในภายหลัง

(3) <u>ระบบเอกสารสัญญา เอกสารเผยแพร่ เอกสารโฆษณา และการประชาสัมพันธ์</u> รวมถึงข้อมูลที่เปิดเผยในงบการเงินที่เผยแพร่สู่สาธารณชน ควรได้รับการตรวจสอบความถูกต้องโดยหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานที่ดูแลด้านการปฏิบัติตามกฎระเบียบ ฝ่ายกฎหมาย หรือฝ่ายงานที่เกี่ยวข้อง เพื่อให้มั่นใจว่า เอกสารสัญญามีผลบังคับตามกฎหมาย และเอกสารที่เผยแพร่มีความชัดเจนและถูกต้อง

<u>ตัวอย่างการปฏิบัติงานที่เหมาะสม</u>

ธนาคารมีการกำหนดแนวทางและวิธีปฏิบัติที่ชัดเจนเกี่ยวกับการประกาศข้อมูลในเรื่องอัตราดอกเบี้ย อัตราส่วนลด และค่าบริการต่างๆ

(4) <u>ระบบการรักษาความปลอดภัยของทรัพย์สินและข้อมูล</u> ผู้บริหารระดับสูงต้องจัดให้มีระบบ ระเบียบหรือวิธีปฏิบัติที่เกี่ยวกับการเข้าถึงทรัพย์สินและข้อมูล รวมทั้งกำหนดชั้นความลับของการเข้าถึงข้อมูลต่างๆ ให้มีความรัดกุม เหมาะสม และดูแลให้มีการปฏิบัติตามระเบียบและวิธีปฏิบัติอย่างเคร่งครัด

(5) <u>การควบคุมการบริหารจัดการระบบข้อมูลสารสนเทศ</u> ผู้บริหารระดับสูงควรกำหนดให้มีมาตรการควบคุมความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการระบบข้อมูลสารสนเทศทั้งในแง่ของความถูกต้อง ความน่าเชื่อถือ การประมวลผล และการรักษาความปลอดภัยของข้อมูลเพื่อป้องกันการทุจริต และการใช้ข้อมูลและการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงประสิทธิภาพในการบริหารงานการจัดเก็บข้อมูล ระบบข้อมูล การลดความเสี่ยงเนื่องจากการหยุดชะงักของระบบคอมพิวเตอร์ และระบบเครือข่ายด้วย ซึ่งระบบการควบคุมขั้นต่ำที่ สง. ควรพิจารณาในเบื้องต้น มีดังนี้

(5.1) สง. ควรมีระบบข้อมูลสำรอง (Back-up) ที่เพียงพอ และจัดเก็บไว้ภายนอกสถานที่ทำการที่ปลอดภัย เพื่อสามารถใช้ปฏิบัติงานได้ทันท่วงที หากระบบข้อมูลได้รับความเสียหายจากเหตุภัยพิบัติต่างๆ ซึ่งขึ้นอยู่กับลักษณะของข้อมูลที่ต้องการสำรอง สถานที่จัดเก็บ และนโยบายของ สง. เป็นสำคัญ โดยมีการวางแผนการจัดการกับข้อมูลและระบบข้อมูลสารสนเทศ ตามมาตรฐานในการบริหารงานระบบข้อมูลสารสนเทศโดยทั่วไป เช่น รายการที่เกิดขึ้นประจำวัน (Daily Transaction) ระบบการกู้คืนข้อมูล ระบบรักษาความปลอดภัยในการจัดเก็บและใช้งานข้อมูล สถานที่จัดเก็บข้อมูลสำรอง เป็นต้น

(5.2) สง. ควรจัดทำคู่มือรายละเอียดขั้นตอนในการใช้ระบบสำรอง การกู้คืนข้อมูล หรือระบบสารสนเทศ รวมถึงการจัดทำแผนรองรับการดำเนินธุรกิจต่อเนื่อง (Business Continuity Plan) เพื่อรองรับการดำเนินงานของระบบงานสำคัญด้วย (รายละเอียดกล่าวไว้ในเรื่องการบริหารความต่อเนื่องทางธุรกิจ)

(5.3) สง. ควรมีมาตรการรักษาความปลอดภัยของข้อมูล เช่น การกำหนดสิทธิการใช้ข้อมูล การเผยแพร่ข้อมูล การแก้ไข หรือการลบข้อมูล การติดตั้งระบบป้องกันและควบคุมการแพร่กระจายของไวรัสคอมพิวเตอร์ และระบบป้องกันการเจาะข้อมูลโดยบุคคลภายนอกอย่างรัดกุมเพื่อรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นต้น

(5.4) ระบบที่พัฒนาโดยผู้ให้บริการจากภายนอก (Outsourcing) สง. ควรกำหนดหลักเกณฑ์การพิจารณาการใช้บริการจากภายนอกอย่างเหมาะสม (ดูประกาศ IT Outsourcing[18]) เนื่องจาก สง. ยังต้องรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ลูกค้าและคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับที่ สง. เป็นผู้ดำเนินการด้านงานเทคโนโลยีสารสนเทศเอง รวมทั้งการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานปกติ เช่น ความเสี่ยงจากการรักษาความลับของข้อมูลลูกค้า เป็นต้น

[18] ประกาศธนาคารแห่งประเทศไทย ที่ สนส.29/2551 เรื่อง การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510319.pdf

- **การบริหารความต่อเนื่องทางธุรกิจ** [19]

สง. ควรมีการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) เพื่อรองรับหรือเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ จากเหตุการณ์ความเสียหายในรูปแบบต่างๆ เช่น การหยุดทำงานของระบบเครือข่ายคอมพิวเตอร์ ระบบสื่อสาร หรือโครงสร้างพื้นฐานในการดำเนินงานด้านต่างๆ การก่อวินาศภัย ภัยพิบัติต่างๆ และภัยจากการระบาดของโรคติดต่อร้ายแรง [20] เป็นต้น โดยต้องครอบคลุมทุกธุรกรรมงานที่สำคัญในองค์กร รวมถึงผู้ให้บริการหลักที่เกี่ยวข้องและปรับปรุงให้เป็นปัจจุบันเสมอเพื่อสามารถนำไปดำเนินงานได้ตรงตามเป้าหมายเมื่อต้องการ

แนวปฏิบัติในการบริหารความต่อเนื่องทางธุรกิจ และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง มีดังนี้

1. คณะกรรมการ สง. และผู้บริหารระดับสูงเป็นผู้รับผิดชอบในการกำหนดกลยุทธ์และนโยบายการบริหารความต่อเนื่องทางธุรกิจของ สง. พร้อมทั้งจัดสรรทรัพยากรเพื่อรองรับการดำเนินงานอย่างเพียงพอ โดยคณะกรรมการอาจมอบหมายหน้าที่ด้านปฏิบัติการให้คณะทำงานหรือผู้บริหารระดับสูงก็ได้ แต่การมอบหมายควรทำเป็นลายลักษณ์อักษร

2. สง. ควรวิเคราะห์และประเมินผลกระทบต่อการหยุดชะงักการดำเนินงานที่สำคัญ (Major Operational Disruptions) เพื่อให้สามารถกำหนดลำดับความสำคัญของการดำเนินงานและทรัพยากรที่จะใช้ในการเรียกคืนการดำเนินงานได้อย่างมีประสิทธิภาพโดยครอบคลุมประเด็นดังต่อไปนี้

- ประเมินความเสี่ยง (Risk Assessment) ที่อาจทำให้ธุรกรรมที่สำคัญเกิดการหยุดชะงักอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่

[19] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) ของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510386.pdf

[20] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การจัดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับกรณีการระบาดของโรคติดต่อร้ายแรง ลงวันที่ 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510387.pdf

สำคัญ โดยควรระบุเหตุการณ์ที่ทำให้เกิดการหยุดชะงัก และประเมินโอกาสที่จะเกิดเหตุการณ์ดังกล่าว เช่น การประท้วงของแรงงาน การสูญเสียผู้บริหารและบุคลากรหลัก เป็นต้น รวมทั้งวิเคราะห์กระบวนการควบคุมความเสี่ยงที่มีอยู่ ปรับปรุงกระบวนการและทรัพยากรที่จำเป็นในการควบคุมความเสี่ยง รวมถึงการจัดทำการประเมินผลและควบคุมกระบวนการดังกล่าว

- วิเคราะห์ผลกระทบทางธุรกิจจากเหตุการณ์ที่อาจเกิดขึ้นกับทุกธุรกรรมที่สำคัญ เพื่อให้ สง. สามารถกำหนดลำดับความสำคัญของการดำเนินงานและจัดสรรทรัพยากรในการเรียกคืนการดำเนินงานได้อย่างมีประสิทธิภาพ โดยพิจารณาถึงผลกระทบต่อผู้มีส่วนได้เสียของ สง. ทั้งในเชิงปริมาณและเชิงคุณภาพ เช่น รายได้ที่อาจสูญเสียไป ค่าใช้จ่ายที่อาจเกิดขึ้น ชื่อเสียงและความน่าเชื่อถือของ สง. เป็นต้น และจัดลำดับความสำคัญของทรัพยากรทั้งภายในและภายนอก สง. ที่จำเป็นในแต่ละธุรกรรมงานที่สำคัญด้วย
- วิเคราะห์และระบุธุรกรรมที่สำคัญ ซึ่งหากมีการหยุดชะงักเกิดขึ้นอาจส่งผลกระทบต่อการดำเนินงาน ชื่อเสียง และผลการดำเนินงานของ สง. อย่างมีนัยสำคัญได้ โดย สง. ควรกำหนดหลักเกณฑ์ที่ชัดเจนในการพิจารณาความสำคัญของแต่ละธุรกรรมงานที่สำคัญด้วย

3. การกำหนดเป้าหมายสำหรับการเรียกคืนการดำเนินงาน

- สง. ควรกำหนดระยะเวลาการหยุดดำเนินงานที่ยอมรับได้และจัดลำดับความสำคัญของแต่ละธุรกรรมที่สำคัญ และกำหนดระยะเวลาในการเรียกคืนการดำเนินงาน โดยระยะเวลาการหยุดดำเนินงานที่ยอมรับได้จะต้องได้รับความเห็นชอบจากคณะกรรมการและผู้บริหารระดับสูงของ สง.
- สง. ควรกำหนดกลยุทธ์การเรียกคืนการดำเนินงานที่เหมาะสมเพื่อให้บรรลุตามเป้าหมายที่ได้กำหนดไว้ โดยต้องจัดสรรทรัพยากรและงบประมาณแก่หน่วยงานที่เกี่ยวข้องอย่างเพียงพอต่อการดำเนิน

กลยุทธ์ดังกล่าว ทั้งนี้ สง. อาจพิจารณาแนวทางการทำประกันภัยเพื่อบรรเทาความเสียหายที่อาจเกิดขึ้น อย่างไรก็ดี การทำประกันภัยไม่ถือเป็นการทดแทนการบริหารความต่อเนื่องทางธุรกิจ

4. สง. ต้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเป็นลายลักษณ์อักษรที่กำหนดขั้นตอนการดำเนินการเพื่อรองรับหรือเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ โดยทุกหน่วยงานที่เกี่ยวข้องต้องมีส่วนร่วมในการทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของตนเอง และเก็บแผนดังกล่าวไว้ที่ผู้รับผิดชอบอย่างน้อยหนึ่งชุดและนอกสถานที่ทำการอีกอย่างน้อยหนึ่งชุด แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องต้องครอบคลุมทุกธุรกรรมงานที่สำคัญในองค์กร รวมถึงผู้ให้บริการหลักที่เกี่ยวข้อง และปรับปรุงให้เป็นปัจจุบันเสมอเพื่อสามารถนำไปดำเนินงานได้ตรงตามเป้าหมายเมื่อต้องการ ซึ่งควรมีรายละเอียดครอบคลุมประเด็นอย่างน้อย ดังนี้

- ขั้นตอนรายละเอียดการดำเนินงานเมื่อมีการหยุดชะงักของธุรกรรมงานที่สำคัญ เพื่อให้สามารถกลับมาดำเนินการได้ตามระยะเวลาที่กำหนด
- ทรัพยากรที่จำเป็นสำหรับปฏิบัติงาน เช่น พนักงาน อุปกรณ์คอมพิวเตอร์ โทรศัพท์ โทรสาร เครื่องใช้สำนักงาน เอกสารสัญญากรมธรรม์ประกันภัย เป็นต้น
- แผนการติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอก สง.
- แผนการจัดตั้งศูนย์ปฏิบัติงานสำรอง (Alternate Sites) เมื่อเห็นว่ามีความจำเป็น

5. หาก สง. ใช้บริการจากผู้ให้บริการหลัก สง. ต้องมั่นใจว่าแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของผู้ให้บริการหลัก มีความสอดคล้องกับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของ สง. ด้วย

- แผนรองรับเหตุฉุกเฉิน (Emergency plan) เป็นแผนปฏิบัติที่มีการกำหนดวิธีการในการรองรับ ควบคุม และแก้ไขเหตุฉุกเฉินต่างๆ เช่น อัคคีภัย แผ่นดินไหว หรืออุบัติเหตุ เป็นต้น ซึ่งจะมีรายละเอียดของมาตรการลดความเสียหายทั้งทางด้านบุคลากร ทรัพย์สินและ

การดำเนินธุรกิจอย่างเหมาะสม มีแผนอพยพพนักงาน และการเคลื่อนย้ายทรัพย์สินที่สำคัญ ตลอดจนมีการกำหนดศูนย์อำนวยการเพื่อแก้ไขเหตุฉุกเฉิน

- แผนสำรองระบบงาน (Back-up plan) เป็นแผนปฏิบัติที่มีรายละเอียดวิธีการในการกำหนดทางเลือกของระบบงาน และวิธีปฏิบัติ เพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง โดยมีการกำหนดสถานที่ปฏิบัติงาน หรือการดำเนินงานสำรอง (Back-up facilities) รวมถึงระบบงานสำรองที่จำเป็นต่าง ๆ (Back-up system) มีการกำหนดการใช้ทรัพยากรในด้านต่างๆ อย่างมีประสิทธิภาพ ตลอดจนมีแผนการติดต่อสื่อสาร และประชาสัมพันธ์กับบุคคล หรือหน่วยงานที่เกี่ยวข้องอื่นๆ
- แผนการฟื้นฟูการดำเนินงาน (Business recovery plan) เป็นแผนปฏิบัติที่มีการกำหนดขั้นตอนการดำเนินการเพื่อฟื้นฟูสภาพความเสียหายให้กลับเข้าสู่การดำเนินธุรกิจตามปกติ

6. สง. ควรกำหนดแผนงานในการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องชัดเจน สอดคล้องกับสถานการณ์ปัจจุบัน นโยบายและกลยุทธ์ของ สง. และจัดให้มีการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับธุรกรรมงานที่สำคัญอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยงในการเกิดการชะงักของการดำเนินการที่มีนัยสำคัญในการดำเนินธุรกิจเกิดขึ้น เพื่อให้มั่นใจว่าแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องมีประสิทธิภาพและสามารถนำไปใช้ปฏิบัติได้จริง การทดสอบและการทบทวนแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องควรครอบคลุมหัวข้อตามที่กำหนดไว้ในแนวปฏิบัติ [21] สง. ควรจัดเก็บข้อมูลผลการทดสอบเพื่อใช้ประเมินผลการทดสอบและพัฒนาประสิทธิภาพของแผนฯ และรายงานผลการทดสอบดังกล่าวต่อคณะกรรมการด้วย

[21] แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) ของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551 http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510386.pdf

7. สง. ควรจัดให้มีการประเมินและทบทวนแผนฯ จากหน่วยงานภายนอกที่มีความเชี่ยวชาญหรือหน่วยงานภายในที่มีความรู้ความสามารถ และมีความเป็นอิสระ และรายงานผลการประเมินและทบทวนแผนฯ ต่อคณะกรรมการ นอกจากนี้ สง. ควรปรับปรุงแผนฯ อย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่ส่งผลกระทบต่อแผนฯ

8. สง. ควรมีการวางแผนการติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอก เพื่อสามารถแจ้งเหตุได้ทันท่วงทีและป้องกันมิให้เกิดความตื่นตระหนกต่อสาธารณชน

9. สง. ควรจัดให้มีการฝึกอบรมแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องแก่พนักงานและมีผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างสม่ำเสมอ นอกจากนี้ สง. ควรจัดให้มีการประชาสัมพันธ์แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง โดยมีการระบุขั้นตอนและวิธีการประชาสัมพันธ์ที่ชัดเจน เพื่อให้พนักงานและผู้มีส่วนเกี่ยวข้องได้รับทราบ

10. หาก สง. มีการหยุดการให้บริการของธุรกรรมงานที่สำคัญ ซึ่งส่งผลกระทบต่อผู้ฝากเงินหรือลูกค้าของ สง. อย่างมีนัยสำคัญ สง. ต้องแจ้งต่อธนาคารแห่งประเทศไทย ในโอกาสแรกที่ทำได้และไม่เกิน 24 ชั่วโมง นับแต่มีการหยุดให้บริการของธุรกรรมงานที่สำคัญนั้น พร้อมรายงานรายละเอียดของเหตุการณ์ที่เกิดขึ้น ทั้งนี้เมื่อธุรกรรมงานที่สำคัญดังกล่าว สามารถกลับมาดำเนินการได้ตามปกติแล้ว ให้ สง. แจ้งธนาคารแห่งประเทศไทยรับทราบด้วย

ภาคผนวก

ประกาศ / หนังสือเวียน / แนวปฏิบัติที่เกี่ยวข้อง

A. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการ ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510385.pdf

B. ประกาศธนาคารแห่งประเทศไทยที่ สนส. 66/2551 เรื่อง หลักเกณฑ์การกำกับแบบรวมกลุ่ม ลงวันที่ 3 สิงหาคม 2551 หน้า 51 ข้อ 104
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510356.pdf

C. ประกาศธนาคารแห่งประเทศไทยที่ สนส.95/2551 เรื่อง หลักเกณฑ์การดำรงเงินกองทุนขั้นต่ำสำหรับความเสี่ยงด้านปฏิบัติการ ลงวันที่ 27 พฤศจิกายน 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510555.pdf

D. ประกาศธนาคารแห่งประเทศไทยที่ สนส. 60/2551 เรื่อง ธรรมาภิบาลของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510350.pdf

E. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง แนวปฏิบัติงานตรวจสอบภายในของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510388.pdf

F. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การกำกับการปฏิบัติตามกฎเกณฑ์ของสถาบันการเงิน (Compliance) ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510389.pdf

G. ประกาศธนาคารแห่งประเทศไทยที่ สนส. 62/2551 เรื่อง หลักเกณฑ์การให้ความเห็นชอบผู้สอบบัญชีของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510352.pdf

H. ประกาศธนาคารแห่งประเทศไทยที่ สนส. 96/2551 เรื่อง การเปิดเผยข้อมูลเกี่ยวกับการดำรงเงินกองทุนสำหรับธนาคารพาณิชย์
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510557.pdf

I. ประกาศธนาคารแห่งประเทศไทยที่ สนส. 43/2551 เรื่อง หลักเกณฑ์เกี่ยวกับการใช้บริการจากบุคคลภายนอก (Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510333.pdf

J. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อ มาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย (Anti-Money Laundering and Combating the Financing of Terrorism : AML/CFT) ของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510390.pdf

K. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) ของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551
http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510386.pdf

L. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การจัดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับกรณีการระบาดของโรคติดต่อร้ายแรง ลงวันที่ 3 สิงหาคม 2551

http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510387.pdf

M. ประกาศธนาคารแห่งประเทศไทยที่ สนส. 79/2551 เรื่อง มาตรฐานขั้นต่ำในการดูแลลูกค้าสำหรับการทำธุรกรรมอนุพันธ์ ลงวันที่ 3 สิงหาคม 2551

http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510369.pdf

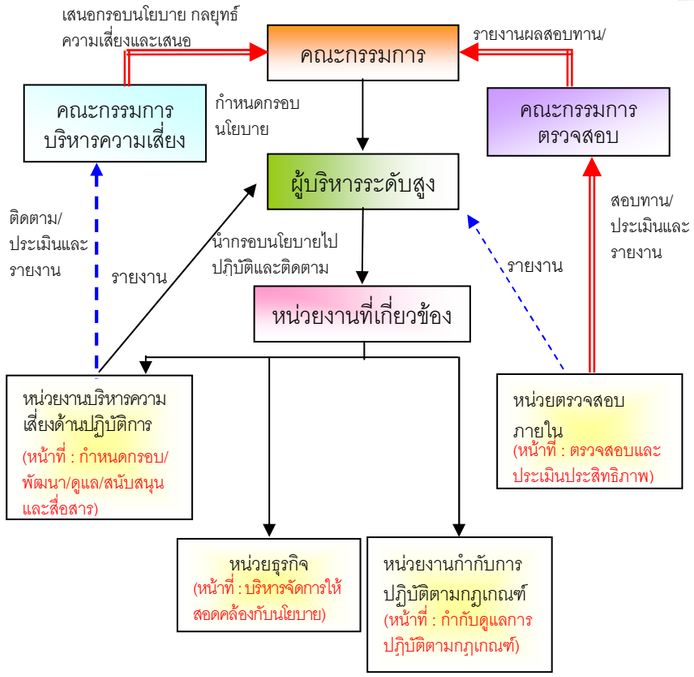
N. ประกาศธนาคารแห่งประเทศไทยที่ สนส. 29/2551 เรื่อง การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ลงวันที่ 3 สิงหาคม 2551

http://www2.bot.or.th/fipcs/Documents/FPG/2551/ThaiPDF/25510319.pdf

ความเสี่ยงด้านปฏิบัติการ

ความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดีหรือขาดธรรมาภิบาลในองค์กร และการขาดการควบคุมที่ดี ที่เกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน คน ระบบงาน หรือ เหตุการณ์ภายนอก และส่งผลกระทบต่อรายได้และเงินกองทุนของสถาบันการเงิน

สภาพแวดล้อมของการบริหารความเสี่ยงด้านปฏิบัติการ



เหตุการณ์ความเสียหายที่เกิดจากความเสี่ยงด้านปฏิบัติการจำแนกได้ 7 ประเภท

1. ความเสี่ยงจากการทุจริตภายใน เช่น การทุจริตของพนักงาน การทำธุรกรรมโดยไม่ได้อนุญาต
2. ความเสี่ยงจากการทุจริตภายนอก เช่น การปลอมเช็ค การโจรกรรม
3. ความเสี่ยงจากการจ้างงานและความปลอดภัยในสถานที่ปฏิบัติงาน เช่น การถูกฟ้องร้องจากการกระทำผิดกฎหมายแรงงาน หรือกฎหมายเกี่ยวกับความปลอดภัยของสถานที่ทำงาน
4. ความเสี่ยงจากการปฏิบัติงานที่ไม่เหมาะสมเกี่ยวกับลูกค้า ผลิตภัณฑ์และวิธีปฏิบัติในการดำเนินธุรกิจ เช่น การที่ลูกค้าใช้ธนาคารพาณิชย์เป็นช่องทางของการฟอกเงิน
5. ความเสี่ยงด้านความปลอดภัยของทรัพย์สิน เช่น ความเสียหายของทรัพย์สินจากภัยธรรมชาติและการก่อการร้าย
6. ความเสี่ยงจากการขัดข้องหรือหยุดชะงักของระบบงานหรือระบบคอมพิวเตอร์ เช่น ความเสียหายจากความล้มเหลวของอุปกรณ์ โปรแกรม หรือระบบเทคโนโลยีสารสเทศ
7. ความเสี่ยงจากกระบวนการทำงาน เช่น ความผิดพลาดของพนักงาน เอกสารสำคัญสูญหาย ความเสียหายที่เกิดจากการใช้บริการจากบุคคลภายนอกของ ธพ.

การบริหารความเสี่ยง

คณะกรรมการตรวจสอบ
- จัดให้มีการรายงานทางการเงินอย่างถูกต้องและเพียงพอ โดยพิจารณาถึงการเปิดเผยข้อมูลที่สำคัญและเป็นประโยชน์
- จัดให้มีระบบควบคุมภายในและการตรวจสอบที่เหมาะสม
- มีการรายงานต่อคณะกรรมการของ สง. เพื่อสามารถปรับปรุงแก้ไขภายในเวลาที่เหมาะสมและรวดเร็ว

หน่วยงานตรวจสอบภายใน
- ประเมินความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน โดยอาจให้บริการในรูปแบบคำปรึกษา
- ประเมินการปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎหมายและข้อบังคับ รวมถึงการบริหารและระบบเทคโนโลยีสารสนเทศ
- ตรวจสอบการทุจริต ข้อผิดพลาด การละเลย และรายการผิดปกติ

คณะกรรมการบริหารความ
- กำหนดกรอบนโยบายและแนวทางการปฏิบัติความเสี่ยงให้สอดคล้องกับกลยุทธ์ของ สง. โดยสามารถ ระบุ วัด ติดตาม รายงาน และควบคุมความเสี่ยงให้อยู่ในระดับที่เหมาะสม
- ทบทวนความเพียงพอของนโยบายและระบบการบริหารความเสี่ยง รวมถึงความมีประสิทธิผลของระบบการปฏิบัติงานและการปฏิบัติตามนโยบายที่กำหนด รวมทั้งดูแลทรัพยากรที่ใช้ในการบริหารความเสี่ยงให้เพียงพอและมีการรายงานต่อคณะกรรมการ

หน่วยงานบริหารความ
- เสนอนโยบาย แผนงานและกระบวนการบริหารความเสี่ยงต่อคณะกรรมการ รวมทั้งดูแลและสนับสนุนให้แต่ละหน่วยงานดำเนินการตามแนวทางที่กำหนดไว้
- ดูแลและสนับสนุนให้มีระบบการจัดเก็บข้อมูลและรายงานความเสี่ยงด้านปฏิบัติการ รวมทั้งศึกษาและพัฒนาแนวทางตลอดจนการสื่อสารให้พนักงานเข้าใจและตระหนักถึงความ สำคัญและหน้าที่ความรับผิดชอบเกี่ยวกับความเสี่ยงด้านปฏิบัติการ

หน่วยธุรกิจ
- ปฏิบัติงานให้สอดคล้องกับนโยบายที่กำหนด รวมทั้งการจัดเก็บและรายงานข้อมูลความเสียหายที่เกิดขึ้น (Loss data) หรือระบบงานที่อยู่ในความรับผิดชอบของหน่วยงาน
- ประเมินโอกาสหรือความถี่และระดับความเสียหายของเหตุการณ์ที่อาจเกิดขึ้น

Compliance Unit
- ให้คำแนะนำ คำปรึกษาเกี่ยวกับกฎหมาย กฎเกณฑ์ต่างๆ
- ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อร่วมกันพัฒนาระบบบริหารความเสี่ยงให้ครอบคลุมการดำเนินการในเรื่องการระบุ การสอบทานและการรายงาน

ทรัพยากรบุคคล
- คัดเลือกบุคลากร และจัดฝึกอบรม รวมทั้งกำหนดระเบียบวิธีการปฏิบัติงาน

ระบุ

เป็นพื้นฐานสำคัญขั้นต้นของการบริหารความเสี่ยง โดยพิจารณาจากปัจจัยดังนี้
- ประสิทธิภาพของระบบการควบคุมภายใน วัฒนธรรมองค์กร ความพร้อมของบุคลากรและทรัพยากรที่ใช้ในการปฏิบัติงาน
- ปริมาณความซับซ้อนและประเภทของธุรกรรม ซึ่งรวมถึงระบบและกลไกที่กระจายผลิตภัณฑ์และให้บริการลูกค้าของ สง.
- เหตุการณ์ความเสียหายที่เกิดขึ้นในอดีต หรือเหตุการณ์ที่จะเกิดขึ้นแต่ สง. สามารถป้องกันความเสียหายได้
- การเปลี่ยนแปลงของเทคโนโลยี การออกผลิตภัณฑ์ใหม่ การเปลี่ยนแปลงทางกฎหมาย สังคม การเมือง และเศรษฐกิจ

ประเมิน

ในการประเมินความเสี่ยงต้องอาศัยดุลพินิจและประสบการณ์ของหน่วยงานเป็นสำคัญ โดย
- ศึกษาและติดตามพัฒนาการของวิธีการและเทคนิคที่ใช้ในการวัดความเสี่ยงอย่างใกล้ชิด เพื่อนำมาปรับใช้ให้เหมาะสมและสะท้อนความเสี่ยงด้านปฏิบัติการขององค์กรอย่างแท้จริง
- ประเมินโอกาสหรือความถี่และระดับความเสียหายของเหตุการณ์ที่อาจเกิดขึ้นประกอบกันในรูปแบบใดรูปแบบหนึ่ง เช่น ตัวเลข สัญลักษณ์ สี หรือคำบรรยายระดับสูงต่ำ โดยกำหนดคำอธิบายที่ชัดเจน

ติดตาม

การติดตามที่มีประสิทธิภาพจะช่วยให้ สง. สามารถป้องกันและควบคุมความเสียหายได้ทันท่วงที โดย
- กำหนดดัชนีชี้วัดความเสี่ยงที่สะท้อนถึงสาเหตุและโอกาสที่จะเกิดความเสียหายจากความเสี่ยงด้านปฏิบัติการเพื่อใช้ในการติดตามดูแลความเสี่ยงที่อาจเกิดขึ้น ซึ่งควรมีลักษณะเป็นการมองไปในอนาคต สามารถสะท้อนแนวโน้มของความเสี่ยงได้
- มีการรายงานการเปลี่ยนแปลงของดัชนีชี้วัดความเสี่ยงอย่างครบถ้วนและเป็นระบบ
- มีการสื่อสารให้ทุกหน่วยงานทราบอย่างชัดเจน เพื่อเพิ่มความโปร่งใสให้กับการบริหารความเสี่ยงด้านปฏิบัติการขององค์กร

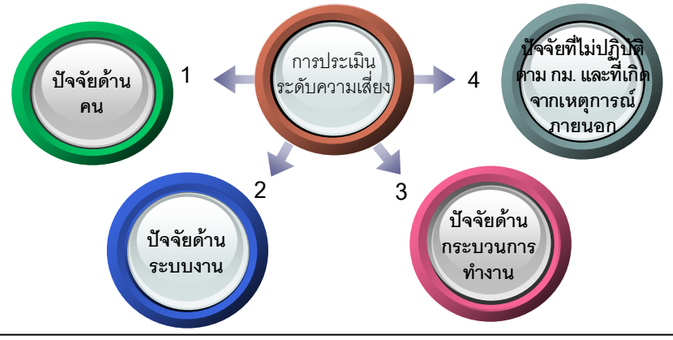
ควบคุม

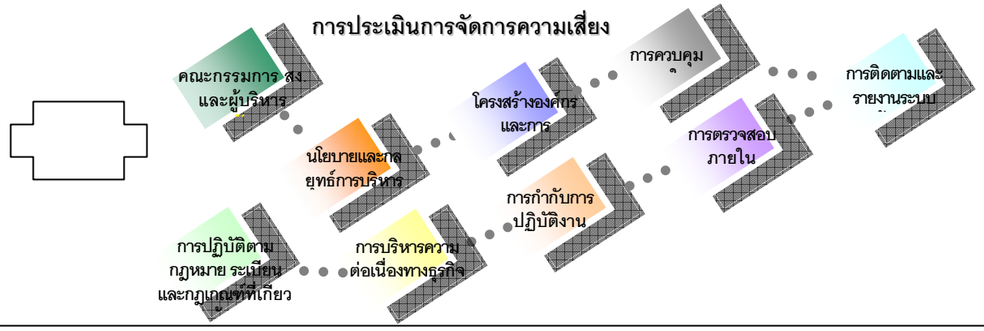
ระบบการควบคุมภายในที่มีประสิทธิภาพเป็นกลไกในการควบคุมและป้องกันความเสียหายที่อาจเกิดขึ้นได้ โดย
- จัดให้มีนโยบายและกระบวนการเพื่อลดความเสี่ยงอย่างชัดเจน พร้อมแนวทางในการดำเนินการที่เหมาะสม
- นำระบบเทคโนโลยีสารสนเทศหรือระบบปฏิบัติงานอัตโนมัติมาใช้ในการดำเนินธุรกิจแทนการปฏิบัติงานของพนักงาน เพื่อเพิ่มประสิทธิภาพในการดำเนินงานและลดความเสี่ยงที่เกิดจากความผิดพลาดของพนักงาน
- กำหนดแผนฉุกเฉินรองรับโดยเฉพาะกับหน่วยงานสำคัญที่อาจจะได้รับผลกระทบ
- การจัดเก็บข้อมูลและรายงานความเสี่ยงด้านปฏิบัติการที่เกิดขึ้น (Loss data) อย่างเป็นระบบ

การลดความเสี่ยง

- บุคลากรและการฝึกอบรม
- กระบวนการปฏิบัติงานและระบบงาน
- การบริหารความต่อเนื่องทางธุรกิจ

การตรวจสอบความเสี่ยงด้านปฏิบัติการ





การประเมินแนวโน้มความเสี่ยง
- ปัจจัยภายใน