



เรียน ผู้จัดการ

สถาบันการเงินเฉพาะกิจทุกแห่ง

ที่ ธปท.ผนส2.ว.๑๙๘/2564 เรื่อง นำส่งประกาศและแนวปฏิบัติธนาคารแห่งประเทศไทย
จำนวน 5 ฉบับ

ธนาคารแห่งประเทศไทย (ธปท.) โดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลัง ได้ออกหลักเกณฑ์การกำกับดูแลสำหรับสถาบันการเงินเฉพาะกิจ (SFIs) เพื่อยกระดับการดำเนินการของ SFIs ให้มีประสิทธิภาพ มั่นคงปลอดภัย และสามารถดำเนินการตามพันธกิจได้อย่างยั่งยืนอย่างต่อเนื่อง โดยครั้งนี้ ธปท. เห็นควรออกหลักเกณฑ์กำกับดูแล SFIs จำนวน 5 ฉบับ ซึ่งจะมีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2565 เป็นต้นไป สรุปสาระสำคัญดังนี้

1. ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 12/2564 เรื่อง หลักเกณฑ์การให้บริการผ่านช่องทางโทรศัพท์และช่องทางดิจิทัลของสถาบันการเงินเฉพาะกิจ

ปัจจุบันการให้บริการผ่านช่องทางโทรศัพท์และช่องทางดิจิทัลของ SFIs มีการพัฒนาและขยายการให้บริการอย่างต่อเนื่อง ธปท. จึงออกหลักเกณฑ์เพื่อส่งเสริมให้ SFIs ให้บริการดังกล่าวภายใต้ขอบเขตตามกฎหมายจัดตั้งและที่กระทรวงการคลังกำหนดได้อย่างเหมาะสม โดยมีกระบวนการบริหารความเสี่ยงที่มีประสิทธิภาพ มีแนวทางดูแลและคุ้มครองผู้ใช้บริการอย่างเป็นธรรม และมีความพร้อมด้านระบบเทคโนโลยีสารสนเทศ โดย SFIs ต้องขออนุญาตจาก ธปท. หากจะนำเทคโนโลยีใหม่ ๆ มาใช้ในครั้งแรกหรือการเปลี่ยนแปลงเทคโนโลยีอย่างมีนัยสำคัญ

2. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินเฉพาะกิจ

ธปท. มุ่งหวังให้ SFIs ให้ความสำคัญกับการบริหารความเสี่ยงด้านปฏิบัติการ มีการสร้างและพัฒนากรอบการกำกับดูแลด้านความเสี่ยงด้านปฏิบัติการ เพื่อส่งเสริมให้ SFIs เป็นองค์กรที่มีสภาพแวดล้อมในการบริหารความเสี่ยงด้านปฏิบัติการ มีระบบการบริหารความเสี่ยงด้านปฏิบัติการที่มีประสิทธิภาพ และมีการเปิดเผยข้อมูลต่อสาธารณชนอย่างเพียงพอ ทั้งนี้ เพื่อช่วยให้ SFIs สามารถป้องกันและลดความเสียหายที่อาจเกิดขึ้นได้ และช่วยเพิ่มประสิทธิภาพในการดำเนินงาน รวมถึงสร้างความเชื่อมั่นให้กับผู้ใช้บริการหรือประชาชน

3. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของสถาบันการเงินเฉพาะกิจ

ธปท. กำหนดแนวทางในการบริหารความต่อเนื่องทางธุรกิจซึ่งครอบคลุมเรื่องการจัดทำนโยบาย BCM และกระบวนการในการดำเนินการเพื่อรองรับเหตุการณ์หยุดชะงักทางธุรกิจ ตั้งแต่การระบุและประเมินความเสี่ยง การจัดทำแผน BCP การดำเนินการตามแผน ตลอดจนการติดตามและประเมินผล

สนสว40-คส000 ๐1-256412 ๐๗

คส000	วันที่ ๗ ธ.ค. 2564
-------	--------------------

เพื่อสร้างความมั่นใจให้กับผู้ให้บริการว่า หากมีเหตุการณ์ที่ทำให้การปฏิบัติงานตามปกติต้องหยุดชะงักเกิดขึ้น ธุรกรรมงานที่สำคัญ (Critical Business Functions) ของ SFIs จะสามารถให้บริการได้อย่างต่อเนื่องหรือกลับมาดำเนินการตามปกติภายในเวลาที่เหมาะสม และลดผลกระทบหรือความสูญเสียทางธุรกิจที่อาจเกิดขึ้น

4. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) ของสถาบันการเงินเฉพาะกิจ

ธปท. กำหนดแนวทางในการบริหารความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ โดยครอบคลุมเรื่องโครงสร้างและสายการบังคับบัญชา การจัดตั้งฝ่ายงานกำกับการปฏิบัติตามกฎเกณฑ์ บทบาท หน้าที่ และความรับผิดชอบของผู้เกี่ยวข้องทุกระดับให้มีความชัดเจนและสอดคล้องกับหลักการ แบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (3 Lines of Defense) ตลอดจนส่งเสริมให้ SFIs มีเครื่องมือและระบบงานที่เพียงพอและเหมาะสม เพื่อลดความเสี่ยงที่จะปฏิบัติฝ่าฝืนกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง ซึ่งอาจส่งผลกระทบต่อชื่อเสียงหรือฐานะทางการเงินของ SFIs ได้

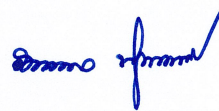
5. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การปฏิบัติงานตรวจสอบภายใน (Internal Audit) ของสถาบันการเงินเฉพาะกิจ

ธปท. ออกแนวปฏิบัติฉบับนี้ เพื่อให้ SFIs ถือปฏิบัติเพิ่มเติมจากระเบียบกระทรวงการคลัง ว่าด้วยคณะกรรมการตรวจสอบและหน่วยตรวจสอบภายในของรัฐบาลกิจ โดยเพิ่มความชัดเจนเรื่องบทบาท หน้าที่ และความรับผิดชอบของสายงานตรวจสอบภายใน เพื่อสนับสนุนให้หน่วยงานตรวจสอบภายใน ปฏิบัติงานได้อย่างเป็นอิสระ โปร่งใส และมีประสิทธิภาพ

ธปท. จึงขอส่งประกาศธนาคารแห่งประเทศไทย ที่ สนส. 12/2564 เรื่อง หลักเกณฑ์ การให้บริการผ่านช่องทางโทรศัพท์และช่องทางดิจิทัลของสถาบันการเงินเฉพาะกิจ ลงวันที่ 4 ตุลาคม 2564 ซึ่งได้ลงประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 138 ตอนพิเศษ 287 ง ลงวันที่ 22 พฤศจิกายน 2564 และแนวปฏิบัติธนาคารแห่งประเทศไทย จำนวน 4 ฉบับ มาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ



(นายรณดล นุ่มนนท์)

รองผู้ว่าการ ด้านเสถียรภาพสถาบันการเงิน

ผู้ว่าการ แทน

- สิ่งที่ส่งมาด้วย
1. ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 12/2564 เรื่อง หลักเกณฑ์การให้บริการผ่านช่องทางโทรศัพท์และช่องทางดิจิทัลของสถาบันการเงินเฉพาะกิจ ลงวันที่ 4 ตุลาคม 2564
 2. แนวปฏิบัติธนาคารแห่งประเทศไทย จำนวน 4 ฉบับ

ฝ่ายนโยบายและกำกับสถาบันการเงิน 1, ฝ่ายนโยบายและกำกับสถาบันการเงิน 2

โทรศัพท์ 0 2283 6876 (ประกาศฯ)

0 2283 5806 (แนวปฏิบัติ Operational Risk และแนวปฏิบัติ BCM และ BCP)

0 2283 6045 (แนวปฏิบัติ Compliance และแนวปฏิบัติ Internal Audit)

อีเมล BPC-RPD1@bot.or.th (ประกาศฯ), CGOP-RPD2@bot.or.th (แนวปฏิบัติฯ)

แนวปฏิบัติธนาคารแห่งประเทศไทย
เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินเฉพาะกิจ

7 ธันวาคม 2564



ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายนโยบายและกำกับสถาบันการเงิน 2

ธนาคารแห่งประเทศไทย

โทรศัพท์ 0 2283 5806

e-mail: RPD2@bot.or.th

สนสว40-คส00001-25641207

คส000	วันที่ 7 ธ.ค. 2564
-------	--------------------

แนวปฏิบัติธนาคารแห่งประเทศไทย
เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินเฉพาะกิจ

1. เหตุผลในการออกแนวปฏิบัติ

ความเสี่ยงด้านปฏิบัติการเป็นความเสี่ยงพื้นฐานที่สำคัญของสถาบันการเงินเฉพาะกิจ ซึ่งความเสี่ยงด้านปฏิบัติการอาจเกิดขึ้นจากการดำเนินการตามปกติของสถาบันการเงินเฉพาะกิจเอง เช่น กระบวนการปฏิบัติงานภายใน ความบกพร่องของบุคลากร ระบบงาน หรือจากปัจจัยภายนอก เช่น สภาพเศรษฐกิจ การแข่งขันในตลาด กฎหมายต่าง ๆ ที่เกี่ยวข้อง นอกจากนี้ ปัจจุบันสถาบันการเงินเฉพาะกิจได้ปรับปรุงแบบการดำเนินธุรกิจเพื่อให้สามารถตอบสนองต่อการให้บริการลูกค้าได้ตรงความต้องการมากขึ้น เช่น การนำเทคโนโลยีมาใช้นับสนับสนุนการให้บริการ การขยายช่องทางการให้บริการทางการเงินผ่านช่องทางดิจิทัล และการใช้บริการจากผู้ให้บริการสนับสนุนการประกอบธุรกิจ โดยรูปแบบการดำเนินธุรกิจที่เปลี่ยนไป ส่งผลให้โครงสร้างความเสี่ยงโดยรวม (Risk Profile) ของสถาบันการเงินเฉพาะกิจมีความซับซ้อนยิ่งขึ้น และความเสี่ยงด้านปฏิบัติการซึ่งเป็นความเสี่ยงที่สำคัญมีแนวโน้มเพิ่มสูงขึ้นด้วย

แม้ว่าที่ผ่านมามาตราการแห่งประเทศไทย ได้ออกหลักเกณฑ์การคำนวณมูลค่าเทียบเท่าสินทรัพย์เสี่ยงด้านปฏิบัติการของสถาบันการเงินเฉพาะกิจ เพื่อให้สถาบันการเงินเฉพาะกิจดำรงเงินกองทุนรองรับความเสี่ยงด้านปฏิบัติการแล้ว อย่างไรก็ตาม การมีระบบการบริหารความเสี่ยงด้านปฏิบัติการที่มีประสิทธิภาพ จะช่วยให้สถาบันการเงินเฉพาะกิจสามารถป้องกันและลดความเสียหายที่อาจเกิดขึ้นได้ และจะช่วยเพิ่มประสิทธิภาพในการดำเนินงาน รวมถึงสร้างความเชื่อมั่นให้กับผู้ให้บริการหรือประชาชนอีกด้วย

ธนาคารแห่งประเทศไทยออกแนวปฏิบัติฉบับนี้ โดยมุ่งหวังให้สถาบันการเงินเฉพาะกิจให้ความสำคัญกับการบริหารความเสี่ยงด้านปฏิบัติการ มีการสร้างและพัฒนากรอบการกำกับดูแลความเสี่ยงด้านปฏิบัติการ ซึ่งเน้นเรื่องที่สำคัญ ได้แก่ (1) บทบาทของคณะกรรมการและผู้บริหารระดับสูงที่เป็นส่วนสำคัญในการสร้างให้สถาบันการเงินเฉพาะกิจเป็นองค์กรที่มีสภาพแวดล้อมในการบริหารความเสี่ยงด้านปฏิบัติการ (Operational Risk Management Environment) ที่เหมาะสม (2) การมีระบบการบริหารความเสี่ยงที่มีประสิทธิภาพ และ (3) การเปิดเผยข้อมูลต่อสาธารณชนอย่างเพียงพอเพื่อเป็นแนวทางให้สถาบันการเงินเฉพาะกิจถือปฏิบัติ

2. ขอบเขตการบังคับใช้

แนวปฏิบัติฉบับนี้ใช้บังคับกับธนาคารออมสิน ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารอาคารสงเคราะห์ ธนาคารอิสลามแห่งประเทศไทย ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย และบริษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม

3. เนื้อหา

3.1 คำจำกัดความ

ในแนวปฏิบัติฉบับนี้

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้น ได้แก่ ธนาคารออมสิน ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารอาคารสงเคราะห์ ธนาคารอิสลามแห่งประเทศไทย ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย และบริษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม

“ความเสี่ยงด้านปฏิบัติการ (Operational Risk)” หมายความว่า ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก รวมถึงความเสี่ยงด้านกฎหมาย เช่น ความเสี่ยงต่อการถูกฟ้องร้อง ถูกดำเนินคดีตามกฎหมาย หรือถูกทางการเปรียบเทียบปรับ ทั้งนี้ ไม่รวมถึงความเสี่ยงด้านกลยุทธ์ (Strategic Risk) และความเสี่ยงด้านชื่อเสียง (Reputational Risk)

3.2 หลักการ

การบริหารความเสี่ยงด้านปฏิบัติการที่มีประสิทธิภาพ จะช่วยป้องกันและลดความเสียหายที่อาจเกิดขึ้นกับสถาบันการเงินเฉพาะกิจได้ โดยสถาบันการเงินเฉพาะกิจควรให้ความสำคัญกับการสร้างและพัฒนากรอบการกำกับดูแลความเสี่ยงด้านปฏิบัติการ โดยส่งเสริมให้สถาบันการเงินเฉพาะกิจเป็นองค์กรที่มีสภาพแวดล้อมในการบริหารความเสี่ยงด้านปฏิบัติการ (Operational Risk Management Environment) ที่เหมาะสม ซึ่งกรอบการกำกับดูแลความเสี่ยงด้านปฏิบัติการ ประกอบด้วย 3 ส่วน ได้แก่

(1) การสร้างและพัฒนาสภาพแวดล้อมในการบริหารความเสี่ยงด้านปฏิบัติการที่เหมาะสม ซึ่งคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินเฉพาะกิจมีส่วนสำคัญในการสร้างและขับเคลื่อนองค์กรให้มีสภาพแวดล้อมดังกล่าว

(2) ระบบการบริหารความเสี่ยงด้านปฏิบัติการที่มีประสิทธิภาพ โดยให้สถาบันการเงินเฉพาะกิจกำหนดและพัฒนาระบบการบริหารความเสี่ยงด้านปฏิบัติการให้สอดคล้องกับวัฒนธรรมองค์กร ลักษณะธุรกิจ ความซับซ้อน และความเสี่ยงของสถาบันการเงินเฉพาะกิจ

(3) การเปิดเผยข้อมูลต่อสาธารณชนอย่างเพียงพอ เพื่อให้ผู้ที่มีส่วนเกี่ยวข้องเข้าใจแนวทางการบริหารความเสี่ยงด้านปฏิบัติการ และใช้ข้อมูลดังกล่าวในการประเมินความมีประสิทธิภาพของระบบการบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินเฉพาะกิจได้

3.3 หลักเกณฑ์

3.3.1 การสร้างและพัฒนาสภาพแวดล้อมในการบริหารความเสี่ยงด้านปฏิบัติการ (Operational Risk Management Environment)

คณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินเฉพาะกิจมีหน้าที่กำหนดทิศทางและนโยบาย สภาพแวดล้อมและวัฒนธรรมองค์กรของสถาบันการเงินเฉพาะกิจ ธนาคารแห่งประเทศไทยจึงได้ออกประกาศธนาคารแห่งประเทศไทยว่าด้วยธรรมาภิบาลของสถาบันการเงินเฉพาะกิจเพื่อกำหนดบทบาทหน้าที่ของคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินเฉพาะกิจเกี่ยวกับการตระหนักถึงการบริหารความเสี่ยงในด้านปฏิบัติการไว้ด้วย นอกจากนี้ เพื่อส่งเสริมการสร้างและพัฒนาสภาพแวดล้อมขององค์กรให้เอื้อต่อการบริหารความเสี่ยงด้านปฏิบัติการ ธนาคารแห่งประเทศไทยได้กำหนดบทบาทหน้าที่ของคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินเฉพาะกิจเพิ่มเติม ดังนี้

(1) การกำหนดนโยบายและกลยุทธ์การบริหารความเสี่ยงด้านปฏิบัติการ

(1.1) คณะกรรมการของสถาบันการเงินเฉพาะกิจมีบทบาทหน้าที่ ดังต่อไปนี้

(1.1.1) กำหนดหรืออนุมัติกรอบนโยบายและกลยุทธ์ในการบริหารความเสี่ยงด้านปฏิบัติการที่เหมาะสมกับองค์กร

(1.1.2) กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ให้สอดคล้องกับลักษณะความเสี่ยง (Risk Profile) และลักษณะการดำเนินธุรกิจของสถาบันการเงินเฉพาะกิจ

(1.2) ผู้บริหารระดับสูงมีบทบาทหน้าที่ ดังต่อไปนี้

(1.2.1) กำหนดหรืออนุมัติ ระเบียบ กฎเกณฑ์ แนวปฏิบัติ รวมถึงแผนงานและกระบวนการบริหารความเสี่ยงด้านปฏิบัติการ ให้สอดคล้องกับกรอบนโยบายและกลยุทธ์ที่ได้รับการอนุมัติจากคณะกรรมการของสถาบันการเงินเฉพาะกิจ

(1.2.2) กำหนดเพดานความเสี่ยง (Risk Limit) ในระดับที่เหมาะสม และสอดคล้องกับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

(1.2.3) สื่อสารกับพนักงานทุกคนในองค์กรให้เข้าใจและให้ความสำคัญกับการบริหารความเสี่ยงด้านปฏิบัติการ รวมทั้งตระหนักถึงหน้าที่ความรับผิดชอบเกี่ยวกับการบริหารความเสี่ยงดังกล่าว

(1.2.4) ควบคุมดูแลให้พนักงานทุกคนในองค์กรมีการปฏิบัติตามนโยบาย ระเบียบ กฎเกณฑ์ที่กำหนดอย่างเคร่งครัด

(2) การกำหนดหน้าที่ความรับผิดชอบในการควบคุม กำกับ และตรวจสอบ (Three lines of defense)

(2.1) คณะกรรมการของสถาบันการเงินเฉพาะกิจมีบทบาทหน้าที่ในการดูแลให้มีกลไกในการควบคุม กำกับ และตรวจสอบที่มีประสิทธิภาพและเป็นอิสระ ผ่านการกำหนดโครงสร้างองค์กรที่หน่วยงานบริหารความเสี่ยงด้านปฏิบัติการ แยกจากหน่วยงานอื่นที่ก่อให้เกิดความเสี่ยง และหน่วยงานตรวจสอบภายในอย่างชัดเจน

(2.2) ผู้บริหารระดับสูงมีบทบาทหน้าที่ดังต่อไปนี้

(2.2.1) กำหนดหน้าที่ความรับผิดชอบและสายการบังคับบัญชาในแต่ละหน่วยงานอย่างชัดเจน เพื่อส่งเสริมให้มีกลไกการตรวจสอบและถ่วงดุลที่เหมาะสม โดยหัวหน้าหน่วยงานควรเป็นผู้รับผิดชอบต่อความเสี่ยงด้านปฏิบัติการในหน่วยงานนั้น เนื่องจากเป็นผู้รู้และเข้าใจความเสี่ยงที่มีอยู่ในหน่วยงานดีที่สุด

(2.2.2) ดูแลสนับสนุนให้แต่ละหน่วยงานสามารถทำหน้าที่ได้อย่างมีประสิทธิภาพ เช่น ดูแลความพร้อมและความเพียงพอของบุคลากร และระบบงานต่าง ๆ

ทั้งนี้ หน่วยงานการบริหารความเสี่ยงด้านปฏิบัติการควรมีสายการบังคับบัญชาที่ขึ้นตรงต่อคณะกรรมการกำกับความเสี่ยงของสถาบันการเงินเฉพาะกิจ และมีหน้าที่ดังต่อไปนี้

1) เสนอนโยบาย แผนงาน และกระบวนการบริหารความเสี่ยงด้านปฏิบัติการต่อคณะกรรมการของสถาบันการเงินเฉพาะกิจเพื่อพิจารณาอนุมัติ

2) ดูแลและสนับสนุนให้แต่ละหน่วยงานดำเนินการบริหารความเสี่ยงด้านปฏิบัติการตามแนวทางที่กำหนดไว้

3) ดูแลและสนับสนุนให้มีระบบการจัดเก็บข้อมูลความเสี่ยงด้านปฏิบัติการ รวมถึงจัดให้มีรายงานข้อมูลความเสี่ยงด้านปฏิบัติการด้วย

4) ดูแลและสนับสนุนให้หน่วยงานต่าง ๆ จัดทำ ทบทวน ปรับปรุงคู่มือการปฏิบัติงานและแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องให้เหมาะสมและเป็นปัจจุบัน

5) ศึกษาและพัฒนาแนวทางการบริหารความเสี่ยงด้านปฏิบัติการ สื่อสารให้พนักงานเข้าใจและตระหนักถึงความสำคัญและหน้าที่ความรับผิดชอบเกี่ยวกับความเสี่ยงด้านปฏิบัติการเพื่อสร้างสภาพแวดล้อมในการบริหารความเสี่ยงด้านปฏิบัติการ (Operational Risk Management Environment) ที่เหมาะสม รวมทั้งประสานงานระหว่างหน่วยงานบริหารความเสี่ยงด้านอื่น เพื่อให้มีการปฏิบัติงานที่สอดคล้องกัน

(3) การสร้างวัฒนธรรมองค์กรด้านการบริหารความเสี่ยง (Risk Culture)

คณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินเฉพาะกิจ มีบทบาทหน้าที่ ดังต่อไปนี้

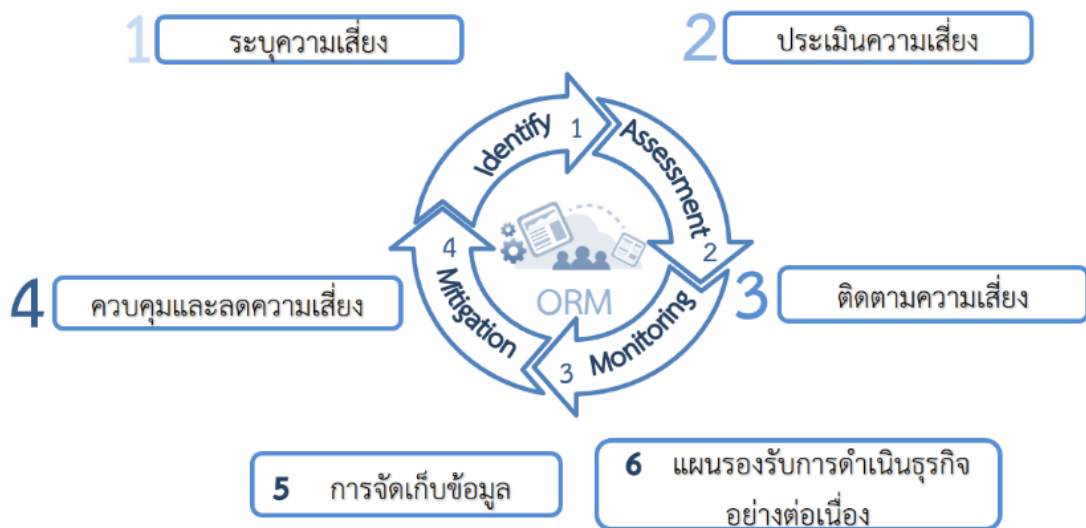
(3.1) ปลุกฝังวัฒนธรรมองค์กรเพื่อให้พนักงานทุกคนในองค์กรให้ความสำคัญกับการบริหารจัดการความเสี่ยงด้านปฏิบัติการ และตระหนักว่าการบริหารความเสี่ยงเป็นส่วนหนึ่งของการปฏิบัติงานตามปกติ

(3.2) ให้ความสำคัญกับการบริหารความเสี่ยงด้านปฏิบัติการในฐานะที่เป็นความเสี่ยงหลักของสถาบันการเงินเฉพาะกิจเช่นเดียวกับการบริหารความเสี่ยงด้านอื่น ๆ เช่น ด้านเครดิต ด้านตลาด ด้านสภาพคล่อง และด้านกลยุทธ์ โดยควรมีการบรรจุเรื่องดังกล่าวเข้าเป็นวาระในการประชุมคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินเฉพาะกิจอย่างสม่ำเสมอ

(3.3) ผู้บริหารระดับสูงควรสนับสนุนการปลุกฝังวัฒนธรรมองค์กรโดยดูแลให้มีการจัดอบรมพนักงานทุกคนในองค์กรให้มีความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านปฏิบัติการ

3.3.2 ระบบบริหารความเสี่ยงด้านปฏิบัติการ

สถาบันการเงินเฉพาะกิจควรกำหนดและพัฒนาระบบการบริหารความเสี่ยงด้านปฏิบัติการที่สอดคล้องเหมาะสมกับวัฒนธรรมองค์กร ขนาด ความซับซ้อน และความเสี่ยงของสถาบันการเงินเฉพาะกิจ โดยพิจารณาแผนกลยุทธ์ แผนการตลาดและการขยายตัวทางธุรกิจของสถาบันการเงินเฉพาะกิจควบคู่ไปด้วย เพื่อให้สามารถรองรับการขยายตัวของธุรกิจและการเพิ่มขึ้นของความเสี่ยงในอนาคตได้



ระบบบริหารความเสี่ยงด้านปฏิบัติการ ประกอบด้วย

(1) การระบุความเสี่ยง (Risk Identification)

ทุกหน่วยงานในสถาบันการเงินเฉพาะกิจควรมีส่วนสำคัญในกระบวนการระบุความเสี่ยง โดยสถาบันการเงินเฉพาะกิจควรระบุจุดที่มีความเสี่ยงหรือแหล่งที่มาของความเสี่ยง ตลอดจนหาสาเหตุหรือปัจจัยที่ทำให้เกิดความเสี่ยง ประเมินความเสี่ยง รวมถึงผลกระทบของความเสี่ยง ด้านปฏิบัติการดังกล่าวด้วย ทั้งนี้ ในการระบุความเสี่ยง สถาบันการเงินเฉพาะกิจอาจพิจารณาจากปัจจัยภายใน ปัจจัยภายนอก รวมถึงจากรายงานต่าง ๆ ที่เกี่ยวข้อง เช่น

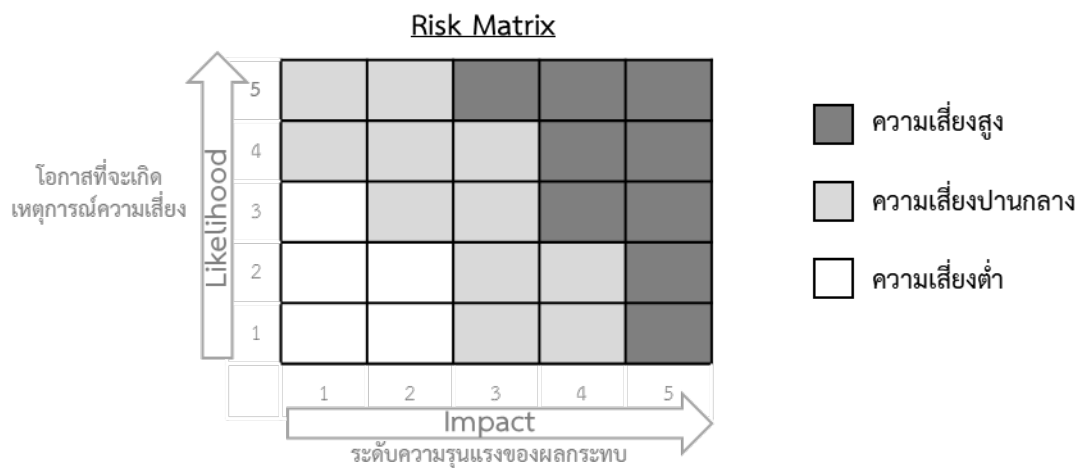
(1.1) ปัจจัยภายใน เช่น ลักษณะการดำเนินธุรกิจ วัฒนธรรมองค์กร ในการบริหารความเสี่ยง ระบบควบคุมภายใน ความพร้อมของบุคลากร ความพอเพียงของทรัพยากรที่ใช้ในการปฏิบัติงาน และระบบงาน

(1.2) ปัจจัยภายนอก เช่น เทคโนโลยีสารสนเทศ สภาพเศรษฐกิจ สังคม การเมือง และกฎหมาย

(1.3) รายงานต่าง ๆ ได้แก่ รายงานข้อมูลความเสียหายที่เกิดขึ้น (Loss Data) และรายงานข้อมูลความเสียหายที่เกิดขึ้นแล้วแต่สถาบันการเงินเฉพาะกิจสามารถป้องกันความเสียหายไว้ได้ (Near-Miss)

(2) การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงมีวัตถุประสงค์เพื่อให้สถาบันการเงินเฉพาะกิจสามารถจัดลำดับความสำคัญของความเสี่ยงต่าง ๆ ที่สถาบันการเงินเฉพาะกิจระบุได้ โดยพิจารณาจากโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง และระดับความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าว ทั้งนี้ สถาบันการเงินเฉพาะกิจจะใช้รูปแบบของสีหรือคำบรรยายระดับสูงต่ำในการจัดทำข้อมูลหรือรายงานเพื่อใช้ในการวิเคราะห์ระดับความสำคัญของความเสี่ยงนั้น ๆ เช่น การทำ Risk Matrix โดยสถาบันการเงินเฉพาะกิจควรกำหนดแนวทางในการประเมินความเสี่ยงด้านปฏิบัติการที่เหมาะสมกับขนาดและความซับซ้อนของสถาบันการเงินเฉพาะกิจ รวมถึงพัฒนาให้มีประสิทธิภาพมากยิ่งขึ้น



ทั้งนี้ สถาบันการเงินเฉพาะกิจควรมีเครื่องมือสำหรับช่วยระบุและประเมินความเสี่ยง เช่น Risk Control Self-Assessment หรือ Risk Mapping และการประเมินความเสี่ยงควรดำเนินการอย่างต่อเนื่อง และทบทวนความเหมาะสมเป็นระยะ รวมถึงประเมินความเสี่ยงด้านปฏิบัติการกรณีมีการออกผลิตภัณฑ์ใหม่ด้วย

(3) การติดตามความเสี่ยง (Risk Monitoring)

(3.1) กระบวนการติดตามความเสี่ยง

สถาบันการเงินเฉพาะกิจควรมีกระบวนการในการติดตามพัฒนาการและแนวโน้มของระดับความเสี่ยงอย่างสม่ำเสมอ เพื่อกำหนดแนวทางในการป้องกันและควบคุมเหตุการณ์ความเสียหายได้อย่างทันทั่วทั้ง โดยในการติดตามดูแลความเสี่ยงที่อาจเกิดขึ้น สถาบันการเงินเฉพาะกิจควรกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) และระดับที่ยอมรับได้ (Tolerance Level) ของดัชนีชี้วัดแต่ละตัว นอกจากนี้ ดัชนีชี้วัดความเสี่ยงที่สถาบันการเงินเฉพาะกิจกำหนดควรมีลักษณะคาดการณ์ไปข้างหน้า (Forward Looking) และสามารถสะท้อนแนวโน้มความเสี่ยงได้ เช่น อัตราการเติบโต

อย่างรวดเร็วของธุรกิจ การออกผลิตภัณฑ์ใหม่ อัตราการลาออกของพนักงาน ระยะเวลาการหยุดชะงักของระบบงาน จำนวนพนักงานในหน่วยงาน จำนวนข้อร้องเรียนจากลูกค้า หรือรายได้จากการดำเนินงานที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(3.2) การรายงานผลการติดตามความเสี่ยง

สถาบันการเงินเฉพาะกิจควรจัดทำรายงานสรุปผลการติดตามความเสี่ยงและการเปลี่ยนแปลงของดัชนีชี้วัดความเสี่ยงอย่างครบถ้วน เพื่อนำเสนอคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินเฉพาะกิจอย่างสม่ำเสมอ รวมถึงต้องสื่อสารให้ทุกหน่วยงานทราบอย่างชัดเจน

นอกจากนี้ สถาบันการเงินเฉพาะกิจควรวิเคราะห์รายงานการติดตามความเสี่ยงเพื่อพัฒนาการบริหารความเสี่ยง รวมถึงนโยบาย กระบวนการทำงาน และแนวปฏิบัติด้วย โดยรายงานดังกล่าวควรประกอบด้วยฐานะการเงิน การดำเนินงาน ข้อมูลปฏิบัติตามกฎเกณฑ์ รวมถึงข้อมูลสถานะภายนอกที่เกี่ยวข้องกับการตัดสินใจ

ทั้งนี้ สถาบันการเงินเฉพาะกิจควรมีมาตรการให้การรายงานเหตุการณ์ความเสียหายหรือดัชนีชี้วัดความเสี่ยงได้มาซึ่งข้อมูลที่ถูกต้องตรงตามความเป็นจริง รวมถึงการสร้าง ความเข้าใจและโน้มน้าวให้หน่วยงานเห็นความสำคัญของการรายงานข้อมูลที่ถูกต้อง พร้อมทั้งให้หน่วยงานตรวจสอบภายในสุ่มตรวจสอบในเรื่องดังกล่าวด้วย

(4) การควบคุมและลดความเสี่ยง (Risk Control and Risk Mitigation)

ระบบการควบคุมภายในที่มีประสิทธิภาพเป็นกลไกสำคัญในการควบคุมและป้องกันความเสียหายที่เกิดขึ้นได้ สถาบันการเงินเฉพาะกิจควรกำหนดนโยบาย กระบวนการ และวิธีปฏิบัติในการควบคุมและลดความเสี่ยงด้านปฏิบัติการที่ชัดเจน และเหมาะสมกับลักษณะธุรกิจและระดับของความเสี่ยงของสถาบันการเงินเฉพาะกิจ เช่น

(4.1) การลดความเสี่ยง (Risk Mitigation) คือ การเพิ่มแนวทางการจัดการความเสี่ยงเพื่อลดโอกาสหรือผลกระทบของความเสี่ยงที่คาดว่าจะเกิดขึ้นให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ เช่น การเพิ่มการควบคุมภายใน การปรับปรุงกระบวนการทำงาน รวมถึงการใช้ระบบเทคโนโลยีสารสนเทศทดแทนการปฏิบัติงานของพนักงาน เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน และลดความเสี่ยงที่อาจเกิดจากความผิดพลาดของพนักงาน

ทั้งนี้ กรณีที่สถาบันการเงินเฉพาะกิจเลือกใช้เทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงด้านปฏิบัติการดังกล่าว ให้สถาบันการเงินเฉพาะกิจปฏิบัติตามประกาศธนาคาร

แห่งประเทศไทย ที่ สนส. 19/2560 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ลงวันที่ 20 ธันวาคม 2560 โดยอนุโลมจนกว่า ธนาคารแห่งประเทศไทยจะออกหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ที่มีผลบังคับใช้กับสถาบันการเงินเฉพาะกิจ

(4.2) การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การโอนย้ายหรือ กระจายความเสี่ยงให้กับบุคคลอื่น เช่น การจัดทำประกัน การใช้บริการจากผู้ให้บริการสนับสนุน การประกอบธุรกิจ การทำสัญญาป้องกันความเสี่ยง

ทั้งนี้ กรณีที่สถาบันการเงินเฉพาะกิจเลือกทำประกันเพื่อถ่ายโอน ความเสี่ยงด้านปฏิบัติการเพื่อลดความเสียหายที่อาจเกิดขึ้น สถาบันการเงินเฉพาะกิจควรคำนึงถึงปัจจัย และเงื่อนไขต่าง ๆ ที่อาจมีผลกระทบต่อการจ่ายค่าสินไหมทดแทน เช่น ฐานะทางการเงินของบริษัท ประกันภัย ระยะเวลาในการเรียกค่าสินไหมทดแทน และเงื่อนไขการจ่ายค่าสินไหมทดแทน รวมถึง ควรพิจารณาค่าความเสียหายสูงสุดที่สถาบันการเงินเฉพาะกิจยอมรับได้ และทบทวนความเสี่ยง ของสถาบันการเงินเฉพาะกิจและการทำประกันเป็นรายปี

นอกจากนี้ กรณีสถาบันการเงินเฉพาะกิจใช้บริการจากผู้ให้บริการ สนับสนุนการประกอบธุรกิจเพื่อถ่ายโอนความเสี่ยงด้านปฏิบัติการ ให้ถือปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการสนับสนุนการประกอบธุรกิจ (Business Facilitator) ของสถาบันการเงินเฉพาะกิจด้วย

(4.3) การยอมรับความเสี่ยง (Risk Acceptance) กรณีที่สถาบันการเงิน เฉพาะกิจพิจารณาว่าความเสี่ยงที่อาจเกิดขึ้นอยู่ในระดับที่ยอมรับได้ สถาบันการเงินเฉพาะกิจควรมี กระบวนการในการติดตามความเสี่ยงดังกล่าวอย่างสม่ำเสมอ

ทั้งนี้ กรณีที่สถาบันการเงินเฉพาะกิจพิจารณาแล้วว่าความเสี่ยง ที่อาจเกิดขึ้นสูงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ สถาบันการเงินเฉพาะกิจอาจตัดสินใจยกเลิก หรือ หลีกเลี่ยงการดำเนินการหรือธุรกรรมที่ก่อให้เกิดความเสี่ยงด้านปฏิบัติการนั้น (Risk Avoidance) เช่น การยกเลิกการให้บริการผลิตภัณฑ์ที่ก่อให้เกิดความเสี่ยงนั้น ๆ หรือปรับเปลี่ยนกระบวนการทำงาน

อย่างไรก็ดี สถาบันการเงินเฉพาะกิจควรตระหนักว่าการใช้ เครื่องมือเพื่อลดหรือถ่ายโอนความเสี่ยงด้านปฏิบัติการ อาจทำให้โครงสร้างความเสี่ยงเปลี่ยนแปลง ไปเป็นความเสี่ยงด้านอื่นแทน เช่น ความเสี่ยงด้านกฎหมาย ความเสี่ยงจากคู่สัญญา หรือความเสี่ยง ด้านเทคโนโลยีสารสนเทศ ดังนั้น สถาบันการเงินเฉพาะกิจจึงควรมีแนวทางรองรับการบริหารความเสี่ยง ที่เปลี่ยนไปด้วย

นอกจากนี้ สถาบันการเงินเฉพาะกิจที่เลือกแนวทางตามข้อ (4.1) – (4.3) ควรควบคุมระดับความเสี่ยงด้านปฏิบัติการดังกล่าวให้อยู่ในระดับที่ยอมรับได้ โดยพิจารณาจากปัจจัยต่าง ๆ เช่น บุคลากร กระบวนการปฏิบัติงานและระบบงาน รวมถึงเหตุการณ์ภายนอกต่าง ๆ โดยเฉพาะกรณีที่มีการออกผลิตภัณฑ์หรือการให้บริการทางการเงินรูปแบบใหม่ หรือมีการนำระบบงานใหม่มาใช้ สถาบันการเงินเฉพาะกิจต้องมั่นใจว่ามีการวิเคราะห์ ระบุ ประเมิน และป้องกันความเสี่ยง รวมทั้งการอนุมัติแผนการบริหารความเสี่ยงด้านปฏิบัติการที่เกี่ยวข้องอย่างเหมาะสมแล้ว (ตัวอย่างการควบคุมความเสี่ยงด้านปฏิบัติการตามเอกสารแนบ 1)

(5) การจัดเก็บและรายงานข้อมูลความเสี่ยงด้านปฏิบัติการ

สถาบันการเงินเฉพาะกิจควรจัดเก็บและรายงานข้อมูลเกี่ยวกับความเสี่ยงด้านปฏิบัติการ เพื่อให้ผู้ที่มีส่วนเกี่ยวข้องทราบถึงแนวโน้มและการเปลี่ยนแปลงของความเสี่ยงด้านปฏิบัติการ และสามารถป้องกัน ควบคุม หรือลดความเสียหายได้ โดยหน่วยงานบริหารความเสี่ยงด้านปฏิบัติการควรจัดทำรายงานข้อมูลความเสี่ยงด้านปฏิบัติการ ซึ่งประกอบด้วย

- 1) เหตุการณ์ความเสียหายที่เกิดขึ้น (Loss data)
- 2) ดัชนีชี้วัดความเสี่ยง
- 3) จุดที่มีความเสี่ยงที่สำคัญ
- 4) แนวทางควบคุมหรือลดความเสียหายที่อาจเกิดขึ้น
- 5) จุดบกพร่องในระบบบริหารความเสี่ยงด้านปฏิบัติการ

ทั้งนี้ การจัดเก็บข้อมูลความเสียหายที่เกิดขึ้นจากความเสี่ยงด้านปฏิบัติการ (Loss Data) สถาบันการเงินเฉพาะกิจควรเก็บข้อมูลโดยแบ่งเป็นสายธุรกิจ โดยสามารถเทียบเคียงได้จากหลักเกณฑ์การคำนวณมูลค่าเทียบเท่าสินทรัพย์เสี่ยงด้านปฏิบัติการโดยวิธี Standardised Approach (วิธี SA-OR) ในประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การคำนวณมูลค่าเทียบเท่าสินทรัพย์เสี่ยงด้านปฏิบัติการของสถาบันการเงินเฉพาะกิจ นอกจากนี้ สถาบันการเงินเฉพาะกิจควรกำหนดความเสียหายขั้นต่ำ (Loss Threshold) ให้เหมาะสมและสะท้อนความเสี่ยงขององค์กร เช่น ไม่ควรกำหนด Loss Threshold ที่สูงเกินไป โดยรายละเอียดของข้อมูลที่จัดเก็บควรรวมถึงรายละเอียดดังต่อไปนี้ (ตัวอย่างตารางการเก็บข้อมูลความเสียหายที่เกิดจากความเสี่ยงด้านปฏิบัติการตามเอกสารแนบ 2)

- 1) วันที่เกิดเหตุ และตรวจพบความเสียหาย
- 2) หน่วยงานที่เกิดความเสียหาย
- 3) ประเภทของเหตุการณ์ความเสียหาย โดยสถาบันการเงินเฉพาะกิจสามารถเทียบเคียงและจัดสรรข้อมูลลงใน 7 ประเภทเหตุการณ์ความเสียหายด้านปฏิบัติการ (ตามเอกสารแนบ 3)
- 4) มูลค่าความเสียหายที่เกิดขึ้น
- 5) เงินชดเชยหรือค่าเสียหายที่เรียกคืนได้ ระยะเวลาที่ใช้ในการเรียกคืน และค่าใช้จ่ายในการดำเนินการ
- 6) รายละเอียด และสาเหตุของเหตุการณ์ความเสียหาย
- 7) การดำเนินการแก้ไขเหตุการณ์ความเสียหายที่เกิดขึ้น

นอกจากนี้ สถาบันการเงินเฉพาะกิจควรจัดเก็บและรายงานข้อมูลเหตุการณ์ที่เกิดขึ้น แต่สถาบันการเงินเฉพาะกิจสามารถป้องกันความเสียหายไว้ได้ (Near-Miss) โดยจัดเก็บข้อมูลและเอกสารต่าง ๆ ที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการในรูปแบบอิเล็กทรอนิกส์เพื่อประโยชน์ในการพัฒนาระบบการบริหารความเสี่ยงด้านปฏิบัติการ และเพื่อให้ธนาคารแห่งประเทศไทยสามารถตรวจสอบได้ หรือจัดส่งให้แก่ธนาคารแห่งประเทศไทยเมื่อร้องขอ

(6) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเป็นส่วนหนึ่งของการบริหารความเสี่ยงของสถาบันการเงินเฉพาะกิจ ที่จะทำให้สถาบันการเงินเฉพาะกิจสามารถดำเนินธุรกิจได้อย่างต่อเนื่องกรณีเกิดวิกฤตหรือเหตุการณ์ฉุกเฉิน ดังนั้น สถาบันการเงินเฉพาะกิจจึงจำเป็นต้องมีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเพื่อรองรับเหตุการณ์ความเสียหายที่เกิดจากปัจจัยต่าง ๆ ซึ่งอยู่นอกเหนือการควบคุมของสถาบันการเงินเฉพาะกิจ เช่น ภัยธรรมชาติ การก่อการร้าย ปัญหาในระบบสาธารณูปโภค เพื่อให้สถาบันการเงินเฉพาะกิจสามารถกลับมาดำเนินธุรกิจได้ตามปกติ โดยสถาบันการเงินเฉพาะกิจสามารถอ้างอิงได้จากแนวปฏิบัติธนาคารแห่งประเทศไทยว่าด้วยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของสถาบันการเงินเฉพาะกิจ

3.3.3 การเปิดเผยข้อมูลการบริหารความเสี่ยงด้านปฏิบัติการ

สถาบันการเงินเฉพาะกิจควรเปิดเผยข้อมูลเกี่ยวกับการบริหารความเสี่ยงด้านปฏิบัติการอย่างเพียงพอ โดยขึ้นอยู่กับขนาด ความซับซ้อน และความเสี่ยงของการดำเนินธุรกิจของสถาบันการเงินเฉพาะกิจแต่ละแห่ง เพื่อให้สาธารณชน ผู้ฝากเงิน และผู้ที่มีส่วนเกี่ยวข้อง เข้าใจแนวทางการบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินเฉพาะกิจ และสามารถประเมินประสิทธิภาพของระบบบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินเฉพาะกิจได้

ในการเปิดเผยข้อมูลดังกล่าว สถาบันการเงินเฉพาะกิจควรอธิบายถึงวัตถุประสงค์และนโยบายในการบริหารความเสี่ยงด้านปฏิบัติการ โดยอย่างน้อยต้องครอบคลุมข้อมูล ดังนี้

- (1) กระบวนการบริหารความเสี่ยงด้านปฏิบัติการ
- (2) โครงสร้างและหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการ
- (3) ขอบเขตและลักษณะของระบบการวัด ติดตาม และการรายงานความเสี่ยงด้านปฏิบัติการ
- (4) นโยบายในการป้องกันหรือลดความเสี่ยงด้านปฏิบัติการ รวมทั้งกระบวนการในการติดตามประสิทธิผลของการป้องกันหรือลดความเสี่ยงดังกล่าว
- (5) แนวทางที่ใช้ในการกำหนด Limit สำหรับการควบคุมความเสี่ยงด้านปฏิบัติการ
- (6) บทบาทและหน้าที่ของผู้ตรวจสอบภายในของสถาบันการเงินเฉพาะกิจ

ทั้งนี้ ให้สถาบันการเงินเฉพาะกิจเปิดเผยข้อมูลการบริหารความเสี่ยงด้านปฏิบัติการบน Website ของสถาบันการเงินเฉพาะกิจ ภายใน 4 เดือน นับจากวันสิ้นปีบัญชี

ตัวอย่างการควบคุมความเสี่ยงด้านปฏิบัติการ

ปัจจัยความเสี่ยง	แนวทางการควบคุมความเสี่ยงด้านปฏิบัติการ
บุคลากร	● คัดเลือก อบรม และพัฒนาพนักงานให้มีคุณสมบัติ ประสิทธิภาพ และความสามารถเหมาะสมต่อการปฏิบัติงาน รวมถึงการจัดให้มีทรัพยากรในการปฏิบัติงานต่าง ๆ อย่างเพียงพอ ● ส่งเสริมให้พนักงานตระหนักถึงหน้าที่ความรับผิดชอบของตนต่อการบริหารความเสี่ยงด้านปฏิบัติการขององค์กร รวมทั้งจริยธรรมในการปฏิบัติงาน โดยเฉพาะหน่วยงานที่ต้องอาศัยความน่าเชื่อถือของพนักงานในการปฏิบัติงาน เช่น หน่วยงานที่ทำหน้าที่เกี่ยวกับการรักษาทรัพย์สินและเงินสดของสถาบันการเงินเฉพาะกิจ ● นำหลักการควบคุมภายในมาใช้ เช่น การแบ่งแยกหน้าที่ (Segregation of Duties) การสอบยันการปฏิบัติงาน (Check and Balance) ระบบการปฏิบัติงานโดย 2 ฝ่าย (Dual Control) การยืนยันกระตบยอดอย่างสม่ำเสมอ (Regular Verification and Reconciliation) และการดูแลให้มีความขัดแย้งด้านผลประโยชน์ (Conflict of Interest) น้อยที่สุด ● ดูแลนโยบายการกำหนดค่าตอบแทนให้เหมาะสม เช่น ไม่กำหนดนโยบายการจ่ายค่าตอบแทนที่สัมพันธ์กับกำไรจากการดำเนินงานระยะสั้นเพียงอย่างเดียว เพราะอาจส่งผลให้มีการปฏิบัติงานที่ไม่เป็นตามกฎระเบียบเพื่อบรรลุเป้าหมายการดำเนินงานในระยะสั้น ● จัดให้มีคู่มือและเอกสารการปฏิบัติงานที่ชัดเจน โดยเฉพาะในส่วนที่เกี่ยวข้องกับระบบปฏิบัติการที่ใช้เทคโนโลยีที่ซับซ้อน มีธุรกรรมจำนวนมาก หรือมีส่วนที่จำเป็นต้องปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ เช่น มาตรการป้องกันและฟอกเงิน รวมทั้งมีการระบุจุดที่มีความเสี่ยงไว้ในคู่มือการปฏิบัติงานด้วย
กระบวนการปฏิบัติงานและระบบงาน	● ระบบเทคโนโลยีสารสนเทศ : สถาบันการเงินเฉพาะกิจควรมั่นใจว่าระบบที่ใช้มีความเหมาะสมกับขนาดและความซับซ้อนของสถาบันการเงินเฉพาะกิจ โดยมีการพัฒนาปรับปรุง ควบคุมและตรวจสอบระบบอย่างสม่ำเสมอ ตลอดจนมีการเตรียมความพร้อมในเรื่องศูนย์สำรองข้อมูลและแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ● ระบบเอกสารคู่มือการปฏิบัติงาน : สถาบันการเงินเฉพาะกิจควรมั่นใจว่ามีเอกสารคู่มือเกี่ยวกับขั้นตอนและกระบวนการปฏิบัติงานภายในส่วนงานและระหว่างส่วนงานต่าง ๆ ที่ละเอียด ชัดเจน และเข้าใจง่าย เพื่อให้ทุกหน่วยงานสามารถปฏิบัติงานได้อย่างต่อเนื่อง และลดความผิดพลาดที่อาจเกิดขึ้นได้

	● ระบบเอกสารสัญญาและเอกสารเผยแพร่ : เอกสารสัญญา เอกสารโฆษณาและประชาสัมพันธ์ รวมถึงข้อมูลที่เปิดเผยในงบการเงินที่เผยแพร่สู่สาธารณชน ควรได้รับการตรวจสอบความถูกต้องโดยหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานที่ดูแลการปฏิบัติตามกฎระเบียบ ฝ่ายกฎหมาย ฝ่ายการตลาด ด้วย เพื่อให้มั่นใจว่าเอกสารสัญญาดังกล่าวมีผลบังคับตามกฎหมาย และเอกสารที่เผยแพร่มีความชัดและถูกต้อง ● ระบบรักษาความปลอดภัยของทรัพย์สินและข้อมูล : สถาบันการเงินเฉพาะกิจควรจัดให้มีระบบ ระเบียบและวิธีปฏิบัติที่เกี่ยวกับการเข้าถึงทรัพย์สินและข้อมูล รวมทั้งชั้นความลับของข้อมูลต่าง ๆ อย่างรัดกุมและเหมาะสม และดูแลให้มีการปฏิบัติตามระเบียบและวิธีปฏิบัติอย่างเคร่งครัด โดยข้อมูลอาจอยู่ในรูปแบบของเอกสาร ข้อมูลอิเล็กทรอนิกส์ ข้อมูลที่พนักงานทราบจากการปฏิบัติงานหรือการเข้าถึงข้อมูลของสถาบันการเงินเฉพาะกิจ เพื่อไม่ให้เกิดกรณีพนักงานใช้ทรัพย์สินหรือข้อมูลเพื่อประโยชน์ส่วนตัว เช่น Insider Trading ซึ่งอาจส่งผลเสียหายทางการเงิน และชื่อเสียงของสถาบันการเงินเฉพาะกิจได้
เหตุการณ์ภายนอกต่าง ๆ	● มีการพิจารณาดูแลปัจจัยความเสี่ยงที่เกิดจากเหตุการณ์ภายนอกอย่างรอบคอบ เช่น ภาวะการแข่งขัน สภาพเศรษฐกิจ ภัยธรรมชาติ ภัยจากการก่อการร้าย การฟอกเงิน และกฎหมายต่าง ๆ ที่เกี่ยวข้อง ทั้งนี้ สถาบันการเงินเฉพาะกิจจะต้องมีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องหรือจัดทำประกันภัยเพื่อรองรับหรือลดความเสียหายที่อาจเกิดขึ้นจากปัจจัยซึ่งอยู่เหนือการควบคุมโดยตรงของสถาบันการเงินเฉพาะกิจ ตามแนวปฏิบัติธนาคารแห่งประเทศไทยว่าด้วยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของสถาบันการเงินเฉพาะกิจ

เอกสารแนบ 2

ตารางตัวอย่างการเก็บข้อมูลความเสียหายที่เกิดจากความเสี่ยงด้านปฏิบัติการ

ลำดับที่	หน่วยงาน	สายธุรกิจ	วันที่เกิด	วันที่ตรวจพบ	รายละเอียด	สาเหตุ	ประเภทเหตุการณ์	จำนวนความเสียหาย	จำนวนที่เรียกคืนได้	วันที่ได้รับเงินคืน	ค่าใช้จ่ายในการดำเนินการ	การดำเนินการเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
1.	Branch- Teller	BL 3 (RB)	18/02/60	29/05/60	พนักงานเบิกเงินเกินบัญชีของลูกค้า โดยทุจริต (Teller Fraud)	พนักงานธนาคารได้รับความไว้วางใจจากลูกค้าธนาคารที่อยู่ใกล้สาขาให้เบิกเงินแทนเจ้าของบัญชี	LET 1 (Internal-Fraud)	50,000	50,000	06/06/60	500	1. ผู้จัดการสาขากำกับพนักงาน teller ให้ปฏิบัติตามกฎระเบียบเรื่องบัญชีเงินฝากอย่างเคร่งครัด พร้อมแจ้งลูกค้าทราบภายใน 1 เดือน 2. ตรวจสอบและกำกับสาขาอื่น ๆ ภายใน 1 เดือน

(1) ลำดับที่

(2) หน่วยงาน / ส่วนงาน / สายงานที่เกิดเหตุการณ์ความเสียหาย

(3) สายธุรกิจ (Business Line) มีทั้งหมด 8 สายธุรกิจ

(4) วันที่เกิดเหตุการณ์ความเสียหาย

(5) วันที่ตรวจพบเหตุการณ์ความเสียหาย

(6) รายละเอียดของเหตุการณ์ความเสียหายที่เกิดขึ้น

(7) สาเหตุของเหตุการณ์ความเสียหายที่หน่วยงานทราบหรือที่ตรวจสอบได้ เพื่อประโยชน์ในการกำหนดมาตรการป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต

(8) ประเภทเหตุการณ์ (Loss Event Type) มีทั้งหมด 7 ประเภทเหตุการณ์ (เอกสารแนบ 2)

(9) ความเสียหายที่เป็นตัวเงินที่เกิดขึ้น ซึ่งรวมถึงความสูญเสียหรือเสียหายต่อทรัพย์สิน (Loss of Damage to Assets) จำนวนเงินที่ต้องรับผิดชอบชดใช้ (Legal Liability) ค่าใช้จ่ายเพื่อ

ดำเนินการให้กลับสู่สภาพเดิม (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

(13) การดำเนินการเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต เช่น ปรับปรุงระบบควบคุมภายใน ดูแลให้มีการปฏิบัติตามกฎระเบียบที่กำหนด หรือพัฒนาระบบรักษาความปลอดภัยให้เข้มงวดขึ้น ซึ่งควรกำหนดกรอบเวลาและผู้รับผิดชอบอย่างชัดเจน พร้อมทั้งติดตามการดำเนินการอย่างใกล้ชิด

ตารางการจำแนกประเภทเหตุการณ์ความเสียหายด้านปฏิบัติการ

ประเภทเหตุการณ์	คำจำกัดความ	ประเภทเหตุการณ์ย่อย	ตัวอย่างกิจกรรม
1. ความเสียหายจากการฉ้อโกง โดยบุคคลภายใน (Internal Fraud)	ความเสียหายที่เกิดจากการกระทำโดยเจตนาของบุคคลภายในหรือบุคคลที่เกี่ยวข้องกับสถาบันการเงินเฉพาะกิจ ตั้งแต่ 1 คนขึ้นไป เพื่อฉ้อโกง เพื่อใช้ทรัพย์สินของสถาบันการเงินเฉพาะกิจในทางที่ไม่เหมาะสม หรือเพื่อหลีกเลี่ยงกฎหมาย หลักเกณฑ์ของทางการ หรือนโยบายของสถาบันการเงินเฉพาะกิจ โดยไม่รวมถึงกรณีที่สถาบันการเงินเฉพาะกิจถูกฟ้องร้องเรียกค่าเสียหายจากการไม่ปฏิบัติตามข้อกำหนดด้านความหลากหลายของพนักงาน (Diversity) หรือการเลือกปฏิบัติ	- การทำธุรกรรมโดยไม่ได้รับอนุญาต	- การทำธุรกรรมโดยไม่ได้รับรายงาน (โดยเจตนา) - การทำธุรกรรมโดยไม่ได้รับอนุญาต (มีความเสียหายที่เป็นตัวเงินเกิดขึ้น) - การบันทึกธุรกรรมหรือฐานะไม่ถูกต้อง (โดยเจตนา)
		- การขโมยและการฉ้อโกง	- การฉ้อโกง การฉ้อโกงด้านเครดิต การฝากเงินโดยไม่มีเม็ดเงินที่แท้จริง - การขโมย การชู้กรรโชก การยกยอก การโจรกรรม - การใช้ทรัพย์สินของสถาบันการเงินเฉพาะกิจในทางที่ไม่เหมาะสม - การทำลายทรัพย์สินของสถาบันการเงินเฉพาะกิจโดยเจตนา - การปลอมแปลงต่าง ๆ - การโอนเงินผ่านเช็คโดยไม่มีเม็ดเงินที่แท้จริง (Check Kiting) - การลักลอบนำสิ่งของเข้าหรือออกจากสถาบันการเงินเฉพาะกิจโดยไม่ได้รับอนุญาต - การลักลอบใช้บัญชีของผู้อื่น (Account Take-Over) หรือการปลอมเป็นบุคคลอื่น (Impersonation) - การไม่ปฏิบัติตามหลักเกณฑ์ทางด้านภาษีหรือการหลบเลี่ยงภาษี (โดยเจตนา) - การติดสินบน หรือการให้เงินใต้โต๊ะ - การทำธุรกรรมซื้อขายหลักทรัพย์โดยใช้ข้อมูลภายใน (Insider Trading) (ไม่ได้ทำผ่านบัญชีของสถาบันการเงินเฉพาะกิจ)

ประเภทเหตุการณ์	คำจำกัดความ	ประเภทเหตุการณ์ย่อย	ตัวอย่างกิจกรรม
2. ความเสียหายจากการฉ้อโกง โดยบุคคลภายนอก (External Fraud)	ความเสียหายที่เกิดจากการกระทำโดยเจตนาของบุคคลที่ไม่มีความเกี่ยวข้องกับสถาบันการเงินเฉพาะกิจเพื่อฉ้อโกง เพื่อใช้ทรัพย์สินของสถาบันการเงินเฉพาะกิจในทางที่ไม่เหมาะสม หรือเพื่อหลีกเลี่ยงกฎหมาย	- การขโมยและการฉ้อโกง	- การขโมย การโจรกรรม - การปลอมแปลงต่าง ๆ - การโอนเงินผ่านเช็คโดยไม่มีเม็ดเงินที่แท้จริง (Check Kiting)
		- ความปลอดภัยของระบบงาน	- ความเสียหายจากการถูกลักลอบเข้าระบบ - การขโมยข้อมูล (มีความเสียหายที่เป็นตัวเงินเกิดขึ้น)
3. ความเสียหายจากแนวปฏิบัติ เกี่ยวกับการจ้างงานและความ ปลอดภัยของพนักงาน (Employment Practices and Workplace Safety)	ความเสียหายที่เกิดจากการกระทำที่ไม่สอดคล้องกับกฎหมายหรือข้อตกลงที่เกี่ยวข้องกับการจ้างงาน สุขภาพหรือความปลอดภัยในที่ทำงาน หรือเกิดจากการจ่ายค่าชดเชยให้แก่พนักงานที่ได้รับบาดเจ็บจากการทำงาน หรือเกิดจากการไม่ปฏิบัติตามข้อกำหนดด้านความปลอดภัยของพนักงานหรือการเลือกปฏิบัติ	- ความสัมพันธ์กับพนักงาน	- ประเด็นเกี่ยวกับค่าตอบแทน ผลประโยชน์ และการเลิกจ้างงาน - กิจกรรมของสหภาพแรงงานหรือการรวมตัวของพนักงาน
		- สภาพแวดล้อมการทำงานที่ปลอดภัย	- ภาวะความรับผิดชอบทั่วไป (เช่น การลื่นหกล้ม) - เหตุการณ์เกี่ยวกับระเบียบข้อบังคับด้านสุขภาพและความปลอดภัยของพนักงาน - การจ่ายค่าชดเชยให้แก่พนักงาน
		- ความหลากหลายของพนักงานและการเลือกปฏิบัติ	- การเลือกปฏิบัติทุกประเภท
4. ความเสียหายจากแนวปฏิบัติ เกี่ยวกับลูกค้า ผลิตภัณฑ์ และ การดำเนินธุรกิจ (Clients, Products and Business Practices)	ความเสียหายที่เกิดจากการไม่สามารถปฏิบัติตามข้อผูกพันที่มีกับลูกค้า (รวมถึง ข้อกำหนดเกี่ยวกับการทำหน้าที่ผู้ได้รับมอบหมายให้จัดการดูแลทรัพย์สิน และความเหมาะสมของการปฏิบัติหน้าที่) โดยไม่ได้ตั้งใจ หรือเพราะความละเลย หรือเกิดจากลักษณะของผลิตภัณฑ์ หรือการออกแบบผลิตภัณฑ์	- ความเหมาะสมของการปฏิบัติหน้าที่ การเปิดเผยข้อมูล และการทำหน้าที่ผู้ได้รับมอบหมายให้จัดการดูแลทรัพย์สิน	- การไม่ปฏิบัติตามข้อกำหนดเกี่ยวกับการทำหน้าที่ผู้ได้รับมอบหมายให้จัดการดูแลทรัพย์สิน และการฝ่าฝืนแนวปฏิบัติ - ประเด็นเกี่ยวกับความเหมาะสมของการปฏิบัติหน้าที่และการเปิดเผยข้อมูล - การฝ่าฝืนหลักเกณฑ์การเปิดเผยข้อมูลของลูกค้ารายย่อย - การละเมิดสิทธิส่วนบุคคล (Breach of Privacy) - การเสนอขายที่มีลักษณะคุกคามลูกค้า

ประเภทเหตุการณ์	คำจำกัดความ	ประเภทเหตุการณ์ย่อย	ตัวอย่างกิจกรรม
			- การทำธุรกรรมเพื่อบัญชีลูกค้าเป็นจำนวนมาก เพื่อให้ได้ค่านายหน้าสูงขึ้น (Account Churning) - การนำข้อมูลที่ควรปกปิดเป็นความลับไปใช้ในทางที่ผิด - ภาระความรับผิดชอบของผู้ให้กู้
		- วิธีปฏิบัติเกี่ยวกับการดำเนินธุรกิจหรือการตลาดที่ไม่เหมาะสม	- การผูกขาดผลิตภัณฑ์หรือบริการ - วิธีปฏิบัติด้านการทำธุรกรรมหรือการตลาดที่ไม่เหมาะสม - การปั่นหุ้นหรือตลาดอื่น ๆ (Market Manipulation) - การทำธุรกรรมซื้อขายหลักทรัพย์โดยใช้ข้อมูลภายใน (โดยทำผ่านบัญชีของสถาบันการเงินเฉพาะกิจเอง) - การทำธุรกรรมที่ไม่ได้รับอนุญาตจากทางการ - การฟอกเงิน
		- ข้อบกพร่องของผลิตภัณฑ์	- ข้อบกพร่องของผลิตภัณฑ์ (เช่น ยังไม่ได้รับอนุญาต) - ข้อผิดพลาดของแบบจำลอง (ถ้ามี)
		- การคัดเลือก การให้การสนับสนุน และการทำธุรกรรมหรือมีฐานะ (Exposure) กับลูกค้า	- การไม่สามารถตรวจสอบลูกค้าได้ตามหลักเกณฑ์ที่กำหนด - การทำธุรกรรมหรือมีฐานะ (Exposure) กับลูกค้าเกินกว่าระดับที่กำหนด
		- การทำหน้าที่ให้คำปรึกษา	- เกิดกรณีโต้แย้งในเรื่องผลงานจากการปฏิบัติหน้าที่ให้คำปรึกษา
5. ความเสียหายต่อทรัพย์สิน (Damage to Physical Assets)	ความเสียหายต่อทรัพย์สินอันเนื่องมาจากภัยพิบัติทางธรรมชาติหรือเหตุการณ์อื่น ๆ	- ภัยพิบัติหรือเหตุการณ์อื่น ๆ	- ความเสียหายจากภัยพิบัติทางธรรมชาติ - ความเสียหายที่เกิดขึ้นจากการกระทำของบุคคลภายนอกองค์กร เช่น การก่อการร้าย การทำลายทรัพย์สิน

ประเภทเหตุการณ์	คำจำกัดความ	ประเภทเหตุการณ์ย่อย	ตัวอย่างกิจกรรม
6. ความเสียหายจากการที่ธุรกิจหยุดชะงักและระบบงานขัดข้อง โดยไม่สามารถใช้งานได้ตามปกติ (Business Disruption and System Failures)	ความเสียหายจากการที่ธุรกิจหยุดชะงัก หรือระบบงานขัดข้องโดยไม่สามารถใช้งานได้ตามปกติ	- ระบบงาน	- เครื่องมือ อุปกรณ์ (Hardware) - โปรแกรม (Software) - โทรคมนาคม - การหยุดชะงักหรือการไม่มีสาธารณูปโภคต่าง ๆ ใช้ในช่วงเวลาหนึ่ง
7. ความเสียหายจากการปฏิบัติการส่งมอบ และการจัดการกระบวนการ (Execution, Delivery and Process Management)	ความเสียหายที่เกิดจากความล้มเหลวของการประมวลผล การทำธุรกรรม หรือการจัดการกระบวนการ หรือที่เกิดจากความสัมพันธ์กับคู่สัญญาและผู้ให้บริการ	- การนำข้อมูลเข้าสู่ระบบ การปฏิบัติการ และการเก็บรักษาข้อมูลเกี่ยวกับการทำธุรกรรม	- การสื่อสารผิดพลาด - ความผิดพลาดในการนำข้อมูลเข้าสู่ระบบ การเก็บรักษา หรือการดึงข้อมูล - ไม่สามารถปฏิบัติงานได้ตามกำหนดเวลา หรือตามหน้าที่ที่ได้รับมอบหมาย - การปฏิบัติงานของระบบงานหรือแบบจำลอง (ถ้ามี) ผิดพลาด - ความผิดพลาดทางด้านบัญชี - ความผิดพลาดของการปฏิบัติงานอื่น ๆ - ความล้มเหลวในการส่งมอบ - ความล้มเหลวในการบริหารหลักประกัน - ความเสียหายหรือความผิดพลาดในการเก็บรักษาข้อมูลที่ใช้อ้างอิง
		- การติดตามและการรายงาน	- การไม่สามารถรายงานข้อมูลได้ตามข้อกำหนด - รายงานที่ส่งออกไปยังภายนอกไม่ถูกต้อง (มีความเสียหายเกิดขึ้น)

ประเภทเหตุการณ์	คำจำกัดความ	ประเภทเหตุการณ์ย่อย	ตัวอย่างกิจกรรม
		- การรับคำสั่งของลูกค้าและการจัดทำเอกสาร	- เอกสารหรือข้อความเกี่ยวกับการให้ความยินยอมของลูกค้าหรือการปฏิเสธความรับผิดชอบ - เอกสารทางด้านกฎหมายสัญญาหรือไม่ครบถ้วน
		- การบริหารจัดการบัญชีของลูกค้า	- การเข้าถึงบัญชีของลูกค้าโดยไม่ได้รับอนุญาต - การบันทึกข้อมูลลูกค้าไม่ถูกต้อง (มีความเสียหายเกิดขึ้น) - ทรัพย์สินของลูกค้าสูญหายหรือเสียหายเพราะความละเลยของสถาบันการเงินเฉพาะกิจ
		- คู่สัญญาของสถาบันการเงินเฉพาะกิจ	- ความผิดพลาดจากการปฏิบัติงานของคู่สัญญาที่ไม่ใช่ลูกค้า - เกิดกรณีโต้แย้งกับคู่สัญญาที่ไม่ใช่ลูกค้า
		- ผู้ให้บริการ หรือผู้จัดหาบริการให้กับสถาบันการเงินเฉพาะกิจ	- การใช้บริการจากผู้ให้บริการสนับสนุนการประกอบธุรกิจ (Business Facilitator) - เกิดกรณีโต้แย้งกับผู้ให้บริการ