ธนาคารแห่งประเทศไทย
BANK OF THAILAND

เอกสารรับฟังความคิดเห็น

(ร่าง) หลักเกณฑ์การบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินและกลุ่มธุรกิจทางการเงิน

สายนโยบายสถาบันการเงิน
ธนาคารแห่งประเทศไทย
ธันวาคม 2565

ประกาศธนาคารแห่งประเทศไทย

ที่ สนส. /2566

เรื่อง หลักเกณฑ์การบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินและกลุ่มธุรกิจทางการเงิน

---

1. เหตุผลในการออกประกาศ

ความเสี่ยงด้านปฏิบัติการถือเป็นความเสี่ยงหลักของสถาบันการเงินเนื่องจากการทำธุรกรรมและการให้บริการทางการเงินทุกประเภทของสถาบันการเงินได้ก่อให้เกิดความเสี่ยงดังกล่าวผ่านตัวขับเคลื่อนความเสี่ยง (risk driver) ทั้งจากปัจจัยภายในของสถาบันการเงิน เช่น กระบวนการปฏิบัติงานภายใน บุคลากร ระบบงาน หรือจากปัจจัยภายนอก เช่น สภาพเศรษฐกิจ การแข่งขันในตลาด กฎหมายต่างๆ ที่เกี่ยวข้อง นอกจากนี้ จากเหตุการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 นับเป็นตัวเร่งสำคัญที่ทำให้เกิดความเปลี่ยนแปลงในด้านเทคโนโลยี (digital disruption) โดยสถาบันการเงินได้ปรับการให้บริการในรูปแบบอิเล็กทรอนิกส์มากขึ้น และปรับรูปแบบการทำงานเป็นแบบ work from home ซึ่งได้กลายเป็นความปกติรูปแบบใหม่ (new normal) ของการทำงานในปัจจุบัน ดังนั้น จากการเปลี่ยนแปลงดังกล่าว แม้จะทำให้เกิดความยืดหยุ่นในการให้บริการแก่ลูกค้าและการปฏิบัติงานให้สามารถดำเนินงานต่อไปได้ แต่ก็ทำให้เกิดความเสี่ยงด้านปฏิบัติการที่เพิ่มขึ้น ซึ่งรวมถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อสถาบันการเงินด้วยเช่นกัน

ธนาคารแห่งประเทศไทย (ธปท.) จึงปรับปรุงหลักเกณฑ์การบริหารความเสี่ยงด้านปฏิบัติการเพื่อให้สอดรับกับบริบทในปัจจุบัน และสอดคล้องกับหลักเกณฑ์สากล โดย ธปท. กำหนดองค์ประกอบของกรอบนโยบายการบริหารความเสี่ยงด้านปฏิบัติการ (operational risk management framework: ORMF) อ้างอิงจากแนวทางของ Basel Committee on Banking Supervision (BCBS) ได้แก่ (1) the principles for the sound management of operational risk ซึ่งกำหนดรายละเอียดในแต่ละองค์ประกอบของ ORMF ที่ชัดเจนขึ้น เช่น การกำหนดหน้าที่ของหน่วยงานกำกับภายใน (second line of defense) ทั้งในส่วนที่เป็นหน่วยงานบริหารความเสี่ยง (risk management function) และหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (compliance function) การยกตัวอย่างเพื่อให้สถาบันการเงินใช้เป็นแนวทางดำเนินการ (เช่น แนวทางการจัดทำชุดนิยามของความเสี่ยงด้านปฏิบัติการ หรือ taxonomy ตัวอย่างเครื่องมือที่ใช้ระบุและประเมินความเสี่ยง รวมทั้งให้ความสำคัญในเรื่องการบริหารจัดการความเปลี่ยนแปลง (change management) และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (2) Principles for operational resilience ซึ่งกำหนดแนวทางเพื่อให้สถาบันการเงินมีความสามารถดำเนินการธุรกรรมสำคัญในสถานการณ์

ไม่ปกติได้อย่างต่อเนื่องหรือกลับมาดำเนินการได้ภายในระยะเวลาที่เหมาะสม (operational resilience หรือ ability to deliver critical operations through disruption[1])

นอกจากนี้ ปัญหาจากความเสี่ยงด้านปฏิบัติการที่เกิดขึ้นกับบริษัทใดบริษัทหนึ่งในกลุ่มธุรกิจทางการเงินอาจลุกลามขยายไปยังสถาบันการเงิน และบริษัทอื่นๆ ในกลุ่มธุรกิจทางการเงินได้ บริษัทแม่ของกลุ่มธุรกิจทางการเงินจึงจำเป็นต้องเข้าใจถึงความเสี่ยงด้านปฏิบัติการของบริษัทลูก และในภาพรวมของกลุ่มธุรกิจทางการเงิน เพื่อให้สามารถบริหารจัดการความเสี่ยงนั้นได้อย่างเหมาะสม ดังนั้น บริษัทแม่ของกลุ่มธุรกิจต้องจัดให้มีนโยบายต่างๆ ในภาพรวมที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการของกลุ่มธุรกิจทางการเงิน โดยให้นำหลักเกณฑ์ที่กำหนดไว้ตามประกาศฉบับนี้บังคับใช้กับบริษัทแม่ของกลุ่มธุรกิจทางการเงินโดยอนุโลมด้วย

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 41 วรรค 3 (2) และ มาตรา 57 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ให้ธนาคารแห่งประเทศไทยออกข้อกำหนดเกี่ยวกับการกำกับการปฏิบัติตามกฎเกณฑ์ของสถาบันการเงิน และกลุ่มธุรกิจทางการเงิน ให้สถาบันการเงิน และกลุ่มธุรกิจทางการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

3. แนวปฏิบัติ ประกาศ และหนังสือเวียนที่ยกเลิก

แนวปฏิบัติ ประกาศ และหนังสือเวียนที่ยกเลิกตามเอกสารแนบ 1

4. ขอบเขตการบังคับใช้

ประกาศนี้ใช้บังคับกับ

4.1 สถาบันการเงินทุกแห่งตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

4.2 บริษัทแม่ของกลุ่มธุรกิจทางการเงินทุกแห่งตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

[1] The Principles for Operational Resilience (POR) issued by the Basel Committee on Banking Supervision (BCBS) in March 2021 defines operational resilience as the ability of a bank to deliver critical operations through disruption.

5. เนื้อหา

5.1 คำจำกัดความ

ในประกาศฉบับนี้

“ความเสี่ยงด้านปฏิบัติการ”[2] หมายความว่า ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดีหรือขาดธรรมาภิบาลในองค์กร และการขาดการควบคุมที่ดี โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน คน ระบบงาน หรือเหตุการณ์ภายนอก และส่งผลกระทบต่อรายได้และเงินกองทุนของสถาบันการเงิน ทั้งนี้ สถาบันการเงินอาจกำหนดคำจำกัดความของความเสี่ยงด้านปฏิบัติการให้กว้างกว่าคำจำกัดความนี้ได้ตามที่สถาบันการเงินเห็นสมควร เพื่อประโยชน์ของการบริหารความเสี่ยงด้านปฏิบัติการขององค์กร

“กลุ่มธุรกิจทางการเงิน” หมายความว่า กลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์เกี่ยวกับโครงสร้างและขอบเขตธุรกิจของกลุ่มธุรกิจทางการเงิน

“ความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (operational resilience)” หมายความว่า ในสถานการณ์ที่สถาบันการเงินถูกคุกคาม หรือถูกแทรกแซง (disrupt) จากปัจจัยทั้งภายในและภายนอก (เช่น อุบัติเหตุ อัคคีภัย ภัยธรรมชาติ การก่อเหตุวินาศกรรม สถานการณ์โรคระบาด ภัยคุกคามไซเบอร์ ฯ) จนส่งผลกระทบต่อการดำเนินงานปกติ สถาบันการเงินยังมีความพร้อมดำเนินการธุรกรรมสำคัญได้อย่างต่อเนื่องหรือกลับมาดำเนินการได้ในเวลาที่เหมาะสม

“สถานการณ์ไม่ปกติ (disruptive event)” หมายความว่า สถานการณ์ที่สถาบันการเงินถูกคุกคาม หรือถูกแทรกแซง (disrupt) จากปัจจัยทั้งภายในและภายนอก (เช่น อุบัติเหตุ อัคคีภัย ภัยธรรมชาติ การก่อเหตุวินาศกรรม สถานการณ์โรคระบาด ภัยคุกคามไซเบอร์ ฯ) จนส่งผลกระทบต่อการดำเนินงานปกติ เช่น ทำให้การดำเนินงานปกติต้องหยุดชะงัก เป็นต้น

“ธุรกรรมสำคัญ (critical operations)” หมายความว่า กิจกรรม กระบวนการบริการ และทรัพยากรที่จำเป็นในการดำเนินงาน ซึ่งรวมถึง บุคลากร เทคโนโลยี ข้อมูล และสิ่งอำนวยความสะดวก ที่หากเกิดสถานการณ์ไม่ปกติส่งผลให้ธุรกรรมสำคัญต้องหยุดชะงัก จะส่งผลกระทบต่อการดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะและผลการดำเนินงานของสถาบันการเงินเอง **หรือระบบสถาบันการเงินอย่างมีนัยสำคัญ**

---

[2] Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. (อ้างอิงจากคำจำกัดความของ The Bank for International Settlements โดย Basel Committee on Banking Supervision)

“ระดับการหยุดชะงักที่ยอมรับได้ (tolerance for disruption)” หมายความว่า ระดับการหยุดชะงักของธุรกรรมสำคัญที่ยอมรับได้มากที่สุด ซึ่งหากเกินกว่าที่กำหนด จะส่งผลกระทบต่อการดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะและผลการดำเนินงานของสถาบันการเงินเองหรือระบบสถาบันการเงินอย่างมีนัยสำคัญ

“สถานการณ์รุนแรงที่มีโอกาสเกิดขึ้น (severe but plausible scenarios)” หมายความว่า สถานการณ์ไม่ปกติอย่างรุนแรงที่สามารถเกิดขึ้นและกระทบต่อธุรกรรมสำคัญ โดยต้องสมเหตุสมผล และเป็นไปได้ เช่น เหตุภัยธรรมชาติ โรคระบาด หรือผู้ให้บริการที่สำคัญไม่สามารถใช้งานได้ เป็นต้น

“เหตุการณ์ผิดปกติ (incident)” หมายความว่า เหตุการณ์ไม่พึงประสงค์หรือเหตุการณ์ไม่ปกติที่เกิดขึ้นจริงในปัจจุบันหรือในอดีต ซึ่งเหตุการณ์ดังกล่าวส่งผลเสียต่อการดำเนินการธุรกรรมสำคัญของสถาบันการเงิน

5.2 หลักการ

ความเสี่ยงด้านปฏิบัติการเป็นความเสี่ยงที่มีอยู่ในผลิตภัณฑ์ การบริการ กระบวนการปฏิบัติงาน และระบบงานของสถาบันการเงิน ดังนั้น สถาบันการเงินต้องจัดให้มีกรอบนโยบายการบริหารความเสี่ยงด้านปฏิบัติการ (operational risk management framework: ORMF) เป็นส่วนหนึ่งของกระบวนการบริหารความเสี่ยงภาพรวม (enterprise risk management: ERM) ขององค์กร ที่สอดคล้องกับขนาด กลยุทธ์ ลักษณะและความซับซ้อนของธุรกิจ รวมถึงความเสี่ยงในภาพรวม เพื่อให้การบริหารความเสี่ยงขององค์กรไปในทิศทางเดียวกัน และผลักดันตามกลยุทธ์ที่องค์กรกำหนดไว้ และเพื่อให้สอดรับกับบริบทในปัจจุบัน ORMF ต้องครอบคลุมในเรื่องการบริหารจัดการความเปลี่ยนแปลง (change management) รวมถึงมีความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (operational resilience) ด้วย

นอกจากนี้ เพื่อให้รองรับความเสี่ยงด้านปฏิบัติการที่อาจเกิดขึ้นจากการดำเนินธุรกิจในลักษณะกลุ่มธุรกิจทางการเงิน และจากการให้การสนับสนุนระหว่างกันภายในกลุ่มธุรกิจทางการเงิน จึงควรมีการบริหารความเสี่ยงด้านปฏิบัติการในภาพรวมของกลุ่มธุรกิจทางการเงินด้วย ซึ่งบริษัทแม่ของกลุ่มธุรกิจทางการเงินต้องเข้าใจและตระหนักถึงความเสี่ยงด้านปฏิบัติการของบริษัทลูกและในภาพรวมของกลุ่มธุรกิจทางการเงิน เพื่อให้สามารถบริหาร ควบคุม และติดตามความเสี่ยงของทุกบริษัทในกลุ่มธุรกิจได้อย่างทั่วถึง ดังนั้น บริษัทแม่ของกลุ่มธุรกิจทางการเงินต้องจัดให้มีนโยบายต่างๆ ในภาพรวมที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการของกลุ่มธุรกิจทางการเงิน โดยให้นำหลักเกณฑ์ที่กำหนดไว้ตามประกาศฉบับนี้บังคับใช้โดยอนุโลมด้วย

สำหรับสาขาธนาคารพาณิชย์ต่างประเทศที่บริษัทแม่ หรือสำนักงานใหญ่มีการกำหนดกรอบการบริหารความเสี่ยงด้านปฏิบัติการ ซึ่งสอดคล้องกับประกาศฉบับนี้ ให้สาขาธนาคารพาณิชย์ต่างประเทศถือปฏิบัติตามกรอบการบริหารความเสี่ยงด้านปฏิบัติการดังกล่าวได้ ทั้งนี้ กรณีสาขาธนาคารพาณิชย์ต่างประเทศใดที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ได้ ให้ขอหารือธนาคารแห่งประเทศไทยเป็นรายกรณี

5.3 องค์ประกอบของกรอบนโยบายการบริหารความเสี่ยงด้านปฏิบัติการ (operational risk management framework: ORMF) ของสถาบันการเงิน

5.3.1 การกำกับดูแลความเสี่ยงด้านปฏิบัติการ (operational risk governance)

คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูงในฐานะผู้นำองค์กร มีบทบาทสำคัญในการกำกับดูแลความเสี่ยงด้านปฏิบัติการ ซึ่งรวมถึงการปลูกฝังวัฒนธรรมด้านความเสี่ยง (risk culture) ที่ทำให้ทุกคนในองค์กรตระหนักถึงความเสี่ยง และปฏิบัติตนอย่างเหมาะสมเพื่อให้การบริหารความเสี่ยงโดยรวมของสถาบันการเงินมีประสิทธิภาพ โดยต้องดำเนินการ ดังนี้

(1) คณะกรรมการสถาบันการเงินต้องดูแลให้สถาบันการเงินจัดทำนโยบายการบริหารความเสี่ยงด้านปฏิบัติการ (ORMF) และอนุมัตินโยบายดังกล่าว รวมทั้งกำหนดให้มีการทบทวนนโยบายตามความถี่ที่พิจารณาแล้วว่าเหมาะสม **โดยในกรณีการปรับปรุงแก้ไขนโยบายในประเด็นที่ไม่มีนัยสำคัญ คณะกรรมการสถาบันการเงินสามารถมอบหมายให้คณะกรรมการชุดย่อยในระดับกำกับดูแลทำหน้าที่ในการอนุมัติได้ และให้นำเสนอต่อคณะกรรมการสถาบันการเงินเพื่อทราบ**

(2) ผู้บริหารระดับสูงต้องนำ ORMF ที่คณะกรรมการสถาบันการเงินอนุมัติมาพัฒนาให้เกิดระเบียบ กฎเกณฑ์ หรือขั้นตอนการปฏิบัติงานในองค์กร **และกำหนดโครงสร้างการกำกับดูแลความเสี่ยง (governance structure) ที่มีประสิทธิภาพ โปร่งใส และเข้มแข็ง ประกอบกับการระบุหน้าที่ความรับผิดชอบในการบริหารความเสี่ยงด้านปฏิบัติการที่ชัดเจน รวมถึง** สื่อสารให้พนักงานทุกคนในองค์กรเข้าใจและตระหนักถึงความสำคัญและหน้าที่ความรับผิดชอบเกี่ยวกับความเสี่ยงด้านปฏิบัติการ เพื่อให้พนักงานทุกคนในองค์กรถือปฏิบัติได้

ทั้งนี้ ให้สถาบันการเงินถือปฏิบัติในเรื่องบทบาทหน้าที่ของกรรมการสถาบันการเงิน และบทบาทหน้าที่ของผู้บริหารระดับสูงตามที่กำหนดไว้ตามประกาศธนาคารแห่งประเทศไทยว่าด้วยธรรมาภิบาลของสถาบันการเงิน

5.3.2 การกำหนดนโยบายการบริหารความเสี่ยงด้านปฏิบัติการ

สถาบันการเงินต้องจัดทำนโยบายการบริหารความเสี่ยงด้านปฏิบัติการเป็นลายลักษณ์อักษร และสื่อสารให้พนักงานทุกคนในองค์กรเข้าใจ **เพื่อใช้เป็นแนวทางในการบริหาร**

ความเสี่ยงด้านปฏิบัติการในทางปฏิบัติ เช่น นิยามของความเสี่ยงด้านปฏิบัติการ (operational risk taxonomy) ระดับความเสี่ยงด้านปฏิบัติการที่ยอมรับได้ (operational risk appetite) เครื่องมือสำหรับการบริหารความเสี่ยง ทั้งนี้ เพื่อให้ภาพรวมของการบริหารความเสี่ยงสอดคล้องและเป็นไปตามเป้าหมายที่องค์กรกำหนดไว้ โดยนโยบายการบริหารความเสี่ยงด้านปฏิบัติการต้องมีข้อมูลอย่างน้อยตามที่กำหนดในเอกสารแนบ 2

5.3.3 หน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการ (three lines of defense)

สถาบันการเงินต้องมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่างหน่วยงานหรือผู้ที่ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (business unit หรือ first line of defense) หน่วยงานกำกับภายใน (second line of defense) และหน่วยงานตรวจสอบภายใน (internal audit หรือ third line of defense) เพื่อให้ผู้มีหน้าที่ในแต่ละหน่วยงานเข้าใจบทบาทหน้าที่ของตน รวมถึงส่วนที่เกี่ยวข้องกับหน่วยงานอื่นซึ่งจะทำให้มีการบริหารความเสี่ยงที่ครอบคลุมทั่วถึงทั้งองค์กร และมีการประสานงานกันเพื่อเพิ่มประสิทธิภาพการบริหารความเสี่ยง โดยให้สถาบันการเงินถือปฏิบัติเกี่ยวกับบทบาทหน้าที่ของแต่ละหน่วยงานตามที่กำหนดในเอกสารแนบ 3

5.3.4 ระบบบริหารความเสี่ยงด้านปฏิบัติการ

ระบบบริหารความเสี่ยงด้านปฏิบัติการที่สถาบันการเงินต้องดำเนินการประกอบด้วย 3 ขั้นตอนสำคัญ ได้แก่ (1) การระบุ (risk identification) และการประเมินความเสี่ยง (risk assessment) (2) ควบคุม (risk control) และลดความเสี่ยง (risk mitigation) (3) การติดตามดูแลความเสี่ยง (risk monitoring) การจัดเก็บข้อมูล และรายงานความเสี่ยงด้านปฏิบัติการ (risk reporting) โดยต้องกำหนดให้เหมาะสมกับขนาด ความซับซ้อน และความเสี่ยง **นอกจากนี้ ต้องสามารถควบคุมความเสี่ยงที่เกิดจากปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงด้านปฏิบัติการ โดยเฉพาะปัจจัยความเสี่ยงที่เกิดจากการริเริ่มความเปลี่ยนแปลง (change initiatives) เช่น การออกผลิตภัณฑ์และบริการทางการเงินรูปแบบใหม่ การเข้าสู่ตลาดใหม่ การปรับเปลี่ยน กระบวนการ ระบบงาน หรือการขยายขอบเขตการดำเนินงานที่อยู่ห่างไกลจากสำนักงานใหญ่ โดยสถาบันการเงินต้องมีนโยบายและกระบวนการบริหารจัดการความเปลี่ยนแปลง (change management) ที่สามารถประเมินความเสี่ยงที่เกี่ยวข้องตั้งแต่ริเริ่มจนสิ้นสุด (เช่น ตลอดวงจรชีวิตของผลิตภัณฑ์) เพื่อให้สามารถควบคุมและลดความเสี่ยงที่อาจเกิดขึ้น**

ทั้งนี้ ให้สถาบันการเงินถือปฏิบัติในเรื่องระบบการบริหารความเสี่ยงด้านปฏิบัติการตามที่กำหนดในเอกสารแนบ 4 และถือปฏิบัติในเรื่องการบริหารความเปลี่ยนแปลงตามที่กำหนดไว้ในเอกสารแนบ 5

5.3.5 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk: IT Risk)

การนำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจแทนการปฏิบัติงานของพนักงานเพื่อเพิ่มประสิทธิภาพในการดำเนินงาน ส่งผลให้ความเสี่ยงของสถาบันการเงินเปลี่ยนแปลงไป **สถาบันการเงินจึงต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management : IT RM) ที่ควบคู่กับการบริหารความเสี่ยงด้านปฏิบัติการและเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงิน (enterprise risk management : ERM) ทั้งนี้ ให้สถาบันการเงินถือปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk) ของสถาบันการเงิน และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก**

5.3.6 การเตรียมความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (การจัดทำ operational resilience framework)

เพื่อให้สถาบันการเงินมีความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ ธปท. จึงกำหนดให้สถาบันการเงินต้องจัดทำ operational resilience framework ซึ่งอย่างน้อยต้องมีองค์ประกอบ 6 ส่วนที่สำคัญ ดังนี้

(1) บทบาทหน้าที่ของคณะกรรมการและผู้บริหารระดับสูง

การจัดทำ operational resilience framework เป็นความรับผิดชอบของคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงิน โดยต้องกำกับดูแลและให้การสนับสนุน รวมทั้งผลักดันให้สถาบันการเงินมีความพร้อมดำเนินการธุรกรรมสำคัญได้อย่างต่อเนื่องหรือกลับมาดำเนินการได้ในเวลาที่เหมาะสม แม้ว่าจะอยู่ในสถานการณ์ที่ไม่ปกติ โดยสถาบันการเงินต้องสามารถตอบสนองและปรับเปลี่ยนการดำเนินงานได้ตามสถานการณ์ รวมถึงสามารถกู้คืนการดำเนินงานที่หยุดชะงักจากเหตุการณ์ไม่ปกติให้กลับสู่ภาวะปกติได้อย่างรวดเร็ว และนำบทเรียนจากสถานการณ์ที่เกิดขึ้นในอดีตมาปรับปรุงการบริหารจัดการให้ดียิ่งขึ้นในปัจจุบันหรือเพื่อป้องกันไม่ให้เกิดเหตุการณ์เช่นเดิมอีก

(2) การกำหนดธุรกรรมสำคัญ (critical operations) ระดับการหยุดชะงักที่ยอมรับได้ (tolerance for disruption) และสถานการณ์รุนแรงที่อาจเกิดขึ้น (severe but plausible scenarios)

สถาบันการเงินต้องมีการวิเคราะห์และกำหนด critical operations ให้สอดคล้องกับประเภท ขนาด ความซับซ้อน ตลอดจนความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

ต่อทั้งสถาบันการเงินเอง**และระบบสถาบันการเงิน โดยในแต่ละธุรกรรมสำคัญต้องกำหนดระดับการหยุดชะงักการดำเนินการที่ยอมรับได้ (tolerance for disruption) ที่เป็นรูปธรรมและประเมินผลได้ เพื่อเป็นตัวชี้วัดที่ชัดเจนและเข้าใจตรงกันภายในองค์กร ทั้งนี้ สถาบันการเงินควรคำนึงถึงสถานการณ์รุนแรงที่มีโอกาสเกิดขึ้น (severe but plausible scenarios) ที่อาจส่งผลกระทบต่อการดำเนินการธุรกรรมสำคัญไว้ล่วงหน้า เพื่อลดผลกระทบ หรือความเสียหายหากสถานการณ์ดังกล่าวเกิดขึ้นจริง ทั้งนี้ สถาบันการเงินต้องทบทวนการกำหนดธุรกรรมสำคัญของสถาบันการเงิน ระดับการหยุดชะงักการดำเนินการธุรกรรมสำคัญที่ยอมรับได้ และสถานการณ์รุนแรงที่มีโอกาสเกิดขึ้น เป็นประจำอย่างน้อยปีละ 1 ครั้งเป็นอย่างน้อย หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ**

(3) การระบุสิ่งที่เกี่ยวข้องและเชื่อมโยงกับธุรกรรมสำคัญ (mapping interconnection and independencies)

การดำเนินการธุรกรรมสำคัญของสถาบันการเงินจะมีความเกี่ยวข้องเชื่องโยงกับองค์ประกอบอื่น เช่น บุคลากร ระบบงาน ข้อมูล อุปกรณ์หรือสถานที่ รวมถึงอาจมีการเชื่อมโยงกับผู้ให้บริการภายนอก ดังนั้น ในแต่ละธุรกรรมสำคัญต้องมีการระบุสิ่งที่เกี่ยวข้องเชื่อมโยงอย่างเพียงพอเพื่อระบุถึงความเสี่ยงที่อาจเกิดขึ้น โดยต้องมีการบันทึกและปรับปรุงให้เป็นปัจจุบัน และใช้เป็นส่วนหนึ่งในการเตรียมความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ

(4) การบริหารความเสี่ยงของธุรกรรมสำคัญภายใต้สถานการณ์ไม่ปกติและแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan: BCP)

สถาบันการเงินควรนำเครื่องมือที่สำคัญในการบริหารจัดการความเสี่ยงมาใช้ ได้แก่ ระบบการบริหารความเสี่ยงด้านปฏิบัติการ การบริหารจัดการผู้ให้บริการภายนอก และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan: BCP) ที่เป็นลายลักษณ์อักษร ครอบคลุมทุกธุรกรรมสำคัญตามที่สถาบันการเงินกำหนด โดยต้องกำหนดขั้นตอนการดำเนินการให้มีความชัดเจน และเป็นไปได้ในทางปฏิบัติ รวมถึงครอบคลุมผู้ให้บริการภายนอกที่เกี่ยวข้อง เพื่อบริหารจัดการให้ธุรกรรมสำคัญสามารถดำเนินการได้อย่างต่อเนื่อง หรือกลับมาดำเนินการได้ในเวลาที่เหมาะสม สอดคล้องตามเป้าหมายความเสี่ยงที่สถาบันการเงินยอมรับได้

(5) การทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

สถาบันการเงินต้องจัดให้มีการทดสอบแผน BCP ในการบริหารจัดการความเสี่ยงของธุรกรรมสำคัญในสถานการณ์รุนแรงที่มีโอกาสเกิดขึ้นอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าแผนงาน กระบวนการ และทรัพยากรที่สถาบันการเงินได้กำหนดไว้ตามแผน

มีประสิทธิภาพเพียงพอที่จะทำให้ธุรกรรมสำคัญยังสามารถดำเนินการอย่างต่อเนื่อง หรือกลับมาดำเนินการได้ในเวลาที่เหมาะสม และให้นำผลการทดสอบดังกล่าวไปพัฒนาและจัดทำแผนงานที่มีประสิทธิภาพมากยิ่งขึ้นต่อไป

(6) การบริหารจัดการเพื่อรับมือเหตุการณ์ผิดปกติ (incident management) ภาวะวิกฤต (crisis management) และการสื่อสารในภาวะวิกฤติ

เมื่อเกิดมีสถานการณ์ไม่ปกติ สถาบันการเงินต้องมีการบริหารจัดการเพื่อรับมือและกู้คืนการดำเนินงานได้อย่างเหมาะสมและทันท่วงที ตั้งแต่การกำหนดระดับความรุนแรงของสถานการณ์ไม่ปกติ หน้าที่ความรับผิดชอบ กระบวนการ และแผนงานที่ชัดเจน เพื่อให้พนักงานในองค์กรทราบถึงขั้นตอน บทบาทหน้าที่ การสื่อสารที่จำเป็น และสิ่งที่ต้องดำเนินการ เพื่อกู้คืนการดำเนินงาน และลดผลกระทบจากเหตุการณ์ที่เกิดขึ้นให้ได้มากที่สุด

ทั้งนี้ ธนาคารแห่งประเทศไทยได้จัดทำแนวทางการเตรียมความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (operational resilience framework guideline) เพื่อให้สถาบันการเงินใช้เป็นแนวทางในการจัดทำ operational resilience framework ของสถาบันการเงิน โดยให้สถาบันการเงินพิจารณาปรับใช้อย่างเหมาะสมตามลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อน และความเสี่ยงของแต่ละสถาบันการเงินได้ตามที่กำหนดในเอกสารแนบ 6

5.3.7 การเปิดเผยข้อมูลการบริหารความเสี่ยงด้านปฏิบัติการ

การเปิดเผยข้อมูลเกี่ยวกับการบริหารความเสี่ยงด้านปฏิบัติการสามารถนำไปสู่ความโปร่งใส และส่งเสริมธรรมเนียมการปฏิบัติในระบบสถาบันการเงินให้ดีขึ้นได้ สถาบันการเงินจึงต้องเปิดเผยข้อมูลเกี่ยวกับการบริหารความเสี่ยงด้านปฏิบัติการอย่างเพียงพอที่สาธารณชนรวมทั้งผู้ฝากเงินและผู้มีส่วนได้เสีย จะเข้าใจแนวทางการบริหารความเสี่ยงด้านปฏิบัติการและสามารถประเมินความมีประสิทธิภาพของระบบบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินได้ ความเพียงพอของข้อมูลที่ควรเปิดเผยนั้น ขึ้นอยู่กับขนาด ความซับซ้อนและความเสี่ยงของการดำเนินธุรกิจสถาบันการเงินแต่ละแห่ง **อย่างไรก็ดี ควรกำหนดให้มีความสอดคล้องกับมาตรฐานที่ได้รับการยอมรับโดยทั่วไป (industry practices) ด้วย**

นอกจากนี้ สถาบันการเงินควรเปิดเผยข้อมูลความเสี่ยงด้านปฏิบัติการที่อาจเกิดขึ้น (operational risk exposure) ที่เกี่ยวข้องกับผู้มีส่วนได้เสีย รวมถึงเหตุการณ์ความเสียหายด้านปฏิบัติการที่มีนัยสำคัญ โดยการเปิดเผยข้อมูลดังกล่าวต้องไม่เป็นการเพิ่มความเสี่ยงด้านปฏิบัติการจากการเปิดเผยด้วย (เช่น จุดบกพร่องของการควบคุมความเสี่ยงที่ยังไม่ได้รับการแก้ไข)

ทั้งนี้ ให้สถาบันการเงินจัดทำนโยบายการเปิดเผยข้อมูล (disclosure policy) พร้อมทั้งเปิดเผยข้อมูลความเสี่ยงด้านปฏิบัติการขั้นต่ำตามที่กำหนดไว้ โดยในกรณีของธนาคารพาณิชย์ให้ปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยการเปิดเผยข้อมูลการดำรงเงินกองทุนสำหรับธนาคารพาณิชย์ สำหรับกรณีของบริษัทเงินทุน และบริษัทเครดิตฟองซิเอร์ ให้ปฏิบัติตามที่กำหนดในหลักเกณฑ์ว่าด้วยการกำกับดูแลด้านเงินกองทุนและการดำรงสินทรัพย์สภาพคล่องสำหรับบริษัทเงินทุน และบริษัทเครดิตฟองซิเอร์

5.4 กรอบการบริหารความเสี่ยงด้านปฏิบัติการ (operational risk management framework: ORMF) ของกลุ่มธุรกิจทางการเงิน

เพื่อให้การบริหารความเสี่ยงด้านปฏิบัติการเป็นไปในทิศทางเดียวกันทั้งกลุ่มธุรกิจทางการเงิน ให้บริษัทแม่ของกลุ่มธุรกิจทางการเงินรับผิดชอบในการจัดให้มีนโยบายในภาพรวมที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการของกลุ่มธุรกิจ **โดยให้นำหลักเกณฑ์ตามข้อ 5.3 มาใช้บังคับโดยอนุโลม โดยในเรื่องการเปิดเผยข้อมูลความเสี่ยงด้านปฏิบัติการข้อ 5.3.7 ในส่วนของการจัดทำนโยบายการเปิดเผยข้อมูลและการเปิดเผยข้อมูลความเสี่ยงด้านปฏิบัติการขั้นต่ำให้ถือปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยการเปิดเผยข้อมูลการดำรงเงินกองทุนของกลุ่มธุรกิจทางการเงิน** ทั้งนี้ บริษัทแม่ของกลุ่มธุรกิจทางการเงินอาจมอบหมายให้คณะกรรมการบริษัทในกลุ่มธุรกิจทางการเงิน **กำหนดนโยบายของตนเองได้ โดยนโยบายดังกล่าวต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงด้านปฏิบัติการของกลุ่มธุรกิจทางการเงินในภาพรวมที่บริษัทแม่กำหนด**

6. วันเริ่มต้นบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

7. กำหนดการรับฟังความคิดเห็น

ธนาคารแห่งประเทศไทยเปิดฟังรับความคิดเห็นและข้อเสนอแนะต่อร่างหลักเกณฑ์การบริหารความเสี่ยงด้านปฏิบัติการของสถาบันการเงินและกลุ่มธุรกิจทางการเงิน ตั้งแต่วันที่ 20 ธันวาคม 2565 จนถึงวันที่ 23 มกราคม 2566

ทั้งนี้ หากท่านมีความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม โปรดส่งแบบแสดงความคิดเห็นกลับมายังงานนโยบายด้านปฏิบัติการ ผ่านทาง Email: FIOP-RPD2@bot.or.th

ผู้ประสานงาน:
งานนโยบายด้านปฏิบัติการ
ฝ่ายนโยบายและกำกับสถาบันการเงิน 2
สายนโยบายสถาบันการเงิน
โทรศัพท์ 0 2283 5806, 0 2283 6988

เอกสารแนบ 1

แนวปฏิบัติ ประกาศ และหนังสือเวียนที่ยกเลิก

1. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการ ลงวันที่ 3 สิงหาคม 2551

2. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของสถาบันการเงิน ลงวันที่ 3 สิงหาคม 2551

3. แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับกรณีการระบาดของโรคติดต่อร้ายแรง ลงวันที่ 3 สิงหาคม 2551

4. ความในข้อ 5.7.1 ของประกาศธนาคารแห่งประเทศไทยที่ สนส. 12/2561 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงของกลุ่มธุรกิจทางการเงิน ลงวันที่ 22 พฤษภาคม 2561

5. ความในข้อ 2.2 และ ข้อ 2.3 ของหนังสือธนาคารแห่งประเทศไทยที่ ธปท.ฝนส.(21) ว. 185/2560 เรื่อง หลักเกณฑ์การกำกับดูแลสำหรับบริษัทเครดิตฟองซิเอร์ ลงวันที่ 1 กุมภาพันธ์ 2560

6. ความในข้อ 2 ของหนังสือธนาคารแห่งประเทศไทยที่ ธปท.ฝนส.(21)ว. 186/2560 เรื่อง หลักเกณฑ์การกำกับดูแลสำหรับบริษัทเงินทุน ลงวันที่ 1 กุมภาพันธ์ 2560

เอกสารแนบ 2

นโยบายการบริหารความเสี่ยงด้านปฏิบัติการ

นโยบายในการบริหารความเสี่ยงด้านปฏิบัติการต้องมีข้อมูลอย่างน้อย ดังนี้

1. นิยามของความเสี่ยงด้านปฏิบัติการ และความเสียหายด้านปฏิบัติการขององค์กร เพื่อใช้ประกอบการระบุ ประเมิน ติดตาม และรายงานความเสี่ยงด้านปฏิบัติการที่เกิดขึ้นในองค์กร โดยอาจจัดทำเป็น taxonomy เพื่อใช้อ้างอิงในการบริหารความเสี่ยงให้สอดคล้องกันทั่วทั้งองค์กร ทั้งนี้ taxonomy ดังกล่าว อาจจำแนกตามประเภทเหตุการณ์ความเสียหาย สาเหตุ ความมีนัยสำคัญ และหน่วยธุรกิจที่เกิดเหตุความเสียหาย ซึ่งอย่างน้อยต้องจำแนกตามประเภทเหตุการณ์ความเสียหาย 7 ประเภท ตามตัวอย่างการจัดทำ taxonomy ที่ ธปท. กำหนดในตารางที่ 1

2. กำหนด operational risk appetite and risk tolerance, thresholds, จุดชี้วัด (trigger) หรือเพดานความเสี่ยง (limit) ที่เกี่ยวเนื่องกับความเสี่ยงด้านปฏิบัติการของกิจกรรมที่มีนัยสำคัญ (เช่น ความเสี่ยงก่อนมีการควบคุม) ความเสี่ยงด้านปฏิบัติการคงเหลือภายหลังมีการควบคุมแล้ว (residual operational risk) กลยุทธ์และเครื่องมือในการบรรเทาความเสี่ยง ทั้งนี้ risk appetite และ tolerance statement ที่มีประสิทธิภาพควรมีลักษณะ ดังนี้

2.1 สื่อความได้ง่าย และผู้มีส่วนได้เสียทุกคนสามารถเข้าใจได้

2.2 คำนึงถึงข้อมูลและสมมติฐานสำคัญที่สะท้อนถึงแผนธุรกิจที่ได้รับอนุมัติแล้ว

2.3 กำหนดประเภทความเสี่ยงที่องค์กรยอมรับได้ หรือความเสี่ยงที่ต้องหลีกเลี่ยง รวมทั้งกำหนดขอบเขตหรือตัวชี้วัด (อาจเป็นเชิงปริมาณ) ที่ใช้ติดตามความเสี่ยงดังกล่าว

2.4 เป็นส่วนหนึ่งในการผลักดันให้กลยุทธ์ โดยเพดานความเสี่ยง (risk limit) ของหน่วยธุรกิจ (business unit) ต้องสอดคล้องกับรูปแบบข้อกำหนดของระดับความเสี่ยงที่ยอมรับได้ (risk appetite statement) ในระดับองค์กร

2.5 มีลักษณะมองไปข้างหน้า (forward-looking) และเหมาะสมในทางปฏิบัติ ซึ่งขึ้นอยู่กับการทดสอบภายใต้ภาวะวิกฤต (scenario and stress testing) เพื่อให้มั่นใจได้ว่าองค์กรสามารถระบุได้ว่าเหตุการณ์ใดที่อาจผลักดันให้เกินกว่าระดับ risk appetite และ tolerance statement

3. โครงสร้างการกำกับดูแล ซึ่งระบุบทบาทหน้าที่ความรับผิดชอบในการบริหารความเสี่ยงด้านปฏิบัติการ และสายการบังคับบัญชาของคณะกรรมการสถาบันการเงิน คณะกรรมการชุดย่อย ผู้บริหารระดับสูง หน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการ (three lines of defense)

4. เครื่องมือสำหรับการระบุ ประเมิน และควบคุมความเสี่ยง รวมถึงบทบาทหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการ ในการใช้เครื่องมือดังกล่าว

5. วิธีการกำหนดและติดตาม thresholds หรือ เพดานความเสี่ยง (limit) ของความเสี่ยงเกี่ยวเนื่องและความเสี่ยงคงเหลือ (residual risk) และวิธีการที่ทำให้มั่นใจว่ามีการควบคุมความเสี่ยงและนำไปถือปฏิบัติได้อย่างมีประสิทธิภาพ

6. ประเภทความเสี่ยงที่กระทบต่อเป้าหมายการทำงานของหน่วยงาน (inventory risks) และวิธีการควบคุมโดยหน่วยธุรกิจ

7. โครงหรือลำดับของการจัดทำรายงานการบริหารจัดการความเสี่ยง เพื่อให้มีการจัดทำรายงานด้วยข้อมูลที่ถูกต้อง ในจังหวะเวลาที่เหมาะสม รวมถึงประเภทของข้อมูลที่ควรระบุในการรายงานการบริหารความเสี่ยง

8. กลไกในการให้ความเห็น สอบทานอย่างเป็นอิสระ และการให้ข้อสังเกต หรือหยิบยกประเด็นจากกระบวนการบริหารความเสี่ยงด้านปฏิบัติการที่เกิดขึ้น

9. ข้อกำหนด หรือเงื่อนไขที่ใช้ทบทวน หรือสอบทานความเหมาะสมของนโยบาย ซึ่งขึ้นอยู่กับการประเมินคุณภาพของการควบคุมที่ใช้ตอบสนองการเปลี่ยนแปลงทั้งจากภายในและภายนอก หรือการเปลี่ยนแปลงที่มีนัยสำคัญต่อความเสี่ยงด้านปฏิบัติการโดยรวม

ทั้งนี้ นโยบายดังกล่าวต้องรองรับกระบวนการที่ใช้ในการบริหารความเสี่ยงด้านปฏิบัติการที่มีลักษณะเฉพาะได้ด้วย เช่น การอนุมัติลูกค้าใหม่ การอนุมัติผลิตภัณฑ์ใหม่ การอนุมัติระบบงานใหม่ การใช้บริการจากภายนอก แผนการดำเนินงานต่อเนื่อง แผนการบริหารจัดการวิกฤติ นอกจากนี้ การบริหารจัดการความเสี่ยงในระดับหน่วยธุรกิจอาจมีการกำหนดนโยบายเพิ่มเติม หรือกระบวนการบางอย่างเป็นการเฉพาะสำหรับการบริหารความเสี่ยงที่มีลักษณะเฉพาะในหน่วยงานนั้น โดยยังต้องสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงด้านปฏิบัติในระดับองค์กร

ตารางที่ 1 แนวทางการจัดทำชุดนิยามของความเสี่ยงด้านปฏิบัติการ (operational risk taxonomy)

การพัฒนานิยาม และการจัดหมวดหมู่ของเหตุการณ์หรือกิจกรรมที่เกี่ยวข้องกับความเสี่ยงด้านปฏิบัติการไว้เป็นชุดข้อมูลเพื่อใช้อ้างอิงเป็นแนวทางในการบริหารจัดการ (เช่น ระบุ ประเมิน ติดตาม และรายงานความเสี่ยงด้านปฏิบัติการ) เป็นการสนับสนุนให้องค์กรมีการบริหารความเสี่ยงไปในทิศทางเดียวกัน มีความสอดคล้องกันต่อเนื่องทั้งกระบวนการ เพื่อผลักดันสู่เป้าหมายที่องค์กรกำหนดไว้ ทั้งนี้ สถาบันการเงินอาจพิจารณาจัดหมวดหมู่นิยามของความเสี่ยงด้านปฏิบัติการได้ตามความเหมาะสม โดยต้องเทียบเคียงได้กับประเภทเหตุการณ์ความเสียหาย (loss event type) ตามที่ Basel Committee on Banking Supervision (BCBS) กำหนดไว้ 7 ประเภท ตัวอย่างเช่น

ประเภทเหตุการณ์ความเสียหาย	นิยาม	ชนิดของประเภทเหตุการณ์ความเสียหาย	ตัวอย่างเหตุการณ์ที่ทำให้เกิดความเสียหาย
1. การทุจริตหรือการฉ้อโกงโดยบุคคลภายในองค์กร (internal fraud)	ความเสียหายที่เกิดจากการฉ้อโกง ยักยอกสินทรัพย์ หรือหลีกเลี่ยงข้อบังคับกฎหมาย หรือ นโยบายขององค์กร ซึ่งกระทำโดยบุคคลภายในองค์กร	การละเว้นการปฏิบัติงานหรือการดำเนินการโดยไม่ได้รับอนุญาต	- การตั้งใจไม่รายงานการทำธุรกรรมต่าง ๆ - การดำเนินการที่นอกเหนือจากหน้าที่ความรับผิดชอบโดยเจตนา
		การโจรกรรมและการทุจริต	- การทุจริต / การโจรกรรมเงินฝาก หรือทรัพย์สิน / การยักยอก / การลักทรัพย์ - การใช้ทรัพย์สินขององค์กรไปในทางไม่เหมาะสม - การทำลายทรัพย์สินโดยเจตนา - การปลอมแปลงเอกสาร - การปลอมเช็ค - การลักลอบขนย้ายทรัพย์สินขององค์กร - การลงบัญชีที่ไม่ปฏิบัติตามหลักการด้านภาษี - การติดสินบน / การรับสินบน

ประเภทเหตุการณ์ความเสียหาย	นิยาม	ชนิดของประเภทเหตุการณ์ความเสียหาย	ตัวอย่างเหตุการณ์ที่ทำให้เกิดความเสียหาย
			- การใช้ข้อมูลภายในเพื่อแสวงหาผลประโยชน์จากการซื้อขายหลักทรัพย์ (insider trading)
2. การทุจริตหรือการฉ้อโกงโดยบุคคลภายนอกองค์กร (external fraud)	ความเสียหายที่เกิดจากการฉ้อโกง ยักยอกสินทรัพย์ หรือหลีกเลี่ยงการปฏิบัติตามกฎหมาย ซึ่งกระทำโดยบุคคลภายนอก	การโจรกรรม และการทุจริต	- การโจรกรรมทรัพย์สิน / การลักทรัพย์ - การปลอมแปลงเอกสาร - การปลอมเช็ค
		ระบบรักษาความปลอดภัย	- ความเสียหายที่เกิดจากการลักลอบเจาะเข้าระบบโปรแกรมคอมพิวเตอร์ขององค์กร - การโจรกรรมข้อมูล
3. การจ้างงานและความปลอดภัยในสถานที่ทำงาน (employment practices and workplace safety)	ความเสียหายที่เกิดจากการกระทำที่ไม่เป็นไปตามกฎหมายการจ้างงาน หรือหลักเกณฑ์ด้านความปลอดภัยในที่ทำงาน หรือ ข้อตกลงอันเกี่ยวกับการจ้างงาน	การบริหารทรัพยากรบุคคล	- การถูกฟ้องร้องจากการกระทำผิดกฎหมายแรงงาน - การจัดสรรทรัพยากรบุคคลกับงานที่ไม่เหมาะสม
		สภาพแวดล้อมในสถานที่ทำงานที่ปลอดภัย	- การถูกฟ้องร้องจากการกระทำผิดกฎหมายเกี่ยวกับความปลอดภัยของสถานที่ทำงาน - ความรับผิดต่ออุบัติเหตุที่เกิดจากการจัดสถานที่ทำงานไม่เหมาะสม ซึ่งทำให้เกิดอุบัติเหตุต่อพนักงาน
4. ลูกค้า ผลิตภัณฑ์ และแนวทางการดำเนินธุรกิจ (clients, products and business practices)	ความเสียหายอันเกิดจากข้อบกพร่องหรือการละเลยไม่ปฏิบัติตามวิชาชีพอันพึงมีกับลูกค้า และออกแบบหรือเสนอผลิตภัณฑ์ต่อลูกค้าที่ไม่เหมาะสม	การปฏิบัติต่อลูกค้าที่ไม่เหมาะสม	- การฝ่าฝืนโดยการเปิดเผยข้อมูลของลูกค้า - การละเมิดความเป็นส่วนตัวของลูกค้า - การนำข้อมูลที่เป็นความลับไปใช้ในทางที่ผิด
		แนวทางการดำเนินธุรกิจที่ไม่เหมาะสม	- กระบวนการซื้อขายที่ไม่เหมาะสม - การสร้างราคาหลักทรัพย์ หรือการปั่นหุ้น - การดำเนินงานต่าง ๆ โดยไม่มีใบอนุญาต - การที่ลูกค้าใช้สถาบันการเงินเป็นช่องทางของการฟอกเงิน

ประเภทเหตุการณ์ความเสียหาย	นิยาม	ชนิดของประเภทเหตุการณ์ความเสียหาย	ตัวอย่างเหตุการณ์ที่ทำให้เกิดความเสียหาย
		ข้อบกพร่องของผลิตภัณฑ์การเงิน	- การออกแบบผลิตภัณฑ์ทางการเงินที่มีข้อผิดพลาด
		การประเมินความเสี่ยง	- ความล้มเหลวในการตรวจสอบข้อมูลลูกค้าตามเกณฑ์การตรวจสอบ - ลูกค้ามีระดับความเสี่ยงสูงเกินกว่าที่กำหนดไว้
5. ความเสียหายต่อทรัพย์สินขององค์กร (damage to physical assets)	ความสูญเสียที่เกิดขึ้นจากภัยพิบัติทางธรรมชาติหรืออุบัติการณ์อื่นๆ	ภัยพิบัติทางธรรมชาติหรืออุบัติการณ์อื่นๆ	- ความเสียหายจากภัยพิบัติทางธรรมชาติ - ความเสียหายจากการก่อการร้าย
6. การหยุดชะงักของธุรกิจ และความขัดข้องของระบบที่สนับสนุนการปฏิบัติงาน (business disruption and system failure)	ความสูญเสียที่เกิดขึ้นจากการหยุดชะงักของธุรกิจและความขัดข้องของระบบงาน เช่น ระบบ IT ระบบสาธารณูปโภค ที่ทำให้ไม่สามารถปฏิบัติงานได้	ระบบงาน	- การหยุดชะงักของฮาร์ดแวร์ - การที่ซอฟท์แวร์ไม่สามารถใช้การได้ - ความเสียหายของการสื่อสารโทรคมนาคม - ระบบสาธารณูปโภคเกิดเหตุขัดข้อง หรือหยุดชะงัก
7. การปฏิบัติงาน การส่งมอบงานและการบริหารกระบวนการทำงาน (execution, delivery and process management)	ความเสียหายที่เกิดจากการดำเนินการหรือการปฏิบัติงานที่ล้มเหลว	การปฏิบัติงานที่ไม่เป็นไปตามกระบวนการที่กำหนด	- เหตุการณ์การดำเนินงานที่ผิดพลาด หรือไม่ถูกต้อง เช่น การสื่อสารที่ผิดพลาด การนำเข้าข้อมูลที่ไม่ถูกต้อง การส่งมอบงานล่าช้ากว่ากำหนด ความผิดพลาดในรายการบัญชี การเก็บรักษาข้อมูลไม่ถูกต้อง
		การรายงาน	- การรายงานต่างๆ เช่น รายงานข้อมูลความเสียหายที่เกิดขึ้น (loss data) ที่ไม่ถูกต้อง

ประเภทเหตุการณ์ความเสียหาย	นิยาม	ชนิดของประเภทเหตุการณ์ความเสียหาย	ตัวอย่างเหตุการณ์ที่ทำให้เกิดความเสียหาย
		การบริหารจัดการข้อมูล เอกสาร และบัญชีลูกค้า	- การดำเนินการโดยไม่ได้รับความยินยอมจากลูกค้า - เอกสารทางกฎหมายสูญหาย/ขาดความสมบูรณ์ - การเข้าถึงข้อมูลโดยมิได้รับอนุญาต - การบันทึกข้อมูลของลูกค้าผิดพลาด - ความเสียหายต่อทรัพย์สินของลูกค้าที่เกิดจากความประมาทขององค์กร
		การทำธุรกรรมกับคู่ค้าทางธุรกิจ	- ความเสียหายจากการดำเนินงานของคู่ค้า หรือจากการใช้บริการจากบุคคลภายนอก - การเกิดข้อพิพาทต่างๆ กับคู่ค้า และผู้ให้บริการภายนอก

หมายเหตุ: ตัวอย่างการจำแนกประเภทของเหตุการณ์ความเสียหายของความเสี่ยงด้านปฏิบัติข้างต้นอ้างอิงมาจาก operational risk data collection exercise โดย Basel Committee on Banking Supervision

เอกสารแนบ 3

บทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการ (three lines of defense)

สถาบันการเงินต้องมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่างหน่วยงานหรือผู้ที่ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (business unit หรือ first line of defense) หน่วยงานกำกับภายใน (second line of defense) และหน่วยงานตรวจสอบภายใน (internal audit หรือ third line of defense) ดังนี้

1. หน่วยงานที่ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (first line of defense) เช่น หน่วยธุรกิจ (business unit) ซึ่งรับผิดชอบการปฏิบัติงานประจำวัน (day-to-day basis) ถือเป็นแนวป้องกันความเสี่ยงชั้นแรก โดยหน่วยธุรกิจควรดำเนินการ ดังต่อไปนี้ เพื่อให้การปฏิบัติตาม ORMF ในแต่ละหน่วยธุรกิจสะท้อนถึงขอบเขตการดำเนินงานของหน่วยธุรกิจ และความเสี่ยงด้านปฏิบัติการที่เกี่ยวข้อง

1.1 ระบุและประเมินความเสี่ยงด้านปฏิบัติการที่มีนัยสำคัญที่เกี่ยวเนื่องกับหน่วยธุรกิจโดยใช้วิธีการหรือเครื่องมือในการบริหารจัดการความเสี่ยงด้านปฏิบัติการ

1.2 กำหนดแนวทางการควบคุมเพื่อบรรเทาความเสี่ยงด้านปฏิบัติการที่เกี่ยวเนื่องกับการดำเนินงาน รวมถึงกำหนดกระบวนการ ขั้นตอน และระบบงาน และมีการประเมินประสิทธิภาพของการควบคุมความเสี่ยงจากการใช้เครื่องมือต่างๆ ในการบริหารความเสี่ยงด้านปฏิบัติการ

1.3 รายงานการขาดแคลนทรัพยากร เครื่องมือ และการอบรมความรู้ที่ไม่เพียงพอสำหรับการระบุและประเมินความเสี่ยงด้านปฏิบัติการของหน่วยธุรกิจ

1.4 ติดตามและรายงานความเสี่ยงด้านปฏิบัติการของหน่วยธุรกิจตาม operational risk appetite และ tolerance statement

1.5 รายงานความเสี่ยงด้านปฏิบัติการส่วนที่ไม่สามารถลดความเสี่ยงได้โดยการควบคุม เหตุการณ์ความเสียหายด้านปฏิบัติการ ความบกพร่องในการควบคุม กระบวนการที่ไม่เพียงพอ และส่วนที่ไม่สามารถปฏิบัติตาม operational risk tolerance ได้

ทั้งนี้ แนวทางในการบริหารความเสี่ยงด้านปฏิบัติการที่เหมาะสมของหน่วยธุรกิจควรกำหนดให้พนักงานตระหนักถึงความเสี่ยงด้านดังกล่าวในหน่วยธุรกิจนั้น และมีการรายงานในเรื่องต่าง ๆ ควบคู่กันทั้งการรายงานตรงต่อสายการบังคับบัญชา และการรายงานต่อหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์

2. หน่วยงานกำกับภายใน (second line of defense) เช่น หน่วยงานบริหารความเสี่ยง (risk management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (compliance) มีบทบาทสำคัญในการสนับสนุนการทำงานของผู้บริหารระดับสูงในการบริหารจัดการความเสี่ยงด้านปฏิบัติการ และมีหน้าที่ในการส่งเสริมและสนับสนุนการปฏิบัติตามนโยบาย กระบวนการ ขั้นตอนของความเสี่ยงด้านปฏิบัติการในองค์กร **ทั้งนี้ หน่วยงานกำกับภายในของสถาบันการเงินต้องสามารถปฏิบัติหน้าที่ได้อย่างเป็นอิสระ โดยควรรายงานไปยังคณะกรรมการในระดับกำกับดูแล เช่น คณะกรรมการสถาบันการเงิน หรือคณะกรรมการกำกับความเสี่ยง หรือคณะกรรมการชุดอื่นที่มีองค์ประกอบเป็นกรรมการสถาบันการเงิน นอกเหนือจากการรายงานต่อผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงิน**

2.1 หน่วยงานบริหารความเสี่ยง (risk management function) ควรดำเนินการดังต่อไปนี้

2.1.1 พัฒนาและดูแลให้มีนโยบาย กระบวนการ และแนวปฏิบัติในระดับองค์กร (corporate-level) สำหรับการบริหารจัดการและการควบคุมความเสี่ยงด้านปฏิบัติการ

2.1.2 เสนอนโยบาย แผนงาน และกระบวนการบริหาร ความเสี่ยงด้านปฏิบัติการต่อคณะกรรมการสถาบันการเงิน **หรือคณะกรรมการที่เกี่ยวข้องเพื่อพิจารณาอนุมัติ**

2.1.3 กำหนดและนำเครื่องมือในการประเมินความเสี่ยงด้านปฏิบัติการ และระบบการจัดเก็บข้อมูลและรายงานความเสี่ยงด้านปฏิบัติการ**ไปใช้ในทางปฏิบัติ**

2.1.4 ให้ความเห็นอย่างเป็นอิสระจากหน่วยธุรกิจในเรื่องการระบุความเสี่ยงด้านปฏิบัติการที่มีนัยสำคัญ การออกแบบและประสิทธิภาพของการควบคุม และ risk tolerance รวมถึงให้ข้อสังเกตเกี่ยวกับการใช้เครื่องมือในการบริหารความเสี่ยงด้านปฏิบัติการโดยหน่วยธุรกิจ

2.1.5 รายงานเกี่ยวกับระบบงาน และรวบรวมข้อมูลหลักฐานที่ใช้ประกอบข้อสังเกตจากการประเมินความมีประสิทธิภาพของระบบงาน

2.1.6 ดูแลความสอดคล้องของการจัดประเภท วิธีการ และขั้นตอนของความเสี่ยงด้านปฏิบัติการ

2.1.7 ทบทวนและจัดทำรายงานการติดตามความเสี่ยงด้านปฏิบัติการนำเสนอต่อคณะกรรมการสถาบันการเงิน หรือคณะกรรมการที่เกี่ยวข้อง

2.1.8 **ดำเนินงานร่วมกับ**หน่วยงานที่เกี่ยวข้อง**เพื่อบริหารจัดการความเสี่ยงใด ๆ ที่ส่งผลกระทบต่อธุรกรรมสำคัญ (critical operations)** บริหารจัดการแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan) **การบริหารจัดการผู้ให้บริการภายนอก (third party dependency management) และการเตรียมแผนล่วงหน้ารองรับการเสริมสร้างความมั่นคงและ**

แก้ไขปัญหา (recovery planning) รวมถึงกรอบการบริหารความเสี่ยงด้านอื่นที่เกี่ยวข้อง เพื่อส่งเสริมให้องค์กรมีความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (operational resilience)

2.1.9 กำหนดและจัดให้มีการอบรมความรู้การบริหารจัดการความเสี่ยงด้านปฏิบัติการ รวมถึงปลูกฝังการตระหนักรู้ถึงความเสี่ยง และให้คำแนะนำในการบริหารความเสี่ยงด้านปฏิบัติการแก่หน่วยธุรกิจ เช่น การใช้เครื่องมือการบริหารความเสี่ยงด้านปฏิบัติการ

2.1.10 ประสานงานกับหน่วยงานต่าง ๆ เพื่อประโยชน์ในการบริหารจัดการความเสี่ยงด้านปฏิบัติการ

2.2 หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (compliance function) บทบาทหน้าที่ของหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ และการบริหารความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ (compliance risk management) ให้ถือปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับการปฏิบัติตามกฎเกณฑ์ (compliance) ของสถาบันการเงิน และกลุ่มธุรกิจทางการเงิน

3. หน่วยงานตรวจสอบภายใน (third line of defense) เป็นหน่วยงานที่มีบทบาทสำคัญในการตรวจสอบประเมินประสิทธิภาพและประสิทธิผลของการดำเนินงานและระบบการควบคุมภายใน **จึงต้องทำหน้าที่ได้อย่างเป็นอิสระเพื่อความเชื่อมั่น (independent assurance)** โดยต้องไม่มีส่วนเกี่ยวข้องกับการกำหนดการปฏิบัติงานด้านการบริหารความเสี่ยงด้านปฏิบัติการ หรือไม่เกี่ยวข้องกับหน่วยธุรกิจ และหน่วยงานกำกับภายใน **นอกจากนี้ หน่วยงานตรวจสอบภายในต้องมีการรายงานตรงต่อคณะกรรมการตรวจสอบ หรือสามารถรายงานเพิ่มเติมต่อคณะกรรมการสถาบันการเงินได้ด้วย ทั้งนี้ ให้ถือปฏิบัติตามหลักเกณฑ์ธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การปฏิบัติงานตรวจสอบภายใน (internal audit) ของสถาบันการเงิน และกลุ่มธุรกิจทางการเงิน**

เอกสารแนบ 4

ระบบบริหารความเสี่ยงด้านปฏิบัติการ

กระบวนการบริหารความเสี่ยงด้านปฏิบัติการประกอบด้วย 3 ขั้นตอนสำคัญ ดังนี้

1. การระบุความเสี่ยง (risk identification) และการประเมินความเสี่ยง (risk assessment)

สถาบันการเงินต้องมีการระบุและประเมินความเสี่ยงอย่างต่อเนื่อง และทบทวนความเหมาะสมเป็นระยะ เนื่องจากเป็นพื้นฐานสำคัญของการบริหารความเสี่ยง **ซึ่งจะช่วยในการกำหนดทรัพยากรในการบริหารความเสี่ยงด้านปฏิบัติการได้อย่างมีประสิทธิภาพ รวมถึงเป็นการสนับสนุนให้สถาบันการเงินมีความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (operational resilience) ด้วย** โดยในการระบุประเภทของความเสี่ยงด้านปฏิบัติการ และประเมินความเสี่ยง**ต้องครอบคลุมความเสี่ยงที่เกี่ยวเนื่องกับผลิตภัณฑ์ กิจกรรมการดำเนินงาน กระบวนการและระบบงาน ทั้งที่มีอยู่ในปัจจุบัน และที่จะเกิดขึ้นใหม่ ซึ่งขึ้นอยู่กับนิยามและการจัดประเภทความเสี่ยงด้านปฏิบัติการที่กำหนดไว้** ทั้งนี้ สถาบันการเงินควรพิจารณาปัจจัยดังต่อไปนี้ประกอบการระบุความเสี่ยง

1.1 ประสิทธิภาพของระบบการควบคุมภายใน วัฒนธรรมองค์กรในการบริหารความเสี่ยงด้านปฏิบัติการ แนวทางบริหารจัดการทรัพยากรบุคคล ความพร้อมของบุคลากรและทรัพยากรที่ใช้ในการปฏิบัติงาน

1.2 **ลักษณะของลูกค้า ผลิตภัณฑ์** ปริมาณ ความซับซ้อน และประเภทของธุรกรรม ซึ่งรวมถึงระบบที่เกี่ยวข้องในการให้บริการลูกค้า (end-to-end operating cycle) และกลไกการกระจายผลิตภัณฑ์และบริการสู่ลูกค้าของสถาบันการเงิน (distribution mechanism)

1.3 เหตุการณ์ความเสียหายที่เกิดขึ้นในอดีต หรือเหตุการณ์ที่จะเกิดขึ้นแต่ธนาคารพาณิชย์สามารถป้องกันความเสียหายไว้ได้ (near-misses)

1.4 เหตุการณ์ความเสียหายที่เกิดขึ้นกับสถาบันการเงินแห่งอื่น

1.5 **การเปลี่ยนแปลงของสภาพแวดล้อมการดำเนินงาน แนวโน้มอุตสาหกรรม รวมถึง** การเปลี่ยนแปลงของเทคโนโลยี การออกผลิตภัณฑ์ใหม่ การเปลี่ยนแปลงทางกฎหมาย สังคม การเมือง และเศรษฐกิจ เป็นต้น

นอกจากนี้ สถาบันการเงินควรมีเครื่องมือที่ได้รับการพัฒนาขึ้นเพื่อช่วยในการระบุและประเมินความเสี่ยงด้านปฏิบัติการ เช่**น event management, operational risk event data**, self assessment, **control monitoring and assurance framework, metrics**, scenario analysis และ benchmarking and comparative analyses เป็นต้น **(รายละเอียดตามตารางที่ 1)**

โดยให้พิจารณาเลือกใช้เครื่องมือที่ทำให้มั่นใจว่าผลลัพธ์ที่ได้จากเครื่องมือนั้น มีการประมวลผลมาจากข้อมูลที่ถูกต้องแม่นยำ ซึ่งต้องมีกระบวนการในการตรวจสอบและพิสูจน์ความถูกต้อง (verification and validation procedures) ที่เข้มแข็ง ได้นำมาเป็นส่วนหนึ่งของกระบวนการกำหนดราคาภายใน (internal pricing) กลไกการวัดผลการปฏิบัติ และการประเมินโอกาสทางธุรกิจด้วย รวมถึงเป็นไปตามแผนการติดตามดูแลของหน่วยงานกำกับภายใน หรือแผนการแก้ไขปัญหา (remediation plans) ในกรณีที่จำเป็น

ทั้งนี้ สถาบันการเงินสามารถนำเครื่องมือในการประเมินความเสี่ยงด้านปฏิบัติการไปประกอบการจัดทำแนวทางการเตรียมความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (operational resilience framework) ได้ โดยเฉพาะ event management, self assessment, scenario analysis ซึ่งช่วยในการระบุและติดตามดูแลจุดอ่อน หรือช่องโหว่ของธุรกรรมสำคัญ (critical operations)

2. การควบคุม (risk control) และลดความเสี่ยง (risk mitigation)

ระบบการควบคุมภายในที่มีประสิทธิภาพเป็นกลไกสำคัญในการควบคุมและป้องกันความเสียหายที่อาจเกิดขึ้นได้ **และให้ความมั่นใจได้ว่า การดำเนินงานขององค์กรมีประสิทธิภาพ มีการดูแลรักษาทรัพยากรขององค์กร มีการรายงานทางการเงินที่น่าเชื่อถือ และมีการปฏิบัติตามกฎหมายและหลักเกณฑ์ ซึ่งจะช่วยลดการเกิดข้อผิดพลาดสำคัญที่อาจเกิดจากบุคลากร ระบบหรือกระบวนการภายในที่ผิดปกติ และช่วยให้มีการตรวจหาข้อผิดพลาดได้อย่างทันท่วงที**

เมื่อระบุความเสี่ยงด้านปฏิบัติการที่สำคัญได้แล้ว สถาบันการเงินต้องดำเนินการให้มีนโยบายและกระบวนการเพื่อลดความเสี่ยงอย่างชัดเจน พร้อมแนวทางในการดำเนินการที่เหมาะสม เช่น กรณีที่ความเสี่ยงสูงเกินระดับที่กำหนดไว้ หน่วยงานต้องจัดให้มีการลดความเสี่ยง ด้วยการเพิ่มการควบคุม หรือลดปริมาณธุรกรรมที่ทำลง ถ้าความเสี่ยงมีสูงเกินกว่าระดับที่ยอมรับได้ สถาบันการเงินอาจตัดสินใจหยุดการทำธุรกรรมนั้น **หรือถ่ายโอนความเสี่ยง**ด้วยการทำประกันภัย (เป็นเพียงการลดความเสียหายที่อาจเกิดขึ้นเท่านั้น ไม่ใช่การลดโอกาสที่เหตุการณ์ความเสียหายจะเกิดขึ้น **และต้องทบทวนแผนการจัดการความเสี่ยงโดยการประกันภัยทุกปีด้วย)** และหากเป็นการทำประกันภัยกับบริษัทประกันภัยภายในกลุ่มธุรกิจทางการเงิน สถาบันการเงินควรดำเนินการให้มั่นใจว่ามีการถ่ายโอนความเสี่ยงออกจากกลุ่มจนอยู่ในระดับที่ยอมรับได้แล้ว

2.1 การกำหนดแนวทางการควบคุมภายในที่เหมาะสม

เพื่อให้การควบคุมภายในมีแนวทางที่เหมาะสมและเป็นรูปธรรม สถาบันการเงินต้องดำเนินการ ดังนี้

2.1.1 มีการกำหนดกระบวนการพิจารณา **และขั้นตอนการอนุมัติ** หรือมอบหมายอำนาจให้ชัดเจน

2.1.2 มีการแบ่งแยกหน้าที่ **เพื่อหลีกเลี่ยง หรือลดโอกาสที่จะเกิด**การขัดแย้งด้านผลประโยชน์ (conflict of interest) กับหน้าที่ความรับผิดชอบของบุคคล (ซึ่งอาจทำให้มีพฤติกรรมที่ไม่เหมาะสม หรือปกปิดความเสียหาย ข้อผิดพลาดได้) **ทั้งนี้ หากไม่สามารถหลีกเลี่ยง หรือขจัดความขัดแย้งด้านผลประโยชน์ได้** ควรมีระบบการปฏิบัติงานโดย 2 ฝ่าย (dual control) **ที่ดำเนินงานโดยบุคคลหรือฝ่ายงานมากกว่า 2 ฝ่ายขึ้นไปแยกกัน เพื่อป้องกันการใช้ข้อมูลอ่อนไหว หรือกำหนดมาตรการตั้งรับอื่นในการติดตามดูแลที่เป็นอิสระ และการตรวจทานเพื่อป้องกันผลเสียหายหรือข้อผิดพลาดหรือการปฏิบัติที่ไม่เหมาะสม**

2.1.3 มีการติดตามดูแลตามเพดานความเสี่ยง (risk limit) หรือ threshold ที่กำหนด และตรวจหาการละเมิดระดับดังกล่าว

2.1.4 มีการป้องกันการเข้าถึงหรือเข้าใช้ทรัพย์สินและข้อมูลขององค์กร

2.1.5 มีการกำหนดระดับพนักงาน และมีการอบรมทักษะ ความเชี่ยวชาญให้เหมาะสมต่อการปฏิบัติงาน

2.1.6 มีกระบวนการในการระบุผลลัพธ์ของการดำเนินงาน หรือผลิตภัณฑ์ที่มีผลต่างจากที่คาดหวังไว้ (เช่น ผลิตภัณฑ์ที่กำหนดไว้ว่ามีความเสี่ยงต่ำ หรือมีสัดส่วนกำไรที่ต่ำ แต่ในทางปฏิบัติให้ผลลัพธ์เป็นผลตอบแทนที่สูง) ซึ่งอาจเป็นข้อบ่งชี้ได้ว่า ผลลัพธ์ดังกล่าวเกิดจากการละเมิดการควบคุมภายในบางอย่าง

2.1.7 มีการพิสูจน์ความถูกต้อง และการยืนยันกระทบยอดอย่างสม่ำเสมอ (regular verification and reconciliation)

2.1.8 มีการกำหนดนโยบายการลางานสำหรับพนักงาน เพื่อเว้นว่างจากหน้าที่ของตนเป็นระยะเวลาหนึ่งตามความเหมาะสมกับบทบาทของพนักงาน ความเสี่ยง และความซับซ้อนของการดำเนินงานนั้น

2.2 การกำหนดแนวทางการควบคุมปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงด้านปฏิบัติการ

นอกจากการกำหนดนโยบายและกระบวนการในการควบคุมตามข้อ 2.1 สถาบันการเงินควรกำหนดแนวทางการควบคุมความเสี่ยงด้านปฏิบัติการที่เกิดจากปัจจัยดังต่อไปนี้ด้วย

2.2.1 การริเริ่มความเปลี่ยนแปลง (change initiatives) ความเสี่ยงด้านปฏิบัติการของสถาบันการเงิน (operational risk exposure) มักเกิดจากการริเริ่ม (change initiatives) เช่น การออกผลิตภัณฑ์และบริการทางการเงินรูปแบบใหม่ การเข้าสู่ตลาดใหม่

การปรับเปลี่ยน กระบวนการ ระบบงาน หรือการขยายขอบเขตการดำเนินงานที่อยู่ห่างไกลจากสำนักงานใหญ่ ดังนั้น สถาบันการเงินต้องมีนโยบายและกระบวนการบริหารจัดการความเปลี่ยนแปลง (change management) ที่สามารถประเมินความเสี่ยงที่เกี่ยวข้องตั้งแต่ริเริ่มจนสิ้นสุด (เช่น ตลอดวงจรชีวิตของผลิตภัณฑ์) เพื่อให้สามารถควบคุมและลดความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ ให้สถาบันการเงินดำเนินการในการเรื่องการบริหารจัดการความเปลี่ยนแปลงตามที่ธนาคารแห่งประเทศไทยกำหนด

2.2.2 การเชื่อมโยงกับบุคคลภายนอก (third party dependencies) การที่สถาบันการเงินต้องอาศัยความเชี่ยวชาญจากบุคคลภายนอกมากขึ้น เพื่อเพิ่มประสิทธิภาพและลดค่าใช้จ่ายในการดำเนินงาน ก่อให้เกิดความเสี่ยงด้านปฏิบัติการจากการใช้บริการจากผู้ให้บริการภายนอก สถาบันการเงินจึงต้องมีการกำหนดแนวทางการควบคุมความเสี่ยงที่เกิดจากปัจจัยดังกล่าว ทั้งนี้ ให้สถาบันการเงินถือปฏิบัติตามหลักเกณฑ์การติดตาม ตรวจสอบ และควบคุมความเสี่ยงจากการใช้บริการจากพันธมิตรทางธุรกิจที่ดำเนินการแทนสถาบันการเงิน ที่กำหนดไว้ในประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจ (business partner) ของสถาบันการเงิน โดยในกรณีที่เป็นการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) ให้สถาบันการเงินถือปฏิบัติตามหัวข้อการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management) ที่กำหนดไว้ในประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารเทศ (information technology risk) ของสถาบันการเงิน และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

2.2.3 การมีสำนักงาน หรือสาขา หรือบริษัทในต่างประเทศ ซึ่งระบบและกระบวนการดำเนินงานในต่างประเทศอาจกระทบต่อความเสี่ยงภาพรวมของสถาบันการเงินได้ ดังนั้น สถาบันการเงินควรเข้าใจถึงความแตกต่างในระบบและกระบวนการของสาขา หรือบริษัทในแต่ละประเทศ เพื่อกำหนดวิธีการควบคุมการดำเนินงานที่เหมาะสม

2.2.4 ข้อมูลเอกสารที่ต้องใช้ติดต่อสื่อสารกับบุคคลภายนอก (external documentation) หมายถึง เอกสารที่สถาบันการเงินจัดทำขึ้นสำหรับการทำธุรกรรมกับลูกค้า คู่ค้า หรือผู้ให้บริการภายนอก เช่น สัญญาการทำธุรกรรม ใบปลิวโฆษณา เป็นต้น ซึ่งหากมีข้อมูลที่ไม่ถูกต้องหรือไม่เหมาะสมอาจทำให้เกิดความเสี่ยงด้านกฎหมายได้ สถาบันการเงินจึงควรมีกระบวนการระบบงานที่เพียงพอในการสอบทานเอกสารดังกล่าวก่อนนำไปใช้ในทางปฏิบัติ โดยคำนึงถึงกฎหมายที่เกี่ยวข้อง ช่องทางหรือวิธีการในการนำส่งเอกสาร เป็นต้น

2.3 การควบคุมการปฏิบัติตามกฎเกณฑ์

สถาบันการเงินต้องมีกระบวนการและขั้นตอนการควบคุม ที่ครอบคลุมระบบและกระบวนการที่จะทำให้มั่นใจได้ว่ามีการปฏิบัติตามนโยบาย กฎเกณฑ์ และกฎหมายด้วย

(compliance) เช่น การสอบทานความคืบหน้าของกลยุทธ์ที่กำหนดไว้ โดยผู้บริหารระดับสูง การพิสูจน์ความถูกต้องของการปฏิบัติตามการควบคุม (verification of compliance with management controls) การสอบทานการปฏิบัติ หรือการแก้ปัญหาส่วนที่ไม่สามารถดำเนินการให้เป็นไปตามหลักเกณฑ์ที่กำหนดไว้ได้ (non-compliance) การประเมินการอนุมัติ และการมอบหมายอำนาจตามที่กำหนด เพื่อตรวจทานความเหมาะสมของการกำหนดหน้าที่ความรับผิดชอบในระดับการบริหาร การติดตามการรายงานรายการที่ได้รับยกเว้นจาก threshold หรือ limit ที่กำหนด หรือรายการที่ override หรือไม่เป็นไปตามนโยบาย กฎเกณฑ์และกฎหมาย

นอกจากนี้ กระบวนการควบคุมความเสี่ยงควรคำนึงถึงการเตรียมความพร้อมดำเนินธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (operational resilience framework) ด้วย

3. การติดตามดูแลความเสี่ยง (risk monitoring) การจัดเก็บข้อมูล และรายงานความเสี่ยงด้านปฏิบัติการ (risk reporting)

กระบวนการในการติดตามความเสี่ยงที่มีประสิทธิภาพจะช่วยให้สถาบันการเงินสามารถป้องกันและควบคุมเหตุการณ์ความเสียหายได้อย่างทันท่วงที **ซึ่งกระบวนการนี้ต้องมีการประเมินความเสี่ยงทั้งเชิงคุณภาพ และปริมาณอย่างต่อเนื่อง (on-going process) ในแง่ของประเภทของความเสี่ยงด้านปฏิบัติการ การประเมินคุณภาพ ความเหมาะสมในการดำเนินการแก้ไขลดความเสี่ยง และมีระบบการควบคุมที่เพียงพอ เพื่อใช้ระบุหรือแก้ปัญหาก่อนที่จะมีผลกระทบอย่างมีนัยสำคัญ**

สถาบันการเงินต้องกำหนดมาตรวัด (metrics) เพื่อใช้ในการติดตามดูแลความเสี่ยงด้านปฏิบัติการที่อาจเกิดขึ้น (operational risk exposure) โดยใช้ข้อมูลเหตุการณ์ความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยง มาประกอบกัน และกำหนด benchmark ด้วยดัชนีชี้วัด เช่น จำนวนเหตุการณ์ความเสียหาย หรือแบบจำลองที่ซับซ้อนมากขึ้นที่สามารถนำมาเปรียบเทียบกับ threshold หรือ limit หรือ tolerance level **ที่กำหนดไว้ล่วงหน้า เพื่อใช้เป็นสัญญาณเตือนเมื่อมีความเสี่ยงด้านปฏิบัติการที่เพิ่มขึ้น หรือมีการละเมิดความเสี่ยงด้านปฏิบัติการที่กำหนดไว้** รวมทั้งกำหนดความถี่ของการติดตามให้เหมาะสม ซึ่งขึ้นอยู่กับประเภท ความซับซ้อน และความเสี่ยงที่แต่ละหน่วยงานมีแตกต่างกัน **รวมถึงสะท้อนถึงจังหวะ และลักษณะของการเปลี่ยนแปลงในสภาพแวดล้อมการดำเนินงานด้วย**

นอกจากนี้ กระบวนการติดตามความเสี่ยงที่มีประสิทธิภาพ ยังเป็นกระบวนการสำคัญที่ทำให้องค์กรมีข้อมูลที่เป็นประโยชน์ในการรายงานให้ผู้บริหารระดับสูงเพื่อประกอบการพิจารณาแก้ไขปัญหาที่อาจเกิดขึ้น โดยสถาบันการเงินต้องดำเนินการให้มีการจัดเก็บและจัดทำรายงานที่เกี่ยวข้องกับความเสี่ยงด้านปฏิบัติการ ดังนี้

3.1 รายงานข้อมูลความเสียหายที่เกิดขึ้น (loss data)

สถาบันการเงินต้องจัดทำและติดตามข้อมูลความเสียหาย บันทึกความถี่ ความรุนแรง และข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความเสียหายนั้นอย่างเป็นระบบ เพื่อประโยชน์ในการบริหารความเสี่ยงขององค์กรพร้อมทั้งกำหนดความเสียหายขั้นต่ำ (loss threshold) ให้เหมาะสมกับองค์กร โดยข้อมูลที่จัดเก็บ ควรรวมถึง วันที่เกิดและตรวจพบความเสียหาย หน่วยงานที่เกิดความเสียหาย ประเภทของเหตุการณ์ความเสียหาย (loss event types) [1] ความเสียหายที่เกิดขึ้น เงินชดเชยหรือค่าเสียหายที่เรียกคืนได้ ระยะเวลาที่ใช้ในการเรียกคืนและค่าใช้จ่ายในการดำเนินการ รายละเอียดและสาเหตุของเหตุการณ์ความเสียหาย การดำเนินการแก้ไขเหตุการณ์ความเสียหายที่เกิดขึ้น เป็นต้น และนอกเหนือจากการจัดเก็บและรายงานข้อมูลความเสียหายที่เกิดขึ้นแล้ว สถาบันการเงินควรเก็บข้อมูลเหตุการณ์ที่เกิดขึ้น แต่สามารถป้องกันความเสียหายไว้ได้ (near-misses) เพื่อประโยชน์ในการศึกษาและพัฒนาระบบบริหารความเสี่ยงด้านปฏิบัติการขององค์กรต่อไป

3.2 รายงานเกี่ยวกับความเสี่ยงด้านปฏิบัติการ

สถาบันการเงิน**ต้อง**จัดให้มีการรายงานเกี่ยวกับความเสี่ยงด้านปฏิบัติการ**ทั้งในภาวะปกติและในสถานการณ์ที่ตลาดอยู่ในภาวะวิกฤต ภายในเวลาที่เหมาะสม โดยข้อมูลในรายงานต้องแสดงถึงการติดตามความเสี่ยงด้านปฏิบัติการภาพรวมภายใต้ risk appetite และ tolerance statement ที่กำหนด ด้วยข้อมูลที่ถูกต้อง กระชับ ครอบคลุมการปฏิบัติงานของหน่วยธุรกิจ และกิจกรรมการดำเนินงานขององค์กร** เพื่อให้แต่ละหน่วยงาน ผู้บริหารระดับสูง และคณะกรรมการทราบถึงแนวโน้มและการเปลี่ยนแปลงของความเสี่ยงด้านปฏิบัติการขององค์กร และสามารถดำเนินการป้องกัน ควบคุมหรือลดความเสียหายที่อาจเกิดขึ้นได้อย่างทันท่วงที **เช่น การละเมิด risk appetite, tolerance statement รวมถึง thresholds, limits หรือข้อกำหนดเชิงคุณภาพอื่น ๆ การวิเคราะห์ความเสี่ยงที่สำคัญที่อาจเกิดขึ้น โดยอาจแสดงด้วยข้อมูล metric ที่แสดงให้เห็นแนวโน้ม การเปลี่ยนแปลงจากการทำ control self-assessments รายงานความเห็นจากการตรวจสอบหรือการปฏิบัติตามกฎเกณฑ์ เหตุการณ์ความเสียหายที่เกิดขึ้น รวมถึงการวิเคราะห์สาเหตุของเหตุการณ์ (root cause) ความเสี่ยงคงเหลือ (residual risk)[2] สถานะของแผนการแก้ไขปัญหา เหตุการณ์ภายนอกที่เกี่ยวข้อง หรือ การเปลี่ยนแปลงเกี่ยวกับหลักเกณฑ์ หรือข้อมูลอื่น ๆ ที่อาจะกระทบต่อสถาบันการเงิน ข้อมูลเหตุการณ์หรือเงื่อนไขอื่นใดที่เกี่ยวข้องกับการตัดสินใจ**

---

[1] Basel Committee on Banking Supervision (BCBS) ได้เสนอแนวทางการแบ่งตามประเภทเหตุการณ์ความเสียหาย (Loss event types) ไว้ (รายละเอียดตามตารางที่ 2) ซึ่งหากสถาบันการเงินมีแนวทางในการเก็บข้อมูลในลักษณะอื่นต้องสามารถเชื่อมโยงกับแนวทางการเก็บข้อมูลที่เสนอโดย BCBS ได้

[2] หน่วยธุรกิจ ควรมีส่วนร่วมในการจัดทำรายงาน residual risk ที่เกี่ยวเนื่องกับจุดบกพร่องในระบบบริหารความเสี่ยงด้านปฏิบัติการ ซึ่งไม่เป็นไปตามระดับความเสี่ยงที่กำหนดไว้

ตารางที่ 1 เครื่องมือในการระบุและประเมินความเสี่ยงด้านปฏิบัติการ

ในการระบุและประเมินความเสี่ยงด้านปฏิบัติการนั้น สถาบันการเงินควรพิจารณาถึงปัจจัยภายในและภายนอกอย่างเหมาะสม ซึ่งเป็นกระบวนการที่สนับสนุนให้สถาบันการเงินเข้าใจถึงลักษณะของความเสี่ยง (risk profile) ของตนเองและสามารถจัดสรรทรัพยากร รวมถึงกำหนดกลยุทธ์ในการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ โดยสถาบันการเงินอาจพิจารณาใช้เครื่องมือในการระบุและประเมินความเสี่ยง ดังต่อไปนี้

เครื่องมือ	คำอธิบาย
1. การบริหารจัดการเหตุการณ์ความเสี่ยง (event management)	เป็นการระบุถึงข้อบ่งชี้ของเหตุการณ์ที่ก่อให้เกิดความเสี่ยงพร้อมทั้งการวิเคราะห์ การบริหารจัดการเหตุการณ์นั้นแบบเบ็ดเสร็จ (end-to-end process) และการรายงานเหตุการณ์ ซึ่งเป็นไปตามกระบวนการที่สถาบันการเงินกำหนดไว้ ทั้งนี้ เพื่อให้การบริหารจัดการเหตุการณ์ความเสี่ยงเป็นไปอย่างเหมาะสม จึงควรมีการวิเคราะห์เหตุการณ์เพื่อระบุถึงความเสี่ยงด้านปฏิบัติการที่อาจเกิดขึ้นใหม่สำหรับองค์กรด้วย และทำความเข้าใจถึงสาเหตุและจุดบกพร่องของการควบคุม พร้อมทั้งกำหนดแนวทางการรับมือเพื่อป้องกันการเกิดเหตุการณ์ในลักษณะซ้ำเดิมอีก นอกจากนี้ ข้อมูลจากการบริหารจัดการนี้ยังใช้เป็นส่วนหนึ่งของการประเมินตนเอง (self-assessment) และการประเมินประสิทธิภาพของการควบคุมได้ด้วย
2. ข้อมูลเหตุการณ์ความเสี่ยงด้านปฏิบัติการ (operational risk event data)	เป็นชุดข้อมูลเหตุการณ์ความเสี่ยงด้านปฏิบัติการที่สถาบันการเงินรวบรวมเหตุการณ์ความเสี่ยงที่มีนัยสำคัญมาจัดเก็บไว้เพื่อประกอบการประเมินความเสี่ยงด้านปฏิบัติการ ซึ่งประกอบด้วย ข้อมูลความเสียหายภายในองค์กร (internal loss data) เหตุการณ์ที่จะเกิดขึ้นแต่สถาบันการสามารถป้องกันความเสียหายไว้ได้ (near-misses) รวมถึงข้อมูลความเสียหายภายนอกองค์กร (ถ้ามี) เนื่องจากอาจมีข้อมูลความเสี่ยงร่วมกันที่มักเกิดขึ้นในธุรกิจสถาบันการเงิน หรือในระบบสถาบันการเงิน โดยการรวบรวมข้อมูลขึ้นอยู่กับชุดนิยามความเสี่ยงด้านปฏิบัติการ (operational risk taxonomy) ที่กำหนดไว้ตามกรอบ ORMF ของแต่ละองค์กร ทั้งนี้ ชุดข้อมูลควรมีรายละเอียดของวันที่ของเหตุการณ์ (วันที่เกิดเหตุ วันที่ตรวจพบ และวันที่บันทึกบัญชี) ผลกระทบด้านการเงิน (กรณีที่มีความเสียหายเกิดขึ้น) และสาเหตุของเหตุการณ์นั้น (root cause) ด้วย
3. การประเมินด้วยตนเอง (self-assessments)	เป็นการประเมินและควบคุมความเสี่ยงด้านปฏิบัติการโดยมีรูปแบบและระดับที่แตกต่างกันสำหรับความเสี่ยงที่เกิดขึ้นก่อนมีการควบคุมหรือจัดการ (inherent risk) ประสิทธิภาพของสภาพแวดล้อมของการควบคุม และความเสี่ยงคงเหลือหลังจากที่มีการควบคุมหรือจัดการแล้ว (residual risk) รวมถึงองค์ประกอบอื่น ๆ ในเชิงปริมาณและคุณภาพ ซึ่งสะท้อนถึงการพิจารณาทั้งโอกาสหรือความถี่ (likelihood) และผลกระทบ (consequence) ของเหตุการณ์ในการกำหนดระดับความเสี่ยง (inherent and residual risk rating) ของสถาบันการเงิน

เครื่องมือ	คำอธิบาย
	ในการประเมินตนเอง สถาบันการเงินควรจัดหมวดหมู่ของการดำเนินธุรกิจ เพื่อระบุถึงขั้นตอนสำคัญในการทำธุรกิจ การดำเนินงานต่างๆ กับความเสี่ยงและจุดบกพร่องของการควบคุมที่เกี่ยวข้อง พร้อมทั้งมีข้อมูลสภาพแวดล้อมการทำธุรกิจ ความเสี่ยงด้านปฏิบัติการ สาเหตุของความเสี่ยง การควบคุม และการประเมินประสิทธิภาพของการควบคุมที่มีรายละเอียดเพียงพอ เพื่อให้ผู้ประเมิน (independent reviewer) สามารถกำหนดแนวทางการบริหารความเสี่ยงด้านปฏิบัติการได้อย่างเหมาะสม ทั้งนี้ ทะเบียนการจัดการความเสี่ยง (risk register) ควรจัดเก็บข้อมูลจากการประเมินภาพรวมของประสิทธิภาพการควบคุมนี้ด้วย โดยจัดทำในรูปแบบที่เป็นประโยชน์ต่อการบริหารจัดการของผู้บริหารระดับสูง คณะกรรมการบริหารความเสี่ยง และคณะกรรมการสถาบันการเงิน
4. กรอบการติดตามและตรวจสอบการควบคุม (control monitoring and assurance framework)	การกำหนดกรอบการติดตามและตรวจสอบการควบคุมทำให้สถาบันการเงินมีแนวทางในการประเมิน สอบทาน ติดตามและทดสอบการควบคุมที่สำคัญได้อย่างต่อเนื่อง นอกจากนี้ การวิเคราะห์การติดตาม ควบคุมดังกล่าวทำให้สถาบันการเงินมั่นใจได้ว่าแนวทางการติดตาม ควบคุมที่กำหนดมีความเหมาะสมกับความเสี่ยงที่ระบุไว้ และได้ดำเนินการอย่างมีประสิทธิภาพแล้ว ทั้งนี้ การติดตามและทดสอบการควบคุมควรเหมาะสมกับความเสี่ยงด้านปฏิบัติการและการควบคุมที่สำคัญของลักษณะการทำธุรกิจแต่ละประเภทที่แตกต่างกันไป
5. มาตรวัด (metrics)	สถาบันการเงินอาจกำหนดมาตรวัดในการประเมินและติดตามความเสี่ยงด้านปฏิบัติการ (operational risk exposure) โดยใช้ข้อมูลเหตุการณ์ความเสี่ยง หรือจากการประเมินความเสี่ยง ซึ่งอาจเป็นตัวชี้วัดที่ไม่ซับซ้อน เช่น จำนวนเหตุการณ์ หรืออาจมีตัวชี้วัดที่ซับซ้อนมากขึ้นจากแบบจำลองที่กำหนดขึ้น การกำหนดมาตรวัดดังกล่าวใช้เป็นสัญญาณเตือนภัยล่วงหน้าในการติดตามความเสี่ยงซึ่งเป็นส่วนหนึ่งของการจัดทำรายงานภาพรวมในการบริหารความเสี่ยงด้านปฏิบัติการ นอกจากนี้ การติดตามมาตรวัดและแนวโน้มที่เกี่ยวข้องในช่วงเวลาหนึ่งเทียบกับ thresholds หรือ limits ที่กำหนดไว้ ช่วยให้สถาบันการเงินมีข้อมูลที่มีประโยชน์ต่อการบริหารจัดการความเสี่ยง
6. การวิเคราะห์สถานการณ์ (scenario analysis)	เป็นกระบวนการในการระบุ วิเคราะห์ ถึงสถานการณ์ต่าง ๆ ที่อาจก่อให้เกิดความเสี่ยงด้านปฏิบัติการ ซึ่งรวมถึงสถานการณ์ที่มีความน่าจะเป็นในการเกิดขึ้นน้อยแต่มีผลกระทบอย่างรุนแรง และอาจนำไปสู่ความเสียหายได้ โดยในทางปฏิบัติ การวิเคราะห์ดังกล่าวต้องอาศัยการทำงานร่วมกันระหว่างผู้บริหารระดับสูง พนักงานสายธุรกิจ และพนักงานที่เกี่ยวข้องกับความเสี่ยงด้านปฏิบัติการ รวมถึงสายงานที่เกี่ยวข้อง เช่น การกำกับการปฏิบัติตามกฎเกณฑ์ ทรัพยากรบุคคล และ การบริหารจัดการด้านเทคโนโลยีสารสนเทศ เพื่อมาพัฒนากระบวนการในการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากสถานการณ์ต่าง ๆ

เครื่องมือ	คำอธิบาย
	ตัวแปรที่ใช้ในการวิเคราะห์สถานการณ์ประกอบด้วยข้อมูลความเสียหาย (loss data) ที่เกิดขึ้นทั้งในและนอกองค์กร ข้อมูลจากการประเมินตนเอง (self-assessments) กรอบการติดตามและตรวจสอบการควบคุม (control monitoring and assurance framework) มาตรวัดที่คาดการณ์ความเสี่ยงที่จะเกิดขึ้น (forward-looking metrics) กรอบกระบวนการในการวิเคราะห์ต้นตอปัญหา (root-cause analyses and the process framework) ทั้งนี้ กระบวนการวิเคราะห์สถานการณ์ (scenario analysis) จะมีประสิทธิภาพในการประเมินความเสี่ยงต้องอยู่ภายใต้กรอบการกำกับดูแลความเสี่ยงที่เข้มแข็งและการสอบทานอย่างอิสระ ซึ่งจะทำให้มั่นใจว่ากระบวนการดังกล่าวมีความถูกต้องและเหมาะสมกับบริบทปัจจุบัน
7. การวิเคราะห์เชิงเปรียบเทียบ (benchmarking and comparative analyses)	เป็นการเปรียบเทียบผลลัพธ์ของวิธีการและเครื่องมือต่างๆ ที่สถาบันการเงินใช้ในการบริหารจัดการความเสี่ยง รวมถึงเปรียบเทียบมาตรวัดความเสี่ยงของสถาบันการเงินกับของสถาบันการเงินแห่งอื่น สถาบันการเงินสามารถใช้การเปรียบเทียบนี้มาช่วยในการทำความเข้าใจลักษณะความเสี่ยงด้านปฏิบัติการของสถาบันการเงิน เช่น การเปรียบเทียบความถี่และความรุนแรงของความเสียหายจากการประเมินตนเอง (self-assessments) ช่วยให้สถาบันการเงินทราบถึงความมีประสิทธิภาพของกระบวนการและกลไกของการประเมินตนเอง นอกจากนี้ สถาบันการเงินสามารถใช้ข้อมูลเกี่ยวกับสถานการณ์ต่างๆ (scenario analysis) มาเปรียบเทียบกับข้อมูลความเสียหายภายในและภายนอกเพื่อให้เข้าใจถึงความรุนแรงของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น

ตารางที่ 2 ตัวอย่างการเก็บข้อมูลความเสียหายที่เกิดจากความเสี่ยงด้านปฏิบัติการ

ลำดับที่ (1)	หน่วยงาน (2)	สายธุรกิจ (3)	วันที่เกิด (4)	วันที่ตรวจพบ (5)	รายละเอียด (6)	สาเหตุ (7)	ประเภทเหตุการณ์ (8)	จำนวนความเสียหาย (9)	จำนวนที่เรียกคืนได้ (10)	วันที่รับเงินคืน (11)	ค่าใช้จ่ายในการดำเนินการ (12)	การดำเนินการเพื่อแก้ไขความเสียหายที่เกิดขึ้น (13)	การดำเนินการเพื่อป้องกันความเสียหาย ที่อาจเกิดขึ้นในอนาคต (14)
1.	branch – teller บางขุนพรหม	BL 3 (RB)	18/02/64	29/05/64	พนักงานเบิกเงินจากบัญชีของลูกค้า โดยทุจริต (teller fraud)	พนักงานธนาคารได้รับความไว้วางใจจากลูกค้าธนาคารที่อยู่ใกล้สาขา ให้เบิกเงินแทนเจ้าของบัญชี	LET 1 (internal-fraud)	50,000	50,000	06/06/64	500	1. ชดเชยความเสียหายให้ลูกค้า 2. ระงับสิทธิ์ของพนักงานรายดังกล่าวในการเข้าใช้ระบบงานทุกระบบของสาขาชั่วคราว 3. ส่วนงานตรวจสอบเข้าตรวจทานการปฏิบัติงานของสาขา 4. ส่งรายงานการตรวจสอบ ให้ฝ่ายตรวจสอบ	1. ผจก. สาขากำชับพนักงาน teller ให้ปฏิบัติตามกฎระเบียบ เรื่อง บ/ช เงินฝากอย่างเคร่งครัด พร้อมแจ้งการดำเนินการให้ลูกค้าทราบทันที 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) การดำเนินการเพื่อแก้ไขความเสียหายที่เกิดขึ้น

(14) การดำเนินการเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต เช่น ปรับปรุงระบบการควบคุมภายใน ดูแลให้มีการปฏิบัติตามกฎระเบียบที่กำหนด หรือพัฒนาระบบรักษาความปลอดภัยให้เข้มงวดขึ้น เป็นต้น ซึ่งควรกำหนดกรอบเวลาและผู้รับผิดชอบอย่างชัดเจน พร้อมทั้งติดตามการดำเนินการอย่างใกล้ชิด

เอกสารแนบ 5

การบริหารจัดการความเปลี่ยนแปลง (change management)

ในการริเริ่มการเปลี่ยนแปลงในสถาบันการเงิน (change initiatives) เช่น การออกผลิตภัณฑ์และบริการทางการเงินรูปแบบใหม่ การขยายธุรกิจไปในตลาดใหม่ มีการนำระบบงานใหม่มาใช้ เป็นต้น สถาบันการเงินต้องมีนโยบายและกระบวนการที่ระบุถึงขั้นตอนวิธีการในการระบุ บริหารจัดการ อนุมัติ ติดตามความเปลี่ยนแปลงตามวัตถุประสงค์ที่กำหนดไว้ และต้องมีการสอบทาน ทบทวนนโยบายและกระบวนการดังกล่าวสม่ำเสมอ เพื่อปรับปรุงให้เหมาะสมกับบริบทปัจจุบัน รวมถึงมีการติดตามควบคุมดูแลการปฏิบัติด้วยกลไกการควบคุมที่กำหนดขึ้นเป็นการเฉพาะ

นอกจากนี้ ควรกำหนดบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงไว้เป็นการเฉพาะ กล่าวคือ หน่วยธุรกิจทำหน้าที่ประเมินและควบคุมความเสี่ยงด้านปฏิบัติการของผลิตภัณฑ์ใหม่ กิจกรรมใหม่ กระบวนการใหม่ ระบบงานใหม่ รวมถึงระบุ และประเมินความจำเป็นในการเปลี่ยนแปลงขั้นตอนการพิจารณาตัดสินใจ ตั้งแต่การวางแผนสู่การปฏิบัติ รวมถึงสอบทานผลการปฏิบัติด้วย สำหรับหน่วยงานกำกับภายใน ทำหน้าที่ให้ข้อสังเกตเกี่ยวกับการประเมินและควบคุมความเสี่ยงด้านปฏิบัติการของหน่วยธุรกิจ รวมทั้งติดตามดูแลวิธีการควบคุมอย่างเหมาะสม หรือการแก้ไขปัญหาในทางปฏิบัติ ซึ่งต้องครอบคลุมทั้งกระบวนการและคำนึงถึงปัจจัยที่เกี่ยวข้อง เช่น การเงิน การกำกับการปฏิบัติตามกฎหมาย เทคโนโลยีสารสนเทศอย่างเหมาะสมแล้ว

สถาบันการเงินควรกำหนดนโยบายและกระบวนการในการสอบทาน และอนุมัติผลิตภัณฑ์ใหม่ กิจกรรมใหม่ กระบวนการใหม่ ระบบงานใหม่ ที่ครอบคลุมประเด็นดังต่อไปนี้

(1) ความเสี่ยงเกี่ยวเนื่อง (inherent risks) (ซึ่งรวมถึง ความเสี่ยงด้านกฎหมาย IT และแบบจำลอง) กับการออกผลิตภัณฑ์และบริการทางการเงินรูปแบบใหม่ กิจกรรมใหม่ การดำเนินธุรกิจในตลาดที่ไม่คุ้นเคย การนำระบบงานใหม่มาใช้ (รวมถึงกรณีที่มีการใช้บริการจากบุคคลภายนอก)

(2) ผลกระทบต่อความเสี่ยงด้านปฏิบัติการโดยรวมของสถาบันการเงิน (operational risk profile) และผลกระทบต่อ risk appetite และ tolerance รวมถึง ผลกระทบต่อความเสี่ยงของผลิตภัณฑ์หรือการดำเนินงานที่มีอยู่

(3) กระบวนการควบคุม กระบวนการบริหารความเสี่ยง และกลยุทธ์ที่จำเป็นในการบรรเทาความเสี่ยง

(4) ความเสี่ยงคงเหลือ (residual risk)

(5) ผลกระทบต่อตัวชี้วัด (trigger) หรือเพดานความเสี่ยง (limit) ที่เกี่ยวข้องกับการบริหารความเสี่ยง

(6) กระบวนการหรือมาตรวัด (metrics) ในการประเมิน ติดตาม และจัดการความเสี่ยงของผลิตภัณฑ์และบริการทางการเงินรูปแบบใหม่ กิจกรรมใหม่ ตลาดใหม่ กระบวนการหรือระบบงานใหม่

ทั้งนี้ กระบวนการสอบทานและพิจารณาอนุมัติข้างต้น หมายรวมถึงการลงทุนในทรัพยากรบุคคลและโครงสร้างพื้นฐานด้านเทคโนโลยี (technology infrastructure) ที่เหมาะสมก่อนริเริ่มความเปลี่ยนแปลง และมีการติดตามความเปลี่ยนแปลงทั้งในช่วงที่อยู่ระหว่างดำเนินการ และภายหลังจากนั้น เพื่อเปรียบเทียบความแตกต่างของความเสี่ยงด้านปฏิบัติการที่คาดไว้ กับความเสี่ยงที่คาดไม่ถึงที่ต้องจัดการ รวมถึงการมีศูนย์กลางในการจัดเก็บข้อมูลผลิตภัณฑ์และบริการดังกล่าวไว้ เพื่อเอื้อต่อการติดตามดูแลการเปลี่ยนแปลงนั้น

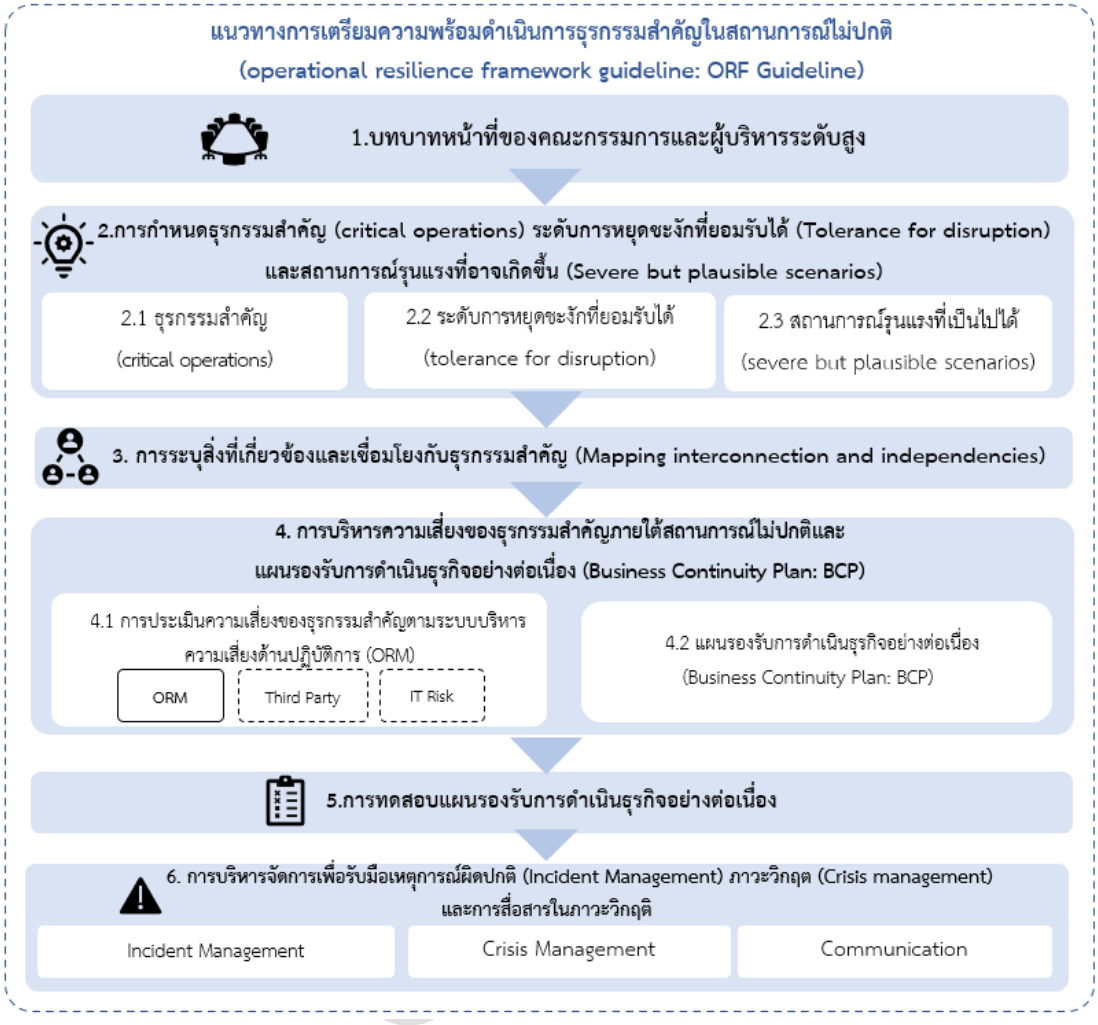
เอกสารแนบ 6

แนวทางการเตรียมความพร้อมดำเนินการธุรกรรมสำคัญในสถานการณ์ไม่ปกติ (operational resilience framework guideline: ORF guideline)

ธนาคารแห่งประเทศไทยได้จัดทำแนวทางการเตรียมความพร้อมดำเนินการธุรกรรมสำคัญในสถานะการณ์ไม่ปกติ หรือ ORF guideline เพื่อให้สถาบันการเงินใช้เป็นแนวทางในการกำหนด operational resilience framework (ORF) ของสถาบันการเงินเอง ทั้งในส่วนนโยบาย มาตรฐาน และกระบวนการทำงาน เพื่อให้มั่นใจว่าในกรณีที่มีสถานการณ์ไม่ปกติมากระทบต่อการดำเนินธุรกิจ สถาบันการเงินยังสามารถดำเนินการธุรกรรมสำคัญได้อย่างต่อเนื่องหรือกลับมาดำเนินการได้ในเวลาที่เหมาะสม ซึ่งการบริหารและการเตรียมความพร้อมที่ดีจะช่วยลดผลกระทบทางการเงิน กฎหมาย ชื่อเสียง และผลกระทบอื่น ๆ ที่อาจเกิดขึ้นได้ต่อสถาบันการเงิน และระบบสถาบันการเงินด้วย

ทั้งนี้ ธนาคารแห่งประเทศไทยกำหนดองค์ประกอบของ ORF ไว้เป็น 6 ส่วนที่สำคัญ ได้แก่ (1) บทบาทหน้าที่ของคณะกรรมการและผู้บริหารระดับสูง (governance) (2) การกำหนดธุรกรรมสำคัญของสถาบันการเงิน (critical operations) ระดับการหยุดชะงักการดำเนินการธุรกรรมสำคัญที่ยอมรับได้ (tolerance for disruption) สถานการณ์รุนแรงที่มีโอกาสเกิดขึ้น (severe but plausible scenarios) (3) การระบุสิ่งที่เกี่ยวข้องเชื่อมโยงต่อธุรกรรมสำคัญอย่างเพียงพอ (mapping interconnection and independencies) (4) การบริหารจัดการความเสี่ยงของธุรกรรมสำคัญในสถานการณ์ไม่ปกติ และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity planning: BCP) (5) การทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และ (6) การบริหารจัดการเพื่อรับมือและกู้คืนการดำเนินงาน ซึ่งสรุปความสัมพันธ์และกระบวนการของแต่ละปัจจัยได้ตามแผนภาพด้านล่าง และมีรายละเอียดที่เป็นแนวทางที่สถาบันการเงินควรดำเนินการ ดังต่อไปนี้

แผนภาพความสัมพันธ์ของแต่ละส่วนที่สำคัญของ ORF



1. บทบาทหน้าที่ของคณะกรรมการและผู้บริหารระดับสูง

1.1 คณะกรรมการของสถาบันการเงินเป็นผู้กำหนดทิศทาง กลยุทธ์ และอนุมัติกรอบนโยบาย ORF พร้อมทั้งสนับสนุนให้ผู้บริหารระดับสูงนำนโยบายดังกล่าวไปใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ มีการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินงาน เพื่อให้มั่นใจว่าในสถานการณ์ไม่ปกติ ธุรกรรมสำคัญของสถาบันการเงินสามารถดำเนินการได้อย่างต่อเนื่องหรือกลับมาให้บริการได้ในเวลาที่หมาะสม ทั้งนี้ ควรกำหนดให้มีการทบทวนนโยบายดังกล่าวเป็นประจำหรือเมื่อมีกาเปลี่ยนแปลง โดยคณะกรรมการสถาบันการเงินสามารถมอบหมายให้คณะกรรมการชุดย่อยในระดับกำกับดูแลพิจารณาอนุมัติการทบทวนนโยบายดังกล่าวได้ โดยให้นำเสนอคณะกรรมการสถาบันการเงินเพื่อทราบ อย่างไรก็ดี คณะกรรมการสถาบันการเงินต้องเป็นผู้พิจารณาอนุมัติหรือเห็นชอบกรณีมีการเปลี่ยนแปลงที่มีนัยสำคัญ

นอกจากนี้ คณะกรรมการอาจมอบหมายหน้าที่การดูแลงานด้านปฏิบัติการให้คณะทำงานหรือผู้บริหารระดับสูงก็ได้ โดยต้องจัดทำเป็นลายลักษณ์อักษร

1.2 ผู้บริหารระดับสูงเป็นผู้กำกับดูแลการจัดทำ ORF เพื่อเสนอขออนุมัติจากคณะกรรมการสถาบันการเงิน และควบคุมให้สถาบันการเงินมีการปฏิบัติตาม ทิศทาง กลยุทธ์ และนโยบายที่ได้รับอนุมัติจากคณะกรรมการ รวมทั้งกำหนดโครงสร้าง สายการบังคับบัญชา และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องให้ชัดเจน

2. การกำหนดธุรกรรมสำคัญ (critical operations) ระดับการหยุดชะงักที่ยอมรับได้ (tolerance for disruption) และสถานการณ์รุนแรงที่อาจเกิดขึ้น (severe but plausible scenarios)

ในการจัดทำ ORF สถาบันการเงินต้องกำหนดพารามิเตอร์ที่สำคัญที่เกี่ยวข้อง ได้แก่

2.1 การกำหนดธุรกรรมสำคัญ

สถาบันการเงินควรกำหนดหลักเกณฑ์ที่ชัดเจนในการพิจารณาและระบุธุรกรรมสำคัญ ซึ่งปกติจะวิเคราะห์และประเมินผลกระทบที่เกิดขึ้นหากธุรกรรมนั้นไม่สามารถดำเนินงานได้ ดังนี้

(1) ผลกระทบต่อเสถียรภาพของสถาบันการเงิน รวมไปถึงผลกระทบต่อลูกค้า ชื่อเสียง ฐานะ ผลการดำเนินงาน และการปฏิบัติตามหน่วยงานกำกับดูแล

(2) ผลกระทบต่อระบบสถาบันการเงิน โดยพิจารณาถึง ผลกระทบต่อการดำเนินงานต่อสถาบันการเงินอื่น เช่น การโอนเงิน การหักบัญชี (clearing) รวมถึงธุรกรรมในลักษณะที่เป็นคู่สัญญาระหว่างธนาคาร

ทั้งนี้ หากเกิดผลกระทบตามปัจจัยใด ปัจจัยหนึ่ง ควรกำหนดให้เข้าข่ายเป็นธุรกรรมสำคัญ

2.2 การกำหนดระดับการหยุดชะงักที่ยอมรับได้

ธุรกรรมสำคัญทั้งหมดที่สถาบันการเงินกำหนดไว้ ควรกำหนดระดับการหยุดชะงักที่ยอมรับได้ โดยควรมีตัวชี้วัดเป็นเวลา (time-bases) เป็นอย่างน้อย และต้องสอดคล้องตามหลักเกณฑ์ ธปท. ที่เกี่ยวข้อง อีกทั้งอาจพิจารณาใช้ตัวชี้วัดอื่นเพิ่มเติมได้ ดังนี้

(1) ตัวชี้วัดเชิงปริมาณ ได้แก่ ระยะเวลาที่ธุรกรรมหยุดชะงักที่ยอมรับได้ ปริมาณหรือมูลค่าของธุรกรรม เป็นต้น

(2) ตัวชี้วัดเชิงคุณภาพ ได้แก่ ชื่อเสียงของสถาบันการเงิน นัยทางกฎหมาย เป็นต้น

ทั้งนี้ สถาบันการเงินควรตระหนักถึงการดำเนินการของแต่ละธุรกรรมสำคัญตามช่วงเวลา (seasonal) หรือรอบธุรกิจ (business cycles) และทบทวนการหยุดชะงักที่ยอมรับได้เป็นประจำตามความเหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

2.3 การกำหนดสถานการณ์รุนแรงที่อาจเกิดขึ้น

การกำหนดสถานการณ์รุนแรงที่อาจเกิดขึ้นและกระทบต่อธุรกรรมสำคัญต้องสมเหตุสมผล มีความเป็นไปได้ เช่น เหตุภัยธรรมชาติ โรคระบาด เหตุการณ์ที่ผู้ให้บริการภายนอกไม่สามารถให้บริการได้ การถูกโจมตีทางไซเบอร์ เป็นต้น นอกจากนี้ ควรกำหนดช่วงระยะเวลาที่สถานการณ์รุนแรงที่อาจเกิดขึ้น ให้สอดคล้องกับการดำเนินธุรกรรมและความเสี่ยงที่เกิดขึ้น เช่น เกิดเหตุการณ์โรคระบาดรุนแรง และยาวนานเป็นเวลา 2 ปี เหตุการณ์ผู้ให้บริการอินเตอร์เน็ตรายใหญ่ขัดข้อง ส่งผลให้ระบบอินเตอร์เน็ตของผู้ให้บริการรายดังกล่าว ไม่สามารถใช้งานได้เป็นเวลา 2 วัน เป็นต้น ทั้งนี้ ควรทบทวนสถานการณ์รุนแรงที่อาจเกิดขึ้นให้สอดคล้องและเกี่ยวเนื่องกับสถานการณ์ปัจจุบัน

ทั้งนี้ สถาบันการเงินควรทบทวนหลักเกณฑ์การกำหนดธุรกรรมสำคัญ ระดับการหยุดชะงักที่ยอมรับได้ และสถานการณ์รุนแรงที่อาจเกิดขึ้น เป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

3. การระบุสิ่งที่เกี่ยวข้องและเชื่อมโยงกับธุรกรรมสำคัญ (mapping interconnection and independencies)

3.1 ควรระบุสิ่งที่จำเป็นต่อการดำเนินธุรกรรมสำคัญที่สถาบันการเงินได้กำหนดขึ้น<u>เป็นรายธุรกรรม</u> โดยมีการบันทึกและปรับปรุงให้เป็นปัจจุบัน ครอบคลุมในเรื่องดังต่อไปนี้เป็นอย่างน้อย

(1) บุคลากรที่เกี่ยวข้อง (people)

(2) กระบวนการที่เกี่ยวข้อง (process)

(3) ระบบงาน หรือเทคโนโลยีที่เกี่ยวข้อง (technology)

(4) ข้อมูลที่จำเป็น (information)

(5) อุปกรณ์ หรือสถานที่ ที่จำเป็น (facility)

3.2 ควรระบุถึงความเชื่อมโยงระหว่างธุรกรรมสำคัญกับสิ่งที่จำเป็นต่อการดำเนินธุรกรรมสำคัญ โดยมีการบันทึกและปรับปรุงให้เป็นปัจจุบัน ให้เพียงพอต่อการใช้ระบุถึงความเสี่ยงจากการเชื่อมโยงนั้น โดยเฉพาะอย่างยิ่งกรณีการเชื่อมโยงของการดำเนินธุรกรรมสำคัญกับผู้ให้บริการภายนอก หรือบริษัทในกลุ่มธุรกิจทางการเงิน

3.3 ควรพิจารณาและประเมินความเสี่ยงที่เกิดจากการกระจุกตัว (concentration risk) ของธุรกรรมสำคัญที่เกี่ยวข้องเชื่อมโยงกับผู้ให้บริการภายนอกรายเดียว ทักษะของบุคลากร ข้อมูลที่

จำเป็น และระบบที่สำคัญที่ยากต่อการทดแทนใหม่ได้อย่างรวดเร็ว และควรพิจารณาหาทางลดความเสี่ยง[1] และผลกระทบที่อาจเกิดจากความเสี่ยงดังกล่าว

4. การบริหารความเสี่ยงของธุรกรรมสำคัญภายใต้สถานการณ์ไม่ปกติและแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan: BCP)

4.1 การประเมินความเสี่ยงของธุรกรรมสำคัญตามระบบบริหารความเสี่ยงด้านปฏิบัติการ (ORM)

สถาบันการเงินควรประเมินความเสี่ยงของธุรกรรมสำคัญตามระบบการบริหารความเสี่ยงด้านปฏิบัติการที่สถาบันการเงินได้กำหนดไว้ (ซึ่งรวมถึงการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอก และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ) เพื่อประเมินความพร้อมในการควบคุม หรือลดความเสี่ยงที่อาจจะเกิดขึ้น โดยควรครอบคลุมกระบวนการดังนี้

(1) ควรประเมินความเสี่ยง (risk assessment) ที่อาจทำให้ธุรกรรมสำคัญเกิดการหยุดชะงักอย่างน้อยปีละครั้ง โดยควรระบุเหตุการณ์ที่อาจทำให้เกิดการหยุดชะงัก ซึ่งอาจส่งผลกระทบต่อสถาบันการเงินทั้งในระยะสั้น ระยะปานกลาง หรือระยะยาว รวมทั้งประเมินโอกาสที่จะเกิดเหตุการณ์ดังกล่าวขึ้น หรือเมื่อเกิดการเปลี่ยนแปลงที่สำคัญทั้งปัจจัยที่มาจากภายในและภายนอกที่อาจส่งผลกระทบต่อสถาบันการเงิน

(2) ควรวิเคราะห์กระบวนการควบคุมความเสี่ยงที่มีอยู่ และปรับปรุงกระบวนการและทรัพยากรที่จำเป็นในการควบคุมความเสี่ยง รวมถึงการจัดทำการประเมินผลและควบคุมกระบวนการดังกล่าว

(3) ควรวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ที่อาจเกิดขึ้นกับทุกธุรกรรมสำคัญ เพื่อให้ทราบถึงความสัมพันธ์ของธุรกรรมสำคัญและผลกระทบจากการหยุดชะงักของธุรกรรมสำคัญนั้น ซึ่งจะทำให้สถาบันการเงินสามารถกำหนดลำดับความสำคัญของการดำเนินงานและจัดสรรทรัพยากรในการเรียกคืนการดำเนินงานได้อย่างมีประสิทธิภาพ โดยการวิเคราะห์ผลกระทบทางธุรกิจควรพิจารณาถึงผลกระทบต่อผู้มีส่วนได้เสียของสถาบันการเงินทั้งในเชิงปริมาณและเชิงคุณภาพ เช่น รายได้ที่อาจสูญเสียไป ค่าใช้จ่ายที่อาจเกิดขึ้น ชื่อเสียงและความน่าเชื่อถือของสถาบันการเงิน เป็นต้น และจัดลำดับความสำคัญของทรัพยากรทั้งภายในและภายนอกสถาบันการเงินที่จำเป็นในแต่ละธุรกรรมสำคัญด้วย

---

[1] ตัวอย่างวิธีการลดความเสี่ยง ได้แก่ การกำหนดศูนย์ปฏิบัติงานหลัก และศูนย์ปฏิบัติงานรอง (primary-secondary site operation) ให้ห่างพอที่จะไม่ได้รับผลกระทบเดียวกัน การกระจายธุรกรรมสำคัญไม่ให้กระจุกตัวมากเกินไป การกระจายทีมปฏิบัติงาน การฝึกอบรมการปฏิบัติงานแบบ cross-training เพื่อให้บุคลากรที่ปฏิบัติงานมีความหลากหลาย และไม่อยู่แค่คนๆเดียว

4.2 แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan: BCP)

เพื่อให้สถาบันการเงินสามารถรองรับหรือเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ และช่วยให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง ครอบคลุมทุกธุรกรรมสำคัญในองค์กร รวมถึงผู้ให้บริการภายนอกที่เกี่ยวข้องสามารถนำไปดำเนินงานได้ตามเป้าหมายการเรียกคืนการดำเนินงาน และอยู่ภายใต้ระดับการหยุดชะงักที่ยอมรับได้ แม้ว่าจะอยู่ในสถานการณ์ไม่ปกติ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องควรมีรายละเอียดดังนี้

(1) การกำหนดเป้าหมายการเรียกคืนการดำเนินงาน (recovery objectives) เพื่อการเรียกคืนการดำเนินงานของธุรกรรมสำคัญให้กลับสู่ภาวะปกติ ประกอบด้วย

(1.1) การกำหนดระยะเวลาเป้าหมายในการเรียกคืนหรือกู้คืนการดำเนินงาน (recovery time objectives : RTO) ของแต่ละธุรกรรมสำคัญ ซึ่งควรสอดคล้องกับสิ่งที่จำเป็นต่อการดำเนินธุรกรรมสำคัญ และระดับการหยุดชะงักที่ยอมรับได้

(1.2) การกำหนดกลยุทธ์การเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ (recovery strategy) ซึ่งควรนำผลที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจมาพิจารณากำหนดกลยุทธ์การเรียกคืนการดำเนินงาน ที่เหมาะสมเพื่อให้บรรลุตามเป้าหมายที่ได้กำหนดไว้ โดยต้องจัดสรรทรัพยากรและงบประมาณแก่หน่วยงานที่เกี่ยวข้องอย่างเพียงพอต่อการดำเนินกลยุทธ์ดังกล่าว

(2) การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

สถาบันการเงินควรจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเป็นลายลักษณ์อักษร มีการกำหนดขั้นตอนการดำเนินการ โดยทุกหน่วยงานที่เกี่ยวข้องควรมีส่วนร่วมในการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของตนเอง และปรับปรุงให้เป็นปัจจุบันเสมอ เพื่อสามารถนำไปดำเนินการได้ตรงตามเป้าหมายเมื่อต้องการ และจัดเก็บไว้ที่ผู้รับผิดชอบอย่างน้อยหนึ่งชุด พร้อมทั้งจัดเก็บชุดสำรองไว้ในช่องทางที่ง่ายต่อการนำไปใช้งาน โดยมีรายละเอียดครอบคลุมประเด็นอย่างน้อย ดังนี้

(2.1) ขั้นตอนรายละเอียดการดำเนินงานเมื่อมีการหยุดชะงักของธุรกรรมสำคัญ ทั้งนี้ ควรพิจารณาครอบคลุมในกรณีที่เกิดสถานการณ์ไม่ปกติจนส่งผลให้พนักงานผู้ปฏิบัติงาน และพนักงานที่จำเป็นต่อการดำเนินแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ไม่สามารถเข้าไปปฏิบัติงาน หรือสนับสนุนการทำงานในสถานที่ทำงานโดยปกติได้ เพื่อให้เกิดการวางแผน เตรียมพร้อมในการปรับตัวตามสถานการณ์ที่อาจเกิดขึ้น และสามารถดำเนินงานได้อย่างต่อเนื่อง หรือกลับมาดำเนินการได้ตามระยะเวลาที่กำหนด

(2.2) ทรัพยากรที่จำเป็นสำหรับปฏิบัติงาน โดยสอดคล้องกับสิ่งที่จำเป็นต่อการดำเนินธุรกรรมสำคัญตามที่ได้สถาบันการเงินได้ระบุไว้เป็นอย่างน้อย

(2.3) แผนการติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอกสถาบันการเงิน

(2.4) แผนการจัดตั้งศูนย์ปฏิบัติงานสำรอง (alternate sites) เมื่อเห็นว่ามีความจำเป็น โดยศูนย์ปฏิบัติงานสำรองควรอยู่ห่างจากศูนย์ปฏิบัติงานหลักพอที่จะไม่ได้รับผลกระทบเดียวกัน และไม่ควรใช้สาธารณูปโภคจากแหล่งเดียวกัน เพื่อป้องกันเหตุการณ์ที่มีผลกระทบในวงกว้าง ทั้งนี้ ศูนย์ปฏิบัติงานสำรองต้องมีความพร้อมในการใช้งานได้ตลอดเวลา และสามารถรองรับเหตุการณ์ความเสียหายในระยะยาวได้ อย่างไรก็ดี สำหรับสาขาธนาคารพาณิชย์ต่างประเทศอาจใช้สาขาอื่นในต่างประเทศดูแลเรื่องศูนย์ปฏิบัติงานสำรองหรือกรณีที่มีธุรกรรมไม่มากพอ อาจไม่จำเป็นต้องจัดตั้งศูนย์ปฏิบัติงานสำรอง เพียงแต่ต้องมีแนวทางดำเนินการทดแทนที่เหมาะสม

(2.5) หากสถาบันการเงินใช้บริการจากผู้ให้บริการหลัก สถาบันการเงินต้องมั่นใจว่าแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของผู้ให้บริการหลัก มีความสอดคล้องกับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงินด้วย

5. การทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

5.1 สถาบันการเงินควรจัดให้มีการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง หรือทดสอบ BCP ภายใต้สถานการณ์รุนแรงที่อาจเกิดขึ้น เพื่อให้มั่นใจได้ว่าธุรกรรมสำคัญยังคงสามารถดำเนินการได้ไม่เกินระดับการหยุดชะงักที่ยอมรับได้ และพร้อมปรับตัวต่อสถานการณ์รุนแรงที่อาจเกิดขึ้นจริง

5.2 การทดสอบ BCP ควรดำเนินการดังต่อไปนี้ เป็นอย่างน้อย

(1) อยู่ภายใต้สมมติฐานที่เป็นจริง และครอบคลุมถึงปัจจัยต่างๆ ที่เกี่ยวข้องเชื่อมโยงกับธุรกรรมสำคัญ ทั้งผู้ให้บริการภายนอก และบริษัทในกลุ่มธุรกิจทางการเงิน

(2) พิจารณาขอบเขตของการทดสอบให้ครอบคลุมถึงกระบวนการ หรือแผนงานที่สถาบันการเงินกำหนดไว้ [2] การจัดให้มีบุคลากรที่เกี่ยวข้องเข้าร่วมทดสอบอย่างเพียงพอ เช่น หน่วยงานที่เกี่ยวข้อง ตามลักษณะตำแหน่งงานของผู้เข้าร่วมทดสอบ ความเชี่ยวชาญที่จำเป็นในการทดสอบ รวมถึงสอดคล้องกับรูปแบบ และความถี่ในการทดสอบด้วย

---

[2] การทดสอบกระบวนการ หรือแผนงานสถาบันการเงินได้กำหนดเอาไว้ ได้แก่ กระบวนการการบริหารจัดการเหตุการณ์ผิดปกติ (Incident Management) กระบวนการบริหารภาวะวิกฤต (crisis management) การติดต่อสื่อสารทั้งภายในและภายนอกองค์กร การกู้คืนธุรกรรมสำคัญ การทดสอบใช้ศูนย์ปฏิบัติงานสำรอง การทดสอบกรณีผู้ปฏิบัติงานหลักที่สำคัญ หรือผู้ให้บริการรายสำคัญไม่สามารถปฏิบัติงานได้ เป็นต้น

(3) กำหนดความถี่ในการทดสอบที่ชัดเจน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยงในการเกิดการหยุดชะงักอย่างมีนัยสำคัญ โดยพิจารณาจากปัจจัยต่าง ๆ รวมไปถึงผลกระทบที่อาจเกิดขึ้นจากสถานการณ์ไม่ปกติ จำนวนธุรกรรมสำคัญที่สถาบันการเงินกำหนด และสภาพแวดล้อมในการปฏิบัติงานที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(4) กำหนดวิธีการและรูปแบบการทดสอบ [3] ตามความเหมาะสม และสอดคล้องกับวัตถุประสงค์ของการทดสอบ ทั้งนี้ ควรประเมินความเสี่ยงที่อาจเกิดขึ้นจากรูปแบบการทดสอบที่เลือกใช้ด้วย

(5) หลังจากการทดสอบ ต้องจัดให้มีการเก็บข้อมูลผลการทดสอบเพื่อเทียบเคียงกับเป้าหมายที่ได้กำหนดไว้ (gap analysis) เพื่อใช้ประเมินผลการทดสอบและพัฒนาประสิทธิภาพของแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และรายงานผลการทดสอบดังกล่าวต่อคณะกรรมการด้วย

6. การบริหารจัดการเพื่อรับมือเหตุการณ์ผิดปกติ (incident management) ภาวะวิกฤต (crisis management) และการสื่อสารในภาวะวิกฤติ

6.1 สถาบันการเงินควรมีการบริหารจัดการเหตุการณ์ผิดปกติ (incident) ที่เกิดขึ้น โดยเฉพาะเหตุการณ์ผิดปกติที่กระทบกับธุรกรรมสำคัญ รวมไปถึงเหตุการณ์ผิดปกติที่อาจเกิดจากผู้ให้บริการภายนอก โดยควรครอบคลุมประเด็นต่อไปนี้เป็นอย่างน้อย

(1) กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ การกำหนดประเภทของเหตุการณ์ผิดปกติที่เกิดขึ้น การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดำเนินการแก้ไข การติดตามการแก้ไข การรายงานเหตุการณ์ผิดปกติ

(2) หลักเกณฑ์ที่ชัดเจนในการพิจารณาการจัดระดับความรุนแรงของเหตุการณ์ผิดปกติ (severity) โดยกำหนดกรอบระยะเวลาในการแก้ไขเหตุผิดปกติที่สอดคล้องกับเป้าหมายการเรียกคืนการดำเนินงาน (recovery objectives) และระดับการหยุดชะงักที่ยอมรับได้ (tolerance for disruption)

(3) การระบุหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้อง ทั้งสถาบันการเงินและผู้ให้บริการภายนอก

---

[3] ตัวอย่างวิธีการทดสอบ ได้แก่ การทดสอบ call-tree การทดสอบการบริหารภาวะวิกฤต (crisis management exercises) การทดสอบการกู้คืนทางธุรกิจ (business recovery test) การทดสอบกู้คืนข้อมูล (data restoration testing) ซึ่งอาจพิจารณาเพิ่มเติมสถานการณ์ตามความเหมาะสมได้ เช่น สถานการณ์ที่จำเป็นต้องใช้ศูนย์คอมพิวเตอร์สำรอง หรือศูนย์ปฏิบัติงานสำรอง สถานการณ์ที่มีบุคลากรจำกัด สถานการณ์ที่ต้องปฏิบัติงานโดยไม่มีผู้ให้บริการภายนอก เป็นต้น โดยตัวอย่างรูปแบบการทดสอบ ได้แก่ ทดสอบบน paper-based ทดสอบบนสถานการณ์จำลอง ไปจนถึง ทดสอบบนสถานการณ์จริง เป็นต้น

(4) การกำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ (escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้องหรือคณะกรรมการของสถาบันการเงินได้รับทราบ ให้สอดคล้องกับระดับความรุนแรงของเหตุการณ์ผิดปกติ

(5) การจัดการรับมือและตอบสนองต่อเหตุผิดปกติ ตามความสำคัญของเหตุการณ์ โดยควรระบุ กระบวนการรับมือ ช่องทางประสานงาน และการติดต่อสื่อสารทั้งภายในและภายนอกองค์กร มีแนวทางการตรวจสอบวิเคราะห์หาสาเหตุ และประเมินผลกระทบ พร้อมทั้งมีการสอบทานและทบทวนกระบวนการดังกล่าวเป็นประจำ

(6) การวิเคราะห์หาสาเหตุที่แท้จริง (root cause) ของปัญหาที่เกิดขึ้นเพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต และพิจารณานำเหตุการณ์ผิดปกติที่เกิดขึ้นมาปรับปรุงกระบวนการในการรับมือและตอบสนองต่อเหตุผิดปกติให้ดียิ่งขึ้น

(7) การจัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อคณะกรรมการของสถาบันการเงิน คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย โดยครอบคลุม วัน เวลา เหตุการณ์ ความเสียหาย การวิเคราะห์สาเหตุที่แท้จริง การวิเคราะห์ผลกระทบ การแก้ไขปัญหาและแนวทางหรือแผนดำเนินการเพื่อ ป้องกันเหตุการณ์ผิดปกติในอนาคต และในกรณีที่เป็นความเสียหายส่งผลกระทบต่อชื่อเสียงและการให้บริการ หรือดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจ อย่างมีนัยสำคัญ ให้รายงานต่อคณะกรรมการสถาบันการเงินทราบด้วย รวมถึงการบันทึกเหตุการณ์ผิดปกติที่เกิดขึ้นในรายงานข้อมูลความเสียหายที่เกิดขึ้น (loss data)

6.2 สถาบันการเงินควรมีการบริหารภาวะวิกฤต (crisis management) เพื่อรองรับกรณีเหตุการณ์ผิดปกติที่เพิ่มระดับความรุนแรงหรือมีความยืดเยื้อ อย่างน้อย ดังนี้

(1) กำหนดโครงสร้างการบริหารภาวะวิกฤตที่ชัดเจน ตั้งแต่ การกำหนดบทบาทหน้าที่ ขั้นตอนการสั่งการและการตัดสินใจ โดยควรประกอบด้วยผู้บริหารระดับสูงจากฝ่ายงานต่าง ๆ เพื่อให้สามารถพิจารณาประเมินสถานการณ์ได้อย่างครอบคลุม และตัดสินใจแก้ไขสถานการณ์ได้อย่างรวดเร็วทันการณ์ บรรเทาผลกระทบหรือความเสียหายและสามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง ตลอดจนกำกับดูแลการดำเนินการต่าง ๆ จนสถานการณ์กลับสู่ภาวะปกติ

(2) กำหนดปัจจัย และเงื่อนไขที่จำเป็นต้องเริ่มต้นใช้กระบวนการบริหารภาวะวิกฤติ ตามโครงสร้างการบริหารภาวะวิกฤตที่กำหนด

(3) กำหนดทีมงานรับผิดชอบดำเนินการด้านต่าง ๆ ได้แก่ ด้านสถานที่ ด้านบุคลากร ด้านธุรกิจ ด้านเทคโนโลยีสารสนเทศ ด้านความปลอดภัย ด้านสื่อสารองค์กร เป็นต้น

ในการประเมินลักษณะและผลกระทบของความเสียหายที่เกิดขึ้น พิจารณาแนวทางบรรเทาผลกระทบและแนวทางรองรับธุรกิจอย่างต่อเนื่อง

(4) กำหนดแผนงาน และขั้นตอนในการดำเนินการ และสนับสนุนการตัดสินใจในภาวะวิกฤต ครอบคลุมการกู้คืนการดำเนินงาน เพื่อนำเสนอต่อผู้มีอำนาจตัดสินใจตามโครงสร้างการบริหารภาวะวิกฤต

(5) จัดเตรียมทรัพยากร และเครื่องมือที่ช่วยสนับสนุนให้เพียงพอที่จะทราบ และประเมินสถานการณ์ในภาวะวิกฤตที่เกิดขึ้นอย่างเป็นปัจจุบัน และทันท่วงที

(6) จัดทำรายชื่อผู้ที่มีความเกี่ยวข้องทั้งภายใน และภายนอกองค์กรที่จำเป็นต้องรับทราบและติดต่อสื่อสารในกรณีที่ธุรกรรมสำคัญเกิดเหตุการณ์ผิดปกติหรือหยุดชะงัก โดยควรกำหนดแผน รูปแบบการสื่อสารเอาไว้ให้เหมาะสมกับผู้ที่มีความเกี่ยวข้องในแต่ละกลุ่ม รวมไปถึงช่องทางในการสื่อสารต่อผู้ที่เกี่ยวข้อง

6.3 การสื่อสารต่อบุคลากรภายในองค์กรในกรณีเกิดเหตุการณ์ผิดปกติร้ายแรงหรืออยู่ในภาวะวิกฤต ควรกำหนดช่องทางในการสื่อสารภายในองค์กรอย่างชัดเจน ทันการณ์ และมีข้อมูลเพียงพอที่ให้บุคลากรภายในองค์กรสามารถหลีกเลี่ยงอันตรายที่อาจเกิดขึ้นจากเหตุการณ์ที่เกิดขึ้น

6.4 การติดต่อสื่อสารต่อผู้ที่มีความเกี่ยวข้ององค์กร ได้แก่ ลูกค้า สื่อมวลชน หน่วยงานของรัฐ หน่วยงานกำกับดูแล และอื่นๆ เพื่อสามารถแจ้งเหตุได้ทันท่วงทีและป้องกันมิให้เกิดความตื่นตระหนกต่อสาธารณชนในช่วงที่เกิดสถานการณ์ผิดปกติหรือหยุดชะงัก หรือเกิดภาวะวิกฤต โดยควรดำเนินการ ดังนี้

(1) ควรมีการวางแผนการติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอกสถาบันการเงิน ตลอดจนพิจารณาความเป็นไปได้ในการเกิดผลกระทบต่อผู้ที่เกี่ยวข้องในต่างประเทศเมื่อเกิดการหยุดชะงักขึ้นด้วย โดยควรระบุ

(1.1) ผู้รับผิดชอบ

(1.2) ขอบเขตอำนาจหน้าที่ในการสื่อสาร

(1.3) ขั้นตอนและช่องทางในการสื่อสาร

(1.4) ระดับของข้อมูลที่เปิดเผย

(1.5) รายชื่อและเบอร์โทรศัพท์ของพนักงานและผู้เกี่ยวข้องภายนอก โดยอาจจัดทำในลักษณะผังรายชื่อ (call tree)

(1.6) แนวทางการติดต่อสื่อสารกับผู้ที่เกี่ยวข้องทั้งภายในและภายนอก และ/หรือในต่างประเทศหากการหยุดดำเนินงานดังกล่าวมีผลกระทบต่อระบบการเงินระหว่างประเทศ

(2) ในกรณีที่เหตุการณ์ที่เกิดขึ้นเกี่ยวข้องกับสถาบันการเงินอื่น หรือเกิดผลกระทบในวงกว้าง สถาบันการเงินควรประสานงานระหว่างกัน เพื่อให้การสื่อสารต่อสาธารณะชนมีความสอดคล้องกัน

(3) ต้องมีการรายงานเหตุการณ์ผิดปกติตามหลักเกณฑ์ ธปท. ที่เกี่ยวข้อง ได้แก่ (1) การรายงานการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายหรือกฎเกณฑ์ตามหลักเกณฑ์ ธปท. ว่าด้วยการกำกับการปฏิบัติตามกฎเกณฑ์ (compliance) ของสถาบันการเงิน และกลุ่มธุรกิจทางการเงิน (2) การรายงานข้อมูลกรณีฉุกเฉินหรือมีเหตุสุดวิสัยที่จำเป็นและมิอาจหลีกเลี่ยงได้ ซึ่งธนาคารพาณิชย์มีการเปลี่ยนแปลงการให้บริการที่กระทบกับผู้ใช้บริการในวงกว้างตามหลักเกณฑ์ ธปท. ว่าด้วย หลักเกณฑ์เกี่ยวกับช่องทางให้บริการของธนาคารพาณิชย์ (3) การรายงานเหตุการณ์หรือการกระทำทุจริตตามหลักเกณฑ์ ธปท. ว่าด้วยหลักเกณฑ์การปฏิบัติงานตรวจสอบภายใน (internal audit) ของสถาบันการเงินและกลุ่มธุรกิจทางการเงิน และ (4) การรายงานปัญหาด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์ ธปท. ว่าด้วยการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk) ของสถาบันการเงิน

เอกสารอ้างอิง

- **Principles for Operational Resilience** – Basel Committee on Banking Supervision (BCBS) มีนาคม 2564
- **Supervisory Policy Manual : Operational Resilience** – Hong Kong Monetary Authority (HKMA) พฤษภาคม 2565
- **Business Continuity Management Guidelines** – Monetary Authority of Singapore (MAS) มิถุนายน 2565
- **RISK MANAGEMENT AND OPERATIONAL RESILIENCE IN A REMOTE WORKING ENVIRONMENT** – Monetary Authority of Singapore (MAS) มีนาคม 2564
- **แนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของสถาบันการเงิน** - ธนาคารแห่งประเทศไทย สิงหาคม 2551
- **แนวปฏิบัติธนาคารแห่งประเทศไทยเรื่องการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับกรณีการระบาดของโรคติดต่อร้ายแรง** - ธนาคารแห่งประเทศไทย สิงหาคม 2551
- **IT Risk Management Implementation Guideline แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ** - ธนาคารแห่งประเทศไทย กุมภาพันธ์ 2564