# การเปิดเผยข้อมูลการบริหารความเสี่ยงด้านปฏิบัติการ

## ความเสี่ยงด้านปฏิบัติการ

ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก รวมถึงความเสี่ยงด้านกฎหมาย แต่ไม่รวมความเสี่ยงด้านกลยุทธ์ (Strategic risk) และความเสี่ยงด้านชื่อเสียง (Reputational risk)

## ภาพรวมการบริหารความเสี่ยงด้านปฏิบัติการของ ธสน.

ธสน. กำหนดนโยบายการบริหารความเสี่ยงด้านปฏิบัติการ ภายใต้กรอบแนวทางของธนาคารแห่งประเทศไทย (ธปท.) กรอบแนวคิดตาม COSO Internal Control 2013 และหลักเกณฑ์การประเมินกระบวนการปฏิบัติงานและการจัดการ Enablers ของรัฐวิสาหกิจ (Statement Enterprise Assessment Model: SE-AM) ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง ด้านการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control: RM&IC) เพื่อให้แนวทางการบริหารความเสี่ยงด้านปฏิบัติการของ ธสน. เป็นไปตามมาตรฐานสากล ตลอดจนสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสีย รวมทั้งช่วยสร้างมูลค่าเพิ่มให้กับ ธสน. อย่างยั่งยืนในระยะยาว

ในปี 2568 ธสน. ปรับปรุงระบบงานและกระบวนการปฏิบัติงานให้มีประสิทธิภาพมากขึ้น โดยดำเนินการการควบคู่ไปกับการทบทวนการประเมินความเสี่ยงและการควบคุมภายในของตนเอง (Risk and Control Self-Assessment : RCSA) เพื่อให้มั่นใจว่าการบริหารความเสี่ยงด้านปฏิบัติการเป็นไปอย่างมีประสิทธิภาพ โดยมีการปรับปรุงกิจกรรมการควบคุมให้เหมาะสม/รัดกุมยิ่งขึ้น เพื่อลดโอกาสที่จะเกิดความเสี่ยงและ/หรือลดระดับความเสียหายที่อาจจะเกิดขึ้น เช่น การปรับโครงสร้างฝ่ายงานของสายงานวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) เพื่อแบ่งแยกบทบาทหน้าที่ให้ชัดเจน และเพิ่มความรัดกุมในการปฏิบัติงาน การกำหนดกระบวนการในการตรวจสอบข้อมูลผู้สอบบัญชี และบัญชีม้าจากฐานข้อมูลระบบ CFR เพื่อรองรับความเสี่ยงที่เกิดจากการทุจริตที่เกี่ยวเนื่องกับผลิตภัณฑ์และบริการของธนาคาร และมีการสื่อสารเพื่อสร้างความรู้ ความเข้าใจ และความตระหนักในการบริหารความเสี่ยงผ่านช่องทางต่างๆ โดยมุ่งเน้นให้เกิดวัฒนธรรมด้านความเสี่ยง (Risk Culture) ภายในองค์กร อาทิ การสื่อสารผ่านโครงการบูรณาการ 2nd และ 3rd Line of Defence การสื่อสารในรูปแบบ One page ผ่านทาง E-mail และระบบ Knowledge Management (KM Portal) โดยมีการสำรวจการรับรู้และนำผลลัพธ์มาปรับปรุงอย่างต่อเนื่อง

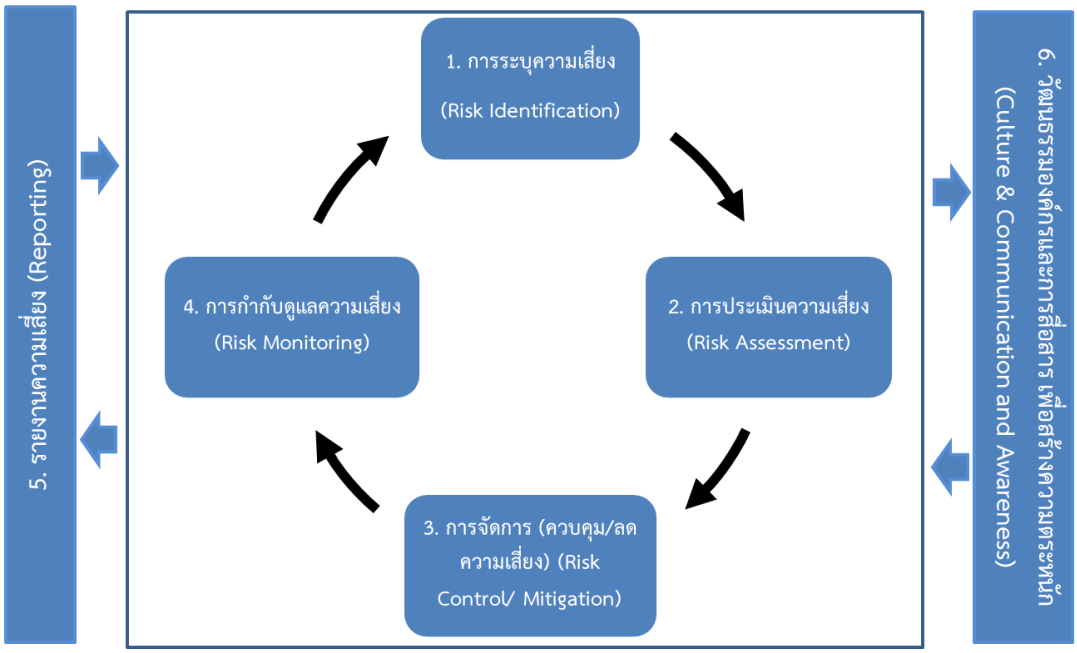
นอกจากนี้ ธสน. ได้ทบทวนนโยบาย แนวปฏิบัติ และปรับปรุงแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และจัดให้มีการซ้อมแผนโดยกำหนดสถานการณ์จำลองครอบคลุมทั้งสำนักงานใหญ่ สาขา และสำนักงานผู้แทนในต่างประเทศ รวมถึงมีการทดสอบการซ้อมรับการโจมตีทางไซเบอร์ เพื่อให้มั่นใจว่า ธสน. สามารถดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดเหตุฉุกเฉินต่าง ๆ

และลดผลกระทบที่อาจเกิดขึ้นต่อพนักงาน ลูกค้า คู่ค้า พันธมิตร หรือบุคคลที่เกี่ยวข้องอื่น ๆ รวมถึงมีการซักซ้อมแผนและทดสอบกับหน่วยงานภายนอก เช่น ธนาคารแห่งประเทศไทย ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด (NCB) และ บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด (National ITMX) เป็นต้น เพื่อให้ครอบคลุมและพร้อมรองรับกับเหตุฉุกเฉินที่อาจเกิดขึ้น ทั้งนี้ ในปี 2568 ธสน. ได้เพิ่มการทดสอบแผนฉุกเฉินสภาพคล่องเพื่อให้มั่นใจว่าแผนฉุกเฉินสภาพคล่องมีความเหมาะสม และสามารถนำไปปฏิบัติได้จริงในสถานการณ์ฉุกเฉินอีกด้วย

**การบริหารจัดการความเสี่ยงด้านปฏิบัติการ**

ธสน. ดำเนินการตามกระบวนการบริหารความเสี่ยงด้านปฏิบัติการมาอย่างต่อเนื่อง และเป็นไปตามมาตรฐานสากล เพื่อเป็นกรอบในการบริหารจัดการความเสี่ยงอย่างเป็นระบบ โดยครอบคลุมการปฏิบัติงานทั้งกระบวนการตั้งแต่ต้นจนจบ (End to End Process) เพื่อให้ ธสน. สามารถบรรลุเป้าหมายที่กำหนดภายใต้ระดับความเสี่ยงที่ยอมรับได้ โดยแบ่งออกเป็น 6 กระบวนการ ดังรูปด้านล่าง

**กระบวนการบริหารความเสี่ยงด้านปฏิบัติการ**




ธสน. มีเครื่องมือในการบริหารความเสี่ยงด้านปฏิบัติการที่สำคัญ ดังนี้

- การประเมินความเสี่ยงและการควบคุมภายในของตนเอง (RCSA) ตามหลัก COSO Internal Control 2013 อย่างน้อยปีละ 1 ครั้ง ซึ่งทุกฝ่ายงานมีหน้าที่ความรับผิดชอบโดยตรงในการบริหารความเสี่ยงด้านปฏิบัติการของฝ่ายงานตนเอง เพื่อระบุความเสี่ยงด้านปฏิบัติการได้อย่างครบถ้วนถูกต้อง ทบทวนปัจจัยเสี่ยงและกิจกรรมการควบคุมตามแนวทางที่เหมาะสม รวมถึงดำเนินการลด

ความเสี่ยง โดยมีการติดตามความคืบหน้าของกิจกรรมการควบคุมอย่างสม่ำเสมอ และรายงานต่อคณะจัดการ คณะกรรมการกำกับความเสี่ยง และคณะกรรมการธนาคาร เพื่อทราบ

- การทบทวนดัชนีชี้วัดความเสี่ยง (Key Risk Indicators: KRIs) ด้านปฏิบัติการ ทั้ง Leading และ Lagging Indicator โดยกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Tolerance) เพื่อใช้ในการกำหนด Limit สำหรับควบคุมและติดตามความเสี่ยงด้านปฏิบัติการให้อยู่ในระดับที่เหมาะสม และสามารถจัดการความเสี่ยงด้านปฏิบัติการได้อย่างทันท่วงที
- การกำหนดให้ฝ่ายงานต่าง ๆ จัดทำ/ทบทวนคู่มือการปฏิบัติงาน เพื่อให้เป็นปัจจุบันอยู่เสมอ ครอบคลุมกระบวนการปฏิบัติงานสำคัญ และเป็นไปตามมาตรฐานเดียวกันทั่วทั้งองค์กร
- การจัดเก็บและรายงานเหตุการณ์ความเสียหายที่เกิดขึ้นจากความเสี่ยงด้านปฏิบัติการ (Loss Data) และเหตุการณ์ที่เกิดขึ้นแต่สามารถป้องกันความเสียหายไว้ได้ (Near-Misses) จากฝ่ายงานที่เป็นเจ้าของความเสี่ยง (Risk Originator) และฝ่ายงานที่ไม่ใช่เจ้าของความเสี่ยง (Non-Risk Originator) เพื่อกำหนดกิจกรรมการควบคุม (Control Activities) ที่เหมาะสม รวมทั้งกำหนดให้มีการนำรายงานฯ ดังกล่าว มาวิเคราะห์พิจารณาใช้ในการปรับปรุง/ทบทวน RCSA และคู่มือการปฏิบัติงานให้เหมาะสมและมีประสิทธิภาพยิ่งขึ้น
- การจัดทำแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ทั้งสำนักงานใหญ่ สาขา และสำนักงานผู้แทนในต่างประเทศ เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่องหากเกิดเหตุฉุกเฉิน/ภัยพิบัติ และกำหนดให้ฝ่ายงานที่เกี่ยวข้องมีการทดสอบแผนฯ เป็นประจำทุกปี
- การสื่อสารการบริหารความเสี่ยงทั่วทั้งองค์กรผ่านช่องทางต่าง ๆ เพื่อสร้างวัฒนธรรมด้านความเสี่ยงที่เข้มแข็ง (Sound Risk Culture) และส่งเสริมให้เกิดความตระหนัก/ระมัดระวัง ความรู้และความเข้าใจ เพื่อป้องกันความเสี่ยงก่อนที่จะเกิดความเสียหาย และมีการสื่อสารจากระดับกรรมการ กรรมการผู้จัดการ และผู้บริหารระดับสูงถ่ายทอดมายังระดับพนักงาน เพื่อเป็นแบบอย่างที่ดี (Tone from the top) รวมถึงมีการสื่อสารแบบ Bottom up ผ่านการประชุม Town Hall ช่องทาง E-mail และระบบ KM Portal เป็นต้น

อีกทั้ง มีช่องทางการรับข้อร้องเรียนและแจ้งเบาะแสสำหรับพนักงานภายในและผู้มีส่วนได้ส่วนเสียภายนอก เพื่อรวบรวมคำแนะนำและข้อคิดเห็นจากช่องทางต่าง ๆ นำไปสู่การพัฒนาและปรับปรุงอย่างเหมาะสม ทั้งนี้ ธสน. ใช้วิธี Basic Indicator Approach (BIA) ในการคำนวณความเพียงพอของเงินกองทุนเพื่อรองรับความเสี่ยงด้านปฏิบัติการ ซึ่งเป็นไปตามแนวทางที่ ธปท. กำหนด

**โครงสร้างและหน้าที่ความรับผิดชอบ**

ธสน. ให้ความสำคัญกับการสร้างและพัฒนาสภาพแวดล้อมขององค์กรให้เอื้อต่อการบริหารความเสี่ยงด้านปฏิบัติการ ซึ่งคณะกรรมการ ผู้บริหารระดับสูง และพนักงาน ล้วนมีส่วนสำคัญในการสร้างและขับเคลื่อน ธสน. ให้มีสภาพแวดล้อมในการบริหารความเสี่ยงด้านปฏิบัติการอย่างเหมาะสม โดยได้

กำหนดบทบาทหน้าที่ความรับผิดชอบ ออกเป็น 3 ระดับ (Three Lines of Defence) เพื่อให้มั่นใจว่าธนาคารมีการบริหารจัดการความเสี่ยงด้านปฏิบัติการได้อย่างมีประสิทธิภาพ ซึ่งสามารถสรุปได้ดังนี้

1. **ระดับปฏิบัติงาน (1st Line of Defence)**

   คือ ฝ่ายงานต่าง ๆ รวมถึงผู้บริหารและพนักงาน ซึ่งเป็นเจ้าของความเสี่ยงในงานของตนเอง มีหน้าที่ในการปฏิบัติงานในความรับผิดชอบให้เป็นไปตามนโยบาย หลักเกณฑ์ และคู่มือที่กำหนดไว้ โดยมีการควบคุมภายในและการบริหารจัดการความเสี่ยงที่เหมาะสม สามารถระบุ ประเมิน ควบคุมและติดตาม พร้อมทั้งรายงานความเสี่ยงตามแนวทางของธนาคาร เพื่อให้มั่นใจว่าความเสี่ยงอยู่ในระดับที่ยอมรับได้

2. **ระดับการบริหารความเสี่ยง (2nd Line of Defence)**

   ประกอบด้วย 3 ฝ่าย คือ ฝ่ายบริหารความเสี่ยงองค์กร ฝ่ายบริหารความเสี่ยงด้านเครดิต และฝ่ายกำกับการปฏิบัติงาน โดยฝ่ายบริหารความเสี่ยงองค์กรมีหน้าที่จัดทำกรอบการกำกับดูแลความเสี่ยงและการควบคุมภายในที่ดี นโยบายการบริหารความเสี่ยงด้านปฏิบัติการ และนโยบายการบริหารความต่อเนื่องทางธุรกิจ รวมถึงหลักเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง โดยครอบคลุมถึงการติดตาม สนับสนุน และสื่อสารให้ทุกฝ่ายงานเกิดความตระหนักถึงความสำคัญของการบริหารความเสี่ยงด้านปฏิบัติการ และสามารถดำเนินการตามแนวทางที่กำหนดไว้ได้อย่างเหมาะสม

   ฝ่ายบริหารความเสี่ยงด้านเครดิต มีหน้าที่จัดทำกรอบการกำกับดูแลความเสี่ยงด้านเครดิตของธนาคาร ครอบคลุมทั้งสินเชื่อและบริการประกัน เพื่อป้องกันความสูญเสียในกรณีที่ลูกหนี้หรือคู่สัญญาไม่สามารถชำระหนี้ได้ตามสัญญา รวมถึงความเสี่ยงอื่นที่เกี่ยวข้องด้านการให้สินเชื่อ

   สำหรับฝ่ายกำกับการปฏิบัติงาน มีหน้าที่จัดทำนโยบายด้านการกำกับการปฏิบัติตามกฎเกณฑ์และกำกับ ติดตาม ควบคุมการปฏิบัติงานให้เป็นไปตามกฎหมาย ข้อบังคับ และกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง เพื่อดูแลให้มีการปฏิบัติตามกฎเกณฑ์ทั้งภายในและภายนอกที่เกี่ยวข้อง

   โดยทั้ง 3 ฝ่ายงานมีรายงานผลการดำเนินงานในด้านต่าง ๆ ต่อคณะกรรมการกำกับความเสี่ยงอย่างสม่ำเสมอ

3. **ระดับการตรวจสอบ (3rd Line of Defence)**

   คือ ฝ่ายตรวจสอบ รับผิดชอบในการทำหน้าที่สอบทานการปฏิบัติงานในภาพรวมและการปฏิบัติงานของระดับปฏิบัติงาน (1st Line of Defence) และระดับการบริหารความเสี่ยง (2nd Line of Defence) รวมถึงการสอบทานความเหมาะสมและประสิทธิผลของการควบคุมภายในตลอดจนตรวจสอบการดำเนินงานตามแผนงานหรือโครงการต่าง ๆ ซึ่งภาระหน้าที่ของฝ่ายตรวจสอบนั้นจะต้องไม่ขัดต่อความเป็นอิสระและความซื่อสัตย์สุจริต

โดย ธสน. ได้จัดทำกฎบัตรการตรวจสอบภายใน เพื่อสื่อสารให้ผู้บริหารและพนักงานทุกระดับได้ทราบถึงวัตถุประสงค์ ขอบเขตการปฏิบัติงาน ความรับผิดชอบ ความเป็นอิสระ ภาระหน้าที่ และสิทธิของผู้ตรวจสอบภายใน รวมทั้งการปฏิบัติตรวจสอบของฝ่ายตรวจสอบที่ตั้งอยู่บนหลักการตามมาตรฐานการปฏิบัติงานวิชาชีพการตรวจสอบที่เป็นสากล เพื่อสร้างสรรค์ความเข้าใจและความร่วมมือในการปฏิบัติงานระหว่างหน่วยงานต่าง ๆ ซึ่งจะก่อให้เกิดการประสานประโยชน์โดยรวมของ ธสน.

ทั้งนี้ อำนาจหน้าที่ และความรับผิดชอบที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านปฏิบัติการของ ธสน. แบ่งเป็น 4 ระดับ คือ ระดับกรรมการ ระดับจัดการ ระดับผู้บริหารระดับสูง และระดับฝ่ายงาน สรุปได้ดังนี้