(ร่าง) หลักเกณฑ์การบริหารจัดการความเสี่ยง
ในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

<u>เค้าโครงร่างหลักเกณฑ์</u>

1. การกำหนดนโยบายการบริหารความเสี่ยง เพื่อประเมินฐานะและผลการดำเนินงาน
2. การกำกับดูแลความเสี่ยง และกระบวนการบริหารจัดการความเสี่ยง ซึ่งต้องครอบคลุมกระบวนการดังนี้
   (1) การระบุความเสี่ยง (Risk identification)
   (2) การประเมินความเสี่ยง (Risk assessment)
   (3) การวัดผลความเสี่ยงกับเกณฑ์ประเมินความเสี่ยง (Risk evaluation)
   (4) การลดความเสี่ยงหลังจากการประเมิน (Risk treatment)
   (5) การติดตามและรายงานผลความเสี่ยงอย่างต่อเนื่อง (Risk monitoring and reporting)
3. การระบุความเสี่ยงที่เกี่ยวข้องกับระบบฯ โดยครอบคลุมความเสี่ยง 5 ด้าน
   (1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)
   (2) ความเสี่ยงด้านการปฏิบัติการ (Operational Risk)
   (3) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)
   (4) ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk)
   (5) ความเสี่ยงด้านการปฏิบัติตามหลักเกณฑ์ (Compliance Risk)
4. การประเมินการปฏิบัติตามแนวทางการบริหารจัดการความเสี่ยงที่แนบท้าย และการจัดส่งผลการประเมิน
5. การทบทวนการประเมินความเสี่ยงประจำปี และในกรณีมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

หลักเกณฑ์การบริหารจัดการความเสี่ยง
ในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

1. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายและมาตรการบริหารจัดการความเสี่ยงซึ่งครอบคลุมความเสี่ยงที่เกี่ยวข้องกับบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประเมินฐานะและผลการดำเนินงาน โดยคำนึงถึงผลกระทบจากความเสี่ยงของการให้บริการเพื่อกำหนดมาตรการและแผนการบรรเทาผลกระทบที่อาจจะเกิดขึ้นอย่างทันท่วงที
2. ผู้รับใบอนุญาตต้องเข้าใจและตระหนักถึงความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ส่งผลกระทบต่อผู้ที่เกี่ยวข้อง รวมถึงบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมกระบวนการในการบริหารจัดการความเสี่ยงดังนี้
   (1) การระบุความเสี่ยงที่เกี่ยวข้องกับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Risk identification) ตามลักษณะของการให้บริการ
   (2) การประเมินความเสี่ยง (Risk assessment) ซึ่งครอบคลุมการประเมินความเสี่ยงตั้งต้นและการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง
   (3) การวัดผลความเสี่ยงกับเกณฑ์การประเมินความเสี่ยง (Risk evaluation)
   (4) การลดความเสี่ยงหลังจากการประเมิน เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Risk treatment)
   (5) การติดตามและรายงานผลความเสี่ยงอย่างต่อเนื่อง (Risk monitoring and reporting)
3. ในการระบุความเสี่ยงที่เกี่ยวข้องกับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ต้องดำเนินการให้ครอบคลุมความเสี่ยง 5 ด้าน ได้แก่
   (1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงของการสูญเสียที่เกิดขึ้นจากการตัดสินใจทางธุรกิจที่ไม่พึงประสงค์ การตัดสินใจทางธุรกิจที่ไม่ดี หรือการไม่ตอบสนองต่อการเปลี่ยนแปลงในอุตสาหกรรมและสภาพแวดล้อมในการดำเนินงาน ทั้งนี้ ความเสี่ยงด้านกลยุทธ์สำหรับผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล มีความคล้ายคลึงกับความเสี่ยงขององค์กรทั่วไป โดยมีปัจจัยที่ต้องคำนึงถึง เช่น นโยบาย แผนกลยุทธ์ และการจัดสรรงบประมาณ อิทธิพลในการตัดสินใจเชิงกลยุทธ์ การบริหารความเสี่ยงในระดับองค์กร เป็นต้น
   (2) ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก เช่น ความเสี่ยงจากการฉ้อโกงโดยบุคคลภายในและบุคคลภายนอก ความเสี่ยงจากการขัดข้องหรือหยุดชะงักของระบบงาน ความเสี่ยงจากแนวปฏิบัติเกี่ยวกับผู้ใช้บริการ การให้บริการและดำเนินธุรกิจ เป็นต้น
   (3) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) หมายถึง ความเสี่ยงของผลลัพธ์ที่ไม่พึงประสงค์ ความเสียหาย การสูญเสีย การละเมิด ความล้มเหลวหรือการหยุดชะงักใดๆ ที่อาจเกิดขึ้นจากการใช้หรือการพึ่งพาฮาร์ดแวร์คอมพิวเตอร์ ซอฟต์แวร์ อุปกรณ์ ระบบ แอปพลิเคชัน และเครือข่าย ความเสี่ยงนี้มักเกี่ยวข้องกับข้อบกพร่องของระบบ ข้อผิดพลาดในการประมวลผล ข้อบกพร่องของซอฟต์แวร์

ข้อผิดพลาดในการทำงาน ความล้มเหลวของฮาร์ดแวร์ ความล้มเหลวของระบบ ความไม่เพียงพอของความจุ ช่องโหว่ของเครือข่าย จุดอ่อนในการควบคุม ข้อบกพร่องด้านความปลอดภัย การโจมตีที่เป็นอันตราย เหตุการณ์การเจาะระบบ โดยทั่วไปความเสี่ยงด้านเทคโนโลยีสำหรับผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล ตัวอย่างเช่น ภัยคุกคามทางไซเบอร์ การรั่วไหลของข้อมูล รวมถึงข้อมูลอ่อนไหวซึ่งมักเป็นองค์ประกอบสำคัญในธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(4) ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk) หมายถึง ความเสี่ยงที่ทำให้ผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้รับผลกระทบทางลบจากสังคม ส่งผลให้สูญเสียชื่อเสียงและความน่าเชื่อถือในการให้บริการ ตัวอย่างเช่น การเปิดเผยข้อมูลส่วนบุคคลของผู้ให้บริการโดยไม่ได้ตั้งใจ เป็นต้น

(5) ความเสี่ยงด้านการปฏิบัติตามหลักเกณฑ์ (Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการที่ผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัลไม่สามารถปฏิบัติงานสอดคล้องตามที่กฎหมาย กฎระเบียบหรือมาตรฐานที่เกี่ยวข้องกับการประกอบธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลกำหนด ทั้งนี้รวมถึงมาตรฐานสากลที่กฎหมายหรือกฎระเบียบอ้างถึงด้วย ตัวอย่างเช่น ไม่มีการปฏิบัติตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต เป็นต้น

4. ผู้รับใบอนุญาตต้องดำเนินการให้สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่แนบท้าย พร้อมจัดส่งผลการประเมินต่อสำนักงานตามรูปแบบและระยะเวลาที่สำนักงานกำหนด โดยผู้บริหารหรือผู้ที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศรับรองผลการประเมินตนเองก่อนนำส่งต่อสำนักงาน
5. ผู้รับใบอนุญาตต้องจัดให้มีการทบทวนจัดให้มีนโยบายและมาตรการบริหารจัดการความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการให้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
