ธนาคารแห่งประเทศไทย

29 กันยายน 2566

เรียน ผู้จัดการ

สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง
ผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจบัตรเครดิตที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับที่มิใช่สถาบันการเงินทุกแห่ง

ที่ ธปท.ฝนช.(09) ว. 689 /2566 เรื่อง นำส่งแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน

ธนาคารแห่งประเทศไทย (ธปท.) ได้ออกแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน โดยมีวัตถุประสงค์เพื่อให้ผู้ให้บริการทางการเงินที่มีการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงิน ใช้อ้างอิงเป็นมาตรฐานเพื่อให้มั่นใจว่าการให้บริการที่เกี่ยวข้องกับเทคโนโลยีชีวมิติมีความมั่นคงปลอดภัย สอดคล้องกับมาตรฐานสากล ซึ่งจะช่วยยกระดับการให้บริการทางการเงินและก่อให้เกิดประโยชน์แก่ผู้ใช้บริการ

แนวปฏิบัตินี้ครอบคลุมหลักการพึงปฏิบัติที่สำคัญในการใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงิน ตั้งแต่ระดับนโยบายขององค์กรไปจนถึงแนวทางดำเนินการและการบริหารความเสี่ยงในการใช้เทคโนโลยีชีวมิติตลอดทั้งวงจรชีวิต (life cycle) ของข้อมูล รวมถึงการคุ้มครองผู้ใช้บริการและปฏิบัติตามกฎหมายที่เกี่ยวข้อง และมีรายละเอียดมาตรฐานเชิงเทคนิคสำหรับการใช้เทคโนโลยีการเปรียบเทียบใบหน้า ซึ่งเป็นเทคโนโลยีหลักที่มีการใช้งานในภาคการเงินในปัจจุบัน โดย ธปท. ได้จัดทำแนวปฏิบัตินี้ขึ้นโดยอ้างอิงจากมาตรฐานสากล และการประเมินโครงการทดสอบการใช้เทคโนโลยีชีวมิติในกระบวนการรู้จักลูกค้าภายใต้ Regulatory sandbox ทั้งนี้ ในระยะต่อไป หากมีการนำเทคโนโลยีชีวมิติในรูปแบบอื่นมาให้บริการ ธปท. จะพิจารณากำหนดมาตรฐานเชิงเทคนิคเพิ่มเติมเพื่อเป็นมาตรฐานที่ดีในการนำไปใช้ต่อไป

สำหรับผู้ให้บริการทางการเงินที่ประสงค์จะนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงิน ต้องปฏิบัติตามแนวทางดังนี้

1. ผู้ให้บริการทางการเงินต้องถือปฏิบัติตามแนวปฏิบัติฉบับนี้อย่างครบถ้วน โดยคำนึงถึงประสิทธิภาพความแม่นยำของเทคโนโลยีที่เลือกใช้ การรักษาความปลอดภัยของข้อมูลลูกค้า และการปฏิบัติตามกฎหมายที่เกี่ยวข้องโดยเฉพาะกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

2. ผู้ให้บริการทางการเงินที่มีความประสงค์จะประยุกต์ใช้เทคโนโลยีชีวมิติประเภทเปรียบเทียบภาพใบหน้าของผู้ใช้บริการ (Facial Recognition) ในกระบวนการพิสูจน์ตัวตนลูกค้าต้องปฏิบัติตามหลักเกณฑ์ของ ธปท. ที่เกี่ยวข้อง ได้แก่ หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน

ทั้งนี้ ผู้ให้บริการทางการเงินต้องนำส่งรายงานการตรวจประเมินการประยุกต์ใช้เทคโนโลยีชีวมิติ (Biometrics) ในการให้บริการทางการเงินเพื่อประกอบการพิจารณาและต้องได้รับความเห็นชอบจาก ธปท. ก่อนให้บริการ

3. ผู้ให้บริการทางการเงินที่ประยุกต์ใช้เทคโนโลยีชีวมิติเพื่อเปรียบเทียบภาพใบหน้าสำหรับกระบวนการรู้จักตัวตนลูกค้าและผ่านการทดสอบภายใต้ regulatory sandbox ของ ธปท. แล้ว สามารถประยุกต์ใช้เทคโนโลยีดังกล่าวกับธุรกรรมการเปิดบัญชีเงินฝาก การเปิดใช้บริการเงินอิเล็กทรอนิกส์ และธุรกรรมอื่นที่มีการพิสูจน์ตัวตนในลักษณะเดียวกัน เช่น การสมัครใช้บริการสินเชื่อ ได้ในวงกว้าง

ทั้งนี้ ผู้ให้บริการทางการเงินที่ผ่านการทดสอบแล้วยังคงต้องรายงานข้อมูลการใช้เทคโนโลยีชีวมิติแก่ ธปท. อย่างต่อเนื่อง ตามรายละเอียดและช่วงเวลาที่กำหนด ตามแบบรายงานการใช้ข้อมูลชีวมิติ จนกว่าจะนำส่งรายงานการตรวจประเมินการประยุกต์ใช้เทคโนโลยีชีวมิติ (Biometrics) ในการให้บริการทางการเงินและได้รับความเห็นชอบจาก ธปท.

4. การประยุกต์ใช้เทคโนโลยีชีวมิติเพื่อเปรียบเทียบภาพใบหน้ากับธุรกรรมอื่น เช่น ธุรกรรมการโอนเงิน ธุรกรรมการชำระเงิน ซึ่งมีความเสี่ยง (risk profile) ที่แตกต่างไปจากการเปิดบัญชีเงินฝากหรือการเปิดใช้บริการเงินอิเล็กทรอนิกส์ หรือกับรูปแบบการให้บริการในลักษณะอื่นนอกเหนือจากข้อ 2. และข้อ 3. ให้ผู้ให้บริการทางการเงินหารือ ธปท. ก่อนดำเนินการ

5. การประยุกต์ใช้เทคโนโลยีชีวมิติประเภทอื่นที่นอกเหนือจากการใช้เทคโนโลยีชีวมิติเพื่อเปรียบเทียบภาพใบหน้าให้หารือ ธปท. ก่อนดำเนินการ

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวสิริธิดา พนมวัน ณ อยุธยา)
ผู้ช่วยผู้ว่าการ สายกำกับระบบการชำระเงิน
และคุ้มครองผู้ใช้บริการทางการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน
2. แบบรายงานการใช้ข้อมูลชีวมิติ
3. แบบรายงานการตรวจประเมินการใช้เทคโนโลยีชีวมิติ (Biometrics) ในการให้บริการทางการเงิน
4. คำถามพบบ่อย (FAQ)

ฝ่ายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
โทรศัพท์ 0 2283 6892
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 5827

หมายเหตุ [ ] ธนาคารแห่งประเทศไทยจะจัดให้มีการประชุมชี้แจงในวันที่ ..... ณ .....
[x] ไม่มีการจัดประชุมชี้แจง

แนวปฏิบัติ
การใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน

กันยายน 2566

ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายนโยบายระบบชำระเงินและเทคโนโลยีทางการเงิน

ฝ่ายกำกับและตรวจสอบเทคโนโลยีสารสนเทศ

สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

ธนาคารแห่งประเทศไทย

โทรศัพท์ 0 2283 6892

0 2283 6816

e-mail: FinTechDept@bot.or.th

สารบัญ

หัวข้อ **หน้า**

1. เหตุผลในการออกแนวปฏิบัติ ... 3

2. แนวปฏิบัติที่ยกเลิก ... 4

3. ขอบเขตการใช้ ... 4

4. คำจำกัดความ ... 4

5. ภาพรวมการใช้เทคโนโลยีชีวมิติ ... 4

   5.1 หลักการทำงานของเทคโนโลยีชีวมิติ ... 4

   5.2 ประเด็นสำคัญที่ควรคำนึงถึงในการป้องกันความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีชีวมิติ ... 6

6. หลักการที่พึงปฏิบัติสำหรับผู้ให้บริการทางการเงิน ... 6

   หลักการที่ 1 กรอบนโยบายและการกำกับดูแลการใช้เทคโนโลยีชีวมิติ ... 7

   หลักการที่ 2 การรวบรวมข้อมูลชีวมิติของผู้ใช้บริการ ... 7

   หลักการที่ 3 การประมวลผลข้อมูลชีวมิติของผู้ใช้บริการ ... 8

   หลักการที่ 4 การรักษาความปลอดภัยข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการ ... 10

   หลักการที่ 5 การคุ้มครองผู้ใช้บริการ ... 12

   หลักการที่ 6 การควบคุมความเสี่ยงด้านปฏิบัติการ ... 13

ภาคผนวก ก ข้อกำหนดเกี่ยวกับมาตรฐานขั้นต่ำและแนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติ ... 15

แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน (Guideline for Biometric Technology Adoption in Financial Services)

1. เหตุผลในการออกแนวปฏิบัติ

เทคโนโลยีชีวมิติ (Biometric technology) เป็นเทคโนโลยีที่ใช้ในการจำแนกอัตลักษณ์ทางกายภาพของบุคคล เช่น ใบหน้า ลายนิ้วมือ หรืออัตลักษณ์ทางพฤติกรรมของบุคคล เช่น การพูด การเขียน เพื่อระบุ พิสูจน์หรือยืนยันตัวตนบุคคล ซึ่งเทคโนโลยีชีวมิติในปัจจุบันมีพัฒนาการที่ก้าวหน้าขึ้นเป็นอย่างมาก ทั้งด้านความแม่นยำในการระบุตัวตนบุคคลและความสะดวกในการใช้งาน และได้ถูกนำมาใช้เพิ่มประสิทธิภาพการให้บริการในภาคการเงินมากขึ้น โดยเฉพาะในการระบุ พิสูจน์ และยืนยันตัวตนผู้ใช้บริการ เช่น การรู้จักผู้ใช้บริการ (Know Your Customer : KYC) สำหรับการเปิดบัญชีหรือสมัครใช้บริการต่าง ๆ เพื่อลดโอกาสการเกิดทุจริตจากการปลอมแปลงตัวบุคคลที่เปิดบัญชีหรือทำธุรกรรมทางการเงิน และเพิ่มช่องทางการให้บริการทางออนไลน์ที่ช่วยให้ผู้ใช้บริการสะดวกขึ้นโดยสามารถรู้จักผู้ใช้บริการผ่านช่องทางอิเล็กทรอนิกส์ (e-KYC) ได้อย่างน่าเชื่อถือ รวมถึงการยืนยันตัวตนสำหรับการทำธุรกรรมอื่น ๆ เพื่อเพิ่มความสะดวกแก่ผู้ใช้บริการ

อย่างไรก็ตาม การนำเทคโนโลยีชีวมิติมาใช้กับบริการทางการเงินเป็นเรื่องเกี่ยวข้องกับการใช้อัตลักษณ์ทางกายภาพหรือพฤติกรรมของบุคคลซึ่งถือเป็นข้อมูลส่วนบุคคลที่สำคัญ หากมีการบริหารจัดการที่ไม่เหมาะสมอาจส่งผลกระทบต่อความเป็นส่วนตัวของบุคคล และความเชื่อมั่นต่อระบบสถาบันการเงินในภาพรวม จึงจำเป็นต้องให้ความสำคัญในหลายมิติ ทั้งความสามารถของเทคโนโลยีในการระบุ พิสูจน์ และยืนยันตัวตน การดูแลรักษาความปลอดภัยข้อมูลส่วนบุคคล รวมทั้งการคุ้มครองและให้ความรู้แก่ผู้ใช้บริการ

ที่ผ่านมา ผู้ให้บริการทางการเงินได้เข้าร่วมทดสอบการนำเทคโนโลยีชีวมิติมาประยุกต์ใช้ในการให้บริการทางการเงินในวงจำกัด ภายใต้แนวทางการเข้าร่วมทดสอบและพัฒนานวัตกรรมที่นำเทคโนโลยีใหม่มาสนับสนุนการให้บริการทางการเงิน (Regulatory sandbox) ของธนาคารแห่งประเทศไทย (ธปท.) โดยใช้เทคโนโลยีชีวมิติเพื่อยกระดับความปลอดภัยในการพิสูจน์ตัวตนของผู้ใช้บริการสำหรับการเปิดบัญชีเงินฝากและบัญชีเงินอิเล็กทรอนิกส์ (e-Money) โดยใช้การเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้ใช้บริการกับแหล่งข้อมูลที่เชื่อถือได้ (Trusted source) เช่น ภาพจากบัตรประจำตัวประชาชน หรือหนังสือเดินทาง และ ธปท. มีการประเมินผลการทดสอบและมีกระบวนการดูแลความเสี่ยงอย่างใกล้ชิด เพื่อให้ผู้ให้บริการทางการเงินมีการดูแลความเสี่ยงที่เกี่ยวข้อง และมีแนวทางคุ้มครองผู้ใช้บริการที่เหมาะสม

ธปท. สนับสนุนการนำเทคโนโลยีมาใช้ในการพัฒนานวัตกรรมทางการเงินที่เป็นประโยชน์ต่อภาคการเงินของประเทศโดยต้องมีการบริหารจัดการความเสี่ยงจากเทคโนโลยีที่รัดกุมและเหมาะสมควบคู่ไปด้วย จึงได้ออกแนวปฏิบัตินี้เพื่อเป็นมาตรฐานขั้นต่ำให้ผู้ให้บริการทางการเงินใช้อ้างอิงในการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงินอย่างปลอดภัย น่าเชื่อถือ เพื่อให้มั่นใจว่าผู้ให้บริการทางการเงินมีนโยบายและการบริหารจัดการในการนำเทคโนโลยีชีวมิติมาใช้ด้วยกระบวนการที่เหมาะสม มั่นคงปลอดภัย เช่น การกำหนดแนวนโยบาย กระบวนการ และ การปฏิบัติในการนำเทคโนโลยีชีวมิติมาใช้อย่างปลอดภัย น่าเชื่อถือตลอดทั้งวงจรชีวิต (Life cycle) ของข้อมูลชีวมิติ ตั้งแต่การรวบรวมข้อมูล การเก็บข้อมูล การประมวลผลเพื่อเปรียบเทียบและตัดสินใจ และการทำลาย และสอดคล้องกับมาตรฐานสากลที่เกี่ยวข้องกับเทคโนโลยีชีวมิติ เช่น มาตรฐาน International Organization for Standardization (ISO) National Institute of Standards and Technology (NIST) Information Systems Audit and Control Association (ISACA) และ FIDO Biometric Requirements ซึ่งจะเป็นประโยชน์ต่อการเข้าถึงบริการทางการเงินของประชาชน การรักษาเสถียรภาพของระบบสถาบันการเงิน และความเชื่อมั่นของประชาชนต่อบริการของผู้ให้บริการทางการเงิน

2. แนวปฏิบัติที่ยกเลิก

แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน ลงวันที่ 22 กรกฎาคม 2563

3. ขอบเขตการใช้

แนวปฏิบัติฉบับนี้ มีวัตถุประสงค์เพื่อให้ผู้ให้บริการทางการเงินที่อยู่ภายใต้การกำกับดูแลของ ธปท. ได้แก่ สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงินที่อยู่ภายใต้การกำกับของธนาคารแห่งประเทศไทย และผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน ที่มีการประยุกต์ใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงินนำไปปฏิบัติ

4. คำจำกัดความ

ในแนวปฏิบัติฉบับนี้

เทคโนโลยีชีวมิติ (Biometric technology) หมายถึง เทคโนโลยีที่ใช้ในการจำแนกอัตลักษณ์ทางกายภาพของบุคคล เช่น ใบหน้า ลายนิ้วมือ หรืออัตลักษณ์ทางพฤติกรรม ของบุคคล เช่น การพูด การเขียน เพื่อระบุ พิสูจน์ หรือยืนยันตัวตนบุคคล

ข้อมูลชีวมิติ (Biometric data)[1] หมายถึง ข้อมูลอัตลักษณ์ของบุคคลหนึ่ง ๆ ที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีชีวมิติในการจำแนกอัตลักษณ์ทางกายภาพของบุคคล เช่น ใบหน้า ลายนิ้วมือ หรืออัตลักษณ์ทางพฤติกรรมของบุคคล เช่น การพูด การเขียน เพื่อระบุ พิสูจน์ หรือยืนยันตัวตนของบุคคลนั้น

ข้อมูลอ้างอิงชีวมิติ (Biometric reference) หมายถึง ข้อมูลชีวมิติที่ถูกจัดเก็บไว้เป็นข้อมูลอ้างอิงเพื่อใช้เปรียบเทียบกับข้อมูลชีวมิติของบุคคล ทั้งนี้ ให้หมายความรวมถึงข้อมูลชีวมิติตั้งต้น หรือเทมเพลตชีวมิติที่มีลักษณะดังกล่าวด้วย

ข้อมูลชีวมิติตั้งต้น (Biometric sample) หมายถึง ข้อมูลชีวมิติที่เกิดจากการรวบรวมอัตลักษณ์ของบุคคลและแปลงให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ โดยข้อมูลดังกล่าวยังไม่ถูกประมวลให้เป็นเทมเพลตชีวมิติ ตัวอย่างเช่น ภาพใบหน้าที่ถูกถ่ายเพื่อนำไปใช้กับเทคโนโลยีการเปรียบเทียบใบหน้า

เทมเพลตชีวมิติ (Biometric template) หมายถึง ข้อมูลชีวมิติที่เป็นผลลัพธ์จากการประมวลข้อมูลชีวมิติตั้งต้นด้วยวิธีการทางอิเล็กทรอนิกส์ ให้อยู่ในรูปแบบที่สามารถนำไปใช้เพื่อเปรียบเทียบข้อมูลชีวมิติของบุคคล และไม่สามารถเปลี่ยนกลับเป็นข้อมูลชีวมิติตั้งต้นได้ เช่น พิกัดตำแหน่งของจุดสังเกตสำคัญต่าง ๆ บนใบหน้า

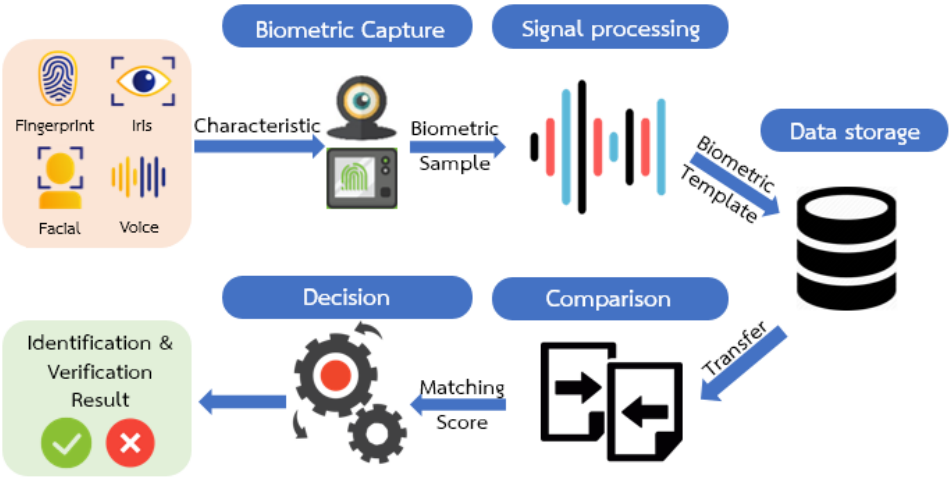
5. ภาพรวมการใช้เทคโนโลยีชีวมิติ

เทคโนโลยีชีวมิติ มีหลักการทำงาน และประเด็นสำคัญที่ควรคำนึงถึงในการป้องกันความเสี่ยงที่เกี่ยวข้อง ดังนี้

5.1 หลักการทำงานของเทคโนโลยีชีวมิติ

หลักการทำงานของเทคโนโลยีชีวมิติประกอบด้วย 5 ขั้นตอน คือ

[1] ข้อมูลชีวมิติ ตามแนวปฏิบัติฯ ฉบับนี้ คือข้อมูลชีวภาพตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล



(1) การรวบรวมข้อมูลชีวมิติ (Capture) เป็นขั้นตอนการรวบรวมอัตลักษณ์ของบุคคลด้วยอุปกรณ์รับข้อมูล (Sensor) ต่าง ๆ และแปลงให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ เพื่อให้ได้มาซึ่งข้อมูลชีวมิติตั้งต้น เช่น การรวบรวมภาพใบหน้าด้วยกล้อง การรวบรวมภาพลายนิ้วมือด้วยอุปกรณ์อ่านลายนิ้วมือ

(2) การประมวลอัตลักษณ์ (Signal processing) เป็นขั้นตอนการประมวลข้อมูลชีวมิติตั้งต้นให้เป็นเทมเพลตชีวมิติ ด้วยวิธีการทางอิเล็กทรอนิกส์ทำให้ไม่สามารถแปลงเทมเพลตชีวมิติให้กลับเป็นข้อมูลชีวมิติตั้งต้นได้ เช่น การประมวลผลภาพใบหน้าจากระยะห่างระหว่างจุดสังเกตสำคัญจำนวนมาก เช่น ดวงตา หางคิ้ว ความกว้างริมฝีปาก จุดสังเกตบนลายนิ้วมือ (Minutiae)

(3) การเก็บข้อมูล (Data storage) เป็นขั้นตอนการจัดเก็บข้อมูลอ้างอิงชีวมิติไว้ในระบบจัดเก็บข้อมูล ซึ่งมีการเชื่อมโยงข้อมูลอ้างอิงชีวมิติกับข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการทางการเงิน (เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน ที่อยู่) เพื่อใช้ในการเปรียบเทียบอัตลักษณ์ของบุคคลนั้น

(4) การเปรียบเทียบอัตลักษณ์ (Comparison) เป็นขั้นตอนการเปรียบเทียบระหว่างข้อมูลชีวมิติที่ต้องการระบุ พิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการ กับข้อมูลอ้างอิงชีวมิติที่เก็บไว้ในระบบจัดเก็บข้อมูลภายในองค์กรหรือแหล่งข้อมูลที่เชื่อถือได้ โดยแสดงผลการเปรียบเทียบเป็นระดับความเชื่อมั่นการเป็นบุคคลเดียวกัน ซึ่งมีการใช้งานหลักใน 2 ลักษณะ ได้แก่

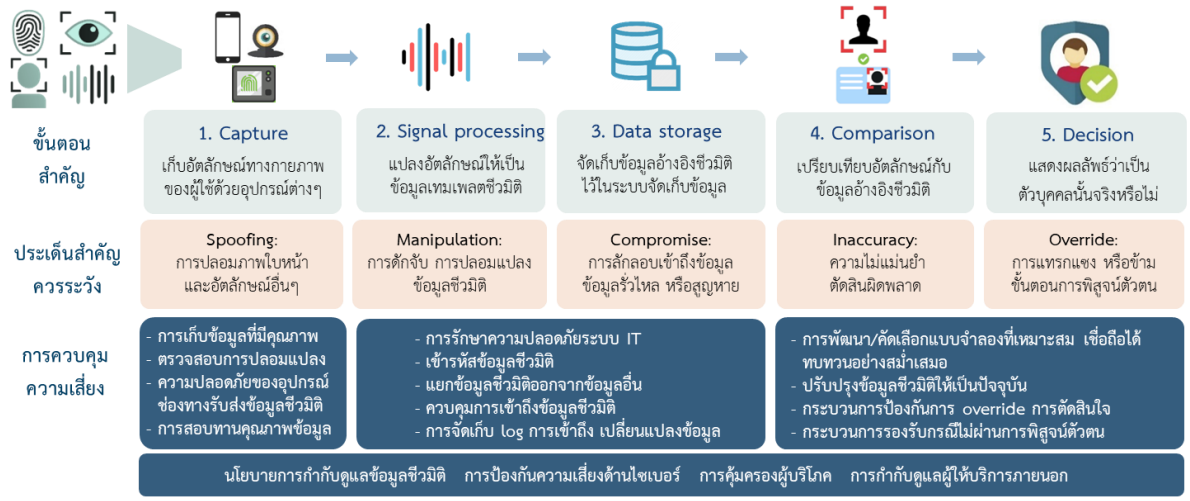
- การระบุตัวตน (Identification) คือ การนำข้อมูลชีวมิติของบุคคลมาเปรียบเทียบตัวบุคคลกับข้อมูลอ้างอิงชีวมิติที่บุคคลนั้นได้ลงทะเบียนไว้ และบันทึกอยู่ในระบบจัดเก็บแล้ว เพื่อระบุว่าเป็นบุคคลที่มีข้อมูลอยู่ในระบบจัดเก็บข้อมูลหรือไม่ เช่น การใช้ภาพใบหน้า เพื่อค้นหาหรือระบุตัวตนของบุคคลหนึ่งที่มีข้อมูลอ้างอิงชีวมิติบันทึกไว้ในระบบจัดเก็บข้อมูลแล้ว

- การพิสูจน์ตัวตนและยืนยันตัวตน (Verification and authentication) คือ การนำข้อมูลชีวมิติของบุคคลมาเปรียบเทียบตัวบุคคลกับแหล่งข้อมูลที่เชื่อถือได้ เพื่อพิสูจน์และยืนยันว่าเป็นบุคคลนั้นจริงตามที่อ้างถึงหรือไม่ เช่น กระบวนการรู้จักผู้ใช้บริการในการเปิดบัญชีเงินฝากด้วยการเปรียบเทียบข้อมูลชีวมิติที่ได้จากการถ่ายภาพบุคคลกับข้อมูลที่บันทึกในบัตรประจำตัวประชาชน

(5) การตัดสินใจ (Decision) เป็นขั้นตอนแสดงผลลัพธ์จากการเปรียบเทียบอัตลักษณ์ของบุคคล โดยเปรียบเทียบค่าคะแนนความเชื่อมั่นที่ยอมรับได้ (Threshold) กับค่าคะแนนความเชื่อมั่นจากการเปรียบเทียบอัตลักษณ์ของบุคคล เพื่อตัดสินใจว่าเป็นบุคคลนั้นจริงหรือไม่

5.2 ประเด็นสำคัญที่ควรคำนึงถึงในการป้องกันความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีชีวมิติ

เทคโนโลยีชีวมิติเกี่ยวข้องกับการใช้ข้อมูลชีวมิติของบุคคลในการระบุ พิสูจน์ หรือยืนยันตัวตน ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความสำคัญ จึงจำเป็นต้องมีการควบคุมดูแลในทุกขั้นตอนการทำงานที่เกี่ยวข้องอย่างเข้มงวดรัดกุม และปลอดภัย โดยมีประเด็นสำคัญที่ต้องพิจารณาและระมัดระวัง เพื่อป้องกันความเสี่ยงในการใช้เทคโนโลยีชีวมิติ สรุปตามแผนภาพ และคำอธิบายได้ ดังนี้



(1) การปลอมแปลงอัตลักษณ์ (Spoofing) คือ การสร้างหรือปรับแต่งลักษณะทางกายภาพและลักษณะทางพฤติกรรม เพื่อเลียนแบบอัตลักษณ์ของบุคคลอื่นด้วยวิธีต่าง ๆ เช่น การใช้วัสดุเทียมเพื่อเลียนแบบลายนิ้วมือ การใช้หน้ากากเพื่อหลอกอุปกรณ์รับข้อมูล และการใช้ภาพถ่ายหรือภาพเคลื่อนไหวที่บันทึกไว้แทนการถ่ายภาพหรือการเคลื่อนไหวจริงของบุคคล

(2) การดักจับข้อมูล (Man-in-the-middle) คือ การลักลอบคัดลอกหรือแก้ไขข้อมูลชีวมิติที่อยู่ระหว่างขั้นตอนการรับส่งข้อมูลระหว่างกันภายในระบบ เช่น การติดตั้งอุปกรณ์ดักจับข้อมูลชีวมิติในโครงข่าย

(3)การลักลอบเข้าถึงข้อมูล (Compromise) คือ การพยายามลักลอบเจาะระบบจัดเก็บข้อมูลอ้างอิงชีวมิติ เพื่อคัดลอก แก้ไข หรือทำลายข้อมูลอ้างอิงชีวมิติ

(4) การตัดสินผิดพลาด (Inaccuracy) คือ การที่ระบบระบุ พิสูจน์ หรือยืนยันตัวตนบุคคลผิดพลาดจากระดับที่กำหนด โดยอาจเกิดจากกระบวนการเปรียบเทียบอัตลักษณ์ที่ไม่แม่นยำหรือกระบวนการเรียนรู้ของระบบ (Model training) ยังไม่เพียงพอ

(5) การแทรกแซงการทำงานของระบบ (Override) คือ การพยายามแก้ไขหรือข้ามขั้นตอนการตัดสินใจของระบบการเปรียบเทียบอัตลักษณ์ เช่น การแก้ไขค่าคะแนนความเชื่อมั่นที่ยอมรับได้ให้อยู่ในระดับต่ำลง (Threshold manipulation) การปรับเปลี่ยนกระบวนการตัดสินใจโดยข้ามหรือแทรกแซงขั้นตอนประมวลผลของระบบจริง

6. หลักการที่พึงปฏิบัติสำหรับผู้ให้บริการทางการเงิน

หลักการพึงปฏิบัติที่สำคัญในการใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงินมี 6 ข้อ ซึ่งผู้ให้บริการทางการเงินต้องถือปฏิบัติเป็นมาตรฐานขั้นต่ำในการให้บริการทางการเงิน โดยมีผลลัพธ์ที่คาดหวังและแนวทางที่พึงปฏิบัติ ดังนี้

หลักการที่ 1 กรอบนโยบายและการกำกับดูแลการใช้เทคโนโลยีชีวมิติ

ผลลัพธ์ที่คาดหวัง (Intended outcome) : ผู้ให้บริการทางการเงินมีความตระหนักถึงประโยชน์และความเสี่ยงในการใช้เทคโนโลยีชีวมิติ มีกรอบนโยบายที่ชัดเจนและมีระเบียบวิธีปฏิบัติ และกระบวนการกำกับดูแลการใช้เทคโนโลยีชีวมิติที่รัดกุมเพื่อให้ผู้ปฏิบัติงานใช้เทคโนโลยีชีวมิติและข้อมูลชีวมิติได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัย สอดคล้องกับลักษณะของเทคโนโลยีชีวมิติและรูปแบบการให้บริการ

แนวทางที่พึงปฏิบัติ

(1) กำหนดให้มีกลไกการกำกับดูแลการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงินที่ชัดเจน เพื่อให้มั่นใจว่ามีการคำนึงถึงการจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีชีวมิติ ทั้งนี้ อาจใช้โครงสร้างการกำกับดูแลที่มีอยู่ในปัจจุบันหรือที่จัดตั้งขึ้นใหม่เป็นการเฉพาะ โดยควรมีผู้เชี่ยวชาญด้านเทคโนโลยีและด้านความเสี่ยงร่วมอยู่ในโครงสร้างการกำกับดูแล ทั้งนี้ โครงสร้างการกำกับดูแลดังกล่าวต้องครอบคลุมการดำเนินงานด้านต่าง ๆ ที่สำคัญ เช่น การวิเคราะห์ความเสี่ยงของเทคโนโลยีชีวมิติ ผลิตภัณฑ์ที่มีการนำเทคโนโลยีชีวมิติมาใช้ และผู้ให้บริการเทคโนโลยีที่เกี่ยวข้อง การกำหนดมาตรการบริหารจัดการความเสี่ยง มาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล และการปฏิบัติตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(2) กำหนดหรือปรับปรุงนโยบายต่าง ๆ ภายในองค์กรสำหรับการกำกับดูแลข้อมูลชีวมิติ เช่น นโยบายการดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) นโยบายการกำกับดูแลข้อมูล (Data governance policy) นโยบายการจัดชั้นความลับ (Data classification policy) โดยนโยบายดังกล่าวต้องมีเนื้อหาครอบคลุมวงจรชีวิตของการใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงินอย่างชัดเจน ตั้งแต่การรวบรวมข้อมูล การเก็บข้อมูล การประมวลผลเพื่อเปรียบเทียบและตัดสินใจ และการทำลาย เพื่อให้ผู้ปฏิบัติงานมีความเข้าใจและสามารถนำไปปฏิบัติได้

(3) ประเมินการนำเทคโนโลยีชีวมิติมาให้บริการอย่างรอบด้านก่อนนำมาใช้ในการให้บริการ ทั้งการประเมินประโยชน์ ความเหมาะสมกับรูปแบบการให้บริการ ผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล[2] ความเสี่ยงของเทคโนโลยีชีวมิติ และแนวทางการจัดการความเสี่ยงด้านต่าง ๆ ที่สำคัญ ได้แก่ ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านชื่อเสียง ความเสี่ยงด้านกฎหมายและการปฏิบัติตามหลักเกณฑ์การกำกับดูแลที่เกี่ยวข้อง รวมถึงความเสี่ยงด้านการคุ้มครองผู้ใช้บริการทางการเงิน

หลักการที่ 2 การรวบรวมข้อมูลชีวมิติของผู้ใช้บริการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีกระบวนการได้มาซึ่งข้อมูลชีวมิติของผู้ใช้บริการที่เหมาะสม มีการดูแลข้อมูลชีวมิติให้มีคุณภาพดีเพียงพอสำหรับการระบุ พิสูจน์ หรือยืนยันตัวตนเพื่อให้บริการทางการเงิน รวมถึงมีการสร้างความเข้าใจกับผู้ใช้บริการเพื่อสร้างความเชื่อมั่นในการนำเทคโนโลยีชีวมิติมาให้บริการ

แนวทางที่พึงปฏิบัติ

(1) กำหนดกระบวนการหรือมาตรฐานการได้มาซึ่งข้อมูลชีวมิติที่มีคุณภาพและครบถ้วนเพียงพอต่อการประมวลผลเพื่อ ระบุ พิสูจน์ หรือยืนยันตัวตนของผู้ใช้บริการอย่างถูกต้องแม่นยำ ซึ่งครอบคลุมทั้งการกำหนดแนวปฏิบัติสำหรับผู้ปฏิบัติงานที่รวบรวมข้อมูล และการให้คำแนะนำผู้ใช้บริการกรณีที่ผู้ใช้บริการดำเนินการ

[2] การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data protection impact assessment) สามารถอ้างอิงได้จากแนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ในการให้ข้อมูลชีวมิติเอง เช่น การถ่ายภาพตนเองด้วยโทรศัพท์เคลื่อนที่ การทำรายการที่เครื่อง Kiosk เพื่อให้มั่นใจว่าข้อมูลชีวมิติที่รวบรวมมีคุณภาพดีเพียงพอในการนำไปประมวลผลต่อไป เช่น การตรวจสอบสภาพแวดล้อมให้มีแสงสว่างเพียงพอต่อการถ่ายภาพ การให้คำแนะนำผู้ใช้บริการไม่ให้มีการสวมหมวกหรือแว่นตาดำก่อนการถ่ายภาพใบหน้า การตรวจสอบคุณภาพของภาพถ่ายก่อนบันทึกเข้าระบบ และขั้นตอนรองรับกรณีที่มีข้อจำกัดในการใช้ข้อมูลชีวมิติ เช่น ภาพในบัตรประจำตัวประชาชนไม่สามารถใช้งานได้ ลายนิ้วมือเลือนราง รวมถึงอาจใช้เทคโนโลยีการประเมินคุณภาพของภาพ เช่น Image quality assessment เข้ามาช่วยในการวิเคราะห์ประเมินคุณภาพของข้อมูลชีวมิติ

ทั้งนี้ กระบวนการและแนวทางการควบคุมคุณภาพของการรวบรวมข้อมูลชีวมิติอาจแตกต่างกันตามรูปแบบและช่องทางการให้บริการ อย่างไรก็ดี กรณีที่มีการใช้ภาพถ่ายใบหน้า ผู้ให้บริการทางการเงินควรพิจารณารายละเอียดในข้อกำหนดเกี่ยวกับมาตรฐานขั้นต่ำและแนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติตามภาคผนวก ก ซึ่งสอดคล้องกับมาตรฐาน ISO 19794-5 Biometric data interchange formats -- Part 5 Face image data

(2) ชี้แจงผู้ใช้บริการเกี่ยวกับวัตถุประสงค์ของการรวบรวมข้อมูลชีวมิติอย่างชัดเจน ก่อนหรือในขณะที่จะเริ่มกระบวนการรวบรวมข้อมูลชีวมิติ พร้อมทั้งชี้แจงเกี่ยวกับประโยชน์จากการใช้เทคโนโลยีชีวมิติ สิทธิที่ผู้ใช้บริการพึงมีในการให้ข้อมูลชีวมิติ และผลกระทบที่อาจเกิดจากการที่ผู้ใช้บริการไม่ให้ข้อมูลดังกล่าว โดยคำนึงถึงการปฏิบัติตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(3) กำหนดกลไกการตรวจสอบการปลอมแปลงอัตลักษณ์ เพื่อป้องกันการสวมรอยเป็นบุคคลอื่นในขั้นตอนการรวบรวมข้อมูลชีวมิติ ทั้งกรณีที่ผู้ให้บริการทางการเงินพบเห็นผู้ใช้บริการต่อหน้า (Face-to-face) และไม่พบเห็นผู้ใช้บริการต่อหน้า (Non face-to-face) เช่น มีการพิสูจน์ หรือยืนยันตัวตนกับแหล่งข้อมูลที่เชื่อถือได้อย่างบัตรประจำตัวประชาชนหรือหนังสือเดินทาง มีกระบวนการหรือเทคโนโลยีตรวจจับการปลอมแปลงชีวมิติ (Presentation attack detection) เช่น Liveness detection หรือมีกระบวนการอื่นเพิ่มเติมที่รัดกุมเพียงพอ

(4) กำหนดแนวทางและกระบวนการควบคุมภายใน และมีการสอบทานความถูกต้องของกระบวนการได้มาซึ่งข้อมูลชีวมิติจากผู้ใช้บริการอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามีการปฏิบัติเป็นไปตามนโยบาย แนวปฏิบัติและกระบวนการที่กำหนดไว้

(5) กำหนดแนวทางการดูแลอุปกรณ์ที่ใช้รวบรวมข้อมูลชีวมิติที่นำมาให้บริการ เช่น อุปกรณ์ถ่ายภาพและระบบงานที่สาขาหรือจุดรวบรวมข้อมูลชีวมิติ เครื่องอ่านลายนิ้วมือที่ตู้ Kiosk รวมถึงช่องทางการรับส่งข้อมูลชีวมิติของผู้ใช้บริการ ให้อยู่ในสภาพที่พร้อมให้บริการเพื่อให้สามารถรวบรวมข้อมูลได้อย่างมีคุณภาพ มีความปลอดภัย ไม่มีการเก็บหรือคงค้างข้อมูลชีวมิติอยู่ในอุปกรณ์หรือระบบที่ใช้ในการรวบรวมข้อมูลชีวมิติของผู้ให้บริการทางการเงิน ซึ่งรวมถึงกรณีที่มีการรวบรวมข้อมูลชีวมิติผ่านช่องทางของผู้ให้บริการภายนอก (3^{rd} party service provider)

หลักการที่ 3 การประมวลผลข้อมูลชีวมิติของผู้ใช้บริการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีการประมวลผลอัตลักษณ์ การเปรียบเทียบอัตลักษณ์และการตัดสินใจที่ถูกต้องแม่นยำอยู่ในระดับที่สูงเพียงพอต่อการให้บริการทางการเงิน รวมถึงสามารถป้องกันการปลอมแปลงอัตลักษณ์ เพื่อให้บริการทางการเงินมีความปลอดภัยและความน่าเชื่อถือต่อผู้ใช้บริการ

แนวทางที่พึงปฏิบัติ

(1) กำหนดแนวทางการพัฒนาหรือคัดเลือกเทคโนโลยีในการเปรียบเทียบข้อมูลชีวมิติอย่างเหมาะสม โดยคำนึงถึงความแม่นยำในการเปรียบเทียบอัตลักษณ์ที่เหมาะสมกับ รูปแบบการให้บริการ ประเภทและระดับความเสี่ยงของธุรกรรม และเทียบเคียงได้กับมาตรฐานสากล[3] รวมถึงมีความสามารถในการตรวจจับการปลอมแปลงชีวมิติ[4] เช่น การป้องกันการใช้ภาพใบหน้าหรือลายนิ้วมือปลอมแทนอัตลักษณ์จริง

ในการพัฒนาแบบจำลองหรือคัดเลือกแบบจำลองจากผู้ให้บริการภายนอก ควรคำนึงถึงการทดสอบด้วยกลุ่มตัวอย่าง (Test sample) ที่มีคุณภาพ มีปริมาณ (Sample size) และความหลากหลายมากเพียงพอ เหมาะสมกับรูปแบบของการให้บริการ[5] ทั้งนี้ แบบจำลองควรผ่านการประเมินความแม่นยำเทียบกับมาตรฐานสากล โดยองค์กรกลางหรือผู้เชี่ยวชาญที่มีความน่าเชื่อถือ ด้วยวิธีการทดสอบแบบจำลองที่สอดคล้องตามมาตรฐานสากล[6] รวมถึงมีการสอบทานและยกระดับความแม่นยำของแบบจำลองอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามีความแม่นยำตามที่ผู้ให้บริการทางการเงินกำหนด

(2) มีกระบวนการตรวจสอบว่าข้อมูลและเอกสารที่ใช้เพื่อระบุ พิสูจน์ หรือยืนยันตัวตนเชื่อถือได้เป็นปัจจุบัน เช่น มีกลไกตรวจสอบความแท้จริงและเป็นปัจจุบันของบัตรประจำตัวประชาชนหรือหนังสือเดินทางที่ใช้เป็นแหล่งข้อมูลที่เชื่อถือได้ในการเปรียบเทียบอัตลักษณ์ และมีกลไกการรวบรวมข้อมูลชีวมิติที่เป็นปัจจุบันของผู้ใช้บริการ เช่น กำหนดระยะเวลาหรือเงื่อนไขในการปรับปรุงข้อมูลภาพถ่ายผู้ใช้บริการที่เหมาะสมกับลักษณะของบริการหรือธุรกรรม หรือสอดคล้องตามหลักเกณฑ์ที่เกี่ยวข้อง

(3) กำหนดกลไกการตรวจจับและป้องกันการปลอมแปลงข้อมูลชีวมิติในขั้นตอนการเปรียบเทียบอัตลักษณ์ หรือความพยายามในการข้ามหรือแทรกแซง ขั้นตอนการเปรียบเทียบอัตลักษณ์เพื่อพิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการ เช่น จำกัดจำนวนครั้งที่ผู้ใช้บริการสามารถพิสูจน์ หรือยืนยันตัวตนด้วยข้อมูลชีวมิติ

---

[3] ค่าความแม่นยำในการเปรียบเทียบอัตลักษณ์อ้างอิงตามกระบวนการทดสอบมาตรฐานสากล เช่น การพิสูจน์ตัวตนด้วยภาพใบหน้าเทียบกับแหล่งข้อมูลที่เชื่อถือได้ ควรมีค่าอัตราส่วนการยอมรับที่ผิดพลาด (False Acceptance Ratio, FAR) ไม่เกิน 0.1% ตามมาตรฐาน NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management และค่าอัตราส่วนการปฏิเสธที่ผิดพลาด (False Reject Ratio, FRR) ไม่เกิน 3% อ้างอิงตามมาตรฐาน FIDO Biometric Requirements ซึ่งกำหนดกระบวนการ วิธี และระดับความแม่นยำขั้นต่ำในการยืนยันตัวตนด้วยเทคโนโลยีชีวมิติ ทั้งนี้ ควรพิจารณาถึงประสิทธิภาพของ Algorithm ของผู้ให้บริการเทคโนโลยีภายใต้การทดสอบของ NIST FRVT 1:1 Verification ควบคู่กัน เช่น มีลำดับค่า False non-match Rate (FNMR) อยู่ภายในผลลัพธ์ 50 ลำดับแรก เป็นต้น

[4] การทดสอบความสามารถในการตรวจจับการปลอมแปลงชีวมิติ แบ่งตามระดับความซับซ้อนได้ดังนี้

ระดับต่ำ : ใช้อุปกรณ์ที่หาได้ทั่วไป ใช้เวลาเตรียมการน้อย ต้องการทักษะการปลอมแปลงต่ำ และอาศัยข้อมูลอัตลักษณ์ของบุคคลที่เข้าถึงได้ง่ายในการปลอมแปลง (ตัวอย่างเช่น การใช้ภาพใบหน้าที่เป็นภาพนิ่งแทนใบหน้าของบุคคลจริง เช่น ภาพใบหน้าที่หาได้จาก Social media ต่าง ๆ ภาพใบหน้าจากการตัดต่อด้วยโปรแกรมตัดต่อภาพ)

ระดับปานกลาง : ใช้อุปกรณ์เฉพาะทางหรืออุปกรณ์ที่หาได้ทั่วไป ใช้เวลาในการเตรียมการปานกลาง ต้องการทักษะการปลอมแปลงระดับหนึ่ง และอาศัยข้อมูลอัตลักษณ์ของบุคคลที่เข้าถึงได้ไม่ยากมากนัก ในการปลอมแปลง (ตัวอย่าง เช่น ใช้ภาพวิดีโอหรือภาพเคลื่อนไหวของบุคคลที่มีคุณภาพสูง เพื่อลอกเลียนการทำท่าทางตามกระบวนการ Liveness detection)

ระดับสูง : ใช้อุปกรณ์เฉพาะทาง ใช้เวลาในการเตรียมการมาก ต้องการทักษะการปลอมแปลงระดับสูง และอาศัยข้อมูลอัตลักษณ์ของบุคคลที่เข้าถึงได้ยาก ในการปลอมแปลง (ตัวอย่างเช่น ใช้หน้ากาก 3D mask เลียนแบบใบหน้าบุคคลจริง)

ผู้ให้บริการทางการเงินควรพิจารณาการทดสอบการปลอมแปลงโดยอ้างอิงมาตรฐานสากล เช่น NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management, ISO30107 – Biometric presentation attack detection และ FIDO Biometric Requirements

[5] ในการทดสอบเทคโนโลยีชีวมิติเพื่อการพิสูจน์และยืนยันตัวตนลูกค้าสำหรับการเปิดบัญชีเงินฝากและเงินอิเล็กทรอนิกส์ ควรมีการกำหนดจำนวนกลุ่มตัวอย่างทดสอบขั้นต่ำอย่างน้อย 2,000 คน ขึ้นไป ทั้งนี้ ผู้ให้บริการเทคโนโลยีชีวมิติที่ผ่านการประเมินความแม่นยำเทียบกับมาตรฐานสากลโดยองค์กรกลางหรือผู้เชี่ยวชาญที่มีความน่าเชื่อถือ และผลการประเมินอยู่ในระดับที่ ธปท. กำหนด สามารถกำหนดจำนวนกลุ่มตัวอย่างทดสอบขั้นต่ำอย่างน้อย 1,000 คน ขึ้นไปได้

[6] มาตรฐานสากลเกี่ยวกับการพัฒนาและทดสอบแบบจำลอง ได้แก่ ISO 19795 - Biometric performance testing and reporting

ได้ต่อเนื่องเพื่อป้องกันการทดลองทำซ้ำ[7] กำหนดระยะเวลาที่ระบบยอมให้ทำธุรกรรมด้วยข้อมูลชีวมิติโดยผู้ใช้บริการต้องยืนยันตัวตนใหม่หากไม่มีกิจกรรมใด ๆ เกิดขึ้น (Time-out policy)

(4) กำหนดกระบวนการรองรับกรณีที่ระบบการเปรียบเทียบอัตลักษณ์ไม่สามารถใช้งานได้ หรือกรณีที่ผู้ใช้บริการตัวจริงพิสูจน์หรือยืนยันตัวตนไม่สำเร็จ (False reject) โดยควรมีกระบวนการรองรับที่เหมาะสมกับรูปแบบการให้บริการ รวมทั้งลักษณะและความเสี่ยงของธุรกรรม เช่น การมีทางเลือกให้ผู้ใช้บริการพิสูจน์ หรือยืนยันตัวตนด้วยวิธีอื่น หรือการแสดงหลักฐานอื่นเพิ่มเติมประกอบการพิสูจน์ หรือยืนยันตัวตน

(5) กำหนดแนวทางการดูแลรักษาความปลอดภัยของข้อมูลในขั้นตอนการประมวลอัตลักษณ์และขั้นตอนเปรียบเทียบอัตลักษณ์ โดยเฉพาะกรณีที่ผู้ให้บริการทางการเงินมีการใช้บริการประมวลอัตลักษณ์หรือเปรียบเทียบอัตลักษณ์ผ่านระบบของผู้ให้บริการภายนอก จะต้องไม่มีการเก็บหรือคงค้างข้อมูลชีวมิติในระบบของผู้ให้บริการภายนอก

หลักการที่ 4 การรักษาความปลอดภัยข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีการดูแลรักษาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการที่เข้มงวดและรัดกุมตามมาตรฐานสากล เพื่อให้มั่นใจว่าข้อมูลของผู้ใช้บริการได้รับการปกป้องดูแลอย่างปลอดภัย

แนวทางที่พึงปฏิบัติ

(1) กำหนดนโยบายและออกแบบระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT infrastructure) ที่คำนึงถึงความปลอดภัยของข้อมูลชีวมิติและความสามารถในการขยายขนาดเพื่อรองรับปริมาณธุรกรรมที่เพิ่มขึ้นในอนาคต

(2) ไม่เก็บข้อมูลชีวมิติตั้งต้นของผู้ใช้บริการ โดยให้จัดเก็บเป็นเทมเพลตชีวมิติเพื่อใช้ในการเปรียบเทียบอัตลักษณ์ และต้องไม่สามารถแปลงย้อนกลับเป็นข้อมูลชีวมิติตั้งต้นได้ ยกเว้นกรณีภาพถ่ายใบหน้าของลูกค้า หรือกรณีที่ผู้ให้บริการทางการเงินมีความจำเป็นในการจัดเก็บข้อมูลชีวมิติตั้งต้นเพื่อปฏิบัติตามกฎหมาย นอกจากนี้ ให้ปฏิบัติตามกฎหมายที่เกี่ยวข้องด้วย เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(3) กำหนดกระบวนการจัดเก็บ รับส่ง และเชื่อมโยงข้อมูลอ้างอิงชีวมิติ ที่มีความรัดกุมปลอดภัย ได้แก่

(3.1) จัดเก็บและรับส่งข้อมูลอ้างอิงชีวมิติเพื่อให้ไม่สามารถระบุตัวตนเจ้าของข้อมูล และไม่สามารถนำไปใช้ต่อได้โดยไม่ได้รับอนุญาต เช่น การเข้ารหัสข้อมูลอ้างอิงชีวมิติสำหรับการรับส่งข้อมูล (Data-in-transit) ระหว่างขั้นตอนต่าง ๆ ตั้งแต่อุปกรณ์รับข้อมูล สายสื่อสาร จนถึงการบันทึกข้อมูลอ้างอิงชีวมิติ (Data-at-rest) มีการเข้ารหัสในระดับฟิลด์ของระบบจัดเก็บข้อมูลหรือระดับไฟล์ ด้วยมาตรฐานการเข้ารหัสข้อมูลที่มีความมั่นคงปลอดภัยสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป เช่น อัลกอริธึมการเข้ารหัส (Encryption algorithm) และขนาดความยาวของกุญแจเข้ารหัสข้อมูล เป็นต้น รวมถึงมีกระบวนการเก็บรักษากุญแจเข้ารหัสที่มีความรัดกุม

---

[7] สามารถอ้างอิงการกำหนดจำนวนครั้งและระยะเวลาตามมาตรฐาน NIST SP 800-63B Digital Identity Guidelines Authentication and Lifecycle Management และ ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจำกัดจำนวนครั้งของการยืนยันตัวตนด้วยชีวมิติให้ผิดพลาดอย่างต่อเนื่องได้ไม่เกิน 5 ครั้งกรณีทั่วไป หรือไม่เกิน 10 ครั้ง กรณีที่ใช้งานการตรวจจับการปลอมแปลงชีวมิติ โดยหากครบกำหนดแล้วต้องดำเนินการอย่างใดอย่างหนึ่ง ดังนี้

- หน่วงเวลาอย่างน้อย 30 วินาทีก่อนอนุญาตให้ยืนยันตัวตนครั้งถัดไป และเพิ่มการหน่วงเวลาก่อนอนุญาตให้ยืนยันตัวตนครั้งต่อไปแบบ Exponential เช่น หน่วงเวลาอย่างน้อย 30 วินาที 1 นาที 2 นาที 4 นาที 8 นาที และเพิ่มขึ้นตามจำนวนครั้งของการยืนยันตัวตนผิดพลาด
- ระงับการยืนยันตัวตนด้วยชีวมิติและให้ผู้ใช้บริการยืนยันตัวตนด้วยวิธีอื่น

(3.2) จัดเก็บข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการแยกออกจากข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการ เช่น ชื่อ-นามสกุล หรือเลขประจำตัวประชาชน ในระดับเซิร์ฟเวอร์หรือฐานข้อมูล เพื่อป้องกันไม่ให้ข้อมูลอ้างอิงชีวมิติรั่วไหลพร้อมข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการ เช่น ระบบฐานข้อมูลภาพใบหน้าแยกจากระบบฐานข้อมูลทั่วไปของผู้ใช้บริการ จัดให้มีการดูแลและการเข้าถึงทั้งสองระบบแยกจากกัน รวมถึงหากมีการเข้ารหัสข้อมูลต้องใช้กุญแจเข้ารหัส (Encryption key) ที่แตกต่างกัน

(3.3) ไม่ระบุข้อมูลอ้างอิงชีวมิติโดยอ้างอิงด้วยข้อมูลที่สามารถใช้ระบุตัวตนของผู้ใช้บริการได้โดยตรง (Indirect reference) เช่น เลขประจำตัวประชาชน และเลขประจำตัวผู้ใช้บริการที่ออกโดยผู้ให้บริการทางการเงินซึ่งถูกใช้งานเพื่ออ้างอิงตัวบุคคลของผู้ใช้บริการได้ในหลายระบบงานของผู้ให้บริการทางการเงิน เพื่อป้องกันไม่ให้สามารถระบุตัวตนของข้อมูลอ้างอิงชีวมิติได้หากเกิดเหตุการณ์โจมตีหรือข้อมูลรั่วไหล

(3.4) แบ่งขอบเขตเครือข่าย (Network zoning) และจัดวางระบบและข้อมูลอ้างอิงชีวมิติ โดยคำนึงถึงระดับชั้นความลับของข้อมูล เช่น ไม่จัดวางระบบและข้อมูลอ้างอิงชีวมิติใน Demilitarized zone (DMZ) เพื่อป้องกันผลกระทบหรือการโจมตีจากเครือข่ายที่ไม่ปลอดภัย

(3.5) ใช้ช่องทางสื่อสารและวิธีการที่ปลอดภัยในการรับส่งข้อมูลชีวมิติระหว่างระบบงานทั้งภายนอกและภายในหน่วยงาน

(4) มีกระบวนการควบคุมการเข้าถึงข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการอย่างเข้มงวด การให้สิทธิการเข้าถึงข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการเท่าที่จำเป็นโดยผู้ปฏิบัติงานที่เกี่ยวข้องเท่านั้น และมีการสอบทานสิทธิอย่างสม่ำเสมอ รวมถึงการมีกระบวนการตรวจสอบความถูกต้องเชื่อถือได้ (Integrity check) ของข้อมูลอ้างอิงชีวมิติเพื่อป้องกันการลักลอบเปลี่ยนแปลงหรือแก้ไขข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการโดยไม่ได้รับอนุญาต

(5) มีการบริหารจัดการช่องโหว่ (Vulnerability management) ของระบบที่เหมาะสมตามระดับความเสี่ยง เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ โดยผู้ให้บริการทางการเงินต้องประเมินช่องโหว่ของระบบโครงสร้างพื้นฐานที่เกี่ยวข้องกับข้อมูลชีวมิติอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงผู้ให้บริการเทคโนโลยีชีวมิติ หรือเมื่อมีการแจ้งเตือนช่องโหว่ด้านความปลอดภัยที่มีผลกระทบกับระบบที่มีความเกี่ยวข้องกับข้อมูลชีวมิติเป็นวงกว้าง เป็นต้น

(6) มีการทดสอบเจาะระบบ (Penetration test) โดยจัดให้มีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ทั้งนี้ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

(7) มีกระบวนการแก้ไขจุดอ่อนความปลอดภัยของระบบ (Patch management) ซึ่งครอบคลุมระบบงานที่รองรับการประมวลผลและจัดเก็บข้อมูลอ้างอิงชีวมิติ รวมถึงกระบวนการสนับสนุนทางด้านอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ (Hardware and software support) รองรับกรณีที่เทคโนโลยีนั้นมีจุดอ่อนหรือตรวจพบความผิดพลาด โดยผู้ให้บริการเทคโนโลยีชีวมิติจะต้องสามารถแก้ไขจุดอ่อนของเทคโนโลยีได้อย่างทันท่วงทีที่มีการแจ้งเตือน

(8) จัดเก็บบันทึกเหตุการณ์ (Log) ที่เกี่ยวข้องกับข้อมูลชีวมิติ โดยครอบคลุมบันทึกการเข้าถึง (Access log) บันทึกการดำเนินงาน (Activity log) บันทึกร่องรอยการทำกิจกรรมธุรกรรม (Transaction log) และบันทึกด้านการรักษาความปลอดภัย (Security event log) ด้วยวิธีการที่มีความปลอดภัยและมีความเพียงพอต่อการสอบทานย้อนหลัง การตรวจสอบในกรณีเกิดเหตุการณ์ผิดปกติ และการใช้เป็นหลักฐานทางกฎหมาย

(9) กำหนดนโยบายและการดูแลข้อมูลชีวมิติอย่างเข้มงวด ในกรณีใช้เทคโนโลยีคลาวด์คอมพิวติ้ง (Cloud computing) เพื่อการประมวลผลหรือเก็บข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการ โดยมีการควบคุมการเข้าถึงข้อมูลอย่างรัดกุม มีการประเมินมาตรฐานการรักษาความปลอดภัยข้อมูลของผู้ให้บริการคลาวด์ (Cloud service provider) โดยคำนึงปัจจัยที่เกี่ยวข้อง[8] เช่น การได้รับใบรับรองมาตรฐานสากลด้านความปลอดภัยข้อมูล นโยบายการดูแลความปลอดภัยข้อมูลของผู้ให้บริการ การประเมินความเสี่ยงจากการกระจุกตัว (Concentration risk) ของระบบคลาวด์ที่จัดเก็บข้อมูลอ้างอิงชีวมิติ รวมถึงการจัดทำข้อตกลงให้ผู้ให้บริการทางการเงินสามารถเข้าตรวจสอบการจัดเก็บข้อมูลได้ และการมีกระบวนการรองรับความพร้อมใช้ของระบบและเก็บข้อมูลอ้างอิงชีวมิติเพื่อความพร้อมใช้ภายในประเทศ

(10) กำหนดให้มีการตรวจสอบกระบวนการรักษาความปลอดภัยข้อมูลชีวมิติของผู้ใช้บริการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายใน (Internal auditor) หรือผู้ตรวจสอบภายนอก (External auditor) ซึ่งครอบคลุมกรณีที่ใช้บริการจากผู้ให้บริการภายนอก

หลักการที่ 5 การคุ้มครองผู้ใช้บริการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีแนวทางคุ้มครองผู้ใช้บริการและมีการให้ความรู้เกี่ยวกับการทำธุรกรรมด้วยเทคโนโลยีชีวมิติอย่างเพียงพอ เหมาะสม เพื่อให้ผู้ใช้บริการได้รับบริการด้วยความปลอดภัย เป็นธรรม และสอดคล้องกับกฎหมายที่เกี่ยวข้อง โดยคงไว้ซึ่งการคุ้มครองสิทธิและข้อมูลส่วนบุคคล

แนวทางที่พึงปฏิบัติ

(1) จัดให้มีกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลชีวมิติให้เป็นไปตามที่กฎหมายกำหนด เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลชีวมิติ ผู้ให้บริการทางการเงินต้องได้รับความยินยอมโดยชัดแจ้งจากผู้ใช้บริการ เว้นแต่เข้าข้อยกเว้นตามกฎหมาย ในกรณีที่ต้องได้รับความยินยอม ผู้ให้บริการทางการเงินจะต้องได้รับความยินยอมจากผู้ใช้บริการก่อนหรือในขณะนั้น (Opt-in consent) นอกจากนี้ การเก็บรวบรวมข้อมูลชีวมิติ ให้เก็บรวบรวมได้เฉพาะเท่าที่มีความจำเป็น โดยผู้ให้บริการทางการเงินต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมให้ผู้ใช้บริการทราบก่อนหรือในขณะที่เก็บรวบรวม เช่น เพื่อการเข้าทำสัญญา หรือเพื่อการให้บริการทางการเงินเพิ่มเติม และผู้ให้บริการทางการเงินต้องใช้ข้อมูลชีวมิติดังกล่าวตามวัตถุประสงค์ที่ผู้ใช้บริการได้ให้ความยินยอมหรือตามที่กฎหมายกำหนดเท่านั้น รวมทั้งผู้ให้บริการทางการเงินต้องแจ้งให้ผู้ใช้บริการทราบถึงรายละเอียดต่าง ๆ ตามที่กฎหมายกำหนด เช่น ประเภทของบุคคลหรือหน่วยงานที่อาจได้รับข้อมูลชีวมิติหรือข้อมูลที่เกี่ยวข้องจากผู้ให้บริการทางการเงินเพื่อประโยชน์ในการให้บริการ

(2) จัดให้มีการขอความยินยอมตามที่กฎหมายกำหนด โดยผู้ให้บริการทางการเงินต้องขอความยินยอมจากผู้ใช้บริการ โดยทำเป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์ และต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ไม่ก่อให้เกิดความเข้าใจผิด และต้องให้อิสระแก่ผู้ใช้บริการในการตัดสินใจให้ความยินยอมด้วยความสมัครใจ นอกจากนี้ หากจะมีการใช้ข้อมูลชีวมิติแตกต่างไปจากวัตถุประสงค์ที่ผู้ใช้บริการได้ให้ความยินยอมไว้ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงข้อกำหนดการให้บริการซึ่งส่งผลกระทบกับขอบเขตความยินยอมเดิมที่ผู้ใช้บริการได้ให้ไว้ ผู้ให้บริการทางการเงินต้องขอความยินยอมจากผู้ใช้บริการใหม่อีกครั้งก่อน โดยแสดงข้อกำหนดที่มีการเปลี่ยนแปลงให้ผู้ใช้บริการเห็นได้อย่างชัดเจน เพื่อที่ผู้ใช้บริการจะได้รับทราบข้อมูลที่เป็นปัจจุบันเกี่ยวกับการใช้งานข้อมูลชีวมิติและสิทธิของผู้ใช้บริการ

[8] ผู้ให้บริการทางการเงินสามารถอ้างอิงแนวทางการประเมินผู้ให้บริการคลาวด์ตามแนวปฏิบัติ ธปท. ว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

(3) แจ้งให้ผู้ใช้บริการทราบถึงสิทธิของผู้ใช้บริการในฐานะเจ้าของข้อมูลชีวมิติ เช่น สิทธิขอเข้าถึงข้อมูลชีวมิติ สิทธิขอเปลี่ยนแปลงข้อมูลชีวมิติให้เป็นปัจจุบันและสมบูรณ์ รวมถึงเงื่อนไขที่เกี่ยวข้องกับข้อมูลชีวมิติ เช่น ผลกระทบต่อสิทธิหรือบริการที่จะได้รับในกรณีที่ผู้ใช้บริการประสงค์จะไม่ให้เก็บรวบรวมข้อมูลชีวมิติ ทั้งนี้ต้องเป็นไปตามกฎหมายที่เกี่ยวข้องกำหนด

(4) จัดให้มีกระบวนการคุ้มครองผู้ใช้บริการในฐานะเจ้าของข้อมูลชีวมิติ เช่น การจัดให้ผู้ใช้บริการสามารถตรวจสอบประวัติการให้ความยินยอมที่เกี่ยวข้องกับข้อมูลชีวมิติ การจัดให้ผู้ใช้บริการสามารถถอนความยินยอมได้ตามหลักเกณฑ์ที่กฎหมายกำหนด โดยจัดให้มีช่องทางรับเรื่องร้องเรียนหรือแจ้งปัญหาจากการใช้บริการที่เกี่ยวข้องกับเทคโนโลยีชีวมิติ และมีการกำหนดระยะเวลาในการแก้ปัญหา (Service level agreement) ที่ชัดเจน รวมถึงมีแนวทางสื่อสารกับผู้ใช้บริการ และหน่วยงานกำกับดูแลที่เกี่ยวข้อง กรณีที่เกิดเหตุการณ์ที่มีผลกระทบกับข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการ รวมถึงมีมาตรการเยียวยาผู้ใช้บริการที่ได้รับผลกระทบ

(5) ให้ความรู้แก่ผู้ใช้บริการเกี่ยวกับการนำเทคโนโลยีชีวมิติมาให้บริการในภาคการเงิน เพื่อให้เข้าใจถึงประโยชน์และสิทธิของผู้ใช้บริการที่เกี่ยวข้องกับการใช้เทคโนโลยีชีวมิติ

(6) กำหนดให้มีกระบวนการเปิดเผยข้อมูลชีวมิติตามที่กฎหมายกำหนด โดยในกรณีที่มีการส่งข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการให้บุคคลที่สาม เช่น ผู้ให้บริการภายนอก ผู้ให้บริการทางการเงินต้องได้รับความยินยอมจากผู้ใช้บริการก่อนหรือในขณะนั้น หรือเป็นไปตามที่กฎหมายกำหนด และต้องดำเนินการอย่างระมัดระวัง โดยต้องแจ้งข้อมูลเกี่ยวกับเปิดเผยหรือส่งข้อมูลชีวมิตินั้นให้ผู้ใช้บริการทราบ รวมทั้งให้บุคคลที่สามที่ได้รับข้อมูลชีวมิติของผู้ใช้บริการ สามารถใช้งานข้อมูลชีวมิติได้เท่าที่ได้รับความยินยอมหรือตามที่กฎหมายกำหนดเท่านั้น

หลักการที่ 6 การควบคุมความเสี่ยงด้านปฏิบัติการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีการบริหารจัดการความเสี่ยงด้านปฏิบัติการที่สำคัญโดยครอบคลุมทั้งกระบวนการรองรับการให้บริการอย่างต่อเนื่อง การตรวจสอบธุรกรรมที่อาจผิดปกติ รวมถึงมีกระบวนการควบคุมต่าง ๆ ที่เกี่ยวข้องกับผู้ให้บริการภายนอก เพื่อให้มั่นใจได้ว่าผู้ใช้บริการจะได้รับบริการทางการเงินด้วยเทคโนโลยีชีวมิติที่มั่นคงปลอดภัยและเชื่อถือได้

แนวทางที่พึงปฏิบัติ

(1) มีแนวทางรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business continuity plan) สำหรับการให้บริการทางการเงินด้วยเทคโนโลยีชีวมิติ ซึ่งครอบคลุมระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและกระบวนการปฏิบัติงานหากระบบขัดข้อง นอกจากนี้ผู้ให้บริการทางการเงินควรมีแผนรับมือเหตุการณ์ฉุกเฉินด้านไซเบอร์ที่ครอบคลุมข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติ เช่น เหตุการณ์พยายามลักลอบเข้าถึงข้อมูล เหตุการณ์ข้อมูลรั่วไหล รวมถึงมีการซักซ้อมการดำเนินการตามแผนดังกล่าวอย่างสม่ำเสมอ

(2) มีกระบวนการวิเคราะห์ ตรวจสอบธุรกรรมที่อาจผิดปกติ (Fraud monitoring) ที่เกี่ยวกับการทำธุรกรรมด้วยข้อมูลชีวมิติ เช่น การเปลี่ยนภาพใบหน้าของผู้ใช้บริการหลายครั้งภายในช่วงเวลาสั้น ๆ มีการกำหนดมาตรการพิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการเพิ่มเติม เพื่อให้สามารถพิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการได้อย่างมั่นใจมากขึ้นตามความจำเป็น เช่น การขอข้อมูลหรือเอกสารพิสูจน์ตัวตนอื่น ๆ จากแหล่งข้อมูลที่เชื่อถือได้ การส่งเรื่องให้ทีมงานเฉพาะด้านพิจารณาในเชิงลึก เป็นต้น

(3) มีการบริหารจัดการผู้ให้บริการภายนอกที่เกี่ยวข้องกับข้อมูลชีวมิติ เช่น การรวบรวมข้อมูลชีวมิติ การประมวลอัตลักษณ์และการเปรียบเทียบอัตลักษณ์ของผู้ใช้บริการผ่านช่องทางตัวแทน การเก็บข้อมูลอ้างอิงชีวมิติบนระบบคลาวด์คอมพิวติ้ง ต้องมีการวิเคราะห์ความเสี่ยงและกำหนดแนวทางป้องกันความเสี่ยงอย่างรัดกุม รวมถึงมีการทำสัญญาหรือข้อตกลงโดยระบุหน้าที่ ความรับผิดชอบ สิทธิในการตรวจสอบโดยหน่วยงานผู้กำกับดูแล และเงื่อนไขการให้บริการระหว่างกันโดยเฉพาะในเรื่องการดูแลข้อมูลชีวมิติของผู้ใช้บริการ และต้องคำนึงถึงความต่อเนื่องในการดำเนินธุรกิจรวมถึงการป้องกันความเสี่ยงที่อาจเกิดจากการยกเลิกหรือสิ้นสุดสัญญาข้อตกลง เพื่อให้ผู้ให้บริการทางการเงินสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และพร้อมรับการเปลี่ยนแปลงด้านเทคโนโลยีที่อาจเกิดขึ้นในอนาคต

ภาคผนวก ก
ข้อกำหนดเกี่ยวกับมาตรฐานขั้นต่ำและแนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติ

1. หลักการและเหตุผล

ธปท. จัดทำข้อกำหนดนี้ขึ้นเพื่อให้ผู้ให้บริการทางการเงินมีมาตรฐานขั้นต่ำและแนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าของผู้ใช้บริการ ในการที่จะได้รับข้อมูลที่มีคุณภาพเพียงพอต่อการนำไปประมวลผลเพื่อ ระบุ พิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการได้อย่างแม่นยำ น่าเชื่อถือ สอดคล้องกับมาตรฐานสากล

2. รายละเอียดของข้อกำหนด

ส่วนที่ 1 มาตรฐานขั้นต่ำสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติ[9]

การรวบรวมภาพใบหน้า ทั้งกรณีที่ผู้ให้บริการทางการเงินพบเห็นผู้ใช้บริการต่อหน้า และไม่พบเห็นผู้ใช้บริการต่อหน้า ภาพใบหน้าต้องมีคุณลักษณะอย่างน้อยดังต่อไปนี้

1.1 ความละเอียดของภาพไม่น้อยกว่า 1280 x 720 pixels หรือ 1080 x 1080 pixels ทั้งนี้ อาจปรับเปลี่ยนขนาดความกว้างและความสูงของภาพให้สอดคล้องกับพัฒนาการของเทคโนโลยีได้ หากยังคงสามารถรักษาระดับความแม่นยำได้ตามเกณฑ์ที่กำหนด

1.2 การบีบอัดข้อมูลภาพถ่ายควรใช้การบีบอัดข้อมูลแบบไม่สูญเสีย (Lossless data compression) หรือในกรณีที่ใช้การบีบอัดข้อมูลแบบสูญเสียบางส่วน (Lossy data compression) ต้องตรวจสอบให้มั่นใจได้ว่าคุณภาพของภาพอยู่ในระดับที่เพียงพอต่อการใช้งาน

1.3 ภาพเป็นชนิดภาพสี

1.4 ลูกค้าต้องแสดงใบหน้าทั้งหมด ในลักษณะปกติ (ไม่ยิ้ม และปากปิด) ใบหน้าตรง และมองตรงมายังกล้อง

1.5 ภาพต้องคมชัด และอยู่ในโฟกัส

1.6 ภาพต้องแสดงส่วนของศีรษะทั้งหมดของผู้ใช้บริการโดยปราศจากสิ่งปกคลุม ยกเว้นกรณีสวมเครื่องแต่งกายของศาสนา หรือวัสดุทางการแพทย์ ทั้งนี้ ภาพต้องแสดงใบหน้าทั้งหมดของผู้ใช้บริการอย่างชัดเจน

1.7 ภาพต้องแสดงดวงตาของผู้ใช้บริการอย่างชัดเจน และไม่มีสีแดง (Red-eye)

1.8 ผู้ใช้บริการสามารถใส่แว่นสายตาขณะถ่ายภาพ หากภาพที่ถ่ายออกมาแสดงให้เห็นดวงตาอย่างชัดเจนโดยไม่มีเงาหรือแสงสะท้อนจากแว่น

1.9 ผู้ใช้บริการไม่สามารถใส่แว่นตากันแดด หรือแว่นเคลือบสีขณะถ่ายภาพ

1.10 ความยาวของใบหน้า (จากศีรษะถึงคาง) ประมาณร้อยละ 60-80 ของความสูงของภาพ

---

[9] อ้างอิงตามมาตรฐาน ISO 19794-5 Biometric data interchange formats -- Part 5 Face image data

1.11 ภาพต้องไม่แสดงส่วนหนึ่งส่วนใดของบุคคลหรือวัตถุอื่นบนใบหน้าของผู้ใช้บริการหรือบนฉากหลังของภาพ ในลักษณะที่อาจส่งผลกระทบต่อความสามารถในการนำไปใช้เพื่อการเปรียบเทียบข้อมูลชีวมิติอย่างมีนัยสำคัญ

1.12 ใบหน้าของผู้ใช้บริการที่ปรากฏอยู่ในภาพต้องมีความสว่างเพียงพอ

ส่วนที่ 2 แนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติ[10]

ผู้ให้บริการทางการเงินอาจมีกระบวนการการถ่ายภาพและมีองค์ประกอบของภาพตามคุณลักษณะดังต่อไปนี้ เพื่อให้มั่นใจว่าผู้ให้บริการทางการเงินได้รับภาพที่มีคุณภาพที่ดีสำหรับนำไปประมวลผลต่อไป

2.1 ใบหน้าไม่ควรมีการก้ม เงย หัน หรือเอียงในระดับที่อาจส่งผลกระทบต่อความสามารถในการนำไปใช้เพื่อการเปรียบเทียบข้อมูลชีวมิติอย่างมีนัยสำคัญ

2.2 ไม่ควรมีเงามืดในเบ้าตาปรากฏบนใบหน้า

2.3 ความกว้างของใบหน้า (จากหูซ้ายถึงหูขวา) ประมาณร้อยละ 60-75 ของความกว้างของภาพ

2.4 ฉากหลังของภาพควรมีสีอ่อนและไม่มีลวดลาย รวมถึงไม่ปรากฏเงาของผู้ใช้บริการบนฉากหลังเพื่อให้สามารถแยกแยะใบหน้าของผู้ใช้บริการและฉากหลังได้อย่างชัดเจน

2.5 ไม่ควรมีใบหน้าของบุคคลอื่นปรากฏอยู่ในภาพ หรือมีระบบที่มีความสามารถในการแยกภาพใบหน้าของผู้ใช้บริการจากบุคคลอื่นอย่างแม่นยำ

2.6 ควรจัดให้มีสภาพแวดล้อมที่มีแสงเพียงพอต่อการถ่ายภาพสำหรับกรณีการถ่ายภาพที่สาขาหรือจุดให้บริการ และมีคำแนะนำสภาพแวดล้อมที่เหมาะสมแก่ผู้ใช้บริการในการถ่ายภาพกรณีการถ่ายภาพด้วยตนเองผ่านโทรศัพท์เคลื่อนที่ ทั้งนี้ แสงที่ตกกระทบบนใบหน้าควรมีความสม่ำเสมอ โดยไม่มีจุดสว่าง (Hot spots) ปรากฏโดยเด่นชัดบนใบหน้า

2.7 ในขณะที่ทำการถ่ายภาพ ควรมีการแสดงกรอบ หรือเส้นช่วยนำ ในจอภาพของผู้ปฏิบัติงานหรือหน้าจอโทรศัพท์เคลื่อนที่หรือคอมพิวเตอร์ของผู้ใช้บริการ ที่จะช่วยให้สามารถปรับเปลี่ยนตำแหน่งการถ่ายภาพเพื่อให้ได้ภาพถ่ายที่มีคุณภาพตามที่กำหนดได้ง่ายขึ้น

[10] อ้างอิงตามมาตรฐาน ISO 19794-5 Biometric data interchange formats -- Part 5 Face image data

เอกสารแนบ 2

แบบรายงานข้อมูลการใช้เทคโนโลยี Biometrics

ชื่อผู้ให้บริการ.....

สำหรับรอบสิ้นสุดวันที่.....

หัวข้อ	การรายงานข้อมูล	ความถี่	กำหนดส่ง
1. ความแม่นยำของเทคโนโลยี Biometrics	1) Accuracy rate 2) False acceptance rate 3) False rejection rate	ราย 6 เดือน หรือเมื่อมีการปรับปรุงแบบจำลอง	ภายใน 21 วันนับจากวันสิ้นงวดที่รายงาน หากวันที่ครบกำหนดส่งตรงกับวันหยุดให้ส่งข้อมูลภายในวันทำการถัดไป
2. ความพร้อมใช้ของระบบที่เกี่ยวข้องกับการใช้ Biometrics	ร้อยละ ..... (ไม่นับรวม maintenance downtime)	รายไตรมาส	
3. ปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยี Biometrics รวมถึงแนวทางแก้ปัญหา (ถ้ามี)	1) จำนวนและรายละเอียดข้อร้องเรียน 2) จำนวนและเหตุการณ์ทุจริต 3) จำนวนและข้อผิดพลาดที่พบ 4) ประเด็นอื่น ๆ ที่พบ	รายไตรมาส	

<u>หมายเหตุ</u>

1. Accuracy rate = $\frac{\text{(True Accept+True Reject)}}{\text{(True Accept+True Reject+False Accept+False Reject)}} \times 100$

2. False acceptance rate = $\frac{\text{False Accept}}{\text{False Accept+True Reject}} \times 100$

3. False rejection rate = $\frac{\text{False Reject}}{\text{False Reject+True Accept}} \times 100$

คำถามพบบ่อย (FAQ)
แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometrics Technology) ในการให้บริการทางการเงิน
กันยายน 2566

ส่วนที่ 1 ขอบเขตของแนวปฏิบัติ

คำถาม	คำตอบ
1. การประยุกต์ใช้เทคโนโลยีชีวมิติกับธุรกรรมทางการเงินในลักษณะใดบ้างที่ต้องหารือ ธปท. ก่อนดำเนินการ	การใช้เทคโนโลยี Facial Recognition กับธุรกรรมที่มีความเสี่ยงแตกต่างจากการเปิดบัญชี เช่น การชำระเงิน การถอนเงินที่ตู้ ATM การแลกเปลี่ยนเงินตราต่างประเทศที่ FX Booth การทำธุรกรรมที่ Banking Agent ผู้ให้บริการทางการเงินต้องหารือ ธปท. ก่อนดำเนินการ ทั้งนี้ สำหรับธุรกรรมที่มีความเสี่ยงต่ำกว่าการเปิดบัญชี เช่น การ Log-in เข้า Mobile Application การยืนยันการทำธุรกรรมการเงินมูลค่าสูงผ่าน Mobile Application ผู้ให้บริการทางการเงินสามารถดำเนินการได้โดยปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้อง สำหรับการเปรียบเทียบลายนิ้วมือ (Fingerprint Recognition) การเปรียบเทียบภาพม่านตา (Iris Recognition) การเปรียบเทียบเสียง (Voice Recognition) ผู้ให้บริการทางการเงินสามารถติดต่อฝ่ายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธปท. เพื่อนัดหมายการประชุมหารือรายละเอียดเบื้องต้น โดยส่งการนัดหมายที่ E-Mail : FinTechDept@bot.or.th หรือโทรศัพท์ 02-283-6892
2. การนำเทคโนโลยีชีวมิติมาใช้ในลักษณะใดที่เข้าข่ายต้องทดสอบใน Regulatory Sandbox	การใช้เทคโนโลยีชีวมิติที่จะถูกกำหนดให้เป็นมาตรฐานกลางร่วมกันในภาคการเงิน ยกตัวอย่าง เช่น การใช้ Voice recognition ซึ่งอาจได้รับการพิจารณาร่วมกันให้กำหนดเป็นมาตรฐานกลางในอนาคต เป็นต้น
3. การนำเทคโนโลยีชีวมิติมาใช้ในลักษณะใดที่ไม่เข้าข่ายต้องทดสอบใน Regulatory Sandbox หรือ Own Sandbox	การนำเทคโนโลยีชีวมิติมาใช้โดยมีลักษณะดังต่อไปนี้ 1. การใช้เทคโนโลยี Facial Recognition ในกระบวนการพิสูจน์ตัวตนลูกค้า สำหรับธุรกรรมการเปิดบัญชีเงินฝาก เปิดบัญชี e-Money สมัครใช้บริการสินเชื่อ และธุรกรรมอื่นที่มีการพิสูจน์ตัวตนและมีความเสี่ยงในลักษณะเดียวกัน ผู้ให้บริการทางการเงินสามารถดำเนินการได้โดยไม่จำเป็นต้องทดสอบใน Regulatory Sandbox โดยต้องปฏิบัติตามหลักเกณฑ์ของ ธปท. ที่เกี่ยวข้อง และนำส่งรายงานการตรวจประเมินการประยุกต์ใช้เทคโนโลยีชีวมิติ (Biometrics) ในการให้บริการทางการเงินซึ่งได้ผ่านการประเมินครบถ้วนแล้วประกอบการพิจารณา 2. เป็นการใช้เทคโนโลยีชีวมิติเพื่อการปฏิบัติงานภายในองค์กรและไม่เกี่ยวข้องกับข้อมูลของลูกค้า เช่น การตรวจสอบข้อมูลชีวมิติของพนักงานเพื่อเข้าพื้นที่ปฏิบัติงานที่มีความอ่อนไหว เป็นต้น 3. เป็นการใช้เทคโนโลยีชีวมิติในลักษณะเป็นบริการอำนวยความสะดวกหรือเพิ่มความปลอดภัยให้แก่ลูกค้า เช่น การใช้ภาพใบหน้าหรือลายนิ้วมือของโทรศัพท์มือถือของลูกค้าเพื่อ

คำถาม	คำตอบ
	- Login เข้าใช้งาน Mobile Application ของผู้ให้บริการทางการเงินแทนการใช้รหัสผ่าน - การเข้า Mobile Application กรณีการเปลี่ยนโทรศัพท์มือถือ - การยืนยันการทำธุรกรรมการเงินมูลค่าสูงผ่าน Mobile Application เป็นต้น
4. ผู้ให้บริการทางการเงินที่ผ่านการทดสอบการใช้ Facial Recognition ใน Regulatory Sandbox และ Own Sandbox แล้วจะต้องดำเนินการอย่างไร	ผู้ให้บริการทางการเงินจะต้องรายงานประสิทธิภาพของเทคโนโลยี Facial recognition ให้ ธปท. รับทราบ ทุก 6 เดือน ตามแบบฟอร์มที่ ธปท. กำหนด จนกว่าจะนำส่งรายงานการตรวจประเมินการใช้เทคโนโลยีชีวมิติ (Biometrics) และได้รับการเห็นชอบจาก ธปท. จึงจะสามารถยุติการส่งรายงานประสิทธิภาพของเทคโนโลยี Facial recognition ได้
5. สถาบันการเงินและผู้ให้บริการระบบชำระเงินที่ต้องการนำเทคโนโลยี Facial recognition มาประยุกต์ใช้สำหรับการพิสูจน์ตัวตนลูกค้า (KYC) แต่ยังไม่เคยทดสอบใน Regulatory Sandbox หรือ Own Sandbox ต้องดำเนินการอย่างไร	นำส่งรายงานการตรวจประเมินการใช้เทคโนโลยีชีวมิติซึ่งได้ผ่านการประเมินครบถ้วนแล้วให้ ธปท. ให้ความเห็นชอบก่อนให้บริการ โดยนำส่งผ่านระบบ e-Application ของ ธปท. ตามหลักเกณฑ์การกำกับดูแลที่เกี่ยวข้อง
6. ความมีนัยสำคัญของการใช้เทคโนโลยี Facial Recognition กับบริการทางการเงินสามารถประเมินจากปัจจัยใดบ้าง	ประเมินได้จากปัจจัยต่างๆ ดังนี้ - ผลกระทบต่อลูกค้าส่วนใหญ่ของธนาคาร เช่น มีความเกี่ยวข้องต่อข้อมูลส่วนบุคคลหรืออัตลักษณ์ของลูกค้าซึ่งจัดเป็น Sensitive Data หรือมีความจำเป็นต้องมีการเก็บข้อมูลภาพใบหน้าจากลูกค้าจำนวนมาก - กระทบต่อระบบสถาบันการเงินในวงกว้าง เช่น มีการแลกเปลี่ยนข้อมูลภาพใบหน้าหรือข้อมูล KYC ของลูกค้ากับองค์กรภายนอก
7. กรณีผู้ให้บริการทางการเงินที่เคยผ่านการตรวจประเมินแล้ว แต่มีการเปลี่ยนแปลงผู้ให้บริการเทคโนโลยี (vendor) สำหรับระบบ Facial recognition ในภายหลัง จำเป็นต้องมีการตรวจประเมินการใช้เทคโนโลยีชีวมิติอีกครั้งหรือไม่	ไม่จำเป็นต้องตรวจประเมินการใช้เทคโนโลยีชีวมิติอีกครั้ง อย่างไรก็ตาม ผู้ให้บริการทางการเงินควรรายงานการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information echnology Risk) ของ ธปท. และปฏิบัติตามแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน อย่างเคร่งครัด

คำถาม	คำตอบ
8. การจัดทำรายงานการตรวจประเมินการใช้เทคโนโลยีชีวมิติ (Biometrics) ในการให้บริการทางการเงิน เกี่ยวข้องกับกรณีใดบ้าง	1) ผู้ให้บริการทางการเงินที่ต้องการนำเทคโนโลยี Facial recognition มาใช้ในการให้บริการทางการเงิน เช่น การทำ e-KYC สำหรับเปิดบัญชีเงินฝาก เปิดบัญชี e-Money ที่ยังไม่เคยผ่านการทดสอบเทคโนโลยี Facial Recognition ใน Regulatory Sandbox ต้องนำส่งรายงานการตรวจประเมินการใช้เทคโนโลยี ชีวมิติ (Biometrics) เพื่อประกอบการพิจารณา รวมถึงกรณีที่ผู้ให้บริการทางการเงินมีการใช้ตัวแทนหรือผู้ให้บริการภายนอกในการรวบรวมข้อมูลชีวมิติจากลูกค้า (เช่น Dip Chip Agent) ต้องนำส่งรายงานการตรวจประเมินการใช้เทคโนโลยีชีวมิติของตัวแทนด้วย 2) ผู้ให้บริการทางการเงินที่ผ่านการทดสอบภายใต้ Regulatory Sandbox ของ ธปท. แล้ว หากนำส่งรายงานการตรวจประเมินการใช้เทคโนโลยีชีวมิติให้ ธปท. พิจารณา และ ธปท. ไม่มีประเด็นขัดข้องแล้ว ผู้ให้บริการสามารถหยุดการนำส่งแบบรายงานข้อมูลการใช้เทคโนโลยี Biometrics ได้ ทั้งนี้ ผู้ให้บริการทางการเงินสามารถนำส่งรายงานการตรวจประเมินการใช้เทคโนโลยีชีวมิติ(Biometrics) ให้ ธปท. พิจารณา ผ่านทางระบบ e-Application
9. การตรวจประเมินการใช้เทคโนโลยีชีวมิติ (Biometrics) สามารถดำเนินการโดยใครได้บ้าง	การตรวจประเมินการใช้เทคโนโลยีชีวมิติ (Biometrics) สามารถดำเนินการได้โดยผู้ตรวจสอบภายใน (Internal Audit) ที่มีความเป็นอิสระ หรือผู้ตรวจสอบภายนอกที่มีความเชี่ยวชาญ
10. สำหรับผู้ให้บริการทางการเงินที่ผ่านการทดสอบใน Regulatory Sandbox ก่อนแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometrics Technology) ในการให้บริการทางการเงิน ฉบับปรับปรุงปี 2566 จะมีกำหนดการตรวจประเมินอย่างไร	ผู้ให้บริการทางการเงินสามารถส่งรายงานการตรวจประเมินให้แล้วเสร็จภายในปี 2567
11. ผู้ให้บริการทางการเงินที่ผ่านการทดสอบใน Regulatory Sandbox สามารถใช้รายงานอื่นมานำส่งทดแทนรายงานการตรวจประเมินได้หรือไม่	ผู้ให้บริการทางการเงินยังคงต้องนำส่งรายงานตรวจประเมิน โดยสามารถนำรายงานหรือผลการทดสอบที่เกี่ยวข้องเช่น รายงานทดสอบเจาะระบบ รายงานการทดสอบ Presentation attack detection ซึ่งได้ดำเนินการไว้แล้วมาประกอบ/อ้างอิงในรายงานการตรวจประเมินได้ หากวันที่ได้รายงานหรือดำเนินการทดสอบดังกล่าวอยู่ในช่วงเวลา 2 ปี ก่อนหน้าวันที่นำส่งรายงานการตรวจประเมิน

ส่วนที่ 2 สาระสำคัญของแนวปฏิบัติ

คำถาม	คำตอบ
1. ผู้ให้บริการทางการเงินต้องจัดทำนโยบายด้านชีวมิติภายในองค์กรฉบับใหม่ขึ้นมาเพิ่มเติมสำหรับการกำกับดูแลข้อมูลชีวมิติโดยเฉพาะหรือไม่	ผู้ให้บริการทางการเงินสามารถปรับปรุงนโยบายต่าง ๆ ภายในองค์กรที่มีอยู่เดิม ให้มีเนื้อหาครอบคลุมเรื่องการกำกับดูแลข้อมูลชีวมิติ ทั้งนี้ ผู้ให้บริการทางการเงินอาจพิจารณาจัดทำนโยบายภายในองค์กรฉบับใหม่สำหรับการกำกับดูแลข้อมูลชีวมิติ เพื่อให้ผู้ปฏิบัติงานมีความเข้าใจและสามารถนำไปปฏิบัติได้
2. การประเมินการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงินในด้านต่างๆ สามารถดำเนินการได้โดยใครบ้าง	ผู้ให้บริการทางการเงินสามารถมอบหมายให้คณะกรรมการ คณะทำงาน หรือหน่วยงานธุรกิจภายในองค์กรที่เกี่ยวข้องกับการประยุกต์ใช้หรือบริหารจัดการข้อมูลชีวมิติเป็นผู้ประเมินความเหมาะสมและความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีชีวมิติ
3. กรณีลูกค้าที่อาศัยอยู่ในต่างประเทศมีความจำเป็นต้องพิสูจน์ยืนยันตัวตนในกระบวนการ KYC หรือมาตรการป้องกันการทุจริต แต่มีข้อจำกัดเรื่องการเข้าถึงจุดบริการอ่านบัตรประชาชน (Dip Chip) ผู้ให้บริการทางการเงินสามารถให้บริการรองรับลูกค้าด้วยวิธีการใดได้บ้าง	ผู้ให้บริการทางการเงินอาจพิจารณาการใช้เทคโนโลยี Facial recognition จากแหล่งข้อมูลที่เชื่อถือได้ (Trusted sources) อื่น เช่น - ใช้การพิสูจน์ตัวตนลูกค้าจากการเปรียบเทียบข้อมูลภาพใบหน้าจาก NFC Chip ในหนังสือเดินทางกับการถ่ายภาพ Selfie ใน Mobile Application ของธนาคาร - ใช้การพิสูจน์ตัวตนลูกค้าผ่านบริการ NDID (ในกรณีที่ลูกค้าเคยลงทะเบียน NDID กับธนาคารอื่นก่อนหน้า) ทั้งนี้ ผู้ให้บริการทางการเงินควรคำนึงถึงความแม่นยำและเชื่อถือได้ของเทคโนโลยี Facial recognition และความปลอดภัยข้อมูลชีวมิติของลูกค้าเป็นสำคัญ
4. ผู้ให้บริการทางการเงินต้องจัดให้มีเทคโนโลยี Liveness Detection สำหรับการลงทะเบียนผู้ใช้บริการแบบต่อหน้า (Face-to-Face) หรือไม่	ไม่จำเป็น อย่างไรก็ตาม ผู้ให้บริการทางการเงินยังคงต้องกำหนดให้มีกลไกการตรวจสอบการปลอมแปลงอัตลักษณ์ เช่น มีกระบวนการให้เจ้าหน้าที่ต้องพิสูจน์หรือยืนยันตัวตนลูกค้ากับแหล่งข้อมูลที่เชื่อถือได้ควบคู่กับกระบวนการอื่นที่เพิ่มเติมที่มีความรัดกุมเพียงพอ
5. การทดสอบความสามารถในการปลอมแปลงชีวมิติ (Presentation Attack Detection Testing) ควรดำเนินการอย่างไร	การทดสอบความสามารถในการตรวจจับการปลอมแปลงชีวมิติควรมีจำนวนผู้เข้าร่วมทดสอบที่มากเพียงพอและทดสอบการปลอมแปลงชีวมิติด้วยวิธีการในระดับความซับซ้อนที่หลากหลาย โดยมีจำนวน Test Case รวมไม่ต่ำกว่า 100 Test Case ทั้งนี้ เทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติที่ทำการทดสอบควรสามารถป้องกันการปลอมแปลงชีวมิติที่ระดับต่ำและปานกลางได้อย่างน้อยร้อยละ 90 และต้องดำเนินการแก้ไขข้อบกพร่องต่างๆ ให้เรียบร้อยก่อนให้บริการ หรือมีมาตรการอื่นทดแทนเพื่อปิดความเสี่ยง
6. ผู้ให้บริการทางการเงินสามารถประยุกต์ใช้การถ่ายภาพใบหน้าในบัตรประจำตัวประชาชนแทนการอ่านข้อมูลภาพใบหน้าจากชิปในบัตรประจำตัวประชาชน (Dip Chip) ได้ในกรณีใดบ้าง	สามารถใช้การถ่ายภาพหน้าบัตรประจำตัวประชาชนได้กับธุรกรรมการเปิดบัญชี e-Money ที่มีระดับความเสี่ยงต่ำและความเสี่ยงสูงบรรเทา ทั้งนี้ ควรมีกระบวนการหรือเทคโนโลยีพิสูจน์การปลอมแปลงบัตรควบคู่ด้วย

คำถาม	คำตอบ
7. การกำหนดระยะเวลาการปรับปรุงข้อมูลชีวมิติของผู้ใช้บริการให้เป็นปัจจุบันขึ้นอยู่กับปัจจัยใดบ้าง	ผู้ให้บริการทางการเงินควรมีการตรวจสอบและปรับปรุงข้อมูลชีวมิติของผู้ใช้บริการให้มีความถูกต้อง แท้จริง และเป็นปัจจุบันอย่างสม่ำเสมอ โดยคำนึงถึงความเปลี่ยนแปลงของอัตลักษณ์ทางชีวมิติของบุคคลที่เปลี่ยนแปลงตามกาลเวลา ประเภทธุรกรรม หลักเกณฑ์ที่เกี่ยวข้อง และแนวทางการบริหารความเสี่ยงของผู้ให้บริการทางการเงิน ทั้งนี้ ไม่ควรเกินระยะเวลาที่เอกสารหลักฐานที่ลูกค้าใช้ในการแสดงตนและพิสูจน์ตัวตนหมดอายุ
8. กรณีผู้ใช้บริการที่มีข้อจำกัดในการพิสูจน์ตัวตนด้วยเทคโนโลยี Facial Recognition เช่น เป็นคนพิการทางการเห็นหรือมีข้อจำกัดในการมองเห็น มีฝาแฝดหรือมีใบหน้าคล้ายกัน ผู้ให้บริการทางการเงินควรมีแนวทางรองรับอย่างไร	สำหรับการช่วยเหลือผู้ใช้บริการที่มีความพิการทางการเห็นหรือมีข้อจำกัดในการมองเห็น ผู้ให้บริการทางการเงินควรจัดให้มีเครื่องมือหรือแนวทางเสริม เช่น - มีเสียงอธิบายประกอบในขั้นตอนการทำ Liveness detection ใน Mobile Application -ให้พนักงานอำนวยความสะดวกและให้ความช่วยเหลือในการทำธุรกรรมที่สาขาเมื่อคนพิการร้องขอ สำหรับกรณีลูกค้ามีฝาแฝด ผู้ให้บริการทางการเงินควรระบุข้อจำกัดของเทคโนโลยีในการเปรียบเทียบอัตลักษณ์ สำหรับกรณีที่ผู้ใช้บริการมีฝาแฝดหรือใบหน้าคล้ายกันไว้ใน Terms and Conditions ของเอกสารคำขอเปิดบัญชี และการขอใช้บริการต่างๆ ที่เกี่ยวข้อง เพื่อให้ลูกค้าทราบถึงข้อจำกัดของเทคโนโลยีดังกล่าว
9. กรณีที่ผู้ใช้บริการพิสูจน์หรือยืนยันตัวตนด้วยข้อมูลชีวมิติไม่สำเร็จ ผู้ให้บริการทางการเงินควรมีกระบวนการจำกัดจำนวนครั้งที่ผู้ใช้บริการสามารถพิสูจน์หรือยืนยันตัวตนด้วยข้อมูลชีวมิติไม่สำเร็จอย่างไร	ผู้ให้บริการทางการเงินควรมีมาตรการในการจำกัดจำนวนครั้งที่ผู้ใช้บริการสามารถพิสูจน์หรือยืนยันตัวตนด้วยข้อมูลชีวมิติ โดยอาจจำกัดจำนวนครั้งของการยืนยันตัวตนด้วยชีวมิติให้ผิดพลาดอย่างต่อเนื่องได้ไม่เกิน 5 ครั้งกรณีทั่วไป หรือไม่เกิน 10 ครั้ง กรณีที่ใช้งานการตรวจจับการปลอมแปลงชีวมิติ โดยหากครบกำหนดแล้วอาจดำเนินการอย่างใดอย่างหนึ่ง ดังนี้ 1) หน่วงเวลาอย่างน้อย 30 วินาทีก่อนอนุญาตให้ยืนยันตัวตนครั้งถัดไป และเพิ่มการหน่วงเวลาก่อนอนุญาตให้ยืนยันตัวตนครั้งต่อไป เช่น หน่วงเวลาอย่างน้อย 2 นาที 4 นาที 8 นาที และเพิ่มขึ้นตามจำนวนครั้งของการยืนยันตัวตนผิดพลาด 2) ระงับการยืนยันตัวตนด้วยชีวมิติและให้ผู้ใช้บริการยืนยันตัวตนด้วยวิธีอื่น
10. การกำหนดขอบเขตการตรวจสอบกระบวนการรักษาความปลอดภัยข้อมูลชีวมิติในรอบการตรวจสอบประจำปีสามารถพิจารณาจากปัจจัยใดบ้าง	ผู้ให้บริการทางการเงินสามารถกำหนดขอบเขตการตรวจสอบโดยพิจารณาจากผลการประเมินความเสี่ยงธุรกรรมที่เกี่ยวข้องกับข้อมูลชีวมิติ ผลการตรวจสอบในรอบปีที่ผ่านมา รวมถึงเหตุการณ์ผิดปกติที่เคยเกิดในอดีต เพื่อให้บรรลุถึงเป้าหมายในการรักษา/เพิ่มระดับความมั่นคงปลอดภัยที่ได้รับการยอมรับตามเกณฑ์ที่เกี่ยวข้อง และมาตรฐานสากล

คำถาม	คำตอบ
11. การกำหนดให้ความละเอียดขั้นต่ำของภาพใบหน้ามีความสำคัญอย่างไร	การกำหนดความละเอียดของภาพขั้นต่ำมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่าภาพที่รวบรวมมาได้นั้น จะเป็นข้อมูลที่มีคุณภาพที่ดีต่อการนำไปประมวลผล เพื่อ ระบุ พิสูจน์หรือยืนยันตัวตนผู้ใช้บริการได้อย่างแม่นยำ น่าเชื่อถือ สอดคล้องกับมาตรฐานสากล รวมถึงการพัฒนานวัตกรรมต่อยอดในอนาคต ทั้งนี้ หากผู้ให้บริการทางการเงินมีการรวบรวมภาพใบหน้าโดยมีความละเอียดต่ำกว่าความละเอียดของภาพขั้นต่ำที่กำหนด ผู้ให้บริการทางการเงินต้องมีมาตรการในการพิสูจน์ให้มั่นใจว่าความแม่นยำในการเปรียบเทียบอัตลักษณ์ของระบบ เช่น ค่า FAR FRR มีความแม่นยำอยู่ในระดับที่กำหนด
12. การกำหนดให้ลูกค้าต้องแสดงใบหน้าทั้งหมด ในลักษณะปกติ (เช่น ไม่ยิ้ม และปากปิด) ในขั้นตอนการลงทะเบียนลูกค้า มีความสำคัญอย่างไร	การกำหนดให้ลูกค้าต้องแสดงใบหน้าทั้งหมด ในลักษณะปกติ (ไม่ยิ้ม และปากปิด) มีวัตถุประสงค์เพื่อให้มั่นใจได้ว่าภาพที่รวบรวมมาได้นั้น จะเป็นข้อมูลที่มีคุณภาพที่ดีต่อการนำไปประมวลผลเพื่อระบุ พิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการได้อย่างแม่นยำ น่าเชื่อถือ สอดคล้องกับมาตรฐานสากล ทั้งนี้ หากผู้ให้บริการทางการเงินมีการรวบรวมภาพใบหน้าลูกค้าโดยมีลักษณะยิ้มหรือเปิดปาก ผู้ให้บริการทางการเงินต้องมีมาตรการในการพิสูจน์ให้มั่นใจว่าความแม่นยำในการเปรียบเทียบอัตลักษณ์ของระบบยังมีความแม่นยำ เช่น ค่า FAR FRR อยู่ในระดับที่กำหนด
13. การรับส่งข้อมูลชีวมิติภายในศูนย์ประมวลผลภายในจำเป็นต้องใช้การเข้ารหัสข้อมูลในระหว่างการรับส่ง (Data-in-Transit) หรือไม่	ผู้ให้บริการทางการเงินควรพิจารณาใช้การเข้ารหัสข้อมูลชีวมิติโดยอ้างอิงตามนโยบายการจัดชั้นความลับข้อมูล (Data Classification Policy) อย่างไรก็ตาม การรับส่งข้อมูลชีวมิติภายในศูนย์ประมวลผลภายในองค์กรควรมีการป้องกันการเข้าถึงจาก Network Zone ภายนอกและ Network Zone ที่ไม่เกี่ยวข้องอย่างรัดกุม รวมถึงมีการใช้วิธีการที่ปลอดภัยในการรับส่งข้อมูลชีวมิติระหว่างระบบงาน
14. การประเมินช่องโหว่และการทดสอบเจาะระบบสำหรับระบบที่เกี่ยวข้องกับข้อมูลชีวมิติสามารถดำเนินการร่วมกับการทดสอบที่ผู้ให้บริการทางการเงินจัดให้มีอยู่แล้วเป็นประจำทุกปีได้หรือไม่	สามารถทำได้ ทั้งนี้ ขอบเขตการทดสอบดังกล่าวควรครอบคลุมถึงระบบงานและโครงสร้างพื้นฐานที่เกี่ยวข้องกับข้อมูลชีวมิติด้วย

แนวทางการตรวจประเมินการปฏิบัติตามแนวปฏิบัติชีวมิติ (Biometrics) ในการให้บริการทางการเงิน

ธนาคาร/บริษัท.....

วันที่ประเมิน/ออกรายงาน.....

ชื่อบริษัทผู้ประเมิน.....

สรุปภาพรวมผลการตรวจประเมิน
ขอบเขตการประเมิน
ภาพรวมผลการประเมิน
ด้านการกำกับดูแล
ด้านความปลอดภัยข้อมูลชีวมิติ

ด้านความน่าเชื่อถือของเทคโนโลยี
ด้านความพร้อมใช้
ข้อเสนอแนะและคำแนะนำ
รายชื่อผู้ประเมิน

ส่วนที่ 1 ข้อมูลเบื้องต้น

ตารางข้อมูลประกอบการพิจารณา

หัวข้อ	คำอธิบาย	รายละเอียด
1. ลักษณะบริการทางการเงิน		
1.1 รูปแบบและขอบเขตธุรกรรม	• *เช่น เปิดบัญชีเงินฝาก หรือบัญชี e-Money*	
1.2 กลุ่มลูกค้าเป้าหมาย	• *เช่น ลูกค้าลูกค้าบุคคลธรรมดา สัญชาติไทย อายุ 15 ปีขึ้นไป ลูกค้าธุรกิจ ลูกค้าต่างชาติ เป็นต้น*	
1.3 ช่องทางบริการ	• *เช่น ผ่านสาขา, Mobile Application ของผู้ให้บริการ*	
1.4 Business Model / Action Plan ในการดำเนินการในอนาคต	• *ระบุแผนการ deployment และบริการที่จะนำไปต่อยอด เช่น การเชื่อมต่อกับ NDID หรือช่องทางที่จะให้บริการเพิ่มเติมในอนาคต เช่น Banking Agent เครื่อง EDC device ของลูกค้า*	
2. เทคโนโลยีชีวมิติที่ใช้รองรับบริการ		
2.1 ชื่อเทคโนโลยีการเปรียบเทียบข้อมูลชีวมิติ ที่เลือกใช้ ชื่อบริษัทผู้พัฒนาและเหตุผลที่เลือกใช้	• ระบุชื่อบริษัทหรือชื่อเทคโนโลยี • โครงการที่ผ่านมาในอดีตทั้งในไทยและต่างประเทศ • *ผู้ให้บริการภายนอก/Vendor ที่ผู้ให้บริการเลือกใช้ พร้อมข้อมูลเกี่ยวกับผู้ให้บริการภายนอก/Vendor เช่น เป็น Vendor ของประเทศใด มีการให้บริการเทคโนโลยี Biometrics กับผู้ให้บริการรายอื่นด้วยหรือไม่ ใครบ้าง ธุรกิจ/บริการอะไร อาจยกตัวอย่างเบื้องต้น และเหตุผลที่เลือกผู้ให้บริการภายนอก/Vendor รายดังกล่าว*	
2.2 ผลการประเมินหรือรับรองเทคโนโลยีการเปรียบเทียบข้อมูลชีวมิติ	• *ข้อมูลเกี่ยวกับการได้รับการรับรองมาตรฐานหรือรับรองความน่าเชื่อถือของเทคโนโลยีจากองค์กรภายนอก (ถ้ามี)*	

หัวข้อ	คำอธิบาย	รายละเอียด
จากองค์กรภายนอก และมาตรฐานที่เกี่ยวข้อง	• *ผลการทดสอบและลำดับที่จากการจัดอันดับจากหน่วยงานภายนอก (ถ้ามี) เช่น การทดสอบ Face Recognition Vendor Test (FRVT) ของ NIST* • *มาตรฐานที่เกี่ยวข้องกับการรับรองหรือประเมินเทคโนโลยี (ถ้ามี)*	
2.3 ผลการทดสอบ Lab Test ของเทคโนโลยีการเปรียบเทียบข้อมูลชีวมิติที่ใช้	• *เป็นการทดสอบภายในที่ยังไม่ใช่การให้บริการกับลูกค้าจริง* • *ระบุจำนวนกลุ่มทดสอบ โดยควรมีจำนวน Sample size ที่ถูกนำมาใช้ในการทดสอบความแม่นยำแบบ NxN อย่างน้อย 1,000 ราย (อ้างอิงตามหัวข้อ I2.1 และ I3.1)* • *แสดงรายละเอียดวิธีการคำนวณ* • *ผลการทดสอบต้องมีค่า FAR ไม่เกิน 0.1% และ FRR ไม่เกิน 3%*	
2.4 ชื่อเทคโนโลยีการตรวจสอบการปลอมแปลงชีวมิติ (Presentation Attack Detection) ที่เลือกใช้และชื่อบริษัทผู้พัฒนาและให้บริการเทคโนโลยีดังกล่าว พร้อมเหตุผลที่เลือกใช้	• *ระบุรายละเอียดเกี่ยวกับเทคโนโลยีพอสังเขป* • *ผู้ให้บริการภายนอก/Vendor ที่ผู้ให้บริการเลือกใช้ พร้อมข้อมูลเกี่ยวกับผู้ให้บริการภายนอก/Vendor เช่น เป็น Vendor ของประเทศใด มีการให้บริการเทคโนโลยี Biometrics กับผู้ให้บริการรายอื่นด้วยหรือไม่ ใครบ้าง ธุรกิจ/บริการอะไร อาจยกตัวอย่างเบื้องต้น และเหตุผลที่เลือกผู้ให้บริการภายนอก/Vendor รายดังกล่าว*	
2.5 ผลการประเมินหรือรับรองเทคโนโลยีการตรวจสอบการปลอมแปลงชีวมิติจากองค์กรภายนอกและมาตรฐานที่เกี่ยวข้อง	• *ระบุข้อมูลเกี่ยวกับการได้รับการรับรองมาตรฐานหรือรับรองความน่าเชื่อถือของเทคโนโลยีจากองค์กรภายนอก (ถ้ามี) เช่น การทดสอบโดย Lab ที่ได้รับการรับรองโดย NIST หรือมาตรฐานที่เกี่ยวข้องกับการรับรองหรือประเมินเทคโนโลยี (ถ้ามี)*	

หัวข้อ	คำอธิบาย	รายละเอียด
3. กระบวนการรู้จักตัวตนลูกค้า (Know-Your-Customer)		
3.1 เอกสารหลักฐานที่ใช้สำหรับการแสดงตน (Identification)	• *ระบุเอกสารหลักฐานที่ใช้ในการแสดงตน เช่น บัตรประจำตัวประชาชน หรือ Passport*	
3.2 วิธีการตรวจสอบความถูกต้อง แท้จริง เป็นปัจจุบันของเอกสารหลักฐานที่ใช้สำหรับการพิสูจน์และยืนยันตัวตน	• *ระบุวิธีการในการตรวจสอบความถูกต้องแท้จริงของเอกสารหลักฐาน เช่น ใช้การ Verify DOPA Online ใช้การอ่านบัตรด้วยเครื่อง Smart Card Reader (Dip Chip) บริการยืนยันตัวตนรูปแบบดิจิทัล (NDID) เป็นต้น*	
3.3 กระบวนการพิสูจน์/ยืนยันตัวตน (โดยสังเขป)	• *แสดงขั้นตอนการทำ KYC/E-KYC โดยสังเขป* • *เปรียบเทียบกับกระบวนการในปัจจุบัน ซึ่งแสดง Customer Journey และ Operational flows ของผู้ให้บริการ*	
4. การคุ้มครองผู้ใช้บริการ		
4.1 ช่องทางการติดต่อและรับข้อร้องเรียน รวมทั้งกระบวนการจัดการปัญหาข้อร้องเรียน และดูแลผู้ใช้บริการทางการเงิน	• *ระบุช่องทางติดต่อและรับข้อร้องเรียนต่างๆ เช่น สาขา Call Center เป็นต้น* • *ความพร้อม/ความเพียงพอของพนักงานในทุกช่องทางที่ใช้ในการรับข้อร้องเรียนที่เกี่ยวข้องกับ Biometrics* • *มีกระบวนการในการรับและดำเนินการข้อร้องเรียน เก็บข้อมูลข้อร้องเรียน การติดตามความคืบหน้า การป้องกันการเกิดปัญหาซ้ำ กำหนดระยะเวลา SLA*	

หัวข้อ	คำอธิบาย	รายละเอียด
5. ด้านกฎเกณฑ์ที่เกี่ยวข้อง		
5.1 หลักเกณฑ์อื่นๆ ที่เกี่ยวข้อง พร้อมเหตุผลและความจำเป็น	• *พิจารณาว่าเป็นเทคโนโลยีที่มีนัยสำคัญที่จะต้องปฏิบัติตามหลักเกณฑ์ด้าน IT Risk ของ ธปท. หรือไม่* • *พิจารณาว่าเป็นการเพิ่มเติม/เปลี่ยนแปลงการให้บริการที่จะต้องปฏิบัติตามหลักเกณฑ์ของผู้ให้บริการชำระเงิน หรือผู้ให้บริการโอนเงินระหว่างประเทศหรือไม่* • *พิจารณาว่าเข้าข่ายต้องขออนุญาตหรือแจ้ง ธปท. เพื่อทราบในหลักเกณฑ์อื่นใดอีกหรือไม่*	

ส่วนที่ 2 แนวทางการตรวจประเมินการประยุกต์ใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงิน

หัวข้อที่ 1 - ด้านการกำกับดูแลการใช้เทคโนโลยีชีวมิติ (Governance)

หัวข้อ	วิธีการประเมิน	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
G1. การมีกลไกสำหรับกำกับดูแลการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงิน			
G1.1 มีคณะกรรมการภายในธนาคารหรือบริษัท ทำหน้าที่วิเคราะห์ ประเมิน หรือกลั่นกรองการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการกับลูกค้า	• *ระบุชื่อคณะกรรมการและสมาชิก หรือผู้บริหารที่เกี่ยวข้องกับการพิจารณาการใช้เทคโนโลยีชีวมิติ*		ระบุผล เช่น - ผ่าน - ไม่ผ่าน - ควรปรับปรุง ในประเด็นต่างๆ ได้แก่ ...
G1.2 คณะกรรมการดังกล่าวมีการประเมินความเหมาะสมในทางธุรกิจ เช่น ประโยชน์ของเทคโนโลยีชีวมิติที่นำมาใช้นั้นสามารถเพิ่มประสิทธิภาพในการให้บริการลูกค้าในธุรกรรมใดบ้าง รวมถึงประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลชีวมิติ เช่น ระดับความแม่นยำของเทคโนโลยี ความเสี่ยงจากภัยคุกคามทางไซเบอร์กับข้อมูลชีวมิติ เป็นต้น	• *มีมติพร้อมข้อคิดเห็นจากคณะกรรมการของ สง./คณะกรรมการ หรือหน่วยงานธุรกิจที่เกี่ยวข้องด้านการบริหารจัดการหรือด้านความเสี่ยง ตลอดจนการคุ้มครองผู้ใช้บริการทางการเงิน (ลูกค้า/ร้านค้า/หน่วยงานราชการ) เกี่ยวกับบริการที่ทดสอบ เช่น บันทึกการประชุม หรือเอกสารที่แสดงมติที่ประชุม ผลการอนุมัติ พร้อมข้อคิดเห็นที่คณะกรรมการพิจารณาในประเด็นที่เกี่ยวข้อง*		
G2: มีการกำหนดนโยบายต่างๆ ภายในองค์กรสำหรับการกำกับดูแลข้อมูลชีวมิติ			
G2.1 นโยบายด้าน IT มีเนื้อหาครอบคลุมการใช้เทคโนโลยีและข้อมูลชีวมิติ	• *ระบุนโยบายที่เกี่ยวข้องกับข้อมูลชีวมิติ เช่น นโยบายการดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) นโยบายการกำกับดูแลข้อมูล (Data*		

หัวข้อ	วิธีการประเมิน	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	governance policy) นโยบายการจัดชั้นความลับ (Data classification policy) • *หากมี Biometrics Policy ที่มีนโยบายที่ครอบคลุมในด้านต่อไปนี้ครบถ้วนแล้ว ได้แก่ IT Security, IT Risk Management, Data Governance และ Data Classification ผู้ให้บริการไม่จำเป็นต้องปรับปรุงเอกสารนโยบายอื่น ๆ ให้ครอบคลุมการใช้งาน biometrics เช่น IT Security Policy IT Risk Management Policy Data Governance Policy และ Data Classification Policy* • *หากไม่มีเอกสาร Biometrics Policy สามารถอ้างอิงเอกสารนโยบายฉบับอื่นที่ได้รับการ review ให้ครอบคลุมการใช้งาน biometrics แทนได้*		
G2.2 มีการกำหนดชั้นความลับและแนวทางจัดการข้อมูลประเภท Biometrics	• *ระบุชั้นความลับของข้อมูลขององค์กร และอธิบายเกณฑ์การจัดชั้นความลับ (Data Classification) ซึ่งอาจเป็นการปรับปรุงนโยบายการจัดชั้นความลับข้อมูลเดิมให้ครอบคลุมข้อมูลชีวมิติ* • *มีการกำหนดแนวทางในการดูแลรักษาความมั่นคงปลอดภัย ในการใช้งาน/จัดเก็บ/รับส่ง/ทำลาย ของข้อมูลแต่ละระดับชั้นความลับ (Data Handling)*		
G3: มีนโยบายหรือแนวทางในการกำกับดูแลผู้ให้บริการภายนอก (3rd Party Service Provider)			
G3.1 นโยบายการกำกับดูแลด้าน IT มีเนื้อหาครอบคลุมการดูแลความเสี่ยงจากการใช้ระบบประมวลผล	• *ระบุมาตรฐานขั้นต่ำที่ใช้ในปัจจุบัน เช่น* มาตรฐานขั้นต่ำด้านความปลอดภัยสำหรับการเชื่อมต่อกับผู้ให้บริการภายนอก		

หัวข้อ	วิธีการประเมิน	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
และการเก็บข้อมูลชีวมิติที่ระบบของผู้ให้บริการภายนอก	• *มีการระบุความเสี่ยงที่คาดว่าจะเกิดขึ้น (Risk Identification and Assessment) และการประเมินความเสี่ยง และแนวทางการบริหารจัดการความเสี่ยงที่ระบุ โดยครอบคลุมความเสี่ยงสำคัญ เช่น การรักษาความปลอดภัยข้อมูล ข้อมูลรั่วไหล และความเพียงพอของหลักฐานในการทำธุรกรรม* • *มีการระบุความเสี่ยง การควบคุมความเสี่ยง ระดับความเสี่ยงภายหลังพิจารณาการควบคุม*		
G3.2 มีการตรวจสอบบริการประมวลผลและจัดเก็บข้อมูลชีวมิติจากผู้ให้บริการภายนอก (3rd Party) อย่างสม่ำเสมอ และสอดคล้องตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก	• *ระบุรายละเอียดที่เกี่ยวข้องกับการสอบทานรายงานตรวจสอบความปลอดภัยของระบบ IT ของ 3rd Party Service Provider ในการรวบรวมข้อมูล Biometrics เป็นต้น โดยครอบคลุม* System Diagram และ Network Diagram ต้องครอบคลุมถึงระบบ IT และอุปกรณ์ Endpoint ที่เกี่ยวข้อง ของ 3rd Party Service Provider • *หากใช้อุปกรณ์ Endpoint ของผู้ให้บริการภายนอก บริษัทต้องทราบข้อมูลด้านความปลอดภัยต่าง ๆ มากเพียงพอ เสมือนกับเป็นผู้ดูแลอุปกรณ์นั้นเอง* • *ระบุเนื้อหาของขอบเขตและผลการสอบทานความปลอดภัยด้าน IT ที่ใช้บริการจาก Third Party แบบ End-to-End รวมถึงข้อสังเกตที่พบจากการสอบทานและแนวทางปรับปรุงตามข้อสังเกต และระบุเอกสารการอ้างอิงหลัก ที่ใช้ในการประเมิน/สอบทาน 3rd Party* • *ในสัญญา/ข้อตกลง มีกำหนดเรื่องความรับผิดชอบกรณีข้อมูลของลูกค้ารั่วไหลไว้หรือไม่ อย่างไรบ้าง ใน*		

หัวข้อ	วิธีการประเมิน	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	สัญญา/ข้อตกลง มีกำหนดเรื่องความรับผิดชอบ ต่อความถูกต้องเชื่อถือได้ของข้อมูลฯ ไว้อย่างไรบ้าง		
G3.3 มีการตรวจสอบบริการประมวลผลและจัดเก็บข้อมูลชีวมิติจากกรณีมีการใช้ Cloud Computing สำหรับการประมวลผลหรือจัดเก็บข้อมูลชีวมิติของผู้ใช้บริการ	• *มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยของผู้ให้บริการ Cloud หรืออาจอ้างอิงรายงานผลการสอบทาน/ตรวจสอบด้านการรักษาความมั่นคงปลอดภัยของผู้ให้บริการ Cloud โดยอาจใช้รายงานที่ออกโดยผู้เชี่ยวชาญที่มีความเป็นอิสระได้ (เช่น SOC 2 Type 2)*		
G4: มีนโยบายการดูแลและคุ้มครองข้อมูลของผู้ใช้บริการ			
G4.1 นโยบายการคุ้มครองข้อมูลส่วนบุคคลมีเนื้อหาครอบคลุมการดูแลข้อมูลชีวมิติของผู้ใช้บริการ	• *รูปแบบการขอ Consent มีการแบ่งแยกตามโครงการ/ธุรกรรม/บริการ/วิธีการในการเก็บรวบรวมภาพถ่ายจากลูกค้า เช่น ถ่ายภาพผ่าน Mobile Application บนโทรศัพท์มือถือของลูกค้าเอง ถ่ายภาพโดยพนักงานสาขา ถ่ายภาพผ่านอุปกรณ์ Kiosk* • *ข้อความสำหรับใช้ขอความยินยอม มีการแสดงรายการของข้อมูลที่ขอ และวัตถุประสงค์ของการนำข้อมูลไปใช้ที่เฉพาะเจาะจงและชัดเจน* • *ในกรณีที่ผู้ใช้งานมีความต้องการยกเลิกการใช้ Biometrics ผู้ให้บริการทางการเงิน ต้องมีการดำเนินการให้สอดคล้องกับพรบ คุ้มครองข้อมูล รวมถึงแจ้งข้อจำกัดการใช้งานในอนาคต และให้คำแนะนำอื่นๆ ที่จะอำนวยความสะดวกให้ผู้ใช้บริการสามารถดำเนินธุรกรรมต่อไปได้*		

สรุปผลการประเมินด้านการกำกับดูแลการใช้เทคโนโลยีชีวมิติ (Governance)

หัวข้อที่ 2 - ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลชีวมิติ (Confidentiality)

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
C1. มีแนวทางการดูแลอุปกรณ์ที่ใช้รวบรวมข้อมูลชีวมิติ (Endpoint) มีความปลอดภัย			
C1.1 มีแนวทางการรักษาความปลอดภัยของอุปกรณ์ Endpoint ที่เกี่ยวข้องกับการใช้เก็บรวบรวมและใช้งานข้อมูล Biometrics	• *แสดงรายละเอียดข้อมูลครอบคลุมอุปกรณ์ Endpoint ของผู้ให้บริการทางการเงินทุกประเภทที่ใช้งานร่วมกับข้อมูล Biometrics และการ dip-chip ดังต่อไปนี้* *1.ข้อมูลทั่วไปของอุปกรณ์ Endpoint* *1.1. ประเภทของอุปกรณ์ เช่น Apple iPad, Android Tablet, Smart Phone, Kiosk, EDC, POS, ATM/VTM, PC เป็นต้น* *1.2. รายละเอียด Technical Specification ของอุปกรณ์ เช่น ยี่ห้อ, รุ่น, Hardware, OS version, Software version เป็นต้น* *1.3. มีการใช้งานร่วมกับบริการอื่นหรือไม่ อย่างไร เช่น ใช้ kiosk ร่วมกับการชำระบิล, ใช้ POS ร่วมกับการชำระเงิน, ใช้ tablet/smart phone ร่วมกับการใช้งานทั่วไปของสาขา เป็นต้น* *2. การควบคุมความปลอดภัยทางกายภาพ* *2.1 อธิบายวิธีการรักษาความมั่นคงปลอดภัยทางกายภาพ เช่น วิธีป้องกันการติดตั้งอุปกรณ์ดักจับข้อมูล*		ระบุผล - ผ่าน - ไม่ผ่าน - ควรปรับปรุง

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	(tampering/skimming device) วิธีป้องกันการเข้าถึง port เชื่อมต่อ วิธีการป้องกันการดัดแปลงอุปกรณ์ เช่น เครื่อง Electronic Data Capture (EDC) เป็นต้น *2.2 อธิบายการสอบทานความปลอดภัยทางกายภาพ เช่น หน่วยงานที่รับผิดชอบ วิธีการสอบทาน รอบความถี่ในการสอบทาน จำนวนอุปกรณ์ที่ได้รับการสอบทาน เป็นต้น* *<u>3. การควบคุมความมั่นคงปลอดภัยทางสารสนเทศ</u>* *3.1 อธิบายวิธีการป้องกัน malware และการติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต (เช่น antivirus หรือ whitelist เป็นต้น)* *3.2 อธิบายวิธีการป้องกันการใช้งานอุปกรณ์ด้วยสิทธิ์ระดับสูง/สิทธิ์ผู้ดูแล (เช่น Root, Jailbreak เป็นต้น)* *3.3 อธิบายวิธีการป้องกันการเชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาต (เช่น อุปกรณ์เชื่อมต่อทาง port USB, Bluetooth เป็นต้น)* *3.4 อธิบายวิธีการป้องกันการเชื่อมต่อเครือข่ายที่ไม่ได้รับอนุญาต (เช่น WiFi สาธารณะ, WiFi hotspot, Internet เป็นต้น)* *3.5 อธิบายวิธีการป้องกันการเข้าถึง Storage ที่ไม่ได้รับอนุญาต (เช่น cloud storage, shared drive, removable media, external harddisk เป็นต้น)* *<u>4. มาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัยขั้นต่ำ</u> (Security Configuration Baseline)* *4.1 อธิบายการพิจารณาอนุมัติ Baseline ของอุปกรณ์ Endpoint ให้ความมั่นคงปลอดภัยและเหมาะสมกับลักษณะการใช้งาน เช่น หน่วยงานที่รับผิดชอบจัดทำ ผู้ที่*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	อนุมัติใช้งาน มาตรฐานที่อ้างอิง รอบความถี่ในการทบทวน เป็นต้น *4.2 เอกสาร Baseline ที่ใช้สำหรับอุปกรณ์ Endpoint* *4.3 Baseline ข้างต้นอ้างอิงตาม Standard หรือ Guideline ใด* *4.4 อธิบายการสอบทานการตั้งค่าของอุปกรณ์ Endpoint ให้สอดคล้องกับ Baseline เช่น หน่วยงานที่รับผิดชอบ วิธีการสอบทาน รอบความถี่ในการสอบทาน จำนวนอุปกรณ์ที่ได้รับการสอบทาน เป็นต้น* *5. การป้องกันข้อมูลรั่วไหลจากอุปกรณ์ Endpoint* *5.1 อธิบายวิธีการควบคุมไม่ให้มีการจัดเก็บข้อมูล Biometrics รวมถึงข้อมูล sensitive อื่นไว้บน Endpoint* *5.2 มีการพักข้อมูล Biometrics ไว้ชั่วคราวบนอุปกรณ์ Endpoint เช่น การ save เป็น temporary file และลบออกหลังจากใช้งานเสร็จ เป็นต้น หรือไม่ ถูกเข้ารหัสหรือไม่ มีการควบคุมอย่างไร* *6. ผลการประเมิน/ทดสอบด้านความปลอดภัย (เช่น VA / Pentest) ของอุปกรณ์ Endpoint* *7. แนวทางการบริหารจัดการ Security patch management ของอุปกรณ์ Endpoint*		
C1.2 กรณีมีการใช้บริการประมวลผลจากผู้ให้บริการภายนอก ควรไม่มีการเก็บข้อมูลชีวมิติคงค้างในอุปกรณ์ของผู้ให้บริการภายนอก	• *หากใช้อุปกรณ์ Endpoint ของผู้ให้บริการภายนอก บริษัทต้องทราบข้อมูลด้านความปลอดภัยต่าง ๆ มากเพียงพอ เสมือนกับเป็นผู้ดูแลอุปกรณ์นั้นเอง*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
C2: ระบบประมวลผลข้อมูลชีวมิติมีความปลอดภัยเชื่อถือได้			
C2.1 มีกระบวนการรักษาความปลอดภัยข้อมูลชีวมิติที่เข้มงวด หรือไม่มีการเก็บข้อมูลชีวมิติคงค้างในระบบประมวลผล	• *ระบุเส้นทางการไหล (Data Flow) ของข้อมูลชีวมิติ โดยครอบคลุมผู้ให้บริการที่เกี่ยวข้องและระบบที่เกี่ยวข้อง ตั้งแต่ อุปกรณ์ที่เก็บรวบรวม จนถึงการจัดเก็บในระบบจัดเก็บข้อมูล แบบ End-to-End* • *ระบุรายละเอียดการการจัดเก็บข้อมูล Biometrics แบบเข้ารหัส โดยครอบคลุมจุดเชื่อมต่อระบบและจุดจัดเก็บข้อมูลแบบ End-to-End อ้างอิงตามแผนภาพ IT Architecture* • *การจัดเก็บข้อมูล Biometrics ต้องมีการเข้ารหัส ทั้งนี้หากยังไม่มีการเข้ารหัสข้อมูลในปัจจุบัน ควรระบุแผนการปรับปรุงระบบ เช่น กรอบเวลาในการปรับปรุงระบบ วิธีการเข้ารหัส ระดับการเข้ารหัส ความยาวของ Encryption Key ที่ใช้ เป็นต้น*		
C2.2 กรณีมีการใช้บริการประมวลผลจากผู้ให้บริการภายนอก ควรไม่มีการเก็บข้อมูลชีวมิติคงค้างในระบบประมวลผลของผู้ให้บริการภายนอก	• *หากมีการใช้บริการประมวลผลชีวมิติผู้ให้บริการภายนอก บริษัทต้องทราบข้อมูลด้านความปลอดภัยต่าง ๆ มากเพียงพอ เสมือนกับเป็นผู้ดูแลอุปกรณ์นั้นเอง* • *ผู้ให้บริการทางการเงินต้องมีกระบวนการที่ทำให้มั่นใจว่า ผู้ให้บริการภายนอกจะไม่มีการเก็บข้อมูลชีวมิติของลูกค้าไว้ในระบบ เช่น การสอบทานรายงานตรวจสอบ เป็นต้น*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
C3: ระบบ IT Infrastructure ที่รองรับการประมวลผลข้อมูลชีวมิติมีความปลอดภัยเชื่อถือได้			
C3.1 แบ่งแยก Network Zone สำหรับฐานข้อมูลชีวมิติออกจากฐานข้อมูลส่วนบุคคลของลูกค้า รวมถึงแบ่งขอบเขตระบบเครือข่าย (Network zoning) และจัดวางระบบและข้อมูลอ้างอิงชีวมิติโดยคำนึงถึงระดับชั้นความลับข้อมูล	• *ระบุ Network Zone สำหรับระบบจัดเก็บข้อมูล Biometrics* • *ระบุแนวทางการรักษาความมั่นคงความปลอดภัยของข้อมูลชีวมิติและวิธีการการป้องกันการเข้าถึง (Access control) ทั้งนี้ ควรจัดวางระบบและฐานข้อมูล Biometrics ไว้ใน Network Zone ที่มีความปลอดภัยสูง และไม่จัดเก็บไว้ใน External Zone หรือ DMZ Zone*		
C3.2 มีอุปกรณ์ Firewall และ Intrusion Prevention System ป้องกันการเข้าถึงฐานข้อมูลชีวมิติของผู้ใช้บริการทางการเงิน	• *ระบุรายละเอียดอุปกรณ์ Firewall และ Intrusion Prevention System สำหรับการป้องกันการเข้าถึงข้อมูลชีวมิติ รวมถึงอุปกรณ์อื่นๆ ที่เกี่ยวข้อง เช่น Data Loss Prevention (DLP) เป็นต้น*		
C4: จัดเก็บข้อมูลชีวมิติด้วยความปลอดภัย			
C4.1 แยกฐานข้อมูลชีวมิติของลูกค้าออกจากฐานข้อมูลส่วนบุคคลอื่น	• *ระบุรายละเอียดเกี่ยวกับการจัดเก็บข้อมูล Biometrics ว่าจัดเก็บอยู่ที่ใด ในรูปแบบใด สามารถอ้างอิงถึงได้อย่างไร* • *ระบุรายละเอียดการจัดเก็บข้อมูลส่วนตัวอื่น ๆ ของลูกค้าว่า จัดเก็บอยู่ที่ใด ในรูปแบบใด สามารถอ้างอิงถึงได้อย่างไร* • *ต้องจัดเก็บข้อมูล Biometrics แยกจากข้อมูลส่วนตัวอื่นของลูกค้า (แยกในระดับ Server หรือ Database) ทั้งนี้หากยังไม่มีการแยกการจัดเก็บในปัจจุบัน ขอทราบแผนการปรับปรุงระบบ เช่น กรอบเวลาในการปรับปรุงระบบ แยกข้อมูลอะไรบ้าง นำไปเก็บไว้ที่*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	ใด เมื่อแยกแล้ววิธีการเข้าถึงข้อมูลจะแตกต่างกันอย่างไร ระหว่างข้อมูลแต่ละประเภท เป็นต้น		
C4.2 ไม่มีการเก็บข้อมูลชีวมิติตั้งต้นของผู้ใช้บริการ หรือมีการเก็บข้อมูลภาพใบหน้าลูกค้าในกรณีที่มีความจำเป็นและได้รับความยินยอมจากลูกค้า	• *ระบุขั้นตอนการเก็บข้อมูลชีวมิติหรือการเก็บข้อมูลภาพใบหน้า และมีเอกสารประกอบว่าไม่มีการเก็บข้อมูลชีวมิติตั้งต้นของผู้ใช้บริการ*		
C4.3 ไม่ระบุข้อมูลอ้างอิงชีวมิติโดยอ้างอิงด้วยข้อมูลที่สามารถระบุตัวตนของผู้ใช้บริการได้โดยตรง (Indirect reference)	• *ระบุวิธีการในการอ้างอิงเชื่อมโยงข้อมูลระหว่างข้อมูล Biometrics กับข้อมูลส่วนตัวอื่น ๆ ของลูกค้า และรายละเอียดการจัดเก็บโดยไม่สามารถระบุ/อ้างถึงข้อมูล Biometrics ด้วยข้อมูลส่วนตัวของลูกค้าโดยตรง เช่น หมายเลขบัตรประชาชน เลขประจำตัวผู้ใช้บริการ เป็นต้น* • *ทั้งนี้ หากมีการอ้างอิงข้อมูล Biometrics ด้วยข้อมูลส่วนตัวลูกค้าโดยตรงได้ในปัจจุบัน ขอให้ระบุแผนการปรับปรุงระบบ เช่น กรอบเวลาในการปรับปรุงระบบ ใช้ข้อมูลอะไรเป็น Reference เป็นต้น*		
C5: รับส่งข้อมูลชีวมิติด้วยความปลอดภัย			
C5.1 ใช้กระบวนการเข้ารหัสข้อมูลด้วยมาตรฐานที่มีความปลอดภัย	• *ระบุกระบวนการ Encryption Algorithm ที่ใช้ในแต่ละจุด ในขณะ Data at Rest โดยระบุว่าเป็นการเข้ารหัสในระดับใด เช่น ระดับ Field, File, Database, Hard disk, หรือ Storage* • *ระบุกระบวนการ Encryption Algorithm ที่ใช้ในแต่ละจุด ในขณะรับ/ส่งข้อมูล (Data in Transit) และรายละเอียดการจัดการ Encryption Key และ Key*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	Management ที่ใช้ในขณะ Data in Transit รวมถึงใช้มาตรฐาน Encryption ที่มีความปลอดภัย ไม่มีช่องโหว่ และมีความเป็นปัจจุบัน		
C5.2 จัดเก็บกุญแจสำหรับเข้ารหัสข้อมูลด้วยความปลอดภัย	• *ระบุรายละเอียดการจัดการ Encryption Key และ Key Management ที่ใช้ในขณะ Data at Rest เช่น ระบบ Vault จัดเก็บ Key อยู่ที่ใด (เช่น cloud /on-premise), ขั้นตอนการนำ Encryption Key ออกจาก Vault ไปติดตั้ง/ใช้งาน, อายุการใช้งาน กระบวนการเพิกถอน และการเปลี่ยน Key*		
C5.3 การรับส่งข้อมูลชีวมิติของผู้ใช้บริการกับผู้ให้บริการภายนอก (3rd Party) มีการเข้ารหัสข้อมูลด้วยมาตรฐานที่มีความปลอดภัย	• *มีข้อมูล System Diagram และ Network Diagram ที่ครอบคลุมถึงระบบ IT และอุปกรณ์ Endpoint ที่เกี่ยวข้องของ 3rd Party Service Provider* • *การรับ/ส่งข้อมูล Biometrics ที่มีข้อมูลเพียงพอในการระบุตัวตน กับบุคคลภายนอก (3rd Party / outsource / insource) ต้องมีการเข้ารหัสในระดับช่องทางสื่อสาร (Network/Transport Layer) และเข้ารหัสในระดับเนื้อข้อมูล Biometrics (ระดับ field/file)*		
C6: มีกระบวนการควบคุมการเข้าถึงข้อมูลชีวมิติหรือข้อมูลชีวมิติของผู้ใช้บริการอย่างเข้มงวด			
C6.1 กระบวนการให้สิทธิการเข้าถึงข้อมูลชีวมิติหรือข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการเท่าที่จำเป็นโดยผู้ปฏิบัติงานที่เกี่ยวข้องเท่านั้น	• *ระบุมาตรการการควบคุมการเข้าถึงระบบและข้อมูล Biometrics รวมถึงการกำหนดสิทธิ์ผู้ใช้งานและผู้ดูแลระบบ โดยครอบคลุมถึงระบบทั้งหมดที่เกี่ยวข้องกับข้อมูล Biometrics ทั้งในระดับ Application และ System รวมถึงครอบคลุมสิทธิของหน่วยงานภายนอก (ถ้ามี)*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	• *ระบุวิธีการพิสูจน์ตัวตนแบบ Multi-Factor ของบัญชีผู้ใช้งานสิทธิสูง (Privileged User)* • *ระบุวิธีการพิสูจน์ตัวตนแบบ Multi-Factor ของบัญชีผู้ใช้งาน (User) ที่สามารถเข้าถึงข้อมูลลูกค้าที่ระบบสามารถเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet Facing)*		
C6.2 มีการสอบทานสิทธิการเข้าถึงข้อมูลชีวมิติอย่างสม่ำเสมอ	• *มีตาราง Authorization Matrix ที่แสดงถึงสิทธิของบุคคลและระบบต่าง ๆ ที่สามารถเข้าถึงข้อมูล Biometrics ได้และ ต้องครอบคลุมถึงระบบทั้งหมดที่เกี่ยวข้องกับข้อมูล Biometric ทั้งในระดับ Application และ System ทั้งนี้ ผู้มีสิทธิการเข้าถึงข้อมูลชีวมิติ ไม่ควรได้รับสิทธิเข้าถึง แก้ไขบันทึกเหตุการณ์ (Log) ที่เกี่ยวข้องกับข้อมูลชีวมิติ* • *มีผู้รับผิดชอบในการ review Authorization Matrix ให้มั่นใจว่าเป็นการให้สิทธิ์ตามหน้าที่/ความจำเป็น และผู้ดูแลระบบต้องไม่สามารถเข้าถึง/แก้ไขข้อมูล biometrics โดยไม่ได้รับอนุญาต* • *มีการกระบวนจัดการ Privilege ID ที่รัดกุม* • *มีการกำหนดรอบการสอบทานสิทธิที่สอดคล้องกับนโยบายการรักษาความปลอดภัยขององค์กร*		
C6.3 มีกระบวนการตรวจสอบความถูกต้องเชื่อถือได้ (Integrity Check) ของข้อมูลอ้างอิงชีวมิติ เพื่อป้องกันการลักลอบเปลี่ยนแปลง หรือแก้ไขข้อมูลชีวมิติของผู้ใช้บริการโดยไม่ได้รับอนุญาต	• *ระบุแนวทางหรือกระบวนการที่สามารถใช้ตรวจสอบได้ว่าข้อมูลชีวมิติภายในระบบฐานข้อมูลมีความถูกต้องเชื่อถือได้ สามารถตรวจสอบหรือป้องกันการเปลี่ยนแปลงข้อมูลชีวมิติโดยผู้ไม่หวังดีได้*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
C7: มีการบริหารจัดการช่องโหว่ (Vulnerability Management) ของระบบ IT ครอบคลุมข้อมูลชีวมิติของผู้ใช้บริการ			
C7.1 มีการประเมินช่องโหว่ (Vulnerability Assessment) ของระบบโครงสร้างพื้นฐานด้าน IT อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยะสำคัญ	• *มีรายงานผลการทดสอบ VA ที่เกี่ยวข้องกับระบบ Biometrics ครอบคลุมระบบที่เป็น Mobile App. ของลูกค้า, End-point (เช่น Tablet และ kiosk) และระบบ Server ส่วนกลาง* • *ผู้ทดสอบ VA เป็นผู้เชี่ยวชาญที่มีใบรับรองที่เกี่ยวข้อง* • *มีกระบวนการตรวจสอบผลการทดสอบ VA โดยต้องมีการปิดช่องโหว่ที่มีความเสี่ยงสูงและปานกลางก่อนเริ่มให้บริการ โดยหากมีการขอยกเว้นการปิดช่องโหว่ในประเด็นใด ต้องมีหลักฐานการขออนุมัติยกเว้น พร้อมผลการวิเคราะห์ผลกระทบและความเสี่ยง*		
C7.2 มีการทดสอบเจาะระบบ (Penetration Test) กับระบบบริการทางการเงินที่เกี่ยวข้องกับข้อมูลชีวมิติอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยะสำคัญ	• *มีรายงานผลการทดสอบ Penetration Test ที่เกี่ยวข้องกับระบบ Biometrics ครอบคลุมระบบที่เป็น Mobile App. ของลูกค้า, End-point (เช่น Tablet และ kiosk) และระบบ Server ส่วนกลาง* • *ผู้ทดสอบ Penetration Test เป็นผู้เชี่ยวชาญอิสระที่มีใบรับรองที่เกี่ยวข้อง* • *มีกระบวนการตรวจสอบผลการทดสอบ Penetration Test จากหน่วยงานภายในที่เกี่ยวข้อง โดยต้องมีการปิดช่องโหว่ที่มีระดับความเสี่ยงสูงและปานกลางก่อนที่จะเริ่มให้บริการ โดยหากมีการขอยกเว้นการปิดช่องโหว่ในประเด็นใด ต้องมีหลักฐานการขออนุมัติยกเว้น พร้อมผลการวิเคราะห์ผลกระทบและความเสี่ยง*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	• *กรณีที่มีการใช้ระบบที่ให้บริการโดย technology vendor หรือ 3rd Party Service Provider ต้องมีการขอผลการทดสอบ Penetration Test จากผู้ให้บริการมาพิจารณาด้วย*		
C7.3 มีกระบวนการแก้ไขจุดอ่อนความปลอดภัยของระบบ (Patch management) ครอบคลุมระบบ IT ที่รองรับการประมวลผลและจัดเก็บข้อมูลชีวมิติ	• *มีนโยบาย และกระบวนการบริหารจัดการ Patch management ที่ชัดเจน* • *มีการกำหนดระยะเวลาในการติดตั้ง Patch ให้แล้วเสร็จในแต่ละระดับความเสี่ยงของช่องโหว่และระดับความสำคัญของระบบงาน*		
C7.4 ผู้ให้บริการเทคโนโลยีมีการสนับสนุนทางเทคนิคกรณีอุปกรณ์รับข้อมูลชีวมิติมีจุดอ่อนหรือตรวจพบความผิดพลาดอย่างทันท่วงที	• *ระบุกระบวนการ support จาก technology vendor กรณีอุปกรณ์หรือเทคโนโลยีที่ใช้ในการประมวลผลมีปัญหาจากการใช้งาน โดยเมื่อมีการแจ้งเตือนข้อผิดพลาดหรือช่องโหว่ที่เกี่ยวข้องกับระบบของธนาคาร vendor ต้องสามารถนำส่ง software patch เพื่อแก้ปัญหาให้ได้โดยเร็ว* • *มีการกำหนดระยะเวลา Service-Level Agreement (SLA) กับ technology vendor เพื่อให้สามารถปิดช่องโหว่ที่มีความเสี่ยงสูงได้อย่างทันท่วงที*		
C8: มีการจัดเก็บบันทึกเหตุการณ์ (Log) ที่เกี่ยวข้องกับข้อมูลชีวมิติ			
C8.1 ข้อมูล Log ครอบคลุมบันทึกการเข้าถึง (Access Log) บันทึกการดำเนินงาน (Activity Log) บันทึกร่องรอยการทำกิจกรรมธุรกรรม (Journal Log) และบันทึก	• *มีข้อกำหนดในการจัดเก็บข้อมูล Log ของระบบที่เกี่ยวข้องกับ Biometrics* • *มีผลการสอบทาน Log ว่าครอบคลุมและรัดกุมในการเป็นหลักฐานทางกฎหมายและติดตามเหตุการณ์ผิดปกติ*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
ด้านการรักษาความปลอดภัย (Security event Log)			
C8.2 การเก็บข้อมูล Log มีความปลอดภัย มีระยะเวลาการเก็บ Log เป็นไปตามกฎหมายที่เกี่ยวข้องและเพียงพอต่อการสอบทานย้อนหลัง การตรวจสอบในกรณีเกิดเหตุการณ์ผิดปกติ และการใช้เป็นหลักฐานทางกฎหมาย	• *ตัวอย่าง Log ที่จัดเก็บมีความครอบคลุมและเพียงพอต่อการสอบทานย้อนหลัง* • *มีระบบบริหารจัดการ Log เช่น Centralized Log รองรับการเก็บข้อมูลในภาพรวม* • *มีการจัดเก็บ Biometrics ใน Log โดยเข้ารหัส* • *ไม่มีการจัดเก็บข้อมูล Biometrics (รูปภาพใบหน้า) ใน Log โดยไม่ได้เข้ารหัส*		

สรุปผลการประเมินด้านการรักษาความมั่นคงปลอดภัยของข้อมูลชีวมิติ (Confidentiality)

หัวข้อที่ 3 - ด้านความน่าเชื่อถือของเทคโนโลยีชีวมิติ (Integrity)

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
I1. กระบวนการได้มาซึ่งข้อมูลชีวมิติมีคุณภาพและครบถ้วนเพียงพอต่อการประมวลผล			
I1.1 มีแนวทางสำหรับผู้ปฏิบัติงานเพื่อรวบรวมข้อมูล และการให้คำแนะนำแก่ผู้ใช้บริการกรณีที่	• *ระบุกระบวนการของเจ้าหน้าที่ผู้ปฏิบัติงานที่สาขาสำหรับขั้นตอนการเปิดบัญชีด้วยภาพใบหน้าหรือคำแนะนำสำหรับผู้ใช้บริการในการเปิดบัญชีผ่านสมาร์ตโฟนหรือเครื่อง Kiosk*		ระบุผล - ผ่าน - ไม่ผ่าน - ควรปรับปรุง

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
ผู้ใช้บริการดำเนินการให้ข้อมูลชีวมิติด้วยตนเอง			
I1.2 มีขั้นตอนรองรับกรณีที่ผู้ใช้บริการหรือลูกค้ามีข้อจำกัดในการใช้ข้อมูลชีวมิติ เช่น การ override	• *อธิบายแยกตามวิธีในการเก็บรวบรวมภาพถ่ายจากลูกค้า เช่น ถ่ายภาพผ่านโทรศัพท์มือถือของลูกค้าเอง ถ่ายภาพโดยพนักงานสาขา ถ่ายภาพผ่านอุปกรณ์ Kiosk* • *มีการกำหนด range/threshold ของระดับความเชื่อมั่น (มั่นใจ=เขียว/ปานกลาง=เหลือง/ไม่มั่นใจ=แดง) อย่างไร ที่ค่าเท่าใด* • *กระบวนการ override/ fallback (ทางเลือกที่ไม่ใช้ biometrics) ต้องมีความรัดกุมน่าเชื่อถือไม่น้อยกว่าการใช้ Biometric*		
I1.3 มีกลไกการตรวจสอบความแท้จริงและเป็นปัจจุบันของแหล่งข้อมูลที่เชื่อถือได้ (Trusted source) เช่น บัตรประชาชน หนังสือเดินทาง	• *ระบุแหล่งข้อมูลที่เชื่อถือได้สำหรับการพิสูจน์ตัวตน เช่น บัตรประชาชน หรือพาสปอร์ต และวิธีการที่ใช้ในการตรวจสอบว่าบัตรประชาชนสามารถใช้งานได้และยังไม่หมดอายุ เป็นต้น*		
I2: กระบวนการพัฒนาแบบจำลองมีความแม่นยำ ผ่านการทดสอบกลุ่มตัวอย่างที่มีความหลากหลายและมีปริมาณเพียงพอ			
I2.1 มีการทดสอบกับกลุ่มทดลองด้วยจำนวนที่เพียงพอก่อนเริ่มให้บริการในวงกว้าง	• *ระบุจำนวนกลุ่มทดสอบ โดยควรมีจำนวน Sample size ที่ถูกนำมาใช้ในการทดสอบความแม่นยำแบบ NxN (อย่างน้อย 1,000 ราย สำหรับการใช้ Vendor ใน NIST Top 100 หรือเคยผ่านการทดสอบใน Regulatory Sandbox หรือ อย่างน้อย 2,000 รายสำหรับกรณีอื่น) โดย* • *กลุ่มทดลองหรือกลุ่มทดสอบอาจใช้พนักงานภายในองค์กรหรือจัดหาโดย Vendor*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
I2.2 สำหรับการใช้ Facial recognition มีการทดสอบความแม่นยำในการจำแนกแฝด หรือบุคคลที่มีการเปลี่ยนแปลงใบหน้าอย่างมีนัยสำคัญ เช่น ผ่านการทำศัลยกรรม เป็นต้น	• *มีมาตรการป้องกันการสวมรอย เช่น กรณีมีฝาแฝดหรือหน้าคล้าย ได้ เช่น มีให้ลูกค้ารับรองข้อมูลที่ให้แก่ผู้ให้บริการว่า ถูกต้องครบถ้วน และเป็นความจริง* • *มีวิธีการปรับปรุงภาพถ่ายของลูกค้าให้ถูกต้องเป็นปัจจุบัน เช่น มีรอบการอัพเดทข้อมูลลูกค้าที่ชัดเจน*		
I2.3 มีแนวทางการทบทวนการใช้งาน Biometrics อย่างสม่ำเสมอ ครอบคลุมเรื่องประสิทธิภาพ (ความแม่นยำ, ความเร็ว) ผลการใช้งาน (คุณภาพ, การปฏิบัติงานของเจ้าหน้าที่) และภัยคุกคาม (เหตุการณ์ผิดปกติ, ช่องโหว่, ความล้าสมัย)	• *ประสิทธิภาพ: ความแม่นยำ / ความเร็ว - มีแนวทางในการทบทวนค่าความแม่นยำของระบบ Facial Recognition และความเร็วในการให้บริการของระบบ* • *ผลการใช้งาน: คุณภาพ / การปฏิบัติงานของเจ้าหน้าที่ - มีกระบวนการทบทวนการควบคุมคุณภาพของข้อมูล Biometrics และกระบวนการที่เกี่ยวข้อง เช่น การนำภาพที่ถูก Reject มาทบทวนดูว่าสาเหตุเกิดจากปัญหาด้านคุณภาพหรือไม่ เป็นต้น หรือมีการ Accept ภาพถ่ายที่ไม่ได้คุณภาพเข้าสู่ระบบมากน้อยเพียงใด* • *ภัยคุกคาม: เหตุการณ์ผิดปกติ / ช่องโหว่ / ความล้าสมัย - มีแนวทางในการ Response ต่อความเสี่ยงด้านเทคโนโลยี Biometrics โดยเฉพาะ เช่น การโจมตีด้วยใบหน้าปลอมรูปแบบใหม่ เป็นต้น*		
I3: แบบจำลองผ่านการประเมินความแม่นยำตามมาตรฐานสากล			
I3.1 Facial recognition technology ที่เลือกใช้มีความแม่นยำ โดย (1) Accuracy Rate (%) ไม่ต่ำกว่า 99% (2) False Acceptance Rate (FAR) (%) ไม่เกิน 0.1%	• *ระบุรายละเอียดแจกแจงวิธีการคำนวณ และการแทนค่าต่าง ๆ ในสูตร* 1. Accuracy rate = $\frac{(\text{True Accept}+\text{True Reject})}{(\text{True Accept}+\text{True Reject}+\text{False Accept}+\text{False Reject})} \times 100$ 2. False acceptance rate = $\frac{\text{False Accept}}{\text{False Accept}+\text{True Reject}} \times 100$ 3. False rejection rate = $\frac{\text{False Reject}}{\text{False Reject}+\text{True Accept}} \times 100$		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
(3) False Rejection Rate (FRR) (%) ไม่เกิน 3%	*ทั้งนี้ กรณีผู้ให้บริการทางการเงินเป็นผู้พัฒนาระบบ Facial Recognition เอง ควรมีการประเมินความแม่นยำโดยผู้เชี่ยวชาญภายนอกที่มีความน่าเชื่อถือ*		
I4: มีกระบวนการป้องกันการปลอมแปลงชีวมิติ (Presentation Attack Detection) ที่มีประสิทธิภาพ			
I4.1 มีการทดสอบ Presentation Attack Detection ก่อนเริ่มให้บริการกับผู้ใช้บริการ	• *มีจำนวน Test case มากกว่า 100 ตัวอย่าง (จำนวน Test Case = Test Scenario x Test Crew) (เช่น กรณีที่ผู้ให้บริการออกแบบการทดสอบให้มี 2 Test Scenario คือ ภาพใบหน้าปริ้นสี กับภาพวิดีโอ และจำนวนผู้เข้าร่วมการทดสอบ (Test Crew) 50 คน จะทำให้มีภาพใบหน้า กับภาพวิดีโอ อย่างละ 50 คน สรุปมีจำนวน Test Case ทั้งหมดรวมเป็น 100 Test Case) และต้องสามารถป้องกันการปลอมแปลงได้ในทุก Test Case ที่ทำการทดสอบ*		
I4.2 ผลการทดสอบ Presentation Attack Detection สามารถตรวจจับการปลอมแปลงชีวมิติที่มีระดับความซับซ้อนต่ำและปานกลางได้ โดยควรอ้างอิงกับมาตรฐานที่เชื่อถือได้ เช่น FIDO หรือ ETDA	• *Test Scenario ที่ครอบคลุมการใช้ข้อมูล Biometrics มาหลอกระบบ ครอบคลุมความเสี่ยงระดับต่ำและระดับปานกลางเป็นอย่างน้อย โดย* ○ *<u>ระดับต่ำ</u> หมายถึง ใช้อุปกรณ์ที่หาได้ทั่วไป ใช้เวลาเตรียมการน้อย ต้องการทักษะการปลอมแปลงต่ำ และอาศัยข้อมูลอัตลักษณ์ของบุคคลที่เข้าถึงได้ง่าย ในการปลอมแปลง (ตัวอย่างเช่น การใช้ภาพใบหน้าที่เป็นภาพนิ่งแทนใบหน้าของบุคคลจริง เช่น ภาพใบหน้าที่หาได้จาก Social media ต่าง ๆ ภาพใบหน้าจากการตัดต่อด้วยโปรแกรมตัดต่อภาพ)* ○ *<u>ระดับปานกลาง</u> หมายถึง ใช้อุปกรณ์เฉพาะทางหรืออุปกรณ์ที่หาได้ทั่วไป ใช้เวลาในการเตรียมการปานกลาง ต้องการทักษะการปลอมแปลงระดับหนึ่ง และอาศัยข้อมูลอัตลักษณ์ของบุคคลที่เข้าถึงได้ไม่ยากมากนัก ในการปลอมแปลง (ตัวอย่าง เช่น*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
	ใช้ภาพวิดีโอหรือภาพเคลื่อนไหวของบุคคลที่มีคุณภาพสูง เพื่อลอกเลียนการทำท่าทางตามกระบวนการ Liveness detection)		

สรุปผลการประเมินด้านความน่าเชื่อถือของเทคโนโลยีชีวมิติ (Integrity)

หัวข้อที่ 4 - ด้านความพร้อมใช้ของเทคโนโลยีชีวมิติ (Availability)

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
A1: มีแนวทางรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) รองรับบริการทางการเงินที่ใช้เทคโนโลยีชีวมิติ			
A1.1 มีแผน BCP และ DRP รองรับเหตุการณ์บริการทางการเงินที่เกี่ยวข้องกับเทคโนโลยีชีวมิติขัดข้องและครอบคลุม Scenario สำคัญ	• *มีกระบวนการรองรับกรณีเกิดเหตุฉุกเฉิน ทั้งกรณีที่สามารถย้ายไปใช้ระบบสำรองได้ และกรณีที่ไม่สามารถใช้ระบบสำรองได้* • *กระบวนการควรครอบคลุมถึงผู้ให้บริการที่สาขาระบบหลังบ้านต่าง ๆ และอื่นๆที่เกี่ยวข้อง*		ระบุผล - ผ่าน - ไม่ผ่าน - ควรปรับปรุง
A1.2 มีการทดสอบแผน BCP และ DRP ที่เกี่ยวข้องกับเทคโนโลยีชีวมิติอย่างสม่ำเสมอ	• *ระบุแผนการทดสอบที่ผ่านมา ทั้งในแง่ความถี่และขอบเขตการทดสอบ*		
A1.3 แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องครอบคลุมถึงกรณีการใช้บริการจากผู้ให้บริการภายนอกเกิดเหตุขัดข้อง	• *ระบุรายชื่อผู้ให้บริการภายนอกและขอบเขตการทดสอบแผน BCP*		

หัวข้อ	รายละเอียดของการดำเนินการ	การปฏิบัติงานในปัจจุบัน	ผลการประเมิน
A2: ระบบ IT มี Disaster recovery plan (DRP) รองรับบริการทางการเงินที่ใช้เทคโนโลยีชีวมิติ ตามระดับความสำคัญของลักษณะธุรกิจ			
A2.1 มีระบบ IT รองรับบริการทางการเงินที่เกี่ยวข้องกับข้อมูลชีวมิติของลูกค้า ตามระดับความสำคัญของระบบงาน	• *มีการสำรองข้อมูลชีวมิติรองรับการให้บริการ* • *มีรอบการสำรองข้อมูล และความถี่ และระยะเวลาในการจัดเก็บที่ชัดเจน* • *สามารถระบุสถานที่จัดเก็บข้อมูลชีวมิติสำรองได้ชัดเจน* • *มีแนวทางการทดสอบความพร้อมใช้ของข้อมูลที่เก็บสำรองไว้*		
A2.2 แผน DRP รองรับกรณีระบบของผู้ให้บริการ Cloud Computing ขัดข้อง (สำหรับกรณีที่มีการใช้บริการ Cloud Computing)	• *ระบุรายชื่อผู้ให้บริการ Cloud Service และขอบเขตการทดสอบแผน BCP* • *มีแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของระบบที่ใช้บริการ Cloud Computing*		
A3: มีการทดสอบประสิทธิภาพระบบ IT			
A3.1 มีการทดสอบหรือแผนที่จะดำเนินการทดสอบระบบการให้บริการก่อนเริ่มให้บริการ	• *มีการทดสอบระบบก่อนให้บริการ ได้แก่ Unit Test, system and Integration Test , User Acceptance Test, Performance test*		

สรุปผลการประเมินด้านความพร้อมใช้ของเทคโนโลยีชีวมิติ (Availability)