กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA

การประชุมรับฟังความคิดเห็นต่อ

แนวทางในการพัฒนาร่างหลักเกณฑ์การตรวจประเมินประจำปี สำหรับผู้ประกอบธุรกิจบริการ Digital ID

วันศุกร์ที่ 11 ตุลาคม 2567
เวลา 09.00-12.00 น.

AGENDA

เวลา	กำหนดการ
09.00 – 09.30 น.	ลงทะเบียน
09.30 – 09.35 น.	เปิดการประชุม
09.35 – 11.00 น.	**นำเสนอแนวทางในการพัฒนาร่างหลักเกณฑ์การตรวจประเมินประจำปีสำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล** • ผลการศึกษาแนวทางการกำกับดูแลสำหรับการตรวจประเมินประจำปี • แนวทางในการพัฒนาร่างหลักเกณฑ์การตรวจประเมินประจำปีสำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
11.00 – 12.00 น.	ถาม-ตอบ

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

วัตถุประสงค์

- **เพื่อนำเสนอแนวทางการจัดทำร่างหลักเกณฑ์การตรวจประเมินประจำปีสำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล**
- **เพื่อรวบรวมความเห็น และข้อเสนอแนะจากผู้เข้าร่วมการประชุมนำมาประกอบการพัฒนา หลักเกณฑ์การตรวจประเมินประจำปีสำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล**

<u>เนื้อหาที่นำเสนออ้างอิงจากเอกสาร</u>

- แนวทางในการพัฒนาร่างหลักเกณฑ์การตรวจประเมินประจำปีสำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- แบบประเมินประจำปีเพื่อระบุระดับความเสี่ยงของผู้ประกอบธุรกิจ

หัวข้อการประชุม

แนวทางการพัฒนาร่างหลักเกณฑ์การตรวจประเมินประจำปี
สำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการ
เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ETDA

ขั้นตอนการพัฒนาร่างหลักเกณฑ์

ภาพแสดงขั้นตอนการพัฒนา (ร่าง) หลักเกณฑ์การตรวจประเมินประจำปี

สรุปประเด็นจากการศึกษา Framework ในต่างประเทศ

Digital ID Trust Frameworks	ขอบเขตการตรวจประเมิน	หัวข้อการประเมินประจำปี						วิธีการตรวจประเมิน	ความถี่ในการตรวจประเมิน
		Risk	ITSec	Privacy	Fraud	DID Controls	User Protection		
Trusted Digital Identity Framework (TDIF)	ครอบคลุมทุกส่วนของการให้บริการ Digital ID	X	X	X	X	X	X	ต้องตรวจประเมิน Functional Assessment โดยผู้ตรวจสอบอิสระจากภายนอก ปีเว้นปี	ตรวจปีเว้นปี เช่น ได้ตรวจประเมินในปี พ.ศ. 2566 แล้ว ปีต่อไปที่จะตรวจประเมิน คือ ปี พ.ศ. 2568
AADHAAR by UIDAI	ครอบคลุมการจัดการและใช้งานข้อมูล Aadhaar	X	X	X	X	X		ตรวจประเมินโดยผู้ตรวจประเมินที่ได้รับการรับรอง certified by a recognized body	ตรวจทุกปี
[EU] eIDAS Regulation	ครอบคลุมผู้ให้บริการ eID และTrust Services	X	X	X				ตรวจประเมินโดยผู้ตรวจสอบอิสระจาก Conformity Assessment Body (CAB)	ทุก 2 ปีสำหรับการตรวจประเมินเต็มรูปแบบ และตรวจติดตามทุกปี
[CANADA] PCTF DIACC	ครอบคลุมผู้ให้บริการ Digital ID ในบทบาทต่าง ๆ Authentication Service, Credential Service.	X	X	X		X		การตรวจโดยผู้ตรวจสอบอิสระ ที่ได้รับการรับรองจาก DIACC	ตรวจทุกปี ในรูปแบบวัฏจักร 3 ปี คือ Full Audit ในปีที่ 1,4,7... และ Surveillance Audit ในปีอื่นๆ

สรุปประเด็นที่เกี่ยวข้องจากรวบรวมข้อมูลจากผู้ประกอบธุรกิจ

หัวข้อ: การตรวจสอบจากหน่วยงานกำกับ ฯ มีความซ้ำซ้อนกัน โดยเฉพาะในด้าน IT Security

ข้อเสนอแนะ: นำข้อมูลที่เคยถูกตรวจประเมินก่อนโดยหน่วยงานกำกับ ฯ อื่นในรอบปีการตรวจประเมินเดียวกัน มาใช้กับตอบคำถามในการตรวจประเมินของหน่วยงานกำกับ ฯ อีกหน่วยงาน ที่มีกำหนดการตรวจประเมินหลัง ในกรณีที่หลักเกณฑ์ที่ใช้ตรวจประเมินเหมือนกัน

ประโยชน์:

1. ลดภาระงานให้กับ Service Provider
2. ลดค่าใช้จ่ายในการตรวจประเมิน เนื่องจากบางองค์กรไม่มีหน่วยงานที่ทำหน้าที่ตรวจประเมินภายใน จึงต้องว่าจ้างผู้ตรวจประเมินจากภายนอก

หัวข้อ: วิธีการตรวจ/ประเมินไม่ชัดเจน

ข้อเสนอแนะ: ควรกำหนดวิธีการตรวจ/ประเมินให้ชัดเจน เช่น จัดทำคู่มือการตรวจ/ประเมิน จัดทำคำอธิบายหลักเกณฑ์ที่ใช้ประเมินเพื่อความเข้าใจที่ตรงกัน อบรมผู้ที่จะทำหน้าที่ประเมิน

ประโยชน์:

1. ผู้ปฏิบัติงานเข้าใจวัตถุประสงค์ของหลักเกณฑ์ในแต่ละข้อ ทำให้สามารถเตรียมเอกสารและหลักฐานได้ครบถ้วน
2. ผู้ตรวจประเมินเข้าใจประเด็นและวัตถุประสงค์ของหลักเกณฑ์ในแต่ละข้อ ทำให้ถามคำถามได้อย่างตรงจุดตรงประเด็น
3. ผู้ปฏิบัติงานและผู้ตรวจประเมินมีความเข้าใจตรงกัน ลดปัญหาในการสื่อสาร

สรุปประเด็นที่เกี่ยวข้องจากรวบรวมข้อมูลจากผู้ประกอบธุรกิจ

หัวข้อ: Template รายงานผลการตรวจประเมินไม่ได้กำหนดไว้อย่างชัดเจน

ข้อเสนอแนะ: ควรจัดทำ template รายงานผลการตรวจประเมิน และอธิบายว่าแต่ละหัวข้อต้องมีการกำหนดเนื้อหาใดบ้าง

ประโยชน์:

1. ผู้ตรวจประเมินสามารถใส่ข้อมูลได้อย่างถูกต้อง ครบถ้วน ตรงตามที่หน่วยงานกำกับ ฯ ต้องการ

หัวข้อ: จำนวนข้อที่ใช้ตรวจประเมินมีจำนวนมาก ประกอบกับความซ้ำซ้อนของประเด็นในการตรวจประเมิน

ข้อเสนอแนะ: พิจารณาขอบเขตและรอบของการตรวจประเมินโดยใช้แนวทางการประเมินความเสี่ยง

ประโยชน์:

1. ประหยัดเวลา ทรัพยากร และค่าใช้จ่ายให้กับ Service Provider การตรวจประเมินเหมาะสมกับ Service Provider แต่ละประเภทความเสี่ยง

สรุปประเด็นที่เกี่ยวข้องจากรวบรวมข้อมูลจากหน่วยงานกำกับฯ

1. ควรพัฒนามาตรฐาน หลักเกณฑ์ และรอบการตรวจประเมินให้สอดคล้องกัน ระหว่างหน่วยงานกำกับ ฯ เพื่อลดภาระให้กับผู้ประกอบธุรกิจ รวมทั้งแนวทางในการกรอกข้อมูลร่วมกัน

2. ควรพัฒนาแนวทางการระบุความเสี่ยงของผู้ประกอบธุรกิจ เพื่อใช้เป็นข้อมูลสำหรับการควบคุมดูแล สนับสนุน ส่ง ส่งเสริม ให้สอดคล้องกับความเสี่ยงของผู้ประกอบธุรกิจแต่ละราย

3. ควรพิจารณาแนวทางการพัฒนาความรู้ความเข้าใจในหลักเกณฑ์ที่ตรวจประเมิน รวมถึงด้านเทคโนโลยีสารสนเทศ และด้านธุรกิจที่เกี่ยวข้องกับบริการ Digital ID ให้กับบุคคลที่จะเป็นผู้ตรวจประเมิน รวมถึงบุคคลที่เกี่ยวข้อง

4. ควรพิจารณาจัดสรรบุคลากรในหน่วยงานกำกับ ฯ ที่มีความรู้ความเข้าใจเกี่ยวกับหลักเกณฑ์ ด้านเทคโนโลยีสารสนเทศ และด้านธุรกิจที่เกี่ยวข้องกับบริการ Digital ID ให้เพียงพอกับการกำกับดูแล รวมถึงการตรวจประเมินผู้ประกอบธุรกิจโดยสำนักงานเองในกรณีที่จำเป็น การตรวจสอบผลการตรวจหรือการประเมินของผู้ประกอบธุรกิจ และการให้คำแนะนำสำหรับการพัฒนาปรับปรุงการปฏิบัติงานให้สอดคล้องกับหลักเกณฑ์ของหน่วยงานกำกับ ฯ

หัวข้อการประชุม

สาระสำคัญของ (ร่าง) หลักเกณฑ์การตรวจประเมินประจำปี
สำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการ
เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ETDA

หลักเกณฑ์การตรวจประเมินประจำปี ฯ

ส่วนที่ 1 การตรวจประเมินประจำปี

ข้อ 1 ผู้รับใบอนุญาตต้องจัดให้มีการ**ตรวจประเมินระบบการให้บริการอย่างน้อยปีละหนึ่งครั้ง** ให้ครอบคลุมหัวข้ออย่างน้อยดังนี้

1.1 การปฏิบัติตาม**หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ** หมวด 1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ หมวด 2 การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และ หมวด ๓ การบริหารและการจัดการความเสี่ยงของระบบการให้บริการ

1.2 การปฏิบัติตาม**หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ**

1.3 การปฏิบัติตาม**หลักเกณฑ์การตามลักษณะของการให้บริการหลักเกณฑ์ตามลักษณะของการให้บริการ**

1.4 หัวข้ออื่น ๆ ตามได้รับแจ้งจากสำนักงาน

หลักเกณฑ์การตรวจประเมินประจำปี ฯ

ส่วนที่ 1 การตรวจประเมินประจำปี

ข้อ 2 **ขอบเขตในการตรวจประเมิน**ต้องครอบคลุมระบบการให้บริการสำหรับบริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน บริการยืนยันตัวตน และบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งประกอบด้วยการปฏิบัติงาน กระบวนการทำงาน และระบบงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

ข้อ 3 ผู้รับใบอนุญาตต้องดำเนินการ**ประเมินความเสี่ยงให้**สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงานตามรูปแบบที่สำนักงานกำหนด พร้อมจัด**ส่งผลการประเมินต่อสำนักงานภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน** โดยผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินก่อนนำส่งต่อสำนักงาน

ข้อ 4 การตรวจประเมินตามข้อ 1.4 ต้องกำหนดแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง ให้**ครอบคลุมส่วนที่มีการเปลี่ยนแปลง**ของระบบการให้บริการ

หลักเกณฑ์การตรวจประเมินประจำปี ฯ

ส่วนที่ 1 การตรวจประเมินประจำปี

ข้อ 5 การตรวจประเมินตามข้อ 1.1 1.2 และ 1.3 ต้องกำหนดแผนงานและดำเนินการ**ตรวจประเมินให้สอดคล้องกับระดับความเสี่ยงการประกอบธุรกิจ**ของผู้รับใบอนุญาต โดยมีรายละเอียดดังนี้

5.1 กรณีเป็นผู้ประกอบธุรกิจที่มี**ความเสี่ยงระดับต่ำ** ต้องกำหนดแผนงานและดำเนินการ**ตรวจประเมินการ**ปฏิบัติตามข้อกำหนดให้ครอบคลุม**ข้อกำหนดทั้งหมดภายใต้หลักเกณฑ์ (full scope) แบบปีเว้นปี**

5.1.1 ปีที่เป็นการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) ต้องจัดทำแผนงานและดำเนินการตรวจประเมินให้ครบทุกข้อกำหนดภายใต้หลักเกณฑ์

5.1.2 ปีที่ไม่ได้มีการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) สามารถจัดทำแผนงานและดำเนินการตรวจประเมินข้อกำหนดบางส่วน โดยพิจารณาตามความเสี่ยงและความเหมาะสม

5.2 กรณีเป็นผู้ประกอบธุรกิจที่มี**ความเสี่ยงระดับปานกลางหรือสูง** ต้องจัดทำแผนงานและดำเนินการ**ตรวจประเมิน**การปฏิบัติตามข้อกำหนด**ให้ครบทุกข้อกำหนดภายใต้หลักเกณฑ์ (full scope) ทุกปี**

หลักเกณฑ์การตรวจประเมินประจำปี ฯ

ส่วนที่ 1 การตรวจประเมินประจำปี

ข้อ 6 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการและรายงานผลการตรวจประเมินระบบการให้บริการให้สอดคล้องกับหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ

ข้อ 7 ผู้รับใบอนุญาตต้อง**รายงานผลการตรวจประเมินประจำปี**ตามรูปแบบที่สำนักงานกำหนด **ภายใน 30 วัน**นับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ **แต่ไม่เกินวันที่ 31 มกราคมของปีถัดไป**

ข้อ 8 การรายงานผลการตรวจประเมินประจำปีต่อสำนักงาน ผู้รับใบอนุญาต**สามารถรวบรวมผลจากหลายรอบการตรวจประเมินที่ดำเนินการภายในปีปฏิทินเดียวกัน** โดยต้องจัดทำรายงานผลการตรวจประเมินประจำปีให้มีรายละเอียดครบถ้วนตามหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ และ**ต้องจัดทำตารางเพื่อแสดงข้อกำหนดภายใต้หลักเกณฑ์และขอบเขตที่ตรวจประเมินในแต่ละรอบการตรวจ** เพื่อให้มั่นว่าการตรวจประเมินในแต่ละปีครอบคลุมหลักเกณฑ์และระบบการให้บริการที่เกี่ยวข้อง

ข้อ 9 ผู้รับใบอนุญาตต้อง**จัดเก็บรายงานผลการตรวจประเมิน**ไว้เป็นระยะเวลา**ไม่น้อยกว่า 2 ปี**นับแต่วันที่จัดทำรายงาน เพื่อให้พร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดยสำนักงาน

หลักเกณฑ์การตรวจประเมินประจำปี ฯ

ส่วนที่ 2 การพิจารณาความมีนัยสำคัญ

ข้อ 10 ผู้รับใบอนุญาตต้อง**จัดให้มีข้อกำหนดในการพิจารณาความมีนัยสำคัญ**หรือความสำคัญที่ชัดเจนเพื่อใช้พิจารณาดำเนินการในเรื่องต่าง ๆ โดยดำเนินการดังนี้

10.1 ข้อกำหนดดังกล่าวต้อง**ผ่านการพิจารณร่วมกันของหน่วยงานที่เกี่ยวข้อง รวมทั้งต้องได้รับอนุมัติ**จากผู้บริหาร คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย

10.2 ข้อกำหนดในการพิจารณาความมีนัยสำคัญต้องพิจารณาภายใต้กรอบหลักการที่**คำนึงถึงความเสี่ยงและผลกระทบต่อการให้บริการของผู้รับใบอนุญาตในวงกว้าง** เช่น กระทบลูกค้าหรือผู้ใช้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้รับใบอนุญาต และ**คำนึงถึงผลกระทบต่อระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในวงกว้าง** เช่น กระทบต่อระบบงานกลางที่มีนัยสำคัญเชิงโครงสร้างต่อการให้บริการของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

10.3 ต้อง**ทบทวนข้อกำหนดอย่างน้อยปีละ 1 ครั้ง** และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบต่อการให้บริการ

ข้อ 11 ผู้รับใบอนุญาตต้อง**สื่อสารข้อกำหนด**ดังกล่าวให้แก่บุคลากรและบุคคลภายนอกที่เกี่ยวข้องทราบและนำไปปฏิบัติ

หลักเกณฑ์การตรวจประเมินประจำปี ฯ

ส่วนที่ 3 การแจ้งการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการ

ข้อ 12 การแจ้งนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการ

12.1 ผู้รับใบอนุญาตที่นำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยี โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนดที่ผู้รับใบอนุญาตได้กำหนดขึ้นตามข้อ 10 ทั้งกรณีที่ผู้รับใบอนุญาตดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้อง **แจ้งการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวต่อสำนักงานล่วงหน้าไม่น้อยกว่า 30 วันก่อนดำเนินการ** ตามรูปแบบและวิธีที่สำนักงานกำหนด เว้นแต่สำนักงานมีคำสั่งให้ผู้รับใบอนุญาตไม่ต้องแจ้งการนำเทคโนโลยีมาใช้หรือเปลี่ยนแปลงระบบ หรือเทคโนโลยีที่มีนัยสำคัญ

หัวข้อการประชุม

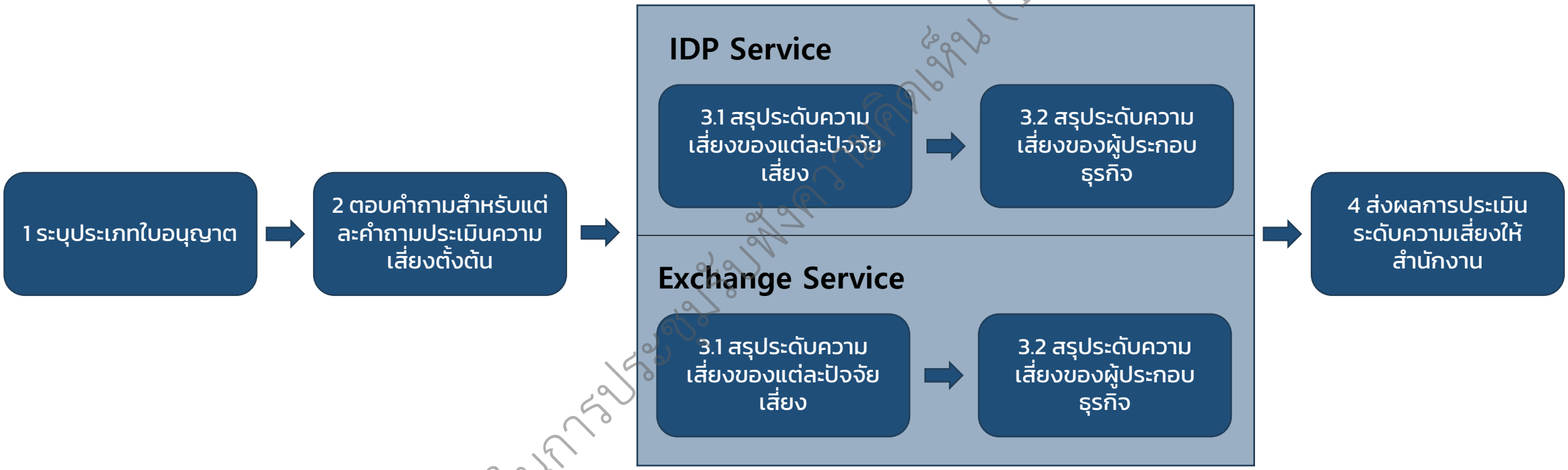
แนวทางการประเมินเพื่อระบุระดับความเสี่ยงของผู้ประกอบธุรกิจ และแบบประเมิน

อ้างถึง หลักเกณฑ์การตรวจประเมินประจำปี ฯ

ส่วนที่ 1 การตรวจประเมินประจำปี

ข้อ 3 ผู้รับใบอนุญาตต้องดำเนินการ**ประเมินความเสี่ยงให้**สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงานตามรูปแบบที่สำนักงานกำหนด พร้อมจัด**ส่งผลการประเมินต่อสำนักงานภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน** โดยผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินก่อนนำส่งต่อสำนักงาน

ขั้นตอนการประเมินความเสี่ยง



ปัจจัยเสี่ยง

- เทคโนโลยีและช่องทางการให้บริการ
- ลักษณะผลิตภัณฑ์และการให้บริการ
- ประวัติเหตุการณ์ไม่พึงประสงค์

ปัจจัยเสี่ยงและหัวข้อคำถามประเมินความเสี่ยง

เทคโนโลยีและช่องทางการให้บริการ	
32.การใช้งานแผนสำรองฉุกเฉิน (BCP และ DRP) ที่เกี่ยวข้องกับการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด	General
33.ช่องโหว่ภายในระบบหรือแอปพลิเคชันสำหรับบริการ Digital ID ที่มีความเสี่ยงของช่องโหว่ระดับ High หรือ Critical	General
59.จำนวนการใช้บริการจากผู้รับดำเนินการแทนในการให้บริการ	General
63.จำนวนผู้อาศัยการยืนยันตัวตน (RP) ที่มีการเชื่อมต่อเพื่อให้บริการพิสูจน์ตัวตน [IDP1]	IDP1 only
64.จำนวนจุดให้บริการการพิสูจน์ตัวตนรวมทั้งหมดที่อยู่ในความดูแลของหน่วยงาน [IDP1]	IDP1 only
71.จำนวนผู้อาศัยการยืนยันตัวตน (RP) และผู้พิสูจน์และยืนยันตัวตน (IdP) ที่มีการเชื่อมต่อเพื่อให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล [Ex.]	Exchange only

ลักษณะผลิตภัณฑ์และการให้บริการ	
62.ระดับความน่าเชื่อถือของการพิสูจน์ตันตน (IAL) สูงสุดที่องค์กรสามารถให้บริการ [IDP1]	IDP1 only
65.จำนวน transaction ต่อปี สำหรับบริการพิสูจน์ตัวตน [IDP1]	IDP1 only
67.ระดับความน่าเชื่อถือของการยืนยันตันตน (AAL) สูงสุดที่องค์กรสามารถให้บริการ [IDP2/3]	IDP2/3 only
69.จำนวน transaction ต่อปี สำหรับบริการยืนยันตัวตน [IDP2/3]	IDP2/3 only
70.จำนวนผู้ใช้บริการ (subscriber) ที่ลงทะเบียนและพร้อมใช้งานบริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือบริการยืนยันตัวตน [IDP2/3]	IDP2/3 only
72.จำนวน transaction ต่อปี สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด [Ex.]	Exchange only

ปัจจัยเสี่ยงและหัวข้อคำถามประเมินความเสี่ยง

ประวัติเหตุการณ์ไม่พึงประสงค์	
15.จำนวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล	General
18.จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID	General
19.ระยะเวลารวมของการหยุดให้บริการชั่วคราวของระบบการให้บริการ Digital ID ที่มีผลกระทบต่อลูกค้าหรือผู้ใช้บริการและไม่ได้เป็นการเตรียมการไว้ล่วงหน้า	General
20.จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ (incident) ที่มีผลกระทบในระดับกลางขึ้นไป	General

2. การตอบแบบสอบถามเพื่อประเมินระดับความเสี่ยง

แบบประเมินประจำปีเพื่อระบุระดับความเสี่ยงของผู้ประกอบธุรกิจ

Part 1: สำหรับทุกลักษณะการให้บริการ

No.	คำถามสำหรับการประเมิน	ผลการประเมิน (ต่ำ/ปานกลาง/สูง)	ข้อมูลหรือคำชี้แจงประกอบผลการประเมิน	ระดับความเสี่ยง			หมายเหตุ
				ต่ำ	ปานกลาง	สูง	
15	จำนวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล* ครอบคลุมการรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ อ้างอิง ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565			ไม่มี	1-2 เหตุการณ์	มากกว่า 2 เหตุการณ์	
18	จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด เช่น การถูกปลอมแปลงตัวตน			ไม่มี	1-2 เหตุการณ์	มากกว่า 2 เหตุการณ์	
19	ระยะเวลารวมของการหยุดให้บริการชั่วคราวของระบบการให้บริการ Digital ID ที่ไม่ได้เป็นการเตรียมการไว้ล่วงหน้า และมีผลกระทบต่อลูกค้าหรือผู้ใช้บริการ ในรอบปีปฏิทินล่าสุด			น้อยกว่า 8 ชั่วโมง	8-16 ชั่วโมง	มากกว่า 16 ชั่วโมง	
20	จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ (incident) ที่มีผลกระทบในระดับกลางขึ้นไป* เช่น ภัยคุกคามทางไซเบอร์, ข้อมูลรั่วไหล, ระบบหรือบริการหยุดชะงักเป็นเวลานาน (มากกว่า 8 ชั่วโมง), ความผิดปกติอย่างร้ายแรงของระบบที่เกี่ยวกับการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด หมายเหตุ ผลกระทบในระดับกลางขึ้นไปหมายถึงมูลค่าความเสียหาย มากกว่า 1 ล้านบาท/ผู้เสียหายมากกว่า 10,000 คน/กระทบต่อชีวิต ร่างกายหรืออนามัยของคน/กระทบต่อความมั่นคงของรัฐ (อ้างอิงประกาศ คธอ. เรื่อง ประเภทธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีแบบปลอดภัย พ.ศ. 2555)			ไม่มี	1-2 เหตุการณ์	มากกว่า 2 เหตุการณ์	

2. การตอบแบบสอบถามเพื่อประเมินระดับความเสี่ยง

No.	คำถามสำหรับการประเมิน	ผลการประเมิน (ต่ำ/ปานกลาง/สูง)	ข้อมูลหรือคำชี้แจงประกอบผลการประเมิน	ระดับความเสี่ยง			หมายเหตุ
				ต่ำ	ปานกลาง	สูง	
32	การใช้งานแผนสำรองฉุกเฉิน (BCP และ DRP) ที่เกี่ยวข้องกับการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด			น้อยกว่า 2 ครั้ง	2-3 ครั้ง	มากกว่า 3 ครั้ง	
33	ช่องโหว่ภายในระบบหรือแอปพลิเคชันสำหรับบริการ Digital ID ที่มีความเสี่ยงของช่องโหว่ระดับ High หรือ Critical			ไม่มีช่องโหว่ที่มีความเสี่ยงระดับ High หรือ Critical ที่ยังไม่ได้รับการแก้ไข	มี 1-3 ช่องโหว่ที่มีความเสี่ยงระดับ High หรือ Critical ที่ยังไม่ได้รับการแก้ไข	มีมากกว่า 3 ช่องโหว่ที่มีความเสี่ยงระดับ High หรือ Critical ที่ยังไม่ได้รับการแก้ไข	นับจำนวน ตามจำนวนช่องโหว่ที่พบทั้งหมดรวมกัน จากผลการทดสอบระบบในระดับแอปพลิเคชัน ระบบปฏิบัติการ และระดับเครือข่าย (ไม่ใช่นับตามประเภทของช่องโหว่ที่พบ)
59	จำนวนการใช้บริการจากผู้รับดำเนินการแทนในการให้บริการ			ไม่มีการใช้บริการจากผู้รับดำเนินการแทน	1 - 2 หน่วยงาน	มากกว่า 2 หน่วยงาน	"ผู้รับดำเนินการแทน" หมายความว่า บุคคลภายนอกซึ่งเป็นบุคคลธรรมดาหรือนิติบุคคลที่มีการทำสัญญาหรือข้อตกลงร่วมกับผู้รับใบอนุญาตในการดำเนินการแทนผู้รับใบอนุญาตสำหรับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ตัวแทนในการเก็บรวบรวมข้อมูลผู้ใช้บริการ เป็นต้น ซึ่งอาจมีการเชื่อมต่อระบบงานด้านเทคโนโลยีสารสนเทศกับผู้รับใบอนุญาตด้วย

2. การตอบแบบสอบถามเพื่อประเมินระดับความเสี่ยง

No.	คำถามสำหรับการประเมิน	ผลการประเมิน (ต่ำ/ปานกลาง/สูง)	ข้อมูลหรือคำชี้แจงประกอบผลการประเมิน	ระดับความเสี่ยง ต่ำ	ระดับความเสี่ยง ปานกลาง	ระดับความเสี่ยง สูง	หมายเหตุ
Part 2: กรณีเป็นบริการพิสูจน์ตัวตน (IdP1)							
62	ระดับความน่าเชื่อถือของการพิสูจน์ตันตน (IAL) สูงสุดที่องค์กรสามารถให้บริการ			IAL2.1	IAL2.2	IAL2.3, IAL3	
63	จำนวนผู้อาศัยการยืนยันตัวตน (RP) ที่มีการเชื่อมต่อเพื่อให้บริการพิสูจน์ตัวตน ทั้งกรณีเชื่อมต่อโดยตรงและเชื่อมต่อโดยอ้อม เช่น ผ่าน Exchange			น้อยกว่า 10 ราย	10 - 50 ราย	มากกว่า 50 ราย	กรณีมีการเชื่อมต่อมากกว่า 1 ช่องทาง ให้นับจากผลรวมของจำนวนผู้อาศัยการยืนยันตัวตน (RP) ในแต่ละช่องทางที่เชื่อมต่อ ตัวอย่างเช่น ผลรวมของจำนวน RP ที่เชื่อมต่อโดยตรง + จำนวน RP ที่เชื่อมต่อผ่าน Exchange1 + จำนวน RP ที่อย่างต่อผ่าน Exchange2
64	จำนวนจุดให้บริการการพิสูจน์ตัวตนรวมทั้งหมดที่อยู่ในความดูแลของหน่วยงาน ณ วันสิ้นปีปฏิทิน			น้อยกว่า 500 จุด	500-5000 จุด	มากกว่า 5,000 จุด	นับจากจำนวนจุดให้บริการทางกายภาพของหน่วยงาน รวมกับจุดให้บริการโดยผู้รับดำเนินการแทนที่ไม่ได้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยัน ตัวอย่างจุดให้บริการ เช่น ตู้ smart kiosk, เคาน์เตอร์บริการ (ใน 1 สถานที่อาจมีได้มากกว่า 1 จุดบริการ)
65	จำนวน transaction ต่อปี สำหรับบริการพิสูจน์ตัวตนทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด			น้อยกว่า 50,000 รายการ	50,000 - 500,000 รายการ	มากกว่า 500,000 รายการ	
Part 3: กรณีเป็นบริการบริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (IdP2) และบริการยืนยันตัวตน (IdP3)							
67	ระดับความน่าเชื่อถือของการยืนยันตันตน (AAL) สูงสุดที่องค์กรสามารถให้บริการ			AAL1	AAL2	AAL3	
69	จำนวน transaction ต่อปี สำหรับบริการยืนยันตัวตนทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด			น้อยกว่า 100,000 รายการ	100,000 - 1,000,000 รายการ	มากกว่า 1,000,000 รายการ	
70	จำนวนผู้ใช้บริการ (subscriber) ที่ลงทะเบียนและพร้อมใช้งานบริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือบริการยืนยันตัวตน ณ วันสิ้นปีปฏิทิน			น้อยกว่า 100,000 ราย	100,000 - 1,000,000 ราย	มากกว่า 1,000,000 ราย	

2. การตอบแบบสอบถามเพื่อประเมินระดับความเสี่ยง

No.	คำถามสำหรับการประเมิน	ผลการประเมิน (ต่ำ/ปานกลาง/สูง)	ข้อมูลหรือคำชี้แจงประกอบผลการประเมิน	ระดับความเสี่ยง			หมายเหตุ
				ต่ำ	ปานกลาง	สูง	
Part 4: กรณีเป็นบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Ex.)							
71	จำนวนผู้อาศัยการยืนยันตัวตน (RP) และผู้พิสูจน์และยืนยันตัวตน (IdP) ที่มีการเชื่อมต่อเพื่อให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล			น้อยกว่า 10 ราย	10 -30 ราย	มากกว่า 30 ราย	
72	จำนวน transaction ต่อปี สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด			น้อยกว่า 400,000 รายการ	400,000 - 4,000,000 รายการ	มากกว่า 4,000,000 รายการ	

3.1 การสรุประดับความเสี่ยงของแต่ละปัจจัยเสี่ยง

สำหรับปัจจัยเสี่ยง **เทคโนโลยีและช่องทางการให้บริการ** และ **ลักษณะผลิตภัณฑ์และการให้บริการ**

ใช้ค่าที่มีจำนวนมากที่สุด (ฐานนิยม) เป็นผลการประเมิน และพิจารณาเงื่อนไขประกอบการประเมิน ดังนี้

เงื่อนไข ก : กรณีที่ฐานนิยมมี 2 ค่า ให้ใช้ค่าที่สูงกว่าเป็นผลการประเมิน

เงื่อนไข ข : กรณีไม่มีฐานนิยม (จำนวนข้อ ต่ำ ปาน กลางสูง เท่ากัน) ให้ใช้ค่าเป็น ปานกลาง เป็นผลการประเมิน

เงื่อนไข ค : กรณีผลการประเมินเป็นระดับต่ำ ให้นำจำนวนของข้อที่เป็นระดับปานกลางและสูง มารวมกัน

- หากค่าดังกล่าวมากกว่าหรือเท่ากับจำนวนข้อของระดับต่ำ ให้กำหนดระดับความเสี่ยงของปัจจัยเสี่ยงเป็นระดับปานกลาง
- หากค่าดังกล่าวน้อยกว่าจำนวนข้อของระดับต่ำ ให้กำหนดระดับความเสี่ยงของปัจจัยเสี่ยงเป็นระดับต่ำ

3.2 การสรุประดับความเสี่ยงของผู้ประกอบธุรกิจ

3.2.1 พิจารณาระดับความเสี่ยงขั้นต้น (RLA1) ของผู้ประกอบธุรกิจโดยอ้างอิงเกณฑ์ตามตาราง

เกณฑ์การพิจารณาระดับความเสี่ยงขั้นต้น (RLA1)		ปัจจัยเสี่ยง: **ลักษณะผลิตภัณฑ์และการให้บริการ**		
		ต่ำ	ปานกลาง	สูง
ปัจจัยเสี่ยง: **เทคโนโลยีและช่องทางการให้บริการ**	สูง	RLA1=ปานกลาง	RLA1=สูง	RLA1=สูง
	ปานกลาง	RLA1=ต่ำ	RLA1=ปานกลาง	RLA1=สูง
	ต่ำ	RLA1=ต่ำ	RLA1=ต่ำ	RLA1=ปานกลาง

3.2 การสรุประดับความเสี่ยงของผู้ประกอบธุรกิจ

3.2.2 กำหนดระดับความเสี่ยงของผู้ประกอบธุรกิจ (RLA) โดยพิจารณาร่วมกับประวัติเหตุการณ์ไม่พึงประสงค์

(1) พิจารณา **ระดับความเสี่ยงที่สูงที่สุด** จากคำถามประเมินความเสี่ยงทั้งหมด ของปัจจัยเสี่ยง "ประวัติเหตุการณ์ไม่พึงประสงค์"

ประวัติเหตุการณ์ไม่พึงประสงค์
15.จำนวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
18.จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID
19.ระยะเวลารวมของการหยุดให้บริการชั่วคราวของระบบการให้บริการ Digital ID ที่มีผลกระทบต่อลูกค้าหรือผู้ใช้บริการและไม่ได้เป็นการเตรียมการไว้ล่วงหน้า
20.จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ (incident) ที่มีผลกระทบในระดับกลางขึ้นไป

(2) กำหนดระดับความเสี่ยงผู้ประกอบธุรกิจ (RLA) โดยพิจารณาเงื่อนไข ดังนี้

- หากความเสี่ยงตาม (1) มีระดับสูงกว่า RLA1 ให้กำหนด RLA = ความเสี่ยงตาม (1)
- หากความเสี่ยงตาม (1) มีระดับต่ำกว่าหรือเท่ากับ RLA1 ให้กำหนด RLA = RLA1

ตัวอย่างแนวทางการพิจารณาระดับความเสี่ยงตาม 3.2.1

ตัวอย่าง

IDP Service		A	B	C
ปัจจัยเสี่ยง: ลักษณะผลิตภัณฑ์และการให้บริการ	สูง	1	3	2
	ปานกลาง	2	2	0
	ต่ำ	2	0	0
	RISK LEVEL	ปานกลาง	สูง	สูง
	RISK LEVEL (ปรับตาม 3.1 ค)	ปานกลาง	สูง	สูง
ปัจจัยเสี่ยง: เทคโนโลยีและช่องทางการให้บริการ	สูง	1	1	1
	ปานกลาง	1	1	2
	ต่ำ	3	3	2
	RISK LEVEL	ต่ำ	ต่ำ	ปานกลาง
	RISK LEVEL (ปรับตาม 3.1 ค)	ต่ำ	ต่ำ	ปานกลาง
ระดับความเสี่ยงขั้นต้น	RLA1	ต่ำ	ปานกลาง	สูง

Exchange Service		D	E	F
ปัจจัยเสี่ยง: ลักษณะผลิตภัณฑ์และการให้บริการ	สูง	1	0	0
	ปานกลาง	0	0	1
	ต่ำ	0	1	0
	RISK LEVEL	สูง	ต่ำ	ปานกลาง
	RISK LEVEL (ปรับตาม 3.1 ค)	สูง	ต่ำ	ปานกลาง
ปัจจัยเสี่ยง: ลักษณะผลิตภัณฑ์และการให้บริการ	สูง	1	0	1
	ปานกลาง	0	0	1
	ต่ำ	3	4	2
	RISK LEVEL	ต่ำ	ต่ำ	ต่ำ
	RISK LEVEL (ปรับตาม 3.1 ค)	ต่ำ	ต่ำ	ปานกลาง
ระดับความเสี่ยงขั้นต้น	RLA1	ปานกลาง	ต่ำ	ปานกลาง

ตัวอย่างแนวทางการพิจารณาระดับความเสี่ยงตาม 3.2.2

ตัวอย่าง

ประวัติเหตุการณ์ไม่พึงประสงค์	Risk Level
15.จำนวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล	สูง
18.จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID	ต่ำ
19.ระยะเวลารวมของการหยุดให้บริการชั่วคราวของระบบการให้บริการ Digital ID ที่มีผลกระทบต่อลูกค้าหรือผู้ใช้บริการและไม่ได้เป็นการเตรียมการไว้ล่วงหน้า	ต่ำ
20.จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ (incident) ที่มีผลกระทบในระดับกลางขึ้นไป	ปานกลาง

Highest Risk
=
สูง

ระดับความเสี่ยงขั้นต้น

ระดับความเสี่ยงของผู้ประกอบธุรกิจ

Q&A