ข้อเสนอในการปรับปรุงร่างเอกสารแนวทางการประเมินประจำปีเพื่อระบุระดับความเสี่ยงภายหลังจากการรับฟังความคิดเห็น

ปัจจัยเสี่ยง	คำถามสำหรับการประเมิน ฉบับรับฟังความคิดเห็น	คำถามสำหรับการประเมิน ฉบับปรับปรุง	เหตุผลการปรับปรุง
Part 1: สำหรับทุกลักษณะบริการ			
ประวัติเหตุการณ์ไม่พึงประสงค์	ข้อ 15 จำนวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล* ครอบคลุมการรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ อ้างอิง ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565	**-ไม่มีการแก้ไข-**	
ประวัติเหตุการณ์ไม่พึงประสงค์	ข้อ 18 จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด เช่น การถูกปลอมแปลงตัวตน	ข้อ 18 จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID ที่กระทำการสำเร็จในรอบปีปฏิทินล่าสุด เช่น การพิสูจน์ตัวตนสำเร็จโดยอาศัยการปลอมแปลงตัวตนหรือหลักฐานอันเป็นเท็จ การยืนยันตัวตนสำเร็จโดยอาศัยสิ่งยืนยันตัวตนของบุคคลอื่นหรืออาศัยช่องโหว่ของระบบ เป็นต้น	ปรับข้อความในคำถามประเมินความเสี่ยงข้อ 18 โดยเพิ่มเติมข้อความ "ที่กระทำการสำเร็จ" และเพิ่มเติมตัวอย่างให้ชัดเจนยิ่งขึ้น เพื่อพิจารณาเฉพาะเหตุการณ์ที่อาจมีผลกระทบต่อระบบการให้บริการ เพื่อให้สอดคล้องกับคำถามข้ออื่นๆ ในปัจจัยเสี่ยงประวัติเหตุการณ์ไม่พึงประสงค์

ปัจจัยเสี่ยง	คำถามสำหรับการประเมิน ฉบับรับฟังความคิดเห็น	คำถามสำหรับการประเมิน ฉบับปรับปรุง	เหตุผลการปรับปรุง
			<u>เหตุผลการปรับปรุง</u> - การคิดผลสรุปความเสี่ยงของปัจจัยเสี่ยงด้านประวัติเหตุการณ์ไม่พึงประสงค์ ใช้วิธีคิดจากค่าความเสี่ยงที่สูงที่สุด เนื่องจากคำถามในปัจจัยดังกล่าวสะท้อนให้เห็นถึงความเสี่ยงในด้านการละเมิดข้อมูลส่วนบุคคล, การทุจริตหรือการฉ้อโกงจากการใช้งานระบบ, การหยุดให้บริการ และความมั่นคงปลอดภัยสารสนเทศโดยตรง ซึ่งแตกต่างของปัจจัยอื่นที่เป็นคำถามเพื่อระบุความเสี่ยงตั้งต้น (inherent risk) ดังนั้นการคิดคำนวนจึงให้ความสำคัญกับผลการประเมินในปัจจัยดังกล่าวในการระบุระดับความเสี่ยงของผู้ประกอบธุรกิจ (RLA)
ประวัติเหตุการณ์ไม่พึงประสงค์	ข้อ 19 ระยะเวลารวมของการหยุดให้บริการชั่วคราวของระบบการให้บริการ Digital ID ที่ไม่ได้เป็นการเตรียมการไว้ล่วงหน้า และมีผลกระทบต่อลูกค้าหรือผู้ใช้บริการในรอบปีปฏิทินล่าสุด	**-ไม่มีการแก้ไข-**	

ปัจจัยเสี่ยง	คำถามสำหรับการประเมิน ฉบับรับฟังความคิดเห็น	คำถามสำหรับการประเมิน ฉบับปรับปรุง	เหตุผลการปรับปรุง
ประวัติเหตุการณ์ไม่พึงประสงค์	ข้อ 20 จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ (incident) ที่มีผลกระทบในระดับกลางขึ้นไป* เช่น ภัยคุกคามทางไซเบอร์, ข้อมูลรั่วไหล, ระบบหรือบริการหยุดชะงักเป็นเวลานาน (มากกว่า 8 ชั่วโมง), ความผิดปกติอย่างร้ายแรงของระบบที่เกี่ยวกับการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด หมายเหตุ ผลกระทบในระดับกลางขึ้นไป หมายถึงมูลค่าความเสียหาย มากกว่า 1 ล้านบาท/ผู้เสียหายมากกว่า 10,000 คน/กระทบต่อชีวิต ร่างกายหรืออนามัยของคน/กระทบต่อความมั่นคงของรัฐ (อ้างอิงประกาศ คธอ. เรื่อง ประเภทธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีแบบปลอดภัย พ.ศ. 2555)	-ไม่มีการแก้ไข-	
เทคโนโลยี และช่องทางการให้บริการ	ข้อ 32 การใช้งานแผนสำรองฉุกเฉิน (BCP และ DRP) ที่เกี่ยวข้องกับการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด	-ไม่มีการแก้ไข-	
เทคโนโลยี และช่องทางการให้บริการ	ข้อ 33 ช่องโหว่ภายในระบบหรือแอปพลิเคชันสำหรับบริการ Digital ID ที่มีความเสี่ยงของช่องโหว่ระดับ High หรือ Critical	-ไม่มีการแก้ไข-	

ปัจจัยเสี่ยง	คำถามสำหรับการประเมิน ฉบับรับฟังความคิดเห็น	คำถามสำหรับการประเมิน ฉบับปรับปรุง	เหตุผลการปรับปรุง
	หมายเหตุ: นับจำนวน ตามจำนวนช่องโหว่ที่พบทั้งหมดรวมกัน จากผลการทดสอบระบบในระดับแอปพลิเคชัน ระบบปฏิบัติการ และระดับเครือข่าย (ไม่ใช่นับตามประเภทของช่องโหว่ที่พบ)		
เทคโนโลยี และช่องทางการให้บริการ	ข้อ 59 จำนวนการใช้บริการจากผู้รับดำเนินการแทนในการให้บริการ หมายเหตุ: "ผู้รับดำเนินการแทน" หมายความว่า บุคคลภายนอกซึ่งเป็นบุคคลธรรมดาหรือนิติบุคคลที่มีการทำสัญญาหรือข้อตกลงร่วมกับผู้รับใบอนุญาตในการดำเนินการแทนผู้รับใบอนุญาตสำหรับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ตัวแทนในการเก็บรวบรวมข้อมูลผู้ใช้บริการ เป็นต้น ซึ่งอาจมีการเชื่อมต่อระบบงานด้านเทคโนโลยีสารสนเทศกับผู้รับใบอนุญาตด้วย	-ไม่มีการแก้ไข-	
Part 2: กรณีเป็นบริการพิสูจน์ตัวตน (IdP1)			
ลักษณะผลิตภัณฑ์และการให้บริการ	ข้อ 62 ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) สูงสุดที่องค์กรสามารถให้บริการ	-ไม่มีการแก้ไข-	
เทคโนโลยี และช่องทางการให้บริการ	ข้อ 63 จำนวนผู้อาศัยการยืนยันตัวตน (RP) ที่มีการเชื่อมต่อเพื่อให้บริการพิสูจน์ตัวตน ทั้งกรณีเชื่อมต่อโดยตรงและเชื่อมต่อโดยอ้อม เช่น ผ่าน Exchange	ข้อ 63 จำนวนผู้อาศัยการยืนยันตัวตน (RP) ที่มีการเชื่อมต่อเพื่อให้บริการพิสูจน์ตัวตน ทั้งกรณีเชื่อมต่อโดยตรงและเชื่อมต่อโดยอ้อม เช่น ผ่าน Exchange	ปรับแก้ไขข้อความในหมายเหตุในข้อ 63 เล็กน้อย เหตุผลการปรับปรุง

ปัจจัยเสี่ยง	คำถามสำหรับการประเมิน ฉบับรับฟังความคิดเห็น	คำถามสำหรับการประเมิน ฉบับปรับปรุง	เหตุผลการปรับปรุง
	หมายเหตุ: กรณีมีการเชื่อมต่อมากกว่า 1 ช่องทาง ให้นับจากผลรวมของจำนวนผู้อาศัยการยืนยันตัวตน (RP) ในแต่ละช่องทางที่เชื่อมต่อ ตัวอย่างเช่น ผลรวมของจำนวน RP ที่เชื่อมต่อโดยตรง + จำนวน RP ที่เชื่อมต่อผ่าน Exchange1 + จำนวน RP ที่อย่างต่อผ่าน Exchange2	หมายเหตุ: กรณีมีการเชื่อมต่อมากกว่า 1 ช่องทาง ให้นับจากผลรวมของจำนวนผู้อาศัยการยืนยันตัวตน (RP) ในแต่ละช่องทางที่สามารถเชื่อมต่อมายังบริการของท่าน ตัวอย่างเช่น ผลรวมของจำนวน RP ที่สามารถเชื่อมต่อโดยตรง + จำนวน RP ที่สามารถเชื่อมต่อผ่าน Exchange1 + จำนวน RP ที่สามารถเชื่อมต่อผ่าน Exchange2	เพื่อความชัดเจนในเรื่องแนวทางการนับจำนวน เพื่อตอบแบบประเมินประจำปี เพื่อระบุระดับความเสี่ยงของผู้ประกอบธุรกิจ
เทคโนโลยี และช่องทางการให้บริการ	ข้อ 64 จำนวนจุดให้บริการการพิสูจน์ตัวตนรวมทั้งหมดที่อยู่ในความดูแลของหน่วยงาน ณ วันสิ้นปีปฏิทิน หมายเหตุ: นับจากจำนวนจุดให้บริการทางกายภาพของหน่วยงาน รวมกับจุดให้บริการโดยผู้รับดำเนินการแทนที่ไม่ได้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยัน ตัวอย่างจุดให้บริการ เช่น ตู้ smart kiosk, เคาน์เตอร์บริการ (ใน 1 สถานที่อาจมีได้มากกว่า 1 จุดบริการ)	**-ไม่มีการแก้ไข-**	
ลักษณะผลิตภัณฑ์และการให้บริการ	ข้อ 65 จำนวน transaction ต่อปี สำหรับบริการพิสูจน์ตัวตนทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด	**-ไม่มีการแก้ไข-**	

ปัจจัยเสี่ยง	คำถามสำหรับการประเมิน ฉบับรับฟังความคิดเห็น	คำถามสำหรับการประเมิน ฉบับปรับปรุง	เหตุผลการปรับปรุง
Part 3: กรณีเป็นบริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (IdP2) และบริการยืนยันตัวตน (IdP3)			
ลักษณะผลิตภัณฑ์และการให้บริการ	ข้อ 67 ระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) สูงสุดที่องค์กรสามารถให้บริการ	**-ไม่มีการแก้ไข-**	
ลักษณะผลิตภัณฑ์และการให้บริการ	ข้อ 69 จำนวน transaction ต่อปี สำหรับบริการยืนยันตัวตนทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด	**-ไม่มีการแก้ไข-**	
ลักษณะผลิตภัณฑ์และการให้บริการ	ข้อ 70 จำนวนผู้ใช้บริการ (subscriber) ที่ลงทะเบียนและพร้อมใช้งานบริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือบริการยืนยันตัวตน ณ วันสิ้นปีปฏิทิน	**-ไม่มีการแก้ไข-**	
Part 4: กรณีเป็นบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Ex.)			
เทคโนโลยี และช่องทางการให้บริการ	ข้อ 71 จำนวนผู้อาศัยการยืนยันตัวตน (RP) และผู้พิสูจน์และยืนยันตัวตน (IdP) ที่มีการเชื่อมต่อให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล	**-ไม่มีการแก้ไข-**	
ลักษณะผลิตภัณฑ์และการให้บริการ	ข้อ 72 จำนวน transaction ต่อปี สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด	**-ไม่มีการแก้ไข-**	