คำถาม - คำตอบเพิ่มเติมจากการรับฟังความคิดเห็นต่อ
แนวทางในการพัฒนาร่างหลักเกณฑ์การตรวจประเมินประจำปี

ข้อ	คำถาม	คำตอบ
แนวทางในการพัฒนาร่างหลักเกณฑ์การตรวจประเมินประจำปี		
1.	การตรวจประเมินประจำปีจะต้องดำเนินการตรวจสอบโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก และผู้ตรวจสอบทุกคนต้องได้รับประกาศนียบัตรตามหลักเกณฑ์ที่กำหนดใช่หรือไม่	อ้างอิงตามข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 5 หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ ข้อ 22 ได้มีการกำหนดคุณสมบัติของผู้ตรวจสอบ โดยไม่ได้มีข้อจำกัดว่าต้องดำเนินการตรวจสอบโดยผู้ตรวจสอบภายในหรือภายนอก สำหรับการตรวจประเมินเฉพาะด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กำหนดให้ผู้ตรวจสอบจะต้องผ่านการรับรองและมีวุฒิบัตรหรือได้รับประกาศนียบัตรด้านความมั่นคงปลอดภัยระดับสากลตามที่ประกาศกำหนด
2	การประเมินระดับความเสี่ยงขององค์กร (RLA) ต้องดำเนินการปีละกี่ครั้ง และต้องเริ่มดำเนินการเมื่อใด	ผู้รับใบอนุญาตจะต้องดำเนินการประเมินความเสี่ยงปีละ 1 ครั้ง โดยเมื่อผู้รับใบอนุญาตได้ดำเนินการประเมินความเสี่ยงและนำส่งผลการประเมินต่อสำนักงานเรียบร้อยแล้ว ผู้รับใบอนุญาตต้องดำเนินการตรวจประเมินให้สอดคล้องกับระดับความเสี่ยง พร้อมนำส่งผลรายงานผลการตรวจประเมินประจำปีภายในเวลาที่กำหนด ซึ่งจากการรับฟังความคิดเห็นจะมีการทบทวนการกำหนดเวลานำส่ง เพื่อให้สอดคล้องกับทางปฏิบัติของผู้ประกอบธุรกิจอีกครั้ง ทั้งนี้ สพธอ. คาดว่า ในการออกประกาศหลักเกณฑ์การตรวจประเมินประจำปีในปีแรกอาจมีความยืดหยุ่นในการขยายระยะเวลาการนำส่งผลการประเมินความเสี่ยงเป็นภายในไตรมาส 1 ของปี 2568 หลังจากนั้นในรอบปีถัดไปผู้รับใบอนุญาตนำส่งผลตามที่หลักเกณฑ์กำหนด
3	หน่วยงานใดขององค์กรที่ต้องรับผิดชอบในการประเมินระดับความเสี่ยงขององค์กร (RLA) และต้องผ่านการพิจารณาอนุมัติหรือไม่อย่างไร	ตามร่างหลักเกณฑ์มิได้กำหนดผู้ที่ทำหน้าที่ประเมินความเสี่ยงไว้เป็นการเฉพาะ จึงขึ้นอยู่กับการมอบหมายหรือโครงสร้างขององค์กร โดยผลการประเมินความเสี่ยงต้องผ่านการรายงานต่อผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายก่อนนำส่งต่อ สพธอ.
4	ในกรณีที่หน่วยงานอยู่ระหว่างกระบวนการพิจารณาคำขอรับใบอนุญาตและยังไม่ได้รับใบอนุญาต หน่วยงานจำเป็นต้องดำเนินการประเมินความเสี่ยงและตรวจประเมินประจำปีหรือไม่	สำหรับผู้ขอรับใบอนุญาตที่อยู่ระหว่างการพิจารณาออกใบอนุญาต สพธอ. จะมีการหารือร่วมกับผู้ขอรับใบอนุญาตเป็นรายกรณีไป
5	ในปี 2567 หน่วยงานได้เริ่มดำเนินการการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศไปบางส่วนแล้ว ต้องใช้แบบรายงานผลการตรวจประเมินฉบับใด	สำหรับการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ประจำปี 2567 ให้ดำเนินการใช้แบบรายงานผลการตรวจประเมินระบบการให้บริการฉบับปัจจุบันที่ได้เผยแพร่บนเว็บไซต์

ข้อ	คำถาม	คำตอบ
		https://www.etda.or.th/th/regulator/DigitalID/index.aspx ไปพลางก่อน โดยการดำเนินการตามร่างหลักเกณฑ์จะมีการกำหนดบทรองรับช่วงการเปลี่ยนผ่านการดำเนินการให้สอดคล้องกัน
6	เมื่อมีการประกาศใช้หลักเกณฑ์การตรวจประเมินประจำปี จะมีแบบฟอร์มการรายงานและคู่มือแนวทางการประเมินด้วยหรือไม่	สพธอ. อยู่ระหว่างการพิจารณาจัดทำแบบรายงานผลการตรวจประเมินประจำปี และคู่มือแนวทางการตรวจประเมิน อย่างไรก็ตาม ในระหว่างนี้ขอให้อ้างอิงแนวทางการตรวจประเมินตามประกาศหลักเกณฑ์ฉบับปัจจุบันที่ได้เผยแพร่บนเว็บไซต์ https://www.etda.or.th/th/regulator/DigitalID/law.aspx
7	มีแบบฟอร์มในการพิจารณาความมีนัยสำคัญตามที่กำหนดในร่างหลักเกณฑ์ฯ หรือไม่ หรือสามารถอ้างอิงตามกระบวนการหรือหลักการที่องค์กรมีกำหนดไว้	การพิจารณาความมีนัยสำคัญนั้น ขอให้อ้างอิงตามหลักการหรือแนวทางของผู้รับใบอนุญาตที่มีการพิจารณากำหนดภายในองค์กร ทั้งนี้ การพิจารณากำหนดความมีนัยสำคัญควรพิจารณาภายใต้กรอบหลักการที่คำนึงถึงความเสี่ยงและผลกระทบต่อการให้บริการของผู้รับใบอนุญาตในวงกว้าง
8	การรวบรวมผลการตรวจประเมินจากหลายรอบการตรวจประเมินที่ดำเนินการภายในปีปฏิทินเดียวกันนั้น สามารถใช้ผลย้อนหลัง 12 เดือนแทนได้หรือไม่	องค์กรสามารถดำเนินการประเมินคราวเดียวพร้อมกัน หรือพิจารณาแยกขอบเขตการประเมิน และใช้ผลการตรวจประเมินในขอบเขตที่เกี่ยวข้องภายในรอบปีการประเมินเดียวกันรวบรวมนำส่งได้ แต่ต้องเป็นการประเมินที่ครอบคลุมขอบเขตการให้บริการที่ได้รับใบอนุญาต
9	กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ปีที่ไม่ได้มีการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) สามารถจัดทำแผนงานและดำเนินการตรวจประเมินข้อกำหนดบางส่วน โดยพิจารณาตามความเสี่ยงและความเหมาะสม คำว่าข้อกำหนดบางส่วน มีการกำหนดขั้นต่ำของหัวข้อหรือไม่	ในทางปฏิบัติจะให้ความสำคัญกับการตรวจติดตามผลในรอบปีที่ผ่านมาว่าเป็น minor nonconformity หรือ observation หากผลการตรวจประเมินมีบางประเด็นที่เป็น minor nonconformity ควรจะต้องมีการตรวจติดตามประเด็นนั้นๆ ในปีถัดไป ทั้งนี้ การกำหนดจำนวนขั้นต่ำของหัวข้อที่ต้องทำการตรวจประเมินสำหรับองค์กรที่มีระดับความเสี่ยงต่ำจะพิจารณาความเหมาะสมต่อไป
แนวทางการประเมินเพื่อระบุระดับความเสี่ยงของผู้ประกอบธุรกิจ		
1	การนับจำนวนปริมาณ transaction / จำนวนเหตุการณ์ incident / จำนวนผู้ใช้บริการ ฯลฯ ให้นับตั้งแต่เมื่อใด	การนับจำนวนปริมาณในแต่ละข้อคำถาม จะมีคำอธิบายการเก็บข้อมูลไว้ในหมายเหตุของแต่ละข้อ โดยผู้ประเมินสามารถให้ข้อมูลหรือคำชี้แจงประกอบการประเมินได้
2	ข้อคำถามการประเมินความเสี่ยงเกี่ยวกับช่องโหว่ภายในระบบหรือแอปพลิเคชันสำหรับบริการ Digital ID ที่มีความเสี่ยงของช่องโหว่ระดับ high หรือ critical ให้นับรวมผลการเจาะระบบ (penetration test) หรือการตรวจสอบช่องโหว่ (vulnerability assessment) ใช่หรือไม่	การประเมินจำนวนช่องโหว่ให้พิจารณาจำนวนคงเหลือของระดับ high หรือ critical ณ ขณะที่ทำการประเมิน และนับรวมผลการทดสอบ penetration test และ vulnerability assessment ซึ่งหมายรวมถึงผลการทดสอบช่องโหว่อื่นใดที่หน่วยงานดำเนินการที่อยู่ภายใต้ขอบเขตการให้บริการที่ได้รับใบอนุญาต

ข้อ	คำถาม	คำตอบ
3	ข้อคำถามการประเมินความเสี่ยงเกี่ยวกับจำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด เช่น การถูกปลอมแปลงตัวตน ควรมีการยกตัวอย่างที่ชัดเจน เช่น การแอบอ้างบุคคลอื่นเพื่อเปิดบัญชีธนาคารและได้มีการทำ NDID ไปยังอีกธนาคาร รวมอยู่ในกรณีนี้หรือไม่	กรณีที่มีการเกิดการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ เช่น การปลอมแปลงตัวตนจะนำมาประเมินความเสี่ยงด้วย ไม่ว่าการทุจริตหรือฉ้อโกงนั้นจะสำเร็จหรือไม่สำเร็จก็ตาม
4	ข้อคำถามแบบประเมินความเสี่ยงเกี่ยวกับจำนวนจุดให้บริการการพิสูจน์ตัวตน ต้องเป็นจุดที่ end to end process หรือไม่	ในแบบประเมินความเสี่ยงได้จัดทำคำอธิบาย การนับจำนวนจุดให้บริการทางกายภาพของหน่วยงาน รวมกับจุดให้บริการโดยผู้รับดำเนินการแทน เช่น ตู้ smart kiosk เคาน์เตอร์บริการ ซึ่งในสถานที่หนึ่งแห่งอาจมีได้มากกว่า 1 จุดให้บริการ