

ร่างหลักเกณฑ์การตรวจประเมินประจำปี
สำหรับผู้ได้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
(ฉบับปรับปรุงภายหลังรับฟังความคิดเห็น)

ส่วนที่ 1 การตรวจประเมินประจำปี

ข้อ 1 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการอย่างน้อยปีละหนึ่งครั้ง ให้ครอบคลุมหัวข้ออย่างน้อยดังนี้

- 1.1 การปฏิบัติตามหลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ หมวด 1 ธรรมชาติทางด้านเทคโนโลยีสารสนเทศ หมวด 2 การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และหมวด 3 การบริหารและการจัดการความเสี่ยงของระบบการให้บริการ
- 1.2 การปฏิบัติตามหลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
- 1.3 การปฏิบัติตามหลักเกณฑ์การตามลักษณะของการให้บริการ
- 1.4 หัวข้ออื่น ๆ ตามได้รับแจ้งจากสำนักงาน

ข้อ 2 ขอบเขตในการตรวจประเมินต้องครอบคลุมระบบการให้บริการสำหรับบริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน บริการยืนยันตัวตน และบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งประกอบด้วย การปฏิบัติงาน กระบวนการทำงาน และระบบงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

ข้อ 3 ผู้รับใบอนุญาตต้องดำเนินการประเมินความเสี่ยงให้สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงานตามรูปแบบที่สำนักงานกำหนด พร้อมจัดส่งผลการประเมินต่อสำนักงานภายใน 60 วันนับแต่วันสิ้นปีปฏิทิน โดยผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินก่อนนำส่งต่อสำนักงาน

ข้อ 4 การตรวจประเมินตามข้อ 1.4 ต้องกำหนดแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง ให้ครอบคลุมส่วนที่มีการเปลี่ยนแปลงของระบบการให้บริการ

ข้อ 5 การตรวจประเมินตามข้อ 1.1 1.2 และ 1.3 ต้องกำหนดแผนงานและดำเนินการตรวจประเมินให้สอดคล้องกับระดับความเสี่ยงการประกอบธุรกิจของผู้รับใบอนุญาต โดยมีรายละเอียด ดังนี้

- 5.1 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องกำหนดแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดให้ครอบคลุมข้อกำหนดทั้งหมดภายใต้หลักเกณฑ์ (full scope) แบบปีเว้นปี

5.1.1 ปีที่เป็นการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) ต้องจัดทำแผนงานและดำเนินการตรวจประเมินให้ครบทุกข้อกำหนดภายใต้หลักเกณฑ์

5.1.2 ปีที่ไม่ได้มีการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) สามารถจัดทำแผนงานและดำเนินการตรวจประเมินข้อกำหนดบางส่วน โดยพิจารณาตามความเสี่ยงและความเหมาะสม

5.2 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลางหรือสูง ต้องจัดทำแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดให้ครบทุกข้อกำหนดภายใต้หลักเกณฑ์ (full scope) ทุกปี

ข้อ 6 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการและรายงานผลการตรวจประเมินระบบการให้บริการให้สอดคล้องกับหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ

ข้อ 7 ผู้รับใบอนุญาตต้องรายงานผลการตรวจประเมินประจำปีตามรูปแบบที่สำนักงานกำหนด ภายใน 60 วันนับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ แต่ไม่เกินวันที่ 1 มีนาคมของปีถัดไป

ข้อ 8 การรายงานผลการตรวจประเมินประจำปีต่อสำนักงาน ผู้รับใบอนุญาตสามารถรวบรวมผลจากหลายรอบการตรวจประเมินที่ดำเนินการภายในปีปฏิทินเดียวกัน โดยต้องจัดทำรายงานผลการตรวจประเมินประจำปีให้มีรายละเอียดครบถ้วนตามหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ และต้องจัดทำตารางเพื่อแสดงข้อกำหนดภายใต้หลักเกณฑ์และขอบเขตที่ตรวจประเมินในแต่ละรอบการตรวจ เพื่อให้มั่นใจว่าการตรวจประเมินในแต่ละปีครอบคลุมหลักเกณฑ์และระบบการให้บริการที่เกี่ยวข้อง

ข้อ 9 ผู้รับใบอนุญาตต้องจัดเก็บรายงานผลการตรวจประเมินไว้เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงาน เพื่อให้พร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดยสำนักงาน