แนวทางในการพัฒนาร่างหลักเกณฑ์การตรวจประเมินประจำปี

ส่วนที่ 1 การตรวจประเมินประจำปี

ข้อ 1 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการอย่างน้อยปีละหนึ่งครั้ง ให้ครอบคลุมหัวข้ออย่างน้อยดังนี้

1.1 การปฏิบัติตามหลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ หมวด 1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ หมวด 2 การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และหมวด 3 การบริหารและการจัดการความเสี่ยงของระบบการให้บริการ

1.2 การปฏิบัติตามหลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

1.3 การปฏิบัติตามหลักเกณฑ์การตามลักษณะของการให้บริการหลักเกณฑ์ตามลักษณะของการให้บริการ

1.4 หัวข้ออื่น ๆ ตามได้รับแจ้งจากสำนักงาน

ข้อ 2 ขอบเขตในการตรวจประเมินต้องครอบคลุมระบบการให้บริการสำหรับบริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน บริการยืนยันตัวตน และบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งประกอบด้วยการปฏิบัติงาน กระบวนการทำงาน และระบบงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

ข้อ 3 ผู้รับใบอนุญาตต้องดำเนินการประเมินความเสี่ยงให้สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงานตามรูปแบบที่สำนักงานกำหนด พร้อมจัดส่งผลการประเมินต่อสำนักงานภายใน 30 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 30 วัน นับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ แต่ไม่เกินวันที่ 31 มกราคมของปีถัดไป

ข้อ 8 การรายงานผลการตรวจประเมินประจำปีต่อสำนักงาน ผู้รับใบอนุญาตสามารถรวบรวมผลจากหลายรอบการตรวจประเมินที่ดำเนินการภายในปีปฏิทินเดียวกัน โดยต้องจัดทำรายงานผลการตรวจประเมินประจำปีให้มีรายละเอียดครบถ้วนตามหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ และต้องจัดทำตารางเพื่อแสดงข้อกำหนดภายใต้หลักเกณฑ์และขอบเขตที่ตรวจประเมินในแต่ละรอบการตรวจ เพื่อให้มั่นว่าการตรวจประเมินในแต่ละปีครอบคลุมหลักเกณฑ์และระบบการให้บริการที่เกี่ยวข้อง

ข้อ 9 ผู้รับใบอนุญาตต้องจัดเก็บรายงานผลการตรวจประเมินไว้เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงาน เพื่อให้พร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดยสำนักงาน

ส่วนที่ 2 การพิจารณาความมีนัยสำคัญ

ข้อ 10 ผู้รับใบอนุญาตต้องจัดให้มีข้อกำหนดในการพิจารณาความมีนัยสำคัญหรือความสำคัญที่ชัดเจนเพื่อใช้พิจารณาดำเนินการในเรื่องต่าง ๆ โดยดำเนินการดังนี้

10.1 ข้อกำหนดดังกล่าวต้องผ่านการพิจารณร่วมกันของหน่วยงานที่เกี่ยวข้อง รวมทั้งต้องได้รับอนุมัติจากผู้บริหาร คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย

10.2 ข้อกำหนดในการพิจารณาความมีนัยสำคัญต้องพิจารณาภายใต้กรอบหลักการที่คำนึงถึงความเสี่ยงและผลกระทบต่อการให้บริการของผู้รับใบอนุญาตในวงกว้าง เช่น กระทบลูกค้าหรือผู้ใช้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้รับใบอนุญาต และคำนึงถึงผลกระทบต่อระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในวงกว้าง เช่น กระทบต่อระบบงานกลางที่มีนัยสำคัญเชิงโครงสร้างต่อการให้บริการของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

10.3 ต้องทบทวนข้อกำหนดอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบต่อการให้บริการ

ข้อ 11 ผู้รับใบอนุญาตต้องสื่อสารข้อกำหนดดังกล่าวให้แก่บุคลากรและบุคคลภายนอกที่เกี่ยวข้องทราบและนำไปปฏิบัติ

ส่วนที่ 3 การแจ้งการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการ

ข้อ 12 การแจ้งนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการ

12.1 ผู้รับใบอนุญาตที่นำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยี โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนดที่ผู้รับใบอนุญาตได้กำหนดขึ้นตามข้อ 10 ทั้งกรณีที่ผู้รับใบอนุญาตดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้องแจ้งการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวต่อสำนักงานล่วงหน้าไม่น้อยกว่า 30 วันก่อนดำเนินการ ตามรูปแบบและวิธีที่สำนักงานกำหนด เว้นแต่สำนักงานมีคำสั่งให้ผู้รับใบอนุญาตไม่ต้องแจ้งการนำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบ หรือเทคโนโลยีที่มีนัยสำคัญ