

ข้อเสนอในการปรับปรุงร่างหลักเกณฑ์การตรวจประเมินประจำปีภายหลังจากการรับฟังความคิดเห็น

ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น	ร่างหลักเกณฑ์ฉบับปรับปรุง (ภายหลังจากรับฟังความคิดเห็น)	เหตุผลการปรับปรุง
<b>ส่วนที่ 1 การตรวจประเมินประจำปี</b>		
<p>ข้อ 1 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการอย่างน้อยปีละหนึ่งครั้งให้ครอบคลุมหัวข้ออย่างน้อยดังนี้</p> <p>1.1 การปฏิบัติตามหลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ หมวด 1 ธรรมชาติของเทคโนโลยีสารสนเทศ หมวด 2 การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และหมวด 3 การบริหารและการจัดการความเสี่ยงของระบบการให้บริการ</p> <p>1.2 การปฏิบัติตามหลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ</p> <p>1.3 การปฏิบัติตามหลักเกณฑ์การตามลักษณะของการให้บริการ</p> <p>1.4 หัวข้ออื่น ๆ ตามที่ได้รับแจ้งจากสำนักงาน</p>	-ไม่มีการแก้ไข-	
<p>ข้อ 2 ขอบเขตในการตรวจประเมินต้องครอบคลุมระบบการให้บริการสำหรับบริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ยืนยันตัวตน บริการยืนยันตัวตน และบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งประกอบด้วย การปฏิบัติงาน กระบวนการทำงาน และระบบงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง</p>	-ไม่มีการแก้ไข-	

ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น	ร่างหลักเกณฑ์ฉบับปรับปรุง (ภายหลังรับฟังความคิดเห็น)	เหตุผลการปรับปรุง
<p>ข้อ 3 ผู้รับใบอนุญาตต้องดำเนินการประเมินความเสี่ยงให้สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงานตามรูปแบบที่สำนักงานกำหนด พร้อมจัดส่งผลการประเมินต่อสำนักงานภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน โดยผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินก่อนนำส่งต่อสำนักงาน</p>	<p>ข้อ 3 ผู้รับใบอนุญาตต้องดำเนินการประเมินความเสี่ยงให้สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงานตามรูปแบบที่สำนักงานกำหนด พร้อมจัดส่งผลการประเมินต่อสำนักงานภายใน <del>30</del> 60 วันนับแต่วันสิ้นปีปฏิทิน โดยผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินก่อนนำส่งต่อสำนักงาน</p>	<p>ปรับข้อความในหลักเกณฑ์เป็น "จัดส่งผลการประเมินต่อสำนักงานภายใน 60 วันนับแต่วันสิ้นปีปฏิทิน"</p> <p><u>เหตุผลการปรับปรุง</u></p> <ul style="list-style-type: none"><li>- การประเมินความเสี่ยงโดยอาศัยแบบประเมินประจำปีเพื่อระบุระดับความเสี่ยงของผู้ประกอบธุรกิจจำเป็นต้องรวบรวมข้อมูลจากการประกอบธุรกิจจนถึงวันสิ้นปีปฏิทินประกอบกับช่วงต้นเดือนมกราคมมีวันหยุดต่อเนื่องในเทศกาลปีใหม่ อีกทั้งกรณีเป็นองค์กรขนาดใหญ่อาจจะมีกระบวนการหลายขั้นตอนเพื่ออนุมัติผลการประเมินก่อนส่งออกภายนอกซึ่งอาจเป็นสาเหตุเป็นอุปสรรคต่อการส่งผลการประเมินภายใน 30 วันนับแต่วันสิ้นปีปฏิทินได้ จึงเสนอให้ปรับขยายกำหนดเวลาการส่งเป็น 45 วัน หรือ 60 วัน</li></ul>
<p>ข้อ 4 การตรวจประเมินตามข้อ 1.4 ต้องกำหนดแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง ให้ครอบคลุมส่วนที่มีการเปลี่ยนแปลงของระบบการให้บริการ</p>	<p>-ไม่มีการแก้ไข-</p>	
<p>ข้อ 5 การตรวจประเมินตามข้อ 1.1 1.2 และ 1.3 ต้องกำหนดแผนงานและดำเนินการตรวจประเมินให้สอดคล้องกับระดับความเสี่ยงการประกอบธุรกิจของผู้รับใบอนุญาต โดยมีรายละเอียด ดังนี้</p>	<p>-ไม่มีการแก้ไข-</p>	

ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น	ร่างหลักเกณฑ์ฉบับปรับปรุง (ภายหลังรับฟังความคิดเห็น)	เหตุผลการปรับปรุง
<p>5.1 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องกำหนดแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดให้ครอบคลุมข้อกำหนดทั้งหมดภายใต้หลักเกณฑ์ (full scope) แบบปีเว้นปี</p> <p>5.1.1 ปีที่เป็นการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) ต้องจัดทำแผนงานและดำเนินการตรวจประเมินให้ครบทุกข้อกำหนดภายใต้หลักเกณฑ์</p> <p>5.1.2 ปีที่ไม่ได้มีการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) สามารถจัดทำแผนงานและดำเนินการตรวจประเมินข้อกำหนดบางส่วนโดยพิจารณาตามความเสี่ยงและความเหมาะสม</p> <p>5.2 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลางหรือสูง ต้องจัดทำแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดให้ครบทุกข้อกำหนดภายใต้หลักเกณฑ์ (full scope) ทุกปี</p>	<p>-ไม่มีการแก้ไข-</p>	
<p>ข้อ 6 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการและรายงานผลการตรวจประเมินระบบ การให้บริการให้สอดคล้องกับหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ</p>	<p>-ไม่มีการแก้ไข-</p>	
<p>ข้อ 7 ผู้รับใบอนุญาตต้องรายงานผลการตรวจประเมินประจำปีตามรูปแบบที่สำนักงานกำหนด ภายใน 30 วัน นับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ แต่ไม่เกินวันที่ 31 มกราคมของปีถัดไป</p>	<p>ข้อ 7 ผู้รับใบอนุญาตต้องรายงานผลการตรวจประเมินประจำปีตามรูปแบบที่สำนักงานกำหนด ภายใน <b>30 60</b> วัน นับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ แต่ไม่เกินวันที่ <b>31 มกราคม 1 มีนาคม</b> ของปีถัดไป</p>	<p>ปรับข้อความในหลักเกณฑ์เป็น "รายงานผลการตรวจประเมินประจำปีตามรูปแบบที่สำนักงานกำหนด ภายใน 60 วันนับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ แต่ไม่เกินวันที่ 1 มีนาคมของปีถัดไป"</p>

ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น	ร่างหลักเกณฑ์ฉบับปรับปรุง (ภายหลังรับฟังความคิดเห็น)	เหตุผลการปรับปรุง
		<u>เหตุผลการปรับปรุง</u> - การส่งผลการตรวจประเมินประจำปีอาจปรับให้จำนวนวันสอดคล้องกับการส่งผลการประเมินความเสี่ยง คือ 45 วัน หรือ 60 วัน นับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ แต่ไม่เกินวันที่ 15 กุมภาพันธ์ หรือ 1 มีนาคมของปีถัดไป เพื่อป้องกันความสับสนของผู้ประกอบธุรกิจ - กรณีผู้ประกอบการที่เพิ่งได้รับใบอนุญาตสำนักงานอาจกำหนดเงื่อนไขที่ชัดเจนเกี่ยวกับช่วงเวลาที่ต้องเริ่มปฏิบัติตามข้อกำหนดในหลักเกณฑ์ฉบับนี้ไว้ในเอกสารฉบับอื่นไม่แนะนำให้เนื้อหาที่ไม่ได้บังคับใช้เป็นการทั่วไปมาระบุในหลักเกณฑ์การตรวจประเมินประจำปี
ข้อ 8 การรายงานผลการตรวจประเมินประจำปีต่อสำนักงาน ผู้รับใบอนุญาตสามารถรวบรวมผลจากหลายรอบการตรวจประเมินที่ดำเนินการภายในปีปฏิทินเดียวกัน โดยต้องจัดทำรายงานผลการตรวจประเมินประจำปีให้มีรายละเอียดครบถ้วนตามหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ และต้องจัดทำตารางเพื่อแสดงข้อกำหนดภายใต้หลักเกณฑ์และขอบเขตที่ตรวจประเมินในแต่ละรอบการตรวจ เพื่อให้มั่นใจว่าการตรวจประเมินในแต่ละปีครอบคลุมหลักเกณฑ์และระบบการให้บริการที่เกี่ยวข้อง	-ไม่มีการแก้ไข-	

ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น	ร่างหลักเกณฑ์ฉบับปรับปรุง (ภายหลังรับฟังความคิดเห็น)	เหตุผลการปรับปรุง
ข้อ 9 ผู้รับใบอนุญาตต้องจัดเก็บรายงานผลการตรวจประเมินไว้เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงาน เพื่อให้พร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดยสำนักงาน	-ไม่มีการแก้ไข-	
<b>ส่วนที่ 2 การพิจารณาความมีนัยสำคัญ</b>		
<p>ข้อ 10 ผู้รับใบอนุญาตต้องจัดให้มีข้อกำหนดในการพิจารณาความมีนัยสำคัญหรือความสำคัญที่ชัดเจน เพื่อให้พิจารณาดำเนินการในเรื่องต่าง ๆ โดยดำเนินการดังนี้</p> <p>10.1 ข้อกำหนดดังกล่าวต้องผ่านการพิจารณา ร่วมกันของหน่วยงานที่เกี่ยวข้อง รวมทั้งต้องได้รับ อนุมัติจากผู้บริหาร คณะกรรมการ หรือบุคลากรที่ ได้รับมอบหมาย</p> <p>10.2 ข้อกำหนดในการพิจารณาความมีนัยสำคัญ ต้องพิจารณาภายใต้กรอบหลักการที่คำนึงถึง ความเสี่ยงและผลกระทบต่อ การให้บริการของผู้รับ ใบอนุญาตในวงกว้าง เช่น กระทบลูกค้าหรือ ผู้ใช้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตน ทางดิจิทัลของผู้รับใบอนุญาต และคำนึงถึงผลกระทบต่อระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลใน วงกว้าง เช่น กระทบต่อระบบงานกลางที่มีนัยสำคัญ เชิงโครงสร้างต่อการให้บริการของระบบการพิสูจน์ และยืนยันตัวตนทางดิจิทัล</p>	-ตัดออก-	นำออกจากร่างหลักเกณฑ์ เนื่องจากเนื้อหา ไม่เกี่ยวข้องกับการตรวจประเมินประจำปี พร้อมรับข้อสังเกต นำไปกำหนดไว้ในหลักเกณฑ์ ฉบับอื่น

ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น	ร่างหลักเกณฑ์ฉบับปรับปรุง (ภายหลังรับฟังความคิดเห็น)	เหตุผลการปรับปรุง
10.3 ต้องทบทวนข้อกำหนดอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบต่อการใช้งาน		
ข้อ 11 ผู้รับใบอนุญาตต้องสื่อสารข้อกำหนดดังกล่าวให้แก่บุคลากรและบุคคลภายนอกที่เกี่ยวข้องทราบ และนำไปปฏิบัติ	<b>-ตัดออก-</b>	นำออกจากร่างหลักเกณฑ์ เนื่องจากเนื้อหาไม่เกี่ยวข้องกับการตรวจประเมินประจำปี พร้อมรับข้อสังเกต นำไปกำหนดไว้ในหลักเกณฑ์ฉบับอื่น
<b>ส่วนที่ 3 การแจ้งการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการใช้งาน</b>		
ข้อ 12 การแจ้งนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการใช้งาน 12.1 ผู้รับใบอนุญาตที่นำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยี โดยการนำมาใช้ หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนดที่ผู้รับใบอนุญาตได้กำหนดขึ้นตามข้อ 10 ทั้งกรณีที่ผู้รับใบอนุญาตดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้องแจ้งการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวต่อสำนักงานล่วงหน้าไม่น้อยกว่า 30 วันก่อนดำเนินการ ตามรูปแบบและวิธีที่สำนักงานกำหนด เว้นแต่สำนักงานมีคำสั่งให้ผู้รับใบอนุญาตไม่ต้องแจ้งการนำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบ หรือเทคโนโลยีที่มีนัยสำคัญ	<b>-ตัดออก-</b>	นำออกจากร่างหลักเกณฑ์ เนื่องจากเนื้อหาไม่เกี่ยวข้องกับการตรวจประเมินประจำปี พร้อมรับข้อสังเกต นำไปกำหนดไว้ในหลักเกณฑ์ฉบับอื่น