คำถาม-คำตอบ เกี่ยวกับประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ที่ ธพส. 1/2568
เรื่อง หลักเกณฑ์และระยะเวลาการตรวจประเมินประจำปีและจัดทำรายงานผลการตรวจประเมิน
ระบบการให้บริการสำหรับประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

วันที่ 27 กุมภาพันธ์ 2568

ข้อ	คำถาม	คำตอบ
การประเมินความเสี่ยง		
1.	การประเมินระดับความเสี่ยงขององค์กร (RLA) ต้องดำเนินการปีละกี่ครั้ง และต้องเริ่มดำเนินการ เมื่อใด	• ดำเนินการประเมินความเสี่ยงปีละ 1 ครั้ง โดยเมื่อได้ดำเนินการประเมินความเสี่ยงและนำส่งผลการประเมินต่อสำนักงานเรียบร้อยแล้ว ให้กำหนดแผนงานการตรวจประเมินที่สอดคล้องกับระดับความเสี่ยง พร้อมนำส่งรายงานผลการตรวจประเมินประจำปีภายในเวลาที่กำหนด
2.	บุคคลหรือส่วนงานใดเป็นผู้รับผิดชอบการประเมินความเสี่ยงขององค์กร	• ผู้รับผิดชอบการประเมินความเสี่ยงขององค์กรเป็นไปตามการมอบหมายหรือตามโครงสร้างของแต่ละองค์กร
3.	ผลการประเมินความเสี่ยงต้องผ่านการอนุมัติโดยผู้บริหารสูงสุดทุกกรณีหรือไม่	• ผลการประเมินความเสี่ยงที่จะนำส่งสำนักงาน ต้องผ่านการรายงานหรือมีการอนุมัติผลการประเมินจากผู้บริหารระดับสูง คณะกรรมการหรือบุคลากรที่ได้รับมอบหมายให้รับผิดชอบ เพื่อให้มั่นใจว่าหน่วยงานได้รับทราบและตระหนักถึงความเสี่ยงในเรื่องดังกล่าว เช่น ผู้บริหารสูงสุดมอบหมายให้หัวหน้าทีมประเมินความเสี่ยงเป็นผู้พิจารณาอนุมัติผลการประเมินความเสี่ยงก่อนนำส่งหน่วยงานภายนอก หากได้รับการอนุมัติจากบุคคลดังกล่าว สามารถนำส่งผลได้โดยไม่จำเป็นต้องรอให้ผ่านการรายงานต่อผู้บริหารสูงสุด
4.	กรณีเป็นผู้รับใบอนุญาตที่ประกอบธุรกิจบริการครบทั้ง 4 ประเภท ต้องดำเนินการทำแบบประเมินความเสี่ยงอย่างไร	• เพื่อให้การประเมินความเสี่ยงสะท้อนให้เห็นถึงความเสี่ยงของลักษณะธุรกิจบริการได้อย่างแท้จริง สำนักงานจึงได้จัดทำแบบประเมินความเสี่ยงประจำปีแยกเป็น 2 ชุดเอกสาร ตามลักษณะธุรกิจบริการ ดังนี้ 1) แบบประเมินความเสี่ยงประจำปีสำหรับผู้ประกอบธุรกิจบริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ยืนยันตัวตน บริการยืนยันตัวตน 2) แบบประเมินความเสี่ยงประจำปีสำหรับผู้ประกอบธุรกิจบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ดังนั้น สำหรับผู้รับใบอนุญาตที่ประกอบธุรกิจครบทั้ง 4 ลักษณะบริการ จึงต้องจัดทำแบบประเมินความเสี่ยงประจำปีทั้ง 2 ชุดเอกสารข้างต้น

ข้อ	คำถาม	คำตอบ
การตรวจประเมิน		
4.	ขอทราบคุณสมบัติของผู้ตรวจสอบ	• ผู้ตรวจสอบที่จะทำการตรวจประเมินระบบให้บริการต้องเป็นผู้มีคุณสมบัติตามที่กำหนดไว้ใน ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 5 หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ ข้อ 22 • ทั้งนี้ การตรวจประเมินระบบการให้บริการสามารถดำเนินการโดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอก ก็ได้
5.	ขอทราบรอบการกำหนดแผนการตรวจประเมินและการนำส่งผลการตรวจประเมิน	• สำหรับการตรวจประเมินระบบการให้บริการในปี 2567 เนื่องจากยังไม่มีการประกาศหลักเกณฑ์ลำดับรองเกี่ยวกับการตรวจประเมินประจำปี ผู้รับใบอนุญาตจึงมีหน้าที่ในการตรวจสอบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการอย่างน้อยปีละหนึ่งครั้ง ตามข้อ 39 ของข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 3 โดยสามารถใช้แบบรายงานผลการตรวจประเมินระบบการให้บริการสำหรับการตรวจประเมิน ตามแบบฟอร์ม : แบบรายงานผลการตรวจประเมินระบบการให้บริการ (สำหรับ IT Security ปี 2567) ซึ่งเผยแพร่ตาม link : https://bit.ly/4321mRU โดยยังไม่ต้องนำส่งผลการประเมินมายังสำนักงาน • สำหรับการดำเนินการตั้งแต่ปี 2568 ให้ปฏิบัติตามประกาศฉบับนี้ โดยมีรอบการดำเนินการดังนี้ (1) ปี 2568 ให้ประเมินระดับความเสี่ยงตามแบบประเมินความเสี่ยงประจำปี และนำส่งผลการประเมินต่อสำนักงาน ภายในวันที่ 30 มิถุนายน 2568 (2) ภายในปี 2568 ต้องกำหนดแผนงานการตรวจประเมิน และดำเนินการตรวจประเมินระบบการให้บริการให้แล้วเสร็จภายในวันที่ 31 ธันวาคม 2568 และนำส่งรายงานผลการตรวจประเมินต่อสำนักงาน ภายในวันที่ 31 มีนาคม 2569 (3) ปี 2569 เป็นต้นไป ให้ประเมินระดับความเสี่ยงตามแบบประเมินความเสี่ยงประจำปี และนำส่งผลการประเมินต่อสำนักงาน ภายในวันที่ 31 มีนาคม ของปีนั้น และต้องกำหนดแผนงานการตรวจประเมินและดำเนินการตรวจประเมินระบบการให้บริการให้แล้วเสร็จภายในวันที่ 31 ธันวาคม ของปีนั้น และนำส่งรายงานผลการตรวจประเมินต่อสำนักงาน ภายในวันที่ 31 มีนาคมปีถัดไป

<table>
<tr><th>ข้อ</th><th>คำถาม</th><th>คำตอบ</th></tr>
<tr><td></td><td></td><td>ตัวอย่างรอบการนำส่งข้อมูล
<table>
<tr><th>ปี พ.ศ.</th><th>ผลการประเมิน
ความเสี่ยง</th><th>รายงาน
ผลการตรวจประเมิน</th></tr>
<tr><td>2568</td><td>ภายใน 30 มิถุนายน 2568</td><td>ภายใน 31 มีนาคม 2569</td></tr>
<tr><td>2569</td><td>ภายใน 31 มีนาคม 2569</td><td>ภายใน 31 มีนาคม 2570</td></tr>
<tr><td>2570</td><td>ภายใน 31 มีนาคม 2570</td><td>ภายใน 31 มีนาคม 2571</td></tr>
</table></td></tr>
<tr><td>6.</td><td>กรณีที่ผลการประเมินความเสี่ยงอยู่ในระดับต่ำ
(1) การตรวจประเมินเฉพาะบางข้อกำหนด มีการกำหนดหัวข้อขั้นต่ำหรือไม่
(2) หากผลการประเมินความเสี่ยงของปีถัดไปอยู่ในระดับต่ำเช่นเดียวกัน จะต้องดำเนินการตรวจประเมินอย่างไร</td><td>

กรณีตรวจประเมินเฉพาะบางข้อกำหนด สำนักงานจะไม่ได้กำหนดหัวข้อขั้นต่ำที่ต้องดำเนินการ โดยเปิดให้หน่วยงานสามารถพิจารณาเลือกข้อกำหนดในการตรวจประเมินตามระดับความเสี่ยงที่เหมาะสมกับหน่วยงานนั้นได้
ทั้งนี้ หน่วยงานควรให้ความสำคัญกับการตรวจติดตามผลในรอบปีที่ผ่านมาว่ามี Not Pass หรือ Partially Pass ซึ่งควรจะต้องมีการตรวจติดตามประเด็นนั้นๆ ในปีถัดไป
ตามข้อกำหนดกรณีผลการประเมินอยู่ในความเสี่ยงระดับต่ำที่ให้กำหนดแผนงานและดำเนินการตรวจประเมินระบบการให้บริการครอบคลุมข้อกำหนดทั้งหมดแบบปีเว้นปีนั้น แสดงให้เห็นได้ว่าผู้ประกอบการทุกรายจะต้องจัดให้มีการตรวจประเมินแบบครอบคลุมข้อกำหนดทั้งหมดอย่างน้อยทุก 2 ปี ตัวอย่างเช่น ในปี 2568 ผลการประเมินความเสี่ยงอยู่ในระดับต่ำ จึงตรวจประเมินเฉพาะบางข้อกำหนดครอบคลุมตามหัวข้อหลักเกณฑ์ทั้งหมด ในปี 2569 ผลการประเมินความเสี่ยงอยู่ในระดับต่ำ แต่เนื่องจากในปี 2568 ตรวจประเมินเฉพาะบางข้อกำหนดแล้ว ดังนั้น ในปี 2569 จึงต้องตรวจประเมินแบบครอบคลุมข้อกำหนดทั้งหมด

ตัวอย่างที่ 1 รอบการกำหนดแผนการตรวจประเมิน
<table>
<tr><th>ปี พ.ศ.</th><th>ผลการประเมิน
ความเสี่ยง</th><th>ข้อกำหนดในการตรวจประเมิน</th></tr>
<tr><td>2568</td><td>ระดับต่ำ</td><td>ตรวจประเมินเฉพาะบางข้อกำหนด</td></tr>
<tr><td>2569</td><td>ระดับต่ำ</td><td>ตรวจประเมินแบบครอบคลุม
ข้อกำหนดทั้งหมด</td></tr>
<tr><td>2570</td><td>ระดับปานกลาง</td><td>ตรวจประเมินแบบครอบคลุม
ข้อกำหนดทั้งหมด</td></tr>
<tr><td>2571</td><td>ระดับต่ำ</td><td>ตรวจประเมินเฉพาะบางข้อกำหนด</td></tr>
<tr><td>2572</td><td>ระดับต่ำ</td><td>ตรวจประเมินแบบครอบคลุม
ข้อกำหนดทั้งหมด</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>ข้อ</th><th>คำถาม</th><th>คำตอบ</th></tr>
<tr><td></td><td></td><td>ตัวอย่างที่ 2 รอบการกำหนดแผนการตรวจประเมิน
<table>
<tr><th>ปี พ.ศ.</th><th>ผลการประเมินความเสี่ยง</th><th>ข้อกำหนดในการตรวจประเมิน</th></tr>
<tr><td>2568</td><td>ระดับต่ำ</td><td>ตรวจประเมินแบบครอบคลุมข้อกำหนดทั้งหมด</td></tr>
<tr><td>2569</td><td>ระดับต่ำ</td><td>ตรวจประเมินเฉพาะบางข้อกำหนด</td></tr>
<tr><td>2570</td><td>ระดับต่ำ</td><td>ตรวจประเมินแบบครอบคลุมข้อกำหนดทั้งหมด</td></tr>
<tr><td>2571</td><td>ระดับปานกลาง</td><td>ตรวจประเมินแบบครอบคลุมข้อกำหนดทั้งหมด</td></tr>
<tr><td>2572</td><td>ระดับต่ำ</td><td>ตรวจประเมินเฉพาะบางข้อกำหนด</td></tr>
</table></td></tr>
<tr><td colspan="3">ผลการตรวจประเมิน</td></tr>
<tr><td>7.</td><td>สามารถรวบรวมผลการตรวจประเมินจากหลายรอบ หรือการตรวจประเมินที่ดำเนินการภายในปีปฏิทินเดียวกันได้หรือไม่</td><td>• หน่วยงานสามารถดำเนินการประเมินคราวเดียวพร้อมกัน หรือพิจารณาแยกขอบเขตการประเมิน และใช้ผลการตรวจประเมินในขอบเขตที่เกี่ยวข้องภายในรอบปีการประเมินเดียวกัน หรืออ้างอิงผลการตรวจประเมินจากหน่วยงานอื่น รวบรวมนำส่งได้ แต่ต้องเป็นการประเมินที่ครอบคลุมขอบเขตการให้บริการที่ได้รับใบอนุญาต โดยกรณีอ้างอิงผลการตรวจประเมินจากหน่วยงานอื่นสามารถใช้ผลย้อนหลังได้ไม่เกิน 1 ปี</td></tr>
<tr><td colspan="3">คำถามเพิ่มเติม</td></tr>
<tr><td>8.</td><td>เหตุใดจึงต้องกำหนดวันที่และเวลาที่ได้รับข้อมูล</td><td>• ตามหลักเกณฑ์ข้อ 5 ที่กำหนดวันและเวลาที่สำนักงานได้รับข้อมูลนั้น เป็นการกำหนดให้สอดคล้องกับมาตรา 10 แห่ง พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 เพื่อให้มีความชัดเจนในเรื่องการรับส่งข้อมูลระหว่างสำนักงานกับผู้นำส่งข้อมูล
• ทั้งนี้ สำนักงานกำหนดวันและเวลาทำการ จันทร์ - ศุกร์ เวลา 08:30 -17:30 น.</td></tr>
</table>