ตารางสรุปความคิดเห็นต่อ (ร่าง) ประกาศ สพธอ. ที่ ธพส. ..../2568
เรื่อง การตรวจประเมินประจำปีและการจัดทำรายงานผลการตรวจประเมินธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
เปิดรับฟังความเห็นเพิ่มเติม (ครั้งที่ 2) ระหว่างวันที่ 28 มกราคม – 3 กุมภาพันธ์ 2568

(ร่าง) ประกาศ สพธอ. ฉบับรับฟังความคิดเห็นเพิ่มเติม (ครั้งที่ 2)	ความคิดเห็น/ข้อเสนอแนะ
ข้อ 1 ในประกาศนี้ “ผู้รับใบอนุญาต” หมายความว่า บุคคลที่ได้รับใบอนุญาตให้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต “ระบบการให้บริการ” หมายความว่า ระบบและเทคโนโลยีที่ใช้สำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีลักษณะเป็นบริการที่ต้องได้รับใบอนุญาต และหมายรวมถึงระบบงานที่เกี่ยวข้องกับการประกอบธุรกิจบริการดังกล่าวด้วย “หลักเกณฑ์” หมายความว่า ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่ ธพส. 1/2566 เรื่อง หลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต “พระราชกฤษฎีกา” หมายความว่า พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565 “สำนักงาน” หมายความว่า สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์	**- ไม่มีความเห็นเพิ่มเติม -**

(ร่าง) ประกาศ สพธอ. ฉบับรับฟังความคิดเห็นเพิ่มเติม (ครั้งที่ 2)	ความคิดเห็น/ข้อเสนอแนะ
ข้อ 2 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการตามหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต อย่างน้อยปีละ 1 ครั้ง ประกอบด้วยหลักเกณฑ์ในเรื่องต่อไปนี้ (1) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ (2) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ (3) หลักเกณฑ์ตามลักษณะของการให้บริการ การกำหนดขอบเขตในการตรวจประเมินระบบให้บริการที่ได้รับใบอนุญาตตามวรรคหนึ่ง ต้องครอบคลุมการปฏิบัติงาน กระบวนการทำงานและระบบงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเพียงพอ ทั้งนี้ ผู้รับใบอนุญาตต้องดำเนินการให้สอดคล้องตามหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ ในส่วนที่เกี่ยวกับการตรวจประเมินระบบการให้บริการ	ในส่วนของบริบท ไม่มีแก้ไข ในส่วนของการปฏิบัติ เสนอให้สำนักงานฯ มี Template ในการตรวจประเมินประกอบกับแนวทางในการตรวจประเมิน โดยมี Reference ที่มาของเกณฑ์ต่าง ๆ เช่น ในอนุมาตรา (1) เรื่อง IT Security ว่าอ้างอิงมาจากเกณฑ์ใด ตัวอย่างเช่น NIST หรือ ISO ข้อใด เล่มใด เป็นต้น เนื่องจากในกรณีที่บริษัทฯ มีผลการประเมินที่ผ่านเกณฑ์เดียวกัน สามารถใช้เป็นผลอ้างอิงในการประเมินกับสำนักงานฯ ได้ เพื่อลดความซ้ำซ้อนในการทำงาน 3 หลักเกณฑ์ที่กล่าวถึงมีรายละเอียดอ้างอิงในเอกสารใดหรือประกาศใดหรือไม่ หากไม่มีทางสำนักงานจะมีการออกรายละเอียด เช่น เพิ่มเติมในเกณฑ์หรือออกเป็น Q&A มาให้ผู้ประกอบธุรกิจใช้อ้างอิงหรือไม่
ข้อ 3 การตรวจประเมินระบบการให้บริการตามข้อ 2 ให้ผู้รับใบอนุญาตกำหนดแผนงานการตรวจประเมินให้สอดคล้องตามระดับความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยให้ผู้รับใบอนุญาตดำเนินการประเมินความเสี่ยงตามแบบประเมินความเสี่ยงประจำปีที่สำนักงานประกาศ	โปรดระบุคำนิยามผู้บริหารระดับสูง เช่น ผู้บริหารระดับสูงในฝั่ง Business หรือ Compliance และคณะกรรมการหรือบุคลากรที่ได้รับมอบหมาย หมายถึงคณะกรรมการใด มีคุณสมบัติอย่างไร

(ร่าง) ประกาศ สพธอ. ฉบับรับฟังความคิดเห็นเพิ่มเติม (ครั้งที่ 2)	ความคิดเห็น/ข้อเสนอแนะ
ผลการประเมินระดับความเสี่ยงตามวรรคหนึ่ง ต้องผ่านการพิจารณาจากผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายของผู้ประกอบธุรกิจให้รับผิดชอบในเรื่องดังกล่าว	
ข้อ 4 ในการกำหนดแผนงานการตรวจประเมิน ให้ผู้รับใบอนุญาตพิจารณาตามระดับความเสี่ยงดังนี้ (1) กรณีผลการประเมินอยู่ในความเสี่ยงระดับต่ำ ให้กำหนดแผนงานและดำเนินการตรวจประเมินระบบการให้บริการครอบคลุมข้อกำหนดทั้งหมดภายใต้หลักเกณฑ์ตามข้อ 2 แบบปีเว้นปี โดยปีที่ไม่ได้มีการตรวจประเมินครอบคลุมข้อกำหนดทั้งหมด ให้มีการตรวจประเมินเฉพาะบางข้อกำหนดแต่ต้องครบตามหลักเกณฑ์ในข้อ 2 (2) กรณีผลการประเมินอยู่ในความเสี่ยงระดับปานกลางหรือสูง ให้กำหนดแผนงานและดำเนินการตรวจประเมินระบบการให้บริการครอบคลุมข้อกำหนดทั้งหมดภายใต้หลักเกณฑ์ตามข้อ 2 ทุกปี	(1) ประเมินทุก 3 ปี (Full scope) (2) ประเมินทุกปี "ข้อ 4 (1) ในกรณีมีผลการประเมินความเสี่ยงในระดับต่ำนั้น ปีที่ไม่ได้มีการตรวจประเมิน ให้ตรวจประเมินเฉพาะบางข้อกำหนดแต่ต้องครบตามข้อ 2" จากข้อความข้างต้นนั้น หมายถึงหน่วยงานกำกับฯ จะมีการกำหนดหลักเกณฑ์แยกออกมาในปีที่เป็น Partial ใช่หรือไม่ แล้วมีการตรวจประเมินในประเด็นไหน ควรอธิบายออกมาโดยละเอียด แยกตามระดับความเสี่ยงระบุในเอกสาร เพื่อไม่ให้เกิดความสับสนของผู้ตรวจประเมิน เนื่องจากตารางที่แนบในเอกสารมาด้วยนั้น หลังจากที่ทำการกรอกฟอร์มแล้วไม่เกิดการเปลี่ยนแปลงเกิดขึ้น 1. ขอให้ทางสำนักงานอธิบายกรอบการตรวจประเมิน Partial Scope / Full Scope เพิ่มเติม เช่น กรณีที่ปี 2567 ธนาคารมีการตรวจประเมินเป็น Full Scope ไปแล้ว ทั้งนี้ หากธนาคารประเมิน RLA ปี 2568 ได้ผลเป็นความเสี่ยงต่ำ จะสามารถทำการตรวจประเมินในปี 2568 (ปีแรกสำหรับประกาศฉบับใหม่) เป็นแบบ Partial Scope ได้หรือไม่ 2. สำหรับกรณีข้อย่อย (1) นั้น การตรวจประเมินเฉพาะบางข้อ จะทราบได้อย่างไรว่าต้องเป็นข้อใดบ้าง

(ร่าง) ประกาศ สพธอ. ฉบับรับฟังความคิดเห็นเพิ่มเติม (ครั้งที่ 2)	ความคิดเห็น/ข้อเสนอแนะ
ข้อ 5 ให้ผู้รับใบอนุญาตจัดส่งผลการประเมินความเสี่ยงประจำปี และรายงานผลการตรวจประเมินระบบการให้บริการต่อสำนักงานภายในวันที่ 31 มีนาคม ของปีถัดไป โดยวิธีการทางอิเล็กทรอนิกส์ตามช่องทางที่สำนักงานกำหนด โดยถือว่าสำนักงานได้รับตามวันและเวลาที่ข้อมูลได้เข้าสู่ระบบอิเล็กทรอนิกส์ของสำนักงาน ทั้งนี้ หากเป็นการนำส่งนอกวันและเวลาทำการของสำนักงาน ถือว่าสำนักงานได้รับข้อมูลดังกล่าวในวันและเวลาทำการถัดไป	ต้องผ่าน AC Audit committee ก่อนหรือไม่ และกรณีของ SFIs ต้องดำเนินการส่งรายงานผ่านช่องทางใด 1. ถ้านำส่งพร้อมกันทั้งผลการประเมินความเสี่ยงประจำปีและรายงานการตรวจประเมินระบบ แสดงว่ามีบางปีที่จะส่งแค่ผลประเมินความเสี่ยงและแนบรายงานตรวจประเมินระบบแบบบางข้อตามข้อ 4 ข้อย่อย (1) ข้างต้น หากผลประเมินความเสี่ยงอยู่ในระดับต่ำในปีก่อนหน้า เข้าใจถูกหรือไม่ 2. หากในปีก่อนหน้าประเมินความเสี่ยงประจำปีอยู่ในระดับต่ำ แต่ในปีต่อมาประเมินเพิ่มขึ้นเป็นระดับกลางจะต้องนำส่งรายงานการประเมินระบบแบบใด 3. สำนักงานกำหนดส่งทั้ง 2 รายงานภายในวันที่ 31 มีนาคม ของทุกปีนั้น จะเป็นการนำส่งผลประเมิน RLA ประจำปีดังกล่าว และผลการประเมินระบบบริการของปีก่อนหน้า (ซึ่งยึดแนวทางการตรวจว่าเป็น Partial/Full scope จากผลประเมินความเสี่ยง RLA ที่นำส่งในปีก่อนหน้า) ใช่หรือไม่ รบกวนทางสำนักงานระบุข้อความเพื่อความชัดเจนในส่วนนี้เพิ่มเติมในเกณฑ์ หรือออกเป็นคำอธิบาย/Q&A ให้ด้วย 4. ทางสำนักงานจะแจ้งช่องทางอิเล็กทรอนิกส์สำหรับนำส่งแบบประเมินความเสี่ยงอีกครั้งใช่หรือไม่ หรือมีการแจ้งอยู่แล้วในเกณฑ์ใด ไม่ควรมีข้อความ “ทั้งนี้ หากเป็นการนำส่งนอกวันและเวลาทำการของสำนักงาน ถือว่าสำนักงานได้รับข้อมูลดังกล่าวในวันและเวลาทำการถัดไป” เนื่องจากทำให้กำหนดส่งของแต่ละปีแตกต่างกันออกไป เป็นภาระของผู้ประกอบธุรกิจฯ และอาจจะทำให้ปฏิบัติผิดเกณฑ์แม้ส่งภายในวันที่ 31 มีนาคมก็ตาม

(ร่าง) ประกาศ สพธอ. ฉบับรับฟังความคิดเห็นเพิ่มเติม (ครั้งที่ 2)	ความคิดเห็น/ข้อเสนอแนะ
	(เมื่อเทียบกับการกำหนดให้ส่งรายงานลักษณะเดียวกันจากสำนักงาน ก.ล.ต. ก็ไม่ได้มีการกำหนดโดยมีข้อความลักษณะนี้)
ข้อ 6 ในการตรวจประเมินระบบการให้บริการตามข้อ 2 และการประเมินระดับความเสี่ยงตามที่กำหนดในข้อ 3 สำหรับปี พ.ศ. 2568 ให้ผู้รับใบอนุญาตดำเนินการดังต่อไปนี้ (1) ดำเนินการประเมินและจัดส่งผลการประเมินระดับความเสี่ยงต่อสำนักงาน ภายในวันที่ 30 เมษายน 2568 (2) กำหนดแผนงานการตรวจประเมินและดำเนินการตรวจประเมินระบบการให้บริการ ภายในปี 2568 และนำส่งรายงานผลการตรวจประเมินต่อสำนักงาน ภายในวันที่ 31 มีนาคม 2569	ข้อ 6 (1) ที่จะต้องดำเนินการจัดส่งผลการประเมินระดับความเสี่ยงต่อสำนักงานภายในวันที่ 30 เมษายน 68 นั้น เนื่องด้วยระยะเวลาสำหรับปี 2568 นี้ มีระยะเวลาที่จำกัดไปหรือไม่ ควรขยายเวลาเพิ่มเติม 1. กรอบระยะเวลาการจัดส่งแบบประเมินความเสี่ยงภายใน 30 เมษายน 2568 ค่อนข้างกระชั้น เนื่องจากระยะเวลาหลังจากเกณฑ์นี้จะประกาศใช้ไปจนถึงกำหนดส่งเพียงสองเดือนกว่า ซึ่งธนาคารต้องจัดทำและรวบรวมผลการประเมิน รวมถึงเสนอต่อผู้มีอำนาจในการรับทราบและรับรองผล รวมถึงเดือนเมษายนมีวันหยุดค่อนข้างเยอะ ทางสำนักงานมีความเป็นไปได้ที่จะขยายช่วงเวลาเป็นภายในไตรมาส 2 ปี 2568 สำหรับครั้งแรกได้หรือไม่ 2. อ้างอิงจากเกณฑ์ที่เขียน หมายความว่า RLA ประจำปี 2568 จะส่งในวันที่ 30 เมษายน 2568 และผลประเมินระบบบริการประจำปี 2568 จะส่งในวันที่ 31 มีนาคม 2569 ถูกต้องหรือไม่ เช่นนี้ ผลประเมินระบบบริการจะเป็นลักษณะการส่งผลของปีก่อนหน้าตลอดไปใช่ไหมค รบกวนทางสำนักงานระบุข้อความเพื่อความชัดเจนในส่วนนี้เพิ่มเติมในเกณฑ์ หรือออกเป็นคำอธิบาย/Q&A ให้ด้วย
ข้อ 7 ประกาศฉบับนี้ให้ใช้บังคับกับผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตซึ่งได้ประกอบธุรกิจบริการอยู่ในวันก่อนวันที่พระราชกฤษฎีกาใช้บังคับ ซึ่งอยู่ระหว่างการพิจารณาดำเนินการออกใบอนุญาตด้วย	กรณีผู้ประกอบธุรกิจอยู่ระหว่างดำเนินการขอรับใบอนุญาต และ/หรืออยู่ระหว่างที่ สพธอ. พิจารณาใบอนุญาต ควรมีวิธีและกระบวนการตรวจสอบคุณสมบัติในลักษณะเดียวกันกับผู้ประกอบธุรกิจที่ได้รับใบอนุญาตแล้วหรือไม่
ข้อ 8 ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ .... เป็นต้นไป	**- ไม่มีความเห็นเพิ่มเติม -**

(ร่าง) ประกาศ สพธอ. ฉบับรับฟังความคิดเห็นเพิ่มเติม (ครั้งที่ 2)	ความคิดเห็น/ข้อเสนอแนะ
ข้อเสนอแนะอื่น ๆ เพิ่มเติม	อยากให้สำนักงานฯ ดำเนินการพิจารณาเรื่องของระยะเวลาในการส่งผลการประเมินเพิ่มเติม เช่น หากหน่วยงานได้รับใบอนุญาตเมื่อเดือนธันวาคม จะต้องส่งผลการประเมินเพื่อให้ทันเดือนธันวาคมด้วยหรือไม่ เพื่อให้ทันรอบการต่อใบอนุญาต ธนาคารมีข้อสอบถามเพิ่มเติมเกี่ยวกับ (ร่าง) แบบประเมินประจำปีเพื่อระบุระดับความเสี่ยงของผู้ประกอบธุรกิจ และ (ร่าง) รายงานผลตรวจประเมินประจำปี รายละเอียดตามไฟล์แนบ CIMBT_ข้อสอบถามเพิ่มเติม

รายชื่อบริษัทที่ร่วมแสดงความคิดเห็น

1. บริษัท เอสซีบี เทคเอกซ์ จำกัด
2. ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน)
3. ธนาคารออมสิน
4. บริษัท เนชั่นแนลดิจิทัลไอดี จำกัด
5. ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน)
6. ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
7. ธนาคารกรุงไทย จำกัด (มหาชน)
8. บริษัท ดิจิทัล แอคเซส แพลตฟอร์ม จำกัด