ภาคผนวก ก

คำถามและรายละเอียดสำหรับ
การประเมินตนเอง (Self-assessment)

ส่วนที่ 1
คำถามทั่วไป

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
1	Strategic	นโยบาย/ แผนกลยุทธ์ และการจัดสรรงบประมาณสอดคล้องกับเป้าหมายเชิงกลยุทธ์ทางธุรกิจ โดยเฉพาะอย่างยิ่งเพื่อสนับสนุนการให้บริการ Digital ID อย่างปลอดภัย	มีนโยบาย/แผนกลยุทธ์ และการจัดสรรงบประมาณสอดคล้องกับเป้าเชิงกลยุทธ์ทางธุรกิจในระยะยาว (5 ปีขึ้นไป)	มีนโยบาย/แผนกลยุทธ์ และการจัดสรรงบประมาณสอดคล้องกับเป้าเชิงกลยุทธ์ทางธุรกิจในระยะสั้น (น้อยกว่า 5 ปี)	มีนโยบาย/แผนกลยุทธ์ และการจัดสรรงบประมาณแต่ยังไม่สอดคล้องกับเป้าเชิงกลยุทธ์ทางธุรกิจ หรือไม่มีนโยบาย/แผนกลยุทธ์และการจัดสรรงบประมาณเพื่อสนับสนุนการให้บริการ Digital ID อย่างปลอดภัย	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - เป้าเชิงกลยุทธ์ทางธุรกิจ (ครอบคลุมหรือสำหรับ บริการ Digital ID) - นโยบาย/แผนกลยุทธ์ทางธุรกิจ (ครอบคลุมหรือสำหรับ บริการ Digital ID) - การจัดสรรงบประมาณ (ครอบคลุมหรือสำหรับ บริการ Digital ID)	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
2	Strategic	อิทธิพลจากบริษัทใหญ่ (parent company) รวมถึงผู้ถือหุ้นที่เป็นชาวต่างชาติในการกำหนดกลยุทธ์	องค์กรมีคุณสมบัติ ดังนี้ (1) ไม่เป็นบริษัทย่อยหรือสาขาของบริษัทใหญ่ (parent company) และ (2) ไม่มีผู้ถือหุ้นที่เป็นชาวต่างชาติมากกว่าร้อยละ 50 ของจำนวนหุ้นของบริษัท และ (3) ไม่มีผู้ถือหุ้นที่เป็นชาวต่างชาติที่มีอำนาจควบคุมคะแนนเสียงส่วนใหญ่ในที่ประชุมผู้ถือหุ้นของบริษัท และ (4) ไม่มีผู้ถือหุ้นที่เป็นชาวต่างชาติที่มีอำนาจควบคุม	องค์กรมีคุณสมบัติ ดังนี้ (1) เป็นบริษัทย่อยหรือสาขาของบริษัทใหญ่ (parent company) หรือ (2) มีผู้ถือหุ้นที่เป็นชาวต่างชาติมากกว่าร้อยละ 50 ของจำนวนหุ้นของบริษัท หรือ (3) มีผู้ถือหุ้นที่เป็นชาวต่างชาติที่มีอำนาจควบคุมคะแนนเสียงส่วนใหญ่ในที่ประชุมผู้ถือหุ้นของบริษัท หรือ (4) มีผู้ถือหุ้นที่เป็นชาวต่างชาติที่มีอำนาจควบคุม	N/A	ALL (IDP, DPIS)	สำหรับ (1), (2), (3) และ (4) - สำเนาบัญชีรายชื่อผู้ถือหุ้น (แบบ บอจ.5) และสมุดทะเบียนผู้ถือหุ้นของบริษัทจำกัด หรือ - บัญชีรายชื่อผู้ถือหุ้นของบริษัทมหาชนจำกัด (แบบ บมจ.006) สำหรับข้อ (3) และ (4) - สำเนาข้อบังคับของบริษัท	บริษัทใหญ่ บริษัทย่อย (Parent, Subsidiary) หมายถึง บริษัทจำกัด (Incorporated enterprise) ที่มีอำนาจในการตัดสินใจ และถือครองหุ้นมากกว่าร้อยละ 50 ของจำนวนหุ้นสามัญ (Ordinary share) หรือหุ้นที่ให้สิทธิออกเสียง (Voting stock) ตัวอย่าง บริษัท A เป็นบริษัทใหญ่ของบริษัท B และ C หรือ บริษัท B และ C เป็นบริษัทย่อยของบริษัท A เพราะ : a) บริษัท A ถือครองหุ้นร้อยละ 90 ในบริษัท B หรือ b) บริษัท B ถือครองหุ้นร้อยละ 100 ในบริษัท C ดังนั้น บริษัท C จึงเป็นบริษัทย่อยของบริษัท A ด้วย สาขา (Branch) หมายถึงธุรกิจ (Unincorporated enterprise) ที่บริษัทของท่านถือครองหุ้นทั้งหมด หรือส่วนใหญ่ โดยบริษัทหรือผู้ลงทุน 1 ราย ตัวอย่าง บริษัท C เป็นสาขาของบริษัท B เพราะ บริษัท B ถือครองหุ้นร้อยละ 100 ในบริษัท C อ้างอิง แบบสำรวจ 46 : ข้อมูล

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
			การแต่งตั้งหรือถอดถอนผู้มีอำนาจในการจัดการหรือกรรมการตั้งแต่กึ่งหนึ่งของกรรมการทั้งหมดในบริษัท	การแต่งตั้งหรือถอดถอนผู้มีอำนาจในการจัดการหรือกรรมการตั้งแต่กึ่งหนึ่งของกรรมการทั้งหมดในบริษัท				ฐานะการลงทุนระหว่างประเทศของธนาคารแห่งประเทศไทย

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
3	Strategic	การบริหารความเสี่ยงในระดับองค์กร	มีนโยบายการบริหารความเสี่ยงในระดับองค์กร และ กิจกรรมการบริหารความเสี่ยงในระดับองค์กรที่สอดคล้องกับนโยบาย และมีการรายงานต่อผู้บริหารระดับสูงหรือคณะกรรมการบริษัทอย่างสม่ำเสมอ	ไม่มีนโยบายการบริหารความเสี่ยงในระดับองค์กร แต่มีกิจกรรมการบริหารความเสี่ยงในระดับองค์กรและมีการรายงานต่อผู้บริหารระดับสูงหรือคณะกรรมการบริษัท	ไม่มีกิจกรรมการบริหารความเสี่ยงในระดับองค์กร หรือ ผู้บริหารระดับสูงไม่ได้มีส่วนร่วม	ALL (IDP, DPIS)	- นโยบายการบริหารความเสี่ยงในระดับองค์กร - รายงานผลการประเมินและการบริหารความเสี่ยงในระดับองค์กร ครั้งล่าสุด (ภายในระยะเวลา 1 ปี)	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
4	Strategic, Operational, Technology, Reputation	การควบรวมกิจการเข้าซื้อกิจการ หรือแผนการลดค่าใช้จ่าย ที่อาจส่งผลกระทบต่อบุคลากร กระบวนการ หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับบริการ Digital ID	ไม่มีแผนการควบรวมกิจการเข้าซื้อกิจการหรือแผนการลดค่าใช้จ่าย ที่มีผลกระทบต่อบุคลากร กระบวนการ หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับบริการ Digital ID	มีแผนหรืออยู่ระหว่างดำเนินการควบรวมกิจการเข้าซื้อกิจการหรือแผนการลดค่าใช้จ่าย ที่มีผลกระทบเพียงเล็กน้อยต่อบุคลากร กระบวนการ หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับบริการ Digital ID	มีแผนหรืออยู่ระหว่างดำเนินการเพื่อการควบรวมกิจการเข้าซื้อกิจการหรือแผนการลดค่าใช้จ่าย ที่มีผลกระทบระดับปานกลางถึงมาก หรือยังไม่ได้วิเคราะห์ถึงผลกระทบต่อบุคลากร กระบวนการ หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับบริการ Digital ID	ALL (IDP, DPIS)	- แผนการควบรวมกิจการ เข้าซื้อกิจการ หรือแผนการลดค่าใช้จ่าย - รายงานการวิเคราะห์ผลกระทบต่อบริการ Digital ID สำหรับการควบรวมกิจการ เข้าซื้อกิจการ หรือการลดค่าใช้จ่าย	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
5 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Strategic	สัดส่วนของรายได้จากการประกอบธุรกิจด้าน Digital ID	รายได้จากการประกอบธุรกิจด้าน Digital ID น้อยกว่าร้อยละ 10 ของรายได้ทั้งหมดในรอบปีงบประมาณล่าสุด	รายได้จากการประกอบธุรกิจด้าน Digital ID น้อยกว่าร้อยละ 50 ของรายได้ทั้งหมดในรอบปีงบประมาณล่าสุด	รายได้จากการประกอบธุรกิจด้าน Digital ID ไม่น้อยกว่าร้อยละ 50 ของรายได้ทั้งหมดในรอบปีงบประมาณล่าสุด	ALL (IDP, DPIS)	งบการเงินซึ่งแสดงรายได้จากการประกอบธุรกิจด้าน Digital ID และรายได้รวมของบริษัท ซึ่งได้รับการตรวจสอบจากผู้สอบบัญชีที่ได้รับอนุญาตจากสภาวิชาชีพบัญชี	
5 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Strategic	เป้าหมาย สัดส่วนของรายได้จากการประกอบธุรกิจด้าน Digital ID นับถัดจากวันประเมินไป 1 ปี	รายได้จากการประกอบธุรกิจด้าน Digital ID น้อยกว่าร้อยละ 10 ของรายได้ทั้งหมด	รายได้จากการประกอบธุรกิจด้าน Digital ID น้อยกว่าร้อยละ 50 ของรายได้ทั้งหมด	รายได้จากการประกอบธุรกิจด้าน Digital ID ไม่น้อยกว่าร้อยละ 50 ของรายได้ทั้งหมด	ALL (IDP, DPIS)	-	
6	Strategic	การแข่งขันในอุตสาหกรรมบริการ Digital ID	มีการแข่งขันค่อนข้างต่ำ	มีการแข่งขันตามกลไกตลาดแต่ไม่ได้ส่งผลกระทบต่อกำไรของบริษัทมากนัก	มีการแข่งขันอย่างรุนแรงจนส่งผลกระทบต่อกำไรและการดำเนินธุรกิจของบริษัทอย่างมีนัยสำคัญ	ALL (IDP, DPIS)		

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
7	Strategic, Operational	ผลกระทบจากการเปลี่ยนแปลงกฎหมายหรือกฎเกณฑ์ (พิจารณา กฎหมายหรือกฎเกณฑ์ ที่จะมีผลบังคับใช้ในระยะเวลา 1 ปี นับจากวันที่ทำการประเมิน)	ไม่มีการเปลี่ยนแปลงกฎหมายหรือกฎเกณฑ์ที่มีผลกระทบต่อการดำเนินกลยุทธ์ และ/หรือ การปฏิบัติการเพื่อให้บริการ Digital ID	มีการเปลี่ยนแปลงกฎหมายหรือกฎเกณฑ์ที่มีผลกระทบเล็กน้อยถึงปานกลาง (อยู่ในระดับที่สามารถจัดการได้) ต่อการดำเนินกลยุทธ์ และ/หรือ การปฏิบัติการเพื่อให้บริการ Digital ID	ไม่มีกระบวนการติดตามการเปลี่ยนแปลงกฎหมายหรือกฎเกณฑ์เพื่อนำไปปฏิบัติให้สอดคล้อง หรือมีการเปลี่ยนแปลงกฎหมายหรือกฎเกณฑ์ที่มีผลกระทบอย่างมากต่อการดำเนินกลยุทธ์ และ/หรือ การปฏิบัติการเพื่อให้บริการ Digital ID	ALL (IDP, DPIS)	รายการกฎหมายหรือกฎเกณฑ์ที่เกี่ยวกับบริการ Digital ID ที่ยังไม่มีผลบังคับใช้	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
8	Operational, Technology	การตรวจสอบจากผู้ตรวจสอบอิสระที่ครอบคลุมกระบวนการปฏิบัติงานที่สำคัญและระบบเทคโนโลยีสารสนเทศเพื่อให้บริการ Digital ID	มีการดำเนินการตรวจสอบและรายงานผลต่อผู้บริหารซึ่งครอบคลุมบริการ Digital ID ที่สำคัญทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง	มีการดำเนินการตรวจสอบและรายงานผลต่อผู้บริหารซึ่งครอบคลุมบริการ Digital ID ที่สำคัญเพียงบางส่วน หรือ มีการดำเนินการตรวจสอบและรายงานผลต่อผู้บริหารซึ่งครอบคลุมบริการ Digital ID ที่สำคัญทั้งหมดแต่ไม่สม่ำเสมอ	ไม่มีการดำเนินการตรวจสอบ หรือไม่มีการรายงานผลให้ผู้บริหารรับทราบ	ALL (IDP, DPIS)	รายงานสรุปผลการตรวจสอบที่เกี่ยวข้อง	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
9	Compliance	การตรวจสอบการปฏิบัติตามกฎหมายและกฎเกณฑ์ด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบริการ Digital ID เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์, กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, กฎหมายคุ้มครองข้อมูลส่วนบุคคล	มีการดำเนินการตรวจสอบและรายงานผลต่อผู้บริหารซึ่งครอบคลุมบริการ Digital ID ที่สำคัญทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง	มีการดำเนินการตรวจสอบและรายงานผลต่อผู้บริหารซึ่งครอบคลุมบริการ Digital ID ที่สำคัญเพียงบางส่วน หรือมีการดำเนินการตรวจสอบและรายงานผลต่อผู้บริหารซึ่งครอบคลุมบริการ Digital ID ที่สำคัญทั้งหมดแต่ไม่สม่ำเสมอ	ไม่มีการดำเนินการตรวจสอบ หรือไม่มีการรายงานผลให้ผู้บริหารรับทราบ	ALL (IDP, DPIS)	- รายงานสรุปผลการตรวจสอบที่เกี่ยวข้อง	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
10	Compliance	ปริมาณกฎระเบียบที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศการป้องกันการทุจริตหรือการฉ้อโกงการคุ้มครองข้อมูลส่วนบุคคลที่องค์กรต้องปฏิบัติตาม เช่น กฎระเบียบของหน่วยงานกำกับดูแล (สพธอ. ธปท. คปภ. กลต. กสทช.), สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กรณีเป็น CII)	ต้องปฏิบัติตามกฎระเบียบของหน่วยงานภาครัฐ จำนวน 1 หน่วยงาน	ต้องปฏิบัติตามกฎระเบียบของหน่วยงานภาครัฐ จำนวน 2-3 หน่วยงาน	ต้องปฏิบัติตามกฎระเบียบของหน่วยงานภาครัฐ จำนวนมากกว่า 3 หน่วยงาน	ALL (IDP, DPIS)	- รายชื่อหน่วยงานที่กำกับดูแลองค์กร	หมายเหตุ ไม่นับรวมกฎระเบียบที่ทุก ๆ องค์กรต้องปฏิบัติตาม เช่น กฎระเบียบของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
11	Strategic, Operational, Reputation, Compliance	จำนวนนวัตกรรมเกี่ยวกับบริการ Digital ID ที่อยู่ระหว่างทดสอบหรือมีแผนเข้าทดสอบใน ETDA Sandbox	ไม่มี	1-2 นวัตกรรม	มากกว่า 2 นวัตกรรม	ALL (IDP, DPIS)	- รายการนวัตกรรมเกี่ยวกับบริการ Digital ID	นวัตกรรมหรือบริการประเภทที่สามารถเข้าร่วม ETDA Sandbox 1. เป็นบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ไม่ว่าส่วนหนึ่งส่วนใด เช่น • สามารถพัฒนาเป็นโครงสร้างพื้นฐาน สำหรับงานด้านธุรกรรมทางอิเล็กทรอนิกส์ในการพัฒนาประเทศ หรือช่วยเพิ่มประสิทธิภาพการให้บริการของทั้งภาครัฐและเอกชน • ไม่มีกฎระเบียบรองรับ ซึ่งอาจส่งผลกระทบต่อความน่าเชื่อถือหรือก่อให้เกิดความเสียหายแก่ประชาชน • มีความเสี่ยงที่จะขัดกับกฎระเบียบ หลักเกณฑ์การกำกับดูแลของ ETDA 2. มีการนำเทคโนโลยีมาใช้ซึ่งอาจจะไม่เคยนำไปใช้มาก่อนหรือแตกต่างจากบริการที่มีอยู่แล้วในประเทศ ให้บริการในวงจำกัดหรือเป็นการนำเทคโนโลยีมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ ทั้งนี้ หากเป็นบริการที่มีลักษณะนอกเหนือจากที่ระบุข้างต้นและมีความประสงค์เข้าร่วมทดสอบ

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
								ใน ETDA Sandbox จะได้รับการพิจารณาเป็นรายกรณี อ้างอิง https://www.etda.or.th/th/Useful-Resource/ETDA-Sandbox-Q-and-A.aspx

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
12	Strategic, Technology, Reputation, Compliance	การใช้งาน Innovative Technology ในระบบบริการ Digital ID หมายเหตุ ให้นับรวมเทคโนโลยีของหน่วยงานอื่นที่องค์กรนำมาใช้เพื่อให้บริการในนามขององค์กรด้วย	ไม่มีการใช้งาน	1-2 เทคโนโลยี	มากกว่า 2 เทคโนโลยี	ALL (IDP, DPIS)	- รายการ Innovative Technology ที่มีการใช้ในระบบ Digital ID	Innovative Technology หมายถึง การประมวลผลที่ใช้เทคโนโลยีใหม่ ที่ยังไม่มีมาตรฐานสากลยอมรับ (Unproven technology) เช่น การประมวลผลด้วยปัญญาประดิษฐ์ (Artificial intelligence), การใช้แอปพลิเคชันของเทคโนโลยี IoT, การใช้เทคโนโลยีบล็อกเชน (Blockchain) เป็นต้น หมายเหตุ เทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน และเทคโนโลยีการรู้จำใบหน้า (facial recognition) ถือเป็นเทคโนโลยีที่มีมาตรฐานสากลยอมรับ อ้างอิงจาก ขมธอ. 29 เล่ม 1-2565, ขมธอ. 29 เล่ม 2-2565

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
13	Operational, Technology, Compliance	นโยบาย และแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยระบบสารสนเทศ	มีการจัดทำนโยบาย และแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับมาตรฐานด้านความมั่นคงปลอดภัยที่ได้รับการยอมรับ เช่น ISO27001, PCI DSS, NIST และมีการทบทวนอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง	มีการจัดทำนโยบาย และแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และมีการทบทวนอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง	มีการจัดทำนโยบาย และแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ แต่ไม่ได้ทบทวนอย่างสม่ำเสมอ	ALL (IDP, DPIS)	- นโยบาย และแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ - หลักฐานการทบทวนนโยบายและแนวทางปฏิบัติ - ตารางแสดงความสัมพันธ์ของนโยบาย และแนวทางปฏิบัติกับมาตรฐานสากลที่อ้างอิง เช่น Statement of Applicability (SOA) สำหรับ ISO27001	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
14	Operational, Technology,	การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ	มีกิจกรรมการประเมินและบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศครอบคลุมบริการ Digital ID และระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง มีการทบทวนความเสี่ยงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และมีกระบวนการติดตามความเสี่ยงที่มีประสิทธิภาพ เช่น การกำหนด KPI	มีกิจกรรมการประเมินและบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศครอบคลุมบริการ Digital ID และระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง มีการทบทวนความเสี่ยงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง แต่ยังขาดกระบวนการติดตามความเสี่ยงที่มีประสิทธิภาพ	ไม่มีกิจกรรมการประเมินและบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมบริการ Digital ID และระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง	ALL (IDP, DPIS)	- นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ - รายงานผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมบริการ Digital ID และระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง - รายงานผลการติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศ	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
15	Operational	การบริหารจัดการความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบหรือบริการ Digital ID	มีกิจกรรมการประเมินและบริหารความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบหรือบริการ Digital ID มีการทบทวนความเสี่ยงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และมีกระบวนการติดตามความเสี่ยงที่มีประสิทธิภาพ เช่น การกำหนด KPI	มีกิจกรรมการประเมินและบริหารความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบหรือบริการ Digital ID มีการทบทวนความเสี่ยงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง แต่ยังขาดกระบวนการติดตามความเสี่ยงที่มีประสิทธิภาพ เช่น การกำหนด KPI	ไม่มีกิจกรรมการประเมินและบริหารความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบหรือบริการ Digital ID	ALL (IDP, DPIS)	- รายงานผลการประเมินความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบหรือบริการ Digital ID - รายงานผลการติดตามความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบหรือบริการ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
16	Technology, Reputation, Compliance	การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอ่อนไหว เช่น ข้อมูลเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (ตามมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)	ระบบที่ให้บริการ Digital ID ไม่มีการจัดเก็บประมวลผลถ่ายโอนข้อมูลส่วนบุคคลอ่อนไหว	ระบบที่ให้บริการ Digital ID มีการประมวลผลหรือถ่ายโอนข้อมูลส่วนบุคคลอ่อนไหว แต่ไม่มีการจัดเก็บ	ระบบที่ให้บริการ Digital ID มีการจัดเก็บข้อมูลส่วนบุคคลอ่อนไหว	ALL (IDP, DPIS)	เอกสารการบันทึกรายการประมวลผลข้อมูลส่วนบุคคล หรือ data flow diagram ที่เกี่ยวข้องกับระบบที่ให้บริการ Digital ID	ข้อมูลที่อยู่ในรูปแบบการเข้ารหัสหรือที่ผ่านมาตรการรักษาความปลอดภัยรูปแบบหนึ่งแล้วก็ยังคงถือเป็นข้อมูลส่วนบุคคล

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
17	Operational, Compliance	บุคคลภายนอกที่ประมวลผลข้อมูลแทนที่เกี่ยวกับบริการ Digital ID หมายเหตุ “บุคคลภายนอก” หมายถึง บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการหรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานหรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์หรือบริการของหน่วยงาน	ไม่มีบุคคลภายนอกที่ประมวลผลข้อมูลแทน	มีบุคคลภายนอกที่ประมวลผลข้อมูลแทนแต่ไม่มีข้อมูลผู้ใช้บริการส่งไปเพื่อประมวลผล	มีบุคคลภายนอกที่ประมวลผลข้อมูลแทนโดยเกี่ยวข้องกับข้อมูลของผู้ใช้บริการ	ALL (IDP, DPIS)	สัญญาเกี่ยวกับการใช้หรือประมวลผลข้อมูลแทนที่เกี่ยวข้องกับการให้บริการ Digital ID	การประมวลผลข้อมูลแทน คือ การที่องค์กรจำเป็นต้องส่งข้อมูลบางอย่างไปให้องค์กรภายนอกดำเนินการแทนให้ โดยองค์กรจะได้ผลลัพธ์จากการประมวลผลเพื่อนำไปดำเนินกิจกรรมต่อ

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
18 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Reputation	จำนวนการร้องเรียนหรือแจ้งปัญหาในการใช้งานระบบบริการ Digital ID จากผู้ใช้บริการ รวมถึงหน่วยงานที่เชื่อมต่อเพื่อใช้บริการ (เช่น Relying Party, Identity Provider, Authoritative Source) ในระยะเวลา 1 ปี	น้อยกว่า 10 เรื่อง	10-20 เรื่อง	มากกว่า 20 เรื่อง	ALL (IDP, DPIS)	- รายงานสรุปการร้องเรียนหรือแจ้งปัญหาในการใช้งานระบบบริการ Digital ID จากผู้ใช้บริการในระยะเวลา 1 ปี	
18 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Reputation	การทดสอบการใช้งานระบบและการสร้างประสบการณ์ที่ดีแก่ผู้ใช้บริการสำหรับระบบบริการ Digital ID	มีการทดสอบความสามารถของระบบ (usability test) ครอบคลุมขั้นตอนตั้งแต่ต้นจนจบ กระบวนการในสภาพแวดล้อมที่ใกล้เคียงกับการให้บริการจริง ครอบคลุม	มีการทดสอบความสามารถของระบบ (usability test) ครอบคลุมขั้นตอนตั้งแต่ต้นจนจบ กระบวนการในสภาพแวดล้อมที่ใกล้เคียงกับการให้บริการจริง ครอบคลุม	มีการทดสอบความสามารถของระบบ (usability test) แต่ไม่ครอบคลุมขั้นตอนตั้งแต่ต้นจนจบ กระบวนการหรือไม่ใกล้เคียงกับการให้บริการจริง หรือ	ALL (IDP, DPIS)	- แผนและรายละเอียดการทดสอบระบบ (usability test plans) - รายงานผลการทดสอบความสามารถของระบบ (usability test)	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
			ผู้ใช้บริการกลุ่มต่าง ๆ และผลการทดสอบผ่านเกณฑ์การทดสอบที่กำหนดทั้งหมด	ผู้ใช้บริการกลุ่มต่าง ๆ และผลการทดสอบผ่านเกณฑ์การทดสอบที่กำหนดส่วนใหญ่	ไม่ครอบคลุมผู้ใช้บริการกลุ่มต่าง ๆ			
19 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Operational	จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบหรือบริการ Digital ID ในระยะเวลา 1 ปี	ไม่มีเหตุการณ์ดังกล่าว	1-2 เหตุการณ์	มากกว่า 2 เหตุการณ์	ALL (IDP, DPIS)	- รายงานสรุปเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบหรือบริการ Digital ID ในระยะเวลา 1 ปี	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
19 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Operational	แผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบบริการ Digital ID	มีการจัดทำแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบและสื่อสารอย่างเหมาะสมจนมั่นใจได้ว่าบุคลากรที่เกี่ยวข้องมีความตระหนัก เช่น การวัดผลการเรียนด้วยแบบทดสอบสำหรับพนักงาน , การฝึกซ้อมเชิงปฏิบัติการสำหรับทีมรับมือเหตุการณ์ เป็นต้น	มีการจัดทำแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบและสื่อสารไปยังบุคลากรที่เกี่ยวข้อง	มีการจัดทำแผนการป้องกันการทุจริตแต่การสื่อสารไปยังบุคลากรที่เกี่ยวข้องยังไม่ครบถ้วน	ALL (IDP, DPIS)	- แผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบบริการ Digital ID - หลักฐานการสื่อสารเพื่อสร้างความตระหนักไปยังบุคลากรที่เกี่ยวข้อง	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
20 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Operational, Technology	จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ (incident) ที่มีผลกระทบในระดับกลางขึ้นไป* เช่น ภัยคุกคามทางไซเบอร์, ข้อมูลรั่วไหล, ระบบหยุดชะงักเป็นเวลานาน (มากกว่า 8 ชั่วโมง), ความผิดปกติอย่างร้ายแรงของระบบที่เกี่ยวกับการให้บริการ Digital ID ในระยะเวลา 1 ปี หมายเหตุ ผลกระทบในระดับกลางขึ้นไป หมายถึงมูลค่าความเสียหาย	ไม่มี	1-2 เหตุการณ์	มากกว่า 2 เหตุการณ์	ALL (IDP, DPIS)	- รายงานสรุปเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ (incident) ที่มีผลกระทบในระดับกลางขึ้นไปในระยะเวลา 1 ปี	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
		มากกว่า 1 ล้านบาท/ผู้เสียหาย มากกว่า 10,000 คน/กระทบต่อชีวิต ร่างกายหรืออนามัย ของคน/กระทบต่อ ความมั่นคงของรัฐ (อ้างอิงประกาศ คธอ. เรื่อง ประเภทธุรกรรม ทางอิเล็กทรอนิกส์ และหลักเกณฑ์ การประเมินระดับ ผลกระทบของ ธุรกรรม ทางอิเล็กทรอนิกส์ ตามวิธี แบบปลอดภัย พ.ศ. 2555)						

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
20 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Operational, Technology	การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ (incident)	มีขั้นตอนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ซึ่งครอบคลุมการตรวจพบเหตุการณ์ การแจ้งเหตุการพิสูจน์เหตุการณ์ การรายงานเหตุการณ์ การตอบสนองต่อเหตุการณ์ รวมถึงการรวบรวมและจัดเก็บหลักฐานเพื่อการสืบสวนและสื่อสารอย่างเหมาะสมจนมั่นใจได้ว่าบุคลากรที่เกี่ยวข้อง	มีขั้นตอนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ซึ่งครอบคลุมการตรวจพบเหตุการณ์ การแจ้งเหตุการพิสูจน์เหตุการณ์ การรายงานเหตุการณ์ การตอบสนองต่อเหตุการณ์ รวมถึงการรวบรวมและจัดเก็บหลักฐานเพื่อการสืบสวนและสื่อสารไปยังบุคลากรที่เกี่ยวข้อง	มีขั้นตอนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์แต่เนื้อหายังไม่ครบ หรือการสื่อสารไปยังบุคลากรที่เกี่ยวข้องยังไม่ครบถ้วน	ALL (IDP, DPIS)	- ขั้นตอนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ - หลักฐานการสื่อสารเพื่อสร้างความตระหนักไปยังบุคลากรที่เกี่ยวข้อง	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
			มีความตระหนัก เช่น การวัดผลการเรียนด้วยแบบทดสอบสำหรับพนักงาน , การฝึกซ้อมเชิงปฏิบัติการสำหรับทีมรับมือเหตุการณ์ เป็นต้น					

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
21	Reputation	จำนวนเหตุการณ์ที่ส่งผลกระทบในวงกว้างและมีนัยสำคัญต่อความน่าเชื่อถือของบริษัทในระยะเวลา 1 ปี หมายเหตุ นับรวมเหตุการณ์ที่ไม่เกี่ยวข้องกับบริการ Digital ID เช่น เหตุการณ์ไม่พึงประสงค์ (incident) ของระบบอื่นของหน่วยงาน, การทุจริตหรือความผิดพลาดของบุคลากรที่ผลกระทบระดับกลางขึ้นไป เป็นต้น	ไม่มี	1-2 เหตุการณ์	มากกว่า 2 เหตุการณ์	ALL (IDP, DPIS)	- รายงานสรุปเหตุการณ์ที่ส่งผลกระทบในวงกว้างและมีนัยสำคัญต่อความน่าเชื่อถือของบริษัทในระยะเวลา 1 ปี	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
22	Operational, Compliance	ระดับการพึ่งพาบุคคลในกระบวนการปฏิบัติงานที่เกี่ยวกับการให้บริการ Digital ID	อาศัยระบบอัตโนมัติเป็นส่วนใหญ่ (ขั้นตอนการให้บริการไม่เกินกว่า 30% ต้องพึ่งพาเจ้าหน้าที่)	อาศัยทั้งเจ้าหน้าที่และระบบอัตโนมัติในขั้นตอนการให้บริการในระดับที่ใกล้เคียงกัน (ขั้นตอนการให้บริการ 31-70% ต้องพึ่งพาเจ้าหน้าที่)	อาศัยเจ้าหน้าที่ในการปฏิบัติเป็นส่วนใหญ่ (ขั้นตอนการให้บริการมากกว่า 70% ต้องพึ่งพาเจ้าหน้าที่)	ALL (IDP, DPIS)	- ขั้นตอนการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวกับการให้บริการ Digital ID - Workflow การทำงานของระบบที่เกี่ยวกับการให้บริการ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
23	Operational, Compliance	การทำข้อตกลงกับบุคคลภายนอก หมายเหตุ “บุคคลภายนอก” หมายถึง บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการหรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานหรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์หรือบริการของหน่วยงาน	มีการทำสัญญาหรือข้อตกลงกับบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID ทั้งหมด โดยเนื้อหาสัญญาระบุขอบเขตการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก, หน้าที่และความรับผิดชอบของบุคคลภายนอก, เงื่อนไขหรือสิทธิในการขอเปลี่ยนแปลง ยุติหรือยกเลิกสัญญา, ความรับผิดต่อความเสียหาย	มีการทำสัญญาหรือข้อตกลงกับบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID ทั้งหมด แต่เนื้อหาสัญญายังไม่ครบถ้วน	มีการทำสัญญากับบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID เพียงบางส่วน	ALL (IDP, DPIS)	- รายการบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID - สัญญากับบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
24	Operational, Compliance	การติดตามผลการปฏิบัติงานของบุคคลภายนอก	กำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID ทั้งหมดอย่างต่อเนื่อง มีการประเมินผลการปฏิบัติงานทั้งในด้านประสิทธิภาพ การรักษาความมั่นคงปลอดภัย และการปฏิบัติตามกฎหมาย	กำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID ทั้งหมดอย่างต่อเนื่อง แต่ขาดการประเมินผลการปฏิบัติงานทั้งในด้านประสิทธิภาพ การรักษาความมั่นคงปลอดภัย และการปฏิบัติตามกฎหมาย	มีการกำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID เพียงบางส่วน	ALL (IDP, DPIS)	- รายชื่อผู้รับผิดชอบในการติดตามผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID - รายงานการประเมินผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID	
25	Operational, Compliance	จำนวนผู้ให้บริการภายนอกด้าน IT (IT outsourcing) ที่สนับสนุนการให้บริการ Digital ID เช่น	จำนวนน้อยกว่า 2 ราย	จำนวน 2 - 4 ราย	มากกว่า 4 ราย	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายชื่อผู้ให้บริการภายนอกด้าน IT ที่เกี่ยวข้องกับ	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
		Cloud provider, Internet Service Provider, Developer					การให้บริการ Digital ID	
26	Operational	การใช้บริการผู้ให้บริการภายนอกในการดูแลรักษาอุปกรณ์ IT ที่เกี่ยวข้องกับระบบบริการ Digital ID	ใช้บริการน้อยกว่า 2 ราย	จำนวน 2 - 4 ราย	ใช้บริการมากกว่า 4 ราย	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายชื่อผู้ให้บริการภายนอกด้าน IT ที่เกี่ยวข้องกับการดูแลรักษาอุปกรณ์ (MA) โดยเป็นอุปกรณ์ที่เกี่ยวข้องกับการให้บริการ Digital ID	
27	Operational, Reputation	เป้าหมาย จำนวนบัญชีรวมทั้งหมดที่ลงทะเบียนและพิสูจน์ตัวตนแล้วในระบบบริการ Digital ID นับถัดจากวันประเมินไป 1 ปี	น้อยกว่า 100,000 บัญชี	100,000 - 1,000,000 บัญชี	มากกว่า 1,000,000 บัญชี	ALL (IDP, DPIS)	- หลักฐานแสดงจำนวนบัญชีที่ลงทะเบียนและพิสูจน์ตัวตนแล้วในระบบบริการ Digital ID ในปัจจุบัน และระบุเป้าหมายในอีก 1 ปี	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
28	Operational	จำนวนพนักงานทั้งหมดที่เกี่ยวข้องกับการให้บริการ Digital ID	น้อยกว่า 10 คน	10-100 คน	มากกว่า 100 คน	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - แผนผังองค์กรที่แสดงถึงหน่วยงานที่เกี่ยวข้องกับการให้บริการ Digital ID - จำนวนพนักงานในแต่ละหน่วยงานที่เกี่ยวข้องกับการให้บริการ Digital ID	
29	Operational	จำนวนพนักงานในสายงาน IT ทั้งหมดที่เกี่ยวข้องกับการให้บริการ Digital ID	น้อยกว่า 10 คน	10 - 20 คน	มากกว่า 30 คน	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - จำนวนพนักงาน IT ที่เกี่ยวข้องกับการให้บริการ Digital ID	
30	Operational	จำนวนพนักงานในสายงาน IT ที่เกี่ยวข้องกับการให้บริการ Digital ID และลาออกในระยะเวลา 12 เดือน	มีอัตรา Turnover ต่ำ (น้อยกว่า 10%)	มีอัตรา Turnover ปานกลาง (10-20%)	มีอัตรา Turnover สูง (มากกว่า 20%)	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - จำนวนพนักงาน IT ที่ลาออกและรับผิดชอบกับการให้บริการ Digital ID	นำพนักงานที่ลาออกในช่วง 12 เดือน / อัตรากำลังพนักงานฝ่าย IT (ทั้งนี้ ต้องเป็นพนักงานที่เกี่ยวข้องกับการให้บริการ Digital ID)

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
31	Operational	จำนวนพนักงานที่มีสิทธิ์สูง (เช่น Administrator ของ Network, Database) ที่เกี่ยวข้องกับการให้บริการ Digital ID และลาออกในระยะเวลา 12 เดือน	มีอัตรา Turnover ต่ำ (น้อยกว่า 2%)	มีอัตรา Turnover ปานกลาง (2-8%)	มีอัตรา Turnover สูง (มากกว่า 8%)	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - จำนวนพนักงาน IT ที่ลาออกและได้รับสิทธิ์สูงในการเข้าถึงระบบ Digital ID	นำพนักงาน Admin ที่ลาออกในช่วง 12 เดือน / อัตรากำลังพนักงานฝ่าย IT ทั้งหมดที่เป็น Admin (ทั้งนี้ ต้องเป็นพนักงานที่เกี่ยวข้องกับการให้บริการ Digital ID)
32	Operational	จำนวนพนักงานผู้ให้บริการภายนอก (Outsource/ IT Outsource) ที่เกี่ยวข้องกับการให้บริการ Digital ID และมีสิทธิ์เข้าถึงระบบ Digital ID ขององค์กร	ผู้ให้บริการภายนอกไม่สามารถเข้าถึงได้	1-50 คน	มากกว่า 50 คน	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายชื่อหรือจำนวนพนักงาน IT outsource ที่สามารถเข้าถึงระบบ Digital ID ขององค์กรได้	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
33	Operational	สัดส่วนพนักงานผู้ให้บริการภายนอก (Outsource/ IT Outsource) ที่เกี่ยวข้องกับการให้บริการ Digital ID และได้รับสิทธิ์สูงต่อจำนวนสิทธิ์สูงทั้งหมดในระบบ Digital ID	ผู้ให้บริการภายนอกไม่สามารถเข้าถึงได้	น้อยกว่า 20%	มากกว่า 20%	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายชื่อหรือจำนวนพนักงาน IT outsource ที่มีสิทธิ์สูงและสามารถเข้าถึงระบบ Digital ID ขององค์กรได้ - รายชื่อหรือจำนวนพนักงาน IT ภายในองค์กรที่ได้รับสิทธิ์สูงในการเข้าถึงระบบ Digital ID	นำจำนวนพนักงานของผู้ให้บริการภายนอกที่ได้รับสิทธิ์สูง / จำนวนสิทธิ์สูงทั้งหมดที่องค์กรมี (ทั้งนี้ต้องเป็นพนักงานที่เกี่ยวข้องกับการให้บริการ Digital ID)
34	Operational	จำนวน Account ของพนักงานที่ลาออก หรือผู้ให้บริการภายนอก (Outsource/ IT Outsource) ที่ไม่เกี่ยวข้องที่ตรวจพบว่ายังหลงเหลืออยู่ในระบบ Digital ID ในรอบ 12 เดือน	ไม่มี Account ผู้ที่ไม่เกี่ยวข้องกับองค์กรในระบบ	1-2 Account	มากกว่า 2 Account	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายชื่อพนักงานที่อยู่ในระบบ Digital ID ในปัจจุบัน - รายชื่อพนักงานที่นำออกจากระบบ Digital ID ในระยะเวลา 12 เดือนที่ผ่านมา	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
35 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Operational, Technology	การใช้งานแผนสำรองฉุกเฉิน (BCP และ DRP) ที่เกี่ยวข้องกับการให้บริการ Digital ID ในรอบ 12 เดือนที่ผ่านมา	น้อยกว่า 2 ครั้ง	2-3 ครั้ง	มากกว่า 3 ครั้ง	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - แผนสำรองฉุกเฉิน (BCP และ DRP) ที่เกี่ยวข้องกับระบบ Digital ID - การประกาศใช้งานแผนสำรองฉุกเฉินที่กระทบกับระบบ Digital ID	
35 เลือกตอบข้อ ก หรือ ข เพียงข้อเดียว	Operational, Technology	แผนสำรองฉุกเฉิน (BCP และ DRP) ที่เกี่ยวข้องกับการให้บริการ Digital ID	จัดให้มีแผนสำรองฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) และแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่เกี่ยวข้องกับการให้บริการ Digital ID และมีแผนในการทดสอบร่วมกับผู้ให้บริการและหน่วยงานที่เกี่ยวข้อง	จัดให้มีแผนสำรองฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) และแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่เกี่ยวข้องกับการให้บริการ Digital ID ทั้งนี้ยังไม่มีแผนที่จะทดสอบแผนสำรองฉุกเฉินที่เกี่ยวข้องกับ	มีแผนสำรองฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) หรือแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่เกี่ยวข้องกับการให้บริการ Digital ID อย่างใดอย่างหนึ่งหรือไม่มีทั้งหมด	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - แผนสำรองฉุกเฉิน (BCP และ DRP) ที่เกี่ยวข้องกับระบบ Digital ID - ผลการทดสอบแผนสำรองฉุกเฉิน (BCP และ DRP) ที่เกี่ยวข้องกับระบบ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
			นำผลการทดสอบมาปรับปรุงเอกสาร โดยมีแผนดำเนินการดังกล่าวอย่างน้อยปีละ 1 ครั้ง	การให้บริการ Digital ID				
36	Operational, Technology	ช่องโหว่ภายในระบบหรือแอปพลิเคชันสำหรับบริการ Digital ID ที่มีความเสี่ยงของช่องโหว่ระดับ High หรือ Critical	ไม่มีช่องโหว่ที่มีความเสี่ยงระดับ High หรือ Critical ที่ยังไม่ได้รับการแก้ไข	มี 1-3 ช่องโหว่ที่มีความเสี่ยงระดับ High หรือ Critical ที่ยังไม่ได้รับการแก้ไข	มีมากกว่า 3 ช่องโหว่ที่มีความเสี่ยงระดับ High หรือ Critical ที่ยังไม่ได้รับการแก้ไข	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายงานช่องโหว่ภายในระบบหรือแอปพลิเคชันสำหรับบริการ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
37	Operational, Technology	การบริหารจัดการช่องโหว่ (Vulnerability management) และการทดสอบการเจาะระบบ (Penetration test) ที่เกี่ยวกับระบบ Digital ID	มีแผนดำเนินงานประเมินช่องโหว่ (Vulnerability assessment) และการทดสอบการเจาะระบบ (Penetration test) จากผู้เชี่ยวชาญอย่างน้อยปีละ 1 ครั้ง โดยครอบคลุมระบบ Digital ID ทั้งหมด	มีแผนดำเนินงานประเมินช่องโหว่ (Vulnerability assessment) และการทดสอบการเจาะระบบ (Penetration test) จากผู้เชี่ยวชาญอย่างน้อยปีละ 1 ครั้ง แต่ยังไม่ครอบคลุมระบบ Digital ID ทั้งหมด	มีแผนดำเนินงานประเมินช่องโหว่ (Vulnerability assessment) หรือการทดสอบการเจาะระบบ (Penetration test) สำหรับระบบอื่น แต่ไม่ครอบคลุมระบบ Digital ID หรือยังไม่มีแผนงานดังกล่าว	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - นโยบายที่เกี่ยวข้องกับการบริหารจัดการช่องโหว่ - แผนในการดำเนินการ VA และ Pentest ที่เกี่ยวข้องกับระบบ Digital ID	
38	Technology	จำนวน Internet Service Provider (ISP) ที่เชื่อมต่อและใช้งานกับระบบ Digital ID	น้อยกว่า 2 ราย	2 ราย	มากกว่า 2 ราย	ALL (IDP, DPIS)	รายชื่อ Internet Service Provider (ISP) ที่เชื่อมต่อและใช้งานกับระบบ Digital ID ทั้งหมด	
39	Technology	จำนวน Public IP Address ที่มีการใช้งานเชื่อมต่ออินเทอร์เน็ต หรือ	น้อยกว่า 10 IP Address	10-20 IP Address	มากกว่า 20 IP Address	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - List IP ที่ใช้งานกับระบบ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
		ใช้เชื่อมต่อระบบบริการ Digital ID ขององค์กร						
40	Technology	การใช้งาน Protocol ที่ไม่ปลอดภัยบนระบบบริการ Digital ID เช่น HTTP, FTP, TLS 1.0	Protocol ที่ใช้งานทั้งหมด Secure และทันสมัย	มีการใช้งาน Protocol ที่ Unsecure แต่อยู่ระหว่างการดำเนินการแก้ไข	มีการใช้งาน Protocol ที่ Unsecure และยังไม่มีแผนในการจัดการ	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - มาตรฐาน Protocol ที่ใช้งานภายในองค์กร - Specification และการออกแบบระบบ Digital ID	
41	Technology	จำนวนบริษัทในเครือที่เชื่อมต่อมายังระบบบริการ Digital ID ขององค์กร	ไม่มีบริษัทในเครือที่เชื่อมต่อ	จำนวน 1 - 2 ราย	มากกว่า 2 ราย	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายชื่อบริษัทในเครือที่เชื่อมต่อหรือใช้งานระบบบริการ Digital ID	
42	Technology	วิธีการเชื่อมต่อมายังระบบบริการ Digital ID ของบริษัทในเครือ	Private Link (เช่น MPLS, Leased line) และต้องใช้ VPN หรือไม่มีการเชื่อมต่อ	Private Link (เช่น MPLS, Leased line)	VPN ผ่าน Public internet	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Specification และการออกแบบระบบ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
43	Technology	จำนวนบุคคลภายนอกที่สามารถเข้าถึงระบบบริการ Digital ID ขององค์กร หมายเหตุ “บุคคลภายนอก” หมายถึง บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการหรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานหรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์หรือ	มีจำนวนน้อยกว่า 5 ราย	จำนวน 5 - 10 ราย	มากกว่า 10 ราย	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายชื่อหน่วยงานภายนอกที่เชื่อมต่อหรือใช้งานระบบบริการ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
		บริการของหน่วยงาน						
44	Technology	วิธีการเข้าถึงระบบบริการ Digital ID โดยบุคคลภายนอก	ต้องเข้ามาภายในองค์กรเท่านั้น หรือไม่มีการเชื่อมต่อ	VPN ผ่าน Private Link	VPN ผ่าน Public internet	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - มาตรฐาน Protocol ที่ใช้งานภายในองค์กร - Specification และการออกแบบระบบ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
45	Technology	จำนวนระบบงานที่เกี่ยวกับบริการ Digital ID ที่องค์กรพัฒนาขึ้นเองหรือปรับแต่ง (Customize) จากระบบของบุคคลภายนอกเดิม	มีจำนวนน้อยกว่า 3 ระบบ	จำนวน 3-5 ระบบ	มากกว่า 5 ระบบ	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Specification และการออกแบบระบบ Digital ID - เอกสารการพัฒนาระบบงานที่พัฒนาเองเพื่อใช้ในการให้บริการ Digital ID	
46	Technology	จำนวนระบบงานที่เกี่ยวกับบริการ Digital ID ที่จ้างบุคคลภายนอกพัฒนา	มีจำนวนน้อยกว่า 3 ระบบ	จำนวน 3-5 ระบบ	มากกว่า 5 ระบบ	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - สัญญาการจ้างพัฒนาระบบงานโดยหน่วยงานภายนอกเพื่อใช้ในการให้บริการ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
47	Technology	ระบบงานที่เกี่ยวกับบริการ Digital ID ที่ใกล้ End-of-life หรือ End-of-support ภายในระยะเวลา 2 ปี	ไม่มีระบบงานไหนที่ OS, DB, Software, Hardware ที่ใช้งานอยู่ EOL หรือ EOS ภายใน 2 ปี	มีระบบงานที่ OS, DB, Software, Hardware ที่ใช้งานอยู่จะ EOL หรือ EOS ภายใน 2 ปี	มีการใช้งาน OS, DB, Software, Hardware ที่ใช้งานอยู่จะ EOL หรือ EOS ไปแล้ว	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - ทะเบียนทรัพย์สินที่แสดงถึง Hardware, Software, OS และ DB ที่ใช้ภายในระบบ Digital ID - กระบวนการ Update patch ภายในองค์กร	
48	Technology	จำนวน Open-source Software ทั้งหมดที่ใช้สำหรับให้บริการ, พัฒนา หรือดูแลระบบที่เกี่ยวกับบริการ Digital ID	มีจำนวนน้อยกว่า 5 โปรแกรม	มีจำนวน 5-10 โปรแกรม	มีจำนวนมากกว่า 10 โปรแกรม	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Specification และการออกแบบระบบ Digital ID - ทะเบียนทรัพย์สินที่แสดงถึง Software, ที่ใช้ภายในระบบ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
49	Technology	จำนวนอุปกรณ์เครือข่ายที่มีการใช้งาน (เช่น Firewall, Router, Switch) ที่เกี่ยวกับบริการ Digital ID	มีจำนวนน้อยกว่า 10 เครื่อง	มีจำนวน 10 - 30 เครื่อง	มีจำนวนมากกว่า 30 เครื่อง	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - ทะเบียนทรัพย์สินที่แสดงถึง Hardware, Software ทางด้าน Network ที่ใช้ภายในระบบ Digital ID - Network diagram ของระบบ Digital ID	ทั้งนี้ ให้นับทั้ง Physical และ Logical ด้วย เช่น Virtual firewall
50	Technology	การใช้งาน Cloud computing สำหรับระบบบริการ Digital ID	ไม่มีการใช้งาน Cloud	ใช้งานเฉพาะ Private Cloud	ใช้งาน Public หรือ Hybrid Cloud	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Specification และการออกแบบระบบ Digital ID	
51	Technology	ช่องทางการให้บริการ Digital ID สำหรับลูกค้า	ให้บริการ Digital ID โดยไม่ผ่านอินเทอร์เน็ต	ให้บริการ Digital ID โดยผ่านอินเทอร์เน็ตโดยช่องทางดังกล่าวมีเฉพาะบริการ Digital ID เท่านั้น	ให้บริการ Digital ID โดยผ่านอินเทอร์เน็ตโดยช่องทางดังกล่าวมีการให้บริการอื่น ๆ นอกจากบริการ Digital ID ด้วย เช่น บริการ	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Specification และการออกแบบระบบ Digital ID	ทั้งนี้ ให้ตรวจสอบทุกช่องทางที่ให้บริการลูกค้า ทั้งหน้า Website, Mobile application หรือช่องทางอื่น ๆ ว่าตรงกับระดับความเสี่ยงในข้อใด

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
					ทางธุรกรรมทางการเงิน			
52	Technology	การให้บริการ Digital ID ผ่าน Mobile Application	ไม่มีการให้บริการผ่าน Mobile Application	มี Mobile Application แต่อยู่ระหว่างการทดสอบ	มีการให้บริการผ่าน Mobile Application กับผู้ใช้บริการ	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Specification และการออกแบบ Mobile application สำหรับ Digital ID	
53	Technology	มาตรฐานของ Data center หรือ Cloud ที่เป็นโครงสร้างพื้นฐานให้ระบบที่ให้บริการ Digital ID	Data center หรือ Cloud ผ่านมาตรฐานสากลทางด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศ เช่น ISO27001 หรือ CSA STAR	Data center หรือ Cloud ผ่านมาตรฐานสากลด้านการจัดการ Data center เช่น ISO 20000	Data center หรือ Cloud ยังไม่ผ่านมาตรฐานสากลใด ๆ	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Certification ที่แสดงถึงการผ่านการตรวจสอบมาตรฐานสากลที่มีขอบเขตเกี่ยวข้องกับ Data center ที่ให้บริการระบบ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
54	Technology	ความซับซ้อนของระบบบริการ Digital ID	มีโครงสร้างระบบไม่ซับซ้อน ข้อมูลที่ใช้มีมาตรฐานเดียวกันและเชื่อมโยงกันแบบอัตโนมัติ (automate)	มีโครงสร้างระบบที่ซับซ้อน มีหลายระบบที่เกี่ยวข้อง โดยระบบส่วนใหญ่เชื่อมโยงกันแบบอัตโนมัติ (automate)	มีโครงสร้างระบบที่ซับซ้อนมาก มีหลายระบบที่เกี่ยวข้อง โดยมีระบบส่วนน้อยที่เชื่อมโยงกันแบบอัตโนมัติ (automate) การทำงานต้องมีการดึงข้อมูลออกมาหลายครั้ง	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Specification และการออกแบบระบบ Digital ID	การดึงข้อมูลหรือมีการ rekey ข้อมูลหลายครั้งทำให้ข้อมูลที่จัดเก็บในแต่ละ platform ไม่เหมือนกัน มีความเสี่ยงที่จะดำเนินการผิดพลาดได้
55	Technology	Single Point of Failure ของระบบเครือข่ายที่ให้บริการ Digital ID	ระบบเครือข่ายมีการทำ Redundancy มีประสิทธิภาพใช้งานทดแทนได้ทันที	มีระบบเครือข่าย 1 จุดที่ไม่มีการทำ Redundancy	มีระบบเครือข่ายมากกว่า 1 จุดที่ไม่มีการทำ Redundancy	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - Network diagram ของระบบ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
56	Technology	การ Monitor Capacity ของระบบบริการ Digital ID	มีเครื่องมือในการ Monitor และมีการแจ้งเตือนหากมีความเสี่ยงที่จะใช้ทรัพยากรมากเกินกว่ากำหนดอัตโนมัติ	มีเครื่องมือในการ Monitor แต่ไม่มีการตั้งค่าหรือกระบวนการแจ้งเตือนอัตโนมัติ	ไม่มีเครื่องมือหรือกระบวนการในการ Monitoring	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - ขั้นตอนการ Monitor capacity ภายในขององค์กร - แผนการคาดการณ์การเติบโตของระบบหรือแผนการเพิ่มทรัพยากรของระบบ Digital ID	
57	Technology	การ Monitor Log เช่น Access Log, Error Log รวมไปถึง Security log ของระบบบริการ Digital ID	มีเครื่องมือในการ Monitoring และมีการแจ้งเตือนหากพบเจอเหตุการณ์ผิดปกติอัตโนมัติ	มีเครื่องมือหรือกระบวนการในการ Monitoring แต่ไม่มีการตั้งค่าหรือกระบวนการแจ้งเตือนอัตโนมัติ	ไม่มีเครื่องมือหรือกระบวนการในการ Monitoring	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - ขั้นตอนการ Monitor Log ภายในขององค์กร - อุปกรณ์ที่ใช้ในการ Monitor Log ของระบบ Digital ID	
58	Technology	มีการอนุญาตให้นำอุปกรณ์ส่วนตัวของพนักงาน (BYOD) เชื่อมต่อเข้าระบบงานภายในขององค์กรหรือไม่	ไม่อนุญาตให้ใช้อุปกรณ์ส่วนตัวในการเชื่อมต่อเข้าระบบงานขององค์กร	พนักงานต้องมีการร้องขอการใช้อุปกรณ์ส่วนตัวในการเชื่อมต่อเข้าระบบงานขององค์กร และ	พนักงานทุกคนสามารถใช้อุปกรณ์ส่วนตัวในการเชื่อมต่อเข้าระบบงานขององค์กรได้และสามารถ	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - ขั้นตอนการขอใช้อุปกรณ์ส่วนตัวของพนักงาน (BYOD) เชื่อมต่อเข้าระบบงานภายในขององค์กร	อุปกรณ์ส่วนตัว (BYOD) หมายถึง อุปกรณ์อิเล็กทรอนิกส์ส่วนตัวของพนักงาน อาทิเช่น Laptop, โทรศัพท์มือถือ, Tablet หรือ USB Thumb drive ที่พนักงานนำมาใช้งาน

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
				เข้าถึงระบบงานขององค์กรเท่าที่จำเป็น	เข้าถึงข้อมูลสำคัญขององค์กรได้			
59	Technology	จำนวนเครื่องที่ใช้ปฏิบัติงานของบริษัท (Endpoints) รวมถึงอุปกรณ์ส่วนตัว BYOD (ถ้ามี) ที่เกี่ยวข้องกับการให้บริการ Digital ID	น้อยกว่า 100 เครื่อง	100 - 1000 เครื่อง	มากกว่า 1000 เครื่อง	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - ทะเบียนอุปกรณ์ BYOD ที่ใช้งานภายในองค์กร	
60	Technology	จำนวน Domain และ Subdomain Website ขององค์กรที่เข้าถึงได้จาก Internet ที่เกี่ยวข้องกับการให้บริการ Digital ID	น้อยกว่า 2 Domains	2-10 Domains	มากกว่า 10 Domains	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - รายชื่อ Domain ที่ใช้งานเพื่อให้บริการระบบ Digital ID	

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
61	Technology	กระบวนการสำรองข้อมูลที่เกี่ยวข้องกับระบบบริการ Digital ID	องค์กรมีแผนปฏิบัติงานการสำรองข้อมูลและแผนการกู้คืนข้อมูลที่เกี่ยวข้องกับระบบ Digital ID โดยมีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง	องค์กรมีแผนปฏิบัติงานการสำรองข้อมูลและแผนการกู้คืนข้อมูลที่เกี่ยวข้องกับระบบ Digital ID แต่ยังไม่มีการทดสอบการกู้คืนข้อมูล	องค์กรมีแผนปฏิบัติงานการสำรองข้อมูลและแผนการกู้คืนข้อมูลแต่ยังไม่ครอบคลุมระบบ Digital ID	ALL (IDP, DPIS)	เอกสารที่แสดงถึง - ขั้นตอนในการสำรองข้อมูลของระบบ Digital ID	

ส่วนที่ 2
คำถามเพิ่มเติมสำหรับ AUTH

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
62	Operational, Reputation	ระดับความน่าเชื่อถือของการยืนยันตันตน (AAL) สูงสุดที่องค์กรสามารถให้บริการ	N/A	AAL2	AAL3	AUTH	- หลักฐานแสดงระดับ AAL ที่ให้บริการ	
63	Operational, Reputation	เป้าหมาย จำนวน RP, AS รวมทั้งหมดที่มีการเชื่อมต่อเพื่อให้บริการ Digital ID นับถัดจากวันประเมินไป 1 ปี	น้อยกว่า 10 ราย	10 - 50 ราย	มากกว่า 50 ราย	AUTH	- หลักฐานแสดงจำนวน RP, AS ที่มีการเชื่อมต่อเพื่อให้บริการ Digital ID ในปัจจุบัน และระบุเป้าหมายในอีก 1 ปี	
64	Operational, Reputation	เป้าหมาย จำนวน transaction รวมต่อปีสำหรับการยืนยันตัวตนบนระบบบริการ Digital ID นับถัดจากวันประเมินไป 1 ปี	น้อยกว่า 200,000 รายการ	200,000 - 500,000 รายการ	มากกว่า 500,000 รายการ	AUTH	- หลักฐานแสดงจำนวน transaction การยืนยันตัวตนบนระบบบริการ Digital ID ต่อปีในปัจจุบัน และระบุเป้าหมายในอีก 1 ปี	

ส่วนที่ 3
คำถามเพิ่มเติมสำหรับ IDPRF

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
65	Operational, Reputation	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) สูงสุดที่องค์กรสามารถให้บริการ	IAL2.1, IAL2.2	IAL2.3	IAL3	IDPRF	- หลักฐานแสดงระดับ IAL ที่ให้บริการ	
66	Operational, Technology, Reputation	เป้าหมาย จำนวนจุดให้บริการการพิสูจน์ตัวตนรวมทั้งหมดที่อยู่ในความดูแลของหน่วยงาน เช่น ตู้ kiosk, ตู้ ATM, เคาน์เตอร์สาขา นับถัดจากวันประเมินไป 1 ปี	น้อยกว่า 1,000 จุด	1,000-10,000 จุด	มากกว่า 10,000 จุด	IDPRF	- หลักฐานแสดงจำนวนจุดให้บริการการพิสูจน์ตัวตนในความดูแลของหน่วยงาน และระบุเป้าหมายในอีก 1 ปี	ในความดูแลของหน่วยงาน หมายถึง ที่ให้บริการโดยหน่วยงาน หรือ ที่ให้บริการโดยบุคคลภายนอกภายใต้การกำกับของหน่วยงาน (เฉพาะกรณีที่บุคคลภายนอก ไม่ใช่ผู้ประกอบธุรกิจบริการเกี่ยวกับ Digital ID ที่ต้องได้รับใบอนุญาตจาก สพธอ.)

ส่วนที่ 4
คำถามเพิ่มเติมสำหรับ DIPS

No.	ประเภทความเสี่ยง	คำถามและความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยงตั้งต้น			ผู้ประเมิน	หลักฐานประกอบผลการประเมิน	หมายเหตุ
			ต่ำ	ปานกลาง	สูง			
67	Operational, Reputation	เป้าหมาย จำนวน IDP รวมทั้งหมดที่มีการเชื่อมต่อเพื่อให้บริการ Digital ID นับถัดจากวันประเมินไป 1 ปี	น้อยกว่า 6 ราย	6 - 20 ราย	มากกว่า 20 ราย	DIPS	- หลักฐานแสดงจำนวน IDP ที่มีการเชื่อมต่อเพื่อให้บริการ Digital ID ในปัจจุบัน และระบุเป้าหมายในอีก 1 ปี	
68	Operational, Reputation	เป้าหมาย จำนวน transaction รวมต่อปี สำหรับการยืนยันตัวตนบนระบบบริการ Digital ID นับถัดจากวันประเมินไป 1 ปี	น้อยกว่า 10,000 รายการ	10,000 - 2,000,000 รายการ	มากกว่า 2,000,000 รายการ	DIPS	- หลักฐานแสดงจำนวน transaction การยืนยันตัวตนบนระบบบริการ Digital ID ต่อปีในปัจจุบัน และระบุเป้าหมายในอีก 1 ปี	