

คู่มือการใช้งาน
เครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยง
เพื่อใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ
(Assessment Tool for Government Digital ID)

ฉบับผู้ประเมิน
(Version 1.3.7)

เสนอ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
โดย บริษัท สกาย อาย เทค จำกัด



คำนำ

คู่มือฉบับนี้มีจุดประสงค์เพื่อให้คำแนะนำ วิธีการใช้งาน ตลอดจนวิธีการอ่านผลลัพธ์จากการคำนวณ ประกอบการใช้งานเครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยงเพื่อใช้ในการพิสูจน์และยืนยันตัวตนสำหรับบริการภาครัฐ ซึ่งถูกจัดทำขึ้นเพื่ออำนวยความสะดวกให้เจ้าหน้าที่ของรัฐสามารถใช้ประเมินความเสี่ยงบริการสารสนเทศของหน่วยงาน รวมทั้งสามารถเลือกระดับความความน่าเชื่อถือที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนได้อย่างเหมาะสม โดยอ้างอิงตามมาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐสำหรับบุคคลธรรมดาที่มีสัญชาติไทย ได้แก่ มรด. ๑-๑: ๒๕๖๔ และ มรด. ๑-๒: ๒๕๖๔ ที่ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 11 ตุลาคม 2564 ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สารบัญ

บทที่ 1	รายละเอียดมาตรฐานที่ใช้ในการพัฒนาเครื่องมือฯ	1
1.1	ระดับความน่าเชื่อถือ (Assurance Levels).....	1
1.2	ประเภทบริการภาครัฐ.....	1
1.3	คำแนะนำก่อนการใช้งานเครื่องมือฯ	2
1.4	ภาพรวมของเครื่องมือฯ.....	3
1.5	วิธีการติดตั้งเครื่องมือ	4
บทที่ 2	บันทึกข้อมูลผู้ประเมินและบริการที่ถูกประเมิน (หน้าแรก).....	5
2.1	การกรอกข้อมูลผู้ประเมินความเสี่ยง	5
2.2	การกรอกข้อมูลในตารางข้อมูลบริการและผู้ให้บริการที่ถูกประเมิน	6
2.3	ตารางแสดงวิธีการใช้เครื่องมือประเมินความเสี่ยง.....	6
2.4	การอ่านข้อมูลจากตารางระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ	9
บทที่ 3	การประเมินระดับความน่าเชื่อถือจากประเภทบริการภาครัฐ (STEP 1)	11
3.1	ตารางประเภทของบริการ	11
3.2	ตารางแสดงระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร.	12
3.3	ตารางแสดงข้อมูลประเภทบริการภาครัฐ	12
บทที่ 4	การประเมินระดับผลกระทบที่เป็นไปได้และระดับความเป็นไปได้ (STEP 2).....	14
4.1	การเลือกระดับผลกระทบที่เป็นไปได้และระดับความเป็นไปได้ (STEP 2).....	15
4.2	ตารางแสดงข้อมูลระดับความเสี่ยง.....	17
4.3	ตารางแสดงข้อมูลความเสี่ยงของผลกระทบ	17
บทที่ 5	การประเมินระดับความน่าเชื่อถือจากความเสี่ยงของผลกระทบที่อาจเกิดขึ้น (STEP 3)	19
5.1	ตารางการกำหนดระดับความน่าเชื่อถือ.....	19
5.2	ตารางระดับความน่าเชื่อถือขั้นต่ำที่แนะนำจากระดับความเสี่ยง.....	20
5.3	ตารางระดับความน่าเชื่อถือขั้นต่ำที่แนะนำจากระดับผลกระทบที่เป็นไปได้.....	20

บทที่ 6	สรุประดับผลกระทบที่เป็นไปได้ (หน้าสรุป)	22
บทที่ 7	แสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด (หน้า Printout).....	25
	7.1 หน้าที่ 1.....	25
	7.2 หน้าที่ 2.....	27
	7.3 หน้าที่ 3.....	28
บทที่ 8	การแสดงผลละเอียดวิธีการคำนวณและเกณฑ์การให้คะแนน (ข้อมูลเพิ่มเติม)	29
บทที่ 9	การแสดงผลตัวอย่างเพื่ออำนวยความสะดวกในการกรอกแผ่นงาน STEP 2.....	32
บทที่ 10	ตัวอย่างการกรอกข้อมูล	38

บทที่ 1 รายละเอียดมาตรฐานที่ใช้ในการพัฒนาเครื่องมือฯ

เครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยงเพื่อใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ ถูกพัฒนาขึ้นโดยการศึกษาและอ้างอิงตามมาตรฐานรัฐบาลดิจิทัล ดังนี้

- มรด. ๑ - ๑ : ๒๕๖๔ ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ - ภาพรวม
- มรด. ๑ - ๒ : ๒๕๖๔ ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ - การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

นอกจากนี้ ได้ทำการศึกษาเพิ่มเติมเกี่ยวกับมาตรฐานระดับความน่าเชื่อถือของการแลกเปลี่ยนข้อมูลระหว่างองค์กร (federated assurance level: FAL) จาก NIST Special Publication 800-63C: Digital Identity Guidelines – Federation and Assertions

1.1 ระดับความน่าเชื่อถือ (Assurance Levels)

1. ระดับความน่าเชื่อถือของไอดีเนทีตี (identity assurance level: IAL) คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของผู้สมัครใช้บริการ โดยกำหนดระดับความน่าเชื่อถือของไอดีเนทีตีที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด
2. ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL) คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ โดยกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด
3. ระดับความน่าเชื่อถือของการแลกเปลี่ยนข้อมูลระหว่างองค์กร (federated assurance level: FAL) คือ ระดับความเข้มงวดในการยืนยันตัวตนผู้ให้บริการ โดยทำการแลกเปลี่ยนข้อมูลการยืนยันตัวตนและข้อมูลส่วนตัวของผู้ใช้งาน ระหว่างผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) และผู้ให้บริการภาครัฐ (relying party: RP)

1.2 ประเภทบริการภาครัฐ

1. กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services) คือ บริการเผยแพร่ข้อมูลข่าวสารทั่วไปของหน่วยงานของรัฐ เช่น นโยบายสาธารณะ การกำกับดูแล กฎหมาย ระเบียบ เอกสาร

ที่เกี่ยวข้อง และประเภทการให้บริการภาครัฐ ผ่านทาง เว็บไซต์หรือช่องทางให้บริการข้อมูล ข่าวสารอื่น

2. กลุ่มการให้บริการข้อมูลที่มีปฏิสัมพันธ์กับผู้ใช้บริการ (Enhanced Services) คือ บริการข้อมูล ข่าวสารของหน่วยงานของรัฐในรูปแบบการสื่อสารทางเดียวหรือสองทางกับผู้ใช้บริการ เช่น การรับแจ้งเรื่องร้องเรียน ข้อเสนอแนะ หรือแสดงความคิดเห็น ผ่านทางเว็บไซต์หรือ ช่องทาง ให้บริการข้อมูลข่าวสารอื่น
3. กลุ่มการให้บริการธุรกรรม (Transactional Services) คือ บริการธุรกรรมของหน่วยงานของ รัฐซึ่งมีผลผูกพันทางกฎหมาย เช่น การอนุญาต การจดทะเบียน หรือการดำเนินการใด ๆ กับ หน่วยงานของรัฐ
4. กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน (Connected Services) คือ บริการธุรกรรมที่มีการเชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง และมีผลผูกพันทาง กฎหมาย เช่น การขอรับบริการภาครัฐแบบเบ็ดเสร็จ ณ จุดเดียว

1.3 คำแนะนำก่อนการใช้งานเครื่องมือฯ

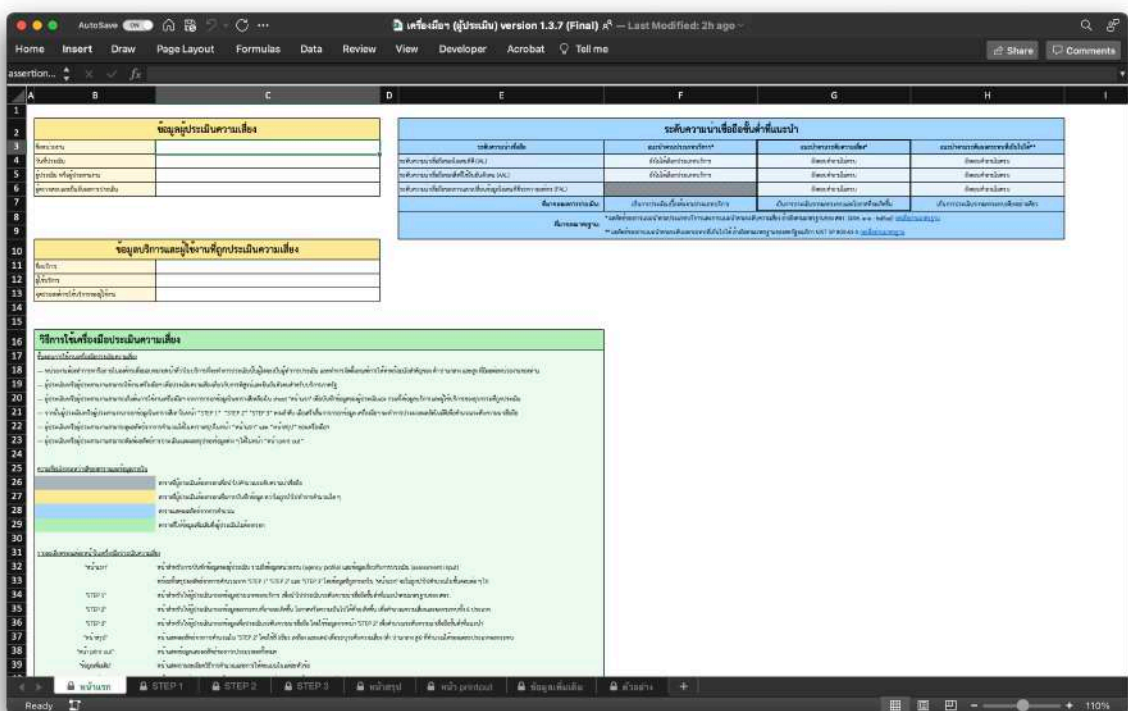
เพื่อให้หน่วยงานภาครัฐสามารถใช้เครื่องมือฯ ได้อย่างราบรื่นและได้รับผลลัพธ์ที่ถูกต้อง แม่นยำจากการคำนวณ หน่วยงานภาครัฐควรทำการหารือร่วมกันระหว่างผู้ที่เกี่ยวข้อง ก่อนเริ่ม ใช้งานเครื่องมือ โดยมีประเด็นที่จำเป็นต้องหาข้อสรุปร่วมกัน ดังนี้

1. กำหนดผู้รับผิดชอบการผู้ประเมิน (บุคคล หรือคณะทำงาน) และแต่งตั้งผู้ตรวจสอบการ ประเมินสำหรับแต่ละบริการเพื่อตรวจสอบความถูกต้องในการประเมิน
2. กำหนดระยะเวลาเพื่อทำการประเมินในแต่ละครั้ง เช่น จะมีการประเมินรายปี หรือทุกครั้งที่มีการอัปเดตระบบหรือมีการเปลี่ยนแปลงกับบริการ
3. กรณีที่หน่วยงานมีบริการมากกว่าหนึ่งบริการ ให้หน่วยงานประเมินแต่ละบริการแยกออกจาก กันตามความเหมาะสม
4. กำหนดเกณฑ์การวัดระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด (impact level) ทั้ง 6 ประเภท เกณฑ์การวัดระดับโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น (likelihood level) และเกณฑ์การวัดผลความเสี่ยง (risk evaluation) ตามเกณฑ์อ้างอิงจาก มรต. ๑-๑: ๒๕๖๔ ทั้งนี้ ผู้ประเมินสามารถกำหนดเกณฑ์อื่น ๆ เพิ่มเติมได้อีกตามความเหมาะสม โดยอ้างอิงจาก มาตรฐานสากลอื่น ๆ เช่น ISO 27000

- สำรวจบริการของหน่วยงานที่ต้องการประเมิน ว่าเป็นบริการภาครัฐประเภทใด (บริการข้อมูลพื้นฐาน บริการข้อมูลที่มีปฏิสัมพันธ์กับผู้ใช้บริการ บริการธุรกรรม และ บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน) ตามเกณฑ์อ้างอิงจาก มรต. ๑ – ๑ : ๒๕๖๔

1.4 ภาพรวมของเครื่องมือฯ

เครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยงเพื่อใช้ในการพิสูจน์และยืนยันตัวตนสำหรับบริการภาครัฐ (Assessment Tool for Government Digital ID) เป็นไฟล์ Excel (.xlsx) ซึ่งสามารถดาวน์โหลดและติดตั้งโดยการสำเนาไปวางในโฟลเดอร์งานในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ซึ่งผู้ประเมินสามารถพิจารณาเปลี่ยนชื่อไฟล์ให้เหมาะสมกับบริการ ครั้งที่ประเมิน ปีที่ประเมิน เป็นต้น



รูปที่ 1 ลักษณะของเครื่องมือฯ

ในแต่ละแผ่นงานของเครื่องมือฯ มีหน้าที่การใช้งานดังนี้

- **หน้าแรก:** หน้าสำหรับการบันทึกข้อมูลของผู้ประเมิน ข้อมูลบริการที่ถูกประเมินและผลลัพธ์จากการคำนวณจาก “STEP 1”, “STEP 2” และ “STEP 3”
- **STEP 1:** หน้าสำหรับให้ผู้ประเมินกรอกข้อมูลประเภทของบริการ เพื่อนำไปประเมินระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร.

- STEP 2: หน้าสำหรับให้ผู้ประเมินกรอกข้อมูลระดับผลกระทบที่เป็นไปได้ที่อาจเกิดขึ้น โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น เพื่อกำหนดความเสี่ยงและระดับผลกระทบทั้ง 6 ด้าน
- STEP 3: หน้าสำหรับให้ผู้ประเมินตอบคำถาม เพื่อแสดงระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ
- หน้าสรุป: หน้าแสดงผลลัพธ์จากการคำนวณใน “STEP 2” โดยการกำหนดสี (เขียว เหลือง และแดง) เพื่ออธิบายถึงระดับความเสี่ยง (ต่ำ ปานกลาง สูง)
- Printout: หน้าแสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด
- ข้อมูลเพิ่มเติม: หน้าแสดงรายละเอียดวิธีการคำนวณและเกณฑ์การให้คะแนนในแต่ละหัวข้อ
- ตัวอย่าง: หน้าแสดงตัวอย่างระดับผลกระทบที่เป็นไปได้ของแต่ละเหตุการณ์อันเป็นความเสี่ยง

1.5 วิธีการติดตั้งเครื่องมือ

เนื่องจากเครื่องมือฯ อยู่ในรูปแบบ Microsoft Excel จึงทำให้ผู้ใช้งานสามารถติดตั้งได้ง่ายตามขั้นตอนดังต่อไปนี้

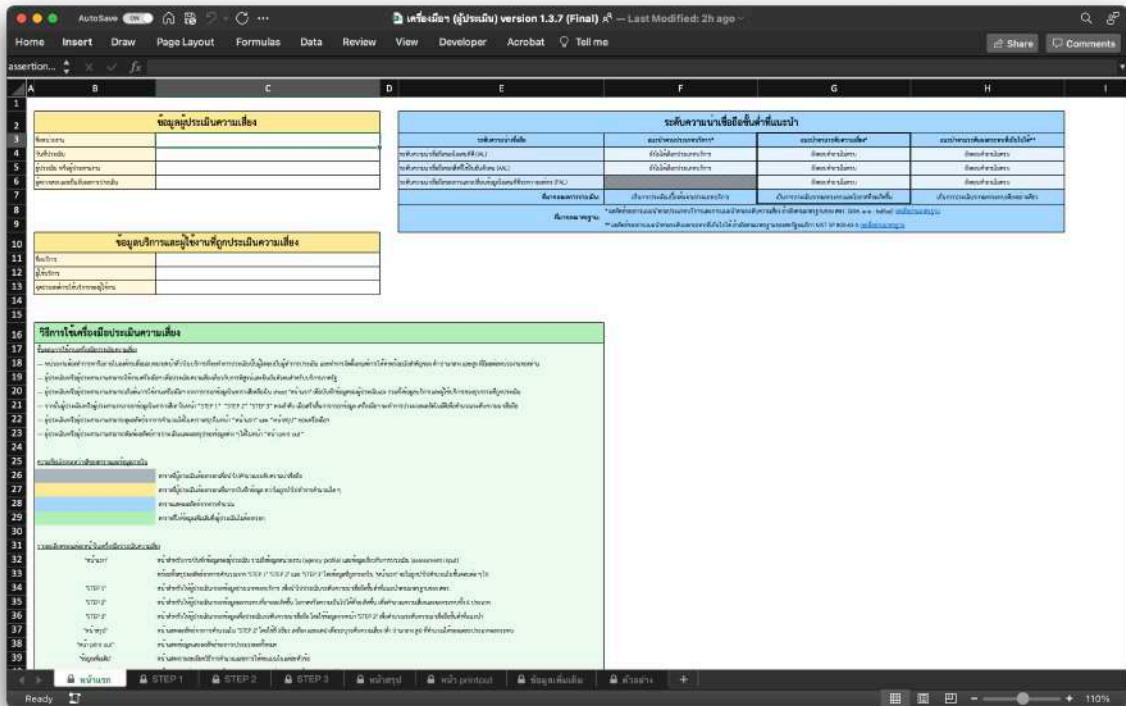
1. ดาวน์โหลดไฟล์เครื่องมือฯ จากแหล่งที่มา (อาทิ เช่น ลิงค์บนอินเทอร์เน็ต หรือไฟล์แนบจากอีเมล)
2. เปิดใช้โปรแกรม Microsoft Excel เวอร์ชัน 2016 ขึ้นไป หรือหากยังไม่ได้ติดตั้ง ให้ติดตั้งโปรแกรม Microsoft Excel ที่มาพร้อมกับ Microsoft Office 365 จากเว็บไซต์ office.com พร้อมทั้งลงทะเบียนเข้าใช้งานก่อน
3. คลิกขวาเพื่อกดเปลี่ยนชื่อ โดยตั้งชื่อไฟล์ให้ง่ายต่อการจดจำและสะดวกต่อการใช้งาน
4. คลิกขวาสองครั้งเพื่อทำการเปิดไฟล์เครื่องมือฯ ด้วยโปรแกรม Microsoft Excel

หากไฟล์เครื่องมือฯ ที่เปิด แสดงผลอยู่ใน “มุมมองที่ได้รับการป้องกัน” (Protected View) ให้คลิกปุ่ม “เปิดใช้งานการแก้ไข” (Enable Editing) ที่แสดงไว้อย่างเด่นชัดใต้แถบเครื่องมือของโปรแกรม¹ เพื่อเริ่มใช้งาน

¹ Microsoft, “มุมมองที่ได้รับการป้องกันคืออะไร” <support.microsoft.com/th-th/topic/มุมมองที่ได้รับการป้องกันคืออะไร-d6f09ac7-e6b9-4495-8e43-2bbcbcb6653>

บทที่ 2 บันทึกข้อมูลผู้ประเมินและบริการที่ถูกประเมิน (หน้าแรก)

ในแผ่นงานแรก (Work Sheet) “หน้าแรก” เป็นหน้าสำหรับการบันทึกข้อมูลของผู้ประเมิน รวมถึงข้อมูลหน่วยงาน (Agency Profile) และข้อมูลบริการที่ถูกประเมิน รวมทั้งผลลัพธ์จากการคำนวณที่ได้จาก “STEP 1” “STEP 2” และ “STEP 3” โดยข้อมูลที่กรอกใน “หน้าแรก” เป็นเพียงข้อมูลที่บันทึกไว้อ้างอิง



รูปที่ 2 ลักษณะของแผ่นงาน “หน้าแรก”

2.1 การกรอกข้อมูลผู้ประเมินความเสี่ยง

ตารางสำหรับให้ผู้ประเมินกรอกและบันทึกข้อมูลผู้ประเมินความเสี่ยง ประกอบด้วย ชื่อหน่วยงาน วันที่ประเมิน ผู้ประเมินหรือผู้ประสานงาน และผู้ตรวจสอบและยืนยันผลการประเมิน ซึ่งข้อมูลในตารางนี้ ไม่ได้มีผลต่อการคำนวณในขั้นตอนถัด ๆ ไป ซึ่งข้อมูลปรากฏอยู่ในหน้า Printout เพื่อให้หน่วยงานสามารถพิมพ์ผลลัพธ์เก็บไว้อ้างอิง

ตารางที่ 1 ตารางข้อมูลผู้ประเมินความเสี่ยง

ข้อมูลผู้ประเมินความเสี่ยง	
ชื่อหน่วยงาน	
วันที่ประเมิน	
ผู้ประเมิน หรือผู้ประสานงาน	
ผู้ตรวจสอบและยืนยันผลการประเมิน	

2.2 การกรอกข้อมูลในตารางข้อมูลบริการและผู้ให้บริการที่ถูกประเมิน

ตารางสำหรับให้ผู้ประเมินกรอกข้อมูลบริการและผู้ให้บริการที่ถูกประเมินประกอบด้วย ชื่อบริการ ผู้ให้บริการ และจุดประสงค์การให้บริการ โดยช่องผู้ให้บริการผู้ประเมินสามารถเลือกรายการ”ประชาชนทั่วไป, เจ้าหน้าที่รัฐในหน่วยงาน, เจ้าหน้าที่รัฐนอกหน่วยงาน” จาก Dropdown List หรือพิมพ์ข้อความ ซึ่งข้อมูลในตารางนี้ไม่ได้มีผลต่อการคำนวณในขั้นตอนถัด ๆ ไป แต่จะปรากฏข้อมูลอยู่ในหน้า Printout เพื่อให้หน่วยงานสามารถพิมพ์ข้อมูลผลลัพธ์หลังการประเมินใช้เครื่องมือฯ เสร็จสิ้น

ตารางที่ 2 ตารางข้อมูลบริการและผู้ให้บริการ

ข้อมูลบริการและผู้ใช้งานที่ถูกประเมินความเสี่ยง	
ชื่อบริการ	
ผู้ให้บริการ	
จุดประสงค์การให้บริการของผู้ใช้งาน	

2.3 ตารางแสดงวิธีการใช้เครื่องมือประเมินความเสี่ยง

ตารางสำหรับอธิบายวิธีการใช้งานเครื่องมือฯ แบ่งเป็น 3 ส่วน

2.3.1 ขั้นตอนการใช้งานเครื่องมือฯ

- กรอกข้อมูลผู้ประเมิน ข้อมูลบริการที่ถูกประเมิน ในตารางสีเหลืองใน “หน้าแรก” และบันทึกข้อมูล
- กรอกข้อมูลหรือเลือกคำตอบจาก Dropdown List ที่กำหนดในตารางสีเทาใน “STEP 1” “STEP 2” และ “STEP 3” ตามลำดับเสร็จเรียบร้อยแล้ว หลังจากนั้นเครื่องมือจะประมวลผลอัตโนมัติและแสดงระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ

ทั้งนี้ ผู้ประเมินสามารถดูผลลัพธ์จากการประมวลผลอัตโนมัติได้ที่ “หน้าแรก” และ “หน้าสรุป” และสามารถพิมพ์ผลลัพธ์ผลลัพธ์จากการประมวลผลอัตโนมัติที่ “หน้า Printout” นอกจากนี้ผู้ประเมินสามารถดูการกำหนดเกณฑ์ สูตรการคำนวณ ความสัมพันธ์ระหว่างระดับผลกระทบที่เป็นไปได้ ระดับความเสี่ยง และโอกาสหรือความเป็นไปได้ พร้อมความหมายและคำอธิบายใน “ข้อมูลเพิ่มเติม” และยังมีตัวอย่างการวิเคราะห์ระดับผลกระทบที่เป็นไปได้ในแต่ละเหตุการณ์อันเป็นความเสี่ยงใน “ตัวอย่าง”

2.3.2 ความเชื่อมโยงระหว่างสีของตารางและข้อมูลที่อยู่ข้างในตารางนั้น ๆ

สีเหลือง	ตารางที่ผู้ประเมินต้องกรอกเพื่อนำไปคำนวณระดับความน่าเชื่อถือ
สีเทา	ตารางที่ผู้ประเมินต้องกรอกเพื่อการบันทึกข้อมูล ไม่ถูกนำไปทำการคำนวณใด ๆ
สีฟ้า	ตารางแสดงผลลัพธ์จากการคำนวณ
สีเขียว	ตารางที่ให้ข้อมูลเพิ่มเติมซึ่งผู้ประเมินไม่ต้องกรอก

2.3.3 รายละเอียดของแต่ละแผ่นงานในเครื่องมือฯ

“หน้าแรก”: หน้าสำหรับการบันทึกข้อมูลของผู้ประเมิน รวมถึงข้อมูลหน่วยงาน (Agency Profile) และข้อมูลเกี่ยวกับการประเมิน (Assessment Input) พร้อมทั้งสรุปผลลัพธ์จากการคำนวณจาก “STEP 1”, “STEP 2” และ “STEP 3” โดยข้อมูลที่ถูกรอกใน “หน้าแรก” จะไม่ถูกนำไปคำนวณในขั้นตอนต่อ ๆ ไป

“STEP 1”: หน้าสำหรับให้ผู้ประเมินเลือกประเภทของบริการภาครัฐทั้ง 4 กลุ่มจาก Dropdown List เพื่อนำไปประเมินระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร. พร้อมตารางอธิบายความหมายของแต่ละกลุ่มการให้บริการ

“STEP 2”: หน้าสำหรับให้ผู้ประเมินพิจารณาเลือกระดับผลกระทบที่เป็นไปได้ (ไม่มี ต่ำ ปานกลาง สูง) และระดับความเป็นไปได้หรือโอกาสที่จะเกิดขึ้น (โอกาสเกิดขึ้นต่ำ โอกาสเกิดขึ้นปานกลาง โอกาสเกิดขึ้นสูง) จาก Dropdown List โดยพิจารณาเหตุการณ์อันเป็นความเสี่ยง

- 1) หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น
- 2) หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน
- 3) หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน
- 4) หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน

หมายเหตุ

1. ผู้ใช้บริการ คือ ผู้ใช้บริการที่ได้ระบุไว้ใน “หน้าแรก”
2. ผลกระทบจากเหตุการณ์อันเป็นความเสี่ยงที่สามารถเกิดกับบุคคลหรือกับองค์กรหรือหลายฝ่าย อย่างไรก็ตามขอให้พิจารณาผลกระทบที่ได้รับมากที่สุด
3. ผู้ประเมินสามารถคลิกเพื่อดูตัวอย่างการวิเคราะห์ระดับผลกระทบที่เป็นไปได้ในแต่ละเหตุการณ์อันเป็นความเสี่ยง

“STEP 3”: หน้าสำหรับให้ผู้ประเมินตอบคำถาม (ใช่/ไม่ใช่, ไม่แน่ใจ) จาก Dropdown List เพื่อแสดงระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ โดยใช้ข้อมูลจาก “STEP 2” มาประกอบการประมวลผลด้วย




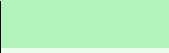
“หน้าสรุป”: หน้าแสดงผลลัพธ์จากการคำนวณผลกระทบใน “STEP 2” โดยสีเขียว คือไม่มีผลกระทบหรือผลกระทบต่ำ ระดับความเสี่ยงที่หน่วยงานสามารถยอมรับได้ สีเหลืองคือ ผลกระทบระดับปานกลาง ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยงให้ไปอยู่ในระดับต่ำ และสีแดง คือ ระดับความเสี่ยงที่หน่วยงานของรัฐไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกัน ไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย และเพื่อระบุระดับความเสี่ยง (ต่ำ ปานกลาง สูง) ที่ได้จากการคำนวณของผลกระทบทั้ง 6 ด้าน

“หน้า Printout”: หน้าแสดงข้อมูลและผลลัพธ์ของการประมวลผลของ “หน้าแรก” และหน้าสรุป”

“ข้อมูลเพิ่มเติม”: หน้าแสดงรายละเอียดวิธีการคำนวณ สูตรการคำนวณ การให้คะแนน การกำหนดเกณฑ์ และความสัมพันธ์ระหว่างระดับผลกระทบที่เป็นไปได้ ระดับความเสี่ยง และโอกาสหรือความเป็นไปได้

“ตัวอย่าง” หน้าแสดงตัวอย่างการวิเคราะห์ระดับผลกระทบที่เป็นไปได้ในแต่ละเหตุการณ์อันเป็นความเสี่ยงโดยใช้ตัวอย่างบริการภาครัฐ (รายละเอียดตามบทที่ 9 การแสดงตัวอย่างเพื่ออำนวยความสะดวกในการกรอกแผ่นงาน STEP 2)

ตารางที่ 3 แสดงวิธีการใช้เครื่องมือประเมินความเสี่ยง

วิธีการใช้เครื่องมือประเมินความเสี่ยง	
ขั้นตอนการใช้งานเครื่องมือประเมินความเสี่ยง	
<ul style="list-style-type: none"> หน่วยงานต้องทำการหารือภายในองค์กรเพื่อมอบหมายหน้าที่ว่าในบริการที่จะทำการประเมินนั้นผู้ใดจะเป็นผู้ทำการประเมิน และทำการจัดตั้งเกณฑ์การให้ค่าพร้อมนัยสำคัญของ ต่ำ ปานกลาง และสูง ที่มีผลต่อหน่วยงานของท่าน ผู้ประเมินหรือผู้ประสานงานสามารถใช้งานเครื่องมือฯ เพื่อประเมินความเสี่ยงเกี่ยวกับการพิสูจน์และยืนยันตัวตนสำหรับบริการภาครัฐ ผู้ประเมินหรือผู้ประสานงานสามารถเริ่มต้นการใช้งานเครื่องมือฯ จากการกรอกข้อมูลในตารางสีเหลืองใน sheet “หน้าแรก” เพื่อบันทึกข้อมูลของผู้ประเมินเอง รวมทั้งข้อมูลบริการและผู้ให้บริการของธุรกรรมที่ถูกประเมิน จากนั้นผู้ประเมินหรือผู้ประสานงานกรอกข้อมูลในตารางสีเทาในหน้า “STEP 1” “STEP 2” “STEP 3” ตามลำดับ เมื่อเสร็จสิ้นการกรอกข้อมูลเครื่องมือฯ จะทำการประมวลผลอัตโนมัติเพื่อคำนวณระดับความน่าเชื่อถือ ผู้ประเมินหรือผู้ประสานงานสามารถดูผลลัพธ์จากการคำนวณได้ในตารางสรุปในหน้า “หน้าแรก” และ “หน้าสรุป” ของเครื่องมือฯ ผู้ประเมินหรือผู้ประสานงานสามารถพิมพ์ผลลัพธ์การประเมินและผลสรุปของข้อมูลต่าง ๆ ได้ในหน้า “หน้า print out” 	
ความเชื่อมโยงระหว่างสีของตารางและข้อมูลภายใน	
	ตารางที่ผู้ประเมินต้องกรอกเพื่อนำไปคำนวณระดับความน่าเชื่อถือ
	ตารางที่ผู้ประเมินต้องกรอกเพื่อการบันทึกข้อมูล ไม่ถูกนำไปทำการคำนวณใด ๆ
	ตารางแสดงผลลัพธ์จากการคำนวณ
	ตารางที่ให้ข้อมูลเพิ่มเติมซึ่งผู้ประเมินไม่ต้องกรอก
“หน้าแรก”	หน้าสำหรับการบันทึกข้อมูลของผู้ประเมิน รวมถึงข้อมูลหน่วยงาน (agency profile) และข้อมูลเกี่ยวกับการประเมิน (assessment input) พร้อมทั้งสรุปผลลัพธ์จากการคำนวณจาก “STEP 1” “STEP 2” และ “STEP 3” โดยข้อมูลที่ถูกรอกใน “หน้าแรก” จะไม่ถูกนำไปคำนวณในขั้นตอนต่อ ๆ ไป
“STEP 1”	หน้าสำหรับให้ผู้ประเมินกรอกข้อมูลประเภทของบริการ เพื่อนำไปประเมินระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร.
“STEP 2”	หน้าสำหรับให้ผู้ประเมินกรอกข้อมูลผลกระทบที่อาจเกิดขึ้น โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น เพื่อคำนวณความเสี่ยงและผลกระทบทั้ง 6 ประเภท
“STEP 3”	หน้าสำหรับให้ผู้ประเมินกรอกข้อมูลเพื่อประเมินระดับความน่าเชื่อถือ โดยใช้ข้อมูลจากหน้า “STEP 2” เพื่อคำนวณระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ
“หน้าสรุป”	หน้าแสดงผลลัพธ์จากการคำนวณใน “STEP 2” โดยใช้สี (เขียว เหลือง และแดง) เพื่อระบุระดับความเสี่ยง (ต่ำ ปานกลาง สูง) ที่คำนวณได้ของแต่ละประเภทผลกระทบ
“หน้า printout”	หน้าแสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด
“ข้อมูลเพิ่มเติม”	หน้าแสดงรายละเอียดวิธีการคำนวณและการให้คะแนนในแต่ละหัวข้อ
“ตัวอย่าง”	หน้าแสดงตัวอย่างการวิเคราะห์ระดับผลกระทบที่เป็นไปได้ของแต่ละเหตุการณ์อันเป็นความเสี่ยง

2.4 การอ่านข้อมูลจากตารางระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ

ตารางสรุปผลลัพธ์ของการคำนวณที่ได้จาก ข้อมูลในแผ่นงาน “STEP 1” “STEP 2” และ “STEP 3” โดยผลลัพธ์ถูกแบ่งออกเป็นสามแถวจากการคำนวณตามช่องแนะนำประกอบด้วย ช่องแนะนำตามประเภท

บริการ: เป็นผลจากการประเมินเบื้องต้น ซึ่งขั้นต่ำของระดับความน่าเชื่อถือของไอเดนทิตี และระดับความน่าเชื่อถือของสิ่งที่ยืนยันตัวตนที่จำแนกตามกลุ่มการให้บริการภาครัฐ อ้างอิงตาม มรด. ๑-๒ : ๒๕๖๔

ช่องแนะนำตามระดับความเสี่ยง: เป็นผลจากการประเมินจากผลกระทบและโอกาสที่เกิดขึ้น ซึ่งเป็นผลลัพธ์ที่อ้างอิงตาม มรด. ๑ - ๑ : ๒๕๖๔ โดยผลการประเมินความเสี่ยงมาประกอบการพิจารณาระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL) หรือระดับความเข้มงวดของกระบวนการพิสูจน์ตัวตน และระดับความเข้มงวดของกระบวนการยืนยันตัวตน หรือระดับความน่าเชื่อถือของสิ่งที่ยืนยันตัวตน (Authenticator Assurance Level: AAL)

ช่องแนะนำตามระดับผลกระทบที่เป็นไปได้: เป็นการประเมินจากผลกระทบเพียงอย่างเดียว ซึ่งเป็นผลลัพธ์ที่อ้างอิงตามมาตรฐานของสหรัฐอเมริกา NIST SP 800-63-3

ทั้งนี้ ผู้ประเมินสามารถศึกษามาตรฐานที่เกี่ยวข้องเพิ่มเติมโดยการ”คลิกเพื่ออ่านมาตรฐาน” ในช่องแหล่งที่มาของมาตรฐาน

ตารางที่ 4 ตารางแสดงระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ

ระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ			
ระดับความน่าเชื่อถือ	แนะนำตามประเภทบริการ*	แนะนำตามระดับความเสี่ยง*	แนะนำตามระดับผลกระทบที่เป็นไปได้**
ระดับความน่าเชื่อถือของไอเดนทิตี (IAL)	ยังไม่ได้เลือกประเภทบริการ	ยังตอบคำถามไม่ครบ	ยังตอบคำถามไม่ครบ
ระดับความน่าเชื่อถือของสิ่งที่ยืนยันตัวตน (AAL)	ยังไม่ได้เลือกประเภทบริการ	ยังตอบคำถามไม่ครบ	ยังตอบคำถามไม่ครบ
ระดับความน่าเชื่อถือของการแลกเปลี่ยนข้อมูลไอเดนทิตีระหว่างองค์กร (FAL)		ยังตอบคำถามไม่ครบ	ยังตอบคำถามไม่ครบ
ที่มาของผลการประเมิน:	เป็นการประเมินเบื้องต้นตามประเภทบริการ	เป็นการประเมินจากผลกระทบและโอกาสที่จะเกิดขึ้น	เป็นการประเมินจากผลกระทบเพียงอย่างเดียว
ที่มาของมาตรฐาน:	* ผลลัพธ์ของการแนะนำตามประเภทบริการและการแนะนำตามระดับความเสี่ยง อ้างอิงตามมาตรฐานของ สพร. (มรด. ๑-๑ : ๒๕๖๔) กดเพื่ออ่านมาตรฐาน ** ผลลัพธ์ของการแนะนำตามระดับผลกระทบที่เป็นไปได้ อ้างอิงตามมาตรฐานของสหรัฐอเมริกา NIST SP 800-63-3 กดเพื่ออ่านมาตรฐาน		

บทที่ 3 การประเมินระดับความน่าเชื่อถือจากประเภทบริการภาครัฐ (STEP 1)

ตารางสำหรับให้ผู้ประเมินกรอกประเภทของบริการที่ถูกประเมินความเสี่ยง ซึ่งข้อมูลที่กรอกจะเป็นตัวกำหนดระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร. โดยผู้ประเมินสามารถเลือกข้อมูลได้จาก dropdown list ได้แก่ กลุ่มการให้บริการข้อมูลพื้นฐาน กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ กลุ่มการให้บริการธุรกรรม และกลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน ซึ่งการพิจารณาเลือกกลุ่มการให้บริการสามารถศึกษารายละเอียดในตารางข้อมูลประเภทบริการภาครัฐ

STEP 1		ข้อมูลประเภทบริการภาครัฐ		
บริการที่ผู้ประเมิน ใช้งานเป็นประจำบนเทคโนโลยีสารสนเทศที่ใช้งานจริง		กลุ่มการให้บริการข้อมูลพื้นฐาน (Essential Service)	บริการที่มีหน่วยงานราชการที่เกี่ยวข้อง ไม่จำเป็นต้องใช้ข้อมูลบุคคล ไม่จำเป็นต้องมีการขอข้อมูลและพิสูจน์ตัวตน	
ระดับความน่าเชื่อถือของข้อมูล (UL)		กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ให้บริการ (Enhanced Service)	บริการที่มีการติดต่อกับผู้ให้บริการ ใช้ข้อมูลส่วนบุคคล หรือไม่ได้ใช้เราเตอร์ข้อมูล ไม่จำเป็นต้องมีผู้ดำเนินการ มีการขอข้อมูลและพิสูจน์ตัวตนผู้ใช้บริการ หรือไม่ได้ ใช้เทคโนโลยีการพิสูจน์ตัวตน	
ระดับความน่าเชื่อถือของข้อมูล (UL)		กลุ่มการให้บริการธุรกรรม (Transactional Service)	ต้องใช้ข้อมูลส่วนบุคคล (เช่น เลขประจำตัวประชาชน 13 หลัก) โดยไม่ต้องขอข้อมูลบุคคล ต้องดำเนินการขอ ๒ ชนิด ข้อมูลการขอเป็นเอกสารดิจิทัล (เช่น แอปพลิเคชัน หรือ อีเมล) ข้อมูลในเอกสารดิจิทัล (เช่น แอปพลิเคชัน หรือ อีเมล)	
ระดับความน่าเชื่อถือของข้อมูล (UL)		กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงระหว่างหน่วยงาน (Connected Service)	ต้องใช้ข้อมูลส่วนบุคคล (เช่น เลขประจำตัวประชาชน 13 หลัก) โดยไม่ต้องขอข้อมูลบุคคล ต้องดำเนินการขอ ๒ ชนิด หรือมีการเชื่อมโยง ข้อมูลการขอเป็นเอกสารดิจิทัล (เช่น แอปพลิเคชัน หรือ อีเมล) โดยไม่ต้องดำเนินการขอข้อมูลบุคคล (เช่น แอปพลิเคชัน หรือ อีเมล) ข้อมูลในเอกสารดิจิทัล (เช่น แอปพลิเคชัน หรือ อีเมล)	

รูปที่ 3 ประเมินระดับความน่าเชื่อถือจากประเภทบริการภาครัฐ (STEP 1)

3.1 ตารางประเภทของบริการ

การเลือกประเภทบริการ จาก Dropdown List ซึ่งประกอบด้วย

- กลุ่มการให้บริการข้อมูลพื้นฐาน
- กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ให้บริการ
- กลุ่มการให้บริการธุรกรรม

- กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน

ตารางที่ 5 ประเมินระดับความน่าเชื่อถือจากประเภทบริการภาครัฐ (STEP 1)

STEP 1	
บริการที่ถูกประเมิน จัดว่าเป็นบริการประเภทใด ตามตารางสีเขียวด้านขวานี้	
ประเภทของบริการ	

3.2 ตารางแสดงระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร.

ตารางแสดงผลลัพธ์โดยเมื่อผู้ประเมินทำการเลือก dropdown list ใน “STEP 1” เป็นที่เรียบร้อยแล้ว จะแสดงระดับความน่าเชื่อถือของไอเดนทิตี (IAL) และระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) ที่แนะนำจะขึ้นมาให้โดยอัตโนมัติ ตามคำแนะนำในมาตรฐาน มรด. ๑ – ๒ : ๒๕๖๔

ตารางที่ 6 ตารางแสดงระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ

ระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร.	
ประเภทระดับความน่าเชื่อถือ	ระดับความน่าเชื่อถือขั้นต่ำ
ระดับความน่าเชื่อถือของไอเดนทิตี (IAL)	ยังไม่ได้เลือกประเภทบริการ
ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL)	ยังไม่ได้เลือกประเภทบริการ

3.3 ตารางแสดงข้อมูลประเภทบริการภาครัฐ

ตารางแสดงข้อมูลเพิ่มเติมอธิบายข้อกำหนดสำหรับแต่ละประเภทบริการภาครัฐ ซึ่งประกอบด้วย 4 กลุ่มการให้บริการ โดยอ้างอิงตามมาตรฐานที่ สพร. กำหนด ได้แก่

1. กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services) คือ การให้บริการเผยแพร่ข้อมูลข่าวสารทั่วไปของหน่วยงานของรัฐ เช่น นโยบายสาธารณะ การกำกับดูแล กฎหมาย ระเบียบ เอกสารที่เกี่ยวข้อง และประเภทการให้บริการภาครัฐ ผ่านทางเว็บไซต์หรือช่องทางให้บริการข้อมูลข่าวสารอื่น
2. กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ (Enhanced Services) คือการให้บริการข้อมูลข่าวสารของหน่วยงานของรัฐในรูปแบบการสื่อสารทางเดียวหรือสองทางกับ

ผู้ใช้บริการ เช่น การรับแจ้งเรื่องร้องเรียน ข้อเสนอแนะ หรือแสดงความคิดเห็น ผ่านทางเว็บไซต์หรือช่องทางให้บริการข้อมูลข่าวสารอื่น

3. กลุ่มการให้บริการธุรกรรม (Transactional Services) คือ การให้บริการธุรกรรมของหน่วยงานของรัฐซึ่งมีผลผูกพันทางกฎหมาย เช่น การอนุญาต การจดทะเบียน หรือการดำเนินการใด ๆ กับหน่วยงานของรัฐ
4. กลุ่มการให้บริการธุรกรรมที่ เชื่อมโยงข้อมูลระหว่างหน่วยงาน (Connected Services) คือ การให้บริการธุรกรรมที่มีการเชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง และมีผลผูกพันทางกฎหมาย เช่น การขอรับบริการภาครัฐแบบเบ็ดเสร็จ ณ จุดเดียว

ตารางที่ 7 ข้อมูลประเภทบริการภาครัฐ

ข้อมูลประเภทบริการภาครัฐ	
กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services)	<ul style="list-style-type: none"> - มีข้อมูลที่เปิดเผยเป็นสาธารณะหรือข้อมูลทั่วไป - ไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคล - ไม่จำเป็นต้องมีการลงทะเบียนและพิสูจน์ตัวตน
กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ (Enhanced Services)	<ul style="list-style-type: none"> - มีการสื่อสารโต้ตอบกับผู้ใช้บริการ - ใช้ข้อมูลส่วนบุคคล หรือไม่ได้โดยเจ้าของข้อมูลส่วนบุคคล ไม่จำเป็นต้องเป็นผู้ดำเนินการเอง - มีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล หรือไม่ได้ - มีช่องทางที่สามารถติดต่อได้
กลุ่มการให้บริการธุรกรรม (Transactional Services)	<ul style="list-style-type: none"> - ต้องใช้ข้อมูลส่วนบุคคล (เช่น เลขประจำตัวประชาชน 13 หลัก) โดยเจ้าของข้อมูลส่วนบุคคล ต้องเป็นผู้ดำเนินการเอง ณ ขณะนั้น - ต้องมีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล - ต้องยืนยันช่องทางติดต่อ (หมายเลขโทรศัพท์ หรือ อีเมล)
กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน (Connected Services)	<ul style="list-style-type: none"> - ต้องมีการเชื่อมโยงหรือใช้ข้อมูลร่วมกับหน่วยงานภายนอกแห่งอื่น - ต้องใช้ข้อมูลส่วนบุคคล (เช่น เลขประจำตัวประชาชน 13 หลัก) โดยเจ้าของข้อมูลส่วนบุคคล ต้องเป็นผู้ดำเนินการเอง ณ ขณะนั้น หรือมีการมอบอำนาจ - ต้องมีการพบเห็นต่อหน้าหรือ เสมือนพบเห็นต่อหน้า (ต้องดำเนินการต่อหน้าเจ้าหน้าที่สำนักงานสำหรับการลงทะเบียนครั้งแรก) - ต้องยืนยันช่องทางติดต่อ (หมายเลขโทรศัพท์ หรือ อีเมล)

บทที่ 4 การประเมินระดับผลกระทบที่เป็นไปได้และระดับความเป็นไปได้ (STEP 2)

เป็นขั้นตอนการวิเคราะห์เหตุการณ์ที่ผู้ใช้บริการกระทำการให้เกิดความเสี่ยงที่ส่งผลกระทบเมื่อมีการพิสูจน์หรือยืนยันตัวตนผิดพลาด และโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น ทั้งนี้ ต้องมีการประชุมเพื่อกำหนดเกณฑ์ของระดับผลกระทบที่เป็นไปได้ และระดับความเป็นไปได้ของแต่ละบริการ ซึ่งผู้ประเมินสามารถดูตัวอย่างระดับผลกระทบและโอกาสโดย “คลิกเพื่อดูตัวอย่าง” เพื่อดูตัวอย่างการวิเคราะห์แต่ละเหตุการณ์ และระดับผลกระทบที่เป็นไปได้

STEP 2				
รายการความเสี่ยง				
	ผลกระทบสูง (H)	ผลกระทบปานกลาง (M)	ผลกระทบต่ำ (L)	
ผลกระทบที่เป็นไปได้				
ผลกระทบสูง (H)				
ผลกระทบปานกลาง (M)				
ผลกระทบต่ำ (L)				
โอกาสสูง (H)				
โอกาสปานกลาง (M)				
โอกาสต่ำ (L)				

รูปที่ 4 ประเมินระดับผลกระทบที่เป็นไปได้และระดับความเป็นไปได้ (STEP 2)

4.1 การเลือกระดับผลกระทบที่เป็นไปได้และระดับความเป็นไปได้ (STEP 2)

ตารางที่ 8 การเลือกระดับผลกระทบที่เป็นไปได้และระดับความเป็นไปได้ (STEP 2)

STEP 2				
<ul style="list-style-type: none"> - ผู้ใช้บริการในที่นี้ คือผู้ให้บริการที่ระบุไว้ในหน้าแรก - ถ้าผลกระทบที่เป็นไปได้จากเหตุการณ์อันเป็นความเสี่ยง สามารถเกิดกับบุคคลหรือองค์กรได้หลายฝ่าย ให้พิจารณาฝ่ายที่ได้รับผลกระทบมากที่สุด - คลิกที่ “คลิกเพื่อดูตัวอย่าง” เพื่ออ่านตัวอย่างการพิจารณาระดับผลกระทบที่เป็นไปได้และโอกาสที่เป็นไปได้ อันเนื่องมาจากเหตุการณ์อันเป็นความเสี่ยง 				
เหตุการณ์อันเป็นความเสี่ยง		ระดับผลกระทบที่เป็นไปได้	ระดับความเป็นไปได้	เหตุผลสนับสนุนคำตอบ (ถ้ามี)
ผลกระทบที่เป็นไปได้ด้านความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง ที่มีต่อบุคคล หรือองค์กร				คลิกเพื่อดูตัวอย่าง
1	หากผู้ให้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2	หากผู้ให้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3	หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน			
4	หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ผลกระทบที่เป็นไปได้ด้านความเสียหายทางการเงิน ที่มีต่อบุคคล หรือองค์กร				คลิกเพื่อดูตัวอย่าง
1	หากผู้ให้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2	หากผู้ให้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3	หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน			
4	หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ผลกระทบที่เป็นไปได้ด้านความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ ที่มีต่อบุคคล หรือองค์กร				คลิกเพื่อดูตัวอย่าง
1	หากผู้ให้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2	หากผู้ให้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3	หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน			
4	หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			

ตารางที่ 8 การเลือกระดับผลกระทบที่เป็นไปได้และระดับความเป็นไปได้ (STEP 2) (ต่อ)

เหตุการณ์อันเป็นความเสี่ยง		ระดับผลกระทบที่เป็นไปได้	ระดับความเป็นไปได้	เหตุผลสนับสนุนคำตอบ (ถ้ามี)
ผลกระทบที่เป็นไปได้ด้านการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ที่มีต่อบุคคล หรือองค์กร				คลิกเพื่อดูตัวอย่าง
1	หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2	หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3	หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน			
4	หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ผลกระทบที่เป็นไปได้ด้านความปลอดภัยของบุคคล ที่มีต่อบุคคล				คลิกเพื่อดูตัวอย่าง
1	หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2	หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3	หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน			
4	หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ผลกระทบที่เป็นไปได้ด้านกระแสเมตทางแห่งหรือทางอาญา ที่มีต่อบุคคล หรือองค์กร				คลิกเพื่อดูตัวอย่าง
1	หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2	หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3	หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน			
4	หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			

ตารางแสดงประเภทผลกระทบทั้ง 6 ด้าน และคำถามเหตุการณ์อันเป็นความเสี่ยงของผลกระทบในแต่ละด้าน ซึ่งผู้ประเมินเลือกกรอกข้อมูลจาก Dropdown List ดังนี้

- ระดับผลกระทบที่เป็นไปได้ที่อาจเกิดขึ้น ผู้ประเมินเลือกกรอกข้อมูลจาก Dropdown List คือ “ไม่มี, ต่ำ, ปานกลาง, สูง”
- ระดับความเป็นไปได้ที่จะเกิดขึ้น ผู้ประเมินเลือกกรอกข้อมูลจาก Dropdown List คือ “มีโอกาสเกิดขึ้นต่ำ, มีโอกาสเกิดขึ้นปานกลาง, มีโอกาสเกิดขึ้นสูง”
- เหตุผลสนับสนุนคำตอบ (ถ้ามี) เป็นช่องว่างที่ให้ผู้ประเมินสามารถพิมพ์อธิบายเหตุผลหรือข้อมูลเพิ่มเติมสนับสนุนคำตอบ ซึ่งคำตอบในแถวนี้จะไม่ได้รับการเอาไปคำนวณต่อใด ๆ

- คลิกเพื่อดูตัวอย่าง ใช้คำสั่ง Hyperlink เพื่อทำการเชื่อมโยงไปยัง “ตัวอย่าง”

4.2 ตารางแสดงข้อมูลระดับความเสี่ยง

ตารางแสดง “ระดับความเสี่ยง (0-9)” เป็นตารางที่หาค่าสูงสุดจากผลลัพธ์ของการคำนวณระดับความเสี่ยงโดยคำนวณจากค่าที่ผู้ประเมินกรอกในแถวระดับผลกระทบที่เป็นไปได้กับระดับความเป็นไปได้ของแต่ละประเภทผลกระทบมาคูณกัน และทำการหาค่าที่ได้สูงที่สุดในแต่ละด้านมาทำการใช้สูตรหาค่าสูงสุด ซึ่งอ้างอิงตามมาตรฐาน. มรด. ๑ - ๒ : ๒๕๖๔

ตารางที่ 9 ตารางแสดงข้อมูลระดับความเสี่ยง

ระดับความเสี่ยง (0-9)			
ประเภทผลกระทบ	พิสูจน์ตัวตน ผิดพลาด	ยืนยันตัวตน ผิดพลาด	เชื่อมโยงกับองค์กรอื่น ผิดพลาด
ความไม่สะดวกสบายและการเสื่อมเสียชื่อเสียง	0	0	0
ความเสียหายทางการเงิน	0	0	0
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	0	0	0
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	0	0	0
ความปลอดภัยของบุคคล	0	0	0
การละเมิดทางแพ่งหรือทางอาญา	0	0	0

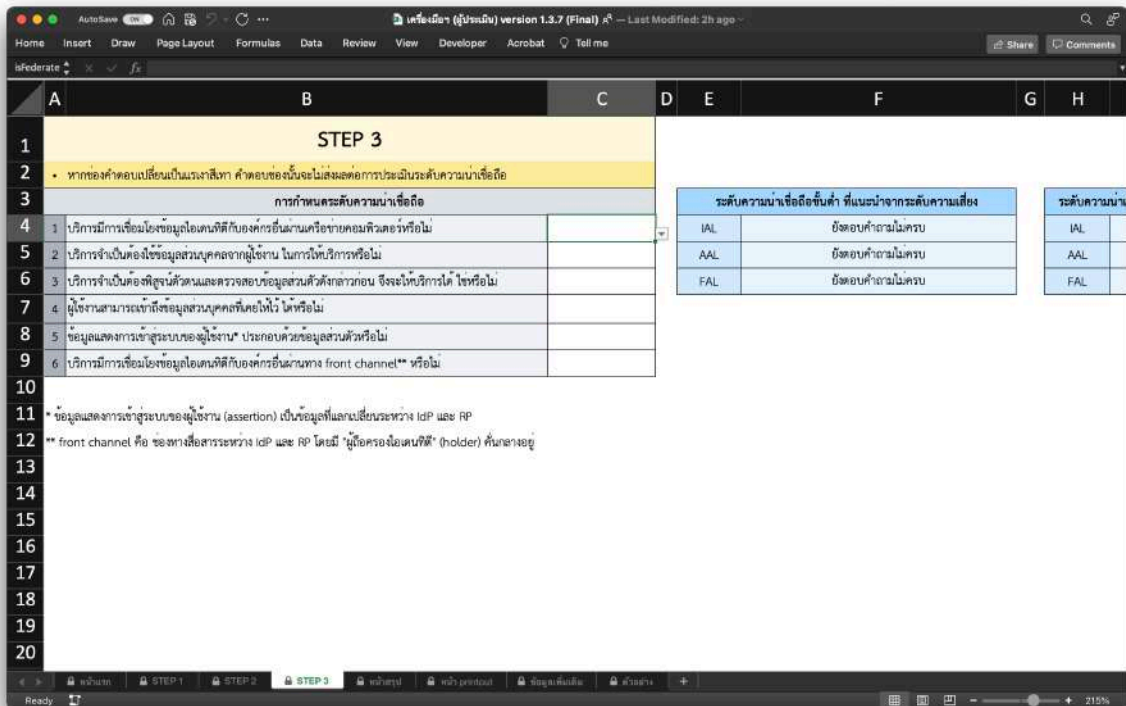
4.3 ตารางแสดงข้อมูลความเสี่ยงของผลกระทบ

ตารางแสดง “ระดับผลกระทบที่เป็นไปได้ (0-3)” เป็นตารางที่หาค่าสูงสุดจากการคำนวณระดับผลกระทบที่เป็นไปได้และทำการหาค่าที่ได้สูงที่สุดในแต่ละด้านมาทำการใช้สูตรหาค่าสูงสุด ซึ่งอ้างอิงตามมาตรฐานของสหรัฐอเมริกา NIST SP 800-63-3

ตารางที่ 10 ตารางแสดงข้อมูลความเสี่ยงของผลกระทบ

ระดับผลกระทบที่เป็นไปได้ (0-3)			
ประเภทผลกระทบ	พิสูจน์ตัวตน ผิดพลาด	ยืนยันตัวตน ผิดพลาด	เชื่อมโยงกับองค์กรอื่น ผิดพลาด
ความไม่สะดวกสบายและการเสื่อมเสียชื่อเสียง	0	0	0
ความเสียหายทางการเงิน	0	0	0
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	0	0	0
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	0	0	0
ความปลอดภัยของบุคคล	0	0	0
การละเมิดทางแพ่งหรือทางอาญา	0	0	0

บทที่ 5 การประเมินระดับความน่าเชื่อถือจากความเสี่ยงของผลกระทบที่อาจเกิดขึ้น (STEP 3)



รูปที่ 5 การประเมินระดับความน่าเชื่อถือจากความเสี่ยงของผลกระทบที่อาจเกิดขึ้น (STEP 3)

5.1 ตารางการกำหนดระดับความน่าเชื่อถือ

ตารางให้ผู้ประเมินกรอกข้อมูลโดยเลือกจาก Dropdown List เพื่อไปคำนวณระดับความน่าเชื่อถือที่เหมาะสมโดยผู้ประเมินสามารถเลือกค่าที่เป็นไปได้ ได้แก่ “ใช่, ไม่ใช่” และสำหรับคำถามข้อ 3 (cell C6) ผู้ประเมินสามารถเลือกตอบค่าที่เป็นไปได้ ได้แก่ “ใช่, ไม่ใช่, ไม่แน่ใจ”

ตารางที่ 11 ตารางการกำหนดระดับความน่าเชื่อถือ

STEP 3	
- หากช่องคำตอบเปลี่ยนเป็นแรงเสีเทา คำตอบช่องนั้นจะไม่ส่งผลต่อการประเมินระดับความน่าเชื่อถือ	
การกำหนดระดับความน่าเชื่อถือ	
1	บริการมีการเชื่อมโยงข้อมูลไอเดนทิตีกับองค์กรอื่นผ่านเครือข่ายคอมพิวเตอร์หรือไม่
2	บริการจำเป็นต้องใช้ข้อมูลส่วนบุคคลจากผู้ใช้งาน ในการให้บริการหรือไม่
3	บริการจำเป็นต้องพิสูจน์ตัวตนและตรวจสอบข้อมูลส่วนตัวดังกล่าวก่อน จึงจะให้บริการได้ ใช่หรือไม่
4	ผู้ใช้งานสามารถเข้าถึงข้อมูลส่วนบุคคลที่เคยให้ไว้ ได้หรือไม่
5	ข้อมูลแสดงการเข้าสู่ระบบของผู้ใช้งาน* ประกอบด้วยข้อมูลส่วนตัวหรือไม่
6	บริการมีการเชื่อมโยงข้อมูลไอเดนทิตีกับองค์กรอื่นผ่านทาง front channel** หรือไม่

* ข้อมูลแสดงการเข้าสู่ระบบของผู้ใช้งาน (assertion) เป็นข้อมูลที่แลกเปลี่ยนระหว่าง IdP และ RP

** front channel คือ ช่องทางสื่อสารระหว่าง IdP และ RP โดยมี “ผู้ถือครองไอเดนทิตี” (holder) คั่นกลางอยู่

5.2 ตารางระดับความน่าเชื่อถือขั้นต่ำที่แนะนำจากระดับความเสี่ยง

ตารางแสดงผลลัพธ์การประเมินเพื่อระบุระดับความน่าเชื่อถือขั้นต่ำที่แนะนำจากระดับความเสี่ยง ซึ่งข้อมูลที่แสดงในตารางนี้ถูกกำหนดให้มีการคำนวณผลลัพธ์ผ่านการดึงข้อมูลจากผู้ประเมินกรอกในตาราง “การกำหนดระดับความน่าเชื่อถือ” และผลลัพธ์การจากคำนวณในหน้า “STEP 2” ตาราง “ระดับความเสี่ยง”

ตารางที่ 12 ตารางระดับความน่าเชื่อถือขั้นต่ำที่แนะนำจากระดับความเสี่ยง

ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับความเสี่ยง	
IAL	ยังตอบคำถามไม่ครบ
AAL	ยังตอบคำถามไม่ครบ
FAL	ยังตอบคำถามไม่ครบ

5.3 ตารางระดับความน่าเชื่อถือขั้นต่ำที่แนะนำจากระดับผลกระทบที่เป็นไปได้

ตารางแสดงผลลัพธ์การประเมินเพื่อระบุระดับความน่าเชื่อถือขั้นต่ำที่แนะนำจากระดับผลกระทบที่เป็นไปได้ ซึ่งข้อมูลที่แสดงในตารางนี้ถูกกำหนดให้มีการคำนวณผลลัพธ์ผ่านการดึงข้อมูลจากผู้ประเมินกรอกในตาราง “การกำหนดระดับความน่าเชื่อถือ” และผลลัพธ์การจากคำนวณในหน้า “STEP 2” ตาราง “ระดับผลกระทบที่เป็นไปได้”

ตารางที่ 13 ตารางระดับความน่าเชื่อถือขั้นต่ำที่แนะนำจากระดับผลกระทบที่เป็นไปได้

ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับผลกระทบที่เป็นไปได้	
IAL	ยังตอบคำถามไม่ครบ
AAL	ยังตอบคำถามไม่ครบ
FAL	ยังตอบคำถามไม่ครบ

บทที่ 6 สรุประดับผลกระทบที่เป็นไปได้ (หน้าสรุป)

ประเภทผลกระทบ	สรุประดับผลกระทบที่เป็นไปได้			อธิบายความหมายของระดับผลกระทบที่เป็นไปได้อีกข้อใดก็ตาม		
	พิกัดระดับผลกระทบ	ขั้นตอนผลกระทบ	เชื่อมโยงกับองค์ประกอบผลกระทบ	ท่า	ปานกลาง	สูง
ความไม่สะดวกและอื่นที่เกี่ยวข้อง	0	0	0	มีความสะดวกและอื่นที่เกี่ยวข้องกับพื้นที่ก่อสร้าง	มีความไม่สะดวกและอื่นที่เกี่ยวข้องกับพื้นที่ก่อสร้างปานกลาง	มีความไม่สะดวกและอื่นที่เกี่ยวข้องกับพื้นที่ก่อสร้างสูง
ความเสียหายทางกายภาพ	0	0	0	มีความเสียหายทางกายภาพเล็กน้อย	มีความเสียหายทางกายภาพปานกลาง	มีความเสียหายทางกายภาพสูง
ความเสียหายทางสังคมและวัฒนธรรมของชุมชนท้องถิ่น	0	0	0	มีความเสียหายทางสังคมและวัฒนธรรมของชุมชนท้องถิ่นเล็กน้อย	มีความเสียหายทางสังคมและวัฒนธรรมของชุมชนท้องถิ่นปานกลาง	มีความเสียหายทางสังคมและวัฒนธรรมของชุมชนท้องถิ่นสูง
การเปลี่ยนแปลงสิ่งแวดล้อมทางกายภาพ	0	0	0	มีการเปลี่ยนแปลงสิ่งแวดล้อมทางกายภาพเล็กน้อย	มีการเปลี่ยนแปลงสิ่งแวดล้อมทางกายภาพปานกลาง	มีการเปลี่ยนแปลงสิ่งแวดล้อมทางกายภาพสูง
ความปลอดภัยของสุขภาพ	0	0	0	มีความปลอดภัยของสุขภาพเล็กน้อย	มีความปลอดภัยของสุขภาพปานกลาง	มีความปลอดภัยของสุขภาพสูง
การเปลี่ยนแปลงสิ่งแวดล้อมทางสังคม	0	0	0	มีการเปลี่ยนแปลงสิ่งแวดล้อมทางสังคมเล็กน้อย	มีการเปลี่ยนแปลงสิ่งแวดล้อมทางสังคมปานกลาง	มีการเปลี่ยนแปลงสิ่งแวดล้อมทางสังคมสูง

ประเภทผลกระทบ	สรุประดับความถี่			อธิบายความหมายของระดับความถี่อีกข้อใดก็ตาม			
	พิกัดระดับผลกระทบ	ขั้นตอนผลกระทบ	เชื่อมโยงกับองค์ประกอบผลกระทบ	ระดับความถี่	ระดับคะแนน	แนวตั้ง	ความหมาย
ความไม่สะดวกและอื่นที่เกี่ยวข้อง	0	0	0	สูง	5-9		ระดับความถี่ที่คำนวณได้ไม่สามารถระบุได้แน่ชัดด้วยการคำนวณเชิงปริมาณในระดับคะแนน โดยอาจจำเป็นต้องมีการคำนวณเชิงคุณภาพ

รูปที่ 6 สรุประดับผลกระทบที่เป็นไปได้

ประเภทผลกระทบ	สรุประดับผลกระทบที่เป็นไปได้			อธิบายความหมายของสีและตัวเลขระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	พิสูจน์ตัวตนผิดพลาด	ยืนยันตัวตนผิดพลาด	เชื่อมโยงกับองค์กรอื่นผิดพลาด	ต่ำ	ปานกลาง	สูง
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	0	0	0	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงในระยะสั้น และจำกัด	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงรุนแรง ระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงระยะยาว หรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	0	0	0	มีความเสียหายทางการเงินที่ไม่มีนัยสำคัญ	มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	0	0	0	มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	0	0	0	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับต่ำ	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาตทำให้ความลับที่เปิดเผยมีผลกระทบระดับปานกลาง	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับสูง
ความปลอดภัยของบุคคล	0	0	0	บาดเจ็บเล็กน้อย ไม่ต้องรับการรักษาพยาบาล	มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องการการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัสหรือถึงแก่ชีวิต
การละเมิดทางแพ่งหรือทางอาญา	0	0	0	การฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อย ซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงเป็นพิเศษในการที่จะถูกบังคับใช้กฎหมาย

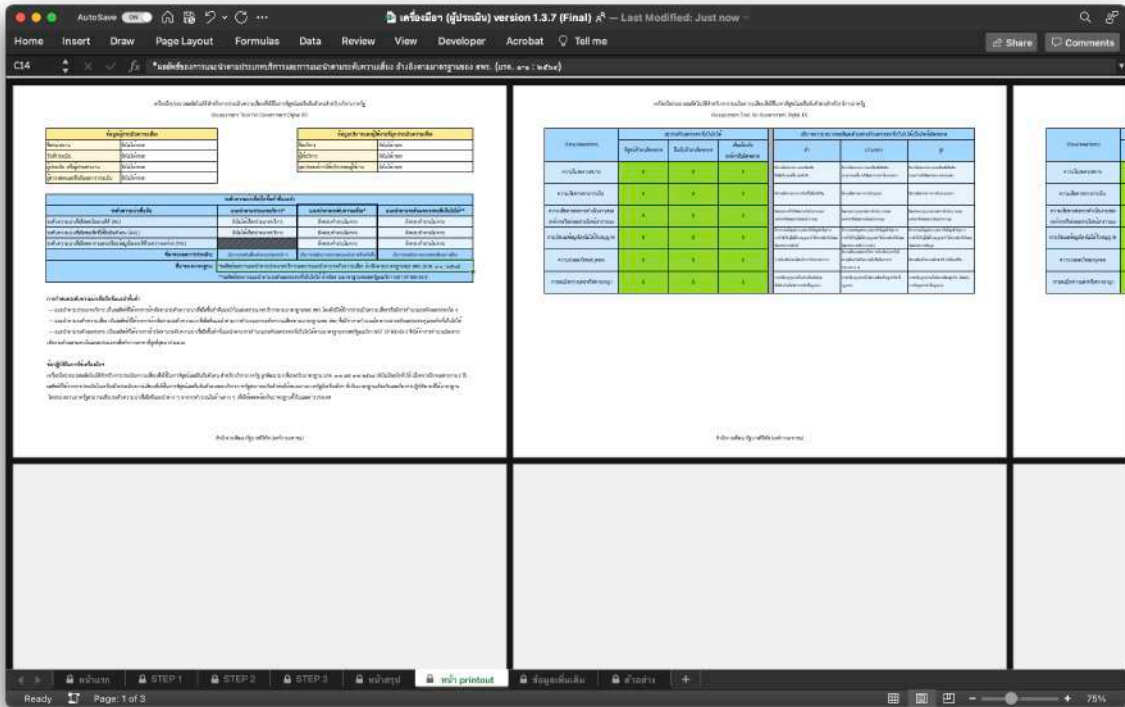
ตารางที่ 15

ตารางแสดงผลลัพธ์การคำนวณตามระดับความเสี่ยงที่ได้จากหน้า “STEP 2”

อ้างอิงตามมาตรฐาน มรด. ๑ - ๒ : ๒๕๖๔

ประเภทผลกระทบ	สรุประดับความเสี่ยง			อธิบายความหมายของสีและตัวเลขระดับความเสี่ยงเมื่อเกิดข้อผิดพลาด			
	พิสูจน์ตัวตนผิดพลาด	ยืนยันตัวตนผิดพลาด	เชื่อมโยงกับองค์กรอื่นผิดพลาด	ระดับความเสี่ยง	ระดับคะแนน	แทนด้วย	ความหมาย
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	0	0	0	สูง	6-9	[Red]	ระดับความเสี่ยงที่หน่วยงานของรัฐไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
ความเสียหายทางการเงิน	0	0	0				
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	0	0	0	ปานกลาง	2-4	[Yellow]	ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	0	0	0				
ความปลอดภัยของบุคคล	0	0	0	ไม่มีหรือต่ำ	0-1	[Green]	ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
การละเมิดทางแพ่งหรือทางอาญา	0	0	0				

บทที่ 7 แสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด (หน้า Printout)



รูปที่ 7 แสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด (หน้า Printout)

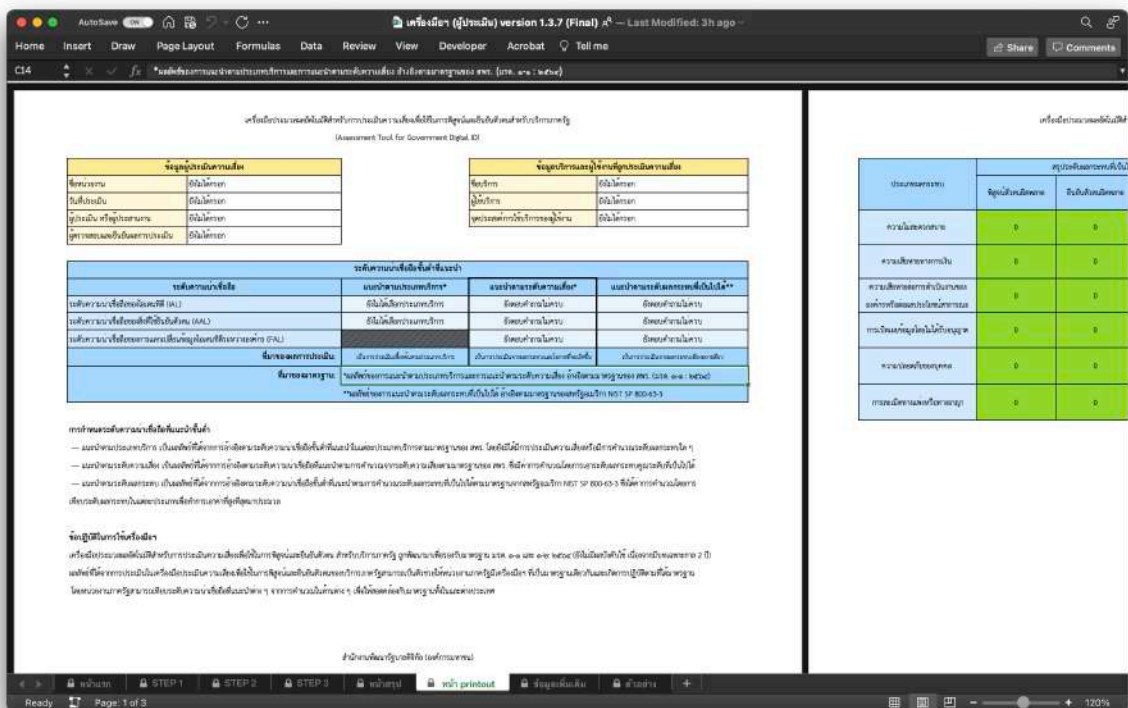
เป็นแผ่นงานที่ผู้ประเมินไม่จำเป็นต้องกรอกอะไร แต่เพื่ออำนวยความสะดวกให้หน่วยงานต่าง ๆ เก็บรวบรวมข้อมูลเพื่ออ้างอิง หลังผู้ประเมินสิ้นสุดการใช้งานเครื่องมือ โดยแผ่นงานนี้ประกอบไปด้วย 3 หน้า 5 ตาราง ดังนี้

7.1 หน้าที่ 1

- ตาราง “ข้อมูลผู้ประเมินความเสี่ยง” ดึงข้อมูลที่ผู้ประเมินกรอกในแผ่นงาน “หน้าแรก”
- ตาราง “ข้อมูลบริการและผู้ใช้งานที่ถูกประเมินความเสี่ยง” ดึงข้อมูลที่ผู้ประเมินกรอกในแผ่นงาน “หน้าแรก”
- ตาราง “ระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ” คือตารางสรุปผลลัพธ์ของการคำนวณที่ได้จากข้อมูลในแผ่นงาน “STEP 1”, “STEP 2” และ “STEP 3” โดยผลลัพธ์ถูกแบ่งออกเป็นสามแถวจากการคำนวณตามสามมาตรฐาน ประกอบด้วย สดมภ์ “แนะนำตามประเภทบริการ”, สดมภ์ “แนะนำตามระดับความเสี่ยง” และ สดมภ์ “แนะนำตามระดับผลกระทบที่เป็นไปได้”

ผู้ประเมินสามารถทำการกดไปยัง “ผลลัพธ์ของการแนะนำตามประเภทบริการและการแนะนำตามระดับความเสี่ยง อ้างอิงตามมาตรฐานของ สพร. (มรด. ๑-๑: ๒๕๖๔) กดเพื่ออ่านมาตรฐาน” และ “ผลลัพธ์ของการแนะนำตามระดับผลกระทบที่เป็นไปได้ อ้างอิงตามมาตรฐานของสหรัฐอเมริกา NIST SP 800-63-3 กดเพื่ออ่านมาตรฐาน” เพื่อทำการเปิดหน้ามาตรฐานดังกล่าวบนเบราว์เซอร์ หัวข้อการกำหนดระดับความน่าเชื่อถือที่แนะนำขั้นต่ำ

- แนะนำตามประเภทบริการ เป็นผลลัพธ์ที่ได้จากการอ้างอิงตามระดับความน่าเชื่อถือขั้นต่ำที่แนะนำในแต่ละประเภทบริการตามมาตรฐานของ สพร. โดยยังมีได้มีการประเมินความเสี่ยงหรือมีการคำนวณระดับผลกระทบที่เป็นไปได้ใด ๆ
- แนะนำตามระดับความเสี่ยง เป็นผลลัพธ์ที่ได้จากการอ้างอิงตามระดับความน่าเชื่อถือที่แนะนำตามการคำนวณจากระดับความเสี่ยงตามมาตรฐานของ สพร. ซึ่งมีค่าการคำนวณโดยการเอาระดับผลกระทบที่เป็นไปได้คูณระดับโอกาสที่เป็นไปได้
- แนะนำตามระดับผลกระทบที่เป็นไปได้ เป็นผลลัพธ์ที่ได้จากการอ้างอิงตามระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามการคำนวณระดับผลกระทบที่เป็นไปได้ตามมาตรฐานจากสหรัฐอเมริกา NIST SP 800-63-3 ซึ่งได้ค่าการคำนวณโดยการเทียบ ระดับผลกระทบที่เป็นไปได้ในแต่ละประเภทเพื่อทำการเอาค่าที่สูงที่สุดมาประมวล



รูปที่ 8 หน้าที่ 1 ของหน้า Printout

7.3 หน้า ที่ 3

ตารางแสดงผลการคำนวณตามระดับความเสี่ยงได้จากหน้า “STEP 2”

ประเภทผลกระทบ	ระดับความถี่			ระดับความรุนแรง			คำอธิบาย
	สูง/มาก	ปานกลาง	ต่ำ/น้อย	รุนแรง	ปานกลาง	ต่ำ/น้อย	
ความเสียหายต่อชื่อเสียง	0	0	0	9	48	High	มีความเสียหายต่อชื่อเสียงขององค์กรในระดับสูง ซึ่งอาจส่งผลต่อความน่าเชื่อถือขององค์กรในระยะยาว
ความเสียหายทางการเงิน	0	0	0	3	24	Medium	มีความเสียหายทางการเงินในระดับปานกลาง ซึ่งอาจส่งผลต่อผลประกอบการในระยะสั้น
ความเสียหายต่อข้อมูลส่วนบุคคลของลูกค้าหรือพันธมิตรทางธุรกิจ	0	0	0	3	24	Medium	มีความเสียหายต่อข้อมูลส่วนบุคคลของลูกค้าหรือพันธมิตรทางธุรกิจในระดับปานกลาง ซึ่งอาจส่งผลต่อความไว้วางใจของลูกค้า
ความเสียหายต่อชื่อเสียงของแบรนด์	0	0	0	3	24	Medium	มีความเสียหายต่อชื่อเสียงของแบรนด์ในระดับปานกลาง ซึ่งอาจส่งผลต่อความน่าเชื่อถือของแบรนด์
การละเมิดกฎหมาย	0	0	0	3	24	Medium	มีความเสียหายต่อชื่อเสียงของแบรนด์ในระดับปานกลาง ซึ่งอาจส่งผลต่อความน่าเชื่อถือของแบรนด์

รูปที่ 10 หน้า ที่ 3 ของหน้า Printout

บทที่ 8 การแสดงรายละเอียดวิธีการคำนวณและเกณฑ์การให้คะแนน (ข้อมูลเพิ่มเติม)

ตารางที่ 16 ตารางแสดงระดับโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น (likelihood levels)

และเกณฑ์การพิจารณา ประกอบไปด้วย “ไม่มี, ต่ำ, ปานกลาง, สูง”

ตารางแสดงระดับโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น (likelihood levels) คือไม่มี และทั้งสามระดับ ระดับสูง ระดับปานกลาง ระดับต่ำ

โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น	คะแนน	ความหมาย
สูง	3	มีโอกาสเกิดขึ้นเป็นประจำบ่อยครั้ง
ปานกลาง	2	มีโอกาสเกิดบางครั้ง
ต่ำ	1	มีโอกาสเกิด แต่นาน ๆ ครั้ง
ไม่มี	0	ไม่มีโอกาสเกิดขึ้น

ตารางที่ 17 ตารางแสดงการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของไอเดนทิตี

และสิ่งที่ใช้ยืนยันตัวตนของผลกระทบในแต่ละด้าน โดยเทียบผลกระทบทั้ง 6 ด้าน

กับระดับความน่าเชื่อถือทั้งสามระดับ

ตารางแสดงการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนของผลกระทบในแต่ละด้าน

ผลกระทบ	ระดับความน่าเชื่อถือ		
	1	2	3
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ	ปานกลาง	สูง
ความเสียหายทางการเงิน	ต่ำ	ปานกลาง	สูง
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ไม่มี	ต่ำ / ปานกลาง	สูง
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี	ต่ำ / ปานกลาง	สูง
ความปลอดภัยของบุคคล	ไม่มี	ต่ำ	ปานกลาง / สูง
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี	ต่ำ / ปานกลาง	สูง

ตารางที่ 18 ตารางแสดงความเชื่อมโยงระหว่างผลกระทบและโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้นว่ามีความเสี่ยงระดับใด โดยมีสูตรการคำนวณ คือ ความเสี่ยง = โอกาสที่จะเกิดขึ้นได้ × ผลกระทบ

ตารางแสดงความเชื่อมโยงความสัมพันธ์ระหว่างผลกระทบและโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้นว่ามีความเสี่ยงระดับใด	
การคำนวณ	
ความเสี่ยง = โอกาสที่จะเกิดขึ้นได้ × ผลกระทบ	

ตารางที่ 19 ตารางแสดงผลระดับความเสี่ยงเป็นตัวเลขและสี โดยแสดงผลที่สัมพันธ์กับผลคูณระหว่างระดับผลกระทบที่เป็นไปได้และโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น ได้แก่ สีเขียว (0, 1) สีเหลือง (2, 3, 4) และ สีแดง (6, 9)

ตารางแสดงผลในรูปแบบการวัดค่าออกเป็นตัวเลขและสีที่มีความหมายถึงระดับความเสี่ยงตามระดับผลกระทบที่เป็นไปได้และโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้นว่ามีความเสี่ยงระดับใด และค่าการแสดงผลที่สัมพันธ์กับการกำหนดเกณฑ์และการแสดงผลที่มีการระบุความหมายของความเสี่ยงตามสี สีเขียว สีเหลือง สีแดง

โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น	ผลกระทบ		
	ต่ำ	ปานกลาง	สูง
สูง	3	6	9
ปานกลาง	2	4	6
ต่ำ	1	2	3
ไม่มี	0	0	0

ตารางที่ 20 ตารางแสดงเกณฑ์ระดับความเสี่ยงที่เป็นไปได้ ระดับคะแนน สีที่แทนด้วย และความหมาย

ความหมายของแต่ละระดับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วย	ความหมาย
สูง	6-9		ระดับความเสี่ยงที่หน่วยงานของรัฐไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกัน ไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
ปานกลาง	2-4		ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
ไม่มี หรือ ต่ำ	0-1		ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้

ตารางที่ 21 ตารางแสดงความหมายของแต่ละระดับกระทบในแต่ละหมวดหมู่ โดยระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด มีทั้งหมด 3 ระดับ ได้แก่ ต่ำ (1 คะแนน), ปานกลาง (2 คะแนน) และ สูง (3 คะแนน)

ความหมายของแต่ละระดับผลกระทบที่เป็นไปได้ในแต่ละหมวดหมู่			
ประเภทผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
	ระดับคะแนน: 1	ระดับคะแนน: 2	ระดับคะแนน: 3
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงในระยะสั้นและจำกัด	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงรุนแรง ระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงระยะยาว หรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	มีความเสียหายทางการเงินที่ไม่สำคัญ	มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับต่ำ	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับปานกลาง	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับสูง
ความปลอดภัยของบุคคล	บาดเจ็บเล็กน้อย ไม่ต้องรับการรักษาพยาบาล	มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องการการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัสหรือถึงแก่ชีวิต
การละเมิดทางแพ่งหรือทางอาญา	การฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อย ซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงเป็นพิเศษในการที่จะถูกบังคับใช้กฎหมาย

บทที่ 9 การแสดงตัวอย่างเพื่ออำนวยความสะดวกในการกรอกแผ่นงาน STEP 2

ตารางที่ 22 ตารางแสดงตัวอย่างการวิเคราะห์ระดับผลกระทบที่เป็นไปได้อันเนื่องมาจากเหตุการณ์อันเป็นความเสี่ยงที่มีความแตกต่างกันไปตามแต่ละลักษณะของบริการ และการใช้งานของผู้ใช้บริการ ซึ่งอยู่ทำการเชื่อมกับแผ่นงาน “STEP 2” โดยผู้ประเมินสามารถกดไปที่ “คลิกเพื่ออ่านตัวอย่าง” ในแผ่นงาน “STEP 2” เพื่อทำการเชื่อมโยงมายังตารางตัวอย่างบริการภาครัฐ ดังนี้

- บริการเราชนะ และคนละครึ่ง ของกระทรวงการคลัง
- บริการ Thailand Pass ของกระทรวงการต่างประเทศ
- บริการผู้ป่วยเอดส์ ของสำนักงานหลักประกันสุขภาพแห่งชาติ
- บริการ Datawarehouse+ ของกรมพัฒนาธุรกิจการค้า
- บริการออกบัตรส่งเสริมการลงทุน ของสำนักงานคณะกรรมการส่งเสริมการลงทุน

ตารางอธิบายตัวอย่าง ตัวอย่าง ของเกณฑ์ ต่ำ ปานกลาง และสูงของระดับผลกระทบที่เป็นไปได้ และโอกาสของผลกระทบที่เป็นไปได้ของแต่ละเหตุการณ์อันเป็นความเสี่ยง			
ผลกระทบด้านความไม่สะดวกสบายและ เสื่อมเสียชื่อเสียง	ตัวอย่างผลกระทบระดับต่ำ	ตัวอย่างผลกระทบระดับปานกลาง	ตัวอย่างผลกระทบระดับสูง
หากผู้ให้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ผู้ใช้งานลงทะเบียนโดยแจ้งข้อมูลอาชีพและรายได้ที่ไม่ตรงกับความเป็นจริง แต่อย่างมากก็เพียงแค่ว่าทำให้เจ้าหน้าที่วิเคราะห์ข้อมูลทางสถิติวิเคราะห์ข้อมูลยากขึ้นเท่านั้น	ผู้ไม่ประสงค์ดีใช้ Sybil attack โจมตีจนทำให้ระบบไม่สามารถให้บริการประชาชนได้อย่างมีประสิทธิภาพ และองค์กรต้องเสียเวลาหลายปีในการสร้างความเชื่อมั่นต่อองค์กรกลับคืนมา	ผู้ไม่ประสงค์ดีใช้ Sybil attack โจมตีจนทำให้ระบบไม่สามารถให้บริการนักท่องเที่ยวทั่วโลกได้ทำให้ประเทศเสื่อมเสียชื่อเสียงในเวทินานาชาติ
หากผู้ให้บริการให้ข้อมูลส่วนตัวผิดพลาด แบบไม่ได้ตั้งใจตอนลงทะเบียน	ผู้ให้บริการกรอกอีเมลผิด ทำให้ไม่ได้รับอีเมลตอบกลับจากระบบ ต้องเริ่มลงทะเบียนใหม่ตั้งแต่ต้น เกิดเป็นความไม่สะดวกสบายในระยะสั้น ๆ	ผู้ให้บริการกรอกอีเมลผิดตอนลงทะเบียนขอใบรับรองการเดินทางเข้าประเทศ ทำให้ไม่ได้รับใบรับรองทันเวลาที่เดินทาง ต้องเสียเวลาจองที่พักและเที่ยวบินใหม่ เป็นความไม่สะดวกสบายอย่างมากแต่แค่ในช่วงสั้น ๆ	ผู้ให้บริการกรอกอีเมลผิดตอนลงทะเบียนขอขึ้นวีซ่าการผลิตภัณฑ์ ทำให้ไม่ได้รับการพิจารณาขึ้นทะเบียนนวัตกรรมในปีนั้น จึงก่อให้เกิดความเสียหายแก่ทั้งบริษัทและพนักงานทั้งหมด และส่งผลในระยะยาวถึงปีถัดไป

ตารางอธิบายตัวอย่าง ตัวอย่าง ของเกณฑ์ ต่ำ ปานกลาง และสูงของระดับผลกระทบที่เป็นไปได้ และโอกาสของผลกระทบที่เป็นไปได้ของแต่ละเหตุการณ์อันเป็นความเสี่ยง			
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้วถูกสวมรอยเข้าใช้งานแทน	ผู้ไม่ประสงค์ดีสวมรอยเข้ามาในภาชนะน้อยกว่าความเป็นจริง เพื่อกลั่นแกล้งให้ผู้ใช้บริการตัวจริงต้องเสียเวลาเดินเรื่องแก้ไขในภายหลัง	ผู้ไม่ประสงค์ดีสวมรอยเข้ามากลั่นแกล้งยกเลิกธุรกรรมที่ค้างไว้จนทำให้ต้องเดินเรื่องและทำเอกสารใหม่ตั้งแต่ต้น รวมถึงสูญเสียโอกาสทางธุรกิจอย่างมีนัยสำคัญ	ผู้ไม่ประสงค์ดีใช้บัญชีเจ้าของบริษัทสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลความลับทางการค้าที่เกี่ยวข้องกับการเจรจา G2G จากนั้นนำไปเผยแพร่ในทางลบจนทำให้ประเทศเสื่อมเสียชื่อเสียงในเวทีนานาชาติ
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน	ข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน มีเพียงชื่อ นามสกุล และอายุเท่านั้น ซึ่งผู้ไม่ประสงค์ดีไม่สามารถนำไปทำอะไรได้มาก	องค์กรต้องเสียเวลาในการปรับปรุงระบบไม่ให้เกิดการขโมยข้อมูลส่วนตัวดังกล่าวได้ และอาจเสื่อมเสียชื่อเสียงเมื่อข่าวนี้แพร่ออกไป	ผู้ไม่ประสงค์ดีดักจับข้อมูลการเข้าสู่ระบบของบริการช่วยเหลือผู้ป่วยโรคเอดส์ ซึ่งเชื่อมโยงข้อมูลยืนยันตัวตนกับหน่วยงานภายนอก และประกอบด้วยชื่อนามสกุลจริง เมื่อข้อมูลรั่วไหลออกไปจะทำให้ผู้ป่วยทั้งหมดเสื่อมเสียชื่อเสียงมาก และเสียในระยะยาว
ผลกระทบด้านความเสียหายทางการเงิน	ตัวอย่างผลกระทบระดับต่ำ	ตัวอย่างผลกระทบระดับปานกลาง	ตัวอย่างผลกระทบระดับสูง
หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จหรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ผู้ใช้งานลงทะเบียนรับเงินเยียวยาโดยแจ้งข้อมูลอาชีพและรายได้ที่ไม่ตรงกับความเป็นจริง แต่ไม่กระทบอะไรกับจำนวนเงินเยียวยาที่ได้รับ	ผู้ไม่ประสงค์ดีใช้ Sybil attack โจมตีจนทำให้ระบบไม่สามารถให้บริการนักท่องเที่ยวทั่วโลกได้ องค์กรต้องจัดสรรงบประมาณจำนวนไม่น้อยในการปรับปรุงระบบ	ผู้ใช้บริการใช้ข้อมูลบัตรประชาชนคนอื่นมาลงทะเบียนรับสิทธิ์เงินช่วยเหลือเยียวยาผู้ได้รับผลกระทบจากภัยพิบัติสึนามิ ทำให้เจ้าของบัตรตัวจริงเสียสิทธิ์ สร้างความเดือดร้อนทางการเงินให้เจ้าของบัตรตัวจริงมาก (เพราะไม่เหลือทรัพย์สินอื่นใดแล้ว)
หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน	ผู้ใช้บริการกรอกเลขบัญชีผิดตอนลงทะเบียนกับหน่วยงานเพื่อชำระค่าธรรมเนียม หน่วยงานได้รับเงินล่าช้า แต่เป็นจำนวนเงินเล็กน้อยเท่านั้น	ผู้ใช้บริการกรอกอีเมลผิดตอนลงทะเบียนขอใบรับรองการเดินทางเข้าประเทศ ทำให้ไม่ได้รับใบรับรองทันเวลาที่จะเดินทางและต้องยกเลิกเที่ยวบินและที่พักโดยไม่ได้เงินคืน	ผู้ใช้บริการไม่สามารถเข้าสู่ระบบเพื่อทำธุรกรรมสำคัญได้ทันเวลาที่จึงทำให้เสียโอกาสทางการเงินอย่างใหญ่หลวง
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้วถูกสวมรอยเข้าใช้งานแทน	ผู้ไม่ประสงค์ดีสวมรอยเข้ามาในภาชนะน้อยกว่าความเป็นจริง เพื่อกลั่นแกล้งให้ผู้ใช้บริการตัวจริงต้องเสียทั้งเงินและเวลาเดินเรื่องแก้ไขในภายหลัง	ผู้ไม่ประสงค์ดีสวมรอยเข้ามารวบรวมข้อมูลส่วนบุคคล ทำให้องค์กรผู้ใช้บริการ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เข้าข่ายประมาทเลินเล่อ ไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ และต้องจ่ายค่าสินไหมทดแทนเป็นจำนวนมาก หากถูกฟ้องแพ่งจากเจ้าของข้อมูลตัวจริง	ผู้ไม่ประสงค์ดีใช้บัญชีเจ้าของบริษัทสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลความลับทางการค้าที่เกี่ยวข้องกับการเจรจา G2G จากนั้นนำไปเผยแพร่ในทางลบ จนทำให้ประเทศสูญเสียโอกาสทางเศรษฐกิจครั้งสำคัญ
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน	เกิด identity theft กับคนผู้ใช้บริการ จากการนำข้อมูลดังกล่าวไปใช้เพื่อดำเนินธุรกรรมทางการเงินเป็นจำนวนไม่เกิน 500 บาท	องค์กรต้องจัดสรรงบประมาณจำนวนไม่น้อยในการปรับปรุงระบบไม่ให้เกิดการขโมยข้อมูลส่วนตัวดังกล่าวได้	เกิด identity theft เป็นวงกว้าง จากการนำข้อมูลดังกล่าวไปใช้เพื่อดำเนินธุรกรรมต่าง ๆ ที่ไม่ชอบด้วยกฎหมาย

ตารางอธิบายตัวอย่าง ตัวอย่าง ของเกณฑ์ ต่ำ ปานกลาง และสูงของระดับผลกระทบที่เป็นไปได้ และโอกาสของผลกระทบที่เป็นไปได้ของแต่ละเหตุการณ์อันเป็นความเสี่ยง

ผลกระทบด้านความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ตัวอย่างผลกระทบระดับต่ำ	ตัวอย่างผลกระทบระดับปานกลาง	ตัวอย่างผลกระทบระดับสูง
หากผู้ให้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จหรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ผู้ใช้งานลงทะเบียนโดยแจ้งข้อมูลอาชีพและรายได้ที่ไม่ตรงกับความเป็นจริง แต่ข้อมูลดังกล่าวนำมาใช้เพื่อประโยชน์ทางสถิติเท่านั้น ไม่ส่งผลกระทบต่อให้บริการ อย่างมากองค์กรก็กระทบแค่ได้ข้อมูลสถิติไม่ถูกต้องนัก	ผู้ไม่ประสงค์ดีใช้ชื่อนามสกุลปลอมเข้ามาลงทะเบียนขอใบรับรองการเดินทางเข้าประเทศเป็นจำนวนมาก ทำให้เจ้าหน้าที่คัดกรองไม่ทัน กระทบกับคนที่ต้องการเดินทางจริง ว่าเป็นวงกว้างจนมีคนตกเครื่องบินบ้าง	ผู้ไม่ประสงค์ดีใช้ Sybil attack โจมตีจนทำให้ระบบไม่สามารถให้บริการนักท่องเที่ยวทั่วโลกได้ และเกิดการชะงักตัวในการรับนักท่องเที่ยว กระทบกับธุรกิจโรงแรมและต่อเนื่องไปอีกหลายภาคส่วน
หากผู้ให้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน	ผู้ใช้งานลงทะเบียนโดยพิมพ์ตัวเลขตกตอนแจ้งข้อมูลรายได้ แต่ข้อมูลดังกล่าวนำมาใช้เพื่อประโยชน์ทางสถิติเท่านั้น ไม่ส่งผลกระทบต่อให้บริการ อย่างมากองค์กรก็กระทบแค่ได้ข้อมูลสถิติไม่ถูกต้องนัก	ผู้ให้บริการให้ข้อมูลผิดพลาดจึงทำให้หน่วยงานอื่นที่จำเป็นต้องมีการส่งต่อข้อมูลเกิดความล่าช้าและกระทบต่อระบบทั้งภายในและภายนอกหน่วยงาน	ผู้ให้บริการให้ข้อมูลผิดพลาดจึงทำให้หน่วยงานอื่นที่จำเป็นต้องมีการส่งต่อข้อมูลเกิดความล่าช้าและกระทบต่อระบบทั้งภายในและภายนอกหน่วยงานถึงขั้นระบบต้องปิดปรับปรุง ทำให้เกิดความเสียหายต่อภาพลักษณ์ขององค์กรและความน่าเชื่อถือระดับชาติ
หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้วถูกสวมรอยเข้าใช้งานแทน	มีผู้ประสงค์ร้ายแอบสวมรอยเข้าใช้บริการ ฝ่ายดูแลระบบขององค์กรมีความยุ่งยากและเสียเวลาในการตรวจสอบความถูกต้องและหาผู้กระทำความผิด	องค์กรต้องปิดการใช้งานระบบอัตโนมัติเป็นเวลาหลายเดือนเพื่อปิดช่องโหว่ในการเชื่อมโยงระบบยืนยันตัวตนกับ NDID และต้องหันมาให้บริการแบบ manual แทนในระหว่างปรับปรุง ทำให้สูญเสียประสิทธิภาพในการให้บริการอย่างมีนัยสำคัญ	ผู้ไม่ประสงค์ดีใช้บัญชีเจ้าของบริษัทสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลความลับทางการค้าที่เกี่ยวข้องกับการเจรจา G2G จากนั้นนำไปเผยแพร่ในทางลบจนทำให้ประเทศสูญเสียโอกาสทางเศรษฐกิจครั้งสำคัญ
หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้วถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน	มีผู้ให้บริการถูกแอบอ้างชื่อในการใช้สิทธิ์ต่าง ๆ เพื่อเข้าถึงบริการที่มีจำนวนจำกัดจึงส่งผลให้ผู้ที่มีสิทธิ์เข้าถึงบริการดังกล่าวตัวจริงไม่ได้รับบริการที่ทั่วถึง	องค์กรต้องปิดการใช้งานระบบอัตโนมัติเป็นเวลาหลายเดือนเพื่อปรับปรุงระบบไม่ให้เกิดการขโมยข้อมูลส่วนตัวดังกล่าวได้ และต้องหันมาให้บริการแบบ manual แทนในระหว่างปรับปรุง ทำให้สูญเสียประสิทธิภาพในการให้บริการอย่างมีนัยสำคัญ	เกิด identity theft เป็นวงกว้าง ประชาชนไม่เกิดความเชื่อมั่นในการใช้งานระบบ และระบบต้องปิดตัวไปอย่างถาวร
ผลกระทบด้านการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ตัวอย่างผลกระทบระดับต่ำ	ตัวอย่างผลกระทบระดับปานกลาง	ตัวอย่างผลกระทบระดับสูง
หากผู้ให้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จหรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ผู้ใช้งานใช้ชื่อนามสกุลของคนอื่นเข้ามาลงทะเบียนใช้ บริการ แต่บริการเป็นเพียงบริการให้ข้อมูลที่ไม่อ่อนไหว จึงแทบไม่กระทบอะไรกับเจ้าของข้อมูลตัวจริง	ผู้ให้บริการจงใจสร้างไอเดนทิตีที่ไม่มีอยู่จริงเพื่อรับสิทธิ์การเยียวยาจากบริการของทางภาครัฐจึงทำให้สิทธิ์เต็มและผู้ที่ต้องการรับการเยียวยาจำนวนมากได้รับผลกระทบจึงต้องมีการเปิดเผยรายชื่อของผู้ลงทะเบียนทั้งหมด	ผู้ไม่ประสงค์ดีใช้ไอเดนทิตีของเจ้าของบริษัทเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลความลับทางการค้า จากนั้นนำไปเผยแพร่ในทางลบจนหุ้นของบริษัททุกบริษัทในภาคอุตสาหกรรมเดียวกันตกกันถ้วนหน้า

ตารางอธิบายตัวอย่าง ตัวอย่าง ของเกณฑ์ ต่ำ ปานกลาง และสูงของระดับผลกระทบที่เป็นไปได้ และโอกาสของผลกระทบที่เป็นไปได้ของแต่ละเหตุการณ์อันเป็นความเสี่ยง			
หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาด แบบไม่ได้ตั้งใจตอนลงทะเบียน	ผู้ใช้บริการกรอกอีเมลผิด ทำให้ระบบส่งอีเมลตอบรับ ที่ประกอบด้วยข้อมูลส่วนตัวไปให้บุคคลอื่นแทน แต่ข้อมูลดังกล่าวมีเพียงชื่อนามสกุล และอายุ เท่านั้น จึงแทบไม่กระทบอะไรกับผู้ใช้บริการตัวจริง	ผู้ใช้บริการกรอกอีเมลผิด ทำให้ระบบส่งอีเมลตอบรับ ที่ประกอบด้วยข้อมูลส่วนตัว ไปให้บุคคลอื่นแทน โดยข้อมูลดังกล่าวประกอบไปด้วยชื่อ นามสกุล และผลการตรวจโรค ร้ายแรง	ผู้ใช้บริการกรอกอีเมลผิด ทำให้ระบบส่งอีเมลตอบรับ ที่ประกอบด้วยข้อมูลอ่อนไหวทางการค้าระดับ G2G ไปให้บุคคลอื่นแทน และบุคคลดังกล่าวอาจนำไปเผยแพร่ในทางลบจนทำให้ประเทศสูญเสียโอกาสทางเศรษฐกิจครั้งสำคัญได้
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน	ผู้ไม่ประสงค์ดีสวมรอยเข้ามาใช้บริการแทน แต่ระบบไม่ได้แสดงข้อมูลอ่อนไหวใด ๆ จึงแทบไม่กระทบอะไรกับผู้ใช้บริการตัวจริง	ผู้ไม่ประสงค์ดีใช้บัญชีเจ้าของบริษัทสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลความลับทางการค้า จากนั้นนำไปเผยแพร่ในทางลบ จนทำให้หุ้นของบริษัทตกได้อย่างมีนัยสำคัญ	ผู้ไม่ประสงค์ดีใช้บัญชีเจ้าของบริษัทสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลความลับทางการค้าที่เกี่ยวข้องกับการเจรจา G2G จากนั้นนำไปเผยแพร่ในทางลบจนทำให้ประเทศสูญเสียโอกาสทางเศรษฐกิจครั้งสำคัญ
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน	ข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน มีเพียงชื่อ นามสกุล และอายุเท่านั้น ซึ่งผู้ไม่ประสงค์ดีไม่สามารถนำไปทำอะไรได้มาก	ข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน ประกอบด้วยข้อมูลอ่อนไหวทางการค้า ทำให้เกิดผลเสียต่อบริษัทที่เกี่ยวข้องอย่างมีนัยสำคัญ	ข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน ประกอบด้วยข้อมูลอ่อนไหวทางการค้าระดับ G2G เมื่อผู้ไม่ประสงค์ดีนำไปเปิดเผยในทางลบทำให้ประเทศสูญเสียโอกาสทางเศรษฐกิจครั้งสำคัญ
ผลกระทบด้านความปลอดภัยของบุคคล	ตัวอย่างผลกระทบระดับต่ำ	ตัวอย่างผลกระทบระดับปานกลาง	ตัวอย่างผลกระทบระดับสูง
หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ผู้ใช้บริการไม่ยอมเปิดเผยตัวตนในการสอบถามเกี่ยวกับการเข้ารับการรักษาโรคเอดส์ ทำให้เจ้าหน้าที่ไม่สามารถติดต่อกลับได้ เกิดเป็นความไม่สะดวกเล็กน้อยต่อเจ้าหน้าที่ในการติดตามผล	ผู้ไม่ประสงค์ดีใช้ไอเดนทิตีของบุคคลอื่นมารับสิทธิ์เยียวยา ผลกระทบอันเนื่องมาจากภัยพิบัติ จนทำให้ผู้ได้รับผลกระทบตัวจริงไม่ได้รับเงินเพื่อใช้ในการรักษาพยาบาลตัวเองอย่างทันท่วงที	ผู้ไม่ประสงค์ดีใช้ Sybil attack โจมตีระบบการจองวัคซีน จนทำให้การฉีดวัคซีนเกิดความล่าช้าเป็นวงกว้าง และไม่ทันการณ์ต่อการลุกลามของโรคระบาดร้ายแรง
หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาด แบบไม่ได้ตั้งใจตอนลงทะเบียน	ผู้ใช้บริการกรอกหมายเลขโทรศัพท์ผิดในการลงทะเบียนอยู่ใน waiting list ของฉีดวัคซีนโรคไข้หวัดใหญ่ ทำให้ไม่ได้รับการติดต่อกลับ แต่เป็นโรคไม่ร้ายแรง ไม่ต้องรีบฉีดก็ได้	ผู้ใช้บริการกรอกหมายเลขโทรศัพท์ผิดในการลงทะเบียนอยู่ใน waiting list ของการฉีดวัคซีน (ที่อาจไม่ต้องฉีดก็ได้) เพื่อเดินทางไปอัฟริกา แต่ไม่ได้รับการติดต่อกลับ และทำให้ป่วยเข้าโรงพยาบาล	ผู้ใช้บริการกรอกหมายเลขโทรศัพท์ผิดในการลงทะเบียนอยู่ใน waiting list ของการปลูกถ่ายอวัยวะ ทำให้ไม่ได้รับการติดต่อกลับ และสูญเสียโอกาสในการรักษา เป็นอันตรายถึงแก่ชีวิต
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน	ผู้ไม่ประสงค์ดีสวมรอยเข้ามาแลกถังเปลี่ยนข้อมูลกลุ่มเลือด แต่แพทย์ต้องตรวจสอบกลุ่มเลือดเองซ้ำอีกครั้งก่อนการรักษาอยู่แล้ว ทำให้ไม่ได้รับอันตรายอะไร	ผู้ไม่ประสงค์ดีสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลบัตรประชาชนของผู้ใช้งานในระบบหรือผู้อื่นที่เกี่ยวข้องได้ ผู้ไม่ประสงค์ดีสามารถใช้อ้างอิงข้อมูลที่อยู่เพื่อจุดประสงค์ในการสะกดรอยตามและทำร้ายร่างกาย (จนต้องเข้ารับการรักษา)	ผู้ไม่ประสงค์ดีสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลส่วนตัวที่เกี่ยวข้องกับการกระทำผิดกฎหมาย และนำข้อมูลดังกล่าวไปใช้สะกดรอยตามและทำร้ายร่างกายเพื่อแก้แค้นเจ้าของข้อมูลจนถึงแก่ชีวิต

ตารางอธิบายตัวอย่าง ตัวอย่าง ของเกณฑ์ ต่ำ ปานกลาง และสูงของระดับผลกระทบที่เป็นไปได้ และโอกาสของผลกระทบที่เป็นไปได้ของแต่ละเหตุการณ์อันเป็นความเสี่ยง			
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน	ผู้ไม่ประสงค์ดีดักจับข้อมูลการเข้าสู่ระบบของบริการช่วยเหลือผู้ป่วยโรคเอดส์ ของบริการช่วยเหลือผู้ป่วยโรคเอดส์ ซึ่งเชื่อมโยงข้อมูลยืนยันตัวตนกับหน่วยงานภายนอก และประกอบด้วยชื่อนามสกุลจริง อย่างไรก็ตามการรั่วไหลดังกล่าวไม่ส่งผลกระทบต่อการรักษา	องค์กรต้องปิดการใช้งานระบบบริการสุขภาพเป็นเวลาหลายเดือน เพื่อปรับปรุงระบบไม่ให้เกิดการขโมยข้อมูลส่วนตัวดังกล่าวได้ และส่งผลกระทบต่อการรักษาคนไข้บางส่วนได้ไม่ทันที่	ผู้ไม่ประสงค์ดีดักจับข้อมูลการเข้าสู่ระบบของอาสาสมัครแห่งชาติและสเว็ทพั่นขนาดใหญ่ และสุดท้ายได้ขโมยข้อมูลส่วนตัวของอาสาสมัครไปทำร้ายร่างกายจนถึงแก่ชีวิต
ผลกระทบด้านการละเมิดทางแพ่งหรือทางอาญา	ตัวอย่างผลกระทบระดับต่ำ	ตัวอย่างผลกระทบระดับปานกลาง	ตัวอย่างผลกระทบระดับสูง
หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จหรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ผู้ใช้งานลงทะเบียนโดยแจ้งข้อมูลอาชีพและรายได้ที่ไม่ตรงกับความเป็นจริง ซึ่งเป็นการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันบิดเบือน ผิด พ.ร.บ. คอมพิวเตอร์ฯ 2560 แต่ข้อมูลเท็จดังกล่าวไม่กระทบกับการให้บริการ ไม่จำเป็นต้องดำเนินการเอาผิด	ผู้ไม่ประสงค์ดีใช้ข้อมูลบัตรประชาชนคนอื่นมาลงทะเบียนรับสิทธิ์เงินช่วยเหลือเยียวยาผู้มีรายได้น้อย ซึ่งหน่วยงานภาครัฐผู้ให้บริการพิจารณาแล้วเห็นว่าจำเป็นต้องติดตามตัวเพื่อดำเนินการเอาผิด (แต่ไม่ต้องถึงกรมสอบสวนคดีพิเศษ)	ผู้ไม่ประสงค์ดีใช้ Sybil attack โจมตีระบบให้บริการนักท่องเที่ยวจากทั่วโลก ซึ่งเป็นการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันบิดเบือน ผิด พ.ร.บ. คอมพิวเตอร์ฯ 2560 และกระทบกับเศรษฐกิจเป็นวงกว้าง จำเป็นต้องดำเนินการเอาผิด
หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน	ผู้ใช้งานลงทะเบียนโดยพิมพ์ตัวเลขตอนแจ้งข้อมูลรายได้ ซึ่งอันที่จริงเป็นการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันบิดเบือน ผิด พ.ร.บ. คอมพิวเตอร์ฯ 2560 แต่ในทางปฏิบัติไม่จำเป็นต้องดำเนินการเอาผิด	ผู้ใช้งานกรอกข้อมูลรายได้ผิดตอนลงทะเบียน ทำให้ได้รับเงินเยียวยามากกว่าที่ควรจะเป็น ต่อเนื่องกันนานหลายปี และภาครัฐต้องดำเนินการยึดเงินส่วนเกินคืน	ผู้ใช้บริการกรอกข้อมูลผิดพลาดตอนลงทะเบียนทำให้หน่วยงานภาครัฐไม่สามารถตรวจสอบและตามตัวได้ จึงก่อให้เกิดการหลีกเลี่ยงการเสียค่าชดใช้มานานหลายปี และไม่สามารถมีเหตุผลมาสนับสนุนการกระทำดังกล่าวได้ จึงทำให้ต้องรับโทษขั้นสูงสุด
หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน	ผู้ไม่ประสงค์ดีสวมรอยเข้ามารวบรวมข้อมูลส่วนบุคคล ทำให้องค์กรผู้ให้บริการ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เข้าข่ายประมาทเลินเล่อ ไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แต่เนื่องจากข้อมูลดังกล่าวไม่สำคัญมาก จึงไม่เกิดการดำเนินคดีใด ๆ	ผู้ไม่ประสงค์ดีสวมรอยเข้ามารวบรวมข้อมูลส่วนบุคคล ทำให้องค์กรผู้ให้บริการ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เข้าข่ายประมาทเลินเล่อ ไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ และถูกฟ้องจากเจ้าของข้อมูลตัวจริง	ผู้ไม่ประสงค์ดีใช้บัญชีเจ้าของบริษัทสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลความลับทางการค้าที่เกี่ยวข้องกับการเจรจา G2G จากนั้นนำไปเผยแพร่ในทางลบ เกิดการฟ้องร้องในระดับที่กรมสอบสวนคดีพิเศษต้องเข้ามาดำเนินการ

ตารางอธิบายตัวอย่าง ตัวอย่าง ของเกณฑ์ ต่ำ ปานกลาง และสูงของระดับผลกระทบที่เป็นไปได้ และโอกาสของผลกระทบที่เป็นไปได้ของแต่ละเหตุการณ์อันเป็นความเสี่ยง

<p>หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน</p>	<p>ข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน มีเพียงชื่อ นามสกุล และอายุเท่านั้น ซึ่งผู้ไม่ประสงค์ดีไม่สามารถนำไปทำอะไรได้มาก จึงไม่มีความจำเป็นต้องดำเนินการเอาผิดกับผู้ใด</p>	<p>องค์กรผู้ให้บริการในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเข้าข่าย ประมาทเลินเล่อ ไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ และเจ้าของข้อมูลตัวจริงดำเนินคดีแพ่งกับองค์กรผู้ให้บริการ</p>	<p>เกิด identity theft เป็นวงกว้าง จากการนำข้อมูลดังกล่าวไปใช้เพื่อดำเนินธุรกรรมต่าง ๆ ที่ไม่ชอบด้วยกฎหมาย จำเป็นต้องดำเนินการเอาผิด</p>
---	---	---	--

ตัวอย่างแผ่นงาน “หน้าแรก”

	A	B	C
1			
2	ข้อมูลผู้ประเมินความเสี่ยง		
3	ชื่อหน่วยงาน	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)	
4	วันที่ประเมิน	29 ธันวาคม พ.ศ. 2564	
5	ผู้ประเมิน หรือผู้ประสานงาน	นาย สมชาย ใจดี	
6	ผู้ตรวจสอบและยืนยันผลการประเมิน	นาง สมหญิง รมเย็น	
7			
8			
9			
10	ข้อมูลบริการและผู้ใช้งานที่ถูกประเมินความเสี่ยง		
11	ชื่อบริการ	เว็บไซต์ https://www.dga.or.th	
12	ผู้ใช้บริการ	ประชาชนทั่วไป	
13	จุดประสงค์การใช้บริการของผู้ใช้งาน	ติดตามข้อมูลข่าวสารและติดต่อเจ้าหน้าที่เพื่อปรึกษา	
14			
15			

ตัวอย่างแผนงาน “STEP 1”

	A	B	C	D
1	STEP 1			
2	บริการที่ถูกประเมิน จัดว่าเป็นบริการประเภทใด ตามตารางสีเขียวด้านขวามือ			
3	ประเภทของบริการ	กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ		กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services)
4	ระดับความน่าเชื่อถือขั้นต่ำที่แนะนำมาตรฐานของ สพร.			
5	ประเภทระดับความน่าเชื่อถือ	ระดับความน่าเชื่อถือขั้นต่ำ		กลุ่มการให้บริการข้อมูลที่มีการ ปฏิสัมพันธ์กับผู้ใช้บริการ (Enhanced Services)
6	ระดับความน่าเชื่อถือของไอเดนทิตี (IAL)	1		
7	ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL)	1		
8				กลุ่มการให้บริการธุรกรรม (Transactional Services)
9				กลุ่มการให้บริการธุรกรรมที่ เชื่อมโยงข้อมูลระหว่างหน่วยงาน (Connected Services)
10				
11				
12				
13				
14				
15				

ตัวอย่างแผนงาน “STEP 2”

	B	C	D	E
1	STEP 2			
2	บุคคลหรือองค์กรได้หลายฝ่าย ไม่พิจารณาฝ่ายที่ได้รับผลกระทบมากที่สุด			
3	ทุกที่เป็นไปได้และโอกาสที่เป็นไปได้ อันเนื่องมาจากเหตุการณ์อันเป็นความเสี่ยง			
4	เป็นความเสี่ยง	ระดับผลกระทบที่เป็นไปได้	ระดับความเป็นไปได้	เหตุผลสนับสนุนคำตอบ (ถ้ามี)
5	ที่มีต่อบุคคล หรือองค์กร	คลิกเพื่อดูตัวอย่าง		
6	ลมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ต่ำ	มีโอกาสเกิดขึ้นปานกลาง	สร้างความไม่สะดวกสบายใจเจ้าหน้าที่ที่จะคอมพิวเตอร์ข้อมูลในระบบ
7		ต่ำ	มีโอกาสเกิดขึ้นปานกลาง	สร้างความไม่สะดวกสบายใจเจ้าหน้าที่ที่จะคอมพิวเตอร์ข้อมูลในระบบ
8		ต่ำ	มีโอกาสเกิดขึ้นต่ำ	สร้างความวุ่นวายและการเข้าใจผิดที่เป็นไปได้ต่อผู้ถูกอ้าง
9	บุคลากรพิสูจน์และยืนยันตัวตน	ไม่มี	มีโอกาสเกิดขึ้นต่ำ	ไม่ได้มีการเก็บข้อมูลสำคัญที่ผู้ร้ายที่ทำการสมรอยจะไขประโยชน์
10	องค์กร	คลิกเพื่อดูตัวอย่าง		
11	ลมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ไม่มี	มีโอกาสเกิดขึ้นต่ำ	ไม่สามารถระงับเหตุการณ์เงินได้
12		ไม่มี	มีโอกาสเกิดขึ้นต่ำ	ไม่สามารถระงับเหตุการณ์เงินได้
13		ไม่มี	มีโอกาสเกิดขึ้นต่ำ	ไม่สามารถระงับเหตุการณ์เงินได้
14	บุคลากรพิสูจน์และยืนยันตัวตน	ไม่มี	มีโอกาสเกิดขึ้นต่ำ	ไม่สามารถระงับเหตุการณ์เงินได้
15	หรือต่อผลประโยชน์สาธารณะ ที่มีต่อบุคคล หรือองค์กร	คลิกเพื่อดูตัวอย่าง		
16	ลมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ต่ำ	มีโอกาสเกิดขึ้นต่ำ	สร้างความล่าช้าต่อการดำเนินการของระบบเพราะคอมพิวเตอร์มาเข้าข้อมูล
17		ต่ำ	มีโอกาสเกิดขึ้นต่ำ	สร้างความล่าช้าต่อการดำเนินการของระบบเพราะคอมพิวเตอร์มาเข้าข้อมูล
18		ต่ำ	มีโอกาสเกิดขึ้นต่ำ	เจ้าหน้าที่เสียเวลาเข้าดูข้อมูลซึ่งส่งผลต่อการดำเนินงาน
19	บุคลากรพิสูจน์และยืนยันตัวตน	ไม่มี	มีโอกาสเกิดขึ้นต่ำ	-
20		คลิกเพื่อดูตัวอย่าง		
21				

ตัวอย่างแผนงาน “STEP 3”

	A	B	C	D	E								
1	STEP 3												
2	หากข้อจำกัดเปลี่ยนแปลงเป็นแรงเสียดทาน ค่าตอบของนั้นจะไม่ส่งผลต่อการประเมินระดับความน่าเชื่อถือ												
3	การกำหนดระดับความน่าเชื่อถือ												
4	1	บริการมีการเชื่อมโยงข้อมูลไอเดนทิตีกับองค์กรอื่นผ่านเครือข่ายคอมพิวเตอร์หรือไม่	ไม่ใช่	<table border="1"> <thead> <tr> <th colspan="2">ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำ</th> </tr> </thead> <tbody> <tr> <td>IAL</td> <td></td> </tr> <tr> <td>AAL</td> <td></td> </tr> <tr> <td>FAL</td> <td>ไม่เกี่ยวข้อง</td> </tr> </tbody> </table>		ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำ		IAL		AAL		FAL	ไม่เกี่ยวข้อง
ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำ													
IAL													
AAL													
FAL	ไม่เกี่ยวข้อง												
5	2	บริการจำเป็นต้องใช้ข้อมูลส่วนบุคคลจากผู้ใช้งาน ในการให้บริการหรือไม่	ใช่										
6	3	บริการจำเป็นต้องพิสูจน์ตัวตนและตรวจสอบข้อมูลส่วนตัวดังกล่าวก่อน จึงจะให้บริการได้ ใช่หรือไม่	ไม่ใช่										
7	4	ผู้ใช้งานสามารถเข้าถึงข้อมูลส่วนบุคคลที่เคยให้ไว้ ได้หรือไม่	ไม่ใช่										
8	5	ข้อมูลแสดงการเข้าสู่ระบบของผู้ใช้งาน* ประกอบด้วยข้อมูลส่วนตัวหรือไม่											
9	6	บริการมีการเชื่อมโยงข้อมูลไอเดนทิตีกับองค์กรอื่นผ่านทาง front channel** หรือไม่											
10													
11	* ข้อมูลแสดงการเข้าสู่ระบบของผู้ใช้งาน (assertion) เป็นข้อมูลที่แลกเปลี่ยนระหว่าง IdP และ RP												
12	** front channel คือ ช่องทางสื่อสารระหว่าง IdP และ RP โดยมี "ผู้ถือครองไอเดนทิตี" (holder) คั่นกลางอยู่												
13													

ตัวอย่างแผนงาน “หน้าสรุป” (แสดงระดับความเสี่ยงของผลกระทบแต่ละด้าน)

ประเภทผลกระทบ	สรุประดับความน่าเชื่อถือ			สรุปความรุนแรงของผลกระทบที่ประเมินได้เมื่อเกิดข้อผิดพลาด		
	พิสูจน์ตัวตนดิจิทัล	ยืนยันตัวตนดิจิทัล	เชื่อมโยงกับองค์กรอื่น	ต่ำ	ปานกลาง	สูง
ความน่าเชื่อถือของข้อมูลดิจิทัล	1	0	1	ต่ำ	ปานกลาง	สูง
ความน่าเชื่อถือของข้อมูลส่วนบุคคล	0	0	0	ต่ำ	ปานกลาง	สูง
ความน่าเชื่อถือของข้อมูลทางการเงิน	1	1	1	ต่ำ	ปานกลาง	สูง
การเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่น	1	1	1	ต่ำ	ปานกลาง	สูง
ความน่าเชื่อถือของข้อมูลส่วนบุคคล	0	0	0	ต่ำ	ปานกลาง	สูง
การเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่น	0	0	0	ต่ำ	ปานกลาง	สูง

ประเภทผลกระทบ	สรุประดับความน่าเชื่อถือ			สรุปความรุนแรงของผลกระทบที่ประเมินได้เมื่อเกิดข้อผิดพลาด			
	พิสูจน์ตัวตนดิจิทัล	ยืนยันตัวตนดิจิทัล	เชื่อมโยงกับองค์กรอื่น	ระดับความรุนแรง	ระดับความรุนแรง	ระดับความรุนแรง	สาเหตุ
ความน่าเชื่อถือของข้อมูลดิจิทัล	2	0	2	สูง	6-9	สูง	ระดับความน่าเชื่อถือของข้อมูลดิจิทัลที่ต่ำลงอาจส่งผลให้เกิดการเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่นที่ไม่เกี่ยวข้องกัน
ความน่าเชื่อถือของข้อมูลส่วนบุคคล	0	0	0	ปานกลาง	2,4	ปานกลาง	ระดับความน่าเชื่อถือของข้อมูลส่วนบุคคลที่ต่ำลงอาจส่งผลให้เกิดการเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่นที่ไม่เกี่ยวข้องกัน
ความน่าเชื่อถือของข้อมูลทางการเงิน	1	1	1	ไม่มีหรือต่ำ	0-1	ไม่มีหรือต่ำ	ระดับความน่าเชื่อถือของข้อมูลทางการเงินที่ต่ำลงอาจส่งผลให้เกิดการเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่นที่ไม่เกี่ยวข้องกัน
การเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่น	1	1	1	ไม่มีหรือต่ำ	0-1	ไม่มีหรือต่ำ	ระดับความน่าเชื่อถือของข้อมูลดิจิทัลที่ต่ำลงอาจส่งผลให้เกิดการเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่นที่ไม่เกี่ยวข้องกัน
ความน่าเชื่อถือของข้อมูลส่วนบุคคล	0	0	0	ไม่มีหรือต่ำ	0-1	ไม่มีหรือต่ำ	ระดับความน่าเชื่อถือของข้อมูลส่วนบุคคลที่ต่ำลงอาจส่งผลให้เกิดการเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่นที่ไม่เกี่ยวข้องกัน
การเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่น	0	0	0	ไม่มีหรือต่ำ	0-1	ไม่มีหรือต่ำ	ระดับความน่าเชื่อถือของข้อมูลดิจิทัลที่ต่ำลงอาจส่งผลให้เกิดการเชื่อมโยงข้อมูลดิจิทัลกับองค์กรอื่นที่ไม่เกี่ยวข้องกัน

ตัวอย่างแผ่นงาน “หน้า printout”

เครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยงที่ใช้ในการพิสูจน์และยืนยันตัวตนสำหรับบริการภาครัฐ
(Assessment Tool for Government Digital ID)

ข้อมูลผู้ประเมินความเสี่ยง		ข้อมูลบริการและผู้ให้บริการที่ผู้ประเมินความเสี่ยง	
ชื่อหน่วยงาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	ผู้ให้บริการ	เว็บไซต์ https://www.dgs.or.th
วันที่ประเมิน	29 ธันวาคม พ.ศ. 2564	ผู้รับบริการ	ประชาชนทั่วไป
ผู้ประเมิน หรือผู้ประสานงาน	นาย ธนชาย ใจดี	จุดประสงค์การใช้บริการของผู้ใช้งาน	ติดตามข้อมูลข่าวสารและติดต่อเจ้าหน้าที่เพื่อปรึกษา
ผู้ตรวจสอบและยืนยันผลการประเมิน	นาง ธนพวีญ รมเย็น		

ระดับความน่าเชื่อถือขั้นต่ำแนะนำ			
ระดับความน่าเชื่อถือ	แนะนำตามประเภทบริการ*	แนะนำตามระดับความเสี่ยง*	แนะนำตามระดับผลกระทบที่เป็นไปได้**
ระดับความน่าเชื่อถือของข้อมูลดิจิทัล (AL)	1	1	1
ระดับความน่าเชื่อถือของสิ่งที่ยืนยันตัวตน (AAL)	1	2	2
ระดับความน่าเชื่อถือของผลการปฏิบัติงานของข้อมูลไม่ระบุตัวตน (FAL)		ไม่เกี่ยวข้องกับการบริการ	ไม่เกี่ยวข้องกับการบริการ
ที่มาของผลการประเมิน:	เป็นการประเมินระดับความน่าเชื่อถือ	เป็นการประเมินจากผลกระทบที่เป็นไปได้	เป็นการประเมินจากผลกระทบที่เป็นไปได้
ที่มาของมาตรฐาน:	*หลักพิจารณาแนะนำตามประเภทบริการและการแนะนำตามระดับความเสี่ยง อ้างอิงตามมาตรฐานของ สท. (พ.ศ. ๑-๑ : ๒๕๖๓) **หลักพิจารณาแนะนำตามระดับผลกระทบที่เป็นไปได้ อ้างอิงตามมาตรฐานของสหรัฐอเมริกา NIST SP 800-63-3		

การกำหนดระดับความน่าเชื่อถือขั้นต่ำแนะนำ

- แนะนำตามประเภทบริการ เป็นหลักที่พิจารณาจากข้อมูลระดับความน่าเชื่อถือขั้นต่ำที่แนะนำในแต่ละประเภทบริการตามมาตรฐานของ สท. โดยยังไม่ได้การประเมินความเสี่ยงหรือมีการคำนวณระดับผลกระทบใด ๆ
- แนะนำตามระดับความเสี่ยง เป็นหลักที่พิจารณาจากข้อมูลระดับความน่าเชื่อถือที่แนะนำตามการคำนวณจากระดับความเสี่ยงตามมาตรฐานของ สท. ซึ่งมีวิธีการคำนวณโดยการหารระดับผลกระทบที่เป็นไปได้
- แนะนำตามระดับผลกระทบ เป็นหลักที่พิจารณาจากข้อมูลระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามการคำนวณระดับผลกระทบที่เป็นไปได้ตามมาตรฐานจากสหรัฐอเมริกา NIST SP 800-63-3 ซึ่งได้ทำการคำนวณโดยพิจารณาถึงผลกระทบในแต่ละประเภทที่เกิดจากภาคธุรกิจผู้ใช้งานประมวลผล

ข้อปฏิบัติในการใช้เครื่องมือ

เครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยงที่ใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ ถูกพัฒนาเพื่อรองรับมาตรฐาน มรด. ๑-๑ และ ๑-๒ ของ สท. (ฉบับมีผลบังคับใช้) เนื่องจากมีผลกระทบ 2 (2) หลักที่พิจารณาการประเมินเครื่องมือประเมินความเสี่ยงที่ใช้ในการพิสูจน์และยืนยันตัวตนของบริการภาครัฐตามที่เป็นตัวชี้วัดหน่วยงานภาครัฐที่มีเครื่องมือที่เป็นมาตรฐานเดียวกันและมีการปฏิบัติตามขั้นตอนมาตรฐาน โดยหน่วยงานภาครัฐสามารถประเมินระดับความน่าเชื่อถือที่แนะนำต่าง ๆ จากการคำนวณในตามต่าง ๆ เพื่อป้องกันผลกระทบที่มาตรฐานทั้งในระดับและต่างประเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

หน้าแรก STEP 1 STEP 2 STEP 3 หน้าสรุป หน้า printout ข้อมูลเพิ่มเติม ตัวอย่าง +