



Digital Government Development Agency

การประชุมเพื่อรับฟังความคิดเห็นต่อเครื่องมือประมวลผลอัตโนมัติ
สำหรับการประเมินความเสี่ยงเพื่อใช้ในการพิสูจน์และยืนยันตัวตน
สำหรับบริการภาครัฐ

ASSESSMENT



นางไอรดา เหลืองวิไล
รองผู้อำนวยการ
สำนักงานพัฒนารัฐบาลดิจิทัล



รศ.ดร. เกริก ภิรมย์โสภา
ประธานคณะทำงานเทคนิค
ด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ



คุณยุทธพล จินะสี
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ผู้แทนกรมสรรพากร



ดร.อุธีรภา เกตุพรหม
ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

facebook
LIVESTREAM

วันพฤหัสบดีที่ 20 มกราคม 2565 เวลา 13.30 - 15.30 น.
ผ่านช่องทาง Facebook DGA Thailand



<https://shorturl.asia/LiSM6>
สำหรับการลงทะเบียน



<https://shorturl.asia/OL8Z7>
ดาวน์โหลดเอกสาร

กำหนดการจัดงานรับฟังความคิดเห็นต่อเครื่องมือฯ

เวลา	หัวข้อบรรยาย/เสวนา	วิทยากร/ผู้ทรงคุณวุฒิ
13.20 – 13.30 น.	ลงทะเบียน	
13.30 – 13.40 น.	กล่าวเปิดงาน	นางไอรดา เหลืองวิไล รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
13.40 – 14.20 น.	การเสวนาในหัวข้อ “มั่นคงปลอดภัย ครอบคลุมบริการ ภาครัฐ ด้วยเครื่องมือด้านดิจิทัลไอดี”	1. รศ.ดร.เกริก ภิรมย์โสภา ประธานคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ 2. ดร.อุรัชฎา เกตุพรหม ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) 3. คุณยุทธพล จินะสี นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ หัวหน้าส่วนพัฒนาระบบบริหาร การเสียหายทางอิเล็กทรอนิกส์ กองบริหารการเสียหายทางอิเล็กทรอนิกส์ กรมสรรพากร
14.20 – 15.00 น.	การนำเสนอเครื่องมือประมวลผล อัตโนมัติสำหรับการประเมินความ เสี่ยงเพื่อใช้ในการพิสูจน์และยืนยัน ตัวตน	1. ผู้แทนฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) 2. ผู้แทนบริษัท สกาย อาย เทคโนโลยี จำกัด (ผู้พัฒนาเครื่องมือฯ)
15.00 – 15.30 น.	ตอบข้อซักถาม	

ช่องทาง การเสนอความคิดเห็น



<https://shorturl.asia/OL8Z7>

สามารถแสดงความคิดเห็นเข้ามาได้
ระหว่างวันที่ 4 มกราคม – 4 กุมภาพันธ์ 2565

https://standard.dga.or.th/standard-activities/activities-sd1/3129/

DGA Standard > กิจกรรมจัดทำมาตรฐาน > กิจกรรมการจัดทำมาตรฐานด้านการกระบวนการหรือการดำเนินงานทางดิจิทัล > ขอเชิญร่วมแสดงความคิดเห็นต่อเครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยงเพื่อใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ (Assessment Tool for Government Digital ID)

ขอเชิญร่วมแสดงความคิดเห็นต่อเครื่องมือประมวลผลอัตโนมัติสำหรับการประเมิน
ความเสี่ยงเพื่อใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ
(Assessment Tool for Government Digital ID)

**ASSESSMENT TOOL
FOR GOVERNMENT DIGITAL ID**

"การประชุมเพื่อรับฟังความคิดเห็น
ต่อเครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยง
เพื่อใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ"

วันพฤหัสบดีที่ 20 มกราคม 2565 เวลา 13.30 - 15.30 น.
ผ่านช่องทาง Facebook DGA Thailand

DGA

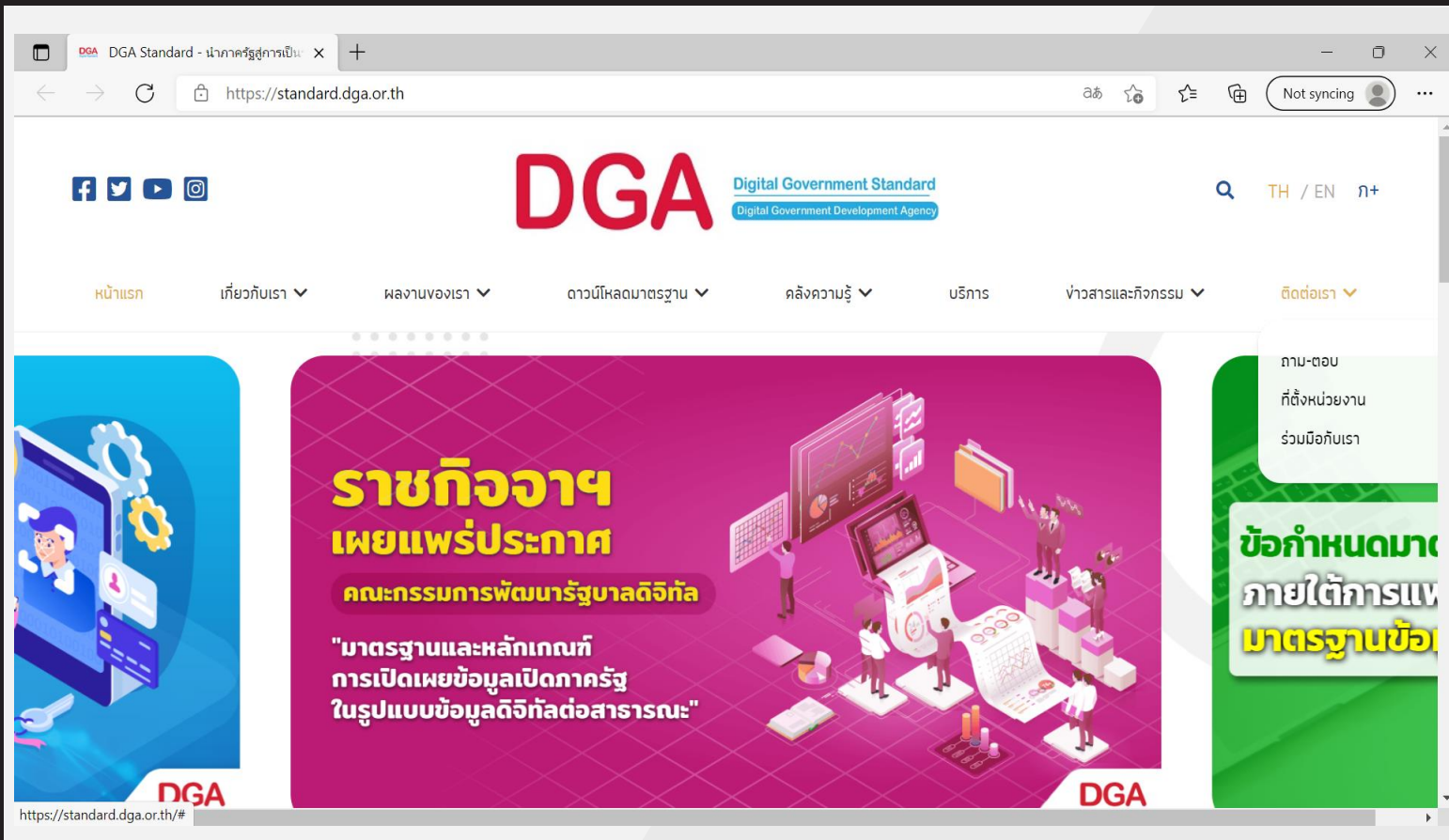
สแกน QR Code
เพื่อแสดงความคิดเห็น
ภายในวันศุกร์ที่ 4 กุมภาพันธ์ 2565

ลงทะเบียนเข้าร่วมงานประชุมรับฟังความเห็นฯ

ตอบแบบสำรวจแสดงความคิดเห็นฯ

Assessment Tool (V 1.3.7)

คู่มือการใช้งาน Assessment Tool (V 1.3.7)



ช่องทางติดต่อเพื่อสอบถาม ข้อมูล รับข่าวสาร หรือร่วม พัฒนามาตรฐาน

ประกอบด้วย 2 ช่องทาง ได้แก่

เว็บไซต์

- <https://standard.dga.or.th>

ติดต่อ DGA Contact Center:

- โทร : (+66) 02 612 6060
- อีเมล: contact@dga.or.th
- เว็บไซต์ : <https://www.dga.or.th/contact-dga/>



ไอรดา เหลืองวิไล

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล





Digital Government Development Agency

การประชุมเพื่อรับฟังความคิดเห็นต่อเครื่องมือประมวลผลอัตโนมัติน
สำหรับการประเมินความเสี่ยงเพื่อใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ

ASSESSMENT TOOL FOR GOVERNMENT DIGITAL ID

หัวข้อการเสวนา

"มั่นคงปลอดภัย ครอบคลุมบริการภาครัฐ ด้วยเครื่องมือด้านดิจิทัลไอดี"



รศ.ดร. เทริท ภิรมย์ไพศา

ประธานคณะทำงานเทคนิค
ด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ



คุณยุทธพล จินะสี

นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ผู้แทนกรมสรรพากร



ดร.จุริชฎา เกตุพรหม

ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ
สำนักงานพัฒนารัฐบาลดิจิทัล
(องค์การมหาชน)

facebook
LIVESTREAM

วันพฤหัสบดีที่ 20 มกราคม 2565 เวลา 13.30 - 15.30 น.
ผ่านช่องทาง Facebook DGA Thailand

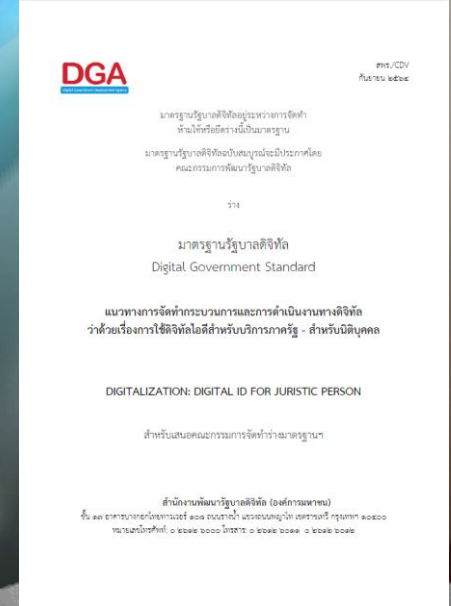
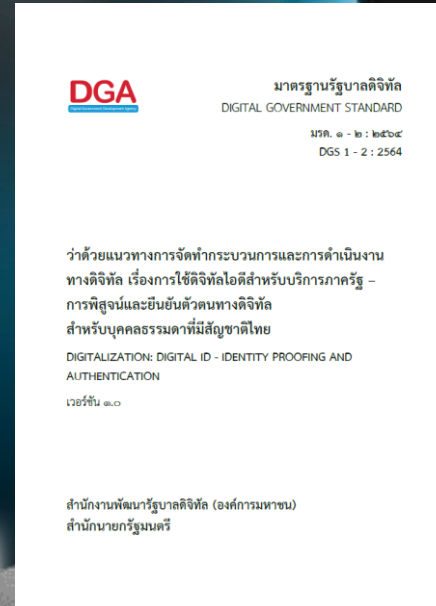
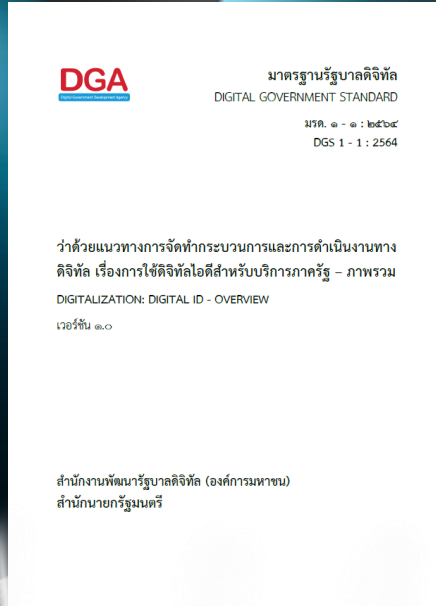
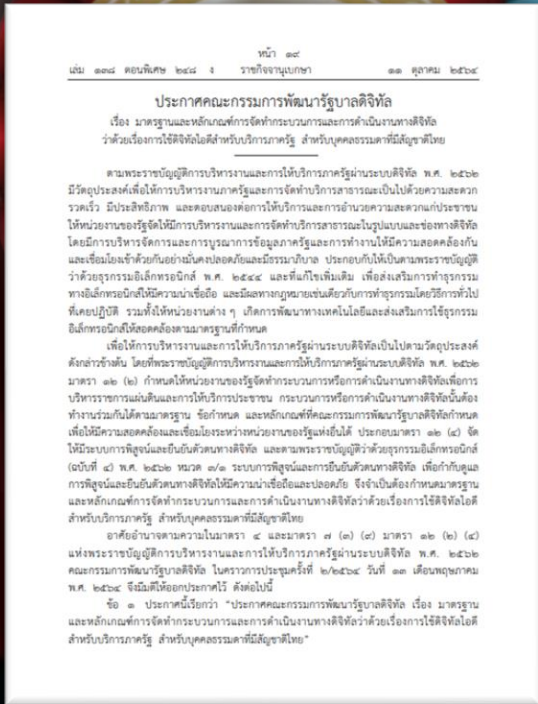
คณะทำงานเทคนิคด้านมาตรฐาน ความมั่นคงปลอดภัยภาครัฐ

หน้าที่และอำนาจ คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ

- 1. ศึกษาและจัดทำมาตรฐานและหลักเกณฑ์**เกี่ยวกับการจัดทำกระบวนการและการดำเนินงานทางดิจิทัลเกี่ยวกับความมั่นคงปลอดภัยภาครัฐ รวมถึงแนวปฏิบัติ คู่มือ และเอกสารอื่นที่เกี่ยวข้อง เพื่อนำเสนอต่อคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 เพื่อให้หน่วยงานของรัฐสามารถจัดทำกระบวนการและการดำเนินงานทางดิจิทัลดังกล่าวได้อย่างมีประสิทธิภาพและความมั่นคงปลอดภัย สามารถตอบสนองต่อความต้องการของทุกภาคส่วน
- 2. ให้ข้อเสนอแนะแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล** เรื่องวิธีการใช้และการใช้ดิจิทัลไอดี (Digital ID) สำหรับบริการภาครัฐ เพื่อประโยชน์ในการอำนวยความสะดวกในการบริการประชาชน ซึ่งมีมาตรฐานและแนวทางที่สอดคล้องกัน ตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด
- 3. ให้ข้อเสนอแนะแนวทางการจัดทำกระบวนการและการดำเนินงานในรูปแบบดิจิทัล (Digitalization)** ที่มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการเข้าสู่บริการดิจิทัลของหน่วยงานของรัฐ เพื่อให้มีกระบวนการที่ประสิทธิภาพ พร้อมใช้ น่าเชื่อถือ และสามารถตรวจสอบได้
4. เชิญผู้แทนจากหน่วยงานของรัฐ หรือหน่วยงานภาคเอกชน เข้าชี้แจงหรือขอให้สนับสนุนข้อมูลใด ๆ ต่อคณะทำงานได้ตามความเหมาะสม
5. ดำเนินการอื่นใดตามที่ผู้อำนวยการหรือคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มอบหมาย

ผลงานเด่น ปีงบประมาณ พ.ศ. 2564

Digital ID ได้ประกาศ ราชกิจจานุเบกษา 11 ตุลาคม 2564



IdP (ผู้พิสูจน์และยืนยันตัวตน)
RP (ผู้ให้บริการภาครัฐ)
AS (แหล่งให้ข้อมูลที่น่าเชื่อถือ)

การพิสูจน์และยืนยันตัวตนที่มีความมั่นคง ปลอดภัย สะดวก รวดเร็ว และทันสมัย

เพื่อให้หน่วยงานของรัฐและเอกชน มีเป็นมาตรฐานในรูปแบบเดียวกัน เกิดการบูรณาการระหว่างหน่วยงาน และในการนำ Digital ID ไปใช้สำหรับการให้บริการประชาชน เพื่อให้เกิดความมั่นคงปลอดภัย ลดขั้นตอน สะดวก รวดเร็ว ทันสมัย ซึ่งมาตรฐานรัฐบาลดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ ประกอบด้วย

- ภาพรวม >>> ได้ประกาศในราชกิจจานุเบกษา
- การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย >>> ได้ประกาศในราชกิจจานุเบกษา
- การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับนิติบุคคล >>> ผ่านคณะกรรมการจัดทำร่างฯ >>> จัดทำประชาพิจารณ์ เดือนมกราคม ๒๕๖๕



Digital Government Development Agency

การประชุมเพื่อรับฟังความคิดเห็นต่อเครื่องมือประมวลผลอัตโนมัต
สำหรับการประเมินความเสี่ยงเพื่อใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ

ASSESSMENT TOOL FOR GOVERNMENT DIGITAL ID



ดร. ธีรวัฒน์ โรจนไพฑูรย์
หัวหน้าทีมมาตรฐานดิจิทัลภาครัฐ 1
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)



นายสัมโมทิก สวิชญาณ
ผู้แทนบริษัท สกาย อาย เทคโนโลยี จำกัด

facebook
LIVESTREAM

วันพฤหัสบดีที่ 20 มกราคม 2565 เวลา 13.30 - 15.30 น.
ผ่านช่องทาง Facebook DGA Thailand

วัตถุประสงค์



เพื่อศึกษา ออกแบบ และพัฒนาเครื่องมือประมวลผลอัตโนมัติสำหรับการประเมินความเสี่ยง ในการใช้งาน Digital ID สำหรับการให้บริการภาครัฐ



เพื่อให้หน่วยงานของรัฐเกิดความเข้าใจรูปแบบวิธีการของการประเมินความเสี่ยง ในการใช้งาน Digital ID รวมทั้งการเลือกระดับความน่าเชื่อถือ (IAL และ AAL)



เพื่อให้หน่วยงานของรัฐมีเครื่องมือในการประเมินความเสี่ยงที่เป็นมาตรฐานเดียวกัน

มาตรฐานที่เกี่ยวข้อง

มาตรฐานภายในประเทศ



แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ

- ประกาศคณะกรรมการรัฐบาลดิจิทัล
- มรต. 1 - 1: 2564 (Overview)
- มรต. 1 - 2: 2564 (IAL & AAL)



แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย

- ขมรอ. 18-2564 (Framework)
- ขมรอ. 19-2564 (IAL)
- ขมรอ. 20-2564 (AAL)

มาตรฐานจากต่างประเทศ



General Services Administration, USA
Digital Identity Risk Assessment (DIRA)



NIST Digital Identity Guidelines

- SP 800-63-3 (Overview)
- SP 800-63-A (IAL)
- SP 800-63-B (AAL)
- SP 800-63-C (FAL)



Office of Management and Budget Memorandum (OMB) M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management

ประเภทกลุ่มการให้บริการของภาครัฐ

กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services)

บริการเผยแพร่ข้อมูลข่าวสารทั่วไป

- 1) เป็นข้อมูลเปิดสาธารณะหรือข้อมูลทั่วไป
- 2) ไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคล
- 3) ไม่จำเป็นต้องมีการลงทะเบียนและพิสูจน์ตัวตน

กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับ ผู้ให้บริการ (Enhanced Services)

บริการข้อมูลข่าวสารในรูปแบบการสื่อสารสองทางกับ
ผู้ให้บริการ เช่น การรับแจ้งเรื่องร้องเรียน

- 1) มีการสื่อสารโต้ตอบกับผู้ให้บริการ
- 2) ใช้ข้อมูลส่วนบุคคลหรือไม่ก็ได้
- 3) มีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลหรือไม่ก็ได้
- 4) มีช่องทางที่สามารถติดต่อได้

กลุ่มการให้บริการธุรกรรม (Transactional Services)

บริการธุรกรรมซึ่งมีผลผูกพันทางกฎหมาย
เช่น การอนุญาต การจดทะเบียน

- 1) ใช้ข้อมูลส่วนบุคคล
- 2) มีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล
- 3) มีการยืนยันช่องทางการติดต่อ

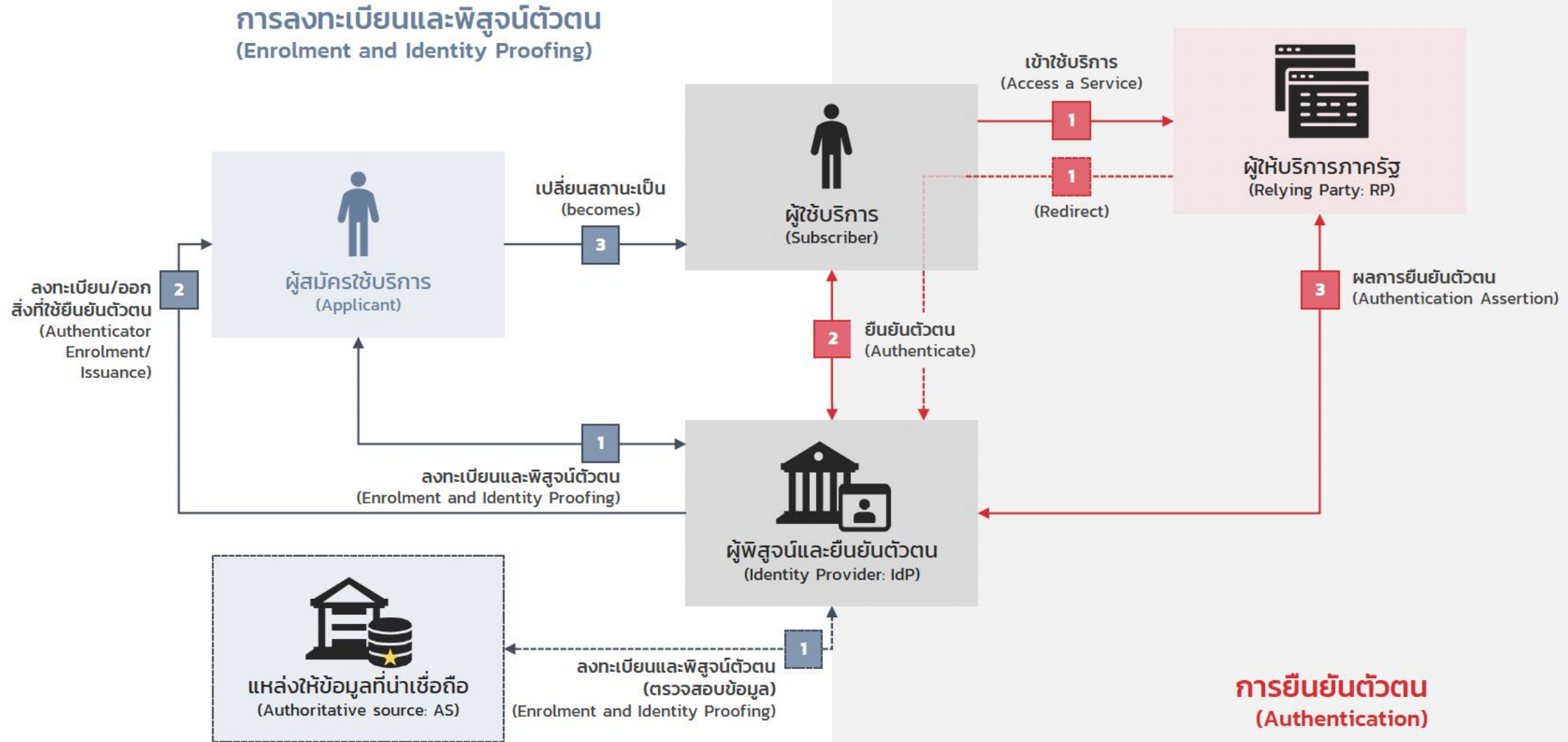
กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูล ระหว่างหน่วยงาน (Connected Services)

บริการธุรกรรมที่มีการเชื่อมโยงข้อมูลระหว่างหน่วยงาน

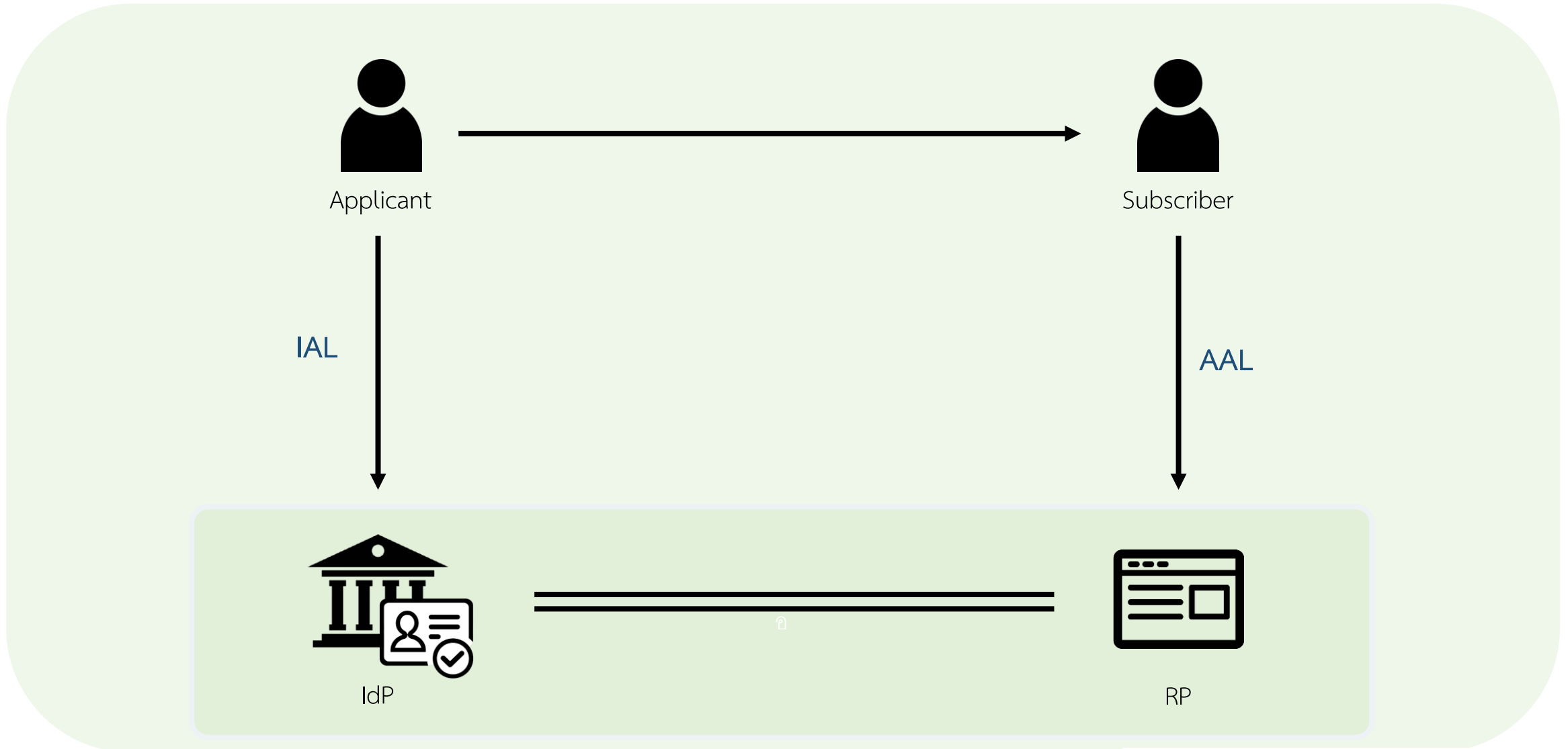
- 1) มีการเชื่อมโยงหรือใช้ข้อมูลร่วมกับหน่วยงาน
ภายนอกแห่งอื่น
- 2) ใช้ข้อมูลส่วนบุคคล
- 3) การลงทะเบียนและพิสูจน์ตัวตนครั้งแรก ต้องมีการ
พบเห็นต่อหน้า หรือเสมือนพบเห็นต่อหน้า
- 4) มีการยืนยันช่องทางการติดต่อ

แบบจำลองดิจิทัลไอดี

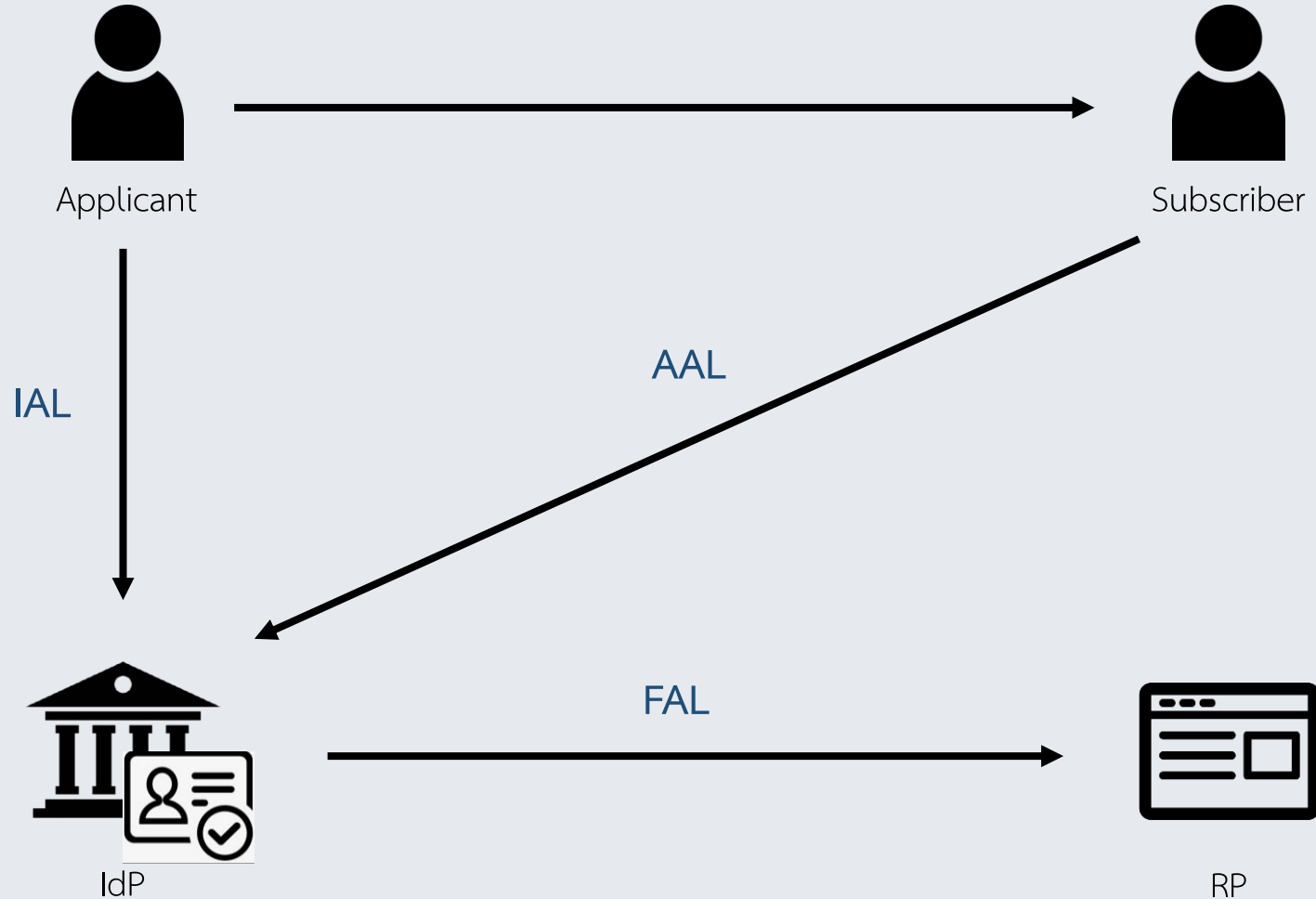
แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ที่เกี่ยวข้องกับแนวทางการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ



รูปแสดงระดับความน่าเชื่อถือต่าง ๆ กรณี **IdP** และ **RP** คือหน่วยงานเดียวกัน



รูปแสดงระดับความน่าเชื่อถือต่าง ๆ กรณี **IdP** และ **RP** คือ **คนละหน่วยงาน**



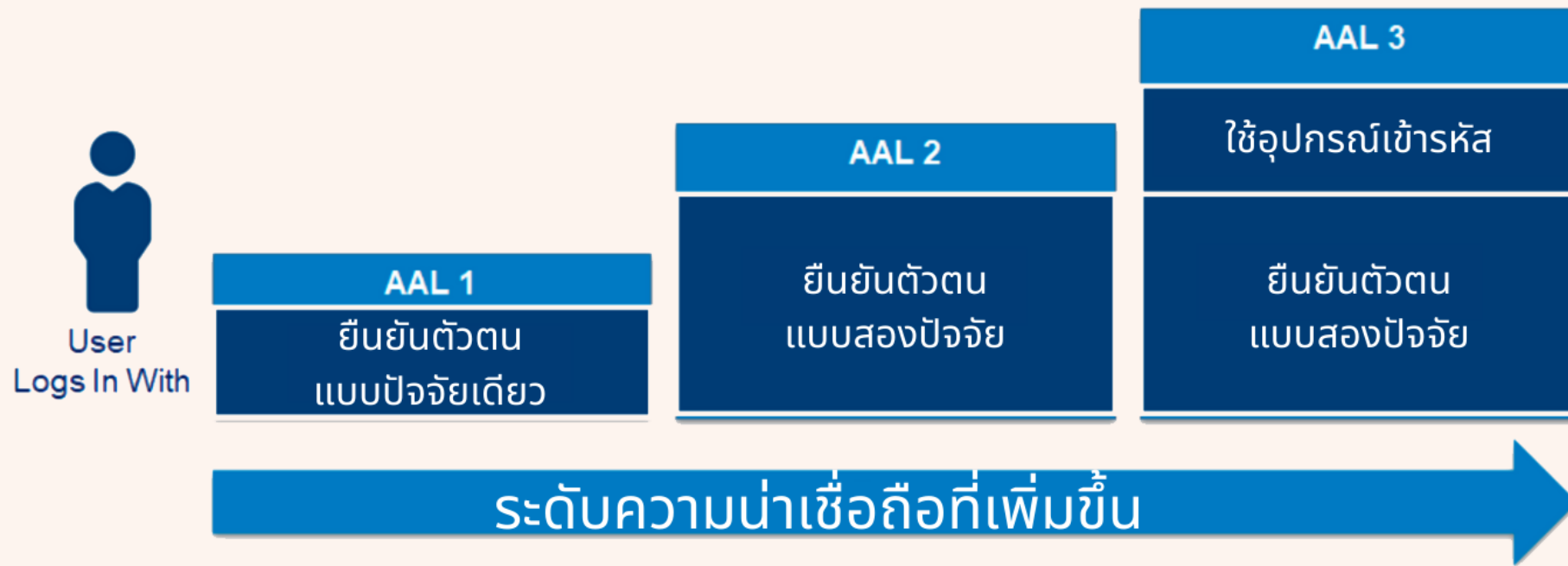
ระดับความน่าเชื่อถือของไอดีนิติ

(Identity Assurance Levels: IAL)



ความเข้มงวดของกระบวนการพิสูจน์ตัวตน เพื่อระบุตัวตนของบุคคลอย่างมั่นใจ IAL ถูกเลือกเพื่อลดข้อผิดพลาดในการพิสูจน์ตัวตนที่อาจเกิดขึ้น

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Levels: AAL)



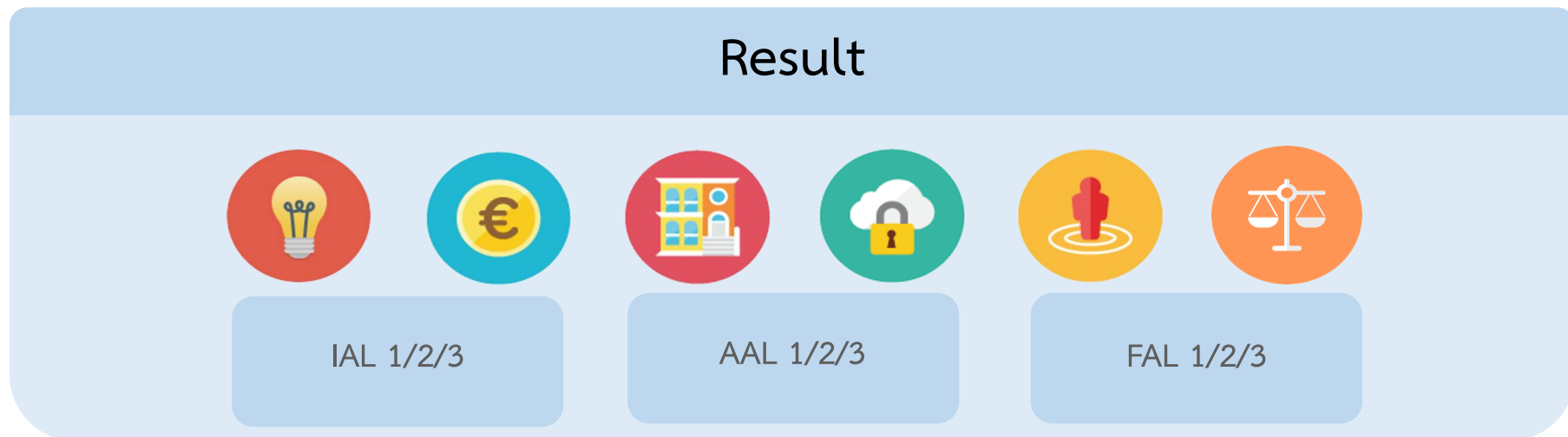
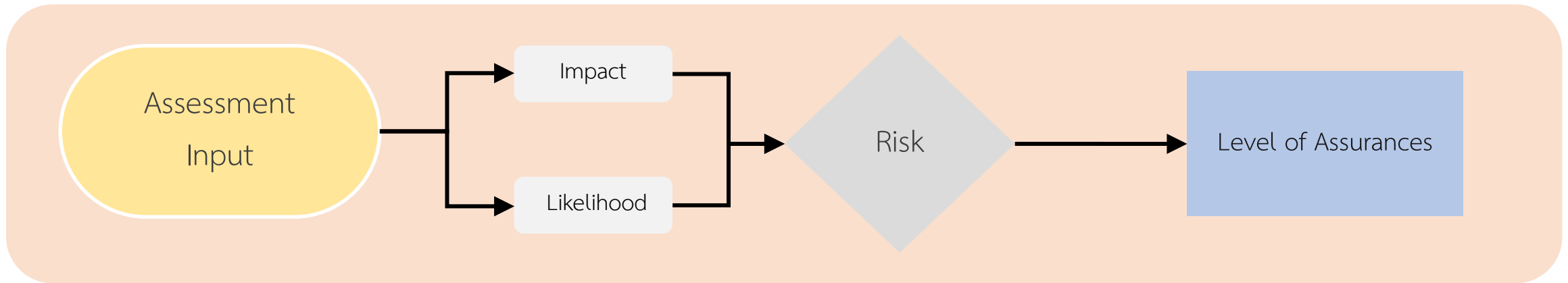
ความเข้มงวดของกระบวนการรับรองความถูกต้อง และการเชื่อมโยงระหว่างผู้ตรวจสอบความถูกต้องกับตัวระบุเฉพาะบุคคล AAL ได้รับเลือกเพื่อลดข้อผิดพลาดในการรับรองความถูกต้องที่อาจเกิดขึ้น

ระดับความน่าเชื่อถือการแลกเปลี่ยนข้อมูลไอดีentiระหว่างองค์กร (Federation Assurance Level: FAL)



ความแข็งแกร่งของโปรโตคอลการยืนยันที่สหพันธรัฐใช้เพื่อสื่อสารข้อมูลการรับรองความถูกต้องและ attribute (ถ้ามี) กับ RP

ขั้นตอนของเครื่องมือฯ (Assessment Tool)



ประเภทผลกระทบ (Impacts)



การใช้งานเครื่องมือประมวลผลอัตโนมัติ สำหรับการประเมินความเสี่ยง เพื่อใช้ในการพิสูจน์และยืนยันตัวตน สำหรับบริการภาครัฐ



Assessment Tool for Government Digital ID

คำแนะนำก่อนการใช้งานเครื่องมือฯ

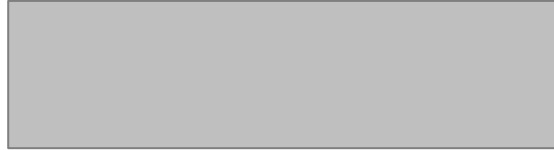
ก่อนใช้งานเครื่องมือหน่วยงานควรมีการหารือร่วมกันระหว่างผู้ที่เกี่ยวข้อง เพื่อหาข้อสรุปร่วมกัน ดังนี้

- กำหนดผู้รับผิดชอบการประเมิน อาจเป็นบุคคล หรือคณะทำงาน
- กรณีหน่วยงานมีบริการมากกว่าหนึ่งบริการ ให้แยกประเมินแต่ละบริการ
- กำหนดเกณฑ์ในการวัดระดับของผลกระทบ และระดับความเป็นไปได้ ในแต่ละด้านที่ประเมินให้ครบถ้วน
- สํารวจบริการของหน่วยงาน และจําแนกกลุ่มการบริการให้บริการ 4 กลุ่ม ตาม มรด. 1-1: 2564

ขั้นตอนการใช้งานเครื่องมือประเมินความเสี่ยง

- ผู้ประเมินสามารถใช้งานเครื่องมือฯ เริ่มประเมินความเสี่ยงเกี่ยวกับการพิสูจน์และยืนยันตัวตนสำหรับบริการภาครัฐ โดยการกรอกข้อมูลในตาราง**สีเหลือง**ใน sheet "หน้าแรก" เพื่อบันทึกข้อมูลของผู้ประเมินเอง รวมทั้ง ข้อมูลประเภทผู้ใช้งานและประเภทของธุรกรรมที่ถูกประเมิน
- ผู้ประเมินกรอกข้อมูลในตาราง**สีเทา**ในหน้า "**STEP 1**" "**STEP 2**" "**STEP 3**" ตามลำดับ เมื่อเสร็จสิ้นการกรอกข้อมูล เครื่องมือฯ จะทำการประมวลผลอัตโนมัติ เพื่อคำนวณระดับความน่าเชื่อถือ และจะปรากฏผลลัพธ์จากการคำนวณได้ในตารางสรุปในหน้า "**หน้าแรก**" และ "**หน้าสรุป**"
- ผู้ประเมินหรือผู้ประสานงานสามารถพิมพ์ผลลัพธ์การประเมินและผลสรุปของข้อมูลต่าง ๆ ได้ในหน้า "**หน้า print out**"

ความเชื่อมโยงระหว่างสีของตารางและข้อมูลภายใน



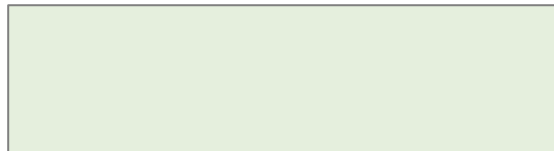
ตารางที่ผู้ประเมินต้องกรอกเพื่อนำไปคำนวณระดับความน่าเชื่อถือ



ตารางที่ผู้ประเมินต้องกรอกเพื่การบันทึกข้อมูล ไม่ถูกนำไปทำการคำนวณใดๆ



ตารางแสดงผลลัพธ์จากการคำนวณ



ตารางที่ให้ข้อมูลเพิ่มเติมซึ่งผู้ประเมินไม่ต้องกรอก

รายละเอียดของแต่ละหน้าในเครื่องมือประเมินความเสี่ยง

- "หน้าแรก"** หน้าสำหรับการกรอกและการบันทึกข้อมูลของผู้ประเมิน รวมถึงข้อมูลหน่วยงาน (agency profile) และข้อมูลเกี่ยวกับการประเมิน (assessment input) พร้อมทั้งสรุปผลลัพธ์จากการคำนวณจาก **"STEP 1"** **"STEP 2"** และ **"STEP 3"**
- "STEP 1"** หน้าสำหรับให้ผู้ประเมินกรอกข้อมูลประเภทของบริการ เพื่อนำไปประเมินระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร.
- "STEP 2"** หน้าสำหรับให้ผู้ประเมินกรอกข้อมูลผลกระทบที่อาจเกิดขึ้น โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น เพื่อกำหนดความเสี่ยงและระดับผลกระทบทั้ง 6 ประเภท
- "STEP 3"** หน้าสำหรับให้ผู้ประเมินกรอกข้อมูล เพื่อประเมินระดับความน่าเชื่อถือ โดยใช้ข้อมูลจากหน้า **"STEP 2"** เพื่อกำหนดระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ
- "หน้าสรุป"** หน้าแสดงผลลัพธ์จากการคำนวณใน **"STEP 2"** โดยใช้สี (**เขียว เหลือง และแดง**) เพื่อระบุระดับความเสี่ยง (ต่ำ ปานกลาง สูง) ที่คำนวณได้ของแต่ละประเภทผลกระทบ
- "หน้า print out"** หน้าแสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด
- "ข้อมูลเพิ่มเติม"** หน้าแสดงรายละเอียดวิธีการคำนวณและการให้คะแนนในแต่ละหัวข้อ

หน้าแรก : กรอกข้อมูลหน่วยงาน (agency profile) และข้อมูลเกี่ยวกับการประเมิน (assessment input) พร้อมทั้งแสดงผลข้อมูลจากการประมวลผล

Step 1: เลือกประเภทของบริการเพื่อ
กำหนดระดับความน่าเชื่อถือขั้นต่ำ

Step 2 : เลือกระดับประเภทของ
ผลกระทบ โอกาสที่จะเกิดขึ้น และเหตุผล
สนับสนุน

Step 3 : การเลือกระดับความน่าเชื่อถือ

หน้าสรุป : แสดงระดับความเสี่ยงและผลกระทบ

หน้า print out : หน้าแสดงข้อมูลและ
ผลลัพธ์ของการประมวลผลทั้งหมด

ข้อมูลเพิ่มเติม : เกณฑ์การให้คะแนนและ
การคำนวณ



เครื่องมือฯ : หน้าแรก

ข้อมูลผู้ประเมินความเสี่ยง	
ชื่อหน่วยงาน	
วันที่ประเมิน	
ผู้ประสานงานการประเมิน	
ผู้ตรวจสอบและยืนยันผลการประเมิน	

ข้อมูลบริการและผู้ใช้งานที่ถูกประเมินความเสี่ยง	
ชื่อบริการ	
ผู้ใช้บริการ	
จุดประสงค์การใช้บริการของผู้ใช้งาน	

ตารางที่ต้องกรอก ไม่มีผลต่อการคำนวณ

ช่องสำหรับให้ผู้ใช้งานกรอกข้อมูลหน่วยงาน
เป็นช่องที่ต้องพิมพ์กรอกเอง
ไม่ได้มีผลต่อการคำนวณ

ตารางที่ต้องกรอก ไม่มีผลต่อการคำนวณ

ช่องสำหรับให้ผู้ใช้งานกรอกข้อมูลผู้ใช้งานและ
ธุรกรรมเป็นช่องที่ต้องพิมพ์กรอกเอง
ไม่ได้มีผลต่อการคำนวณ

ประชาชนทั่วไป
เจ้าหน้าที่รัฐภายในหน่วยงาน
เจ้าหน้าที่รัฐภายนอกหน่วยงาน

ช่อง “ประเภทผู้ใช้งาน” ผู้ประเมินสามารถ
เลือกคำตอบจาก drop down list
หรือสามารถพิมพ์กรอกได้

เครื่องมือฯ : หน้าแรก

ตารางผลลัพธ์

- แนะนำตามประเภทบริการ เป็นผลการประเมินเบื้องต้นตามประเภทบริการ
- แนะนำตามระดับความเสี่ยง เป็นผลการประเมินจากผลกระทบและโอกาสที่จะเกิดขึ้น
- แนะนำตามระดับผลกระทบ เป็นผลการประเมินจากผลกระทบอย่างเดียว

ระดับความน่าเชื่อถือขั้นต่ำที่แนะนำ

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

เครื่องมือฯ : หน้าแรก (วิธีการใช้งานเครื่องมือฯ)

วิธีการใช้เครื่องมือประเมินความเสี่ยง

ขั้นตอนการใช้งานเครื่องมือประเมินความเสี่ยง

- ผู้ประเมินหรือผู้ประสานงานสามารถใช้งานเครื่องมือฯ เพื่อประเมินความเสี่ยงเกี่ยวกับการพิสูจน์และยืนยันตัวตนสำหรับบริการภาครัฐ
- ผู้ประเมินหรือผู้ประสานงานสามารถเริ่มต้นการใช้งานเครื่องมือฯ จากการกรอกข้อมูลในตารางสีเหลืองใน sheet "หน้าแรก" เพื่อบันทึกข้อมูลของผู้ประเมินเอง รวมทั้งข้อมูลบริการและผู้ให้บริการของธุรกรรมที่ถูกประเมิน
- จากนั้นผู้ประเมินหรือผู้ประสานงานกรอกข้อมูลในตารางสีเทาในหน้า "STEP 1" "STEP 2" "STEP 3" ตามลำดับ เมื่อเสร็จสิ้นการกรอกข้อมูล เครื่องมือฯ จะทำการประมวลผลอัตโนมัติเพื่อคำนวณระดับความน่าเชื่อถือ
- ผู้ประเมินหรือผู้ประสานงานสามารถดูผลลัพธ์จากการคำนวณได้ในตารางสรุปในหน้า "หน้าแรก" และ "หน้าสรุป" ของเครื่องมือฯ
- ผู้ประเมินหรือผู้ประสานงานสามารถพิมพ์ผลลัพธ์การประเมินและผลสรุปของข้อมูลต่าง ๆ ได้ในหน้า "หน้า print out"

ความเชื่อมโยงระหว่างสีของตารางและข้อมูลภายใน

	ตารางที่ผู้ประเมินต้องกรอกเพื่อนำไปคำนวณระดับความน่าเชื่อถือ
	ตารางที่ผู้ประเมินต้องกรอกเพื่อนำบันทึกข้อมูล หากไม่ถูกนำไปทำการคำนวณใด ๆ
	ตารางแสดงผลลัพธ์จากการคำนวณ
	ตารางที่ให้ข้อมูลเพิ่มเติมซึ่งผู้ประเมินไม่ต้องกรอก

รายละเอียดของแต่ละหน้าในเครื่องมือประเมินความเสี่ยง

"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"	หน้าสำหรับให้ผู้ประเมินกรอกข้อมูลผลกระทบที่อาจจะเกิดขึ้น 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 print out"	หน้าแสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด
"ข้อมูลเพิ่มเติม"	หน้าแสดงรายละเอียดวิธีการคำนวณและการให้คะแนนในแต่ละหัวข้อ

ตารางข้อมูลเพิ่มเติม

ไม่จำเป็นต้องกรอกอะไร เป็นกล่องอธิบายวิธีการใช้งานเครื่องมือประเมินความเสี่ยง โดยแบ่งเป็น 3 ส่วนคือ

- (1) ขั้นตอนการใช้งานเครื่องมือและสิ่งที่ต้องกรอก
- (2) ความเชื่อมโยงระหว่างสีของตาราง และข้อมูลที่อยู่ข้างในตารางนั้น ๆ
- (3) รายละเอียดของแต่ละหน้าในเครื่องมือประเมินความเสี่ยง

เครื่องมือฯ : STEP 1

Sheet

STEP 1		ข้อมูลประเภทบริการภาครัฐ	
บริการที่ถูกประเมิน จัดว่าเป็นบริการประเภทใด ตามตารางสีเขียวด้านขวานี้		กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services)	มีข้อมูลที่เปิดเป็นสาธารณะหรือข้อมูลทั่วไป
ประเภทของบริการ	กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ให้บริการ		ไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคล
			ไม่จำเป็นต้องมีการลงทะเบียนและพิสูจน์ตัวตน
ระดับความน่าเชื่อถือขั้นต่ำที่แนะนำตามมาตรฐานของ สพร.		กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ให้บริการ (Enhanced Services)	มีการสื่อสารโต้ตอบกับผู้ให้บริการ
ประเภทระดับความน่าเชื่อถือ	ระดับความน่าเชื่อถือขั้นต่ำ		ใช้ข้อมูลส่วนบุคคล หรือไม่ก็ได้โดยเจ้าของข้อมูลส่วนบุคคล ไม่จำเป็นต้องเป็นผู้ดำเนินการเอง
ระดับความน่าเชื่อถือของไอเดนทิตี (IAL)	1		มีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล หรือไม่ได้
ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL)	1		มีช่องทางที่สามารถติดต่อได้
		กลุ่มการให้บริการธุรกรรม (Transactional Services)	ต้องใช้ข้อมูลส่วนบุคคล (เช่น เลขประจำตัว 13 หลัก) โดยเจ้าของข้อมูลส่วนบุคคล ต้องเป็นผู้ดำเนินการเอง ณ ขณะนั้น
			ต้องมีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล
		กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน (Connected Services)	ต้องยืนยันช่องทางการติดต่อ (หมายเลขโทรศัพท์ หรือ อีเมล)
			ต้องมีการเชื่อมโยงหรือใช้ข้อมูลร่วมกับหน่วยงานภายนอกแห่งอื่น
			ต้องใช้ข้อมูลส่วนบุคคล (เช่น เลขประจำตัว 13 หลัก) โดยเจ้าของข้อมูลส่วนบุคคล ต้องเป็นผู้ดำเนินการเอง ณ ขณะนั้น หรือมีการมอบอำนาจ
			ต้องมีการพบเห็นต่อหน้าหรือ เสมือนพบเห็นต่อหน้า (ต้องดำเนินการต่อหน้าเจ้าหน้าที่งานสำหรับการลงทะเบียนครั้งแรก)
			ต้องยืนยันช่องทางการติดต่อ (หมายเลขโทรศัพท์ หรือ อีเมล)

หน้าแรกSTEP 1STEP 2STEP 3หน้าสรุปหน้า printoutข้อมูลเพิ่มเติม

หน้าแรก : กรอกข้อมูลหน่วยงาน (agency profile) และข้อมูลเกี่ยวกับการประเมิน (assessment input) พร้อมทั้ง แสดงผลข้อมูลจากการประมวลผล

STEP 1 : เลือกประเภทของบริการ เพื่อกำหนดระดับความน่าเชื่อถือขั้นต่ำ

STEP 2 : เลือกระดับประเภทของผลกระทบ โอกาสที่จะเกิดขึ้น และผลสนับสนุน

STEP 3 : การเลือกระดับความน่าเชื่อถือ

หน้าสรุป : แสดงระดับความเสี่ยงและผลกระทบ

หน้า print out : หน้าแสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด

ข้อมูลเพิ่มเติม : เกณฑ์การให้คะแนนและการคำนวณ

เครื่องมือฯ : STEP 1 (Drop down list เลือกกลุ่มประเภทของบริการ)

STEP 1	
บริการที่ถูกประเมิน จัดว่าเป็นบริการประเภทใด ตามตารางสีเขียวด้านขวานี้	
ประเภทของบริการ	

ตารางที่ต้องกรอก

กล่องเพื่อแสดงระดับความน่าเชื่อถือขั้นต่ำที่แนะนำสำหรับแต่ละบริการภาครัฐโดยอ้างอิงจากมาตรฐานของ สพร.

ผู้ใช้งานกรอกข้อมูลโดยเลือกข้อมูลจาก Drop down list

กลุ่มการให้บริการข้อมูลพื้นฐาน
 กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ
 กลุ่มการให้บริการธุรกรรม
 กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน

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

ตารางผลลัพธ์

ตารางแสดงผลลัพธ์โดยเมื่อผู้ประเมินทำการเลือก drop down list ใน **STEP 1** เป็นที่เรียบร้อยแล้ว จะมีการแสดงระดับความน่าเชื่อถือที่แนะนำจะขึ้นมาให้โดยอัตโนมัติ

เครื่องมือ 4 : STEP 1 (แสดงข้อมูลแต่ละกลุ่มบริการภาครัฐ)

ข้อมูลประเภทบริการภาครัฐ	
กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services)	มีข้อมูลที่เปิดเป็นสาธารณะหรือข้อมูลทั่วไป ไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคล ไม่จำเป็นต้องมีการลงทะเบียนและพิสูจน์ตัวตน
กลุ่มการให้บริการข้อมูลที่มีการ ปฏิสัมพันธ์กับผู้ใช้บริการ (Enhanced Services)	มีการสื่อสารโต้ตอบกับผู้ใช้บริการ ใช้ข้อมูลส่วนบุคคล หรือไม่ก็ได้โดยเจ้าของข้อมูลส่วนบุคคล ไม่จำเป็นต้องเป็นผู้ดำเนินการเอง มีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล หรือไม่ก็ได้ มีช่องทางที่สามารถติดต่อได้
กลุ่มการให้บริการธุรกรรม (Transactional Services)	ต้องใช้ข้อมูลส่วนบุคคล (เช่น เลขประจำตัว 13 หลัก) โดยเจ้าของข้อมูลส่วนบุคคล ต้องเป็นผู้ดำเนินการเอง ณ ขณะนั้น ต้องมีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล ต้องยืนยันช่องทางการติดต่อ (หมายเลขโทรศัพท์ หรือ อีเมล)
กลุ่มการให้บริการธุรกรรมที่ เชื่อมโยงข้อมูลระหว่างหน่วยงาน (Connected Services)	ต้องมีการเชื่อมโยงหรือใช้ข้อมูลร่วมกับหน่วยงานภายนอกแห่งอื่น ต้องใช้ข้อมูลส่วนบุคคล (เช่น เลขประจำตัว 13 หลัก) โดยเจ้าของข้อมูลส่วนบุคคล ต้องเป็นผู้ดำเนินการเอง ณ ขณะนั้น หรือมีการมอบอำนาจ ต้องมีการพบเห็นต่อหน้าหรือ เสมือนพบเห็นต่อหน้า (ต้องดำเนินการต่อหน้าเจ้าพนักงานสำหรับการลงทะเบียนครั้งแรก) ต้องยืนยันช่องทางการติดต่อ (หมายเลขโทรศัพท์ หรือ อีเมล)

→ ตารางข้อมูลเพิ่มเติม

ไม่จำเป็นต้องกรอกอะไร เป็นกล่องอธิบาย
และให้ข้อมูลประเภทบริการภาครัฐต่าง ๆ
ทั้ง 4 ประเภท โดยอ้างอิงตามมาตรฐานที่
สพร. กำหนด

STEP 1: เลือกประเภทของบริการเพื่อ
กำหนดระดับความน่าเชื่อถือขั้นต่ำ

STEP 2 : เลือกระดับประเภทของ
ผลกระทบ โอกาสที่จะเกิดขึ้น และ
เหตุผลสนับสนุน

STEP 3 : การเลือกระดับความน่าเชื่อถือ

หน้าสรุป : แสดงระดับความเสี่ยงและผลกระทบ

หน้า print out : หน้าแสดงข้อมูลและ
ผลลัพธ์ของการประมวลผลทั้งหมด

ข้อมูลเพิ่มเติม : เกณฑ์การให้คะแนนและ
การคำนวณ

[illegible]

เครื่องมือ 4 : STEP 2

STEP 2			
• ผู้ใช้บริการในที่นี้ คือผู้ให้บริการที่ระบุไว้ในหน้าแรก • ถ้าผลกระทบจากเหตุการณ์อันเป็นความเสี่ยง สามารถเกิดกับบุคคลหรือองค์กรได้หลายฝ่าย ให้พิจารณาฝ่ายที่ได้รับผลกระทบมากที่สุด • คลิกลูกที่ "ตัวอย่าง" เพื่อดูตัวอย่างการพิจารณาผลกระทบและระดับผลกระทบ อันเนื่องมาจากเหตุการณ์อันเป็นความเสี่ยง			
เหตุการณ์อันเป็นความเสี่ยง	ระดับผลกระทบ	ระดับความเป็นไปได้	เหตุผลสนับสนุนคำตอบ (ถ้ามี)
ตัวอย่าง	ผลกระทบด้านความไม่สะดวกสวและเสียชื่อเสียง ที่มีต่อบุคคล หรือองค์กร		
1 หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนที่ปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2 หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสมรอยเข้าใช้งานแทน			
4 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ตัวอย่าง	ผลกระทบด้านความเสียหายทางการเงิน ที่มีต่อบุคคล หรือองค์กร		
1 หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนที่ปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2 หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสมรอยเข้าใช้งานแทน			
4 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ตัวอย่าง	ผลกระทบด้านความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ ที่มีต่อบุคคล หรือองค์กร		
1 หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนที่ปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2 หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสมรอยเข้าใช้งานแทน			
4 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ตัวอย่าง	ผลกระทบด้านความเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ที่มีต่อบุคคล หรือองค์กร		
1 หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนที่ปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2 หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสมรอยเข้าใช้งานแทน			
4 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ตัวอย่าง	ผลกระทบด้านความปลอดภัยของบุคคล ที่มีต่อบุคคล		
1 หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนที่ปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2 หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสมรอยเข้าใช้งานแทน			
4 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			
ตัวอย่าง	ผลกระทบด้านความละเมิดทางแพ่งหรือทางอาญา ที่มีต่อบุคคล หรือองค์กร		
1 หากผู้ใช้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนที่ปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น			
2 หากผู้ใช้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน			
3 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสมรอยเข้าใช้งานแทน			
4 หากผู้ใช้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน			

ตารางที่ต้องกรอก

ผู้ใช้งานกรอกข้อมูลโดยเลือกข้อมูลจาก Drop down list เพื่อเอาไปคำนวณคะแนนในด้านต่าง ๆ

ไม่มี
ต่ำ
ปานกลาง
สูง

มีโอกาสเกิดขึ้นต่ำ
มีโอกาสเกิดขึ้นปานกลาง
มีโอกาสเกิดขึ้นสูง

แถว “เหตุผลสนับสนุนคำตอบ (ถ้ามี)” คือช่องว่างที่ผู้ประเมินสามารถพิมพ์ ผลสนับสนุนคำตอบหรือคำอธิบายเพิ่มเติม โดยจะสามารถเลือกตอบหรือเว้นว่างก็ได้ ไม่ได้มีผลต่อการคำนวณใด ๆ

[illegible]

เครื่องมือ 4 : STEP 2

ระดับความเสี่ยง (0-9)			
ประเภทผลกระทบ	พิสูจน์ตัวตนผิดพลาด	ยืนยันตัวตนผิดพลาด	เชื่อมโยงกับองค์กรอื่นผิดพลาด
ความไม่สะดวกสบายและการเสื่อมเสียชื่อเสียง	0	0	0
ความเสียหายทางการเงิน	0	0	0
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	0	0	0
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	0	0	0
ความปลอดภัยของบุคคล	0	0	0
การละเมิดทางแพ่งหรือทางอาญา	0	0	0

ตารางผลลัพธ์

กล่องแสดงผลลัพธ์ของการคำนวณระดับความเสี่ยงที่ได้จากหน้าที่ 3 (STEP 2) เมื่อกรอกข้อมูลใน STEP 2 ครบ จะขึ้นเป็นเลขคะแนนและสี (เขียว เหลือง แดง) ตามลำดับความรุนแรง โดยมีคะแนนจาก 0-9

ระดับผลกระทบ (0-3)			
ประเภทผลกระทบ	พิสูจน์ตัวตนผิดพลาด	ยืนยันตัวตนผิดพลาด	เชื่อมโยงกับองค์กรอื่นผิดพลาด
ความไม่สะดวกสบายและการเสื่อมเสียชื่อเสียง	0	0	0
ความเสียหายทางการเงิน	0	0	0
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	0	0	0
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	0	0	0
ความปลอดภัยของบุคคล	0	0	0
การละเมิดทางแพ่งหรือทางอาญา	0	0	0

ตารางผลลัพธ์

กล่องแสดงผลลัพธ์ของการคำนวณระดับผลกระทบที่ได้จากหน้าที่ 3 (STEP 2) เมื่อกรอกข้อมูลใน STEP 2 ครบ จะขึ้นเป็นเลขคะแนนและสี (เขียว เหลือง แดง) ตามลำดับความรุนแรง โดยมีคะแนนจาก 0-3

เครื่องมือฯ : STEP 3

Sheet

	A	B	C	D	E	F	G	H	I
1	STEP 3								
2	หากข้อคำถามเปลี่ยนเป็นแรงงาเสียเท่า คำตอบข้อนั้นจะไม่ส่งผลต่อการประเมินระดับความน่าเชื่อถือ								
3	การกำหนดระดับความน่าเชื่อถือ								
4	1	บริการมีการเชื่อมโยงข้อมูลไอเดนติตี้กับองค์กรอื่นผ่านเครือข่ายคอมพิวเตอร์หรือไม่	ไม่ใช่						
5	2	บริการจำเป็นต้องใช้ข้อมูลส่วนบุคคลจากผู้ใช้งาน ในการให้บริการหรือไม่	ใช่						
6	3	บริการจำเป็นต้องพิสูจน์ตัวตนและตรวจสอบข้อมูลส่วนตัวดังกล่าวก่อน จึงจะให้บริการได้ ใช่หรือไม่	ไม่ใช่						
7	4	ผู้ใช้งานสามารถเข้าถึงข้อมูลส่วนบุคคลที่เคยให้ไว้ ได้หรือไม่	ไม่ใช่						
8	5	ข้อมูลแสดงการเข้าสู่ระบบของผู้ใช้งาน* ประกอบด้วยข้อมูลส่วนตัวหรือไม่							
9	6	บริการมีการเชื่อมโยงข้อมูลไอเดนติตี้กับองค์กรอื่นผ่านทาง front channel** หรือไม่							
10									
11	* ข้อมูลแสดงการเข้าสู่ระบบของผู้ใช้งาน (assertion) เป็นข้อมูลที่แลกเปลี่ยนระหว่าง IdP และ RP								
12	** front channel คือ ช่องทางสื่อสารระหว่าง IdP และ RP โดยมี "ผู้ถือครองไอเดนติตี้" (holder) คั่นกลางอยู่								
13									
14									
15									
16									
17									
18									
19									
20									

ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับความเสี่ยง	
IAL	1
AAL	1
FAL	ไม่เกี่ยวข้องกับบริการ

ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับผลกระทบ	
IAL	1
AAL	1
FAL	ไม่เกี่ยวข้องกับบริการ

หน้าแรก

STEP 1

STEP 2

STEP 3

หน้าสรุป

หน้า printout

ข้อมูลเพิ่มเติม

+

:

ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับความเสี่ยง	
IAL	1
AAL	1
FAL	ไม่เกี่ยวข้องกับบริการ

ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับผลกระทบ	
IAL	1
AAL	1
FAL	ไม่เกี่ยวข้องกับบริการ

หน้าแรก : กรอกข้อมูลหน่วยงาน (agency profile) และข้อมูลเกี่ยวกับการประเมิน (assessment input) พร้อมทั้งแสดงผลข้อมูลจากการประมวลผล

STEP 1 : เลือกประเภทของบริการเพื่อกำหนดระดับความน่าเชื่อถือขั้นต่ำ

STEP 2 : เลือกระดับประเภทของผลกระทบ โอกาสที่จะเกิดขึ้น และผลสนับสนุน

STEP 3 : การเลือกระดับความน่าเชื่อถือ

หน้าสรุป : แสดงระดับผลกระทบ

หน้า print out : หน้าแสดงข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด

ข้อมูลเพิ่มเติม : เหนกที่การให้คะแนนและการคำนวณ

เครื่องมือฯ : STEP 3

STEP 3

- หากช่องคำตอบเปลี่ยนเป็นแรงเสีเทา คำตอบช่องนั้นจะไม่ส่งผลการประเมินระดับความน่าเชื่อถือ

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

ตารางที่ต้องกรอก



ผู้ประเมินสามารถเลือกกรอกข้อมูลจากช่องใน drop down list เพื่อเอาไปคำนวณการใช้ระดับความน่าเชื่อถือที่เหมาะสม

เครื่องมือ 4 : STEP 3

ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับความเสี่ยง	
IAL	ยังตอบคำถามไม่ครบ
AAL	ยังตอบคำถามไม่ครบ
FAL	ยังตอบคำถามไม่ครบ



ตารางผลลัพธ์

กล่องแสดงผลลัพธ์ "ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับความเสี่ยง" จะแสดงระดับความน่าเชื่อถือของการคำนวณความเสี่ยงที่ได้จากการกรอกข้อมูลในหน้าที่ 4 (**STEP 3**) และผลลัพธ์จากข้อมูลที่กรอกในหน้าที่ 3 (**STEP 2**) โดยข้อมูลในกล่องผลลัพธ์จะขึ้นให้โดยอัตโนมัติ

ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับผลกระทบ	
IAL	ยังตอบคำถามไม่ครบ
AAL	ยังตอบคำถามไม่ครบ
FAL	ยังตอบคำถามไม่ครบ



ตารางผลลัพธ์

กล่องแสดงผลลัพธ์ "ระดับความน่าเชื่อถือขั้นต่ำ ที่แนะนำจากระดับผลกระทบ" จะแสดงระดับความน่าเชื่อถือของการคำนวณผลกระทบที่ได้จากการกรอกข้อมูลในหน้าที่ 4 (**STEP 3**) และผลลัพธ์จากข้อมูลที่กรอกในหน้าที่ 3 (**STEP 2**) โดยข้อมูลในกล่องผลลัพธ์จะขึ้นให้โดยอัตโนมัติ

เครื่องมือฯ : หน้าสรุป

Sheet

Home Insert Draw Page Layout Formulas Data Review View Tell me									
AB52									

หน้าแรก : กรอกข้อมูลหน่วยงาน (agency profile) และข้อมูลเกี่ยวกับการประเมิน (assessment input) พร้อมทั้งแสดงผลข้อมูลจากการประมวลผล

STEP 1 : เลือกประเภทของบริการเพื่อกำหนดระดับความน่าเชื่อถือขั้นต่ำ

STEP 2 : เลือกระดับประเภทของผลกระทบ โอกาสที่จะเกิดขึ้น และผลสนับสนุน

STEP3 : การเลือกระดับความน่าเชื่อถือ

หน้าสรุป : แสดงระดับความเสี่ยงและผลกระทบ

หน้า print out : หน้าแสดงผลข้อมูลและผลลัพธ์ของการประมวลผลทั้งหมด

ข้อมูลเพิ่มเติม : เกณฑ์การให้คะแนนและการคำนวณ

ตารางผลลัพธ์

กล่องแสดงผลลัพธ์ของการคำนวณที่ได้จากหน้าที่ 3 (STEP 2) เมื่อกรอกข้อมูลใน STEP 2 ครบ จะขึ้นเป็นเลขคะแนนเพราะสี (เขียว เหลือง แดง) ตามลำดับความรุนแรง โดยคำนวณจาก ซึ่งจะมีค่าที่เป็นไปได้ 0-3 คะแนน

ประเภทผลกระทบ	สรุประดับผลกระทบ			อธิบายความหมายของสีและตัวเลขระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	พิสูจน์ตัวตนผิดพลาด	ยืนยันตัวตนผิดพลาด	เชื่อมโยงกับองค์กรอื่นผิดพลาด	ต่ำ	ปานกลาง	สูง
ความไม่สะดวกสบายและเสี่ยงชื่อเสียง	0	0	0	มีความไม่สะดวกสบายและเสี่ยงชื่อเสียงในระยะสั้น และจำกัด	มีความไม่สะดวกสบายและเสี่ยงชื่อเสียงรุนแรง ระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบายและเสี่ยงชื่อเสียงระยะยาว หรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	0	0	0	มีความเสียหายทางการเงินที่ไม่มีนัยสำคัญ	มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	0	0	0	มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	0	0	0	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับต่ำ	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับปานกลาง	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับสูง
ความปลอดภัยของบุคคล	0	0	0	บาดเจ็บเล็กน้อย ไม่ต้องการรักษาพยาบาล	มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องการการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัส หรือถึงแก่ชีวิต
การละเมิดทางแพ่งหรือทางอาญา	0	0	0	การฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อย ซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงเป็นพิเศษในการที่จะถูกบังคับใช้กฎหมาย

ตารางผลลัพธ์

กล่องแสดงผลลัพธ์ของการคำนวณที่ได้จากหน้าที่ 3 (STEP 2) เมื่อกรอกข้อมูลใน STEP 2 ครบ จะขึ้นเป็นเลขคะแนนเพราะสี (เขียว เหลือง แดง) ตามลำดับความรุนแรง โดยคำนวณจาก ซึ่งจะมีค่าที่เป็นไปได้ 0-9 คะแนน

ประเภทผลกระทบ	สรุประดับความเสี่ยง			อธิบายความหมายของสีและตัวเลขระดับความเสี่ยงเมื่อเกิดข้อผิดพลาด			
	พิสูจน์ตัวตนผิดพลาด	ยืนยันตัวตนผิดพลาด	เชื่อมโยงกับองค์กรอื่นผิดพลาด	ระดับความเสี่ยง	ระดับคะแนน	แทนด้วย	ความหมาย
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	0	0	0	สูง	6-9		ระดับความเสี่ยงที่หน่วยงานของรัฐไม่สามารถยอมรับได้และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
ความเสียหายทางการเงิน	0	0	0				
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	0	0	0	ปานกลาง	2-4		ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยงเพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	0	0	0				
ความปลอดภัยของบุคคล	0	0	0	ไม่มีหรือต่ำ	0-1		ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
การละเมิดทางแพ่งหรือทางอาญา	0	0	0				

หน้าแรก : กรอกข้อมูลหน่วยงาน (agency profile) และข้อมูลเกี่ยวกับการประเมิน (assessment input) พร้อมทั้งแสดงผลข้อมูลจากการประมวลผล

Step 2 : เลือกระดับประเภทของ ผลกระทบ โอกาสที่จะเกิดขึ้น และผล สนับสนุน

หน้าสรุป : แสดงระดับความเสี่ยงและผลกระทบ

หน้า print out : หน้าแสดงข้อมูลและ
ผลลัพธ์ของการประมวลผลทั้งหมด

ข้อมูลเพิ่มเติม : เกณฑ์การให้คะแนนและ
การคำนวณ

[illegible]

เป็นหน้าที่รวบรวมผลลัพธ์จากการคำนวณที่ได้จากหน้า “**STEP 1**” “**STEP 2**” และ “**STEP 3**” รวมเอาไว้อยู่ใน sheet เดียวเพื่อหน่วยงานภาครัฐสามารถทำการพิมพ์ผลสรุปจากการคำนวณตามมาตรฐานของทั้งในและต่างประเทศและข้อปฏิบัติหลังการประเมินได้อย่างสะดวก

[illegible]

เครื่องมือประมวลผลข้อมูลดิจิทัลสำหรับการประเมินผลสัมฤทธิ์ในการปฏิรูปและธรรมาภิบาลสำหรับประเทศไทย (Assessment Tool for Government Digital ID)				
ประเภทผลกระทบ	สรุปประเด็นความเสี่ยง			อธิบายความหมายของสีและตัวเลขระดับความเสี่ยงเมื่อเทียบกับขีดจำกัด
	ปัจจัยด้าน ดิจิทัล	ปัจจัยด้าน นิเทศศาสตร์	เชื่อมโยงกับ องค์การนิเทศศาสตร์	
ความไม่สอดคล้องของ	0	0	0	สีแสดงถึงระดับความเสี่ยงที่ต่ำกว่าขีดจำกัด เลขชี้กำลังแสดงถึงระดับความเสี่ยงที่ต่ำกว่าขีดจำกัด เมื่อเทียบกับขีดจำกัด
ความเสียหายทางการเงิน	0	0	0	
ความเสี่ยงต่อการดำเนินงานของ องค์การนิเทศศาสตร์	0	0	0	สีแสดงถึงระดับความเสี่ยงที่ต่ำกว่าขีดจำกัด เลขชี้กำลังแสดงถึงระดับความเสี่ยงที่ต่ำกว่าขีดจำกัด เมื่อเทียบกับขีดจำกัด
การเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต	0	0	0	
ความไม่สอดคล้องของข้อมูล	0	0	0	สีแสดงถึงระดับความเสี่ยงที่ต่ำกว่าขีดจำกัด เลขชี้กำลังแสดงถึงระดับความเสี่ยงที่ต่ำกว่าขีดจำกัด เมื่อเทียบกับขีดจำกัด
การละเมิดทางแพ่งหรืออาญา	0	0	0	

หน้าแรก : กรอกข้อมูลหน่วยงาน (agency profile) และข้อมูลเกี่ยวกับการประเมิน (assessment input) พร้อมทั้งแสดงผลข้อมูลจากการประมวลผล

STEP 2 : เลือกระดับประเภทของ
ผลกระทบ โอกาสที่จะเกิดขึ้น และผล
สนับสนุน

หน้าสรุป : แสดงระดับความเสี่ยงและผลกระทบ

หน้า print out : หน้าแสดงข้อมูลและ
ผลลัพธ์ของการประมวลผลทั้งหมด

ข้อมูลเพิ่มเติม : เกณฑ์การให้คะแนนและ
การคำนวณ

[illegible]

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

ตารางแสดงความเชื่อมโยงความสัมพันธ์ระหว่างผลกระทบและโอกาส
หรือความเป็นไปได้ที่จะเกิดขึ้นว่ามีความเสี่ยงระดับใด

การคำนวณ
ความเสี่ยง = โอกาสที่จะเกิดขึ้นได้ x ผลกระทบ x น้ำหนักคะแนน

ตารางแสดงผลในรูปแบบการวัดค่าออกเป็นตัวเลขและสีที่มีความหมายถึงระดับความ เสี่ยงตามระดับผลกระทบและโอกาสหรือ
ความเป็นไปได้ที่จะเกิดขึ้นว่ามีความเสี่ยงระดับใด และ ค่าการแสดงผล ต้องสัมพันธ์กับการกำหนดเกณฑ์และการแสดงผลต้องมี
การระบุความหมายของความ เสี่ยงตามสี สีเขียว สีเหลือง สีแดง

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

ตารางข้อมูลเพิ่มเติม

ผู้ใช้งานไม่จำเป็นต้องกรอกอะไร เป็นหน้า
แสดงวิธีการคำนวณและการให้คะแนนใน
แต่ละหัวข้อ

ตารางแสดงระดับโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น (likelihood levels) ทั้งสามระดับ ระดับสูง ระดับปานกลาง ระดับต่ำ		
โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น	คะแนน	ความหมาย
สูง	3	มีโอกาสเกิดขึ้นเป็นประจำบ่อยครั้ง
ปานกลาง	2	มีโอกาสเกิดบางครั้ง
ต่ำ	1	มีโอกาสเกิด แต่นาน ๆ ครั้ง
ไม่มี	0	ไม่มีโอกาสเกิดขึ้น

ความหมายของแต่ละระดับความเสี่ยง			
ระดับความเสี่ยง	ระดับคะแนน	แทนด้วย	ความหมาย
สูง	6-9		ระดับความเสี่ยงที่หน่วยงานของรัฐไม่สามารถยอมรับได้ และต้องจัดการลดความ เสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและ
ปานกลาง	2-4		ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยต้องมีมาตรการ ควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับ
ไม่มีหรือต่ำ	0-1		ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้โดยมีมาตรการ ควบคุมอยู่แล้วหรือไม่ก็ได้

เครื่องมือฯ : ตัวอย่างการวิเคราะห์ผลกระทบ

ผลกระทบด้านความเสียหายทางการเงิน	ตัวอย่างผลกระทบระดับต่ำ	ตัวอย่างผลกระทบระดับปานกลาง	ตัวอย่างผลกระทบระดับสูง
หากผู้ให้บริการให้ข้อมูลส่วนตัวอันเป็นเท็จ หรือแสดงตัวด้วยไอเดนทิตีปลอมที่ไม่มีอยู่จริง หรือเป็นของบุคคลอื่น	ผู้ใช้งานลงทะเบียนรับเงินเยียวยาโดยแจ้งข้อมูลอาชีพและรายได้ที่ไม่ตรงกับความเป็นจริง แต่ไม่กระทบอะไรกับจำนวนเงินเยียวยาที่ได้รับ	ผู้ไม่ประสงค์ดี โจมตีจนทำให้ระบบไม่สามารถให้บริการ นักท่องเที่ยวทั่วโลกได้ องค์กรต้องจัดสรรงบประมาณจำนวนไม่น้อยในการปรับปรุงระบบ	ผู้ให้บริการใช้ข้อมูลบัตรประชาชนคนอื่นมาลงทะเบียนรับสิทธิเงินช่วยเหลือเยียวยาผู้ได้รับผลกระทบจากภัยพิบัติซึนามิ ทำให้เจ้าของบัตรตัวจริงเสียสิทธิ์ สร้างความเดือดร้อนทางการเงินให้เจ้าของบัตรตัวจริงมาก (เพราะไม่เหลือทรัพย์สินอื่นใดแล้ว)
หากผู้ให้บริการให้ข้อมูลส่วนตัวผิดพลาดแบบไม่ได้ตั้งใจตอนลงทะเบียน	ผู้ให้บริการกรอกเลขบัญชีผิดตอนลงทะเบียนกับหน่วยงานเพื่อชำระค่าธรรมเนียม หน่วยงานได้รับเงินล่าช้า แต่เป็นจำนวนเงินเล็กน้อยเท่านั้น	ผู้ให้บริการกรอกอีเมลผิดตอนลงทะเบียนขอใบรับรองการเดินทางเข้าประเทศ ทำให้ไม่ได้รับใบรับรองทันเวลาที่จะเดินทาง และต้องยกเลิกเที่ยวบินและที่พักโดยไม่ได้เงินคืน	ผู้ให้บริการไม่สามารถเข้าสู่ระบบเพื่อทำธุรกรรมสำคัญได้ทันที จึงทำให้เสียโอกาสทางการเงินอย่างใหญ่หลวง
หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้ว ถูกสวมรอยเข้าใช้งานแทน	ผู้ไม่ประสงค์ดีสวมรอยเข้ามายืนยันภูมิลำเนาที่น้อยกว่าความเป็นจริง เพื่อกลับแหล่งให้ผู้ให้บริการตัวจริงต้องเสียทั้งเงินและเวลาเดินเรื่องแก้ไขในภายหลัง	ผู้ไม่ประสงค์ดีสวมรอยเข้ามารวบรวมข้อมูลส่วนบุคคล ทำให้องค์กรผู้ให้บริการ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เข้าข่ายประมาทเลินเล่อ ไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ และต้องจ่ายค่าสินไหมทดแทนเป็นจำนวนมาก หากถูกฟ้องแพ่งจากเจ้าของข้อมูลตัวจริง	ผู้ไม่ประสงค์ดีใช้บัญชีเจ้าของบริษัทสวมรอยเข้ามาใช้งานในระบบเพื่อเปิดดูข้อมูลความลับทางการค้าที่เกี่ยวข้องกับการเจรจา G2G จากนั้นนำไปเผยแพร่ในทางลบ จนทำให้ประเทศสูญเสียโอกาสทางเศรษฐกิจครั้งสำคัญ
หากผู้ให้บริการที่เคยลงทะเบียนไว้แล้ว ถูกขโมยข้อมูลส่วนตัวที่ใช้ประกอบการพิสูจน์และยืนยันตัวตน	เกิด identity theft กับคนผู้ให้บริการ จากการนำข้อมูลดังกล่าวไปใช้เพื่อดำเนินธุรกรรมทางการเงินเป็นจำนวนไม่เกิน 500 บาท	องค์กรต้องจัดสรรงบประมาณจำนวนไม่น้อยในการปรับปรุงระบบไม่ให้เกิดการขโมยข้อมูลส่วนตัวดังกล่าวได้	เกิด identity theft เป็นวงกว้าง จากการนำข้อมูลดังกล่าวไปใช้เพื่อดำเนินธุรกรรมต่าง ๆ ที่ไม่ชอบด้วยกฎหมาย

Q & A

THANK YOU