การประชุมเชิงปฏิบัติการ (Workshop)

การจัดทำแนวทางการรายงานข้อมูล ประจำปีสำหรับธุรกิจบริการ Digital ID

11 มีนาคม 2568

Asawin Grand Convention Hotel

เอกสารการประชุม

ขอความอนุเคราะห์ให้ท่านนำเครื่องคอมพิวเตอร์หรือโน้ตบุ๊กมาใช้ระหว่าง
การประชุม เพื่อความสะดวกในการเข้าถึงข้อมูลและการทำกิจกรรมร่วมกัน

กำหนดการประชุมเชิงปฏิบัติการ (Workshop)

วันที่ 11 มีนาคม 2568 ณ ห้องพระอินทร์ 1-2 (ชั้น 2)
Asawin Grand Convention Hotel

เวลา	รายละเอียด
08.00 – 09.00 น.	ลงทะเบียน
09.00 – 09.30 น.	ที่มาและวัตถุประสงค์การดำเนินโครงการ (สพธอ.)
09.30 – 10.00 น.	นำเสนอภาพรวมการกำกับดูแลและผลสรุปการสัมภาษณ์เชิงลึกจากผู้ประกอบการธุรกิจ Digital ID
10.00 – 10.45 น.	รับฟังความเห็นข้อมูลในการรายงาน
10.45 – 11.00 น.	พักเบรก
11.00 – 11.45 น.	รับฟังความเห็นข้อมูลในการรายงาน (ต่อ)
11.45 – 12.30 น.	สรุปผลประชุมเชิงปฏิบัติการ
12.30 น.	รับประทานอาหาร ณ ห้องอาหารโรงแรม

โครงการจัดทำแนวทางการส่งเสริมและสนับสนุนการใช้งาน Digital ID เพื่อรองรับการขับเคลื่อนและยกระดับ Digital GDP

เอกสารประกอบการประชุมเชิงปฏิบัติการ (Workshop)

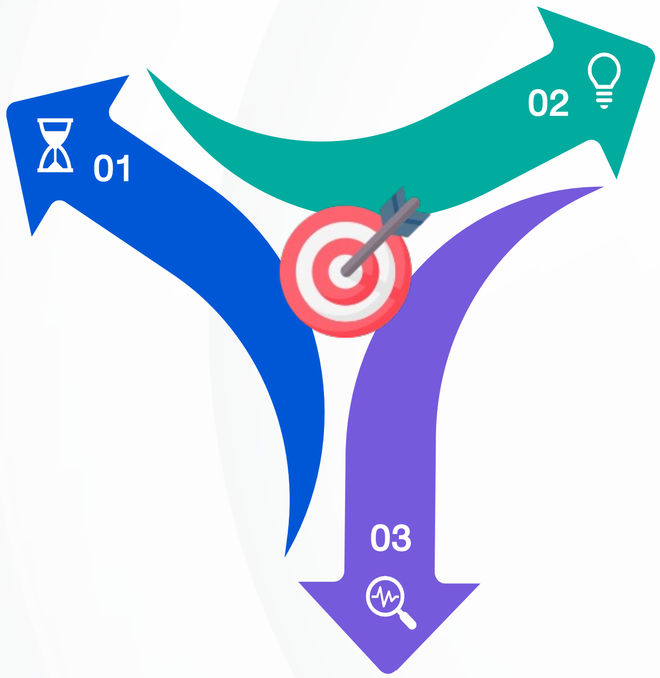
การจัดทำแนวทางการรายงานข้อมูลประจำปีสำหรับธุรกิจบริการ Digital ID

วันที่ 11 มีนาคม 2568

01

ภาพรวมโครงการ

วัตถุประสงค์ของโครงการ



เพื่อสร้างความเข้าใจที่ชัดเจนเกี่ยวกับ Digital ID Landscape และการนำข้อมูลที่ได้จากการสำรวจไปพัฒนากลยุทธ์ในการส่งเสริมการใช้งาน Digital ID ในธุรกิจต่าง ๆ อีกทั้งยังสามารถใช้เป็นแนวทางในการปรับปรุงและพัฒนาเทคโนโลยี Digital ID ในอนาคต

เพื่อวิเคราะห์และประเมินสภาพตลาด การศึกษาพฤติกรรมและความต้องการของผู้บริโภค และประเมินแนวโน้มและเทคโนโลยีใหม่ ๆ ที่จะมีผลต่อการพัฒนา Digital ID

เพื่อศึกษาแนวทางการจัดเก็บข้อมูลจากผู้ประกอบธุรกิจบริการ Digital ID และพัฒนาแนวทางการรายงานประจำปี อันจะช่วยให้สามารถติดตามและกำกับดูแลการดำเนินงานของผู้ประกอบการได้อย่างมีประสิทธิภาพ ผ่านการวิเคราะห์ข้อมูลที่จัดเก็บในรายงานประจำปี รวมถึงช่วยสร้างความไว้วางใจและเสริมสร้างความสัมพันธ์ที่ดีกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร

02

แนวทางในการกำกับดูแลผู้ประกอบธุรกิจบริการ Digital ID

ความสำคัญของผู้ให้บริการ ต่อผู้รับบริการ ประเทศ และหน่วยงาน ในการพัฒนาและส่งเสริมการใช้ Digital ID คือการวางรากฐานสำคัญในการพัฒนาและขับเคลื่อนประเทศไทยสู่เศรษฐกิจและสังคมดิจิทัล

ผู้ให้บริการ Digital ID

ผู้ใช้บริการ

- เข้าถึงบริการต่าง ๆ ได้โดยไม่ต้องลงทะเบียน ID ใหม่ทุกครั้ง
- เข้าถึงบริการดิจิทัลได้ง่าย ไม่ต้องจำรหัสหลายชุด
- ลดความเสี่ยงในการถูกปลอมแปลงตัวตนเพื่อสวมสิทธิ์
- ปกป้องข้อมูลส่วนบุคคลได้

ภาครัฐ

- พัฒนาระบบราชการดิจิทัลได้รวดเร็ว
- ลดภาระและค่าใช้จ่ายในการจัดการระบบ ID ของตนเอง
- ลดการใช้เอกสารโดยสำเนาข้อมูลจากหน่วยงานเจ้าของข้อมูล
- เป็นไปตามนโยบายรัฐบาลและ พ.ร.บ. การปฏิรูปราชการทางอิเล็กทรอนิกส์

ประเทศไทย

- เพิ่มการมีส่วนร่วมในกิจกรรมทางเศรษฐกิจดิจิทัล
- เพิ่มขีดความการแข่งขันทางดิจิทัลของประเทศ

ขับเคลื่อนมูลค่าเศรษฐกิจเติบโตขึ้น

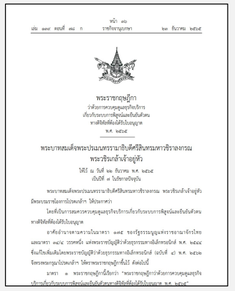
- ขยายการใช้งานเทคโนโลยีในทุกภาคส่วน ทำให้เกิดการแข่งขันทางธุรกิจ เพื่อพัฒนาระบบให้มีประสิทธิภาพ
- สร้างความมั่นใจในการทำธุรกรรมผ่านช่องทางออนไลน์ รวมถึงลดความเสี่ยงและความสูญเสียที่อาจเกิดขึ้น

ส่งเสริมอันดับความสามารถด้านดิจิทัล

- เสริมความเชื่อมั่นและความปลอดภัยทางดิจิทัล ช่วยให้การดำเนินธุรกิจและการใช้งานดิจิทัลมีความราบรื่นและปลอดภัย
- พัฒนาทักษะดิจิทัลขั้นพื้นฐานให้กับประชาชน พร้อมเข้าสู่ในการแข่งขันของประเทศในระดับโลก

ผู้รับใบอนุญาตต้องปฏิบัติตามกฎการแจ้งข้อมูลสำคัญและแก้ไขปัญหาตามคำสั่ง สพธอ. ในฐานะผู้กำกับดูแล พร้อมจัดส่งสรุปผลการดำเนินงานปีละ 1 ครั้งเพื่อให้บริการเป็นไปตามหลักเกณฑ์มาตรฐานและกฎหมาย

พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565



วัตถุประสงค์ในการควบคุมดูแลธุรกิจบริการ Digital ID

- เพื่อเสริมสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีการประยุกต์ใช้ Digital ID ในการอาศัยผลการพิสูจน์และยืนยันตัวตนเพื่อเข้าทำธุรกรรมต่าง ๆ
- เพื่อส่งเสริมประสิทธิภาพของระบบให้บริการ : เพื่อให้การดำเนินการต่างๆ ในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลสามารถดำเนินการได้สอดคล้องตามมาตรฐานสากล
- สนับสนุนให้ผู้ประกอบธุรกิจมีธรรมาภิบาลที่ดี (Good Governance) ในการให้บริการ มีความซื่อสัตย์สุจริตต่อหน้าที่ความรับผิดชอบ
- คุ้มครองผู้ใช้บริการ: เพื่อให้ผู้ประกอบธุรกิจมีความตระหนักถึงสิทธิหน้าที่และมาตรฐานขั้นต่ำในการดูแลผู้ใช้บริการ

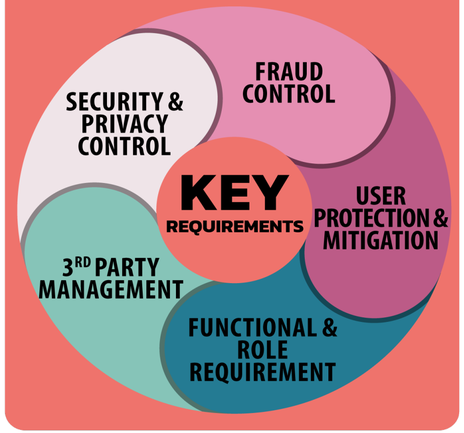
SUPERVISORY FRAMEWORK

INHERENT RISK

Quality of Risk Management Risk Factor

1. STRATEGIC RISK
2. OPERATIONAL RISK
3. INFORMATION TECHNOLOGY RISK
4. REPUTATION RISK
5. COMPLIANCE RISK

CAPABILITY MANAGEMENT



ขอบเขตการกำกับดูแลของ ETDA

มาตรา 20 ผู้รับใบอนุญาตต้องแจ้งต่อสานักงานในกรณีที่ผู้รับใบอนุญาตเปลี่ยนแปลง เรื่องหนึ่งเรื่องใดดังต่อไปนี้

1. ทุนจดทะเบียนของผู้รับใบอนุญาต
2. กรรมการ ผู้จัดการ หรือผู้ซึ่งรับผิดชอบในการดาเนินงานของผู้รับใบอนุญาต
3. ระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการ

มาตรา 26 ผู้รับใบอนุญาตต้องส่งรายงานการเงินและสรุปผลการดำเนินงานเกี่ยวกับการให้บริการต่อสานักงานอย่างน้อยปีละหนึ่งครั้ง

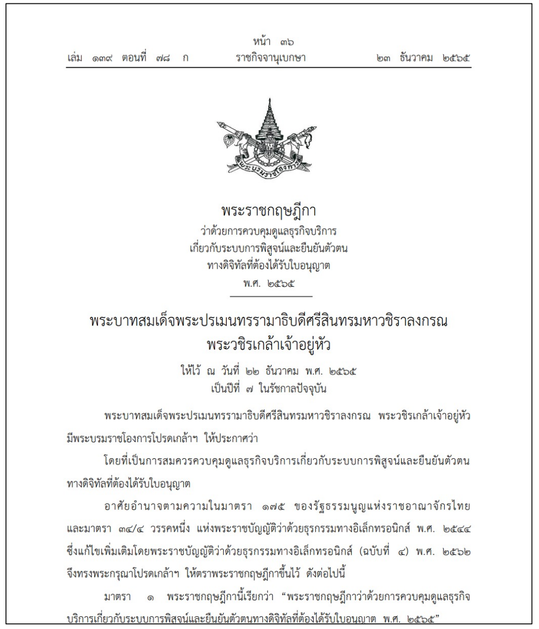
มาตรา 27 ในกรณีที่มีเหตุอันสมควรเพื่อประโยชน์ในการควบคุมดูแลและกำกับ การประกอบธุรกิจ ให้พนักงานเจ้าหน้าที่มีอานาจกำหนดให้ผู้รับใบอนุญาตรายใดส่งรายงานหรือข้อมูลอื่นใด ตลอดจนแสดงเอกสารที่เกี่ยวข้องรวมทั้งให้ชี้แจงเพื่ออธิบายหรือขยายความรายงานหรือข้อมูลหรือเอกสารนั้น

ควบคุมให้ผู้ให้บริการปฏิบัติตามหลักเกณฑ์ต่าง ๆ ในการให้บริการ

1. มาตรการบริหารและการจัดการความเสี่ยงของระบบ
2. มาตรการรักษาความมั่นคงปลอดภัยของระบบ
3. มาตรการควบคุมดูแลและป้องกันการฉ้อโกงหรือการฉ้อฉลจากการใช้งานระบบ
4. มาตรฐานการให้บริการ ซึ่งรวมถึงการจัดการและจัดเก็บข้อมูล
5. การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ
6. การใช้บริการจากบุคคลภายนอกที่เกี่ยวกับระบบการให้บริการ
7. การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ

ผู้รับใบอนุญาตต้องปฏิบัติตามกฎการแจ้งข้อมูลสำคัญและแก้ไขปัญหาตามคำสั่ง สพธอ. ในฐานะผู้กำกับดูแล พร้อมจัดส่งสรุปผลการดำเนินงานปีละ 1 ครั้งเพื่อให้บริการเป็นไปตามหลักเกณฑ์มาตรฐานและกฎหมาย

พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565



หน้า ๑๖
เล่ม ๑๓๙ ตอนที่ ๗๘ ก ราชกิจจานุเบกษา ๒๓ ธันวาคม ๒๕๖๕

พระราชกฤษฎีกา
ว่าด้วยการควบคุมดูแลธุรกิจบริการ
เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตน
ทางดิจิทัลที่ต้องได้รับใบอนุญาต
พ.ศ. ๒๕๖๕

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๒ ธันวาคม พ.ศ. ๒๕๖๕
เป็นปีที่ ๗ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

อาศัยอำนาจตามความในมาตรา ๑๗๕ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และมาตรา ๓๔/๔ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า "พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ๒๕๖๕"

หมวด 3 หน้าที่ของผู้รับใบอนุญาต

กำหนดหน้าที่และอำนาจของคณะกรรมการและเจ้าหน้าที่ในการกำกับดูแลและตรวจสอบการดำเนินงานของผู้รับใบอนุญาต เพื่อให้การให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัลเป็นไปตามกฎหมายและมาตรฐานที่กำหนด

ข้อมูลที่ต้องแจ้งให้ทราบ เช่น
- การร้องเรียนหรือฟ้องร้องเกี่ยวกับการประกอบธุรกิจ
- การตรวจประเมินระบบ

ข้อมูลที่ต้องแจ้งให้ทราบเมื่อมีการเปลี่ยนแปลง เช่น
- กรรมการ ผู้จัดการ หรือผู้รับผิดชอบการดำเนินงาน
- ระบบหรือเทคโนโลยีที่ส่งผลต่อการให้บริการ

- การหยุดหรือเลิกให้บริการ ต้องแจ้ง ETDA ล่วงหน้าอย่างน้อย **90 วัน** พร้อมจัดทำแผนการยุติบริการเพื่อป้องกันผลกระทบต่อผู้ใช้บริการ
- **ETDA มีอำนาจตรวจสอบการดำเนินงานของผู้รับใบอนุญาต** เพื่อให้มั่นใจว่าผู้รับใบอนุญาตปฏิบัติตามกฎหมายและเงื่อนไข

หมวด 4 การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์ และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

กำหนดขั้นตอนและเงื่อนไขสำหรับการขอและออกใบอนุญาตในการให้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

หลักเกณฑ์ต่าง ๆ ในการให้บริการ
1. มาตรการบริหารและการจัดการความเสี่ยงของระบบ
2. มาตรการรักษาความมั่นคงปลอดภัยของระบบ
3. มาตรการควบคุมดูแลและป้องกันการฉ้อโกงหรือการฉ้อฉลจากการใช้งานระบบ
4. มาตรฐานการให้บริการ ซึ่งรวมถึงการจัดการและจัดเก็บข้อมูล
5. การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ
6. การใช้บริการจากบุคคลภายนอกที่เกี่ยวกับระบบการให้บริการ
7. การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ

- ผู้รับใบอนุญาตต้อง**นำส่งงบการเงินและสรุปผลการดำเนินงานเกี่ยวกับการให้บริการ อย่างน้อยปีละ 1 ครั้ง**
- หากมีเหตุอันสมควร พนักงานเจ้าหน้าที่อาจเรียกให้นำส่งรายงาน เอกสาร หรือข้อมูลเพิ่มเติม รวมถึงเรียกบุคคลมาให้ข้อมูลเกี่ยวกับการให้บริการได้
- หากผู้รับใบอนุญาตไม่ดำเนินการให้สอดคล้องตามหลักเกณฑ์ที่สำนักงานอาจสั่งให้แก้ไขภายในระยะเวลาที่กำหนด

แนวทางการกำกับดูแล เพื่อเสริมสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ ส่งเสริมประสิทธิภาพของระบบให้บริการรวมไปถึงสนับสนุนให้ผู้ประกอบธุรกิจมีธรรมาภิบาลที่ดีและคุ้มครองผู้ใช้บริการ

แนวทางการกำกับ ควบคุม ดูแลผู้ให้บริการ

Data Security and Protection (DS)

กลุ่มข้อมูลแสดงภาพรวมที่อธิบายถึงสถาปัตยกรรมความมั่นคงปลอดภัยสารสนเทศ (Security Architecture) สมรรถนะและศักยภาพของผู้ให้บริการเพื่อการป้องกันข้อมูลและความเป็นส่วนบุคคลของข้อมูล

- ข้อมูลด้านความพร้อมและความปลอดภัยของระบบ

Performance & Efficiency (PE)

กลุ่มข้อมูลที่นำไปสู่การวิเคราะห์และประเมินสมรรถนะ คุณภาพ และความสามารถในการให้บริการ

- ข้อมูลการทำธุรกรรม (Transactions)
- ข้อมูลด้านอุบัติการณ์ (Incidents)
- ข้อมูลด้าน Incident ที่เกี่ยวข้องกับการทุจริตและฉ้อโกง (Fraud)
- ข้อมูลประสบการณ์ใช้งานจากลูกค้า (Customer Experiences)

Risk Management (RM)

กลุ่มข้อมูลที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงของผู้ให้บริการ

- นโยบายความเสี่ยงที่เกี่ยวข้องกับธุรกิจ (risk identification) ตามลักษณะการให้บริการ
- ผลการประเมินความเสี่ยง (risk evaluation) ซึ่งครอบคลุมการประเมินความเสี่ยงตั้งต้นและการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง
- โครงสร้างหรือคณะกรรมการ/ผู้รับผิดชอบการบริหารความเสี่ยง (หากมีการเปลี่ยนแปลง)

ETDA

- เพื่อเสริมสร้างความเชื่อมั่นในบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- เพื่อส่งเสริมประสิทธิภาพของระบบให้บริการ ในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้สอดคล้องตามมาตรฐานสากล
- สนับสนุนให้ผู้ประกอบธุรกิจมีธรรมาภิบาลที่ดี (Good Governance)
- คุ้มครองผู้ใช้บริการ: เพื่อให้ผู้ประกอบธุรกิจมีความตระหนักถึงสิทธิหน้าที่และมาตรฐานขั้นต่ำในการดูแลผู้ใช้บริการ

Operational Information (OI)

กลุ่มข้อมูลผลการดำเนินงานและการให้บริการเบื้องต้น ตลอดจนข้อมูลของผู้ให้บริการและผู้ที่มีส่วนได้ส่วนเสียในบริการที่สำคัญ (Critical Interested Parties)

- ข้อมูลทั่วไปและโครงสร้างการดำเนินงาน
- ข้อมูลการให้บริการ เช่น จำนวนผู้ใช้งาน (Users) จำนวน RP ที่มีการเชื่อมต่อ
- ข้อมูลสำคัญอื่น ๆ เช่น นโยบายการกำกับดูแล

Service Development & Improvement (SD)

กลุ่มข้อมูลที่เกี่ยวข้องกับการปรับปรุงองค์ประกอบของบริการ ตลอดจนกระบวนงานที่เกี่ยวข้อง เพื่อนำไปสู่การพัฒนาธุรกิจ โครงสร้างพื้นฐาน ระบบสารสนเทศ ตลอดจนนวัตกรรมและเทคโนโลยีด้าน Digital ID

- ผลดำเนินงานตามเป้าหมายโดยรวม
- แผนการพัฒนาต่อยอดบริการการอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีการพิสูจน์และยืนยันตัวตน

วัตถุประสงค์ของการขอข้อมูลจากระบบ Digital ID ใน 5 ด้านหลักนั้น มุ่งเน้นการนำข้อมูลไปวิเคราะห์ ติดตาม และปรับปรุงบริการ IdP ให้มีความปลอดภัย มีประสิทธิภาพ และรองรับการพัฒนาระบบ Digital ID ของประเทศในอนาคต

1 Operational Information (OI)

- เพื่อใช้เป็นข้อมูลประกอบการกำกับดูแลและติดตามสถานะของผู้ให้บริการ IdP ว่าดำเนินงานสอดคล้องตามหลักเกณฑ์และมาตรฐานที่กำหนด พร้อมตรวจสอบความเสี่ยงที่อาจกระทบต่อความมั่นคงปลอดภัยและความต่อเนื่องของบริการ
- ใช้วิเคราะห์ภาพรวมและแนวโน้มการให้บริการระบบ Digital ID ในประเทศ เช่น จำนวนผู้ใช้บริการ กลุ่มธุรกิจที่เชื่อมต่อ ความครอบคลุมของบริการในแต่ละพื้นที่ เพื่อสนับสนุนการวางนโยบายและพัฒนาระบบ Digital ID ให้ตอบโจทย์การใช้งานและรองรับการเติบโตในอนาคต

2 Performance & Efficiency (PE)

- เพื่อประเมินประสิทธิภาพการให้บริการของผู้ให้บริการ IdP ในด้านปริมาณธุรกรรม ความสำเร็จในการดำเนินงาน และความต่อเนื่องของบริการในแต่ละปี
- เพื่อวิเคราะห์ความเสถียรของระบบจากสถิติการเกิดปัญหาและเหตุการณ์ผิดปกติ (Incident/Fraud) เพื่อสะท้อนศักยภาพการดำเนินงานและความพร้อมในการรองรับการให้บริการ
- เพื่อใช้เป็นฐานข้อมูลเปรียบเทียบผลการดำเนินงานของผู้ให้บริการ IdP รายปี รวมถึงติดตามแนวโน้มด้านประสิทธิภาพและความเสี่ยงเชิงระบบในภาพรวม

3 Data Security and Protection (DS)

- เพื่อใช้ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและความต่อเนื่องในการให้บริการของผู้ให้บริการ IdP จากข้อมูลการหยุดให้บริการ ข้อร้องเรียน และผลการตรวจประเมิน
- เพื่อใช้เป็นข้อมูลประกอบการกำกับดูแลเชิงป้องกันและประเมินความพร้อมของผู้ให้บริการในการรองรับเหตุการณ์ผิดปกติและการจัดการความเสี่ยงที่เกี่ยวข้องกับระบบตามหลักเกณฑ์ที่กำหนด

4 Risk Management (RM)

- เพื่อให้สามารถเปรียบเทียบแนวโน้มความเสี่ยงและปัญหาของผู้ให้บริการ IdP รายต่าง ๆ ได้อย่างต่อเนื่อง และใช้ในการประเมินความเสี่ยงเชิงภาพรวมของระบบ Digital ID ในประเทศ
- เพื่อใช้วิเคราะห์และติดตามความเพียงพอของมาตรการควบคุมความเสี่ยง เช่น มีแผนรองรับกรณีระบบขัดข้อง มีแนวทางป้องกันผลกระทบต่อประชาชน และสามารถลดความถี่หรือผลกระทบจากเหตุการณ์ซ้ำ ๆ

5 Service Development & Improvement (SD)

- เพื่อใช้เป็นข้อมูลในการติดตามความคืบหน้าและความเหมาะสมของการปรับปรุงระบบ พัฒนาฟีเจอร์ใหม่ และขยายขอบเขตการให้บริการของผู้ให้บริการ IdP ให้เป็นไปตามหลักเกณฑ์และพัฒนาเสถียรภาพของระบบ
- เพื่อประเมินแนวโน้มการเติบโตของบริการและวิเคราะห์ศักยภาพในการให้บริการในอนาคต เพื่อสนับสนุนการกำกับดูแลให้สอดคล้องกับทิศทางการพัฒนาระบบ Digital ID ของประเทศในภาพรวม

จากการร้องขอข้อมูลจากการให้บริการ Digital ID นั้น สพธอ. สามารถนำข้อมูลไปใช้ในการกำหนดนโยบาย วิเคราะห์ศักยภาพ สร้างมูลค่าเศรษฐกิจ และควบคุมการให้บริการ Digital ID ให้มีความปลอดภัยและน่าเชื่อถือ

ประโยชน์จากการรายงานข้อมูล

1. การกำกับดูแลและติดตามสถานะการดำเนินงานของผู้ให้บริการ IdP

- ใช้ข้อมูลประกอบการกำกับดูแลและติดตามสถานะของผู้ให้บริการ IdP ว่าดำเนินงานสอดคล้องตามหลักเกณฑ์และมาตรฐานที่กำหนด พร้อมตรวจสอบความเสี่ยงที่อาจกระทบต่อความมั่นคงปลอดภัยและความต่อเนื่องของบริการ
- ใช้ข้อมูลประกอบการกำกับดูแลเชิงป้องกันและประเมินความพร้อมของผู้ให้บริการในการรองรับเหตุการณ์ผิดปกติและการจัดการความเสี่ยงตามหลักเกณฑ์ที่กำหนด

2. การประเมินความเสี่ยงและความมั่นคงปลอดภัยของระบบ

- ใช้ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและความต่อเนื่องในการให้บริการของผู้ให้บริการ IdP จากข้อมูลการหยุดให้บริการ ข้อร้องเรียน และผลการตรวจประเมิน
- ใช้เปรียบเทียบแนวโน้มความเสี่ยงและปัญหาของผู้ให้บริการ IdP รายต่าง ๆ ได้อย่างต่อเนื่อง และใช้ในการประเมิน
  ความเสี่ยงเชิงภาพรวมของระบบ Digital ID ในประเทศ
- ใช้วิเคราะห์และติดตามความเพียงพอของมาตรการควบคุมความเสี่ยง เช่น การมีแผนรองรับกรณีระบบขัดข้อง การป้องกันผลกระทบต่อประชาชน และการลดความถี่ของเหตุการณ์ซ้ำ ๆ

3. การวิเคราะห์ภาพรวมและแนวโน้มการให้บริการระบบ Digital ID

- ใช้วิเคราะห์ภาพรวมและแนวโน้มการให้บริการระบบ Digital ID ในประเทศ เช่น จำนวนผู้ใช้บริการ กลุ่มธุรกิจที่เชื่อมต่อ ความครอบคลุมของบริการในแต่ละพื้นที่ เพื่อสนับสนุนการวางนโยบายและพัฒนาระบบ Digital ID ให้ตอบโจทย์การใช้งานและรองรับการเติบโตในอนาคต

4. การติดตามการพัฒนาและขยายบริการ

- ใช้เป็นข้อมูลในการติดตามความคืบหน้าและความเหมาะสมของการปรับปรุงระบบ พัฒนาฟีเจอร์ใหม่ และขยายขอบเขตการให้บริการของผู้ให้บริการ IdP ให้เป็นไปตามหลักเกณฑ์และไม่ส่งผลกระทบต่อเสถียรภาพของระบบ
- ประเมินแนวโน้มการเติบโตของบริการและวิเคราะห์ศักยภาพในการให้บริการในอนาคต เพื่อสนับสนุนการกำกับดูแลให้สอดคล้องกับทิศทางการพัฒนาระบบ Digital ID ของประเทศในภาพรวม

การนำไปใช้ตอยอดของ ETDA ในฐานะ Regulator

- เพื่อกำหนดนโยบายที่เหมาะสมในการพัฒนาธุรกิจการให้บริการ Digital ID ให้เกิดประโยชน์สูงสุดต่อเศรษฐกิจและสังคมของประเทศ
- เพื่อใช้ในการวิเคราะห์ศักยภาพและความพร้อมของการให้บริการ Digital ID ของประเทศไทย
- เพื่อสร้างประโยชน์แก่ผู้ประกอบธุรกิจ โดยใช้ข้อมูลเพื่อสะท้อนมุมมองทิศทางและศักยภาพของธุรกิจบริการ Digital ID ในภาพรวม
- เพื่อให้ ETDA สามารถประเมินมูลค่าทางเศรษฐกิจจากการให้บริการ Digital ID ที่สามารถสนับสนุนข้อมูลด้าน DGDP/GDP ของประเทศ
- เพื่อให้ ETDA สามารถกำกับดูแลและควบคุมการให้บริการ Digital ID ให้อยู่ในสภาพแวดล้อมที่มั่นคงปลอดภัยน่าเชื่อถือ

1 Operational Information (OI)

Pain Point

User/RP

- ขาดการแจ้งเตือนหรือสื่อสารการเปลี่ยนแปลงที่มีนัยสำคัญต่อการบริหารหรือการให้บริการของ IDP อันกระทบต่อระดับความเชื่อมั่น

Regulator

- ขาดประสิทธิภาพในการกำกับดูแล การมีส่วนร่วม ตลอดจนการสนับสนุนและขับเคลื่อนธุรกิจ IDP เพราะขาดข้อมูลพื้นฐานเพื่อนำไปสู่การวิเคราะห์และวางแผนการกำกับดูแลอย่างเหมาะสมต่อการเปลี่ยนแปลงทั้งปัจจัยภายในที่มาจาก IDP และปัจจัยภายนอก

จุดประสงค์ในการร้องขอข้อมูล

- เพื่อให้ ETDA สามารถติดตาม ตรวจสอบ และประเมินความพร้อมในการดำเนินธุรกิจของผู้ให้บริการ IdP ในภาพรวม โดยมุ่งเน้นการตรวจสอบความถูกต้อง ครบถ้วน และความทันสมัยของข้อมูลโครงสร้างองค์กร การดำเนินงาน การให้บริการ ระบบงาน และนโยบายสำคัญต่าง ๆ ที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประเมินความเสถียรของการให้บริการ ความมั่นคงปลอดภัยในการดำเนินงาน

ชุดข้อมูลที่ต้องร้องขอ (Data Set)

- ข้อมูลทั่วไปและโครงสร้างการดำเนินงาน
- ข้อมูลการให้บริการ เช่น
  - จำนวนผู้ใช้งาน (Users)
  - จำนวน RP ที่มีการเชื่อมต่อ
- ข้อมูลสำคัญอื่น ๆ เช่น นโยบายการกำกับดูแล

ประโยชน์จากการรายงานข้อมูล (Benefits)

- ใช้เป็นข้อมูลประกอบการกำกับดูแลและติดตามสถานะของผู้ให้บริการ IdP ว่าดำเนินงานสอดคล้องตามหลักเกณฑ์และมาตรฐานที่กำหนด พร้อมตรวจสอบความเสี่ยงที่อาจกระทบต่อความมั่นคงปลอดภัยและความต่อเนื่องของบริการ

- ใช้วิเคราะห์ภาพรวมและแนวโน้มการให้บริการระบบ Digital ID ในประเทศ เช่น จำนวนผู้ใช้บริการ กลุ่มธุรกิจที่เชื่อมต่อ ความครอบคลุมของบริการในแต่ละพื้นที่ เพื่อสนับสนุนการวางนโยบายและพัฒนาระบบ Digital ID ให้ตอบโจทย์การใช้งานและรองรับการเติบโตในอนาคต

1. Operational Information (OI)

ข้อมูล		วัตถุประสงค์การรายงาน	อ้างอิง
ข้อมูลทั่วไปและโครงสร้างการดำเนินงาน	**ข้อมูลทั่วไปของธุรกิจ** ➢ ชื่อธุรกิจ / บริษัท ➢ ชื่อหน่วยงาน (ระบุชื่อเต็มภาษาไทย) ➢ ชื่อย่อ (ถ้ามี) ➢ เลขทะเบียนนิติบุคคล ➢ ทุนจดทะเบียน/ทุนจดทะเบียนชำระแล้ว ➢ กรรมการของบริษัท ➢ ผู้จัดการ ➢ ผู้ซึ่งรับผิดชอบในการดำเนินงานของผู้รับใบอนุญาต	• เพื่อระบุตัวตนและสถานะของนิติบุคคลที่ได้รับใบอนุญาตในการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล ตรวจสอบความถูกต้องของหน่วยงานที่ดำเนินธุรกิจ IdP ว่ามีตัวตนทางกฎหมาย มีทุนรองรับธุรกิจเพียงพอ และมีผู้รับผิดชอบในการดำเนินงานอย่างชัดเจนในกรณีเกิดปัญหาในการให้บริการ	• หนังสือนำส่งข้อมูลประกอบการยื่นคำขอรับใบอนุญาตฯ/เอกสารแสดงความพร้อมของระบบงานฯ
	โครงสร้างการประกอบธุรกิจ (ถ้ามีการเปลี่ยนแปลง) ➢ แผนผังโครงสร้างองค์กรที่แสดงถึงฝ่ายหรือส่วนงานต่างๆ ที่เกี่ยวข้องกับการประกอบธุรกิจบริการโครงสร้างองค์กร ➢ หน้าที่และความรับผิดชอบของบุคคลหรือหน่วยงานที่เกี่ยวข้อง	• เพื่อทราบข้อมูลเกี่ยวกับโครงสร้างธุรกิจปัจจุบัน เช่น รูปแบบองค์กร โครงสร้างผู้มีอำนาจ และแผนการสำคัญและข้อมูลที่มีความสำคัญในกรณีที่มีการเปลี่ยนแปลงเช่น การควบรวมกิจการ การปรับโครงสร้างองค์กร หรือการเปลี่ยนแปลงผู้ถือหุ้นให้ผู้เกี่ยวข้องทราบ	
	รายละเอียดการประกอบธุรกิจ ➢ บริการพิสูจน์ตัวตน (IdP1) ➢ บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (IdP2) ➢ บริการยืนยันตัวตน (IdP3) ➢ บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Ex.)	• เพื่อให้ ETDA ตรวจสอบรูปแบบบริการ IdP ว่ามีการให้บริการในลักษณะใดบ้าง (IdP1, IdP2, IdP3, EX หรือ Proxy) และทำความเข้าใจขอบเขตการให้บริการของผู้รับใบอนุญาตว่าเป็นไปตามกรอบนโยบายและมาตรฐานที่กำหนดหรือไม่	
	ความสัมพันธ์ของส่วนงานต่างๆ ที่เกี่ยวข้องกับระบบการให้บริการ (ถ้ามีการเปลี่ยนแปลง)	• เพื่อตรวจสอบความเชื่อมโยงและการประสานงานภายในองค์กรในการดำเนินธุรกิจ IdP ว่ามีการกำหนดบทบาทและหน้าที่ที่ชัดเจนหรือไม่ มีความสอดคล้องกันในกระบวนการทำงานเพื่อรักษาความมั่นคงปลอดภัยและความน่าเชื่อถือของระบบพิสูจน์และยืนยันตัวตน	
	ช่องทางการให้บริการสำหรับผู้ให้บริการ (RP) ➢ Web-to-Web ➢ Web-to-App ➢ App-to-App	• เพื่อทราบถึงวิธีและจุดที่ผู้ใช้งานทั่วไป (End Users) สามารถเข้าถึงบริการ IdP ได้ เช่น เว็บไซต์ แอปพลิเคชัน หรือจุดบริการทางกายภาพ (Kiosk, Smart Reader) เพื่อให้สามารถประเมินความสะดวกในการเข้าถึงและความปลอดภัยในกระบวนการพิสูจน์และยืนยันตัวตน รวมถึงวิเคราะห์ความครอบคลุมในการให้บริการประชาชน	
	ช่องทางการให้บริการสำหรับ Users ➢ Domain ➢ Application ➢ เว็บไซต์ ➢ จุดให้บริการ ❑ จุดให้บริการตัวเอง และ Partners เช่น จำนวนสาขาที่ให้บริการพิสูจน์ตัวตน/ จำนวนจุดให้บริการการพิสูจน์ตัวตน/ ตู้ Kiosk หรือ อุปกรณ์ Smart Reader		

1. Operational Information (OI)

ข้อมูล		วัตถุประสงค์การรายงาน	การนำไปใช้
ข้อมูลทั่วไปและโครงสร้างการดำเนินงาน	**อัตราค่าบริการ** ➢ รายการบริการ ➢ อัตราค่าบริการ ➢ หน่วยการคิดค่าใช้จ่าย	• เพื่อให้ ETDA ตรวจสอบความโปร่งใสและความเหมาะสมของโครงสร้างค่าบริการที่ IdP เรียกเก็บจากผู้ใช้งานหรือผู้ให้บริการที่เกี่ยวข้อง (RP) ทั้งในเชิงความสมเหตุสมผลและการแข่งขันที่เป็นธรรม ตลอดจนเพื่อประเมินผลกระทบด้านต้นทุนต่อการเข้าถึงบริการของภาคประชาชนและธุรกิจ	• หนังสือนำส่งข้อมูลประกอบการยื่นคำขอรับใบอนุญาตฯ/เอกสารแสดงความพร้อมของระบบงานฯ • ร่างหลักเกณฑ์การตรวจประเมินประจำปี
	จำนวนการใช้บริการจากผู้รับดำเนินการแทนในการให้บริการ ➢ รายชื่อผู้รับดำเนินการแทน ➢ ประเภทธุรกิจบริการที่ใช้บริการจากผู้รับดำเนินการแทน ➢ การเปลี่ยนแปลงผู้รับดำเนินการแทน ➢ การตรวจสอบการดำเนินการ	• เพื่อให้ ETDA ทราบถึงการพึ่งพาผู้รับดำเนินการแทน (Outsourcing/Partner) ในกระบวนการให้บริการของ IdP และตรวจสอบความเหมาะสมของผู้ดำเนินการแทนทั้งในด้านคุณสมบัติและความมั่นคงปลอดภัย พร้อมติดตามการเปลี่ยนแปลงและผลการตรวจสอบการดำเนินงานของผู้รับดำเนินการแทน	
	ข้อมูลทางด้านการเงิน ➢ งบการเงินประจำปี	• เพื่อให้ ETDA สามารถประเมินความมั่นคงทางการเงินของ IdP ว่ามีความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง มีเสถียรภาพทางการเงินเพียงพอรองรับการให้บริการที่มีความสำคัญระดับโครงสร้างพื้นฐานของประเทศ รวมถึงตรวจสอบความโปร่งใสในการดำเนินงาน	
ข้อมูลผู้ใช้งาน (Users)	**จำนวน User ที่ ลงทะเบียนอยู่ในระบบ ทั้งการพิสูจน์หรือการยืนยันตัวตน** **จำนวน User ที่เพิ่มขึ้นในรอบปีที่ผ่านมา**	• ตรวจสอบ จำนวนผู้ใช้ที่ลงทะเบียนทั้งหมด และแยกเป็น Active Users / Inactive Users • ตรวจสอบว่าแต่ละระดับความเข้มงวดของการพิสูจน์ตัวตน (IAL) สอดคล้องกับระดับความปลอดภัยของการยืนยันตัวตน (AAL) หรือไม่	
	จำนวน User แยกตามข้อมูลประชากร (Demographic) ได้แก่ พื้นที่ ช่วงวัย	• เพื่อให้ ETDA วิเคราะห์การกระจายตัวของผู้ใช้งานบริการ IdP ทั้งในมิติพื้นที่และช่วงอายุ ว่าสอดคล้องกับเป้าหมายการขยายบริการพิสูจน์และยืนยันตัวตนทางดิจิทัลไปยังประชาชนกลุ่มต่าง ๆ หรือไม่ และตรวจสอบโอกาสในการเข้าถึงบริการของประชากรในแต่ละภูมิภาคหรือกลุ่มวัยที่อาจมีความเสี่ยงถูกกันออกจากระบบดิจิทัล	• ประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 3 ข้อ 36 • ประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 6 ข้อ 6
	กระบวนการตรวจสอบให้ลูกค้าเป็นปัจจุบัน ➢ ความถี่ในการตรวจสอบให้เป็นปัจจุบัน	• เพื่อประเมินว่าผู้ให้บริการ IdP มีการบริหารจัดการข้อมูลผู้ใช้งานให้เป็นปัจจุบันอยู่เสมอหรือไม่ มีความถี่ในการตรวจสอบและอัปเดตข้อมูลเพียงพอหรือเปล่า ซึ่งเป็นส่วนสำคัญในการรักษาความถูกต้องและความน่าเชื่อถือของระบบ รวมถึงป้องกันความเสี่ยงจากการใช้ข้อมูลที่ล้าสมัย	
ข้อมูลผู้ให้บริการ (RP)	**จำนวน RP ที่เชื่อมต่อและกลุ่ม / Sector ผู้ใช้ RP** ➢ กลุ่ม ภาครัฐ ➢ กลุ่ม Bank ➢ กลุ่ม Securities ➢ กลุ่ม AIMC ➢ กลุ่ม Digital Lending ➢ อื่น ๆ	• เพื่อให้ ETDA ทราบถึงการขยายตัวของระบบ IdP ในแง่ของผู้ให้บริการที่เข้ามาเชื่อมต่อ (RP) ทั้งจำนวนและความหลากหลายของกลุ่มธุรกิจหรือภาคส่วนที่ใช้งาน เพื่อวิเคราะห์ผลกระทบทางเศรษฐกิจ สังคม และความมั่นคงปลอดภัย ตลอดจนส่งเสริมการกำหนดแนวทางสนับสนุนหรือกำกับดูแลที่เหมาะสมตามลักษณะของผู้ใช้งานแต่ละกลุ่ม	

1. Operational Information (OI)

ข้อมูล		วัตถุประสงค์การรายงาน	การนำไปใช้
ข้อมูลสำคัญอื่น ๆ	นโยบายการบริหารจัดการความเสี่ยงที่สอดคล้องตามหลักเกณฑ์	• เพื่อให้ ETDA สามารถติดตามและประเมินความเหมาะสมในการบริหารจัดการภายในของผู้ให้บริการ IdP ผ่านการทบทวนและปรับปรุงนโยบายสำคัญต่าง ๆ ให้สอดคล้องกับบริบทที่เปลี่ยนแปลงไป ทั้งด้านกฎหมาย กฎระเบียบ มาตรฐานความมั่นคงปลอดภัย ภัยคุกคามทางไซเบอร์ เทคโนโลยีที่พัฒนาใหม่ รวมถึงการเปลี่ยนแปลงโครงสร้างองค์กรและรูปแบบการให้บริการ โดยมุ่งเน้นให้การดำเนินงานเป็นไปอย่างโปร่งใส มีประสิทธิภาพ และลดความเสี่ยงที่อาจเกิดขึ้นจากการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล ทั้งนี้เพื่อรักษามาตรฐานความปลอดภัย ความน่าเชื่อถือ และความมั่นใจของผู้ใช้บริการในระบบ IdP อย่างต่อเนื่อง	• หนังสือนำส่งข้อมูลประกอบการยื่นคำขอรับใบอนุญาตฯ/เอกสารแสดงความพร้อมของระบบงานฯ • ร่างหลักเกณฑ์การตรวจประเมินประจำปี
	นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy)		
	นโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy)		
	นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy policy)		
	นโยบายด้านการกำกับดูแลปฏิบัติงาน		
	นโยบายเกี่ยวกับการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ		
	นโยบายการบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก		
	นโยบายและแนวปฏิบัติเพิ่มเติมที่มีการประกาศใช้		

2 Performance & Efficiency (PE)

Pain Point

User/RP

- ระบบที่ใช้ Digital ID ล่าช้าในขั้นตอนการยืนยันตัวตน ส่งผลต่อการทำธุรกรรมโดยรวม
- ขาดการระบุปัญหาหรือข้อจำกัดในการใช้งาน จากมุมมองของผู้ใช้งาน

Regulator

ETDA

- ไม่สามารถวิเคราะห์เพื่อหาดัชนีชี้วัดสมรรถนะและศักยภาพของผู้ให้บริการ IDP ในปัจจุบัน

จุดประสงค์ในการร้องขอข้อมูล (Objectives)

- เพื่อติดตามและประเมินประสิทธิภาพการดำเนินงานของผู้ให้บริการ IdP ผ่านข้อมูลปริมาณธุรกรรม เหตุการณ์ผิดปกติ และการทุจริต เพื่อประเมินความพร้อมและความเสี่ยงในการให้บริการ
- เพื่อใช้ประกอบการกำกับดูแลและประเมินความเหมาะสมในการดำเนินงานของผู้ให้บริการ IdP ให้เป็นไปตามหลักเกณฑ์และมาตรฐานที่กำหนด โดยคำนึงถึงความมั่นคงปลอดภัยและผลกระทบต่อผู้ใช้บริการ

ชุดข้อมูลที่ต้องร้องขอ (Data Set)

- ข้อมูลการทำธุรกรรม (Transactions)
- ข้อมูลด้านอุบัติการณ์ (Incidents)
- ข้อมูลด้าน Incident ที่เกี่ยวข้องกับการทุจริตและฉ้อโกง (Fraud)
- ข้อมูลประสบการณ์ใช้งานจากลูกค้า (Customer Experiences)

ประโยชน์จากการรายงานข้อมูล (Benefits)

- เพื่อประเมินประสิทธิภาพการให้บริการของผู้ให้บริการ IdP ในด้านปริมาณธุรกรรม ความสำเร็จในการดำเนินงาน และความต่อเนื่องของบริการในแต่ละปี
- เพื่อวิเคราะห์ความเสถียรของระบบจากสถิติการเกิดปัญหาและเหตุการณ์ผิดปกติ (Incident/Fraud) เพื่อสะท้อนศักยภาพการดำเนินงานและความพร้อมในการรองรับการให้บริการ
- เพื่อใช้เป็นฐานข้อมูลเปรียบเทียบผลการดำเนินงานของผู้ให้บริการ IdP รายปี รวมถึงติดตามแนวโน้มด้านประสิทธิภาพและความเสี่ยงเชิงระบบในภาพรวม

2. Performance & Efficiency (PE)

ข้อมูล		วัตถุประสงค์การรายงาน	อ้างอิง
ข้อมูลการทำธุรกรรม (Transactions)	⭐ จำนวน Transaction ต่อปี สำหรับผู้บริการ (RP) จำแนกตามกลุ่มอุตสาหกรรม (Sector)	• เพื่อให้ ETDA สามารถติดตามและวิเคราะห์การใช้งานบริการพิสูจน์และยืนยันตัวตนทางดิจิทัลจากกลุ่มอุตสาหกรรมต่าง ๆ ว่ามีการขยายตัวหรือเปลี่ยนแปลงมากน้อยเพียงใดในแต่ละปี และใช้เป็นข้อมูลประกอบการกำหนดนโยบายส่งเสริมการใช้งานในภาคส่วนที่สำคัญหรือกลุ่มอุตสาหกรรมที่ยังมีการใช้งานน้อย	• ร่างหลักเกณฑ์การตรวจประเมินประจำปี
	⭐ จำนวน transaction ต่อปี สำหรับบริการพิสูจน์ตัวตนทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด	• เพื่อให้ ETDA สามารถประเมินประสิทธิภาพและความน่าเชื่อถือของกระบวนการพิสูจน์และยืนยันตัวตน โดยเปรียบเทียบจำนวนการทำรายการทั้งหมดกับจำนวนความสำเร็จและความล้มเหลว รวมถึงตรวจสอบแนวโน้มปัญหาที่อาจเกิดขึ้นในกระบวนการพิสูจน์และยืนยันตัวตน	
	⭐ จำนวน transaction ต่อปี สำหรับบริการยืนยันตัวตนทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด		
	⭐ จำนวน transaction ต่อปี สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลทั้งที่ทำรายการสำเร็จและไม่สำเร็จในรอบปีปฏิทินล่าสุด	• เพื่อประเมินประสิทธิภาพและความพร้อมของระบบในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานและระบบต่าง ๆ ว่าดำเนินการได้ราบรื่นและปลอดภัยเพียงใด โดยเฉพาะ ในการทำงานร่วมกับ RP และ Partner เพื่อลดปัญหาความล้มเหลวที่อาจกระทบต่อผู้ใช้งานปลายทาง	
ข้อมูลด้านอุบัติการณ์ (Incident)	⭐ จำนวน Incident จำแนกตามแต่ละประเภท ➢System ➢Network ➢Access control ➢Anti-Virus ➢Email ➢Web Portal ➢Software ➢File Sharing ➢Hardware ➢อื่น ๆ	• เพื่อให้ ETDA ตรวจสอบและวิเคราะห์ประเภทของเหตุการณ์ความผิดปกติที่เกิดขึ้นในระบบ IdP ว่ามีความเสี่ยงในส่วนใดเป็นพิเศษ เช่น ระบบเครือข่าย การควบคุมสิทธิ์เข้าถึง หรือระบบอีเมล เพื่อใช้วางแนวทางเฝ้าระวังและป้องกันเชิงรุกได้ตรงจุด	• ธพส. แนบท้าย ฉ.3 ข้อ 11.3
	⭐ จำนวน Incident จำแนกตามระดับความรุนแรง (Low / Medium / High / Critical)	• เพื่อประเมินระดับความรุนแรงของเหตุการณ์ที่เกิดขึ้นในระบบ IdP ตลอดปี และตรวจสอบว่าเหตุการณ์ระดับสูง (High / Critical) มีการจัดการแก้ไขอย่างเหมาะสมหรือไม่ เพื่อนำไปใช้พัฒนากลไกการรับมือและลดความเสี่ยงในอนาคต	
	⭐ จำนวน Incident จำแนกตามช่วงเวลาการเกิดเหตุ	• เพื่อวิเคราะห์แนวโน้มการเกิดเหตุการณ์ความผิดปกติในแต่ละช่วงเวลา เช่น รายเดือน หรือรายไตรมาส ว่ามีความถี่หรือความเสี่ยงเพิ่มขึ้นในช่วงใดเป็นพิเศษหรือไม่ เพื่อวางแผนเสริมความมั่นคงปลอดภัยในช่วงเวลาที่มีความเสี่ยงสูง	

2.Performance & Efficiency (PE)

ข้อมูล		วัตถุประสงค์การรายงาน	อ้างอิง
ข้อมูลด้าน Incident ที่เกี่ยวข้องกับการทุจริตและฉ้อโกง (Fraud)	จำนวน Fraud ในขั้นตอนการพิสูจน์ตัวตน	• เพื่อให้ ETDA สามารถตรวจสอบความเสี่ยงและแนวโน้มของการฉ้อโกงที่เกิดขึ้นในกระบวนการพิสูจน์และยืนยัน ว่ามีความถี่มากน้อยเพียงใด และใช้เป็นข้อมูลในการประเมินประสิทธิภาพของมาตรการควบคุมความปลอดภัยในขั้นตอนการพิสูจน์ตัวตน	• ประกาศ ธพส. แนบท้าย ฉ.4 ข้อ 8.5
	จำนวน Fraud ในขั้นตอนการยืนยันตัวตน		
	จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID ที่กระทำการสำเร็จในรอบปีปฏิทินล่าสุด	• เพื่อให้ ETDA ติดตามและประเมินความร้ายแรงของเหตุการณ์ทุจริตที่เกิดขึ้นจริงและส่งผลกระทบต่อระบบหรือผู้ใช้งาน พร้อมทั้งวิเคราะห์สาเหตุและผลกระทบจากกรณีที่เกิดการกระทำสำเร็จ เพื่อหาแนวทางป้องกันซ้ำ	
	จำนวน Fraud จำแนกตามแต่ละประเภท ➢การฉ้อโกงเอกลักษณ์ ➢การฉ้อโกงออนไลน์ ➢การฉ้อโกงทางการเงิน ➢การฉ้อโกงภายในองค์กร ➢การฉ้อโกงผู้บริโภค ➢อื่น ๆ	• เพื่อวิเคราะห์รูปแบบของการฉ้อโกงที่เกิดขึ้นในระบบ IdP ว่ามีประเภทใดเป็นความเสี่ยงหลัก เช่น การฉ้อโกงเอกลักษณ์หรือการฉ้อโกงทางการเงิน เพื่อกำหนดแนวทางป้องกันและปรับปรุงมาตรการรักษาความปลอดภัยให้ตรงจุด	
	จำนวน Fraud จำแนกตามระดับความรุนแรง (Low / Medium / High / Critical)	• เพื่อประเมินผลกระทบจากการฉ้อโกงที่เกิดขึ้น โดยจัดลำดับความรุนแรงเพื่อให้ ETDA สามารถวิเคราะห์ความเสี่ยงเชิงระบบและออกแบบมาตรการควบคุมเพิ่มเติมสำหรับเหตุการณ์ที่มีระดับความรุนแรงสูงหรือวิกฤต	
	การตอบสนองและการดำเนินการ	• เพื่อให้ ETDA ติดตามการจัดการเหตุการณ์ฉ้อโกงและความผิดปกติในระบบของ IdP ว่ามีการตอบสนองอย่างรวดเร็วและมีประสิทธิภาพเพียงใด รวมถึงตรวจสอบกระบวนการรับมือและแก้ไขปัญหาตามมาตรฐานที่กำหนด	
Customer Experiences & Satisfaction	Feedback จากผู้ใช้ เช่น ความคิดเห็น หรือข้อเสนอแนะ รวมถึง ปัญหาที่ผู้ใช้รายงาน เช่น ระบบล่ม, การยืนยันตัวตนล้มเหลว, หรือฟีเจอร์ที่ใช้งานไม่ได้	• เพื่อให้ ETDA ประเมินประสบการณ์และความพึงพอใจของผู้ใช้งานระบบ IdP โดยใช้ข้อมูลความคิดเห็นและข้อเสนอแนะมาเป็นแนวทางปรับปรุงคุณภาพการให้บริการให้ตรงกับความต้องการและลดปัญหาที่เกิดซ้ำ	• ร่างหลักเกณฑ์การตรวจประเมินประจำปี
ข้อมูลด้านประสิทธิภาพการให้บริการ	อัตรา การร้องเรียน ต่อ จำนวนผู้ใช้บริการ อัตรา ธุรกรรมที่สำเร็จ ต่อ จำนวนธุรกรรมทั้งหมด อัตรา จำนวนเรื่องร้องเรียนที่ได้รับการแก้ไข ต่อ จำนวนเรื่องร้องเรียนทั้งหมด	• เพื่อตรวจสอบความสามารถในการจัดการข้อร้องเรียนของผู้ให้บริการ IdP ว่ามีการตอบสนองและแก้ไขปัญหาได้มากน้อยเพียงใด สะท้อนถึงคุณภาพการบริหารจัดการปัญหาและการดูแลผู้ใช้งานอย่างมีประสิทธิภาพ	

3 Data Security and Protection (DS)

User

- ความกังวลในการเก็บรักษาข้อมูลส่วนบุคคล เช่น การรั่วไหลข้อมูล การขายข้อมูล
- ความกังวลในการถูกละเมิดและปลอมแปลงข้อมูลส่วนบุคคล (Fraud)
- การเรียกร้องการชดใช้จากผู้ให้บริการหากเกิดความเสียหายต่อข้อมูลส่วนบุคคล

Provider

- ไม่สามารถควบคุมการทำงานของระบบให้เป็นไปตามมาตรฐานจากปัจจัยภายใน เช่น บุคคลภายในหรือระบบทำข้อมูลรั่วไหล และจากปัจจัยภายนอก เช่น การถูกโจมตีระบบ

จุดประสงค์ในการร้องขอข้อมูล (Objectives)

- เพื่อใช้ในการติดตามและประเมินความมั่นคงปลอดภัยของระบบและความต่อเนื่องในการให้บริการของผู้ให้บริการ IdP ผ่านข้อมูลการตรวจประเมิน เหตุการณ์หยุดให้บริการ และข้อร้องเรียนที่เกิดขึ้น
- เพื่อประเมินผลกระทบจากเหตุการณ์ที่ส่งผลต่อการให้บริการ รวมถึงแนวทางการแก้ไขและป้องกัน เพื่อให้การกำกับดูแลด้านความมั่นคงปลอดภัยของข้อมูลและการให้บริการเป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับหลักเกณฑ์ที่กำหนด

ชุดข้อมูลที่ต้องร้องขอ (Data Set)

- ข้อมูลด้านความพร้อมและความปลอดภัยของระบบ

ประโยชน์จากการรายงานข้อมูล (Benefits)

- ใช้ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและความต่อเนื่องในการให้บริการของผู้ให้บริการ IdP จากข้อมูลการหยุดให้บริการ ข้อร้องเรียน และผลการตรวจประเมิน
- ใช้เป็นข้อมูลประกอบการกำกับดูแลเชิงป้องกันและประเมินความพร้อมของผู้ให้บริการในการรองรับเหตุการณ์ผิดปกติและการจัดการความเสี่ยงตามหลักเกณฑ์ที่กำหนด

3. Data Security and Protection (DS)

ข้อมูล		วัตถุประสงค์การรายงาน	อ้างอิง
ข้อมูลด้านความพร้อมและความปลอดภัยของระบบ	**รายการหยุดให้บริการแบบเตรียมการล่วงหน้า** ➢ จำนวนทั้งหมดในรอบปี ➢ จำนวนในแต่ละเดือน ➢ ระบบที่เกี่ยวข้อง ➢ ระยะเวลาหยุดให้บริการโดยเฉลี่ย ➢ ผลกระทบที่เกิดขึ้น ➢ แนวทางการลดผลกระทบ	• เพื่อให้ ETDA ติดตามและวิเคราะห์ความถี่และผลกระทบจากการหยุดให้บริการที่มีการวางแผนล่วงหน้า ตลอดจนประเมินความพร้อมของแผนการแจ้งเตือนและการลดผลกระทบต่อผู้ใช้บริการและระบบ โดยใช้เป็นข้อมูลกำกับดูแลคุณภาพของการบริหารจัดการระบบและบริการให้มีความต่อเนื่องและเสถียรภาพสูงสุด	• ประกาศ ธพส. แนบท้าย ฉ.7 ข้อ 4.1-4.2
	รายการหยุดให้บริการแบบไม่ได้เตรียมการล่วงหน้า ➢ จำนวนทั้งหมดในรอบปี ➢ จำนวนในแต่ละเดือน ➢ ระบบที่เกี่ยวข้อง ➢ ระยะเวลาหยุดให้บริการโดยเฉลี่ย ➢ ผลกระทบที่เกิดขึ้น ➢ แนวทางการลดผลกระทบ		
ข้อมูลเกี่ยวกับการร้องเรียน (Complaints)	**จำนวนและรายละเอียดของเรื่องร้องเรียน**	• เห็นภาพรวมของปัญหาหรือเรื่องร้องเรียนที่เกิดขึ้นและสาเหตุหรือปัญหาที่ทำให้ผู้ใช้บริการเกิดความไม่พอใจ หรือพบข้อผิดพลาดในการให้บริการ	• ประกาศ ธพส. แนบท้าย ฉ.7 ข้อ 9
	ประเภทเรื่องร้องเรียน	• แยกประเภทของปัญหาหรือข้อร้องเรียนที่เกิดขึ้น ซึ่งช่วยให้เห็นปัญหาที่เกิดบ่อยที่สุด และมีความสำคัญสูง	
	เวลา/ช่วงเดือนที่เกิดเรื่องร้องเรียน	• เพื่อระบุช่วงเวลา ที่เกิดเรื่องร้องเรียนมากที่สุด ซึ่งอาจสะท้อนถึงปัญหาที่เกิดจากการใช้งานในช่วงที่มีการใช้งานสูง	
	กลุ่มของผู้ร้องเรียน (User ของ RP เจ้าไหน / RP)	• ระบุว่าเรื่องร้องเรียนมาจากกลุ่มผู้ใช้บริการของ RP (Responsible Party) ใดหรือการร้องเรียนจากผู้ให้บริการ (IdP) ใด	
	จำนวนประเภทของเหตุของการร้องเรียน	• ระบุเหตุผลหลักที่ทำให้ผู้ใช้บริการร้องเรียนหรือฟ้องร้อง ซึ่งจะช่วยในการระบุปัญหาหรือข้อผิดพลาดที่ต้องได้รับการแก้ไข	
	การดำเนินการเพื่อแก้ไขปัญหาการร้องเรียนหรือฟ้องร้องแต่ละรายการ	• ทราบขั้นตอนและวิธีการที่ใช้ในการแก้ไขปัญหาหลังจากที่มีการร้องเรียนหรือฟ้องร้อง	
	แนวทางการป้องกันปัญหาเพื่อไม่ให้เกิดเหตุการณ์ดังกล่าวซ้ำอีก	• ทราบถึงมาตรการและวิธีการที่ใช้ในการป้องกันไม่ให้ปัญหาที่เกิดขึ้นซ้ำอีกในอนาคต	

4 Risk Management (RM)

Pain Point

Provider

- ขาดการแบ่งปันข้อมูลการบริหารความเสี่ยง เพื่อยกระดับมาตรฐานและคุณภาพในการจัดการความเสี่ยงอันเป็นประโยชน์และประสิทธิภาพของผู้ให้บริการในภาพรวม

จุดประสงค์ในการร้องขอข้อมูล (Objectives)

เพื่อให้เกิดการแบ่งปันข้อมูลความเสี่ยงระหว่างธุรกิจของผู้ให้บริการ ทำให้เกิดการวิเคราะห์ในภาพรวม การแบ่งปันข้อมูล แนวทาง และเพิ่มประสิทธิภาพในการจัดการความเสี่ยงธุรกิจ

ชุดข้อมูลที่ต้องร้องขอ (Data Set)

- **นโยบายความเสี่ยงที่เกี่ยวข้องกับธุรกิจ (risk identification)ตามลักษณะการให้บริการ**
  - ความเสี่ยงด้านกลยุทธ์ (strategic risk)
  - ความเสี่ยงด้านการปฏิบัติการ (operational risk)
  - ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk) ประเมินยุแล้วในไอที audit
  - ความเสี่ยงด้านชื่อเสียงขององค์กร (reputation risk)
  - ความเสี่ยงด้านการปฏิบัติตามหลักเกณฑ์ (compliance risk)
  - ความเสี่ยงด้านอื่น ๆ
- **ผลการประเมินความเสี่ยง (risk evaluation)**
  ซึ่งครอบคลุมการประเมินความเสี่ยงตั้งต้นและการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง
- **โครงสร้างหรือคณะกรรมการ/ผู้รับผิดชอบการบริหารความเสี่ยง (หากมีการเปลี่ยนแปลง)**

ประโยชน์จากการรายงานข้อมูล (Benefits)

- เพื่อให้สามารถเปรียบเทียบแนวโน้มความเสี่ยงและปัญหาของผู้ให้บริการ IdP รายต่าง ๆ ได้อย่างต่อเนื่อง และใช้ในการประเมินความเสี่ยงเชิงภาพรวมของระบบ Digital ID ในประเทศ
- เพื่อใช้วิเคราะห์และติดตามความเพียงพอของมาตรการควบคุมความเสี่ยง เช่น มีแผนรองรับกรณีระบบขัดข้องหรือไม่ มีแนวทางป้องกันผลกระทบต่อประชาชนหรือไม่ และสามารถลดความถี่หรือผลกระทบจากเหตุการณ์ซ้ำ ๆ ได้จริงหรือไม่

4. Risk Management (RM)

ข้อมูล		วัตถุประสงค์การรายงาน	การนำไปใช้
ข้อมูลกระบวนการในการบริหารจัดการความเสี่ยง	**นโยบายความเสี่ยงที่เกี่ยวข้องกับธุรกิจตามลักษณะการให้บริการ** ➢ ความเสี่ยงด้านกลยุทธ์ (strategic risk) ➢ ความเสี่ยงด้านการปฏิบัติการ (operational risk) ➢ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk) ประเมินยุแล้วในไอที audit ➢ ความเสี่ยงด้านชื่อเสียงขององค์กร (reputation risk) ➢ ความเสี่ยงด้านการปฏิบัติตามหลักเกณฑ์ (compliance risk) ➢ ความเสี่ยงด้านอื่น ๆ	• เพื่อตรวจสอบความเสี่ยงที่เกี่ยวข้องในมิติต่าง ๆ เช่น กลยุทธ์, การปฏิบัติการ, เทคโนโลยี, ชื่อเสียง, และการปฏิบัติตามหลักเกณฑ์ • เพื่อตรวจสอบความรุนแรงของความเสี่ยงและความสามารถในการบริหารจัดการ • เพื่อตรวจสอบวิธีการลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ • เพื่อทราบถึงตัวชี้วัดความเสี่ยงของแต่ละผู้ให้บริการ	• ใช้ข้อมูลเพื่อระบุความเสี่ยงทางธุรกิจ รวมถึงความเสี่ยงเชิงระบบที่อาจส่งผลต่อบริการ Digital ID • พัฒนาแนวทางป้องกันหรือกำหนดมาตรฐานที่ลดความเสี่ยงที่มีผลกระทบสูง
	ผลการประเมินความเสี่ยง (risk evaluation) ซึ่งครอบคลุมการประเมินความเสี่ยงตั้งต้นและการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง	• เพื่อตรวจสอบความรุนแรงของความเสี่ยงและความสามารถในการบริหารจัดการ	• แนะนำวิธีการปรับปรุงกระบวนการจัดการความเสี่ยงให้มีประสิทธิภาพมากขึ้น
	โครงสร้างหรือคณะกรรมการ/ผู้รับผิดชอบการบริหารความเสี่ยง(หากมีการเปลี่ยนแปลง)	• เพื่อตรวจสอบว่าผู้ให้บริการมีผู้รับผิดชอบการบริหารความเสี่ยงติดตามและรายงานความเสี่ยงอย่างสม่ำเสมอ	• ใช้ข้อมูลในการประเมินความพร้อมของผู้ให้บริการในการบริหารจัดการความเสี่ยง

5 Service Development & Improvement (SD)

Pain Point

Regulator

ETDA

ขาดข้อมูลการพัฒนาและยกระดับคุณภาพและการนำเทคโนโลยีไปต่อยอดสู่บริการอื่นเพื่อการกำหนดทิศทางในการกำกับของธุรกิจในอนาคต

จุดประสงค์ในการร้องขอข้อมูล (Objectives)

- เพื่อติดตามและประเมินการดำเนินงานด้านการพัฒนาระบบและการปรับปรุงบริการของผู้ให้บริการ IdP ในแต่ละปี ทั้งในส่วนของการเพิ่มประสิทธิภาพระบบ การพัฒนาฟีเจอร์ใหม่ และการขยายขอบเขตการให้บริการ เพื่อให้สอดคล้องกับบทบาทและเงื่อนไขตามหลักเกณฑ์ที่กำหนด
- เพื่อใช้เป็นข้อมูลประกอบการกำกับดูแลและเฝ้าระวังการดำเนินงานด้านการพัฒนาบริการว่าอยู่ในขอบเขตที่เหมาะสม มีความพร้อมเพียงพอ และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยและความเชื่อมั่นของระบบ Digital ID ในภาพรวม

ชุดข้อมูลที่ต้องร้องขอ (Data Set)

แผนการพัฒนาต่อยอดบริการที่เกี่ยวข้องกับเทคโนโลยี การพิสูจน์และยืนยันตัวตนในอนาคต (To-Be)

ประโยชน์จากการรายงานข้อมูล (Benefits)

- เพื่อใช้เป็นข้อมูลในการติดตามความคืบหน้าและความเหมาะสมของการปรับปรุงระบบ พัฒนาฟีเจอร์ใหม่ และขยายขอบเขตการให้บริการของผู้ให้บริการ IdP ให้เป็นไปตามหลักเกณฑ์และไม่ส่งผลกระทบต่อเสถียรภาพของระบบ
- เพื่อประเมินแนวโน้มการเติบโตของบริการและวิเคราะห์ศักยภาพในการให้บริการในอนาคต เพื่อสนับสนุนการกำกับดูแลให้สอดคล้องกับทิศทางการพัฒนาระบบ Digital ID ของประเทศในภาพรวม

5. Service Development and Improvement (SD)

ข้อมูล		วัตถุประสงค์การรายงาน	การนำไปใช้
การพัฒนาธุรกิจในอนาคต (To-Be)	**ผลดำเนินงานโดยรวม** ➢ ด้านการขยายช่องทางการให้บริการ เช่น ขยายจุดให้บริการ dip chip ➢ ด้านการขยายกลุ่มเป้าหมาย/ฐานลูกค้า เช่น กลุ่มที่เกี่ยวข้องกับการเงินและการธนาคาร กลุ่มหน่วยงานภาครัฐ ➢ ด้านการขยายการเชื่อมต่อระบบ/การพัฒนาระบบให้บริการ เช่น เพิ่มระบบ Load Balancing ➢ ด้านเทคโนโลยีและนวัตกรรม ใช้ AI วิเคราะห์พฤติกรรมเข้าสู่ระบบเพื่อตรวจจับความผิดปกติ ➢ ด้านอื่นๆ	• เพื่อติดตามและประเมินผลการดำเนินงานด้าน Digital ID • เพื่อใช้เป็นแนวทางในการวิเคราะห์แนวโน้มและพัฒนากลยุทธ์ด้าน Digital ID	• ใช้เป็นข้อมูลสนับสนุนการกำหนดนโยบาย Digital ID • ประเมินประสิทธิภาพการให้บริการ Digital ID • วางแผนพัฒนาระบบ Digital ID ในระยะยาว
	แผนการพัฒนาต่อยอดบริการการอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีการพิสูจน์และยืนยันตัวตน ➢ ประเภทบริการที่ต่อยอด ➢ เป้าหมายของการพัฒนา ➢ รายละเอียดแผนการพัฒนา	• เพื่อตรวจสอบการพัฒนาระบบพิสูจน์ตัวตน เช่น Passwordless Authentication	• ประเมินผลกระทบด้านความปลอดภัยและความสะดวกต่อผู้ใช้งาน- เสนอแนวทางกำกับดูแลที่สอดคล้องกับเทคโนโลยีที่นำมาใช้
	แผนการขยายขอบเขตการให้บริการ (Service Expansion Plans)	• เพื่อตรวจสอบการขยายบริการ Digital ID ไปยังกลุ่มผู้ใช้งานใหม่ หรือการให้บริการข้ามประเทศ	• กำกับดูแลให้การขยายบริการสอดคล้องกับมาตรฐานความปลอดภัยและกฎหมาย
	ข้อเสนอแนะเพิ่มเติมต่อสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ในการสนับสนุนเกี่ยวกับการให้บริการพิสูจน์และยืนยันตัวตน (Digital ID)		

04

สรุปผลจากการสัมภาษณ์เชิงลึกผู้ประกอบธุรกิจบริการ Digital ID

1 Operational Information (OI)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
งบการเงิน	• ในส่วนของรายได้ที่เกี่ยวข้องกับ Digital ID สามารถรายงานแยกได้แต่อาจจะต้องระบุให้ชัดเจนและในส่วนของค่าใช้จ่ายและต้นทุนระบบระบบเดียวกันอาจจะต่อทั้งมุม Digital ID และต่อไปมุมอื่น ๆ ซึ่งอาจจะเป็นระบบเดียวกัน หาก ETDA ต้องการให้รายงานควรจะระบุรายละเอียดและวัตถุประสงค์ของการร้องขอข้อมูลดังกล่าว
ข้อมูล Users	• พื้นที่ตาม Demographic โดยปกติทางหน่วยงาน เช่น Bank มีการเก็บแค่จำนวนธุรกรรม หากต้องการให้รายงานโดยแบ่งแยกตาม Demographic อาจจะต้องมีการตรวจสอบในแง่ของการขอความยินยอมจากลูกค้าว่าสามารถให้ข้อมูลส่วนนี้ได้หรือไม่
	• การแบ่ง Active/Inactive ของ Users ➢ บริการพิสูจน์ตัวตนนั้นเป็นการทำธุรกรรมเพียงครั้งเดียว การแบ่งสถานะของ Users อาจเป็นในแง่ของการ Validate ข้อมูล เช่น วันหมดอายุของบัตรประชาชน ➢ ผู้ให้สัมภาษณ์บางแห่งมองสถานะของ Users ผ่านการพิสูจน์ตัวตนบน NDID ถือว่าเป็น Active หากมีการทำธุรกรรมกับธนาคารแต่ไม่ได้ใช้งานในส่วนของ NDID ก็จะถือว่า เป็น Inactive ในแง่ของ Digital ID ➢ บริการยืนยันตัวตนนั้นส่วนใหญ่แบ่งแยกได้ตามสถานะการทำธุรกรรมทางการเงินของธนาคารโดยอาจใช้ เกณฑ์ 90 วันเป็นตัวแบ่งได้
	• กระบวนการตรวจสอบให้เป็นปัจจุบันบาง Bank ยึดตามหลักเกณฑ์ของ ปปง. ซึ่งเป็นสิ่งที่หลายหน่วยงานปฏิบัติตาม • ในส่วนของ ThaID จะมีข้อกำหนดที่จะให้ลูกค้ามา KYC ใหม่ทุกปี
	• ข้อมูล Users นั้น Proxy ไม่สามารถเก็บได้
ข้อมูล RP	• การแบ่ง Sector ของ RP ในส่วนของธนาคารนั้น บางหน่วยงานเสนอว่าตนให้บริการผ่าน NDID นั้น ใช้เกณฑ์การแบ่งตาม NDID ไม่ได้มีการจัดหมวดหมู่เอาไว้เอง
	• จำนวน RP ที่เชื่อมต่อ บางหน่วยงานมองว่าควรใช้ข้อมูลจาก NDID เพื่อลดความซ้ำซ้อนในการรายงาน • Proxy สามารถแยกข้อมูล RP ได้ เนื่องจากทุกคนที่มาต่อคือ RP
ข้อมูลด้านนโยบาย	• การรายงานการทบทวนนโยบายอาจมีการทำทุกปีอยู่แล้ว โดยอาจให้แบ่งเป็นในส่วนของมีการเปลี่ยนแปลงอย่างมีนัยสำคัญหรือไม่ หากมีนัยสำคัญค่อยอธิบายรายละเอียดการเปลี่ยนแปลง และหากไม่กระทบสาระสำคัญอาจไม่จำเป็นต้องรายงาน

1 Operational Information (OI)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
⭐กระบวนการตรวจสอบลูกค้าให้เป็นปัจจุบัน	• **อ้างอิงจากแนวทางปฏิบัติเรื่อง การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า ของ ปปง.** • บล./บลจ. ต้องตรวจทานและปรับปรุงข้อมูลต่าง ๆ ของลูกค้าที่ใช้ในการแสดงตน การระบุตัวตน และข้อมูลที่นำมาพิจารณาในการบริหารความเสี่ยงด้านการฟอกเงินและการสนับสนุนทางการเงินแก่การ ก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงให้เป็นข้อมูลปัจจุบันและดำเนินการ อย่างสม่ำเสมอจนกว่าจะยุติความสัมพันธ์ทางธุรกิจกับลูกค้า เช่น ตรวจสอบวันหมดอายุของบัตรประจำตัวประชาชนจากฐานข้อมูลของ บล./บลจ. หรือตรวจสอบข้อมูลผ่านระบบการตรวจสอบทางอิเล็กทรอนิกส์ของ หน่วยงานภาครัฐ หรือตรวจสอบจากแหล่งข้อมูลที่น่าเชื่อถือ หรือให้ลูกค้ายืนยัน หรือแก้ไข ข้อมูลจาก ฐานข้อมูลของ บล./บลจ. หรือการให้ลูกค้าทบทวน ยืนยัน หรือแก้ไข ข้อมูลผ่านช่องทางอิเล็กทรอนิกส์ หรือ เว็บเซอร์วิส หรือส่งจดหมายไปยังที่อยู่ของลูกค้า หรือโทรศัพท์ หรืออีเมล หรือส่งข้อความอิเล็กทรอนิกส์ หรือ การเดินทางไปพบลูกค้า หรือการเดินทางไปตรวจสอบธุรกิจของลูกค้า เป็นต้น

2 Performance & Efficiency (PE)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
ข้อมูลการทำธุรกรรม (Transactions)	• ข้อมูลการธุรกรรมหากต้องการข้อมูลที่ย้อนหลังมาก ๆ อาจจะต้องมีการแจ้งล่วงหน้าเนื่องจากบางหน่วยงานมีการเก็บข้อมูลไว้ในระบบคลาวด์ซึ่งทำให้การดูข้อมูลรายการธุรกรรมจะดูย้อนหลังได้แค่ 6 เดือน
	• ข้อมูลธุรกรรมที่ไม่สำเร็จบางแห่งอาจมีการแบ่งประเภทไว้อยู่แล้ว แต่ส่วนใหญ่มีการเก็บ log รายละเอียดไว้
	• บางหน่วยงานใช้เกณฑ์ Error Code ตาม NDID จึงอยากเสนอให้ใช้เป็นมาตรฐานเดียวกัน

2 Performance & Efficiency (PE)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
ข้อมูลด้านอุบัติการณ์ (Incident)	• การแบ่งประเภทความรุนแรงสูง กลาง ต่ำ มีการแบ่งไว้อยู่แล้วตามกรอบของ ISO27001 หรือตามเกณฑ์ในแง่ของ SLA ของแต่ละบริษัท • การแบ่งประเภทของ Incident มีความแตกต่างกันออกไปของแต่ละ IdP
	• อ้างอิงจาก ISO/IEC 27001 (มาตรฐานระบบการจัดการความปลอดภัยของข้อมูล - ISMS)

ระดับความรุนแรง	นิยาม
วิกฤติ (Critical)	ปัญหาที่เกิดกับลูกค้าทุกราย หรือส่งผลกระทบต่อ ทุกระบบงาน ต้องดำเนินการแก้ไขทันทีเพื่อลดผลกระทบที่เกิดขึ้น และแก้ไขโดยเร็วที่สุด ภายใน 4-6 ชั่วโมง
สูง (High)	ปัญหาที่เกิดขึ้นกับลูกค้าหลายราย หรือบางระบบงาน ต้องดำเนินการแก้ไขในระยะเวลาสั้น มีการติดตาม และแก้ไขภายใน 24 ชั่วโมง
ปานกลาง (Medium)	ปัญหาที่เกิดขึ้นกับลูกค้าเพียง 1 ราย หรือ 1 ระบบงาน จะต้องกำหนดวิธีการแก้ไขและเวลาให้เหมาะสม พร้อมติดตามและแก้ไข ภายใน 3-5 วัน
ต่ำ (Low)	ปัญหาที่เกิดขึ้นภายในบริษัทโดยไม่กระทบลูกค้า หรือส่งผลกระทบที่เกิดขึ้นมีผลกระทบน้อยและสามารถแก้ไขได้ในช่วงระยะเวลาสั้น ๆ หรือตามระยะเวลาที่กำหนด ต้องมีการติดตามและแก้ไขภายใน 5-7 วัน

2  Performance & Efficiency (PE)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
ข้อมูลด้านอุบัติการณ์ (Incident)	• อ้างอิงจาก ISO/IEC 27001 (มาตรฐานระบบการจัดการความปลอดภัยของข้อมูล - ISMS)

ประเภทของ Incident	นิยาม	ตัวอย่างเหตุการณ์ (Incident Examples)
System	ปัญหาที่เกิดจากระบบหลัก เช่น ความล้มเหลวของซอฟต์แวร์หรือโครงสร้างพื้นฐานในการจัดการ Digital ID	ระบบยืนยันตัวตนล่มขณะใช้งาน , ปัญหาที่เกี่ยวกับ batch
Network	ปัญหาการเชื่อมต่อหรือความปลอดภัยของเครือข่ายที่ใช้รับส่งข้อมูล Digital ID	Network ล่ม , infra problem (server, db, network)
Access Control	ปัญหาการควบคุมการเข้าถึงระบบหรือข้อมูล Digital ID เช่น สิทธิ์ใช้งานไม่เหมาะสม	ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงฐานข้อมูล Digital ID
Anti-Virus	ปัญหาการป้องกันมัลแวร์หรือไวรัสที่อาจกระทบต่อระบบ Digital ID	มัลแวร์ขโมยข้อมูลตัวตนจากเครื่องผู้ใช้
Email	ปัญหาที่เกี่ยวข้องกับอีเมล เช่น การถูกฟิชชิ่งเพื่อขโมยข้อมูล Digital ID	อีเมลข้อมูลส่วนบุคคลโดยไม่ใส่รหัส
Web Portal	ปัญหาที่เกิดจากพอร์ทัลหรือหน้าเว็บที่ให้บริการ Digital ID เช่น ช่องโหว่ด้านความปลอดภัย	เว็บพอร์ทัลถูกเจาะ ทำให้ข้อมูล Digital ID รั่วไหล
Software	ปัญหาจากซอฟต์แวร์ที่ใช้ในกระบวนการ Digital ID เช่น bug หรือผิดพลาด	ซอฟต์แวร์ e-KYC บันทึกข้อมูลผิดพลาด, เปรียบเทียบหน้าไม่ถูกต้อง
File Sharing	ปัญหาการแชร์ไฟล์ที่มีข้อมูล Digital ID โดยไม่ปลอดภัย	ไฟล์ข้อมูลลูกค้าถูกแชร์ผ่านช่องทางไม่เข้ารหัส
Hardware	ปัญหาจากอุปกรณ์ฮาร์ดแวร์ที่ใช้ในระบบ Digital ID เช่น เซิร์ฟเวอร์หรือเครื่องสแกน biometric	เครื่อง dipchip เสีย ทำให้ยืนยันตัวตนไม่ได้
อื่น ๆ	ปัญหาที่ไม่อยู่ในกลุ่มข้างต้น แต่เกี่ยวข้องกับ Digital ID (ระบุเพิ่มเติมได้)	ความผิดพลาดจากมนุษย์ เช่น พนักงานกรอกข้อมูลผิด เช่น โทรศัพท์ หรือ เป็นจาก customer/user เอง เช่น ตั้งค่าผิด หรือเข้าใจผิด

2  Performance & Efficiency (PE)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
ข้อมูลด้าน Fraud	• บางหน่วยงานให้ความเห็นว่ามีแค่การ Monitor จำนวนครั้งของการยืนยันตัวตนว่าผิดปกติไหม เช่น การทำซ้ำ ทำหลายผู้ว่าจ้าง ซึ่งอาจจะนำไปสู่ แต่ยังไม่ใช่ Fraud • ต้องนิยามให้ชัดว่า Fraud หมายถึงอะไรในด้านของ Digital ID
	• อ้างอิงจาก ISO/IEC 27001 (มาตรฐานระบบการจัดการความปลอดภัยของข้อมูล - ISMS)

ระดับความรุนแรง	นิยาม	ตัวอย่างเหตุการณ์ (Fraud Examples)
วิกฤติ (Critical)	กระทบระบบทั้งหมด อาจทำลายความน่าเชื่อถือของ Digital ID หรือบริษัท	แฮกระบบทั้งหมด ขโมยฐานข้อมูล Digital ID
สูง (High)	ความเสียหายรุนแรง กระทบชื่อเสียงบริษัท หรือผู้ใช้จำนวนมาก	การปลอม ID จำนวนมากเพื่อโจรกรรมเงินหลักล้าน
ปานกลาง (Medium)	กระทบผู้ใช้บางกลุ่มหรือระบบบางส่วน	ขโมย Digital ID ทำให้เสียเงินหลักหมื่น
ต่ำ (Low)	ความเสียหายจำกัด อาจกระทบผู้ใช้รายบุคคล	การฟิชชิ่งล้มเหลว, ขโมย ID แต่ใช้ไม่สำเร็จ

2  Performance & Efficiency (PE)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
ข้อมูลด้าน Fraud	• บางหน่วยงานให้ความเห็นว่ามีแค่การ Monitor จำนวนครั้งของการยืนยันตัวตนว่าผิดปกติไหม เช่น การทำซ้ำ ทำหลายผู้ว่าจ้าง ซึ่งอาจจะนำไปสู่ แต่ยังไม่ใช่ Fraud • ต้องนิยามให้ชัดว่า Fraud หมายถึงอะไรในด้านของ Digital ID
	• อ้างอิงจาก ISO/IEC 27001 (มาตรฐานระบบการจัดการความปลอดภัยของข้อมูล - ISMS)

ประเภทของ Fraud	นิยาม	ตัวอย่างเหตุการณ์ (Fraud Examples)
การปลอมอัตลักษณ์	การปลอมหรือปลอมแปลงข้อมูลตัวตนดิจิทัลเพื่อหลอกระบบ	ใช้ ID ปลอมสมัครบัญชี, ใช้บัตร ปชช. หมดอายุทั้งที่มีบัตรใหม่
การฉ้อโกงออนไลน์	การหลอกลวงผ่านช่องทางดิจิทัลที่เชื่อมโยงกับ Digital ID	ฟิชชิ่งเพื่อขโมยรหัส OTP หรือข้อมูลล็อกอิน
การฉ้อโกงทางการเงิน	การใช้ Digital ID ปลอมเพื่อเข้าถึงทรัพย์สินทางการเงิน	ปลอม Digital ID เพื่อโอนเงินจากบัญชีธนาคาร
การฉ้อโกงภายในองค์กร	การทุจริตโดยพนักงานที่เข้าถึงระบบ Digital ID	พนักงานปลอมข้อมูลลูกค้าในระบบ
การฉ้อโกงผู้บริโภค	การหลอกให้ผู้ใช้ส่งข้อมูล Digital ID เพื่อผลประโยชน์	หลอกให้อัปโหลด ID เพื่อแลกรางวัล

2  Performance & Efficiency (PE)

<table>
<tr><th>ประเด็น</th><th>ข้อคิดเห็น/ข้อกังวล</th></tr>
<tr><td>⭐ข้อมูลด้านข้อร้องเรียน (Complaint)</td><td>

ข้อร้องเรียนส่วนใหญ่จะเป็นข้อร้องเรียนภาพรวมของทั้งองค์กร ซึ่งมีการบันทึกไว้อยู่แล้วและอาจไม่ได้จำเพาะเจาะจงในส่วนของบริการด้าน Digital ID
ข้อร้องเรียนที่เป็นด้านข้อมูล บางแห่งจะนับรวมเป็น Incident ซึ่งจะทำให้การรายงานข้อมูลทับซ้อนกัน อาจจะต้องนิยมให้ชัดเจนว่า ข้อร้องเรียนกับ Incident ต่างกันอย่างไร
รายละเอียดการจำแนกประเภทของข้อมูลด้านการร้องเรียน (Complaints) พิจารณาจาก แนวทางของธนาคารแห่งประเทศไทย (BOT) และ มาตรฐานการจัดการเรื่องร้องเรียน (ISO 10002 - Complaint Handling)

<table>
<tr><th>ประเภทของเรื่องร้องเรียน</th><th>นิยาม</th><th>ตัวอย่างเหตุการณ์ (Complaint Examples)</th></tr>
<tr><td>ปัญหาการลงทะเบียน Digital ID (Registration Issues)</td><td>ปัญหาที่เกิดขึ้นในขั้นตอนการสมัครหรือยืนยันตัวตนผ่านระบบ Digital ID</td><td>• ไม่สามารถลงทะเบียน Digital ID ได้ (เช่น ข้อมูลไม่ตรงกับฐานข้อมูล)
• ระบบแจ้งข้อผิดพลาดเกี่ยวกับเอกสารหรือข้อมูลส่วนบุคคล
• การยืนยันตัวตนผ่านแอปพลิเคชันล้มเหลว (เช่น e-KYC ไม่ผ่าน)</td></tr>
<tr><td>ปัญหาการเข้าถึงและใช้งาน (Access & Usability Issues)</td><td>ปัญหาที่ทำให้ลูกค้าไม่สามารถใช้งาน Digital ID ได้ตามปกติ</td><td>• ไม่สามารถเข้าสู่ระบบหรือใช้งาน Digital ID ได้
• ระบบ NDID ล่มหรือใช้งานไม่ได้ในช่วงเวลาสำคัญ
• ระบบไม่รองรับอุปกรณ์หรือเวอร์ชันของแอปพลิเคชัน</td></tr>
<tr><td>ปัญหาธุรกรรมที่ไม่สำเร็จ (Failed Transactions)</td><td>ธุรกรรมที่ใช้ Digital ID ไม่สำเร็จหรือล่าช้า</td><td>• ยืนยันตัวตนสำเร็จ แต่ไม่สามารถทำธุรกรรมได้
• การโอนเงินหรือสมัครบริการผ่าน Digital ID ไม่สำเร็จ
• ระบบแจ้งเตือนข้อผิดพลาด (Error Code) ที่ไม่ชัดเจน</td></tr>
<tr><td>ปัญหาด้านความปลอดภัยและการฉ้อโกง (Security & Fraud Issues)</td><td>ปัญหาที่เกี่ยวข้องกับการใช้ Digital ID อย่างไม่ปลอดภัย หรือมีความเสี่ยงต่อการฉ้อโกง</td><td>• ถูกขโมย Digital ID หรือถูกใช้โดยไม่ได้รับอนุญาต
• ได้รับ OTP หรือการแจ้งเตือนธุรกรรมที่ไม่ได้ทำเอง
• ถูกหลอกให้กรอกข้อมูล Digital ID ผ่านเว็บไซต์ปลอม</td></tr>
<tr><td>ปัญหาด้านข้อมูลส่วนบุคคล (Privacy & Data Protection Issues)</td><td>ข้อร้องเรียนเกี่ยวกับความเป็นส่วนตัวของข้อมูล Digital ID และการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต</td><td>• ข้อมูล Digital ID ถูกนำไปใช้กับบริการที่ลูกค้าไม่ได้สมัคร
• ข้อมูลส่วนบุคคลรั่วไหลหรือถูกแชร์โดยไม่ได้รับความยินยอม
• ไม่สามารถขอลบหรือแก้ไขข้อมูล Digital ID ได้</td></tr>
<tr><td>ปัญหาด้านการให้บริการลูกค้า (Customer Support Issues)</td><td>ข้อร้องเรียนเกี่ยวกับการให้บริการและการแก้ไขปัญหาที่ไม่เป็นไปตามความคาดหวัง</td><td>• ติดต่อ Call Center แต่ไม่ได้รับคำตอบที่ชัดเจน
• ต้องรอเวลานานเกินไปในการแก้ไขปัญหา Digital ID
• ไม่มีช่องทางติดต่อที่สะดวกสำหรับเรื่อง Digital ID</td></tr>
<tr><td>ปัญหาด้านการยกเลิกหรือเปลี่ยนแปลงข้อมูล Digital ID</td><td>ปัญหาการปิดบัญชี Digital ID หรือเปลี่ยนแปลงข้อมูลที่ไม่สามารถทำได้สะดวก</td><td>• ต้องการยกเลิก Digital ID แต่ทำได้ยาก
• ข้อมูลที่อัปเดต (เช่น หมายเลขโทรศัพท์) ไม่ถูกต้องในระบบ NDID
• ไม่สามารถย้าย Digital ID ไปยังธนาคารอื่นได้</td></tr>
</table>
</td></tr>
</table>

3 Data Security and Protection (DS)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
ข้อมูลด้านความพร้อมและความปลอดภัยของระบบ	• ในบางหน่วยงาน แผนต่าง ๆ ที่เกี่ยวข้องกับความพร้อมของระบบ เช่น BCP DRP มีการทำเป็นภาพรวมของทั้งองค์กรอยู่แล้ว
	• รายการหยุดให้บริการแบบเตรียมการล่วงหน้าและแบบไม่ได้เตรียมการล่วงหน้ามีการรายงานระหว่างปีอยู่แล้วซึ่งบางหน่วยงานคิดว่าไม่ควรให้รายงานซ้ำอีก โดยหากจะให้รายงานสามารถทำได้เนื่องจากมีข้อมูลเก็บไว้อยู่แล้ว
	• บางหน่วยงานมีข้อกังวล ในการรายงานเช่นผล Security Test หรือ ผลการเจาะระบบให้ได้แต่ไม่สามารถให้รายละเอียดของผลได้
	• การทดสอบการเจาะระบบไม่ได้ทำทุกปีเนื่องจากมีค่าใช้จ่าย ส่วนใหญ่ทำ VA สแกนตาม ISO27001
	• มีความซ้ำซ้อนกับการ Audit ประจำปี โดยมองว่าควรใช้รายงานผล Audit เป็นสิ่งยืนยันประกอบการรายงานได้เลย

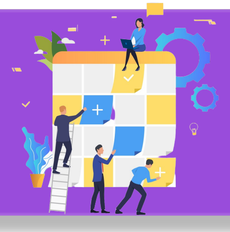
4 Risk Management (RM)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
ข้อมูลกระบวนการในการบริหารจัดการความเสี่ยง	• ความเสี่ยงส่วนใหญ่เป็นการประเมินความเสี่ยงทั้งองค์กร ไม่ได้ประเมินเฉพาะความเสี่ยงที่เกี่ยวข้องกับ DID
	• มองว่าให้ใช้ผล Audit ประจำปี กับรายงานหัวข้อที่อาจจะมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (ทั้งนี้ เฉพาะ IT Risk)
	• อ้างอิงจาก ISO/IEC 31000 (มาตรฐานระบบการจัดการความปลอดภัยของข้อมูล - ISMS)

ระดับความรุนแรง	นิยาม
วิกฤติ (Critical)	ความเสี่ยงในระดับสูง ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีแก้ไขความเสี่ยงและดำเนินการทันที
สูง (High)	ความเสี่ยงในระดับค่อนข้างสูง ไม่สามารถยอมรับยอมรับได้ ต้องพิจารณาหาวิธีแก้ไขความเสี่ยง และดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสม
ปานกลาง (Medium)	ความเสี่ยงในระดับปานกลาง ทำการติดตามผลความเสี่ยง และพิจารณาแก้ไขความเสี่ยง แต่หากมีเหตุจำเป็นก็สามารถพิจารณายอมรับความเสี่ยงได้
ต่ำ (Low)	ความเสี่ยงในระดับที่ต่ำมาก สามารถยอมรับได้โดยไม่ต้องดำเนินการใด ๆ เพิ่มเติม

5 Service Development & Improvement (SD)

ประเด็น	ข้อคิดเห็น/ข้อกังวล
การพัฒนาธุรกิจในอนาคต (To-Be)	• แผนทางธุรกิจ อาจจะมีปัจจัยจาก Partner ข้างนอกที่ยังไม่มีความชัดเจน เลยอยากให้กำหนด Criteria ความชัดเจนในการรายงาน
	• การรายงานการอัปเดทฟีเจอร์อาจจะให้กำหนดว่าเกี่ยวกับเฉพาะ Digital ID เช่น การอัปเดตทั้งแอปพลิเคชันของธนาคาร
	• ข้อมูลที่น่าจะเป็นข้อกังวลอาจจะเป็นเรื่องงบประมาณที่ใช้ ซึ่งให้ตัวเลขได้ไม่ตรง 100% อาจจะเป็นการให้ตัวเลขแบบคร่าว ๆ เนื่องจากแผนการพัฒนาหรือ Feature ใหม่ ๆ จะรู้เรื่องงบประมาณเมื่อไปลงมือทำจริง ๆ
	• แผนการพัฒนาต่อยอดการให้บริการอื่น ๆ หรือ Service การให้บริการ ทางธนคารมีความกังวลในการให้ข้อมูลซึ่งอาจจะเกี่ยวข้องกับความลับทางธุรกิจ
	• มีแผนการคาดการณ์ธุรกิจและพัฒนาในด้าน Digital ID และสามารถรายงานได้แต่ขอเป็น Optional

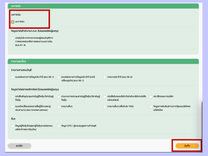


ข้อเสนอแนะอื่น ๆ เพิ่มเติม

ข้อคิดเห็น/ข้อกังวล
• พิจารณาถึงความซ้ำซ้อนเช่น IDP ที่มี Regulator ดูแลอยู่แล้วเช่น Bank อยากให้ข้อมูลที่ส่งมีความ Align ไปกับ Regualtor ละไม่ได้เพิ่มภาระให้กับ IDP
• ความชัดเจนและไม่ต้องตีความเพิ่ม เช่น Template ในการกรอกข้อมูล และ มี Guideline ความคาดหวังของการรายงานในแต่ละหัวข้อของข้อมูลทำให้ IDP ไม่ต้องตีความเพิ่ม
• ความ Lean ของข้อมูล พิจารณาในมุมของความเสี่ยงเช่นถ้าชุดข้อมูลไหนไม่ได้มีความเสี่ยงสูงมากหรือแจ้งไปแล้วตอนขออนุญาต ถ้าไม่ได้มีความเสี่ยงเพิ่มเติม อาจจะมีการ Lean รายงานว่า ส่วนไหนที่มีความเสี่ยงสูงต้องรายงานทุกปี หรือ ส่วนไหนที่มีความเสี่ยงต่ำ / ไม่มีการเปลี่ยนแปลง อาจจะไม่ต้องให้รายงาน
• ความคาดหวังอยากได้การแบ่งปันข้อมูลระหว่าง IdP อาจจะมีการจัดประชุมจากทาง ETDA เพื่อพูดคุยถึงประเด็นต่าง ๆ จากการรายงานไป อาจจะปีละครั้ง โดย ETDA อาจจะสรุปแต่ละประเด็นเพื่อมาแชร์กัน

หน่วยงานกำกับดูแลอื่น ๆ มีช่องทางการส่งข้อมูลที่หลากหลาย ทั้งผ่านระบบอัตโนมัติ เช่น DAP และ SETLink ที่ช่วยจัดเก็บและตรวจสอบข้อมูล รวมถึงการส่งผ่านอีเมลหรือส่งเอกสารทางไปรษณีย์ขึ้นอยู่กับประเภทของข้อมูล

ขั้นตอนและวิธีการนำส่งชุดข้อมูลของหน่วยงานภายใต้การกำกับดูแลอื่น ๆ

หน่วยงาน	1 การเตรียมพร้อมข้อมูลที่ต้องนำส่ง	2 กำหนดระยะเวลาในการส่ง	3 ช่องทางในการนำส่ง
	ชุดข้อมูล (Data Set) เป็นรูปแบบของข้อมูลที่กำหนดให้สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตที่มิใช่สถาบันการเงิน จัดส่งรายงานข้อมูลต่าง ๆ มายัง ธปท. ในรูปแบบต่าง ๆ ตามประกาศที่กำหนด • XML Format (eXtensible Markup Language) • รูปแบบเทมเพลต Excel • รูปแบบรายงานไฟล์ PDF	ภายใน 17.00 น. ของแต่ละวันที่กำหนดของแต่ละชุดข้อมูล ดังนี้ • รายสัปดาห์ • รายปักษ์ • รายเดือน • รายไตรมาส • ราย 6 เดือน • รายปี งบการเงินรอบระยะเวลา 12 เดือน ต้องดำเนินการให้แล้วเสร็จภายใน 21 วัน แต่ต้องไม่เกิน 4 เดือนนับแต่วันสิ้นปีบัญชีนั้น	 ชุดข้อมูล + Certificated  โปรแกรม DAP โดยใช้ Username/Password โดยต้องมีการลงทะเบียนและติดตั้งโปรแกรมก่อน ระบบจะบันทึกข้อมูลในการส่งเอาไว้ รวมถึงแจ้งสถานะการตรวจสอบ
กลต	บริษัทจดทะเบียนมีหน้าที่เปิดเผยข้อมูลที่สำคัญตามระยะเวลาเพื่อผู้ลงทุนและผู้ถือหุ้นได้ทราบข้อมูลสำคัญประกอบการพิจารณาลงทุนหรือตัดสินใจซื้อหรือขายหลักทรัพย์ • งบการเงินประจำปี (ฉบับตรวจสอบ) • งบการเงินรายไตรมาส (ฉบับตรวจสอบ) • แบบรายงาน 56-1 One Report	 • งบการเงินประจำปี ภายในวันที่ 31 มีนาคมนับจากวันสิ้นสุดรอบปี • งบการเงินรายไตรมาส (ฉบับตรวจสอบ) ภายใน 45 หลังสิ้นสุดไตรมาส • แบบรายงาน 56-1 One Report ภายในวันที่ 31 มีนาคมนับจากวันสิ้นสุดรอบปี ก.ล.ต. อาจพิจารณาเปรียบเทียบปรับบริษัทกรณีส่งรายงานตามรอบบัญชีล่าช้า หรือจัดทำข้อมูลไม่ครบถ้วนหรือไม่เป็นไปตามหลักเกณฑ์ที่กำหนด โดยบริษัทอาจต้องระวางโทษปรับไม่เกิน 100,000 บาท และปรับอีกไม่เกินวันละ 3,000 บาท ตลอดระยะเวลาที่ยังมิได้ปฏิบัติให้ถูกต้อง	SETLink ระบบงานที่ตลาดหลักทรัพย์ฯ จัดทำขึ้นเพื่อยกระดับการบริการให้กับบริษัทจดทะเบียนในลักษณะ end to end processสำหรับการเผยแพร่ข้อมูลของบริษัทจดทะเบียน  เลือกชุดข้อมูล กรอกรายละเอียด +แนบไฟล์ 
	แบบฟอร์มการจัดทำรายงาน ประกอบด้วย 4 ส่วน ดังนี้ • ใบนำส่ง • ข้อมูลนิติบุคคล • รายงานการประกอบกิจการ • ชุดข้อมูลที่ต้องนำส่ง รูปแบบเทมเพลต Excel รูปแบบรายงานไฟล์	ผู้รับใบอนุญาตประกอบกิจการกระจายเสียงหรือโทรทัศน์ ต้องจัดทำรายงานแสดงจำนวนผู้รับบริการ รายงานแสดงสถานะทางการเงินโดยแสดงรายรับรายจ่าย ต้นทุนแยกตามประเภทการให้บริการโครงข่ายกระจายเสียงหรือโทรทัศน์ ให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติทราบเป็นหนังสือภายใน 90 วัน ถัดจากวันสิ้นรอบระยะเวลาบัญชีของปี	 เอกสารตัวจริง นำส่งมายัง สำนักงาน กสทช. ด้วยตนเองหรือทางไปรษณีย์  ไฟล์อิเล็กทรอนิกส์นำส่งทาง (E-mail) network.bc@nbtc.go.th

ที่มา: บริการรับ-ส่งข้อมูลของ ธปท., SETLink, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

แนวทางการกำหนดไทม์ไลน์ของการนำส่งรายงานประจำปีของผู้ประกอบธุรกิจบริการ Digital ID นั้นต้องพิจารณาทั้งรูปแบบการทำรายงาน รวมถึงไทม์ไลน์และช่องทางในการจัดส่งเพื่อให้มีความสะดวกมากที่สุด

1 การเตรียมพร้อมข้อมูลที่ต้องนำส่ง

1. รูปแบบ One Report

ข้อดี:
- มีระบบการอนุมัติจากผู้บริหารก่อนนำส่ง ซึ่งช่วยให้ข้อมูลมีความน่าเชื่อถือและถูกต้อง
- รูปแบบเป็นมาตรฐานและสามารถใช้เป็นเอกสารอ้างอิงได้สะดวก อ่านง่าย

ข้อเสีย:
- กระบวนการรวบรวมข้อมูลอาจใช้เวลานาน เนื่องจากต้องรอการอนุมัติจากผู้บริหาร
- อาจเกิดความล่าช้าในการส่งข้อมูล หากฝ่ายใดฝ่ายหนึ่งยังไม่ได้ดำเนินการหรืออนุมัติ

2. รูปแบบ Excel

ข้อดี:
- ง่ายและสะดวกต่อการกรอกข้อมูล สามารถปรับแก้ไขได้อย่างรวดเร็ว
- ลดกระบวนการอนุมัติที่ซับซ้อน ทำให้การส่งข้อมูลรวดเร็ว
- เหมาะสำหรับข้อมูลเชิงปริมาณที่สามารถคำนวณและประมวลผลได้ง่าย

ข้อเสีย:
- มีข้อจำกัดในการส่งข้อมูลเชิงคุณภาพ หรือเอกสารแนบ อาจต้องใช้ช่องทางอื่นในการแนบเอกสารเพิ่มเติม
- ขาดกระบวนการอนุมัติจากผู้บริหารก่อนนำส่ง อาจส่งผลให้ข้อมูลมีความผิดพลาดหรือขาดความน่าเชื่อถือ

2 กำหนดระยะเวลาในการส่ง

ผู้รับใบอนุญาตส่งรายงาน

สิ้นปีดำเนินงาน → จัดเตรียมข้อมูลและทำรายงาน / ส่งรายงานผลการตรวจประเมิน → 90 วัน (31 มีนาคม)

ETDA ตรวจสอบความถูกต้อง

วันที่ได้รับรายงาน → พิจารณาและแจ้งสถานะ → 60 วัน

การขอผ่อนผันการส่งรายงาน

ยื่นคำขอผ่อนผันอย่างเป็นทางการ → อย่างน้อย 30 วันก่อนถึงกำหนดส่ง (หากพบว่าไม่สามารถดำเนินการได้ทันตามกำหนด ให้เตรียมข้อมูลเหตุผลการขอผ่อนผัน) → ETDA พิจารณาภายใน 15 วัน

สรุปไทม์ไลน์

- รอบปีดำเนินงานใช้ปีปฏิทินเป็นเกณฑ์
- มีเวลา 90 วัน ให้ผู้ประกอบการเตรียมข้อมูลและตรวจสอบความถูกต้อง
- สอดคล้องกับกำหนดส่งของ กลต. ที่กำหนดให้ส่งรายงานและงบการเงินภายใน 31 มีนาคม ของปีถัดไป
- อาจต้องพิจารณาบทลงโทษสำหรับผู้ประกอบการที่ส่งข้อมูลล่าช้า

3 ช่องทางในการนำส่ง

1. การส่งฉบับจริง (Hard Copy)

ข้อดี:
- ลดความเสี่ยงเรื่องการถูกดัดแปลงหรือแก้ไขข้อมูลภายหลัง
- สามารถแนบเอกสารสำคัญพร้อมลายเซ็นจริง ทำให้มีน้ำหนักทางกฎหมาย

ข้อเสีย:
- ใช้เวลาและทรัพยากรในการจัดพิมพ์และส่งทางไปรษณีย์หรือแมสเซ็นเจอร์
- อาจเกิดความล่าช้าหรือสูญหายระหว่างการจัดส่ง
- ต้องมีการจัดเก็บเอกสารในรูปแบบกระดาษ ทำให้เพิ่มภาระ

2. การส่งผ่านอีเมล

ข้อดี:
- สะดวก รวดเร็ว และไม่มีต้นทุนด้านการพิมพ์หรือการขนส่ง
- สามารถส่งเอกสารแนบและไฟล์ดิจิทัลได้ในรูปแบบ PDF หรือ Word
- มีหลักฐานการส่งผ่านระบบอีเมล ทำให้สามารถติดตามสถานะการส่งได้

ข้อเสีย:
- หากไม่มีการเข้ารหัสข้อมูล อาจเกิดปัญหาด้านความปลอดภัยและการรั่วไหลของข้อมูล

3. ระบบสนับสนุนการกำกับธุรกิจบริการทางดิจิทัล

ข้อดี:
- มีความปลอดภัยสูง เพราะใช้ระบบที่ควบคุมการเข้าถึงข้อมูล
- สามารถตรวจสอบสถานะการส่งและรับข้อมูลได้อย่างเป็นระบบ
- รองรับการแนบไฟล์และเอกสารดิจิทัลที่มีลายเซ็นอิเล็กทรอนิกส์ (e-Signature) ทำให้มีความน่าเชื่อถือ

ข้อเสีย:
- หากระบบมีปัญหาหรือเกิดความขัดข้อง อาจส่งผลกระทบต่อกำหนดการส่งเอกสาร

05

การต่อยอดข้อมูลจากการรายงาน

ตัวอย่างการรายงานข้อมูลการกำกับดูแลกิจการ สามารถใช้วิเคราะห์โดยเน้นการวิเคราะห์บทบาทของบริการต่าง ๆ การพัฒนาธุรกิจ และการกำหนดเป้าหมายในการพัฒนาซึ่งสามารถนำมาปรับใช้ในมุมมองของ Digital ID ได้

รายงานข้อมูลการกำกับดูแลจากหน่วยงานต่าง ๆ

ส่วนที่ 1

สถานะผู้ได้รับใบอนุญาติธุรกิจ สถิติการออกใบอนุญาต การคงสถานะ และอัตราการเปลี่ยนแปลง

ส่วนที่ 2

- สภาพตลาด หรือการใช้งานในปัจจุบัน
- จำนวนผู้ใช้งาน และอัตราการเปลี่ยนแปลง
- จำนวนการใช้งาน และอัตราการเปลี่ยนแปลง
- อัตราค่าบริการ และอัตราการเปลี่ยนแปลง
- รายได้ ค่าใช้จ่ายอื่น ๆ

ส่วนที่ 3

- การทดสอบมาตรฐานคุณภาพการให้บริการ
- ค่าเป้าหมายมาตรฐานของคุณภาพ
- ผลการทดสอบ

ส่วนที่ 4

- เรื่องร้องเรียน
- จำนวนเรื่องร้องเรียนแยกตามประเภท และอัตราการเปลี่ยนแปลง
- จำนวนเรื่องร้องเรียนแยกตามรายการ และอัตราการเปลี่ยนแปลง

การวิเคราะห์บทบาทความสำคัญและความจำเป็นของแต่ละบริการ

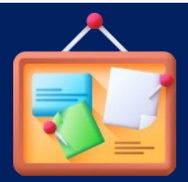
ทิศทางการพัฒนาของธุรกิจบริการ

การพัฒนาในปัจจุบันส่งเสริมความเชื่อมั่นในการงานใช้งาน

การเพิ่มขึ้นของการใช้งานอย่างแพร่หลายเป็นวงกว้าง ทำให้สามารถมองเห็นขอบเขตครอบคลุมทุกภาคส่วน

สาธารณสุข | การพัฒนาฝีมือแรงงาน | e-Commerce | บริการภาครัฐ | ภาคเอกชน

การกำหนดเป้าหมาย นโยบาย และกลยุทธ์ ในการพัฒนาบริการ



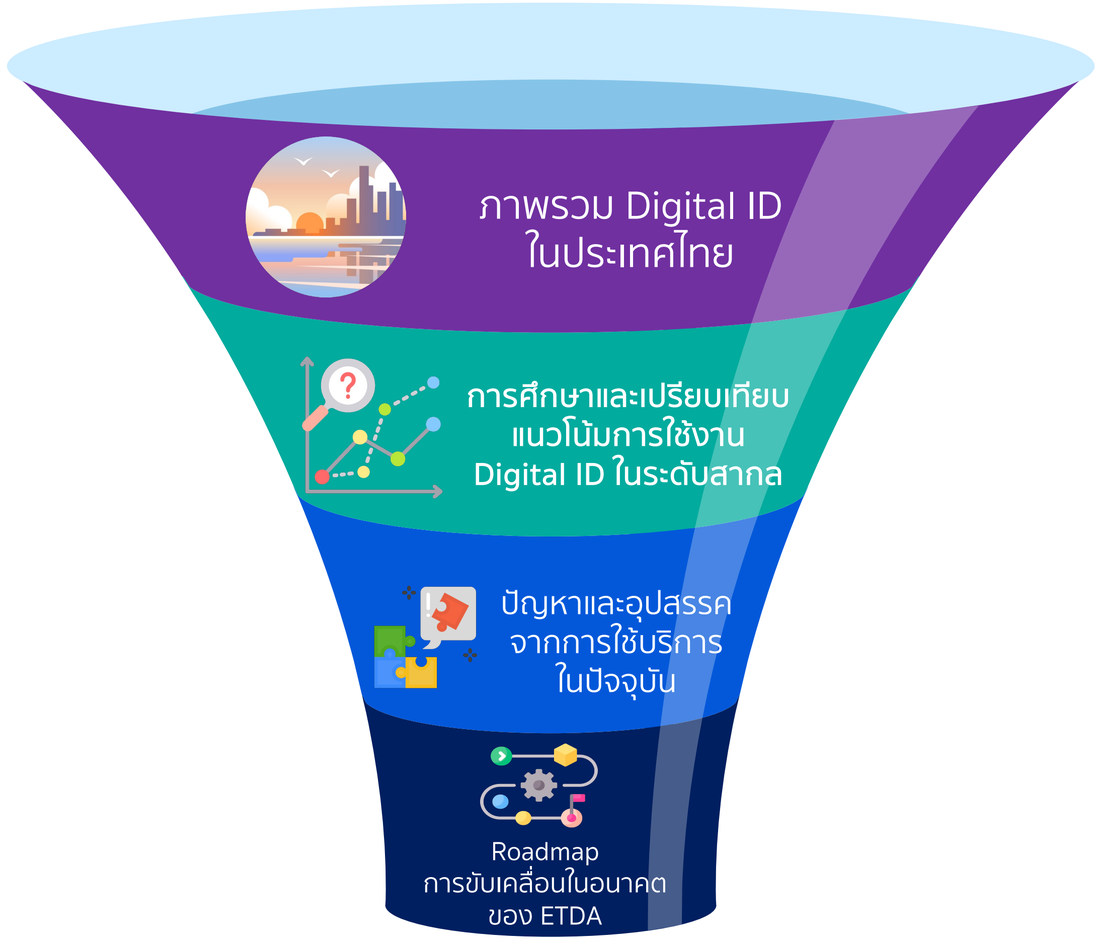
การสร้างตัวชี้วัด (Key Performance Indicators: KPIs) สำหรับ Digital ID

เช่น

- ตัวชี้วัดด้านประสิทธิภาพของระบบ Digital ID
- ตัวชี้วัดด้านการยอมรับและการใช้งาน

IdP คาดหวังให้ สพธอ. เป็นหน่วยงานกำกับดูแลเชิงรุก ที่ไม่เพียงกำกับดูแลแต่ต้องสังเคราะห์ข้อมูล วิเคราะห์แนวโน้ม แก้ไขอุปสรรค และกำหนดทิศทางระยาว เพื่อให้ Digital ID เติบโตอย่างมีประสิทธิภาพและสร้างความเชื่อมั่นต่อผู้ใช้บริการ

ความคาดหวังแนวทางการสังเคราะห์ข้อมูลเพื่อการนำไปใช้ประโยชน์



ภาพรวม Digital ID ในประเทศไทย

- IdP คาดหวังให้ ETDA สามารถรวบรวมและวิเคราะห์ข้อมูลจากผู้ให้บริการ Digital ID ในภาคส่วนต่าง ๆ เพื่อสร้าง**ฐานข้อมูลกลางที่สะท้อนถึงอัตราการเติบโตของผู้ใช้ Digital ID ในประเทศ**
- โดยข้อมูลเหล่านี้จะช่วยให้ IdP สามารถปรับกลยุทธ์การให้บริการให้ตรงกับแนวโน้มของตลาดและความต้องการของผู้ใช้ได้ดีขึ้น
- ตัวอย่างข้อมูล : ผลสรุปในรูปแบบกราฟ หรือ ผลสรุปเชิงพรรณนา

การศึกษาและเปรียบเทียบแนวโน้มการใช้งาน Digital ID ในระดับสากล

- IdP ต้องการให้ ETDA ทำหน้าที่เป็น **ศูนย์กลางข้อมูล** ที่ช่วยเปรียบเทียบสถานะของ Digital ID ไทยกับประเทศอื่น ๆ เพื่อให้ทราบว่า **ประเทศไทยอยู่ในระดับใดเมื่อเทียบกับมาตรฐานสากล หรือแนวโน้มการพัฒนา Digital ID ในต่างประเทศ เช่น เทคโนโลยีใหม่ ๆ**
- โดยข้อมูลจะช่วยผลักดันให้ประเทศไทยมีมาตรฐานการเชื่อมต่อที่รองรับการใช้ Digital ID ระดับสากล
- ตัวอย่างข้อมูล : ผลการจัดอันดับความสามารถในการเข้าถึง Digital ID ของประเทศไทย หรือ บทสรุปผู้บริหารสำหรับการพัฒนาทางธุรกิจ

การวิเคราะห์ปัญหาและอุปสรรคของ Digital ID ในปัจจุบัน

- IdP คาดหวังว่า ETDA จะนำข้อมูลจาก IdP และผู้ใช้บริการมาประมวลผล เพื่อวิเคราะห์ปัญหาหลักที่เกิดขึ้น เพื่อให้ ETDA ทำหน้าที่เป็น **ผู้ประสานงานหลัก** ที่ช่วยผลักดันให้มีการแก้ไขปัญหาเหล่านี้อย่างเป็นระบบ เช่น ปัญหาด้านอุบัติการณ์ที่เกิดขึ้นกับระบบพิสูจน์และยืนยันตัวตน ความเชื่อมั่นต่อการใช้งาน เป็นต้น
- ตัวอย่างข้อมูล : สรุปแนวโน้มปัญหาด้านอุบัติการณ์พร้อมแนวทางการแก้ไข หรือการจัดประชุม Committee เพื่อการหาแนวทางร่วมกัน

การกำหนด Roadmap ในอนาคตเพื่อขับเคลื่อน Digital ID ไทย

- IdP คาดหวังว่า ETDA จะกำหนด **แผนยุทธศาสตร์ระยะยาว (Roadmap)** ที่ชัดเจนโดยให้ความสำคัญกับการขับเคลื่อน นโยบายและมาตรฐานที่ส่งเสริมการใช้ Digital ID อย่างยั่งยืน เพื่อให้บริการของ IdP สามารถขยายตัวและพัฒนาไปในทิศทางที่สอดคล้องกับแนวโน้มระดับโลก


jenosize
consulting