(ร่าง) แนวทางการบริหารจัดการความเสี่ยง สำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID Risk Management Framework)

ฝ่าย.....
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Version .....
..... 2022

Version History

Version	Date	Description	Revised By
.....	 2565	.....	.....

สารบัญ

1. วัตถุประสงค์ 4

2. การกำหนดขอบเขต (Define scope) 4

3. การทำความเข้าใจบริบท (Understand context) 4

3.1 วัตถุประสงค์และความต้องการของผู้กำกับดูแล 4

3.2 วัตถุประสงค์และความต้องการขององค์กรที่ให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล 5

3.3 ปัจจัยภายนอกที่อาจส่งผลต่อการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล 5

4. กำหนดรูปแบบการประเมินความเสี่ยง (Define risk management model) 6

4.1 ขั้นตอนการพัฒนารูปแบบการประเมินความเสี่ยง 6

4.2 ภาพรวมของการประเมินและบริหารจัดการความเสี่ยงของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล .. 7

4.3 การประเมินความเสี่ยงตั้งต้นและความสามารถในการบริหารจัดการความเสี่ยง (Assess inherent risk and risk management capability) 29

4.4 กำหนดเกณฑ์การประเมินความเสี่ยง (Define risk criteria) 37

4.5 ขั้นตอนการประเมินความเสี่ยง ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) และการตอบสนองกับความเสี่ยง (Risk response) 39

4.6 การติดตามและรายงานผลความเสี่ยง (Risk monitoring and reporting) 49

5. คำจำกัดความ 50

แนวทางการบริหารจัดการความเสี่ยง
สำหรับธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

1. วัตถุประสงค์

ในปัจจุบันการดำเนินธุรกิจในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลกำลังเติบโตและมีแนวโน้มที่จะมีบทบาทอย่างมากในการขับเคลื่อนธุรกิจในประเทศไทย ทั้งนี้ความซับซ้อนของการให้บริการและเทคโนโลยีที่นำมาใช้ย่อมทำให้ธุรกิจในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเสี่ยงมากขึ้น ไม่ว่าจะเป็นความเสี่ยงทางด้านธุรกิจ ชื่อเสียง กฎหมายหรือเทคโนโลยี ดังนั้น สพธอ. จึงได้จัดทำเอกสารฉบับนี้ขึ้นเพื่อเป็นแนวทางในการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลอย่างเหมาะสม สอดคล้องตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลรวมถึงมาตรฐานสากลอื่นๆ ที่ยอมรับโดยทั่วไป รวมถึงสามารถดำเนินการจัดการและแก้ไขความเสี่ยงที่ถูกระบุขึ้นได้อย่างมีประสิทธิภาพ

ทาง สพธอ. มุ่งหวังว่าแนวทางปฏิบัตินี้จะมีประโยชน์อันกว้างต่อองค์กรที่ให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมถึงองค์กรอื่นๆ ที่สนใจนำไปปรับใช้เป็นแนวปฏิบัติในการประเมินความเสี่ยงเพื่อสร้างความเชื่อมั่นและความปลอดภัยในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ให้บริการต่อผู้ใช้บริการประชาชนทั่วไป

2. การกำหนดขอบเขต (Define scope)

เพื่อให้องค์กรสามารถที่จะประเมินและบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ การระบุขอบเขตถือเป็นกิจกรรมที่สำคัญที่ช่วยให้เข้าใจความเสี่ยงของระบบที่สนใจ สามารถสื่อสารทำความเข้าใจไปยังผู้ที่เกี่ยวข้องและสามารถแก้ไขและบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากที่สุด ทั้งนี้ขอบเขตในการประเมินความเสี่ยง คือ “กระบวนการทางธุรกิจที่เกี่ยวข้องหรือมีผลกระทบต่อความปลอดภัยและความน่าเชื่อถือของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล” โดยจะใช้ขอบเขตนี้เพื่อทำความเข้าใจบริบทขององค์กรที่ให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล, ระบุถึงกิจกรรมที่สำคัญ, การระบุปัจจัยความเสี่ยงที่เกี่ยวข้อง และนำไปสู่การประเมินความเสี่ยงและบริหารจัดการความเสี่ยงตามขอบเขตต่อไป

3. การทำความเข้าใจบริบท (Understand context)

สภาพแวดล้อมของการดำเนินการทางธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลถือว่าเป็นพื้นฐานที่สำคัญ และช่วยส่งผลในการระบุปัจจัยความเสี่ยงที่เกี่ยวข้องภายในธุรกิจ รวมถึงช่วยกำหนดถึงกลยุทธ์ในการรับมือและตอบสนองกับความเสี่ยง โดยทั้งนี้ได้มีการพิจารณาบริบทที่เกี่ยวข้องดังต่อไปนี้

3.1 วัตถุประสงค์และความต้องการของผู้กำกับดูแล

- เสริมสร้างให้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความน่าเชื่อถือและปลอดภัย
- ต้องการให้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลคำนึงเรื่องความเป็นส่วนตัว การใช้งานข้อมูลส่วนบุคคลเท่าที่จำเป็น และมีการควบคุมดูแลข้อมูลอย่างเหมาะสม
- ลดความเสี่ยงจากการปลอมแปลงตัวตนภายในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- ต้องการให้ระบบการพิสูจน์และยืนยันตนทางดิจิทัลโปร่งใส สามารถดำเนินการประเมินและตรวจสอบได้

3.2 วัตถุประสงค์และความต้องการขององค์กรที่ให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

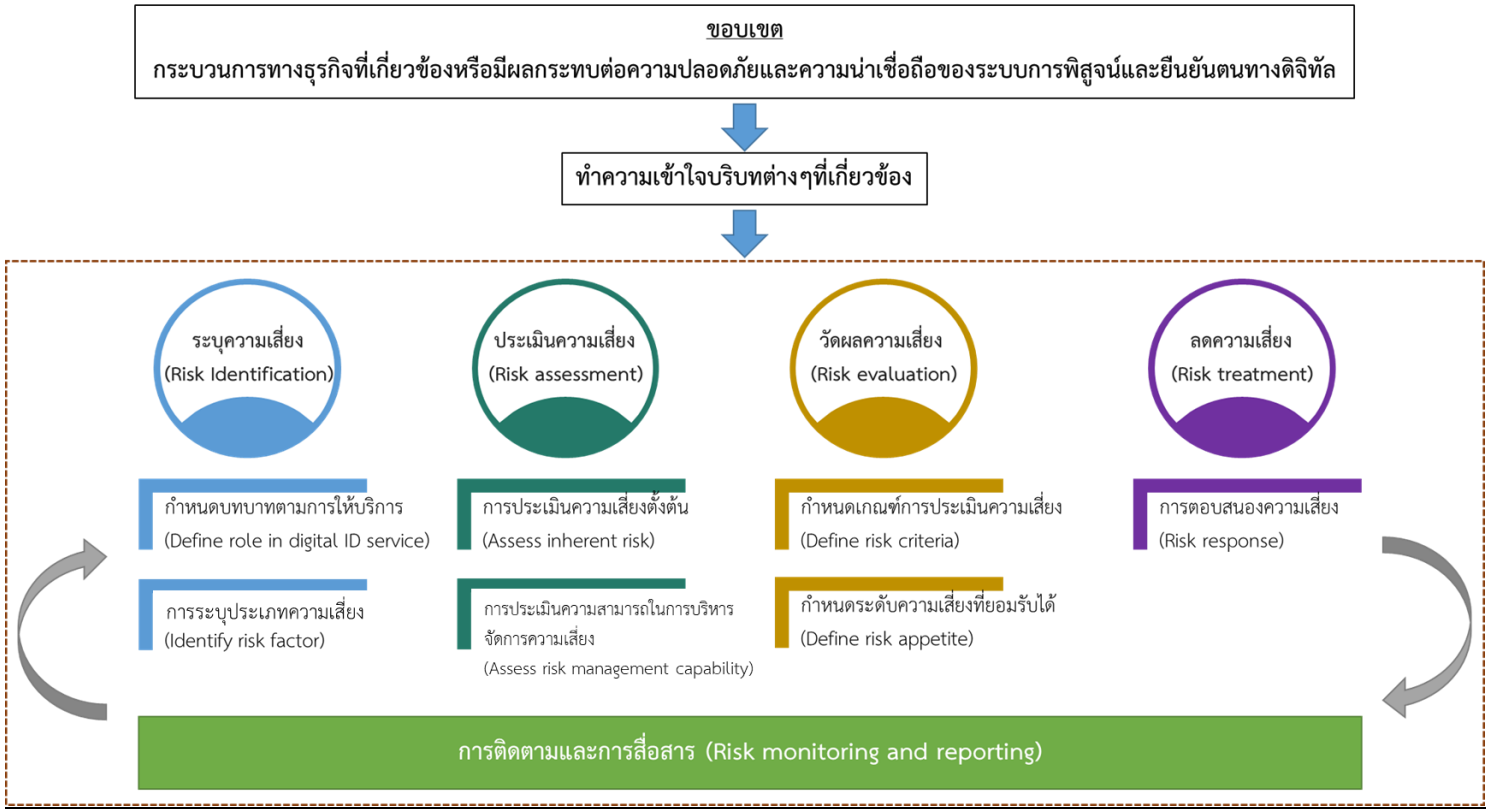
- ต้องป้องกันไม่ให้มีการปลอมแปลงข้อมูลที่อาจจะเกิดขึ้นขณะที่ให้บริการ
- เสริมสร้างการควบคุมภายใน เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- สามารถระบุความเสี่ยงด้านธุรกิจทั่วไปได้ นอกเหนือจากความเสี่ยงทางเทคนิค
- สามารถประยุกต์การประเมินความเสี่ยงที่องค์กรมีอยู่แล้ว มาใช้ในการระบุความเสี่ยงด้านการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

3.3 ปัจจัยภายนอกที่อาจส่งผลต่อการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

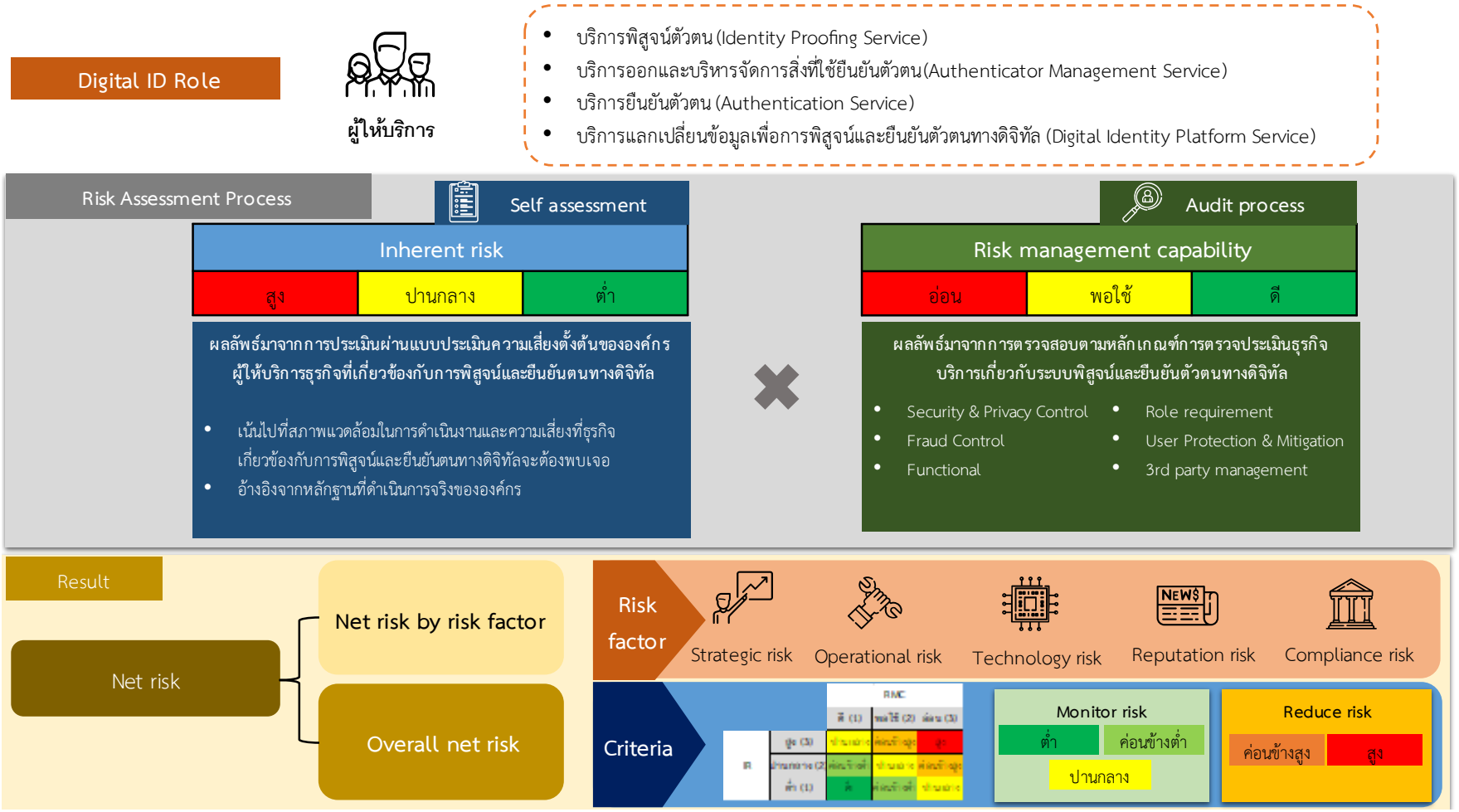
- ความก้าวหน้าของเทคโนโลยีที่นำมาใช้ในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- สภาพเศรษฐกิจ สังคม และการแข่งขันทางธุรกิจ
- แนวโน้มของภัยคุกคาม และความเสี่ยงที่อาจเกิดขึ้นในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- การดำเนินการของผู้ให้บริการภายนอกที่อาจเกี่ยวข้องกับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- สามารถดำเนินการได้ตามกฎหมายและหลักเกณฑ์ของประเทศ

4. กำหนดรูปแบบการประเมินความเสี่ยง (Define risk management model)

4.1 ขั้นตอนการพัฒนารูปแบบการประเมินความเสี่ยง



4.2 ภาพรวมของการประเมินและบริหารจัดการความเสี่ยงของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล



จากการกำหนดขอบเขตและการทำความเข้าใจบริบทต่างๆ ที่เกี่ยวข้องแล้วนั้น สพธอ. จึงได้กำหนดกรอบในการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องหรือมีผลกระทบต่อความปลอดภัยและความน่าเชื่อถือของระบบการพิสูจน์และยืนยันตนทางดิจิทัล โดยอ้างอิงตามหลักเกณฑ์การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลรวมถึงมาตรฐานสากลอื่นๆ เพื่อให้ทุกองค์กรที่ให้บริการระบบระบบการพิสูจน์และยืนยันตนทางดิจิทัลมีแนวทางในการประเมินเพื่อระบุความเสี่ยงตั้งต้นที่องค์กรมี (Inherent risk) ที่ใช้รองรับในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมถึงประเมินความสามารถในการบริหารจัดการความเสี่ยงภายในองค์กรเพื่อลดความเสี่ยงที่มีอยู่ (Risk management capability) ซึ่งจากการประเมินทั้ง 2 ส่วนนี้จะนำมาซึ่งความเสี่ยงสุทธิ (Net risk) ที่สามารถระบุแนวโน้มความเสี่ยงและหัวข้อที่องค์กรต้องพิจารณาปรับปรุงการควบคุมเพิ่มเติมในอนาคตได้

ทั้งนี้กรอบในการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องหรือมีผลกระทบต่อความปลอดภัยและความน่าเชื่อถือของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลนั้นจะประกอบไปด้วย 5 กิจกรรมที่สำคัญดังต่อไปนี้

- การระบุความเสี่ยงที่เกี่ยวข้องกับธุรกิจการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Risk identification)
- การประเมินความเสี่ยง (Risk assessment) ทั้งในส่วนของความเสี่ยงตั้งต้นและการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง
- การวัดผลความเสี่ยงกับเกณฑ์ประเมินความเสี่ยง (Risk evaluation)
- การลดความเสี่ยงหลังจากการประเมิน เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Risk treatment)
- การติดตามและรายงานผลความเสี่ยงอย่างต่อเนื่อง (Risk monitoring and reporting)

โดยในแต่ละกิจกรรมจะมีรายละเอียดขั้นตอนการปฏิบัติเพื่อให้เป็นไปตามกรอบในการประเมินและบริหารจัดการความเสี่ยงตามหัวข้อด้านล่าง

(1) กำหนดบทบาทตามลักษณะการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Define role in digital ID service)

สำหรับกิจกรรมการระบุความเสี่ยง จะเริ่มต้นด้วยการกำหนดบทบาทตามลักษณะการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยทั้งนี้ให้อ้างอิงจากบริการที่องค์กรได้ให้บริการกับทางผู้ใช้บริการ

โดยทั้งนี้จากที่ได้มีการกำหนดขอบเขตในการประเมินและบริหารจัดการความเสี่ยงไปในเบื้องต้นทำให้สามารถแจกแจงบทบาทที่สำคัญที่จะเกิดขึ้นจากการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ดังต่อไปนี้

1) หน่วยงานผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider Service : IdP) คือ หน่วยงานที่รับข้อมูลและบริหารข้อมูลจากผู้ใช้บริการในการดำเนินการพิสูจน์และยืนยันตัวตนทางดิจิทัล ทั้งนี้ในหน่วยงาน IdP ดังกล่าวจะสามารถแบ่งกระบวนการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนได้ ดังต่อไปนี้

1.1 บริการพิสูจน์ตัวตน (Identity Proofing Service) บริการที่ประกอบด้วย กระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น

1.2 บริการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Management Service) บริการที่ประกอบด้วย กระบวนการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น เช่น การออก Username ควบคู่กับ Password ให้ผู้ใช้บริการนำไปใช้ในการยืนยันตัวตน

1.3 บริการยืนยันตัวตน (Authentication Service) บริการที่ประกอบด้วย กระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น เช่น ยืนยัน Username และ Password ที่ผู้ใช้บริการนำมายืนยันตัวตนเพื่อ Login เข้าใช้บริการของผู้ให้บริการรายอื่น

2) หน่วยงานผู้ให้บริการบริการการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Exchange) คือ หน่วยงานที่รับหน้าที่เป็นตัวกลาง โดยมีเครือข่ายหรือระบบที่ใช้ในการเชื่อมโยงและเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(2) การระบุความเสี่ยง (Identify risk factor)

(2.1) ปัจจัยความเสี่ยง

ปัจจัยความเสี่ยงเป็นปัจจัยในด้านต่างๆ ที่สามารถระบุความเสี่ยงที่จะเกิดขึ้นจากการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยเบื้องต้นปัจจัยความเสี่ยงที่ได้ระบุในกรอบการประเมินนี้แบ่งออกเป็น 5 ปัจจัย ดังต่อไปนี้

- **ความเสี่ยงด้านกลยุทธ์ (Strategic risk)** หมายถึง ความเสี่ยงของการสูญเสียที่เกิดขึ้นจากการตัดสินใจทางธุรกิจที่ไม่พึงประสงค์ การตัดสินใจทางธุรกิจที่ไม่ดี หรือการไม่ตอบสนองต่อการเปลี่ยนแปลงในอุตสาหกรรมและสภาพแวดล้อมในการดำเนินงาน ทั้งนี้ ความเสี่ยงด้านกลยุทธ์สำหรับผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล มีความคล้ายคลึงกับความเสี่ยงขององค์กรทั่วไป โดยมีปัจจัยที่ต้องคำนึงถึง เช่น นโยบาย แผนกลยุทธ์ และการจัดสรรงบประมาณ อิทธิพลในการตัดสินใจเชิงกลยุทธ์ การบริหารความเสี่ยงในระดับองค์กร เป็นต้น
- **ความเสี่ยงด้านการปฏิบัติงาน (Operational risk)** หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก เช่น ความเสี่ยงจากการฉ้อโกงโดยบุคคลภายในและบุคคลภายนอก ความเสี่ยงจากการขัดข้องหรือหยุดชะงักของระบบงาน ความเสี่ยงจากแนวปฏิบัติเกี่ยวกับผู้ใช้บริการ การให้บริการและดำเนินธุรกิจ เป็นต้น
- **ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk)** ความเสี่ยงของผลลัพธ์ที่ไม่พึงประสงค์ ความเสียหาย การสูญเสีย การละเมิด ความล้มเหลวหรือการหยุดชะงักใดๆ ที่อาจเกิดขึ้นจากการใช้หรือการพึ่งพาฮาร์ดแวร์คอมพิวเตอร์ ซอฟต์แวร์ อุปกรณ์ ระบบ แอปพลิเคชัน และเครือข่าย ความเสี่ยงนี้มักเกี่ยวข้องกับข้อบกพร่องของระบบ ข้อผิดพลาดในการประมวลผล ข้อบกพร่องของซอฟต์แวร์ ข้อผิดพลาดในการทำงาน ความล้มเหลวของฮาร์ดแวร์ ความล้มเหลวของระบบ ความไม่เพียงพอของความจุ ช่องโหว่ของ

เครือข่าย จุดอ่อนในการควบคุม ข้อบกพร่องด้านความปลอดภัย การโจมตีที่เป็นอันตราย เหตุการณ์การเจาะระบบ โดยทั่วไปความเสี่ยงด้านเทคโนโลยีสำหรับผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล ตัวอย่างเช่น ภัยคุกคามทางไซเบอร์ การรั่วไหลของข้อมูล รวมถึงข้อมูลอ่อนไหวซึ่งมักเป็นองค์ประกอบสำคัญในธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- **ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation risk)** ความเสี่ยงที่ทำให้ผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้รับผลกระทบทางลบจากสังคม ส่งผลให้สูญเสียชื่อเสียงและความน่าเชื่อถือในการให้บริการ ตัวอย่างเช่น การเปิดเผยข้อมูลส่วนบุคคลของผู้ให้บริการโดยไม่ได้ตั้งใจ เป็นต้น
- **ความเสี่ยงทางด้านการปฏิบัติตามหลักเกณฑ์ (Compliance risk)** ความเสี่ยงที่เกิดจากการที่ผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัลไม่สามารถปฏิบัติงานสอดคล้องตามที่กฎหมาย กฎระเบียบหรือมาตรฐานที่เกี่ยวข้องกับการประกอบธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลกำหนด ทั้งนี้รวมถึงมาตรฐานสากลที่กฎหมายหรือกฎระเบียบอ้างถึงด้วย ตัวอย่างเช่น ไม่มีการปฏิบัติตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต เป็นต้น

(2.2) การกำหนดระดับความเสี่ยง

นอกจากนี้กรอบในการประเมินและบริหารจัดการความเสี่ยงมีการประเมินความเสี่ยงตั้งต้น (Inherent risk) ที่แบ่งระดับความเสี่ยงได้ 3 ระดับ ประกอบด้วย

- ระดับต่ำ
- ระดับปานกลาง
- ระดับสูง

เช่นเดียวกับการประเมินความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) ที่แบ่งระดับการควบคุมได้ 3 ระดับ ประกอบด้วย

- ระดับดี
- ระดับพอใช้
- ระดับอ่อน

ดังนั้น เพื่อให้ความชัดเจนในการแบ่งระดับความเสี่ยงและการควบคุมดังกล่าว จึงได้อธิบายรายละเอียดความหมายของการแบ่งระดับความเสี่ยงและการควบคุม โดยแยกเป็น 5 ปัจจัยความเสี่ยง ได้ดังต่อไปนี้

1. ความเสี่ยงด้านกลยุทธ์ (Strategic risk)	
ระดับความเสี่ยงตั้งต้น (Inherent risk)	
ต่ำ	ผู้ให้บริการมีการวางแผนด้านนโยบายและกลยุทธ์ที่ช่วยส่งเสริมการบริหารจัดการความเสี่ยงเป็นไปอย่างมีประสิทธิภาพในระยะยาว สะท้อนให้เห็นถึง เป้าหมาย วิสัยทัศน์ จุดแข็ง จุดอ่อน โอกาส และอุปสรรคในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลขององค์กรได้เป็นอย่างดี ส่งผลให้องค์กรมีความชัดเจนต่อการเปลี่ยนแปลงต่างๆ ที่อาจเกิดขึ้นในอนาคต รวมถึงมีการสื่อสารด้านนโยบายและกลยุทธ์อย่างทั่วถึงให้กับบุคลากรในองค์กรและบุคคลที่เกี่ยวข้อง รวมถึงองค์กรมีผลกระทบต่อการเปลี่ยนแปลงทั้งในส่วนภายในองค์กร (เช่น การควบรวมบริษัท, การเปลี่ยนแปลงตำแหน่ง) หรือภายนอกองค์กร (เช่น ความก้าวหน้าของเทคโนโลยีการพิสูจน์และยืนยันตัวตนทางดิจิทัล, พฤติกรรมของผู้ใช้บริการเปลี่ยนแปลง) เพียงเล็กน้อย ไม่ส่งผลกระทบอย่างมีนัยสำคัญกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
ปานกลาง	ผู้ให้บริการมีการวางแผนด้านนโยบายและกลยุทธ์ที่ช่วยส่งเสริมการบริหารจัดการความเสี่ยงโดยสะท้อนให้เห็นถึง เป้าหมาย วิสัยทัศน์ จุดแข็ง จุดอ่อน โอกาส และอุปสรรคในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลขององค์กร ทั้งนี้บางนโยบายหรือกลยุทธ์ยังอยู่ในระหว่างการตัดสินใจ ส่งผลให้องค์กรอาจมีการยังไม่มีความชัดเจนต่อการเปลี่ยนแปลงต่างๆ ในบางเรื่อง ทั้งนี้มีช่องทางในการสื่อสารด้านนโยบายและกลยุทธ์อย่างทั่วถึงให้กับบุคลากรในองค์กรและบุคคลที่เกี่ยวข้อง รวมถึงองค์กรมีผลกระทบต่อการเปลี่ยนแปลงทั้งในส่วนภายในองค์กร (เช่น การควบรวมบริษัท, การเปลี่ยนแปลงตำแหน่ง) หรือภายนอกองค์กร (เช่น ความก้าวหน้าของเทคโนโลยีการพิสูจน์และยืนยันตัวตนทางดิจิทัล, พฤติกรรมของผู้ใช้บริการเปลี่ยนแปลง) พอสมควรโดยไม่มีนัยสำคัญส่งผลกระทบกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพียงเล็กน้อย
สูง	ผู้ให้บริการยังไม่มีการวางแผนด้านนโยบายและกลยุทธ์ที่ช่วยส่งเสริมการบริหารจัดการความเสี่ยงโดยที่สะท้อนให้เห็นถึง เป้าหมาย วิสัยทัศน์ จุดแข็ง จุดอ่อน โอกาส และอุปสรรคในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลขององค์กร ทั้งนี้นโยบายหรือกลยุทธ์ที่สำคัญยังอยู่ในระหว่างร่างและทบทวน ส่งผลให้องค์กรยังไม่มีความชัดเจนต่อการเปลี่ยนแปลงต่างๆ และไม่สามารถตอบสนองต่อการเปลี่ยนแปลงที่เกิดขึ้นในอนาคต หรือยังไม่มีการสื่อสารด้านนโยบายและกลยุทธ์อย่างทั่วถึงให้กับบุคลากรในองค์กรและบุคคลที่เกี่ยวข้อง

	รวมถึงองค์กรมีผลกระทบต่อการเปลี่ยนแปลงทั้งในส่วนภายในองค์กร (เช่น การควบรวมบริษัท, การเปลี่ยนแปลงตำแหน่ง) หรือภายนอกองค์กร (เช่น ความก้าวหน้าของเทคโนโลยีการพิสูจน์และยืนยันตัวตนทางดิจิทัล, พฤติกรรมของผู้ใช้บริการเปลี่ยนแปลง) ที่มีนัยสำคัญต่อองค์กร ส่งผลกระทบกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพียงอย่างมาก ซึ่งอาจนำไปสู่ผลกระทบในแง่ลบต่อองค์กร
ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	
ดี	องค์กรมีนโยบาย แผนกลยุทธ์และการจัดสรรงบประมาณที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เช่น การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ, นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล, การจัดสรรงบประมาณที่สอดคล้องกับเป้าเชิงกลยุทธ์ที่เกี่ยวข้องกับการดำเนินธุรกิจพิสูจน์และยืนยันตัวตนทางดิจิทัล) ระบุไว้อย่างชัดเจน ช่วยให้ธุรกิจดำเนินไปได้ตามเป้าหมายขององค์กร ลดความเสี่ยงหรือผลกระทบจากความเสี่ยงที่เกิดขึ้น มีการทบทวนประสิทธิภาพในการบังคับใช้นโยบายและปรับปรุงให้ดียิ่งขึ้น มีการสื่อสารให้บุคลากรในองค์กรและบุคคลที่เกี่ยวข้องถึงหากมีการเปลี่ยนแปลงในด้านนโยบายหรือแผนกลยุทธ์ มีคณะกรรมการที่มีบทบาทหน้าที่ชัดเจน มีประสบการณ์และคุณสมบัติครบถ้วน เข้าร่วมตัดสินใจในทุกกิจกรรมสำคัญ ทั้งนี้ไม่มีผู้ใดมีอำนาจครอบงำผู้อื่น ดูแลรับผิดชอบความเสี่ยงทั้งหมดที่อาจเกิดขึ้นภายในองค์กร สามารถพัฒนาทิศทางกลยุทธ์และเพิ่มประสิทธิภาพในการปฏิบัติตามกลยุทธ์และในการดำเนินงานขององค์กร จนประสบความสำเร็จตามเป้าหมายกลยุทธ์ที่องค์กรตั้งใจไว้ นอกจากนี้องค์กรยังมีกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลและแนวทางปฏิบัติในเรื่องการจัดการความเสี่ยงนั้นครอบคลุมทุกกระบวนการตั้งแต่การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามทบทวนความเสี่ยง และการรายงานความเสี่ยง โดยมีการดำเนินการอย่างต่อเนื่องเป็นประจำเพื่อที่จะสามารถระบุความเสี่ยงที่อาจเกิดขึ้นจากระบบ Digital ID แล้วสามารถดำเนินการจัดการกับความเสี่ยงได้ทันท่วงที
พอใช้	องค์กรมีนโยบาย แผนกลยุทธ์และการจัดสรรงบประมาณที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เช่น การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ, นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล, การจัดสรรงบประมาณที่สอดคล้องกับเป้าเชิงกลยุทธ์ที่เกี่ยวข้องกับการดำเนินธุรกิจพิสูจน์และยืนยันตัวตนทางดิจิทัล) ทั้งนี้พบว่านโยบาย แผนกลยุทธ์และการจัดสรรงบประมาณบางหัวข้ออาจอยู่ระหว่างการตัดสินใจและการสื่อสาร ซึ่งอาจก่อให้เกิดความไม่ชัดเจนเล็กน้อยในเรื่องแนวทางการดำเนินงานขององค์กร มีการทบทวนประสิทธิภาพ

	ในการบังคับใช้นโยบายและปรับปรุงให้ดียิ่งขึ้น แต่ดำเนินการไม่สม่ำเสมอ มีการสื่อสารให้บุคลากรในองค์กรและบุคคลที่เกี่ยวข้องถึงการเปลี่ยนแปลงในด้านนโยบายหรือแผนกลยุทธ์ มีคณะกรรมการที่มีบทบาทหน้าที่ชัดเจน มีประสบการณ์และคุณสมบัติครบถ้วนโดยอาจไม่เข้าร่วมในการตัดสินใจทุกครั้ง แต่ไม่มีผลกระทบที่มีนัยสำคัญ ไม่มีผู้ใดมีอำนาจครอบงำผู้อื่น รวมถึงดูแลรับผิดชอบความเสี่ยงทั้งหมดที่อาจเกิดขึ้นภายในองค์กร นอกจากนี้องค์กรยังมีกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยนโยบายและแนวทางปฏิบัติในเรื่องการจัดการความเสี่ยงนั้นครอบคลุมทุกกระบวนการตั้งแต่การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามทบทว น ความเสี่ยง และการรายงานความเสี่ยง โดยมีการดำเนินการอย่างต่อเนื่องเป็นประจำ แต่ยังไม่สามารถระบุความเสี่ยงได้ครบถ้วน ซึ่งอาจส่งผลให้ไม่สามารถแก้ไขจัดการความเสี่ยงได้ครบถ้วน และอาจเกิดเหตุการณ์ภายในระบบ Digital ID ที่คาดไม่ถึง
อ่อน	องค์กรยังไม่มีนโยบาย แผนกลยุทธ์และการจัดสรรงบประมาณที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เช่น การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ, นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล, การจัดสรรงบประมาณที่สอดคล้องกับเป้าเชิงกลยุทธ์ที่เกี่ยวข้องกับการดำเนินธุรกิจพิสูจน์และยืนยันตัวตนทางดิจิทัล) อาจทำให้เป้าหมายในการดำเนินธุรกิจขององค์กรไม่ชัดเจนส่งผลให้การดำเนินการธุรกิจไม่สามารถบรรลุตามเป้าหมายได้และมีผลกระทบต่อองค์กร ไม่มีการทบทวนประสิทธิภาพในนโยบาย ส่งผลให้ไม่สามารถพัฒนาระบบการทำงานให้ดียิ่งขึ้นได้ มีคณะกรรมการที่มีบทบาทหน้าไม่ชัดเจน หรือมีประสบการณ์และคุณสมบัติไม่เพียงพอต่อการทำงานในหน้าที่ที่ได้รับมอบหมาย ไม่เข้าร่วมในการตัดสินใจทุกครั้งบ่อยครั้ง และมีผู้มีอำนาจครอบงำผู้อื่น ส่งผลให้ไม่สามารถพัฒนาทิศทางกลยุทธ์และเพิ่มประสิทธิภาพในการปฏิบัติต ามกลยุทธ์และในการดำเนินงานขององค์กรได้ นอกจากนี้ถึงแม้องค์กรยังจะมีกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล แต่ทั้งนี้นโยบายและแนวทางปฏิบัติไม่ครอบคลุมครบทุกเรื่องตั้งแต่การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามทบทวนความเสี่ยง และการรายงานความเสี่ยง รวมถึงมีการดำเนินการที่ไม่ต่อเนื่อง ส่งผลให้ไม่สามารถระบุหรือแก้ไขจัดการความเสี่ยงได้ครบถ้วนจนนำไปสู่ผลกระทบไม่มากก็น้อยต่อระบบ Digital ID

2. ความเสี่ยงด้านการปฏิบัติงาน (Operational risk)	
ระดับความเสี่ยงตั้งต้น (Inherent risk)	
ต่ำ	จำนวนของผู้ให้บริการภายนอกที่มีนัยสำคัญกับการให้บริการ Digital ID อยู่นั้น มีจำนวนเล็กน้อยและเกี่ยวข้องกับการให้บริการเพียงบางส่วนเท่านั้น ซึ่งหากเกิดการดำเนินการที่ผิดพลาดจากผู้ให้บริการภายนอกอาจไม่ส่งกระทบต่อชื่อเสียง รายได้หรือโอกาสขององค์กร ความซับซ้อนของระบบ Digital ID น้อยเนื่องจากไม่ได้มีการใช้นวัตกรรมหรือมีการประยุกต์ในการให้บริการในรูปแบบใหม่ มีการใช้ระดับความน่าเชื่อถือของการพิสูจน์ตัวตนและการยืนยันตัวตนที่ต่ำ ทำให้ไม่มีการใช้งานข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงและดำเนินการไม่ซับซ้อน ปริมาณบัญชีผู้ใช้งานระบบ Digital ID และจำนวนจุดที่ให้บริการยังมีปริมาณที่ไม่มากอันส่งผลกระทบเพียงเล็กน้อยหากมีความผิดพลาดในการดำเนินการดูแลและพัฒนาระบบ มีการหยุดชะงักในการให้บริการ รวมไปถึงมีการทุจริตเกิดขึ้นในระบบ ทั้งนี้องค์กรไม่พบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือพบเหตุการณ์การทุจริต หรือการฉ้อโกงที่เกี่ยวกับการให้บริการ Digital ID โดยมีผลกระทบในระดับกลางขึ้นไป จำนวนของพนักงานมีปริมาณไม่มาก อัตราการลาออกของพนักงานอยู่ในระดับต่ำในรอบ 12 เดือนที่ผ่านมา ซึ่งพนักงานที่ลาออกนั้น ส่วนมากไม่ได้มีสิทธิ์สูงภายในระบบ Digital ID ผู้ให้บริการภายนอกมีหน้าที่เกี่ยวข้องกับการดูแลระบบ Digital ID เพียงเล็กน้อย โดยที่ผู้ดูแลระบบส่วนใหญ่จะเป็นพนักงานขององค์กรเองที่ดูแลรับผิดชอบ ดังนั้นจึงมีความเสี่ยงภายในระบบ Digital ID เพียงเล็กน้อยและเกิดผลกระทบที่ไม่ร้ายแรง
ปานกลาง	จำนวนของหน่วยงานภายนอกที่มีนัยสำคัญกับการให้บริการ Digital ID อยู่นั้น มีจำนวนพอประมาณและเกี่ยวข้องกับการให้บริการอย่างมีนัยสำคัญ ซึ่งหากเกิดการดำเนินการที่ผิดพลาดจากผู้ให้บริการภายนอกอาจส่งกระทบต่อชื่อเสียง รายได้หรือโอกาสขององค์กร ความซับซ้อนของระบบ Digital ID น้อยในปัจจุบัน แต่ในอนาคตอาจมีการใช้งานนวัตกรรม หรือบริการในรูปแบบใหม่ที่อยู่ระหว่างการทดสอบ มีการใช้ระดับความน่าเชื่อถือของการพิสูจน์ตัวตนและการยืนยันตัวตนระดับกลาง ทำให้มีการใช้งานข้อมูลส่วนบุคคลและดำเนินการที่ซับซ้อ น พอประมาณ ทั้งนี้ปริมาณบัญชีผู้ใช้งานระบบ Digital ID และจำนวนจุดที่ให้บริการยังมีปริมาณอยู่ในระดับที่ไม่มีนัยสำคัญอันส่งผลกระทบหากมีความผิดพลาดในการดำเนินการดูแลและพัฒนาระบบ มีการหยุดชะงักในการให้บริการ รวมไปถึงมีการทุจริตเกิดขึ้นในระบบ แต่ยังอยู่ในระดับที่สามารถรับมือได้อย่างรวดเร็ว

	ทั้งนี้องค์กรพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือพบเหตุการณ์การทุจริต หรือการฉ้อโกงที่เกี่ยวกับการให้บริการ Digital ID โดยมีผลกระทบในระดับกลางขึ้นไปบ้าง แต่ไม่ถึงพบเหตุการณ์ที่ร้ายแรงที่ส่งผลกระทบต่อการดำเนินธุรกิจขององค์กร จำนวนของพนักงานมีปริมาณพอใช้ อัตราการลาออกของพนักงานอยู่ในระดับปานกลางในรอบ 12 เดือนที่ผ่านมา ซึ่งพนักงานที่ลาออกนั้น ส่วนมากอาจมีสิทธิ์สูงภายในระบบ Digital ID ด้วย ทำให้อาจมีความเสี่ยงต่อการบริหารจัดการบัญชีสิทธิ์สูง แต่อยู่ในระดับที่ไม่สูงมาก องค์กรมีการใช้งานผู้ให้บริการภายนอกเพื่อดูแลระบบ Digital ID พอประมาณ โดยมีการแบ่งหน้าที่ผู้ดูแลระบบบางส่วนให้กับผู้ให้บริการภายนอกดูแลรับผิดชอบ ดังนั้นจึงมีความเสี่ยงภายในระบบ Digital ID ที่เกิดจากการดำเนินการที่ผิดพลาดหรือไม่เป็นกระบวนการขององค์กรจากหน่วยงานภายนอก ซึ่งอาจเกิดผลกระทบได้
สูง	จำนวนของหน่วยงานภายนอกที่มีนัยสำคัญกับการให้บริการ Digital ID อยู่นั้น มีจำนวนมากและเกี่ยวข้องกับการให้บริการอย่างมีนัยสำคัญ ซึ่งหากเกิดการดำเนินการที่ผิดพลาดจากผู้ให้บริการภายนอกอาจส่งกระทบต่อชื่อเสียง รายได้หรือโอกาสขององค์กรในระดับสูง มีความซับซ้อนของระบบ Digital ID เนื่องจากมีการใช้งานนวัตกรรมใหม่ในการให้บริการ ซึ่งอาจเพิ่มความเสี่ยงจากความบกพร่องหรือผิดพลาด มีการใช้ระดับความน่าเชื่อถือของการพิสูจน์ตัวตนและการยืนยันตัวตนระดับสูงทำให้มีการใช้งานข้อมูลส่วนบุคคลที่สำคัญและดำเนินการที่ ซับซ้อน ทั้งนี้ปริมาณบัญชีผู้ใช้งานระบบ Digital ID และจำนวนจุดที่ให้บริการมีจำนวนมากซึ่งอาจส่งผลกระทบสูงต่อองค์กรหากมีความผิดพลาดในการดำเนินการดูแลและพัฒนาระบบ มีการหยุดชะงักในการให้บริการ รวมไปถึงมีการทุจริตเกิดขึ้นในระบบ ทั้งนี้องค์กรพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือพบเหตุการณ์การทุจริต หรือการฉ้อโกงที่เกี่ยวกับการให้บริการ Digital ID โดยมีผลกระทบในระดับสูง ซึ่งเป็นเหตุการณ์ที่ร้ายแรงและส่งผลกระทบต่อการดำเนินธุรกิจขององค์กร ทำให้การดำเนินการธุรกิจขององค์กรต้องหยุดชะงักลง จำนวนของพนักงานมีปริมาณมาก อัตราการลาออกของพนักงานอยู่ในระดับสูงในรอบ 12 เดือนที่ผ่านมา ซึ่งพนักงานที่ลาออกนั้น ส่วนมากอาจมีสิทธิ์สูงภายในระบบ Digital ID ด้วยทำให้อาจมีความเสี่ยงต่อการบริหารจัดการบัญชีสิทธิ์สูง ทั้งนี้องค์กรมีการใช้งานผู้ให้บริการภายนอกเพื่อดูแลระบบ Digital ID เป็นจำนวนมากและมีการแบ่งหน้าที่ผู้ดูแลระบบจำนวนนึงให้กับผู้ให้บริการภายนอกดูแลรับผิดชอบ ดังนั้นจึงมีความเสี่ยงภายในระบบ Digital ID ที่เกิดจากการดำเนินการที่ผิดพลาดหรือไม่เป็นกระบวนการขององค์กรจากหน่วยงานภายนอก

ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	
ดี	องค์กรมีการกำหนดแผนในการป้องกันและจัดการการฉ้อโกงหรือการทุจริต ซึ่งมีเนื้อหาที่เกี่ยวข้องกับการบริหารจัดการบุคลากร วิธีการส่งเสริมและควบคุมไม่ให้เกิดการฉ้อโกงหรือทุจริต กลไกในติดตามและจัดการกับเหตุที่เกิดขึ้น รวมไปถึงขั้นตอนการให้ความช่วยเหลือผู้ใช้บริการ จากเหตุการณ์ทุจริตหรือฉ้อโกงภายในระบบ Digital ID ครบถ้วน ทั้งนี้นโยบายและขั้นตอนการปฏิบัติดังกล่าวมีการประกาศใช้งานภายในองค์กร มีการกำหนดคณะกรรมการและคณะทำงานที่รับผิดชอบ รวมถึงมีการทบทวนและประเมินนโยบายดังกล่าวเป็นระยะ องค์กรมีการกำหนดนโยบายและขั้นตอนในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งมีเนื้อหาในส่วนของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศ รวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจ ทั้งนี้นโยบายและขั้นตอนการปฏิบัติมีการประกาศใช้งานภายในองค์กร มีการกำหนดคณะกรรมการและคณะทำงานที่รับผิดชอบ รวมถึงมีการทบทวนและประเมินนโยบายดังกล่าวเป็นระยะ นอกจากนี้ยังมีคณะกรรมการและคณะทำงานที่ดูแลทางด้านข้อมูลส่วนบุคคลโดยส่งเสริมให้มีความตระหนักด้านการใช้งานข้อมูลส่วนบุคคลภายในองค์กรและจัดเตรียมแผนการตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ในส่วนของการให้บริการด้าน Digital ID หากเป็นหน่วยงานผู้ให้บริการพิสูจน์และยืนยันตัวตน องค์กรจะมีการกำหนดขั้นตอนในการจัดการกระบวนการพิสูจน์ตัวตนและยืนยันตัวตนที่ชัดเจน มีการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนกับข้อกำหนดต่างๆ รวมถึงมีขั้นตอนการยกระดับความน่าเชื่อถือในการยืนยันตัวตนหากทางผู้ใช้บริการร้องขอ เช่นเดียวกับกรณีที่เป็นหน่วยงานที่ให้บริการบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล องค์กรจะจัดให้มีมาตรการในการควบคุมและปกป้องข้อมูลการพิสูจน์และยืนยันตัวตนอย่างปลอดภัย สามารถตรวจสอบกิจกรรมในการแลกเปลี่ยนได้ และมีการทดสอบระบบก่อนที่จะให้บริการกับผู้ใช้งานทุกครั้ง
พอใช้	องค์กรมีการกำหนดแผนในการป้องกันและจัดการการฉ้อโกงหรือการทุจริต ซึ่งมีเนื้อหาที่เกี่ยวข้องกับการบริหารจัดการบุคลากร วิธีการส่งเสริมและควบคุมไม่ให้เกิดการฉ้อโกงหรือทุจริต กลไกในติดตามและจัดการกับเหตุที่เกิดขึ้น รวมไปถึงขั้นตอนการให้ความช่วยเหลือผู้ใช้บริการ จากเหตุการณ์ทุจริตหรือฉ้อโกงภายในระบบ Digital ID ทั้งนี้เนื้อหาบางส่วนอาจยังไม่ครบถ้วนบ้าง แต่นโยบายและขั้นตอนการปฏิบัติดังกล่าวมีการประกาศใช้งานภายในองค์กร มีการกำหนดคณะกรรมการและคณะทำงานที่รับผิดชอบ รวมถึงมีการทบทวนอย่างเพียงพอ

	องค์กรมีการกำหนดนโยบายและขั้นตอนในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งมีเนื้อหาในส่วนของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจ ทั้งนี้เนื้อหาบางส่วนอาจยังไม่ครบถ้วนบ้าง แต่นโยบายและขั้นตอนการปฏิบัติดังกล่าวมีการประกาศใช้งานภายในองค์กร มีการกำหนดคณะกรรมการและคณะทำงานที่รับผิดชอบ รวมถึงมีการทบทวนอย่างเพียงพอ นอกจากนี้ยังมีคณะกรรมการและคณะทำงานที่ดูแลทางด้านข้อมูลส่วนบุคคล ส่งเสริมให้มีความตระหนักด้านการใช้งานข้อมูลส่วนบุคคลภายในองค์กรแต่อาจจะยังไม่ต่อเนื่องและจัดเตรียมแผนการตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแต่อาจจะยังไม่ได้มีการซักซ้อมหรือการประเมินคุณภาพของแผนการรับมือ ในส่วนของการให้บริการด้าน Digital ID หากเป็นหน่วยงานผู้ให้บริการพิสูจน์และยืนยันตัวตน องค์กรจะมีการกำหนดขั้นตอนในการจัดการกระบวนการพิสูจน์ตัวตนและยืนยันตัวตน แต่ขั้นตอนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนกับข้อกำหนดต่างๆ รวมถึงขั้นตอนการยกระดับความน่าเชื่อถือในการยืนยันตัวตนหากทางผู้ใช้บริการร้องขออาจจะไม่ครบถ้วน เช่นเดียวกับกรณีที่เป็นหน่วยงานที่ให้บริการบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล องค์กรจะจัดให้มีมาตรการในการควบคุมและปกป้องข้อมูลการพิสูจน์และยืนยันตัวตนอย่างปลอดภัย แต่อาจจะยังไม่ดำเนินการบางหัวข้อให้ครบถ้วน เช่น การจัดเก็บ Log หรือ การกำหนด Sharing policy สำหรับข้อมูลแต่ละประเภท
อ่อน	องค์กรอาจยังไม่มีการกำหนดแผนในการป้องกันและจัดการการฉ้อโกงหรือการทุจริต หรือมีการกำหนดแผนแล้วแต่มีเนื้อหาที่เกี่ยวข้องกับการบริการจัดการบุคลากร วิธีการส่งเสริมและควบคุมไม่ให้เกิดการฉ้อโกงหรือทุจริต กลไกในติดตามและจัดการกับเหตุที่เกิดขึ้น รวมไปถึงขั้นตอนการให้ความช่วยเหลือผู้ใช้บริการจากเหตุการณ์ทุจริตหรือฉ้อโกงภายในระบบ Digital ID ไม่ครบถ้วนเป็นส่วนมาก ซึ่งนโยบายและขั้นตอนการปฏิบัติดังกล่าวอยู่ระหว่างจัดทำและยังไม่มีการประกาศใช้งาน รวมไปถึงคณะกรรมการและคณะทำงานที่รับผิดชอบยังไม่ชัดเจน เพื่อมาควบคุมและประเมินผลแผนในการจัดการให้มีประสิทธิภาพที่เพียงพอ องค์กรอาจยังไม่มีการกำหนดนโยบายและขั้นตอนในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หรือมีการกำหนดแล้วแต่มีเนื้อหาในส่วนของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและ

	การบริหารความต่อเนื่องทางธุรกิจ ไม่ครบถ้วนเป็นส่วนมาก ซึ่งนโยบายและขั้นตอนการปฏิบัติดังกล่าวอยู่ระหว่างจัดทำและยังไม่มีการประ กาศใช้งาน รวมไปถึงคณะกรรมการและคณะทำงานที่รับผิดชอบยังไม่ชัดเจนเพื่อดูแลระบบและขั้นตอนการปฏิบัติงานเพื่อรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ นอกจากนี้คณะกรรมการและคณะทำงานที่ดูแลทางด้านข้อมูลส่วนบุคคลยังไม่ชัดเจน ยังไม่มีการส่งเสริมให้มีความตระหนักด้านการใช้งานข้อมูลส่วนบุคคลภายในองค์กรและจัดเตรียมแผนการตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ในส่วนของการให้บริการด้าน Digital ID หากเป็นหน่วยงานผู้ให้บริการพิสูจน์และยืนยันตัวตน องค์กรยังไม่มีการกำหนดขั้นตอนในการจัดการกระบวนการพิสูจน์ตัวตนและยืนยันตัวตนเป็นลายลักษณ์อักษร จะใช้การปฏิบัติงานตามที่เจ้าหน้าที่หน้างานดำเนินการเป็นประจำซึ่งมีความเสี่ยงสูงที่อาจให้เกิดการดำเนินงานที่บกพร่อง เช่นเดียวกับกรณีที่เป็นหน่วยงานที่ให้บริการบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล องค์กรยังไม่มีมาตรการในการควบคุมและปกป้องข้อมูลการพิสูจน์และยืนยันตัวตนอย่างปลอดภัยซึ่งอาจนำไปสู่การถูกโจมตีการผู้ไม่ประสงค์ดีหรือความบกพร่องต่อการดำเนินงานได้

3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk)	
ระดับความเสี่ยงตั้งต้น (Inherent risk)	
ต่ำ	องค์กรไม่มีการใช้งานเทคโนโลยีใหม่ๆ ที่ยังไม่มีมาตรฐานสากลยอมรับในการประมวลผลข้อมูลในระบบ Digital ID เช่น การประมวลผลด้วยปัญญาประดิษฐ์ (Artificial intelligence), การใช้แอปพลิเคชันของเทคโนโลยี IoT เป็นต้น ส่งผลให้ลดความเสี่ยงในการพบเจอเหตุการณ์ที่ไม่พึงประสงค์รูปแบบใหม่ที่ไม่เคยพบเจอมาก่อนได้ รวมถึงโครงสร้างในระบบไม่ได้มีความซับซ้อนมีการใช้งาน Protocol ที่เป็นมาตรฐานเดียวกันและดำเนินการแบบอัตโนมัติซึ่งช่วยให้การดำเนินการในระบบ Digital ID เป็นในรูปแบบมาตรฐานเดียวกัน ลดความเสี่ยงด้านการผิดพลาดได้ ระบบสารสนเทศที่สนับสนุนไม่ได้มีการใช้งาน Cloud computing โดยมี Data center ภายในและ Data center สำรองที่เป็นสถานที่ขององค์กรเองด้วย ระบบมีการทำ Redundancy ซึ่งมีประสิทธิภาพใช้งานทดแทนได้ทันที รวมถึงไม่ได้มีการให้บริการกับหน่วยงานภายนอกด้วยทำให้มีความเสี่ยงต่ำในการใช้งานระบบ ในส่วนของระบบเครือข่ายและการเข้าถึงระบบ Digital ID มีช่องทางเชื่อมต่ออินเทอร์เน็ตที่น้อย มีใช้งาน Protocol ที่ปลอดภัยทั้งหมด มีการแยกเครือข่ายระหว่างบุคคลภายนอกและพนักงานดูแลระบบที่ชัดเจน รวมถึงมีการเชื่อมต่อระหว่างหน่วยงานผ่าน Private link และใช้ VPN ทำให้การเข้าใช้งานระบบ Digital ID ผ่านระบบเครือข่ายมีความปลอดภัยสูง ในส่วนของการพัฒนาระบบ มีการใช้งานระบบที่พัฒนาปรับแต่งเอง รวมถึงจ้างหน่วยงานภายนอกพัฒนาในจำนวนไม่มาก ไม่มีระบบงานไหนที่ Operating system, Database, Software และ Hardware ที่ใช้งานอยู่ End of life หรือ End of support ภายในช่วงระยะเวลา 2 ปี และมีจำนวนอุปกรณ์ด้านเทคโนโลยีสารสนเทศไม่มากทำให้สามารถดูแลรักษาอุปกรณ์ด้านเทคโนโลยีสารสนเทศได้ครบถ้วน ระบบ Digital ID มีเครื่องมือในการติดตามการใช้งานทรัพยากรในระบบ รวมไปถึงการติดตามและตรวจสอบ Log มีการสำรองข้อมูลอย่างต่อเนื่องส่งผลให้ผู้ดูแลระบบสามารถรับมือกับความเสี่ยงและตอบสนองได้ทันท่วงที
ปานกลาง	องค์กรมีการใช้งานเทคโนโลยีใหม่ๆ ที่ยังไม่มีมาตรฐานสากลยอมรับในการประมวลผลข้อมูลในระบบ Digital ID (เช่น การประมวลผลด้วยปัญญาประดิษฐ์ (Artificial intelligence), การใช้แอปพลิเคชันของเทคโนโลยี IoT เป็นต้น) ทำให้มีความเสี่ยงในการพบเจอเหตุการณ์ที่ไม่พึงประสงค์รูปแบบใหม่ที่ไม่เคยพบเจอมาก่อนได้ รวมถึงโครงสร้างในระบบมีความซับซ้อนเล็กน้อย มีระบบบางส่วนที่ต้องเชื่อมโยงกันเพิ่มเติม ซึ่งทำให้การดำเนินการในระบบ Digital ID อาจเกิดความผิดพลาดได้หากไม่มีการควบคุมหรือพัฒนาระบบที่ดี

	ระบบสารสนเทศที่สนับสนุนมีการใช้งาน Cloud computing โดยมี Data center ภายในหรือ Data center สำรองเป็นลักษณะเช่าสถานที่หรือใช้บริการ Data center ภายนอกโดยแยกออกจากผู้ให้บริการรายอื่น ระบบมีการทำ Redundancy ซึ่งมีประสิทธิภาพใช้งานทดแทนได้ทันที แต่อาจมีระบบบางอย่างที่ยังไม่สามารถดำเนินการได้ ทำให้อาจเกิดความเสี่ยงเรื่องความต่อเนื่องในการใช้งานระบบได้ ในส่วนของระบบเครือข่ายและการเข้าถึงระบบ Digital ID มีช่องทางเชื่อมต่ออินเทอร์เน็ตจำนวนหนึ่ง อาจมีใช้งาน Protocol ที่ไม่ปลอดภัยทั้งหมด มีการแยกเครือข่ายระหว่างบุคคลภายนอกและพนักงานดูแลระบบ รวมถึงมีการเชื่อมต่อระหว่างหน่วยงานผ่าน Private link ทำให้การเข้าใช้งานระบบ Digital ID ผ่านระบบเครือข่ายมีความปลอดภัยแต่ยังมีความเสี่ยงเล็กน้อยบ้าง ในส่วนของการพัฒนาระบบ มีการใช้งานระบบที่พัฒนาปรับแต่งเอง รวมถึงจ้างหน่วยงานภายนอกพัฒนาบ้าง อาจมีระบบงานที่ Operating system, Database, Software และ Hardware ที่ใช้งานอยู่ End of life หรือ End of support ภายในช่วงระยะเวลา 2 ปี และมีจำนวนอุปกรณ์ด้านเทคโนโลยีสารสนเทศจำนวนหนึ่งซึ่งอาจมีความเสี่ยงได้ในอนาคตหากมีการดูแลควบคุมที่ไม่ดีพอ ระบบ Digital ID มีเครื่องมือในการติดตามการใช้งานทรัพยากรในระบบ เช่นเดียวกันกับการติดตามและตรวจสอบ Log แต่ระบบดังกล่าวยังไม่มีการแจ้งเตือนหากพบเจอเหตุการณ์ผิดปกติอัตโนมัติ มีการสำรองข้อมูลอยู่เป็นประจำแต่อาจจะยังไม่ต่อเนื่อง ส่งผลให้ผู้ดูแลระบบสามารถรับมือกับความเสี่ยงและตอบสนองได้ แต่อาจจะสามารถตอบสนองได้ทันที
สูง	องค์กรมีการใช้งานเทคโนโลยีใหม่ๆ ที่ยังไม่มีมาตรฐานสากลยอมรับในการประมวลผลข้อมูลในระบบ Digital ID (เช่น การประมวลผลด้วยปัญญาประดิษฐ์ (Artificial intelligence), การใช้แอปพลิเคชันของเทคโนโลยี IoT เป็นต้น) ทำให้มีความเสี่ยงในการพบเจอเหตุการณ์ที่ไม่พึงประสงค์รูปแบบใหม่ที่ไม่เคยพบเจอมาก่อนได้ รวมถึงโครงสร้างในระบบมีความซับซ้อนมาก มีระบบหลายส่วนที่ ต้องมีการดึงข้อมูลออกมาเชื่อมโยงกันหลายครั้ง ซึ่งทำให้การดำเนินการในระบบ Digital ID อาจเกิดความผิดพลาดได้สูงหากไม่มีการควบคุมหรือพัฒนาระบบที่ดี ระบบสารสนเทศที่สนับสนุนมีการใช้งาน Cloud computing โดยมี Data center ภายในหรือ Data center สำรองเป็นลักษณะเช่าสถานที่หรือใช้บริการ Data center ภายนอกแต่ไม่ได้แยกกับผู้ใช้บริการอื่นๆ ระบบมีการทำ Redundancy ซึ่งมีประสิทธิภาพใช้งานทดแทนได้ทันที แต่อาจมีระบบหลายส่วนที่ยังไม่สามารถดำเนินการได้ ทำให้อาจเกิดความเสี่ยงเรื่องความต่อเนื่องในการใช้งานระบบสูง ในส่วนของระบบเครือข่ายและการเข้าถึงระบบ Digital ID มีช่องทางเชื่อมต่ออินเทอร์เน็ตจำนวนมากและอาจมีใช้งาน Protocol ที่ไม่ปลอดภัยรวมอยู่ด้วย ยังไม่มีการแยกเครือข่ายระหว่างบุคคลภายนอกและพนักงานดูแลระบบ รวมถึงมีการเชื่อมต่อระหว่างหน่วยงานผ่าน Public internet ทำให้การเข้าใช้งานระบบ Digital ID ผ่านระบบเครือข่ายมีความเสี่ยงสูง

	ในส่วนของการพัฒนาระบบ มีการใช้งานระบบที่พัฒนาปรับแต่งเอง รวมถึงจ้างหน่วยงานภายนอกพัฒนาอยู่จำนวนมาก โดยอาจมีระบบงานที่ Operating system, Database, Software และ Hardware ที่ใช้งานอยู่ End of life หรือ End of support ในปัจจุบัน รวมทั้งมีจำนวนอุปกรณ์ด้านเทคโนโลยีสารสนเทศจำนวนมากทำให้อาจมีความเสี่ยงสูงได้ในอนาคตเนื่องจากการดูแลรักษาระบบค่อนข้างยาก ระบบ Digital ID ไม่มีเครื่องมือในการติดตามการใช้งานทรัพยากรในระบบ เช่นเดียวกันการติดตาม Log ที่ไม่มีเครื่องมือในการติดตามไม่มีการสำรองข้อมูลหรือสำรองข้อมูลบางครั้ง ส่งผลให้ผู้ดูแลระบบไม่สามารถรับมือกับความเสี่ยงและตอบสนองได้ทันท่วงที มีความเสี่ยงสูงที่ระบบ Digital ID จะหยุดชะงักได้
ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	
ดี	องค์กรมีกระบวนการและเทคโนโลยีต่างๆ เข้ามาช่วยในการรักษาความมั่นคงปลอดภัยภายในระบบ Digital ID ซึ่งช่วยให้การควบคุมการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจเป็นไปอย่างมีประสิทธิภาพ ช่วยลดความเสี่ยงที่เกิดขึ้นจาก ภัยคุกคามทางไซเบอร์ การรั่วไหลของข้อมูล รวมถึงข้อมูลอ่อนไหวซึ่งมักเป็นองค์ประกอบสำคัญในบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล นอกจากนั้นองค์กรยังดำเนินการบริหารจัดการช่องโหว่ภายในระบบ Digital ID อย่างมีประสิทธิภาพ มีการบริหารจัดการการติดตั้งโปรแกรมสำหรับแก้ไขข้อบกพร่อง (Patch management) โดยมีกระบวนการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง ดำเนินการบริหารจัดการช่องโหว่ของระบบ (Vulnerability management) และจัดให้มีทดสอบการเจาะระบบ (Penetration test) ในระบบ Digital ID โดยผู้เชี่ยวชาญที่เหมาะสม และดำเนินการต่อเนื่องเป็นประจำ
พอใช้	องค์กรมีกระบวนการและเทคโนโลยีต่างๆ เข้ามาช่วยในการรักษาความมั่นคงปลอดภัยภายในระบบ Digital ID ทั้งนี้กระบวนการและเทคโนโลยีดังกล่าวสามารถควบคุมการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ และการจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจได้อย่างเพียงพอ ทำให้สามารถควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับบริการ

	พิสูจน์และยืนยันตัวตนทางดิจิทัลได้ แต่ยังสามารถเพิ่มประสิทธิภาพในการควบคุมให้ดียิ่งขึ้นเพื่อให้สามารถรับมือกับการเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์ นอกจากนั้นองค์กรยังดำเนินการบริหารจัดการช่องโหว่ภายในระบบ Digital ID ทั้งในส่วนของการบริหารจัดการการติดตั้งโปรแกรมสำหรับแก้ไขข้อบกพร่อง (Patch management) โดยมีกระบวนการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง การดำเนินการบริหารจัดการช่องโหว่ของระบบ (Vulnerability management) หรือการจัดให้มีทดสอบการเจาะระบบ (Penetration test) ในระบบ Digital ID โดยผู้เชี่ยวชาญที่เหมาะสม ทั้งนี้ในภาพรวมองค์กรมีการควบคุมเรื่องช่องโหว่ภายในระบบ Digital ID แล้วแต่อาจยังพบเจอช่องโหว่ที่มีระดับผลกระทบสูงบางส่วนที่ยังไม่สามารถแก้ไขได้
อ่อน	องค์กรยังไม่มีกระบวนการและเทคโนโลยีต่างๆ ในการรักษาความมั่นคงปลอดภัยภายในระบบ Digital ID ที่สามารถควบคุมการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ และการจัดการ แผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจได้ครบถ้วน ส่งผลให้องค์กรมีความเสี่ยงด้านเทคโนโลยีสารสนเทศภายในระบบ Digital ID และอาจเกิดผลกระทบเมื่อมีภัยคุกคามทางไซเบอร์โจมตีระบบ Digital ID ขององค์กรได้ นอกจากนั้นองค์กรยังไม่มีการดำเนินการบริหารจัดการช่องโหว่ภายในระบบ Digital ID ที่ครบถ้วน โดยอาจจะบกพร่องทั้งในส่วนของการบริหารจัดการการติดตั้งโปรแกรมสำหรับแก้ไขข้อบกพร่อง (Patch management) การดำเนินการบริหารจัดการช่องโหว่ของระบบ (Vulnerability management) หรือการจัดให้มีทดสอบการเจาะระบบ (Penetration test) ในระบบ Digital ID ทั้งนี้ในภาพรวมองค์กรอาจทำให้พบเจอช่องโหว่ที่มีระดับผลกระทบสูงจำนวนมาก โดยที่ยังไม่สามารถระบุช่องโหว่ดังกล่าวหรือไม่สามารถแก้ไขได้

4. ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation risk)	
ระดับความเสี่ยงตั้งต้น (Inherent risk)	
ต่ำ	องค์กรพบการร้องเรียนหรือแจ้งปัญหาในการใช้งานระบบบริการ Digital ID จากผู้ใช้บริการ รวมถึงหน่วยงานที่เชื่อมต่อเพื่อใช้บริการในจำนวนน้อย รวมถึงองค์กรยังไม่มีเหตุการณ์การทุจริต เหตุการณ์ที่เกิดจากความผิดพลาดของบุคลากร หรือเหตุการณ์ที่ไม่พึงประสงค์อื่นๆ ที่ส่งผลกระทบในวงกว้างและมีนัยสำคัญต่อความน่าเชื่อถือขององค์กร พบการร้องเรียนหรือแจ้งปัญหาในการใช้งานระบบบริการ Digital ID จากผู้ใช้บริการ รวมถึงหน่วยงานที่เชื่อมต่อเพื่อใช้บริการในจำนวนน้อย จำนวนผู้ใช้บริการและจำนวนผู้ให้บริการ Digital ID ยังมีจำนวนไม่มาก ส่งผลให้รายการธุรกรรมการยืนยันตัวตนบนระบบบริการ Digital ID ยังมีจำนวนน้อย ข้อมูลที่ใช้ในการพิสูจน์ตัวตนที่ใช้งานในระบบ Digital ID มีความเสี่ยงและผลกระทบต่อเจ้าของข้อมูลน้อย ซึ่งหากเกิดเหตุการณ์อันไม่พึงประสงค์ต่อการให้บริการพิสูจน์และยืนยันตัวตน อาจไม่ส่งผลกระทบมากต่อชื่อเสียงขององค์กร
ปานกลาง	พบการร้องเรียนหรือแจ้งปัญหาในการใช้งานระบบบริการ Digital ID จากผู้ใช้บริการ รวมถึงหน่วยงานที่เชื่อมต่อเพื่อใช้บริการบ้าง แต่ยังไม่มีการร้องเรียนจำนวนมาก รวมถึงองค์กรพบเจอเหตุการณ์การทุจริต เหตุการณ์ที่เกิดจากความผิดพลาดของบุคลากร หรือเหตุการณ์ที่ไม่พึงประสงค์อื่นๆ ที่ส่งผลกระทบในวงกว้างและมีนัยสำคัญต่อความน่าเชื่อถือขององค์กรอยู่บ้าง และพบการร้องเรียนหรือแจ้งปัญหาในการใช้งานระบบบริการ Digital ID จากผู้ใช้บริการ รวมถึงหน่วยงานที่เชื่อมต่อเพื่อใช้บริการในจำนวนหนึ่ง ทั้งนี้ จำนวนผู้ใช้บริการและจำนวนผู้ให้บริการ Digital ID ยังมีจำนวนปานกลาง ส่งผลให้รายการธุรกรรมการยืนยันตัวตนบนระบบบริการ Digital ID มีอยู่พอประมาณ ข้อมูลที่ใช้ในการพิสูจน์ตัวตนที่ใช้งานในระบบ Digital ID มีความเสี่ยงและผลกระทบต่อเจ้าของข้อมูลในระดับปานกลาง ซึ่งหากเกิดเหตุการณ์อันไม่พึงประสงค์ต่อการให้บริการพิสูจน์และยืนยันตัวตน อาจส่งผลกระทบเล็กน้อยต่อชื่อเสียงขององค์กร

สูง	พบการร้องเรียนหรือแจ้งปัญหาในการใช้งานระบบบริการ Digital ID จากผู้ใช้บริการ รวมถึงหน่วยงานที่เชื่อมต่อเพื่อใช้บริการจำนวนมาก รวมถึงองค์กรพบเจอเหตุการณ์การทุจริต เหตุการณ์ที่เกิดจากความผิดพลาดของบุคลากร หรือเหตุการณ์ที่ไม่พึงประสงค์อื่นๆ ที่ส่งผลกระทบในวงกว้างและมีนัยสำคัญต่อความน่าเชื่อถือขององค์กรจำนวนมาก และพบการร้องเรียนหรือแจ้งปัญหาในการใช้งานระบบบริการ Digital ID จากผู้ใช้บริการรวมถึงหน่วยงานที่เชื่อมต่อเพื่อใช้บริการในจำนวนมากเช่นกัน ทั้งนี้ จำนวนผู้ใช้บริการและจำนวนผู้ให้บริการ Digital ID มีจำนวนสูง ส่งผลให้รายการธุรกรรมการยืนยันตัวตนบนระบบบริการ Digital ID มีอยู่จำนวนมาก ข้อมูลที่ใช้ในการพิสูจน์ตัวตนที่ใช้งานในระบบ Digital ID มีความเสี่ยงและผลกระทบต่อเจ้าของข้อมูลในระดับสูง ซึ่งหากเกิดเหตุการณ์อันไม่พึงประสงค์ต่อการให้บริการพิสูจน์และยืนยันตัวตน อาจส่งผลกระทบเป็นอย่างมากต่อชื่อเสียงขององค์กร
ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	
ดี	องค์กรมีการแจ้งรายละเอียดเกี่ยวกับข้อกำหนดการให้บริการที่เกี่ยวข้องกับการให้บริการ พิสูจน์และยืนยันตัวตนหรือการแลกเปลี่ยนข้อมูลการพิสูจน์และยืนยันตัวตนอย่างครบถ้วน โดยมีการแจ้งเกี่ยวกับข้อมูลโดยทั่วไปของผู้ให้บริการ, วิธีการจัดเก็บและรวบรวมข้อมูล, การรักษาความปลอดภัยและความลับของข้อมูล, ช่องทางการติดต่อสื่อสาร, สิทธิที่ผู้ใช้บริการสามารถปฏิบัติได้ รวมไปถึงข้อกำหนดจากกฎหมายหรือข้อกำหนดอื่นๆ ที่จะมีผลกระทบต่อผู้ใช้บริการ ทั้งนี้ข้อกำหนดการต่างๆ มีการทบทวนอยู่เป็นประจำ นอกจากนี้มีช่องทางรับเรื่องร้องเรียนหรือแจ้งเหตุที่ไม่พึงประสงค์จากผู้ใช้บริการ และมีกระบวนการให้ความช่วยเหลือผู้ใช้บริการจากเหตุการณ์ที่ไม่พึงประสงค์อย่างครบถ้วน ทั้งนี้กระบวนการรับมือต่อเหตุร้องเรียนหรือแจ้งเหตุที่ไม่พึงประสงค์มีการพัฒนาปรับปรุงอย่างสม่ำเสมอ ทำให้กระบวนการดังกล่าวมีประสิทธิภาพที่ดี ส่งผลให้สามารถรับมือจากข้อร้องเรียนหรือเหตุการณ์ไม่พึงประสงค์ได้อย่างทันท่วงที และไม่ส่งผลกระทบต่อชื่อเสียงในการดำเนินงานพิสูจน์และยืนยันตัวตนขององค์กร

พอใช้	องค์กรมีการแจ้งรายละเอียดเกี่ยวกับข้อกำหนดการให้บริการที่เกี่ยวข้องกับการให้บริการ พิสูจน์และยืนยันตัวตนหรือการแลกเปลี่ยนข้อมูลการพิสูจน์และยืนยันตัวตน โดยมีการแจ้งเกี่ยวกับข้อมูลโดยทั่วไปของผู้ให้บริการ, วิธีการจัดเก็บและรวบรวมข้อมูล, การรักษาความปลอดภัยและความลับของข้อมูล, ช่องทางการติดต่อสื่อสาร, สิทธิที่ผู้ใช้บริการสามารถปฏิบัติได้ รวมไปถึงข้อกำหนดจากกฎหมายหรือข้อกำหนดอื่นๆ ที่จะมีผลกระทบต่อผู้ใช้บริการ นอกจากนี้มีช่องทางรับเรื่องร้องเรียนหรือแจ้งเหตุที่ไม่พึงประสงค์จากผู้ใช้บริการ และมีกระบวนการให้ความช่วยเหลือผู้ใช้บริการจากเหตุการณ์ที่ไม่พึงประสงค์แต่กระบวนการดังกล่าวยังไม่ได้มีการปรับปรุงให้มีประสิทธิภาพที่ดียิ่งขึ้น ส่งผลให้สามารถรับมือจากข้อร้องเรียนหรือเหตุการณ์ไม่พึงประสงค์ได้ในระดับหนึ่ง อาจส่งผลกระทบเล็กน้อยต่อชื่อเสียงในการดำเนินงานพิสูจน์และยืนยันตัวตนขององค์กร
อ่อน	องค์กรมีการแจ้งรายละเอียดเกี่ยวกับข้อกำหนดการให้บริการที่เกี่ยวข้องกับการให้บริการ พิสูจน์และยืนยันตัวตนหรือการแลกเปลี่ยนข้อมูลการพิสูจน์และยืนยันตัวตนไม่ครบถ้วนหรือยังไม่มีข้อกำหนดการให้บริการ ทำให้ผู้ใช้บริการไม่มีช่องทางการติดต่อสื่อสารหรือทำความเข้าใจถึงสิทธิที่ผู้ใช้บริการสามารถปฏิบัติได้ รวมไปถึงข้อกำหนดจากกฎหมายหรือข้อกำหนดอื่นๆ ที่จะมีผลกระทบต่อผู้ใช้บริการ นอกจากนี้ยังไม่มีช่องทางรับเรื่องร้องเรียนหรือแจ้งเหตุที่ไม่พึงประสงค์จากผู้ใช้บริการ หรือไม่มีกระบวนการให้ความช่วยเหลือผู้ใช้บริการจากเหตุการณ์ที่ไม่พึงประสงค์ ส่งผลให้ไม่สามารถรับมือจากข้อร้องเรียนหรือเหตุการณ์ไม่พึงประสงค์ได้และอาจส่งผลกระทบอย่างมากต่อชื่อเสียงในการดำเนินงานพิสูจน์และยืนยันตัวตนขององค์กร

5. ความเสี่ยงทางด้านการปฏิบัติตามหลักเกณฑ์ (Compliance risk)	
ระดับความเสี่ยงตั้งต้น (Inherent risk)	
ต่ำ	องค์กรมีการทำสัญญาหรือข้อตกลงกับบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID ทั้งหมด โดยเนื้อหาสัญญาระบุขอบเขตการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก, หน้าที่และความรับผิดชอบของบุคคลภายนอก, เงื่อนไขหรือสิทธิในการขอเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาและความรับผิดต่อความเสียหาย โดยมีการกำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID ทั้งหมดอย่างต่อเนื่อง มีการประเมินประสิทธิภาพทั้งในด้านการรักษาความมั่นคงปลอดภัยและการปฏิบัติตามกฎหมาย ทั้งนี้จำนวนบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID มีจำนวนไม่เยอะมาก ทั้งนี้ องค์กรจัดให้มีการตรวจสอบโดยผู้ตรวจสอบที่มีความเป็นอิสระ เพื่อตรวจสอบการดำเนินงานว่าเป็นไปตามมาตรฐานของบริษัท ประกาศจากหน่วยงานกำกับ รวมไปถึงมาตรฐานสากลที่เกี่ยวข้อง รวมถึงมีการแก้ไขติดตามปัญหาที่เป็นประเด็นจากการตรวจสอบอย่างต่อเนื่องและจัดทำแผนการป้องกันการเกิดเหตุซ้ำเพื่อทำให้มั่นใจได้ว่ามีการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างมีประสิทธิภาพ
ปานกลาง	องค์กรมีการทำสัญญาหรือข้อตกลงกับบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID ทั้งหมด แต่เนื้อหาสัญญายังไม่ครบถ้วน โดยมีการกำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID ทั้งหมดอย่างต่อเนื่อง แต่ขาดการประเมินประสิทธิภาพทั้งในด้านการรักษาความมั่นคงปลอดภัยและการปฏิบัติตามกฎหมาย ทั้งนี้จำนวนบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID มีจำนวนพอประมาณ ทั้งนี้ องค์กรจัดให้มีการตรวจสอบโดยผู้ตรวจสอบที่มีความเป็นอิสระ เพื่อตรวจสอบการดำเนินงานว่าเป็นไปตามมาตรฐานของบริษัท ประกาศจากหน่วยงานกำกับ รวมไปถึงมาตรฐานสากลที่เกี่ยวข้อง รวมถึงมีการแก้ไขติดตามปัญหาที่เป็นประเด็นจากการตรวจสอบอย่างต่อเนื่ อง ทำให้มีการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเพียงพอ

สูง	องค์กรมีการทำสัญญากับบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID เพียงบางส่วน และมีบุคคลภายนอกบางส่วนที่ไม่มีการทำสัญญาด้วย รวมถึงยังมีการกำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID แค่บางส่วนเท่านั้น ทำให้อาจมีบางโครงการไม่มีการติดตามผลการปฏิบัติงานของบุคคลภายนอก ทั้งนี้ จำนวนบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID อาจมีจำนวนมาก ซึ่งทำให้ควบคุมการดำเนินงานจากบุคคลภายนอกได้ยาก ทั้งนี้ องค์กรยังไม่มีการตรวจสอบโดยผู้ตรวจสอบที่มีความเป็นอิสระอย่างครบถ้วน ทำให้ไม่สามารถตรวจสอบประสิทธิภาพในการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องได้ ส่งผลกระทบต่อความไม่สอดคล้องต่อกฎหมายและกฎระเบียบ
ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	
ดี	องค์กรมีการศึกษาผลกระทบต่อบริษัทในการดำเนินการตามกฎหมายหรือกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตน ไม่ว่าจะเป็นกฎระเบียบด้านเทคโนโลยีสารสนเทศ, กฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล หรือกฎระเบียบอื่นๆ จากหน่วยงานกำกับที่เกี่ยวข้อง รวมถึงมีกระบวนการทบทวนกฎระเบียบและนโยบายบริษัทให้สอดคล้องกับกฎหมายและกฎระเบียบต่างๆ และสื่อสารให้พนักงานรู้และเข้าใจในการเปลี่ยนแปลงของนโยบายต่างๆ โดยมีการวัดผลเพื่อให้มั่นใจได้ว่าการสื่อสารเป็นไปอย่างมีประสิทธิภาพ รวมไปถึงมีการตรวจสอบการปฏิบัติตามกฎหมายและกฎเกณฑ์ โดยผู้ตรวจสอบที่มีความเป็นอิสระและมีความสามารถ ซึ่งครอบคลุมไปถึงระบบและการให้บริการด้านพิสูจน์และยืนยันตัวตน มีกระบวนการในการติดตามและปรับปรุงประเด็นที่ได้จากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างมีประสิทธิภาพ รายงานผลต่อผู้บริหารถึงผลการตรวจสอบทั้งหมดอย่างสม่ำเสมอ

พอใช้	องค์กรมีการศึกษาผลกระทบต่อบริษัทในการดำเนินการตามกฎหมายหรือกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตน แต่อาจจะไม่ครบถ้วนในทุกด้าน ซึ่งประกอบด้วยกฎระเบียบด้านเทคโนโลยีสารสนเทศ, กฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล หรือกฎระเบียบอื่นๆ จากหน่วยงานกำกับที่เกี่ยวข้อง รวมถึงมีกระบวนการทบทวนกฎระเบียบและนโยบายบริษัทให้สอดคล้องกับกฎหมายและกฎระเบียบต่างๆ แต่อาจจะยังขาดการสื่อสารหรือให้ความรู้กับพนักงานที่เกี่ยวข้องเพื่อให้เข้าใจถึงกฎหมายและกฎระเบียบต่างๆ ที่มีการเปลี่ยนแปลง รวมไปถึงมีการตรวจสอบการปฏิบัติตามกฎหมายและกฎเกณฑ์ โดยผู้ตรวจสอบที่มีความเป็นอิสระและมีความสามารถ แต่ยังไม่ครอบคลุมทุกระบบและการให้บริการด้านพิสูจน์และยืนยันตัวตน ทั้งนี้ องค์กรมีกระบวนการในการติดตามและปรับปรุงประเด็นที่ได้จากการตรวจสอบเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยง รายงานผลต่อผู้บริหารถึงผลการตรวจสอบทั้งหมดแต่ไม่ได้สม่ำเสมอ
อ่อน	องค์กรไม่มีการศึกษาผลกระทบต่อบริษัทในการดำเนินการตามกฎหมายหรือกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตน รวมถึงไม่มีกระบวนการทบทวนกฎระเบียบและนโยบายบริษัทให้สอดคล้องกับกฎหมายและกฎระเบียบต่างๆ ส่งผลให้นโยบายและแนวทางปฏิบัติขององค์ไม่สอดคล้องกับกฎหมายหรือกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตน และพนักงานไม่สามารถปฏิบัติงานได้ถูกต้องตามกฎหมาย อีกทั้ง องค์กรไม่มีการตรวจสอบการปฏิบัติตามกฎหมายและกฎเกณฑ์ โดยผู้ตรวจสอบที่มีความเป็นอิสระและมีความสามารถ หรือมีการตรวจสอบแต่ไม่มีการติดตามและปรับปรุงประเด็นที่ได้จากการตรวจสอบเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยง ส่งผลให้องค์กรไม่สามารถระบุประเด็นที่ควรจะต้องแก้ไขหรือพัฒนาให้ดียิ่งขึ้นเพื่อให้สอดคล้องกับกับกฎหมายและกฎเกณฑ์ต่างๆ

4.3 การประเมินความเสี่ยงตั้งต้นและความสามารถในการบริหารจัดการความเสี่ยง (Assess inherent risk and risk management capability)

สำหรับกรอบในการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องหรือมีผลกระทบต่อความปลอดภัย ความน่าเชื่อถือของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลนี้ได้แบ่งการประเมินออกเป็น 2 ส่วนประกอบไปด้วยความเสี่ยงตั้งต้น (Inherent risk) และความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) ซึ่งผลลัพธ์จากการประเมินทั้ง 2 ส่วนจะสามารถระบุถึงความเสี่ยงสุทธิ (Net risk) ได้ โดยความเสี่ยงสุทธิที่ได้จะมีผลลัพธ์ออกมาเป็น 2 แบบ

1. **ความเสี่ยงสุทธิแบ่งแยกตามประเภทความเสี่ยง (Net risk by risk factor)** ได้มาจากการประเมินความเสี่ยงตั้งต้น (Inherent risk) ตามประเภทความเสี่ยงแต่ละด้าน มาจับคู่กับความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) ตามประเภทความเสี่ยงแต่ละด้าน โดยผลลัพธ์ที่ได้คือความเสี่ยงสุทธิ (Net risk) ที่แบ่งแยกตามประเภทของความเสี่ยง ทั้ง 5 ด้าน ซึ่งสามารถนำผลลัพธ์นี้เข้ากระบวนการตอบสนองความเสี่ยงเพื่อวิเคราะห์ว่าปัจจัยความเสี่ยงใดมีผลกระทบต่อองค์กรมากที่สุด รวมถึงใช้ในการติดตามและรายงานผลความเสี่ยงได้
2. **ความเสี่ยงสุทธิขององค์กร (Overall net risk)** ได้มาจากการประเมินความเสี่ยงตั้งต้น (Inherent risk) ขององค์กร มาจับคู่กับความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) ขององค์กร โดยผลความเสี่ยงสุทธินี้สามารถสะท้อนให้เห็นถึงความเสี่ยงสุทธิ (Net risk) ในภาพรวมขององค์กร

ซึ่งขั้นตอนการได้มาซึ่งความเสี่ยงสุทธิ (Net risk) ทั้ง 2 แบบ จะมีตัวอย่างอธิบายอย่างละเอียดในหัวข้อ 4.5 ทั้งนี้ก่อนจะไปดูถึงตัวอย่างการประเมิน รูปแบบในการประเมินและรายละเอียดการประเมินความเสี่ยงตั้งต้นและความสามารถในการบริหารจัดการความเสี่ยงมีรูปแบบดังต่อไปนี้

<u>ความเสี่ยงตั้งต้น (Inherent risk)</u>

Inherent Risk Factors					
Strategic	Operational	Technology	Reputation	Compliance	Total of IR

เป็นความเสี่ยงที่มีอยู่ขององค์กรผู้ให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะต้องพบเจอ ทั้งนี้อ อาจก่อให้เกิดความสูญเสียจากปัจจัยภายในและภายนอกต่างๆ โดยจะเน้นไปที่ปัจจัยความเสี่ยง ทั้ง 5 ด้านตามที่ระบุไว้ในหัวข้อที่ 4.2 การระบุประเภทความเสี่ยง (Identify risk factor) ซึ่งประกอบไปด้วย ความเสี่ยงด้านกลยุทธ์ (Strategic risk), ความเสี่ยงด้านการปฏิบัติงาน (Operational risk), ความเสี่ยงด้านเทคโนโลยีที่นำมาใช้ (Technology risk), ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation risk) และความเสี่ยงทางด้านกฎหมายและกฎระเบียบ (Compliance risk)

โดยในการประเมินในส่วนนี้จะใช้ในรูปแบบการประเมินตนเอง (Self-assessment) ที่สอบถามถึงสภาพแวดล้อมการดำเนินงานขององค์กรในด้านการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยอ้างอิงจากหลักฐานที่ดำเนินการจริงขององค์กรซึ่งจะสะท้อนให้เห็นถึงโอกาสการเกิดหรือผลกระทบที่อาจจะเกิดเหตุการณ์ความเสี่ยงได้ในอนาคต ทั้งนี้ ได้แบ่งผลการประเมินออกเป็น 3 ระดับนั้นคือ ต่ำ ปานกลาง และสูง ซึ่งมีรายละเอียดของเกณฑ์จะระบุเพิ่มเติมใน “หัวข้อที่ 4.4 กำหนดเกณฑ์การประเมินความเสี่ยง (Define risk criteria)” โดยองค์กรสามารถนำข้อมูลหลักฐานการดำเนินการตามคอลัมน์ “หลักฐานอ้างอิง” ประกอบการพิจารณาเลือกผลการประเมิน รวมถึงได้แบ่งการประเมินในบางหัวข้อเพื่อระบุความเสี่ยงเฉพาะด้าน โดยมีการแบ่งคำถามระหว่าง “หน่วยงานที่เปิดให้บริการด้าน Digital ID แล้ว” กับ “หน่วยงานที่ยังไม่เปิดให้บริการด้าน Digital ID” และมีคำถามเฉพาะแบ่งตามรูปแบบการให้บริการของหน่วยงานที่ประเมิน ซึ่งหน่วยงานที่ให้บริการในแต่ละรูปแบบจะมีจำนวนข้อที่ต้องประเมินดังต่อไปนี้

ผู้ประเมิน	รายละเอียดผู้ประเมิน	จำนวนข้อ
ALL	ทุกหน่วยงานจำเป็นต้องตอบคำถามดังกล่าว ทั้งในส่วนของ 1. ผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider Service) 2. ผู้ให้บริการบริการการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service)	61 ข้อ
AUTHM	ในกรณีเป็นผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider Service) ที่ให้บริการจัดการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Management) จำเป็นต้องตอบคำถามดังกล่าวทั้งหมด	61 ข้อ
AUTH	ในกรณีเป็นผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider Service) ที่ให้บริการยืนยันตัวตน (Authentication Service) จำเป็นต้องตอบคำถามดังกล่าวทั้งหมด	64 ข้อ (มีเพิ่มเติม 3 ข้อ)
IDPRF	ในกรณีเป็นผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider Service) ที่ให้บริการพิสูจน์ตัวตน (Identity Proofing) จำเป็นต้องตอบคำถามดังกล่าวทั้งหมด	63 ข้อ (มีเพิ่มเติม 2 ข้อ)

DIPS	ในกรณีเป็นผู้ให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service) จำเป็นต้องตอบคำถามดังกล่าวทั้งหมด	63 ข้อ (มีเพิ่มเติม 2 ข้อ)

<u>เป้าหมายในการประเมิน</u>

1. เข้าใจสภาพแวดล้อมในการให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมถึงผลกระทบต่อระดับความเสี่ยงซึ่งเป็นผลจากสภาพแวดล้อมดังกล่าว
2. เข้าใจปัจจัยที่ก่อให้เกิดความเสี่ยงต่อองค์กร
3. เข้าใจเป้าหมายขององค์กร ลักษณะการดำเนินการ รวมถึงโครงสร้างพื้นฐานระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนการให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัล

คำถามในแบบสอบถามประเมินตนเอง (Self-assessment) เพื่อให้สามารถสะท้อนให้เห็นถึงความเสี่ยงในการดำเนินธุรกิจขององค์กรในด้านการพิสูจน์และยืนยันตัวตนทางดิจิทัล จึงได้มีการระบุหัวข้อความเสี่ยงที่เกี่ยวข้องกับคำถามดังกล่าว เพื่อที่จะสามารถระบุได้ว่าคำถามในแต่ละข้อต้องการจะสอบถามถึงเรื่องความเสี่ยงในด้านอะไร รวมถึงสามารถจัดกลุ่มเชื่อมโยงไปยังประเภทความเสี่ยงได้ตามตารางในด้านล่าง

#	หัวข้อความเสี่ยง	ประเภทความเสี่ยง				
		Strategic	Operational	Technology	Reputation	Compliance
1	Audit Quality		x	x		x
2	Authenticator Threats		x		x	
3	Business Competition	x				
4	Business Continuity		x	x		
5	Capacity Monitoring			x		
6	Customer Perception				x	
7	Cyber Attack Surface			x		
8	Data Center Security			x		
9	Enrollment Threats		x		x	
10	Event Monitoring			x		

#	หัวข้อความเสี่ยง	ประเภทความเสี่ยง				
		Strategic	Operational	Technology	Reputation	Compliance
11	External Fraud		x			
12	Human Resource Security		x			
13	Identify Exchange Threats		x		x	
14	Identity Proofing		x	x	x	
15	Information Backup			x		
16	Information Security Policies		x	x		x
17	Initiative and Innovation	x	x	x	x	x
18	Insecure Protocol			x		
19	IT Access Management		x			
20	IT Risk Management		x	x		
21	Law and Regulations	x	x			
22	Mergers, Acquisitions, Divestitures	x	x	x	x	
23	Operational Error		x			x
24	Privacy & Data Protection		x	x	x	x
25	Regulatory compliance					x
26	Reputation				x	

#	หัวข้อความเสี่ยง	ประเภทความเสี่ยง				
		Strategic	Operational	Technology	Reputation	Compliance
27	Revenue & Capital Management	x				
28	Risk Management	x				
29	Security Incident		x	x		
30	Software Development			x		
31	Strategic Planning	x				
32	System Architecture			x		
33	Technical Vulnerability Management		x	x		
34	Third Party Management		x	x		x

ทั้งนี้ ผู้ประเมินสามารถดำเนินการประเมินโดยใช้ชุดคำถามและรายละเอียดตามภาคผนวก ก.

ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)

Risk management capability					
Strategic	Operational	Technology	Reputation	Compliance	Total of RMC

เป็นความสามารถในการบริหารจัดการความเสี่ยงที่ผู้ให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีอยู่ ควบคุมความเสี่ยงในด้านต่างๆ ให้อยู่ในระดับที่องค์กรสามารถยอมรับได้ โดยทั้งนี้จะเน้นไปที่ประเภทความเสี่ยงทั้ง 5 ด้านตามที่ระบุไว้ในหัวข้อที่ 4.2 การระบุประเภทความเสี่ยง (Identify risk factor) ซึ่งประกอบไปด้วย ความเสี่ยงด้านกลยุทธ์ (Strategic risk), ความเสี่ยงด้านการปฏิบัติงาน (Operational risk), ความเสี่ยงด้านเทคโนโลยีที่นำมาใช้ (Technology risk), ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation risk) และความเสี่ยงทางด้านกฎหมายและกฎระเบียบ (Compliance risk)

โดยในการประเมินในส่วนนี้จะใช้รูปแบบการตรวจประเมินโดยผู้ตรวจสอบอิสระ (Internal/External auditor) โดยตรวจสอบการควบคุมตามข้อกำหนดที่ระบุในหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ทั้งนี้ทาง สพธอ. มีเอกสารคู่มือในการตรวจสอบอ้างอิงการตรวจสำหรับหลักเกณฑ์ทั้ง 10 หัวข้อ ซึ่งมีรายละเอียด วิธีการและกระบวนการตรวจสอบตามหลักเกณฑ์ดังกล่าว ประกอบไปด้วยหัวข้อดังต่อไปนี้

1. หลักเกณฑ์เกี่ยวกับข้อตกลงการให้บริการ
2. หลักเกณฑ์เกี่ยวกับการออกแบบการใช้งานระบบ
3. หลักเกณฑ์การทดสอบด้านเทคนิคของระบบและซอฟต์แวร์ที่เกี่ยวข้อง
4. หลักเกณฑ์ด้านการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
5. หลักเกณฑ์ด้านการรักษาความมั่นคงปลอดภัยของระบบการให้บริการสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต
6. หลักเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคล
7. หลักเกณฑ์ด้านการตรวจประเมินระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
8. หลักเกณฑ์การตรวจประเมินระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลประจำปี
9. หลักเกณฑ์สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล
10. หลักเกณฑ์สำหรับการให้บริการการพิสูจน์ตัวตนบริการการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการการยืนยันตัวตน

ทั้งนี้รายละเอียดการควบคุมแต่ละข้อจะมีระบุประเภทความเสี่ยงที่เกี่ยวข้อง (Risk factor) รวมถึงแบ่งระดับผลการตรวจสอบออกเป็นประเภทต่างๆ โดยสามารถดูรายละเอียดระดับการประเมินกับผลคะแนนที่จะได้รับตามตาราง ดังต่อไปนี้

อ่อน (3)	**ระดับผลการตรวจ : Major Non-Conformity (Major NC)** **คำอธิบาย** : ไม่มีการปฏิบัติตามหลักเกณฑ์ฯ ไม่มีกระบวนการหรือการดำเนินงานที่ชัดเจน **เช่น :** ไม่ได้มีนโยบายหรือกระบวนการที่เกี่ยวกับการประเมินความเสี่ยง
	ระดับผลการตรวจ : Minor Non-Conformity (Minor NC) **คำอธิบาย** : มีการดำเนินการตามหลักเกณฑ์ฯ แต่ยังไม่เป็นระบบหรือยังไม่มีกระบวนการที่ชัดเจน **เช่น :** มีนโยบายและกระบวนการในการประเมินความเสี่ยงภายในองค์กร **แต่<u>ไม่มีกิจกรรม</u>** ในการตอบสนองความเสี่ยงที่เกินกว่าระดับยอมรับได้
พอใช้ (2)	**ระดับผลการตรวจ : Observation** **คำอธิบาย :** มีการดำเนินการตามหลักเกณฑ์ฯ แต่พบว่าสามารถปรับปรุงพัฒนากระบวนการให้ดียิ่งขึ้นได้ เพื่อป้องกันไม่ให้เกิดการละเลยซึ่งอาจนำไปสู่ความไม่สอดคล้องในอนาคต

	เช่น : มีการประเมินด้าน Risk management มีการวางแผนในการแก้ไขความเสี่ยงแล้วแต่ยังไม่มีการติดตามผลที่ชัดเจน เพื่อให้มั่นใจว่าแผนในการลดความเสี่ยงสามารถดำเนินการได้ครบถ้วนและตรงกับวัตถุประสงค์การดำเนินงานขององค์กร
ดี (1)	**ระดับผลการตรวจ : Conformity** **คำอธิบาย :** มีการดำเนินการครบถ้วน มีการติดตาม วัดผลและพัฒนากระบวนการอย่างต่อเนื่อง **เช่น :** มีการประเมินด้าน Risk management รวมถึงมีการการวัดผลการดำเนินงานเพื่อให้มั่นใจว่ากิจกรรมด้าน Risk management สอดคล้องกับความเสี่ยงและวัตถุประสงค์การดำเนินงานขององค์กร

นอกจากนี้ผู้ตรวจประเมินสามารถให้คำแนะนำเพิ่มเติมในการบริหารจัดการความเสี่ยงนอกเหนือจากหลักเกณฑ์ฯ ได้เพื่อเป็นข้อเสนอแนะให้องค์กรพิจารณาปรับปรุงหรือเพิ่มเติมการปฏิบัติให้ดียิ่งขึ้นในอนาคต โดยระบุประเด็นข้อเสนอแนะเป็น Opportunity For Improvement

ตัวอย่างรูปแบบการตรวจสอบของผู้ตรวจสอบอิสระตามตารางด้านล่าง ทั้งนี้สามารถศึกษารายละเอียดหัวข้อในการตรวจสอบเพิ่มเติมในเอกสาร คู่มือการตรวจประเมินธุรกิจบริการ

ตัวอย่าง Audit checklist เพื่อดำเนินการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)

ตารางการควบคุมที่พึงมีและแนวทางการประเมิน	วิธีการตรวจสอบและการสุ่มตัวอย่าง	รายการหลักฐาน	Status	Audit Note	Role
Privacy Control 01: มาตรการในการคุ้มครองข้อมูลส่วนบุคคล	การสัมภาษณ์ 1. สัมภาษณ์ผู้ให้บริการในเรื่องของมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด สอบทานเอกสาร 1. สอบทานเอกสารที่ระบุถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด	นโยบายคุ้มครองข้อมูลส่วนบุคคล	**Conformity**	บริษัทมีการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมเนื้อหาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่มีหน้าที่ในการจัดการและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	☒ IDP (Identity Proofing) ☒ IDP (Authenticator Management) ☒ IDP (Authentication) ☒ Platform

4.4 กำหนดเกณฑ์การประเมินความเสี่ยง (Define risk criteria)

จากการประเมินความเสี่ยงในหัวข้อ 4.3 จำเป็นจะต้องมีการระบุเกณฑ์การประเมินความเสี่ยงต่างๆ ซึ่งประกอบไปด้วย

- เกณฑ์การประเมินความเสี่ยงตั้งต้น (Inherent risk criteria)
- เกณฑ์การประเมินความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability criteria)
- เกณฑ์การประเมินความเสี่ยงสุทธิ (Net risk criteria)

ทั้งนี้เกณฑ์การประเมินในแต่ละแบบจะมีรายละเอียดดังต่อไปนี้

เกณฑ์การประเมินความเสี่ยงตั้งต้น (Inherent risk criteria) จะถูกแบ่งออกเป็น 3 ระดับโดยมีรายละเอียดในระดับภาพรวมขององค์กรดังต่อไปนี้

		รายละเอียด
ความเสี่ยงตั้งต้น (IR)	**สูง (3)**	**องค์กรมีความเสี่ยงตั้งต้นสูง** อันเนื่องมาจากลักษณะการดำเนินงานและการให้บริการกับลูกค้าจำนวนมาก มีโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เชื่อมต่อกับองค์กรภายนอก หรือมีโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศภายในที่มีความซับซ้อน โดยมีผลมาจากการนำเทคโนโลยีใหม่ ๆ เข้ามาดำเนินการ เช่น เทคโนโลยีปัญญาประดิษฐ์ ซึ่งอาจทำให้เกิดความเสี่ยงที่ไม่เคยพบเจอมาก่อนเกิดขึ้นได้หรือองค์กรมีปัจจัยด้านบุคลากรภายในองค์กรที่มีการเปลี่ยนแปลงปล่อยครั้งส่งผลกระทบต่อการดำเนินงานในปัจจุบันหรืออาจรวมถึงองค์กรไม่สามารถปฏิบัติตาม ระเบียบ กฎหมาย หรือแนวทางปฏิบัติส่งผลให้สภาพแวดล้อมในการดำเนินธุรกิจเกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลมีความเสี่ยงอยู่ในระดับที่สูง
	ปานกลาง (2)	**องค์กรมีความเสี่ยงตั้งต้นปานกลาง** อันเนื่องมาจากลักษณะการดำเนินงานและการให้บริการกับลูกค้าจำนวนหนึ่ง โดยมีโครงสร้างพื้นฐานด้านสารสนเทศที่มีทั้งระบบปิดและเชื่อมต่อกับองค์กรภายนอก องค์กรมีระดับไม่ซับซ้อนมาก มีการประยุกต์เทคโนโลยีใหม่ๆ มาใช้งานบ้าง แต่ไม่ถึงเป็นระบบหลักที่ใช้เพื่อการพิสูจน์และยืนยันตน มีการเปลี่ยนแปลงบุคลากรแต่ไม่ส่งผลกระทบต่อการดำเนินงานมาก ทั้งนี้องค์กรสามารถที่จะปฏิบัติตามระเบียบ กฎหมาย หรือ แนวทางปฏิบัติส่วนใหญ่ได้แต่ยังมีบางหัวข้อที่อยู่ระหว่างการดำเนินงานแก้ไขส่งผลให้สภาพแวดล้อมในการดำเนินธุรกิจเกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลมีความเสี่ยงอยู่ในระดับปานกลาง
	ต่ำ (1)	**องค์กรมีความเสี่ยงตั้งต้นต่ำ** อันเนื่องมาจากลักษณะการดำเนินงานและการให้บริการกับลูกค้าที่ไม่มาก โครงสร้างภายในขององค์กรเป็นขนาดเล็กไม่ซับซ้อนรวมไปถึงโครงสร้างพื้นฐานด้านสารสนเทศส่วนมากดำเนินการในเครือข่ายที่เป็นระบบปิด บุคลากรภายในองค์กรมีการเปลี่ยนแปลงน้อยมากจนไปถึงไม่มีการเปลี่ยนแปลง

		หรืออาจรวมถึงองค์กรสามารถดำเนินการตามระเบียบ กฎหมาย หรือแนวทางปฏิบัติครบถ้วนส่งผลให้สภาพแวดล้อมในการดำเนินธุรกิจเกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลมีความเสี่ยงอยู่ในระดับต่ำ

เกณฑ์การประเมินความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability criteria) จะถูกแบ่งออกเป็น 3 ระดับโดยมีรายละเอียดของแต่ละระดับดังต่อไปนี้

		รายละเอียด
ความสามารถในการบริหารจัดการความเสี่ยง (RMC)	**อ่อน (3)**	ไม่มีการปฏิบัติตามหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลหรือไม่มีกระบวนการตามประกาศที่ชัดเจนซึ่งนำไปสู่ความเสียหายอย่างร้ายแรงต่อระบบหรือกรณีที่ไม่ปฏิบัติตามหลักเกณฑ์ฯหลายหัวข้อรวมกันซึ่งเมื่อพิจารณาแล้วมีผลกระทบต่อระบบการจัดการโดยรวม
	พอใช้ (2)	มีการดำเนินการตามประกาศหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลแล้วแต่พบประเด็นบางเรื่องที่หากปล่อยละเลยไว้อาจนำไปสู่ความไม่สอดคล้องในอนาคตได้ควรต้องดำเนินการปรับปรุงหรือพัฒนากระบวนการให้ดียิ่งขึ้นเพื่อป้องกันไม่ให้ เกิดการละเลยซึ่งอาจนำไปสู่ความไม่สอดคล้องในอนาคต
	ดี (1)	มีการปฏิบัติตามหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลครบถ้วนมีกระบวนการที่ชัดเจนรวมถึงมีการวัดผลอย่างต่อเนื่อง

เกณฑ์การประเมินความเสี่ยงสุทธิ (Net risk criteria) จะเป็นการนำผลของการประเมินความเสี่ยงตั้งต้น (Inherent risk) กับผลของการประเมินความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) มาประเมินร่วมกัน ซึ่งจะสามารถระบุความเสี่ยงสุทธิทั้งในระดับภาพรวมขององค์กรและความเสี่ยงสุทธิในแต่ละปัจจัยความเสี่ยงได้อีกด้วย โดยจะมีการแบ่งระดับออกเป็น 5 ระดับโดยมีรายละเอียดดังต่อไปนี้

		RMC		
		ดี (1)	**พอใช้ (2)**	**อ่อน (3)**
IR	**สูง (3)**	ปานกลาง	ค่อนข้างสูง	สูง
	ปานกลาง (2)	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง
	ต่ำ (1)	ต่ำ	ค่อนข้างต่ำ	ปานกลาง

ซึ่งคำอธิบายระดับความเสี่ยงสุทธิทั้ง 5 ระดับจะมีรายละเอียดดังต่อไปนี้

คำอธิบายความเสี่ยงสุทธิ (Net risk) ในแต่ละระดับ	
ต่ำ	ความเสี่ยงรวมสุทธิอยู่ในระดับ**ต่ำ** ในปัจจุบันองค์กรสามารถกำกับดูแลและบริหารจัดการความเสี่ยงได้เป็นอย่างดี
ค่อนข้างต่ำ	ความเสี่ยงรวมสุทธิอยู่ในระดับ**ค่อนข้างต่ำ** องค์กรสามารถกำกับดูแลและบริหารจัดการได้ค่อนข้างดี
ปานกลาง	ความเสี่ยงรวมสุทธิอยู่ในระดับ**ปานกลาง** องค์กรสามารถกำกับดูแลและบริหารจัดการความเสี่ยงได้พอใช้ สามารถดำเนินงานเพิ่มเติมเพื่อปรับปรุงให้ดียิ่งขึ้นได้
ค่อนข้างสูง	ความเสี่ยงรวมสุทธิอยู่ในระดับ**ค่อนข้างสูง** องค์กรสามารถกำกับดูแลและบริหารจัดการความเสี่ยงได้ต่ำ มีการดำเนินงานที่ต้องปรับปรุงให้ดีขึ้นกว่าการดำเนินงานในปัจจุบัน ทั้งนี้**ต้องมีแผน**ในการดำเนินการลดความเสี่ยงเพื่อลดความเสี่ยงให้ไปอยู่ในระดับที่ต่ำกว่านี้
สูง	ความเสี่ยงรวมสุทธิอยู่ในระดับ**สูง** องค์กรสามารถกำกับดูแลและบริหารจัดการความเสี่ยงได้ต่ำมาก การดำเนินงานที่เกี่ยวข้องต้องมีการปรับปรุงให้ดีขึ้นกว่าการดำเนินงานในปัจจุบัน ทั้งนี้**ต้องมีแผน**ในการดำเนินการลดความเสี่ยงเพื่อลดความเสี่ยงให้ไปอยู่ในระดับที่ต่ำกว่านี้ และจำเป็นต้องปฏิบัติตามแผนลดความเสี่ยงทันที

โดยตารางด้านบนสามารถสรุปได้ว่าความเสี่ยงสุทธิที่ยอมรับได้ (Risk appetite) จะอยู่ในระดับต่ำ, ค่อนข้างต่ำ และปานกลาง ส่วนความเสี่ยงสุทธิที่ยอมรับไม่ได้และต้องดำเนินการแก้ไขควบคุมความเสี่ยงจะอยู่ในระดับค่อนข้างสูง และสูง ทั้งนี้รายละเอียดเพิ่มเติมสามารถเรื่องระดับการยอมรับความเสี่ยงและจัดการความเสี่ยงจะระบุเพิ่มเติมในหัวข้อ 4.5

4.5 ขั้นตอนการประเมินความเสี่ยง ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) และการตอบสนองกับความเสี่ยง (Risk response)

ขั้นตอนการประเมินความเสี่ยง

1. ดำเนินการประเมินผลความเสี่ยงตั้งต้น (Inherent risk)

ผู้ประเมินดำเนินการประเมินตนเอง (Self-assessment) ตามแบบฟอร์ม “แบบประเมินความเสี่ยงตั้งต้นขององค์กรผู้ให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัล (IR Self-Assessment)” โดยการประเมินตนเองนั้นสามารถอ้างอิงจากหลักฐานการดำเนินงานขององค์กรเพื่อประกอบการตัดสินใจในการเลือกระดับความเสี่ยงต่างๆ จากนั้นจะสามารถสรุปผลความเสี่ยงตั้งต้นของประเภทความเสี่ยงทั้ง 5 ได้จากการรวมคะแนนและเฉลี่ยคะแนนภายในปัจจัยเดียวกัน ตารางด้านล่างแสดงให้เห็นข้อคำถามในแต่ละข้อเกี่ยวข้องกับปัจจัยความเสี่ยงประเภทใด

	Inherent Risk Factors				
	Strategic	Operational	Technology	Reputation	Compliance
ข้อคำถาม	1,2,3,4,5,6,7,11,12	4,7,8,11,13,14,15,17,19,20,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,62,63,64,65,66,67,68	4,8,12,13,14,16,20,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,66	4,11,12,16,18,21,27,62,63,64,65,66,67,68	9,10,11,12,13,16,17,22,23,24,25

ซึ่งเมื่อนำคะแนนในแต่ละข้อที่อยู่ในประเภทความเสี่ยงเดียวกันมาเฉลี่ยจะได้คะแนนความเสี่ยงเบื้องต้นของประเภทความเสี่ยงในแต่ละด้าน ทั้งนี้ จากการรวมคะแนนและเฉลี่ยจะได้ผลลัพธ์ออกมาเป็นจุดทศนิยมซึ่งจะสามารถใช้ตารางด้านล่างเพื่อแบ่งช่วงระดับความเสี่ยงตั้งต้น

ตารางแบ่งช่วงระดับความเสี่ยงตั้งต้น

	ระดับช่วง IR
สูง	2.31 – 3.00
ปานกลาง	1.71 – 2.30
ต่ำ	1.00 – 1.70

ตัวอย่างการสรุปผลระดับความเสี่ยงตั้งต้นแยกตามประเภทความเสี่ยง

หากองค์กรที่มีบทบาท Platform ทำการประเมินตนเองในด้าน Reputation มีผลตามตารางด้านล่าง

หัวข้อการประเมิน	ผลการประเมิน	คะแนน
การควบรวมกิจการ เข้าซื้อกิจการ หรือแผนการลดค่าใช้จ่ายที่อาจส่งผลกระทบต่อบุคลากร กระบวนการ หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับบริการ Digital ID	ปานกลาง	2
นวัตกรรมเกี่ยวกับบริการ Digital ID ที่ยังไม่มีหลักเกณฑ์หรือประกาศของ สพธอ. รองรับ	สูง	3
การใช้งาน Innovative Technology ในระบบ Digital ID	สูง	3
การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอ่อนไหว เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (ตามมาตรา 26 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)	สูง	3
จำนวนการร้องเรียนหรือแจ้งปัญหาการใช้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัลจากผู้ใช้บริการ รวมถึงหน่วยงานที่เชื่อมต่อเพื่อใช้บริการ (เช่น Relying Party, Identity Provider, Authorative Source) ในระยะเวลา 12 เดือน	สูง	3
จำนวนคดีความที่เกี่ยวกับการให้บริการ Digital ID ที่ถูกตัดสินว่ามีความผิดตามกฎหมาย หรือ ละเมิดกฎเกณฑ์ของหน่วยงานกำกับดูแล ในระยะเวลา 12 เดือน	สูง	3
จำนวนหน่วยงานภายนอกที่มีนัยสำคัญต่อบริการ Digital ID เช่น Digital Identity Platform Service, Authoritative Source, Cloud Provider, IDP Agent, Developer เป็นต้น	ปานกลาง	2
จำนวนเหตุการณ์ที่ส่งผลกระทบในวงกว้างและมีนัยสำคัญ ต่อความน่าเชื่อถือของบริษัท ในระยะเวลา 12 เดือน	สูง	3
จำนวน IDP ที่การเชื่อมต่อเพื่อให้บริการ Digital ID	ปานกลาง	2
จำนวนบัญชีที่ลงทะเบียนและพิสูจน์ตัวตนแล้วในระบบบริการ Digital ID	ปานกลาง	2

เมื่อนำคะแนนทั้งหมดในประเภทความเสี่ยงเดียวกันมาเฉลี่ยจะได้ผลตามตาราง

ปัจจัยเสี่ยง	คะแนน ความเสี่ยงตั้งต้น	ระดับ ความเสี่ยงตั้งต้น (IR)
1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)	1.50	ต่ำ
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)	2.00	ปานกลาง
3. ความเสี่ยงด้านเทคโนโลยีที่นำมาใช้ (Technology Risk)	1.35	ต่ำ
4. ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk)	2.60	สูง
5. ความเสี่ยงทางด้านกฎหมายและกฎระเบียบ (Compliance Risk)	2.20	ปานกลาง

หมายเหตุ ตัวเลขในตารางเป็นเพียงตัวอย่างเพื่อแสดงให้เห็นรูปแบบในการประเมิน รวมถึงแสดงตัวอย่างการทดสอบประเมินผลแค่ด้าน Reputation เท่านั้น

สุดท้ายแล้วจะสามารถหาระดับความเสี่ยงตั้งต้น (IR) ขององค์กรได้โดยการนำคะแนนความเสี่ยงตั้งต้นของแต่ละปัจจัยนำมาเฉลี่ยและเทียบกับตารางแบ่งช่วงระดับความเสี่ยงตั้งต้นมีผลตัวอย่างตามตารางด้านล่าง

ตัวอย่างการสรุปผลระดับความเสี่ยงตั้งต้นขององค์กร

Inherent Risk Factors					
Strategic	Operational	Technology	Reputation	Compliance	Total of IR
1.50	2.00	1.35	2.60	2.20	คะแนนเฉลี่ยรวมจากทั้ง 5 ปัจจัย

Average

	คะแนนความเสี่ยงตั้งต้นขององค์กร	ระดับความเสี่ยงตั้งต้นขององค์กร (IR)
องค์กร A	1.93	ปานกลาง

2. ดำเนินการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)

องค์กรดำเนินการตรวจประเมินความสามารถในการบริหารจัดการความเสี่ยงจากผู้ตรวจสอบอิสระ (Internal/External auditor) โดยตรวจสอบการควบคุมตามข้อกำหนดที่ระบุในหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล จำนวน 10 หัวข้อ โดยสามารถใช้แบบฟอร์ม “Audit checklist การตรวจประเมินธุรกิจบริการ” ในการบันทึกผลการตรวจสอบ ซึ่งจะสามารถสรุปการบริหารจัดการความเสี่ยงของประเภทความเสี่ยง (Risk factor) ทั้ง 5 ได้จากการรวมคะแนนและเฉลี่ยคะแนนภายในประเภทเดียวกัน ตารางด้านล่างแสดงให้เห็นหัวข้อที่ตรวจสอบในแต่ละข้อเกี่ยวข้องกับประเภทความเสี่ยงประเภทใด ทั้งนี้ รายละเอียดในตารางอ้างอิงมาจากเอกสาร “Audit checklist การตรวจประเมินธุรกิจบริการ”

ซึ่งเมื่อนำคะแนนในแต่ละข้อที่อยู่ในประเภทความเสี่ยงเดียวกันมาเฉลี่ยจะได้คะแนนความสามารถในการบริหารจัดการความเสี่ยงของประเภทความเสี่ยงในแต่ละด้าน ทั้งนี้ จากการรวมคะแนนและเฉลี่ยจะได้ผลลัพธ์ออกมาเป็นจุดทศนิยมซึ่งจะสามารถใช้ตารางด้านล่างเพื่อแบ่งช่วงระดับความสามารถในการบริหารจัดการความเสี่ยง

ตารางแบ่งช่วงระดับความสามารถในการบริหารจัดการความเสี่ยง

	ระดับช่วง RMC
อ่อน	2.31 – 3.00
พอใช้	1.71 – 2.30
ดี	1.00 – 1.70

ตัวอย่างการสรุปผลระดับความสามารถในการบริหารจัดการความเสี่ยง

หากองค์กรที่มีบทบาท Platform ทำการประเมินจากผู้ตรวจสอบอิสระในด้าน Reputation มีผลตามตารางด้านล่าง

หัวข้อการประเมิน	ผลการประเมิน	คะแนน	ระดับความสามารถในการบริหารจัดการความเสี่ยง
UST01 - ข้อตกลงในการให้บริการ	Conformity	1	ดี
UST02 – การใช้บริการจากบุคคลภายนอกที่เกี่ยวกับระบบการให้บริการ	Conformity	1	ดี

UST03 - รายละเอียดของค่าธรรมเนียมที่เรียกเก็บจาก ผู้ใช้บริการระบบ	Major NC	3	อ่อน
UST04 - มาตรการการคุ้มครอง และการบรรเทาความเสียหายและการชดใช้แก่ผู้ใช้บริการ	Observation	2	พอใช้
USX01 - ข้อกำหนดทั่วไปเกี่ยวกับความต้องการในการใช้งาน (Usability Requirement)	Conformity	1	ดี
USX02 - ข้อกำหนดเกี่ยวกับการออกแบบส่วนต่อประสานและการสร้างประสบการณ์ที่ดีแก่ผู้ใช้บริการในขั้นตอนการพิสูจน์ตัวตน (Requirements for the identity verification journey)	Observation	2	พอใช้
USX04 - การทดสอบความสามารถของระบบ	Compliance	1	ดี
FRC10 - การให้ความช่วยเหลือผู้ใช้บริการจากเหตุการณ์การทุจริตหรือฉ้อโกงในระบบ	Minor NC	3	อ่อน
PRC22 - การรับเรื่องร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล	Observation	2	พอใช้
PFM01 - การเปิดเผยข้อมูลโดยทั่วไป	Compliance	1	ดี
PFM02 - การคุ้มครองข้อมูลส่วนบุคคล: ไม่นำข้อมูลส่วนบุคคลไปใช้โดยตรง	Minor NC	3	อ่อน
PFM03 - การคุ้มครองข้อมูลส่วนบุคคล: ไม่จัดเก็บข้อมูลส่วนบุคคล (เป็นการชั่วคราว) เว้นแต่ เก็บโดยปลอดภัย	Compliance	1	ดี
PFM04 - การคุ้มครองข้อมูลส่วนบุคคล: กรณีที่มีการเก็บชั่วคราว บุคลากรต้องไม่สามารถเข้าถึงได้	Minor NC	3	อ่อน

เมื่อนำคะแนนทั้งหมดในประเภทความเสี่ยงเดียวกันมาเฉลี่ยจะได้ผลตามตาราง

ปัจจัยเสี่ยง	คะแนนความสามารถในการบริหารจัดการความเสี่ยง	ระดับความสามารถในการบริหารจัดการความเสี่ยง (RMC)
1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)	1.50	ดี
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)	1.30	ดี

3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)	1.80	พอใช้
4. ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk)	1.85	พอใช้
5. ความเสี่ยงทางด้านการปฏิบัติตามหลักเกณฑ์ (Compliance Risk)	1.80	พอใช้

หมายเหตุ ตัวเลขในตารางเป็นเพียงตัวอย่างเพื่อแสดงให้เห็นรูปแบบในการประเมิน รวมถึงแสดงตัวอย่างการทดสอบประเมินผลแค่ด้าน Reputation เท่านั้น

สุดท้ายแล้วจะสามารถหาระดับความสามารถในการบริหารจัดการความเสี่ยง (RMC) ของทั้งองค์กรได้โดยการนำคะแนนความสามารถในการบริหารจัดการความเสี่ยงของแต่ละประเภทนำมาเฉลี่ยและเทียบกับตารางแบ่งช่วงระดับความสามารถในการบริหารจัดการความเสี่ยงมีผลตัวอย่างตามตารางด้านล่าง

ตัวอย่างการสรุปผลระดับความสามารถในการบริหารจัดการความเสี่ยงขององค์กร

Risk management capability					
Strategic	Operational	Technology	Reputation	Compliance	Total of RMC
1.50	1.30	1.80	1.85	1.80	คะแนนเฉลี่ยรวมจากทั้ง 5 ปัจจัย

Average

	คะแนนความสามารถในการบริหารจัดการความเสี่ยงขององค์กร	ระดับความสามารถในการบริหารจัดการความเสี่ยงขององค์กร (RMC)
องค์กร A	1.65	ดี

หมายเหตุ ในการดำเนินการจริงผู้ตรวจสอบจะต้องดำเนินการตรวจสอบและประเมินผลให้ครบถ้วนตามแบบฟอร์ม “Audit checklist การตรวจประเมินธุรกิจบริการ”

3. ดำเนินการสรุปผลความเสี่ยงสุทธิ (Net risk)

เมื่อดำเนินการประเมินผลทั้งในส่วนของความเสี่ยงตั้งต้น (Inherent risk) และความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) ภาพรวมของการประเมินจะสามารถสรุปผลเป็นความเสี่ยงสุทธิ (Net risk) ได้ 2 รูปแบบคือ

1. ความเสี่ยงสุทธิแบ่งแยกตามประเภทความเสี่ยง (Net risk by risk factor)
2. ความเสี่ยงสุทธิขององค์กร (Overall net risk)

โดยการนำผลของความเสี่ยงตั้งต้น (Inherent risk) และความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) ไปเปรียบเทียบกับตารางในหัวข้อ “4.4 กำหนดเกณฑ์การประเมินความเสี่ยง (Define risk criteria)” ในหัวข้อเกณฑ์การประเมินความเสี่ยงสุทธิ (Net risk criteria) ซึ่งจะสรุปผลได้ตามตัวอย่างตารางด้านล่าง

ตัวอย่างการสรุปผลความเสี่ยงสุทธิแยกตามประเภทความเสี่ยง (Net risk by risk factor)

ปัจจัยเสี่ยง	ความเสี่ยงตั้งต้น (IR)	ความสามารถในการบริหารจัดการความเสี่ยง (RMC)	ความเสี่ยงสุทธิ (Net Risk)
1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)	ต่ำ	ดี	ต่ำ
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)	ปานกลาง	ดี	ค่อนข้างต่ำ
3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)	ต่ำ	พอใช้	ปานกลาง
4. ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk)	สูง	พอใช้	ค่อนข้างสูง
5. ความเสี่ยงทางด้านการปฏิบัติตามหลักเกณฑ์ (Compliance Risk)	ปานกลาง	พอใช้	ปานกลาง

ตัวอย่างการสรุปผลความเสี่ยงสุทธิขององค์กร

ระดับความเสี่ยงตั้งต้นขององค์กร (IR)	ระดับความสามารถในการบริหารจัดการความเสี่ยงขององค์กร (RMC)	ระดับความเสี่ยงสุทธิขององค์กร (NR)
ปานกลาง	ดี	ค่อนข้างต่ำ

พิจารณาความเสี่ยงที่พบและระดับความเสี่ยงที่ยอมรับได้ (Risk appetite)

จากผลการสรุปผลความเสี่ยงสุทธิแยกตามประเภทความเสี่ยง (Net risk by risk factor) สามารถนำมาพิจารณาความเสี่ยงที่พบเพื่อลดความเสี่ยงที่เกินกว่าที่ยอมรับได้ และนำไปสู่ภาพรวมความเสี่ยงสุทธิขององค์กร (Overall net risk) ที่ดีขึ้น

โดยทั้งนี้ระดับความเสี่ยงที่สามารถยอมรับได้ (Risk appetite) คือความเสี่ยงสุทธิในระดับที่ต่ำ, ค่อนข้างต่ำ และปานกลาง ซึ่งหากองค์กรมีความเสี่ยงสุทธิมากกว่าระดับความเสี่ยงที่ยอมรับได้

(Risk appetite) องค์กรจำเป็นต้องจัดหาแผนลดความเสี่ยงเพื่อดำเนินการลดความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้ ทั้งนี้ องค์กรต้องระบุแผนดังกล่าวในเอกสารรายงานการประเมินความเสี่ยงสำหรับธุรกิจบริการระบบการพิสูจน์และยืนยันตนทางดิจิทัล และ Corrective action form

โดยจากตัวอย่างการประเมินตามตารางด้านล่างจะเห็นว่าความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation risk) มีความเสี่ยงสุทธิสูงเกินกว่าระดับที่ยอมรับได้ ดังนั้น จึงต้องจัดทำแผนแก้ไขเพื่อลดความเสี่ยงซึ่งจะมีรายละเอียดในหัวข้อถัดไป

ปัจจัยเสี่ยง	ความเสี่ยงตั้งต้น (IR)	ความสามารถในการบริหารจัดการความเสี่ยง (RMC)	ความเสี่ยงสุทธิ (Net Risk)
1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)	ต่ำ	ดี	ต่ำ
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)	ปานกลาง	ดี	ค่อนข้างต่ำ
3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)	ต่ำ	พอใช้	ปานกลาง
4. ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk)	สูง	พอใช้	ค่อนข้างสูง
5. ความเสี่ยงทางด้านการปฏิบัติตามหลักเกณฑ์ (Compliance Risk)	ปานกลาง	พอใช้	ปานกลาง

<u>การตอบสนองกับความเสี่ยง (Risk response)</u>

องค์กรสามารถตอบสนองกับความเสี่ยง (Risk response) ได้อยู่ 2 รูปแบบ ประกอบด้วย

1. ปรับปรุงความสามารถในการบริการจัดการความเสี่ยง (Risk management capability) ให้ดียิ่งขึ้นโดยให้พิจารณาผลการตรวจสอบจากผู้ตรวจสอบอิสระในหัวข้อที่ได้รับการประเมินในระดับ Major NC, Minor NC และ Observation และดำเนินการตามตารางด้านล่าง

ผลการประเมิน	การดำเนินการ	การส่งหลักฐานเพิ่มเติม
ผลการตรวจประเมินใน Audit process พบว่ามี Major NC	หน่วยงาน**<u>จัดทำแผนการแก้ไข (Corrective Action Plan)</u>** สำหรับหัวข้อที่เกี่ยวข้องกับความไม่สอดคล้องและ**<u>ดำเนินการแก้ไขภายใน 90 วัน</u>** นับจากหลังตรวจประเมิน	หน่วยงานส่งรายงานการประเมินความเสี่ยงสำหรับธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล, แบบฟอร์มระบุวิธีการแก้ไขความไม่สอดคล้อง พร้อมทั้งแนบหรือแสดงหลักฐานการแก้ไข

ผลการตรวจประเมินใน Audit process พบว่ามี Minor NC	หน่วยงาน**จัดทำแผนการแก้ไข (Corrective Action Plan)** สำหรับหัวข้อที่เกี่ยวข้องกับความไม่สอดคล้อง พร้อมทั้งส่งแผนให้ทาง สพธอ. พิจารณา**ภายใน 30 วัน**นับจากหลังตรวจประเมิน	หน่วยงานส่งรายงานการประเมินความเสี่ยงสำหรับธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และแบบฟอร์มระบุวิธีการแก้ไขความไม่สอดคล้อง
ผลการตรวจประเมินใน Audit process พบว่ามี Observation	หน่วยงานพิจารณาการปรับปรุงเพิ่มเติมตามประเด็นที่ตรวจพบ ทั้งนี้ ในการตรวจสอบครั้งถัดไป หากยังพบเจอประเด็นเดิม ผู้ตรวจสอบสามารถพิจารณาเพิ่มระดับเป็น Nonconformity ได้	หน่วยงานส่งรายงานการประเมินความเสี่ยงสำหรับธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และแบบฟอร์มระบุวิธีการแก้ไขความไม่สอดคล้อง (หากดำเนินการแก้ไข)

ประเด็นการตรวจประเมินที่เป็น Major NC และ Minor NC องค์กรจำเป็นต้องจัดทำ**แผนการแก้ไข (Corrective Action Plan)** ที่ระบุถึง Root cause ของปัญหา, แผนการแก้ไขระยะสั้น, แผนการป้องกันการเกิดปัญหาซ้ำ รวมถึงระบุถึงหน่วยงานที่รับผิดชอบและระยะเวลาที่คาดว่าจะแล้วเสร็จ ซึ่งต้องผ่านการอนุมัติจากผู้บริหารในองค์กรภายในแล้ว ในส่วนของการตรวจประเมินที่เป็น Observation สามารถพิจารณาดำเนินการแก้ไขหรือไม่แก้ไขได้ตามความเสี่ยงสุทธิที่องค์กรประเมิน ทั้งนี้ หากต้องการแก้ไข องค์กรจำเป็นต้องจัดทำแผนการแก้ไข (Corrective Action Plan) เพิ่มเติมด้วย

2. ลดความเสี่ยงตั้งต้น (Inherent risk) ที่เกิดขึ้นจากการดำเนินการในปัจจุบัน โดยพิจารณาจากการดำเนินการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลว่ามีกระบวนการใดที่มีความเสี่ยงสูงบ้างและใช้กลยุทธ์สำหรับการลดความเสี่ยงในการจัดการความเสี่ยงดังกล่าว

ทั้งนี้ กลยุทธ์สำหรับการลดความเสี่ยง (Risk treatment) ที่องค์กรสามารถเลือกนำไปใช้ได้มีอยู่ทั้งหมด 4 รูปแบบซึ่งรายละเอียดมีดังต่อไปนี้

2.1 การลดความเสี่ยง (Risk Mitigation) องค์กรมีการกำหนดให้มีการบริหารจัดการความเสี่ยงที่รัดกุมยิ่งขึ้น หรือมีกิจกรรมในการควบคุมเพิ่มเติมเพื่อลดโอกาสเกิดหรือผลกระทบจากความเสี่ยงนั้นๆ ตัวอย่างเช่น การพัฒนาบุคลากร ความชำนาญ, การจัดตั้งให้มีนโยบายด้านความปลอดภัยของเทคโนโลยีสารสนเทศ เป็นต้น

2.2 การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการหลีกเลี่ยงกิจกรรมหรือสาเหตุที่อาจก่อให้เกิดความเสี่ยง ทั้งนี้ ต้องมั่นใจได้ว่าการหลีกเลี่ยงกิจกรรมดังกล่าวจะไม่กระทบต่อการดำเนินการในส่วนอื่นๆ ด้วย

2.3 การถ่ายโอนความเสี่ยง (Risk Transfer) เป็นการลดความถี่ในการเกิดหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น โดยกระจายหรือโอนไปยังบุคคลอื่น ตัวอย่างเช่น การจัดหาประกันภัย, การร่วมทุนพันธมิตร เป็นต้น

2.4 การยอมรับความเสี่ยง (Risk Acceptance) เป็นการที่ไม่มีการกำหนดกิจกรรมใด ๆ เพื่อตอบสนองต่อความเสี่ยงที่อาจเกิดขึ้น โดยผู้บริหารยอมรับผลที่อาจเกิดขึ้นจากความเสี่ยงนั้น ทั้งนี้

ผู้ที่สามารถตัดสินใจยอมรับความเสี่ยงจะต้องเป็นผู้บริหารขององค์กรที่มีอำนาจและสามารถพิจารณาความเสี่ยงดังกล่าวว่าควรจะต้องยอมรับความเสี่ยงหรือไม่

เมื่อองค์กรมีการเตรียมแผนสำหรับการปรับปรุงความสามารถในการบริการจัดการความเสี่ยง (Risk management capability) หรือมีการลดความเสี่ยงตั้งต้น (Inherent risk) ให้องค์กรทำการประเมินความเสี่ยงที่หลงเหลือ (Residual risk) อยู่อีกครั้งเพื่อยืนยันว่าความเสี่ยงในทุกปัจจัยความเสี่ยงอยู่ในระดับที่ยอมรับได้

จากตัวอย่างการประเมินความเสี่ยงที่ผ่านมา หากองค์กรมีการวางแผนเพื่อจัดความเสี่ยงแล้ว หลังจากประเมินความเสี่ยงที่หลงเหลือ (Residual risk) จะพบว่า ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk) ลดลงเหลือระดับ “ค่อนข้างต่ำ” ซึ่งอยู่ในระดับที่ยอมรับได้

ปัจจัยเสี่ยง	ความเสี่ยงตั้งต้น (IR)	ความสามารถในการบริหารจัดการความเสี่ยง (CF)	ความเสี่ยงสุทธิ (Net Risk)
1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)	ต่ำ	ดี	ต่ำ
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)	ปานกลาง	ดี	ค่อนข้างต่ำ
3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)	ต่ำ	พอใช้	ปานกลาง
4. ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk)	ปานกลาง	ดี	ค่อนข้างต่ำ
5. ความเสี่ยงทางด้านการปฏิบัติตามหลักเกณฑ์ (Compliance Risk)	ปานกลาง	พอใช้	ปานกลาง

4.6 การติดตามและรายงานผลความเสี่ยง (Risk monitoring and reporting)

องค์กรจำเป็นจะต้องดำเนินการประเมินความเสี่ยงตั้งต้น (Inherent risk) และความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) เพื่อสรุปผลเป็นความเสี่ยงสุทธิ (Net risk) ซึ่งมีเอกสารที่ต้องส่งประกอบไปด้วยเอกสารดังต่อไปนี้

1. รายงานการประเมินความเสี่ยงสำหรับธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
2. รายงานการตรวจประเมินระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล
3. แบบฟอร์มระบุวิธีการแก้ไขความไม่สอดคล้อง (หากมีประเด็นความไม่สอดคล้อง)

โดยจะต้องยื่นเอกสารทั้งหมดให้กับทาง สพธอ. ตรวจสอบและควรจัดเตรียมข้อมูลสนับสนุนที่เกี่ยวข้องกับการดำเนินการพิสูจน์และยืนยันตัวตนทางดิจิทัลในกรณีที่ทาง สพธอ. ร้องขอรายละเอียดเพิ่มเติม

นอกจากนี้ องค์กรมีหน้าที่ธำรงรักษาความมั่นคงปลอดภัยและความน่าเชื่อถือของระบบที่อยู่ในความรับผิดชอบโดยต้องดำเนินการลดความเสี่ยงที่เกินกว่าที่จะยอมรับได้ และดำเนินการประเมินความเสี่ยงใหม่อีกครั้งทั้งในส่วนความเสี่ยงตั้งต้น (Inherent risk) และความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) ภายในระยะเวลา 1 ปีนับตั้งแต่วันที่ประเมินความเสี่ยงครั้งล่าสุดหรือเมื่อมีการเปลี่ยนแปลงภายในระบบหรือองค์กรที่สำคัญ อาทิเช่น การควบรวมกิจการ, การเปลี่ยนโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศใหม่ทั้งหมดไปสู่ Cloud เป็นต้น ซึ่งจะต้องส่งเอกสารชุดเดิมที่มีการปรับปรุงแก้ไขแล้วให้ทาง สพธอ. อีกครั้งหนึ่ง

ในกรณีที่ สพธอ. เห็นสมควรหรือคาดการณ์ว่าจะเกิดอุบัติการณ์ร้ายแรงด้านความมั่นคงปลอดภัยหรือการรั่วไหลของข้อมูลส่วนบุคคลหรือมีการเปลี่ยนแปลงของภัยคุกคามที่อาจส่งผลกระทบหรือทำให้เกิดความเสี่ยงอย่างมีนัยยะสำคัญต่อระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล อาจร้องขอให้องค์กรเข้าสู่กระบวนการประเมินเป็นกรณีพิเศษตามกรอบและกระบวนการในการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องหรือมีผลกระทบต่อความปลอดภัยและความน่าเชื่อถือของระบบการพิสูจน์และยืนยันตนทางดิจิทัล

5. คำจำกัดความ

คำศัพท์	คำจำกัดความ
ความเสี่ยงตั้งต้นที่องค์กรมี (Inherent risk)	ความเสี่ยงที่มีอยู่ของผู้ให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะต้องพบเจอ ทั้งนี้ อาจก่อให้เกิดความสูญเสียจากปัจจัยภายในและภายนอกต่างๆ
ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	ความสามารถในการบริหารจัดการความเสี่ยงที่ผู้ให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลมีอยู่ ซึ่งอ้างอิงจากหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
ความเสี่ยงสุทธิที่หลงเหลืออยู่ (Net risk)	ความเสี่ยงสุทธิที่หลงเหลืออยู่ภายหลังจากที่ Risk management capability ได้บริหารจัดการ Inherent risk แล้ว
หน่วยงานผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider Service)	หน่วยงานที่รับข้อมูลและบริหารข้อมูลจากผู้ใช้บริการในการดำเนินการพิสูจน์และยืนยันตัวตนทางดิจิทัล

บริการพิสูจน์ตัวตน (Identity Proofing Service)	บริการที่รวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น
บริการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Management Service)	บริการที่เชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริการจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น
บริการยืนยันตัวตน (Authentication Service)	บริการที่ตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น
หน่วยงานผู้ให้บริการบริการการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service)	หน่วยงานที่รับหน้าที่เป็นตัวกลาง โดยมีเครือข่ายหรือระบบที่ใช้ในการเชื่อมโยงและเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล
บริษัทใหญ่ บริษัทย่อย (Parent, Subsidiary)	บริษัทจำกัด (Incorporated enterprise) ที่มีอำนาจในการตัดสินใจ และถือครองหุ้นมากกว่าร้อยละ 50 ของจำนวนหุ้นสามัญ (Ordinary share) หรือหุ้นที่ให้สิทธิออกเสียง (Voting stock)
สาขา (Branch)	ธุรกิจ (Unincorporated enterprise) ที่บริษัทของท่านถือครองหุ้นทั้งหมด หรือส่วนใหญ่ โดยบริษัทหรือผู้ลงทุน 1 ราย
Innovative Technology	การประมวลผลที่ใช้เทคโนโลยีใหม่ ที่ยังไม่มีมาตรฐานสากลยอมรับ (Unproven technology)
ระดับความน่าเชื่อถือของการพิสูจน์ตันตน (IAL)	ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล สามารถแบ่งได้ 3 ระดับคือ IAL1, IAL2 และ IAL3
ระดับความน่าเชื่อถือของการยืนยันตันตน (AAL)	ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ สามารถแบ่งได้ 3 ระดับคือ AAL1, AAL2 และ AAL3
ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite)	เป็นความเสี่ยงที่องค์กรยังคงมี แต่ทว่ายังสามารถดำเนินการให้ธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลให้บรรลุตามเป้าหมายได้