แนวทาง

การบริหารจัดการความเสี่ยง สำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ศูนย์กำกับดูแลและตรวจสอบธุรกิจ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เวอร์ชัน 1.0 | มิถุนายน 2566

ETDA

Version History

Version	Date	Description	Revised By
1.0	มิ.ย. 2566	แนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล	ศูนย์กำกับดูแลและตรวจสอบธุรกิจ สพธอ.

สารบัญ

1. วัตถุประสงค์ 5
2. การกำหนดขอบเขต (define scope) 5
3. การทำความเข้าใจบริบท (understand context) 6
4. การบริหารจัดการความเสี่ยง (risk management) 7
4.1 การระบุความเสี่ยง (risk identification) 8
4.1.1 กำหนดบทบาทตามลักษณะการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล 8
4.1.2 ระบุประเภทความเสี่ยง (Identify risk factor) 9
4.2 การประเมินความเสี่ยง (risk assessment) 10
4.2.1 การประเมินความเสี่ยงตั้งต้น (inherent risk: IR) 10
4.2.2 การประเมินความสามารถในการบริหารจัดการความเสี่ยง (risk management capability: RMC) 12
4.2.3 ความเสี่ยงสุทธิ (net risk) 13
4.3 การวัดผลความเสี่ยงกับเกณฑ์ประเมินความเสี่ยง (risk evaluation) 14
4.3.1 กำหนดเกณฑ์การประเมินความเสี่ยง (define risk criteria) 14
4.3.2 ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) 19
4.4 การลดความเสี่ยง (Risk treatment) 20
4.4.1 ลดความเสี่ยงตั้งต้น 20
4.4.2 ปรับปรุงความสามารถในการบริการจัดการความเสี่ยง 20
4.5 การติดตามและรายงานผลความเสี่ยง (Risk monitoring and reporting) 21
5. คำจำกัดความ 22
ภาคผนวก ก: คำอธิบายการแบ่งระดับความเสี่ยงและระดับความสามารถในการบริหารจัดการความเสี่ยง 23

สารบัญภาพ

รูป 1 กระบวนการบริหารจัดการความเสี่ยง 7
รูป 2 ภาพรวมการประเมินและบริหารจัดการความเสี่ยงของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล 8
รูป 3 วิธีการคำนวณความเสี่ยงสุทธิ (net risk) 13

แนวทางการบริหารจัดการความเสี่ยง
สำหรับธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

1. วัตถุประสงค์

ในปัจจุบันการดำเนินธุรกิจในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลกำลังเติบโตและมีแนวโน้มที่จะมีบทบาทอย่างมากในการขับเคลื่อนธุรกิจในประเทศไทย ทั้งนี้ความซับซ้อนของการให้บริการและเทคโนโลยีที่นำมาใช้ย่อมทำให้ธุรกิจในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเสี่ยงมากขึ้น ไม่ว่าจะเป็นความเสี่ยงทางด้านธุรกิจ ชื่อเสียง กฎหมายหรือเทคโนโลยี ดังนั้น สำนักงานจึงได้จัดทำเอกสารฉบับนี้ขึ้นเพื่อเป็นแนวทางในการบริหารจัดการความเสี่ยงสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลอย่างเหมาะสมและสอดคล้องตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต และมาตรฐานสากลอื่นๆ ที่ยอมรับโดยทั่วไป รวมถึงสามารถดำเนินการจัดการและแก้ไขความเสี่ยงที่ถูกระบุขึ้นได้อย่างมีประสิทธิภาพ

สำนักงานมุ่งหวังว่าแนวทางปฏิบัตินี้จะมีประโยชน์ต่อองค์กรที่ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมถึงองค์กรอื่นๆ ที่สนใจนำไปปรับใช้เป็นแนวปฏิบัติในการประเมินความเสี่ยงเพื่อสร้างความเชื่อมั่นและความปลอดภัยในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ให้บริการต่อผู้ใช้บริการประชาชนทั่วไป

2. การกำหนดขอบเขต (define scope)

เพื่อให้องค์กรสามารถที่จะประเมินและบริหารจัดการความเสี่ยงสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้อย่างมีประสิทธิภาพ การระบุขอบเขตจึงเป็นกิจกรรมสำคัญที่ช่วยให้เข้าใจความเสี่ยงของระบบที่เกี่ยวข้องกับการให้บริการ และสามารถสื่อสารทำความเข้าใจไปยังผู้ที่เกี่ยวข้อง รวมถึงสามารถแก้ไขและบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากที่สุด ทั้งนี้ ขอบเขตในการประเมินความเสี่ยง ได้แก่กระบวนการทางธุรกิจที่เกี่ยวข้องหรือมีผลกระทบต่อความปลอดภัยและความน่าเชื่อถือของการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยขอบเขตที่พิจารณากำหนดนี้เพื่อทำความเข้าใจบริบทขององค์กรที่ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล การระบุถึงกิจกรรมที่สำคัญ และระบุประเภทความเสี่ยงที่เกี่ยวข้อง เพื่อนำไปสู่การประเมินความเสี่ยงและบริหารจัดการความเสี่ยงตามขอบเขตต่อไป

3. การทำความเข้าใจบริบท (understand context)

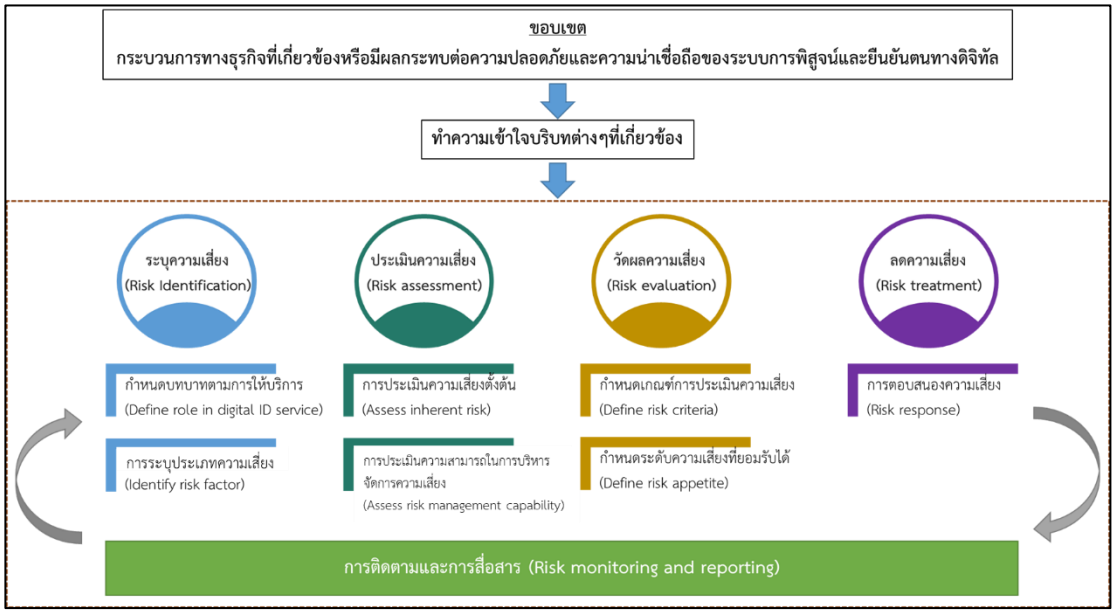
สภาพแวดล้อมของการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลถือว่าเป็นพื้นฐานที่สำคัญ และส่งผลต่อการระบุประเภทความเสี่ยงที่เกี่ยวข้องกับธุรกิจบริการดังกล่าว รวมถึงช่วยกำหนดกลยุทธ์ในการรับมือและตอบสนองกับความเสี่ยง โดยมีการพิจารณาบริบทที่เกี่ยวข้องดังต่อไปนี้

1) วัตถุประสงค์และความต้องการของผู้กำกับดูแล
    1.1) การเสริมสร้างให้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความน่าเชื่อถือและมั่นคงปลอดภัย
    1.2) ต้องการให้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลคำนึงเรื่องความเป็นส่วนตัว การใช้งานข้อมูลส่วนบุคคลเท่าที่จำเป็น และมีการควบคุมดูแลข้อมูลอย่างเหมาะสม
    1.3) ลดความเสี่ยงจากการปลอมแปลงตัวตน
    1.4) ต้องการให้ระบบการพิสูจน์และยืนยันตนทางดิจิทัลโปร่งใส สามารถดำเนินการประเมินและตรวจสอบได้
2) วัตถุประสงค์และความต้องการขององค์กรที่ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
    2.1) ต้องป้องกันไม่ให้มีการปลอมแปลงข้อมูลที่อาจจะเกิดขึ้นในระบบการให้บริการ
    2.2) เสริมสร้างการควบคุมภายใน เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นในระบบการให้บริการ
    2.3) สามารถระบุความเสี่ยงด้านธุรกิจทั่วไปได้ นอกเหนือจากความเสี่ยงทางเทคนิค
    2.4) สามารถประยุกต์การประเมินความเสี่ยงที่องค์กรมีอยู่แล้ว มาใช้ในการระบุความเสี่ยงสำหรับระบบการให้บริการ
3) ปัจจัยภายนอกที่อาจส่งผลต่อการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
    3.1) ความก้าวหน้าของเทคโนโลยีที่นำมาใช้ในระบบการให้บริการ
    3.2) สภาพเศรษฐกิจ สังคม และการแข่งขันทางธุรกิจ
    3.3) แนวโน้มของภัยคุกคาม และความเสี่ยงที่อาจเกิดขึ้นในระบบการให้บริการ
    3.4) การดำเนินการของผู้ให้บริการภายนอกที่อาจเกี่ยวข้องกับระบบการให้บริการ
    3.5) ความสามารถในดำเนินการตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

4. การบริหารจัดการความเสี่ยง (risk management)

การบริหารจัดการความเสี่ยงในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่อประเมินฐานะและผลการดำเนินงาน พิจารณาโดยคำนึงถึงผลกระทบจากความเสี่ยงของการประกอบธุรกิจบริการเพื่อกำหนดมาตรการและแผนการบรรเทาผลกระทบที่อาจจะเกิดขึ้นอย่างทันท่วงที ดังนั้น องค์กรจึงต้องเข้าใจและตระหนักถึงความเสี่ยงสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งอาจส่งผลกระทบต่อผู้ที่เกี่ยวข้อง รวมถึงบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมกระบวนการในการบริหารจัดการความเสี่ยงที่สำคัญดังต่อไปนี้

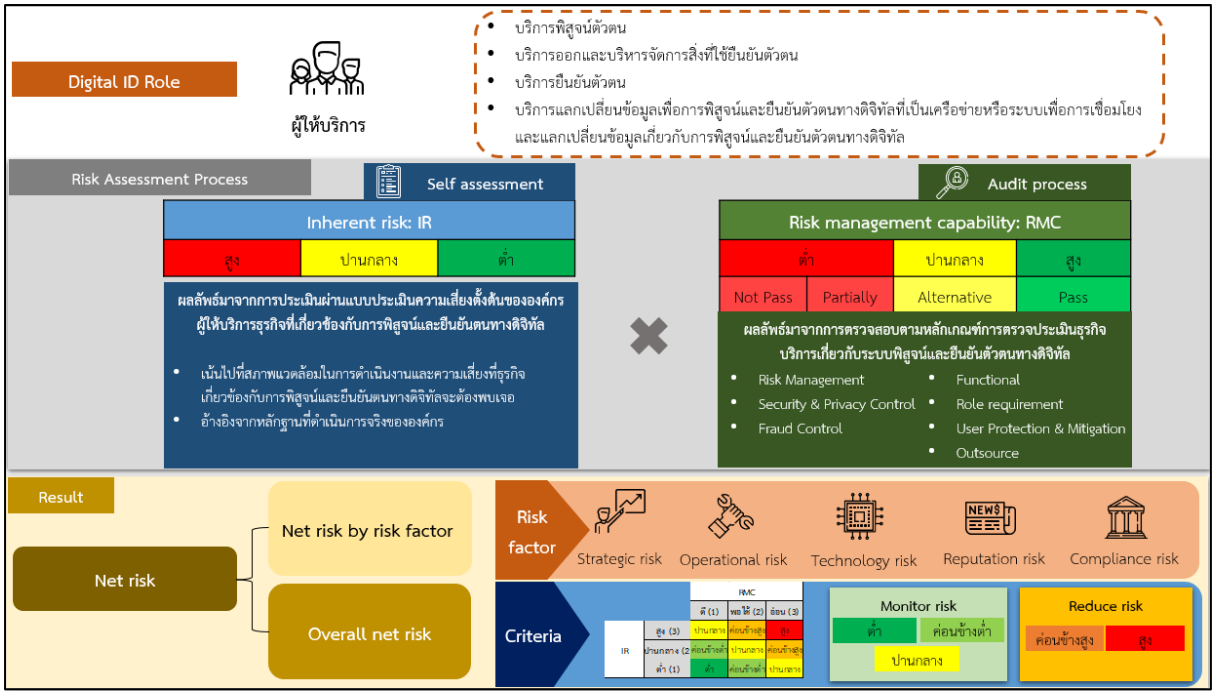
1) การระบุความเสี่ยงที่เกี่ยวข้องกับธุรกิจการพิสูจน์และยืนยันตัวตนทางดิจิทัล (risk identification)
2) การประเมินความเสี่ยง (risk assessment) ทั้งในส่วนของความเสี่ยงตั้งต้นและการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง
3) การวัดผลความเสี่ยงกับเกณฑ์ประเมินความเสี่ยง (risk evaluation)
4) การลดความเสี่ยงหลังจากการประเมิน เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (risk treatment)
5) การติดตามและรายงานผลความเสี่ยงอย่างต่อเนื่อง (risk monitoring and reporting)



รูป 1 กระบวนการบริหารจัดการความเสี่ยง

จากการกำหนดขอบเขตและการทำความเข้าใจบริบทต่าง ๆ ที่เกี่ยวข้อง สำนักงานจึงได้กำหนดกรอบในการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องหรือมีผลกระทบต่อความปลอดภัยและความน่าเชื่อถือสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตนทางดิจิทัล โดยอ้างอิงตามหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตตามที่สำนักงานประกาศกำหนด เพื่อให้ทุกองค์กรที่ให้บริการระบบการพิสูจน์และยืนยันตนทางดิจิทัลมีแนวทางในการประเมิน เพื่อระบุความเสี่ยงตั้งต้นที่องค์กรมี (inherent risk: IR) ที่ใช้รองรับใน

การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมถึงประเมินความสามารถในการบริหารจัดการความเสี่ยงภายในองค์กรเพื่อลดความเสี่ยงที่มีอยู่ (risk management capability: RMC) ซึ่งจากการประเมินทั้ง 2 ส่วนนี้จะนำมาซึ่งความเสี่ยงสุทธิ (net risk) ที่สามารถระบุแนวโน้มความเสี่ยงและหัวข้อที่องค์กรต้องพิจารณาปรับปรุงการควบคุมเพิ่มเติมในอนาคตได้ โดยมีรายละเอียดดังนี้



รูป 2 ภาพรวมการประเมินและบริหารจัดการความเสี่ยงของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

โดยภาพรวมของการประเมินและบริหารจัดการความเสี่ยงของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะมีรายละเอียดขั้นตอนการปฏิบัติที่เป็นไปตามกระบวนการบริหารจัดการความเสี่ยง ดังนี้

4.1 การระบุความเสี่ยง (risk identification)

การระบุความเสี่ยงที่เกี่ยวข้องกับธุรกิจการพิสูจน์และยืนยันตัวตนทางดิจิทัล ประกอบด้วยกิจกรรม ดังนี้

4.1.1 กำหนดบทบาทตามลักษณะการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล

สำหรับกิจกรรมการ**ระบุความเสี่ยง จะเริ่มต้นด้วยการกำหนดบทบาทตามลักษณะการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยอ้างอิงจากบริการที่องค์กรได้ให้บริการกับทางผู้ใช้บริการ ซึ่ง**จากการกำหนดขอบเขตในการประเมินและบริหารจัดการความเสี่ยงในเบื้องต้นทำให้สามารถแจกแจงบทบาทที่สำคัญที่จะเกิดขึ้นจากการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ดังต่อไปนี้

1) บริการพิสูจน์ตัวตน ซึ่งครอบคลุมกระบวนการหลัก 3 กระบวนการ ได้แก่ กระบวนการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล กระบวนการตรวจสอบความถูกต้องแท้จริงและความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และกระบวนการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น
2) บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ครอบคลุมกระบวนการสำคัญ ได้แก่ กระบวนการออกหรือลงทะเบียนชนิดของสิ่งที่ใช้ในการยืนยันตัวตน และกระบวนการ

บริหารจัดการสิ่งที่ใช้ในการยืนยันตัวตนซึ่งเป็นการการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน รวมถึงบริหารจัดการการใช้งานสิ่งที่ใช้ยืนยันตัวตน

3) บริการยืนยันตัวตน อันเป็นกระบวนการยืนยันอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้น

4) บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่เป็นเครือข่ายหรือระบบเพื่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งเป็นบริการเพื่อการเชื่อมโยงระหว่างผู้รับใบอนุญาตกับผู้ประสงค์จะอาศัยการพิสูจน์และยืนยันตัวตนหรือผู้ที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่อแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล

4.1.2 ระบุประเภทความเสี่ยง (Identify risk factor)

เป็นการพิจารณาปัจจัยความเสี่ยงในด้านต่าง ๆ ที่สามารถระบุความเสี่ยงหรือคาดการณ์เหตุการณ์ที่อาจจะเกิดขึ้นจากการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งจะทำให้องค์กรเสียคุณค่าหรือขัดขวางทำให้องค์กรทำงานไม่บรรลุผลสำเร็จ โดยเบื้องต้นความเสี่ยงที่ระบุสำหรับกรอบการประเมินนี้ จำแนกออกเป็น 5 ด้าน ดังนี้

1) **ความเสี่ยงด้านกลยุทธ์ (strategic risk)** หมายถึง ความเสี่ยงของการสูญเสียที่เกิดขึ้นจากการตัดสินใจทางธุรกิจที่ไม่พึงประสงค์ การตัดสินใจทางธุรกิจที่ไม่ดี หรือการไม่ตอบสนองต่อการเปลี่ยนแปลงในอุตสาหกรรมและสภาพแวดล้อมในการดำเนินงาน ทั้งนี้ ความเสี่ยงด้านกลยุทธ์สำหรับผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความคล้ายคลึงกับความเสี่ยงขององค์กรทั่วไป โดยมีปัจจัยที่ต้องคำนึงถึง เช่น นโยบาย แผนกลยุทธ์ และการจัดสรรงบประมาณ อิทธิพลในการตัดสินใจเชิงกลยุทธ์ การบริหารความเสี่ยงในระดับองค์กร เป็นต้น

2) **ความเสี่ยงด้านการปฏิบัติการ (operational risk)** หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก เช่น ความเสี่ยงจากการฉ้อโกงโดยบุคคลภายในและบุคคลภายนอก ความเสี่ยงจากการขัดข้องหรือหยุดชะงักของระบบงาน ความเสี่ยงจากแนวปฏิบัติเกี่ยวกับผู้ใช้บริการ การให้บริการและดำเนินธุรกิจ

3) **ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk)** หมายถึง ความเสี่ยงของผลลัพธ์ที่ไม่พึงประสงค์ ความเสียหาย การสูญเสีย การละเมิด ความล้มเหลวหรือการหยุดชะงักใดๆ ที่อาจเกิดขึ้นจากการใช้หรือการพึ่งพาฮาร์ดแวร์ คอมพิวเตอร์ ซอฟต์แวร์ อุปidกรณ์ ระบบ แอปพลิเคชัน และเครือข่าย ความเสี่ยงนี้มักเกี่ยวข้องกับข้อบกพร่องของระบบ ข้อผิดพลาดในการประมวลผล ข้อบกพร่องของซอฟต์แวร์ ข้อผิดพลาดในการทำงาน ความล้มเหลวของฮาร์ดแวร์ ความล้มเหลวของระบบ ความไม่เพียงพอของความจุ ช่องโหว่ของเครือข่าย จุดอ่อนในการควบคุม ข้อบกพร่องด้านความปลอดภัย การโจมตีที่เป็นอันตราย เหตุการณ์การเจาะระบบ โดยทั่วไปความเสี่ยงด้านเทคโนโลยีสำหรับผู้ประกอบธุรกิจบริการเกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล ตัวอย่างเช่น ภัยคุกคามทางไซเบอร์ การรั่วไหลของข้อมูล รวมถึงข้อมูลอ่อนไหวซึ่ง

มักเป็นองค์ประกอบสำคัญในธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

4) **ความเสี่ยงด้านชื่อเสียงขององค์กร (reputation risk)** หมายถึง ความเสี่ยงที่ทำให้การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้รับผลกระทบทางลบจากสังคม ส่งผลให้สูญเสียชื่อเสียงและความน่าเชื่อถือในการให้บริการ ตัวอย่างเช่น การเปิดเผยข้อมูลส่วนบุคคลของผู้ให้บริการโดยไม่ได้ตั้งใจ

5) **ความเสี่ยงด้านการปฏิบัติตามหลักเกณฑ์ (compliance risk)** หมายถึง ความเสี่ยงที่เกิดจากการที่ผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลไม่สามารถปฏิบัติงานสอดคล้องตามที่กฎหมาย กฎระเบียบหรือมาตรฐานที่เกี่ยวข้องกับการประกอบธุรกิจบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลกำหนด ทั้งนี้รวมถึงมาตรฐานสากลที่กฎหมายหรือกฎระเบียบอ้างถึงด้วย เช่น การไม่ปฏิบัติตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

ทั้งนี้ ประเภทความเสี่ยงทั้ง 5 ด้านข้างต้น จะถูกนำไปพิจารณาในการประเมินความเสี่ยงตั้งต้นเพื่อระบุความเสี่ยงตั้งต้นที่องค์กรมี (Inherent risk) ซึ่งแบ่งระดับความเสี่ยงได้ 3 ระดับ ประกอบด้วย

- ระดับต่ำ
- ระดับปานกลาง
- ระดับสูง

เช่นเดียวกับการประเมินความสามารถในการบริหารจัดการความเสี่ยงภายในองค์กรเพื่อลดความเสี่ยงที่มีอยู่ (Risk management capability) ซึ่งแบ่งระดับการควบคุมเป็น 3 ระดับ ประกอบด้วย

- ระดับสูง
- ระดับปานกลาง
- ระดับต่ำ

สำหรับคำอธิบายเพื่อให้ความชัดเจนเกี่ยวกับการแบ่งระดับความเสี่ยงและการประเมินความสามารถในการบริหารจัดการความเสี่ยงดังกล่าว สามารถศึกษาได้ตามรายละเอียดที่ปรากฏใน ภาคผนวก ก

4.2 การประเมินความเสี่ยง (risk assessment)

สำหรับกรอบในการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องหรือมีผลกระทบต่อความปลอดภัย ความน่าเชื่อถือของการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล แบ่งการประเมินออกเป็น 2 ส่วนประกอบไปด้วย (1) การประเมินความเสี่ยงตั้งต้น (inherent risk: IR) (2) การประเมินความสามารถในการบริหารจัดการความเสี่ยง (risk management capability: RMC) ซึ่งเมื่อได้ผลการประเมินทั้งสองส่วนแล้ว จะนำผลการประเมินทั้งสองส่วนมาคำนวณเพื่อให้ได้ค่าความเสี่ยงสุทธิ (net risk) ซึ่งเป็นค่าความเสี่ยงในภาพรวมขององค์กร

4.2.1 การประเมินความเสี่ยงตั้งต้น (inherent risk: IR)

ความเสี่ยงตั้งต้นเป็นความเสี่ยงที่มีอยู่ขององค์กร ซึ่งผู้ประกอบธุรกิจบริการที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะต้องพบเจอ ซึ่งความเสี่ยงดังกล่าวอาจก่อให้เกิดความสูญเสียจากปัจจัยภายในและภายนอกต่าง ๆ โดยจะเน้นไปที่ประเภทความเสี่ยงทั้ง 5 ด้านตามที่ระบุไว้ในหัวข้อที่ 4.1.2

Inherent Risk Factors					
Strategic	Operational	Technology	Reputation	Compliance	Total of IR

สำหรับการประเมินความเสี่ยงตั้งต้น หรือ IR จะใช้รูปแบบการประเมินตนเอง (self-assessment) เพื่อให้มีความเข้าใจถึงสภาพแวดล้อมในการประกอบธุรกิจบริการ รวมถึงผลกระทบต่อระดับความเสี่ยงซึ่งเป็นผลจากสภาพแวดล้อมดังกล่าว เข้าใจปัจจัยที่ก่อให้เกิดความเสี่ยงต่อองค์กร รวมถึงเป้าหมายขององค์กร ลักษณะการดำเนินการ รวมถึงโครงสร้างพื้นฐานระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนการประกอบธุรกิจบริการ โดยอ้างอิงจากหลักฐานที่ดำเนินการจริงขององค์กรซึ่งจะสะท้อนให้เห็นถึงโอกาสการเกิดหรือผลกระทบที่อาจจะเกิดเหตุการณ์ความเสี่ยงได้ในอนาคต ทั้งนี้ มีการจัดแบ่งผลการประเมินออกเป็น 3 ระดับ ได้แก่ ระดับต่ำ ระดับปานกลาง และระดับสูง ซึ่งจะมีการกำหนดรายละเอียดของเกณฑ์เพิ่มเติมในหัวข้อ 4.3.1

ทั้งนี้ สำนักงานได้จัดเตรียมเอกสารสำหรับให้องค์กรนำไปใช้ในการประเมินตนเองสำหรับการประเมินความเสี่ยงตั้งต้น ซึ่งประกอบด้วยชุดคำถามสำหรับการประเมินความเสี่ยงตั้งต้นที่สอดคล้องกับประเภทความเสี่ยงทั้ง 5 ด้าน และแนวทางการพิจารณาซึ่งองค์กรสามารถใช้เป็นแนวทางในการพิจารณาข้อมูลหลักฐานการดำเนินงานขององค์กรเองสำหรับการประเมินความเสี่ยงตามชุดคำถามเพื่อประกอบการตัดสินใจในการเลือกระดับความเสี่ยงต่าง ๆ รวมถึงได้แบ่งการประเมินในบางหัวข้อเพื่อระบุความเสี่ยงเฉพาะด้าน โดยมีการแบ่งคำถามระหว่าง “หน่วยงานที่เปิดให้บริการด้าน Digital ID แล้ว” กับ “หน่วยงานที่ยังไม่เปิดให้บริการด้าน Digital ID” และมีแบ่งคำถามตามลักษณะการให้บริการของหน่วยงานที่ประเมิน ซึ่งหน่วยงานที่ให้บริการในแต่ละลักษณะมีจำนวนข้อที่ต้องประเมินดังต่อไปนี้

คำถามสำหรับการประเมินความเสี่ยงตั้งต้น	จำนวนข้อ
1.ชุดคำถามทั่วไป ซึ่งผู้ประกอบธุรกิจบริการในทุกลักษณะบริการต้องตอบคำถามดังกล่าว	60 ข้อ
2.ชุดคำถามเฉพาะตามลักษณะบริการ	
2.1 บริการพิสูจน์ตัวตน	คำถามเพิ่มเติม 3 ข้อ
2.2 บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และ/หรือ บริการยืนยันตัวตน	คำถามเพิ่มเติม 3 ข้อ
2.3 บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล	คำถามเพิ่มเติม 2 ข้อ

คำถามในแบบสอบถามประเมินตนเอง (self-assessment) สามารถเชื่อมโยงไปยังประเภทความเสี่ยงได้ เพื่อสามารถระบุได้ว่าคำถามในแต่ละข้อต้องการจะสอบถามถึงความเสี่ยงในด้านใดและสะท้อนให้เห็นถึงความเสี่ยงในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งผู้ประเมินสามารถดำเนินการประเมินโดยใช้ชุดคำถามและรายละเอียดตามแบบประเมินสำหรับการบริหารจัดการความเสี่ยงธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

4.2.2 การประเมินความสามารถในการบริหารจัดการความเสี่ยง (risk management capability: RMC)

ในส่วนนี้เป็นการประเมินความสามารถในการบริหารจัดการความเสี่ยงที่ผู้ประกอบธุรกิจบริการที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีอยู่ โดยองค์กรต้องมีการประเมินและบริหารจัดการความเสี่ยงเพื่อควบคุมให้อยู่ในระดับที่องค์กรสามารถยอมรับได้ โดยจะเน้นไปที่ประเภทความเสี่ยงทั้ง 5 ด้าน ตามที่ระบุไว้ในหัวข้อที่ 4.1.2

Risk management capability					
Strategic	Operational	Technology	Reputation	Compliance	Total of RMC

การประเมินในส่วนนี้จะใช้รูปแบบการตรวจประเมินโดยผู้ตรวจสอบอิสระ (internal/external auditor) โดยตรวจประเมินการควบคุมตามลักษณะการให้บริการที่ขอรับใบอนุญาตตามที่ระบุในหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตที่สำนักงานประกาศกำหนด ประกอบไปด้วยหัวข้อดังต่อไปนี้

1) หลักเกณฑ์การบริหารและจัดการความเสี่ยงในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
2) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ
3) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
4) หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ
5) หลักเกณฑ์ตามลักษณะของการให้บริการ
6) หลักเกณฑ์การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ
7) หลักเกณฑ์การใช้บริการจากผู้รับดำเนินการแทน (ถ้ามี)

ทั้งนี้ รายละเอียดการควบคุมแต่ละข้อจะระบุประเภทความเสี่ยงที่เกี่ยวข้อง รวมถึงแบ่งระดับผลการตรวจประเมินออกเป็นระดับการควบคุมประเภทต่าง ๆ ซึ่งสามารถศึกษารายละเอียดระดับการควบคุมกับระดับความสามารถในการบริหารจัดการความเสี่ยง (RMC) ได้ตามตารางด้านล่าง

ระดับความสามารถในการบริหารจัดการความเสี่ยง (RMC)	ระดับการควบคุม
ต่ำ (3)	ผลการประเมิน : **Not Pass** คำอธิบาย :ไม่ผ่านเกณฑ์ที่กำหนดทั้งหมด
	ผลการประเมิน : **Partially Pass** คำอธิบาย : ผ่านเกณฑ์ที่กำหนดบางส่วน

ระดับความสามารถในการบริหารจัดการความเสี่ยง (RMC)	ระดับการควบคุม
ปานกลาง (2)	ผลการประเมิน : **Alternative Control** คำอธิบาย : ไม่มีการควบคุมที่พึงมีตามเกณฑ์ที่กำหนด แต่มีการควบคุมอื่นที่เทียบเท่าทดแทน
สูง (1)	ผลการประเมิน : **Pass** คำอธิบาย : ผ่านเกณฑ์ที่กำหนดทั้งหมด

4.2.3 ความเสี่ยงสุทธิ (net risk)

ผลลัพธ์ที่ได้จากการประเมินความเสี่ยงตั้งต้น (IR) และความสามารถในการบริหารจัดการความเสี่ยง (RMC) จะถูกนำมาพิจารณาประกอบกัน และแสดงออกมาในรูปของความเสี่ยงสุทธิ (net risk) ซึ่งแสดงให้เห็นถึงแนวโน้มความเสี่ยงและหัวข้อที่องค์กรต้องพิจารณาปรับปรุงการควบคุมเพิ่มเติมในอนาคต ซึ่งความเสี่ยงสุทธิที่ได้จะมีผลลัพธ์ออกมาเป็น 2 แบบ ดังนี้

รูป 3 วิธีการคำนวณความเสี่ยงสุทธิ (net risk)

1) **ความเสี่ยงสุทธิแบ่งแยกตามประเภทความเสี่ยง (Net risk by risk factor)** ได้มาจากการประเมินความเสี่ยงตั้งต้น (IR) ตามประเภทความเสี่ยงแต่ละด้าน มาจับคู่กับความสามารถในการบริหารจัดการความเสี่ยง (RMC) ตามประเภทความเสี่ยงแต่ละด้าน โดยผลลัพธ์ที่ได้คือความเสี่ยงสุทธิ (net risk) ที่แบ่งแยกตามประเภทของความเสี่ยงทั้ง 5 ด้าน ซึ่งสามารถนำผลลัพธ์นี้เข้ากระบวนการตอบสนองความเสี่ยงเพื่อวิเคราะห์ว่าความเสี่ยงประเภทใดมีผลกระทบต่อองค์กรมากที่สุด รวมถึงใช้ในการติดตามและรายงานผลความเสี่ยงได้

2) **ความเสี่ยงสุทธิขององค์กร (Overall net risk)** ได้มาจากการประเมินความเสี่ยงตั้งต้น (IR) ขององค์กร มาจับคู่กับความสามารถในการบริหารจัดการความเสี่ยง (RMC) ขององค์กร

ทั้งนี้ ขั้นตอนการได้มาซึ่งความเสี่ยงสุทธิ (Net risk) ทั้ง 2 แบบ จะมีตัวอย่างอธิบายโดยละเอียดในหัวข้อ 4.3.1

4.3 การวัดผลความเสี่ยงกับเกณฑ์ประเมินความเสี่ยง (risk evaluation)

การวัดผลความเสี่ยงกับเกณฑ์ประเมินความเสี่ยงเป็นการวัดระดับความเสี่ยงเพื่อพิจารณาความสำคัญของความเสี่ยงที่มีอยู่โดยวัดผลความเสี่ยงเปรียบเทียบกับเกณฑ์การประเมินความเสี่ยงที่กำหนดเพื่อใช้พิจารณาระดับความเสียหายหรือความรุนแรงที่อาจจะเกิดขึ้น และสามารถนำความเสี่ยงที่พบมาพิจารณาหรือหาแนวทางการลดความเสี่ยงที่เกินกว่าระดับความเสี่ยงที่ยอมรับได้ ซึ่งในการการวัดผลความเสี่ยงกับเกณฑ์ประเมินความเสี่ยงจำเป็นต้องมีการดำเนินการดังต่อไปนี้

4.3.1 กำหนดเกณฑ์การประเมินความเสี่ยง (define risk criteria)

จากการประเมินความเสี่ยงในหัวข้อ 4.2 จำเป็นจะต้องมีการระบุเกณฑ์การประเมินความเสี่ยงต่าง ๆ ซึ่งประกอบไปด้วย

1) **เกณฑ์การประเมินผลความเสี่ยงตั้งต้น (Inherent risk criteria)** จะถูกแบ่งออกเป็น 3 ระดับ โดยมีรายละเอียดในระดับภาพรวมขององค์กรดังต่อไปนี้

ความเสี่ยงตั้งต้น (IR)	ระดับช่วง (IR)	รายละเอียด
สูง (3)	2.31 – 3.00	**องค์กรมีความเสี่ยงตั้งต้นสูง** อันเนื่องมาจากลักษณะการดำเนินงานและการให้บริการกับลูกค้าจำนวนมากมีโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เชื่อมต่อกับองค์กรภายนอก หรือมีโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศภายในที่มีความซับซ้อน โดยมีผลมาจากการนำเทคโนโลยีใหม่ ๆ เข้ามาดำเนินการ เช่น เทคโนโลยีปัญญาประดิษฐ์ ซึ่งอาจทำให้เกิดความเสี่ยงที่ไม่เคยพบเจอมาก่อนเกิดขึ้นได้หรือองค์กรมีปัจจัยด้านบุคลากรภายในองค์กรที่มีการเปลี่ยนแปลงปล่อยครั้งส่งผลกระทบต่อการดำเนินงานในปัจจุบันหรืออาจรวมถึงองค์กรไม่สามารถปฏิบัติตาม ระเบียบ กฎหมาย หรือแนวทางปฏิบัติส่งผลให้สภาพแวดล้อมในการดำเนินธุรกิจเกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลมีความเสี่ยงอยู่ในระดับที่สูง
ปานกลาง (2)	1.71 – 2.30	**องค์กรมีความเสี่ยงตั้งต้นปานกลาง** อันเนื่องมาจากลักษณะการดำเนินงานและการให้บริการกับลูกค้าจำนวนหนึ่ง โดยมีโครงสร้างพื้นฐานด้านสารสนเทศที่มีทั้งระบบปิดและเชื่อมต่อกับองค์กร ภายนอก องค์กรมีระดับไม่ซับซ้อนมาก มีการประยุกต์เทคโนโลยีใหม่ๆ มาใช้งานบ้าง แต่ไม่ถึงเป็นระบบหลักที่ใช้เพื่อการพิสูจน์และยืนยันตน มีการเปลี่ยนแปลงบุคลากรแต่ไม่ส่งผลกระทบต่อการดำเนินงานมาก ทั้งนี้ องค์กรสามารถที่จะปฏิบัติตามระเบียบ กฎหมาย หรือ แนวทางปฏิบัติ ส่วนใหญ่ได้แต่ยังมีบางหัวข้อที่อยู่ระหว่างการดำเนินงานแก้ไขส่งผลให้ สภาพแวดล้อมในการดำเนินธุรกิจเกี่ยวข้องกับการพิสูจน์และยืนยันตนทาง ดิจิทัลมีความเสี่ยงอยู่ในระดับปานกลาง

ความเสี่ยงตั้งต้น (IR)	ระดับช่วง (IR)	รายละเอียด
ต่ำ (1)	1.00 – 1.70	**องค์กรมีความเสี่ยงตั้งต้นต่ำ** อันเนื่องมาจากลักษณะการดำเนินงานและการให้บริการกับลูกค้าที่ไม่มากโครงสร้างภายในขององค์กรเป็นขนาดเล็กไม่ซับซ้อนรวมไปถึงโครงสร้างพื้นฐาน ด้านสารสนเทศส่วนมากดำเนินการในเครือข่ายที่เป็นระบบปิด บุคลากรภายในองค์กรมีการเปลี่ยนแปลงน้อยมากจนไปถึงไม่มีการเปลี่ยนแปลง หรืออาจรวมถึงองค์กรสามารถดำเนินการตามระเบียบ กฎหมาย หรือ แนวทางปฏิบัติครบถ้วนส่งผลให้สภาพแวดล้อมในการดำเนินธุรกิจเกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลมีความเสี่ยงอยู่ในระดับต่ำ

โดยในดำเนินการประเมินตนเอง (Self-assessment) สามารถอ้างอิงจากหลักฐานการดำเนินงานขององค์กรเพื่อประกอบการตัดสินใจในการเลือกระดับความเสี่ยงต่าง ๆ จากนั้นจะสามารถสรุปผลความเสี่ยงตั้งต้นตามประเภทความเสี่ยงทั้ง 5 ด้าน โดยระบุถึงคะแนนความเสี่ยงตั้งต้นและระดับความเสี่ยงตั้งต้น (IR) ได้ตามตัวอย่างตารางด้านล่าง

ตัวอย่างการสรุปผลระดับความเสี่ยงตั้งต้นแยกตามประเภทความเสี่ยง

ประเภทความเสี่ยง	คะแนนความเสี่ยงตั้งต้น	ระดับความเสี่ยงตั้งต้น (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 *ตัวเลขในตารางเป็นเพียงตัวอย่างเพื่อแสดงให้เห็นรูปแบบในการประเมินเท่านั้น*

ทั้งนี้ ระดับความเสี่ยงตั้งต้น (IR) ขององค์กรในภาพรวมสามารถพิจารณาได้โดยการนำคะแนนความเสี่ยงตั้งต้นของแต่ละประเภทมาเฉลี่ยและเทียบกับระดับช่วงความเสี่ยงตั้งต้น ซึ่งมีผลตัวอย่างตามตารางด้านล่าง

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

หมายเหตุ *ในการดำเนินการจริงแบบประเมินสำหรับการบริหารจัดการความเสี่ยงธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะดำเนินการสรุปผลให้โดยอัตโนมัติเมื่อผู้ประเมินดำเนินการตอบคำถามประเมินตนเองครบถ้วน*

2) เกณฑ์การประเมินความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability criteria) จะถูกแบ่งออกเป็น 3 ระดับ โดยมีรายละเอียดในระดับภาพรวมขององค์กรดังต่อไปนี้

ความสามารถในการบริหารจัดการความเสี่ยง (RMC)	ระดับช่วง (RMC)	รายละเอียด
สูง (3)	2.31 – 3.00	ไม่มีการปฏิบัติตามหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล หรือไม่มีกระบวนการตามประกาศที่ชัดเจนซึ่งนำไปสู่ความเสียหายอย่างร้ายแรงต่อ ระบบหรือกรณีที่ไม่ปฏิบัติตามหลักเกณฑ์ฯหลายหัวข้อรวมกันซึ่งเมื่อพิจารณา แล้วมีผลกระทบต่อระบบการจัดการโดยรวม
ปานกลาง (2)	1.71 – 2.30	มีการดำเนินการตามประกาศหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลแล้ว แต่พบประเด็นบางเรื่องที่หากปล่อยละเลยไว้อาจนำไปสู่ความไม่สอดคล้องใน อนาคตได้ควรต้องดำเนินการปรับปรุงหรือพัฒนากระบวนการให้ดียิ่งขึ้นเพื่อ ป้องกันไม่ให้ เกิดการละเลยซึ่งอาจนำไปสู่ความไม่สอดคล้องในอนาคต
ต่ำ (1)	1.00 – 1.70	มีการปฏิบัติตามหลักเกณฑ์ว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลครบถ้วน มีกระบวนการที่ชัดเจนรวมถึงมีการวัดผลอย่างต่อเนื่อง

โดยองค์กรดำเนินการตรวจประเมินความสามารถในการบริหารจัดการความเสี่ยงจากผู้ตรวจสอบอิสระ (Internal/External auditor) ตามหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตตามที่สำนักงานประกาศกำหนด โดยใช้แบบประเมินสำหรับการบริหารจัดการความเสี่ยงธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในการบันทึกผลการตรวจประเมิน ซึ่งจะต้องอธิบายเหตุผลประกอบผลการประเมินทุกข้อตามลักษณะการให้บริการ

จากผลการตรวจประเมินสามารถสรุปความสามารถในการบริหารจัดการความเสี่ยงของประเภทความเสี่ยงทั้ง 5 ด้าน ซึ่งจะระบุถึงคะแนนความสามารถในการบริหารจัดการความเสี่ยง และระดับความสามารถในการบริหารจัดการความเสี่ยง (RMC) ได้ตามตัวอย่างตารางด้านล่าง

ตัวอย่างการสรุปผลระดับความสามารถในการบริหารจัดการความเสี่ยง

ประเภทความเสี่ยง	คะแนนความสามารถในการบริหารจัดการความเสี่ยง	ระดับความสามารถในการบริหารจัดการความเสี่ยง (RMC)
1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)	**1.50**	สูง
2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)	**1.30**	สูง
3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)	**1.80**	ปานกลาง
4. ความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation Risk)	**1.85**	ปานกลาง
5. ความเสี่ยงทางด้านการปฏิบัติตามหลักเกณฑ์ (Compliance Risk)	**1.80**	ปานกลาง

หมายเหตุ *ตัวเลขในตารางเป็นเพียงตัวอย่างเพื่อแสดงให้เห็นรูปแบบในการประเมินเท่านั้น*

ทั้งนี้ ระดับความสามารถในการบริหารจัดการความเสี่ยง (RMC) ขององค์กรในภาพรวมสามารถพิจารณาได้โดยการนำคะแนนความสามารถในการบริหารจัดการความเสี่ยงของแต่ละประเภทนำมาเฉลี่ยและเทียบระดับช่วงความสามารถในการบริหารจัดการความเสี่ยงมีผลตัวอย่างตามตารางด้านล่าง

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**	สูง

หมายเหตุ *ในการดำเนินการจริงแบบประเมินสำหรับการบริหารจัดการความเสี่ยงธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะดำเนินการสรุปผลให้โดยอัตโนมัติเมื่อผู้ประเมินดำเนินการบันทึกผลการตรวจประเมินครบถ้วน*

3) เกณฑ์การประเมินความเสี่ยงสุทธิ (Net risk criteria) เป็นการนำผลของการประเมินความเสี่ยงตั้งต้น (IR) กับผลของการประเมินความสามารถในการบริหารจัดการความเสี่ยง (RMC) มาประเมินร่วมกัน ซึ่งจะสามารถระบุความเสี่ยงสุทธิทั้งในระดับภาพรวมขององค์กรและความเสี่ยงสุทธิในแต่ละประเภทความเสี่ยงได้ โดยจะมีการแบ่งระดับออกเป็น 5 ระดับ ตามตารางแสดงระดับความเสี่ยงสุทธิ (Net risk) ดังต่อไปนี้

		RMC		
		สูง (1)	**ปานกลาง(2)**	**ต่ำ (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

จากการดำเนินการประเมินผลทั้งในส่วนของความเสี่ยงตั้งต้น (IR) และความสามารถในการบริหารจัดการความเสี่ยง (RMC) ภาพรวมของการประเมินจะสามารถสรุปผลเป็นความเสี่ยงสุทธิ (Net risk) ได้ 2 รูปแบบ คือ

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

โดยการนำผลของความเสี่ยงตั้งต้น (IR) และความสามารถในการบริหารจัดการความเสี่ยง (RMC) มาจัดวางในตารางแสดงระดับความเสี่ยงสุทธิ (Net risk) ซึ่งสามารถสรุปผลได้ตามตัวอย่าง ดังต่อไปนี้

ตัวอย่างการสรุปผลความเสี่ยงสุทธิแยกตามประเภทความเสี่ยง (Net risk by risk factor)

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

ตัวอย่างการสรุปผลความเสี่ยงสุทธิขององค์กร (Overall net risk)

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

4.3.2 ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite)

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

โดย**ระดับความเสี่ยงที่สามารถยอมรับได้ (Risk appetite) คือ ความเสี่ยงสุทธิในระดับที่ต่ำ ค่อนข้างต่ำ และปานกลาง** ซึ่งหากองค์กรมีความเสี่ยงสุทธิมากกว่าระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) องค์กรจำเป็นต้องจัดหาแผนลดความเสี่ยงเพื่อดำเนินการลดความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้ ซึ่งองค์กรต้องระบุแผนดังกล่าวในแบบประเมินสำหรับการบริหารจัดการความเสี่ยงธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

จากตัวอย่างการสรุปผลความเสี่ยงสุทธิแยกตามประเภทความเสี่ยง (Net risk by risk factor) จะเห็นว่าความเสี่ยงด้านชื่อเสียงขององค์กร (Reputation risk) มีความเสี่ยงสุทธิสูงเกินกว่าระดับที่ยอมรับได้ ดังนั้น จึงต้องมีแผนในการดำเนินการลดความเสี่ยงเพื่อลดความเสี่ยงให้ไปอยู่ในระดับที่ต่ำกว่านี้

4.4 การลดความเสี่ยง (Risk treatment)

การลดความเสี่ยงหลังจากการประเมินเพื่อให้อยู่ในระดับที่ยอมรับได้ โดยองค์การสามารถตอบสนองกับความเสี่ยง (Risk response) ได้อยู่ 2 รูปแบบ ประกอบด้วย

4.4.1 ลดความเสี่ยงตั้งต้น

การลดความเสี่ยงตั้งตนที่เกิดขึ้นจากการดำเนินการในปัจจุบันเป็นการพิจารณาจากการดำเนินการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลว่ามีกระบวนการใดที่มีความเสี่ยงสูงบ้างและใช้กลยุทธ์สำหรับการลดความเสี่ยงในการจัดการความเสี่ยงดังกล่าว

ทั้งนี้ กลยุทธ์สำหรับการลดความเสี่ยง (Risk treatment) ที่องค์กรสามารถเลือกนำไปใช้ได้มีอยู่ทั้งหมด 4 รูปแบบซึ่งรายละเอียดมีดังต่อไปนี้

1) การลดความเสี่ยง (Risk Mitigation) องค์กรมีการกำหนดให้มีการบริหารจัดการความเสี่ยงที่รัดกุมยิ่งขึ้น หรือมีกิจกรรมในการควบคุมเพิ่มเติมเพื่อลดโอกาสเกิดหรือผลกระทบจากความเสี่ยงนั้นๆ เช่น การพัฒนาบุคลากร ความชำนาญ การจัดตั้งให้มีนโยบายด้านความปลอดภัยของเทคโนโลยีสารสนเทศ

2) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการหลีกเลี่ยงกิจกรรมหรือสาเหตุที่อาจก่อให้เกิดความเสี่ยง ทั้งนี้ ต้องมั่นใจได้ว่าการหลีกเลี่ยงกิจกรรมดังกล่าวจะไม่กระทบต่อการดำเนินการในส่วนอื่นๆ ด้วย

3) การถ่ายโอนความเสี่ยง (Risk Transfer) เป็นการลดความถี่ในการเกิดหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น โดยกระจายหรือโอนไปยังบุคคลอื่น ตัวอย่างเช่น การจัดหาประกันภัย การร่วมทุนพันธมิตร

4) การยอมรับความเสี่ยง (Risk Acceptance) เป็นการที่ไม่มีการกำหนดกิจกรรมใดๆ เพื่อตอบสนองต่อความเสี่ยงที่อาจเกิดขึ้น โดยผู้บริหารยอมรับผลที่อาจเกิดขึ้นจากความเสี่ยงนั้น ทั้งนี้ผู้ที่สามารถตัดสินใจยอมรับความเสี่ยงจะต้องเป็นผู้บริหารขององค์กรที่มีอำนาจและสามารถพิจารณาความเสี่ยงดังกล่าวว่าควรจะต้องยอมรับความเสี่ยงหรือไม่

4.4.2 ปรับปรุงความสามารถในการบริการจัดการความเสี่ยง

การปรับปรุงความสามารถในการบริหารจัดการความเสี่ยง เพื่อให้สามารถตอบสนองต่อการจัดการความเสี่ยงให้ดียิ่งขึ้นโดยพิจารณาผลการตรวจประเมินจากผู้ตรวจสอบอิสระในหัวข้อที่ได้รับการประเมินในระดับ Not Pass และ Partially Pass และดำเนินการตามตารางด้านล่าง

ผลการประเมิน	การดำเนินการ
Not Pass	องค์กรดำเนินการวิเคราะห์สาเหตุ ผลกระทบที่อาจจะเกิดขึ้น และแนวทางการแก้ไข รวมถึงระบุวันที่ดำเนินการแล้วเสร็จ พร้อมทั้งแนบหรือแสดงหลักฐานการแก้ไขสำหรับหัวข้อที่เกี่ยวข้อง**ภายใน 90 วัน** นับจากหลังตรวจประเมิน
Partially Pass	องค์กรดำเนินการวิเคราะห์สาเหตุ ระบุผลกระทบที่อาจจะเกิดขึ้น และแผนการแก้ไข รวมถึงระบุวันที่คาดว่าจะดำเนินการแล้วเสร็จ สำหรับหัวข้อที่เกี่ยวข้อง **ภายใน 30 วัน** นับจากหลังตรวจประเมิน

กรณีผลการประเมินในระดับ Alternative Control และ Pass ให้องค์กรพิจารณานำส่งเอกสารอ้างอิง (ถ้ามี) หรือตามที่สำนักงานร้องขอ

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

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

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

4.5 การติดตามและรายงานผลความเสี่ยง (Risk monitoring and reporting)

องค์กรจำเป็นจะต้องดำเนินการประเมินความเสี่ยงตั้งต้น (Inherent risk) และความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) เพื่อสรุปผลเป็นความเสี่ยงสุทธิ (Net risk) โดยนำส่งผลการประเมินให้กับสำนักงานเพื่อสอบทาน รวมถึงควรจัดเตรียมข้อมูลสนับสนุนที่เกี่ยวข้องกับการดำเนินการพิสูจน์และยืนยันตัวตนทางดิจิทัลในกรณีที่ทางสำนักงานร้องขอรายละเอียดเพิ่มเติม

นอกจากนี้ องค์กรมีหน้าที่ธำรงรักษาความมั่นคงปลอดภัยและความน่าเชื่อถือของระบบที่อยู่ในความรับผิดชอบโดยต้องดำเนินการลดความเสี่ยงที่เกินกว่าที่จะยอมรับได้ และดำเนินการประเมินความเสี่ยงใหม่อีกครั้งทั้งในส่วนความเสี่ยงตั้งต้น (Inherent risk) และความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability) ตามรอบระยะเวลาที่สำนักงานกำหนดหรือเมื่อมีการเปลี่ยนแปลงภายในระบบหรือองค์กรที่สำคัญ อาทิเช่น การควบรวมกิจการ การเปลี่ยนโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศใหม่ทั้งหมดไปสู่ Cloud เป็นต้น ซึ่งจะต้องส่งเอกสารชุดเดิมที่มีการปรับปรุงแก้ไขแล้วให้ทางสำนักงานอีกครั้งหนึ่ง

5. คำจำกัดความ

คำศัพท์	คำจำกัดความ
ความเสี่ยงตั้งต้น (inherent risk)	ความเสี่ยงที่มีอยู่ของผู้ให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะต้องพบเจอ ทั้งนี้ อาจก่อให้เกิดความสูญเสียจากปัจจัยภายในและภายนอกต่าง ๆ
ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	ความสามารถในการบริหารจัดการความเสี่ยงที่ผู้ให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลมีอยู่ ซึ่งอ้างอิงจากหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตตามที่สำนักงานประกาศกำหนด
ความเสี่ยงสุทธิ (Net risk)	ความเสี่ยงสุทธิที่หลงเหลืออยู่ภายหลังจากประเมินความเสี่ยงตั้งต้น (IR) และความสามารถในการบริหารจัดการความเสี่ยง (RMC) ซึ่งเป็นระดับความเสี่ยงขององค์กรตามประเภทความเสี่ยงทั้ง 5 ด้าน
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

ภาคผนวก ก

: คำอธิบายการแบ่งระดับความเสี่ยงและระดับความสามารถในการบริหารจัดการความเสี่ยง

1. ความเสี่ยงด้านกลยุทธ์ (Strategic risk)

ระดับความเสี่ยงตั้งต้น (inherent risk)	
ต่ำ	ผู้ให้บริการมีการวางแผนด้านนโยบายและกลยุทธ์ที่ช่วยส่งเสริมการบริหารจัดการความเสี่ยงเป็นไปอย่างมีประสิทธิภาพในระยะยาว สะท้อนให้เห็นถึงเป้าหมาย วิสัยทัศน์ จุดแข็ง จุดอ่อน โอกาส และอุปสรรคในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลขององค์กรได้เป็นอย่ างดี ส่งผลให้องค์กรมีความชัดเจนต่อการเปลี่ยนแปลงต่างๆ ที่อาจเกิดขึ้นในอนาคต และมีการสื่อสารด้านนโยบายและกลยุทธ์อย่างทั่วถึงให้กับบุคลากรในองค์กรและบุคคลที่เกี่ยวข้อง รวมถึงองค์กรมีผลกระทบต่อการเปลี่ยนแปลงทั้งในส่วนภายในองค์กร (เช่น การควบรวมบริษัท การเปลี่ยนแปลงตำแหน่ง) หรือภายนอกองค์กร (เช่น ความก้าวหน้าของเทคโนโลยีการพิสูจน์และยืนยันตัวตนทางดิจิทัล พฤติกรรมของผู้ใช้บริการเปลี่ยนแปลง) เพียงเล็กน้อย ไม่ส่งผลกระทบอย่างมีนัยสำคัญกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
ปานกลาง	ผู้ให้บริการมีการวางแผนด้านนโยบายและกลยุทธ์ที่ช่วยส่งเสริมการบริหารจัดการความเสี่ยงโดยสะท้อนให้เห็นถึง เป้าหมาย วิสัยทัศน์ จุดแข็ง จุดอ่อน โอกาส และอุปสรรคในการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลขององค์กร ทั้งนี้บางนโยบายหรือกลยุทธ์ยังอยู่ในระหว่างการตั ดสินใจ ส่งผลให้องค์กรอาจมีการยังไม่มีความชัดเจนต่อการเปลี่ยนแปลงต่าง ๆ ในบางเรื่อง ทั้งนี้มีช่องทางในการสื่อสารด้านนโยบายและกลยุทธ์อย่างทั่วถึงให้กับบุคลากรในองค์กรและบุคคลที่เกี่ยวข้อง รวมถึงองค์กรมีผลกระทบต่อการเปลี่ยนแปลงทั้งในส่วนภายในองค์กร (เช่น การควบรวมบริษัท การเปลี่ยนแปลงตำแหน่ง) หรือภายนอกองค์กร (เช่น ความก้าวหน้าของเทคโนโลยีการพิสูจน์และยืนยันตัวตนทางดิจิทัล พฤติกรรมของผู้ใช้บริการเปลี่ยนแปลง) พอสมควรโดยไม่มีนัยสำคัญ ส่งผลกระทบกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพียงเล็กน้อย
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)	
สูง	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
ปานกลาง	องค์กรมีนโยบาย แผนกลยุทธ์และการจัดสรรงบประมาณที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เช่น การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล การจัดสรรงบประมาณที่สอดคล้องกับเป้าเชิงกลยุทธ์ที่เกี่ยวข้องกับการดำเนินธุรกิจพิสูจน์และยืนยันตัวตนทางดิจิทัล) ทั้งนี้พบว่านโยบาย แผนกลยุทธ์และการจัดสรรงบประมาณบางหัวข้ออาจอยู่ระหว่างการตัดสินใจและการสื่อสาร ซึ่งอาจก่อให้เกิดความไม่ชัดเจนเล็กน้อยในเรื่องแนวทางการดำเนินงานขององค์กร มีการทบทวนประสิทธิภาพในการบังคับใช้นโยบายและปรับปรุงให้ดียิ่งขึ้น แต่ดำเนินการไม่สม่ำเสมอ มีการสื่อสารให้บุคลากรในองค์กรและบุคคลที่เกี่ยวข้องถึงการเปลี่ยนแปลงในด้านนโยบายหรือแผนกลยุทธ์ มีคณะกรรมการที่มีบทบาทหน้าที่ชัดเจน มีประสบการณ์และคุณสมบัติครบถ้วนโดยอาจไม่เข้าร่วมในการตัดสินใจทุกครั้ง แต่ไม่มีผลกระทบที่มีนัยสำคัญ ไม่มีผู้ใดมีอำนาจครอบงำผู้อื่น รวมถึงดูแลรับผิดชอบความเสี่ยงทั้งหมดที่อาจเกิดขึ้นภายในองค์กร นอกจากนี้องค์กรยังมีกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยนโยบายและแนวทางปฏิบัติในเรื่องการจัดการความเสี่ยงนั้นครอบคลุมทุกกระบวนการตั้งแต่การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามทบทวนความเสี่ยง และ

	การรายงานความเสี่ยง โดยมีการดำเนินการอย่างต่อเนื่องเป็นประจำ แต่ยังไม่สามารถระบุความเสี่ยงได้ครบถ้วน ซึ่งอาจส่งผลให้ไม่สามารถ แก้ไขจัดการความเสี่ยงได้ครบถ้วน และอาจเกิดเหตุการณ์ภายในระบบ Digital ID ที่คาดไม่ถึง
ต่ำ	องค์กรยังไม่มีนโยบาย แผนกลยุทธ์และการจัดสรรงบประมาณที่เกี่ยวข้องกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เช่น การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล การจัดสรรงบประมาณที่สอดคล้องกับเป้าเชิงกลยุทธ์ที่เกี่ยวข้องกับการดำเนินธุรกิจพิสูจน์และยืนยันตัวตนทางดิจิทัล) อาจทำให้เป้าหมายในการดำเนินธุรกิจขององค์กรไม่ชัดเจนส่งผลให้การดำเนินการธุรกิจไม่สามารถบรรลุตามเป้าหมายได้และมีผลกระทบต่อองค์กร ไม่มีการทบทวนประสิทธิภาพในนโยบาย ส่งผลให้ไม่สามารถพัฒนาระบบการทำงานให้ดียิ่งขึ้นได้ มีคณะกรรมการที่มีบทบาทหน้าไม่ชัดเจน หรือมีประสบการณ์และคุณสมบัติไม่เพียงพอต่อการทำงานในหน้าที่ที่ได้รับมอบหมาย ไม่เข้าร่วมในการตัดสินใจทุกครั้งบ่อยครั้ง และมีผู้มีอำนาจครอบงำผู้อื่น ส่งผลให้ไม่สามารถพัฒนาทิศทางกลยุทธ์และเพิ่มประสิทธิภาพในการปฏิบัติตามกลยุทธ์และในการดำเนินงานขององค์กรได้ 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 ทำให้มีการใช้งานข้อมูลส่วนบุคคลและดำเนินการที่ซับซ้อนพอประมาณ ทั้งนี้ปริมาณบัญชีผู้ใช้งานระบบ Digital ID และจำนวนจุดที่ให้บริการยังมีปริมาณอยู่ในระดับที่ไม่มีนัยสำคัญอันส่งผลกระทบหากมีความผิดพลาดในการดำเนินการดูแลและพัฒนาระบบ มีการหยุดชะงักในการให้บริการ รวมไปถึงมีการทุจริตเกิดขึ้นในระบบ แต่ยังอยู่ในระดับที่สามารถรับมือได้อย่างรวดเร็ว ทั้งนี้องค์กรพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือพบเหตุการณ์การทุจริต หรือการฉ้อโกงที่เกี่ยวกับการให้บริการ Digital ID โดยมีผลกระทบในระดับกลางขึ้นไปบ้าง แต่ไม่ถึงพบเหตุการณ์ที่ร้ายแรงที่ส่งผลกระทบต่อการดำเนินธุรกิจขององค์กร

	จำนวนของพนักงานมีปริมาณพอใช้ อัตราการลาออกของพนักงานอยู่ในระดับปานกลางในรอบ 12 เดือนที่ผ่านมา ซึ่งพนักงานที่ลาออกนั้นส่วนมากอาจมีสิทธิ์สูงภายในระบบ 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 มีการใช้ระดับความน่าเชื่อถือของการพิสูจน์ตัวตนและการยืนยันตัวตนระดับสูงทำให้มีการใช้งานข้อมูลส่วนบุคคลที่สำ คัญและดำเนินการที่ซับซ้อน 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)	
สูง	องค์กรมีการกำหนดแผนในการป้องกันและจัดการการฉ้อโกงหรือการทุจริต ซึ่งมีเนื้อหาที่เกี่ยวข้องกับการบริหารจัดการบุคลากร วิธีการส่งเสริมและควบคุมไม่ให้เกิดการฉ้อโกงหรือทุจริต กลไกในติดตามและจัดการกับเหตุที่เกิดขึ้น รวมไปถึงขั้นตอนการให้ความช่วยเหลือผู้ใช้บริการ จากเหตุการณ์ทุจริตหรือฉ้อโกงภายในระบบ Digital ID ครบถ้วน ทั้งนี้นโยบายและขั้นตอนการปฏิบัติดังกล่าวมีการประกาศใช้งานภายในองค์กร มีการกำหนดคณะกรรมการและคณะทำงานที่รับผิดชอบ รวมถึงมีการทบทวนและประเมินนโยบายดังกล่าวเป็นระยะ องค์กรมีการกำหนดนโยบายและขั้นตอนในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งมีเนื้อหาในส่วนของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศ รวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุ รกิจ ทั้งนี้นโยบายและขั้นตอนการปฏิบัติมีการประกาศใช้งานภายในองค์กร มีการกำหนดคณะกรรมการและคณะทำงานที่รับผิดชอบ รวมถึงมีการทบทวนและประเมินนโยบายดังกล่าวเป็นระยะ นอกจากนี้ยังมีคณะกรรมการและคณะทำงานที่ดูแลทางด้านข้อมูลส่วนบุคคลโดยส่งเสริมให้มีความตระหนักด้านการใช้งานข้อมูลส่วนบุคคลภายในองค์กรและจัดเตรียมแผนการตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ในส่วนของการให้บริการด้าน Digital ID หากเป็นหน่วยงานผู้ให้บริการพิสูจน์และยืนยันตัวตน องค์กรจะมีการกำหนดขั้นตอนในการจัดการกระบวนการพิสูจน์ตัวตนและยืนยันตัวตนที่ชัดเจน มีการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนกับข้อกำหนดต่างๆ รวมถึงมี ขั้นตอนการยกระดับความน่าเชื่อถือในการยืนยันตัวตนหากทางผู้ใช้บริการร้องขอ เช่นเดียวกับกรณีที่เป็นหน่วยงานที่ให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล องค์กรจะจัดให้มีมาตรการในการควบคุมและปกป้องข้อมูลการพิสูจน์และยืนยันตัวตนอย่างปลอดภัย สามารถตรวจสอบกิจกรรมในการแลกเปลี่ยนได้ และมีการทดสอบระบบก่อนที่จะให้บริการกับผู้ใช้งานทุกครั้ง
ปานกลาง	องค์กรมีการกำหนดแผนในการป้องกันและจัดการการฉ้อโกงหรือการทุจริต ซึ่งมีเนื้อหาที่เกี่ยวข้องกับการบริหารจัดการบุคลากร วิธีการส่งเสริมและควบคุมไม่ให้เกิดการฉ้อโกงหรือทุจริต กลไกในติดตามและจัดการกับเหตุที่เกิดขึ้น รวมไปถึงขั้นตอนการให้ความช่วยเหลือผู้ใช้บริการ จากเหตุการณ์ทุจริตหรือฉ้อโกงภายในระบบ Digital ID ทั้งนี้เนื้อหาบางส่วนอาจยังไม่ครบถ้วนบ้าง แต่นโยบายและขั้นตอนการปฏิบัติดังกล่าวมีการประกาศใช้งานภายในองค์กร มีการกำหนดคณะกรรมการและคณะทำงานที่รับผิดชอบ รวมถึงมีการทบทวนอย่างเพียงพอ

	องค์กรมีการกำหนดนโยบายและขั้นตอนในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งมีเนื้อหาในส่วนของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุ รกิจ ทั้งนี้เนื้อหาบางส่วนอาจยังไม่ครบถ้วนบ้าง แต่นโยบายและขั้นตอนการปฏิบัติดังกล่าวมีการประกาศใช้งานภายในองค์กร มีการกำหนดคณะกรรมการและคณะทำงานที่รับผิดชอบ รวมถึงมีการทบทวนอย่างเพียงพอ นอกจากนี้ยังมีคณะกรรมการและคณะทำงานที่ดูแลทางด้านข้อมูลส่วนบุคคล ส่งเสริมให้มีความตระหนักด้านการใช้งานข้อมูลส่วนบุคคลภายในองค์กรแต่อาจจะยังไม่ต่อเนื่องและจัดเตรียมแผนการตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแต่อาจจะยังไม่ได้มีการซักซ้อมหรือการประเมินคุณภาพของแผนการรับมือ ในส่วนของการให้บริการด้าน Digital ID หากเป็นหน่วยงานผู้ให้บริการพิสูจน์และยืนยันตัวตน องค์กรจะมีการกำหนดขั้นตอนในการจัดการกระบวนการพิสูจน์ตัวตนและยืนยันตัวตน แต่ขั้นตอนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนกับข้อกำหนดต่างๆ รวมถึงขั้นตอนการยกระดับความน่าเชื่อถือในการยืนยันตัวตนหากทางผู้ใช้บริการร้องขออาจจะไม่ครบถ้วน เช่นเดียวกับกรณีที่เป็นหน่วยงานที่ให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล องค์กรจะจัดให้มีมาตรการในการควบคุมและปกป้องข้อมูลการพิสูจน์และยืนยันตัวตนอย่างปลอดภัยแต่อาจจะยังไม่ดำเนินการบางหัวข้อให้ครบถ้วน เช่น การจัดเก็บ Log หรือ การกำหนด Sharing policy สำหรับข้อมูลแต่ละประเภท
ต่ำ	องค์กรอาจยังไม่มีการกำหนดแผนในการป้องกันและจัดการการฉ้อโกงหรือการทุจริต หรือมีการกำหนดแผนแล้วแต่มีเนื้อหาที่เกี่ยวข้องกับการบริการจัดการบุคลากร วิธีการส่งเสริมและควบคุมไม่ให้เกิดการฉ้อโกงหรือทุจริต กลไกในติดตามและจัดการกับเหตุที่เกิดขึ้น รวมไปถึงขั้นตอนการให้ความช่วยเหลือผู้ใช้บริการจากเหตุการณ์ทุจริตหรือฉ้อโกงภายในระบบ Digital ID ไม่ครบถ้วนเป็นส่วนมาก ซึ่งนโยบายและขั้นตอนการปฏิบัติดังกล่าวอยู่ระหว่างจัดทำและยังไม่มีการประกาศใช้งาน รวมไปถึงคณะกรรมการและคณะทำงานที่รับผิดชอบยังไม่ชัดเจน เพื่อมาควบคุมและประเมินผลแผนในการจัดการให้มีประสิทธิภาพที่เพียงพอ องค์กรอาจยังไม่มีการกำหนดนโยบายและขั้นตอนในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หรือมีการกำหนดแล้วแต่มีเนื้อหาในส่วนของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจ ไม่ครบถ้วนเป็นส่วนมาก ซึ่งนโยบายและขั้นตอนการปฏิบัติดังกล่าวอยู่ระหว่างจัดทำและยังไม่มีการประกาศใช้

	งาน รวมไปถึงคณะกรรมการและคณะทำงานที่รับผิดชอบยังไม่ชัดเจนเพื่อดูแลระบบและขั้นตอนการปฏิบัติงานเพื่อรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ นอกจากนี้คณะกรรมการและคณะทำงานที่ดูแลทางด้านข้อมูลส่วนบุคคลยังไม่ชัดเจน ยังไม่มีการส่งเสริมให้มีความตระหนักด้านการใช้งานข้อมูลส่วนบุคคลภายในองค์กรและจัดเตรียมแผนการตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ในส่วนของการให้บริการด้าน Digital ID หากเป็นหน่วยงานผู้ให้บริการพิสูจน์และยืนยันตัวตน องค์กรยังไม่มีการกำหนดขั้นตอนในการจัดการกระบวนการพิสูจน์ตัวตนและยืนยันตัวตนเป็นลายลักษณ์อักษร จะใช้การปฏิบัติงานตามที่เจ้าหน้าที่หน้างานดำเนินการเป็นประจำซึ่งมีความเสี่ยงสูงที่อาจให้เกิดการดำเนินงานที่บกพร่อง เช่นเดียวกับกรณีที่เป็นหน่วยงานที่ให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนท างดิจิทัล องค์กรยังไม่มีมาตรการในการควบคุมและปกป้องข้อมูลการพิสูจน์และยืนยันตัวตนอย่างปลอดภัยซึ่งอาจนำไปสู่การถูกโจมตีการผู้ไม่ประสงค์ดี หรือความบกพร่องต่อการดำเนินงานได้

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 มีการสำรองข้อมูลอย่างต่อเนื่อง ส่งผลให้ผู้ดูแลระบบสามารถรับมือกับความเสี่ยงและตอบสนองได้ทันท่วงที
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 มีระบบหลายส่วนที่ต้องมีการดึงข้อมูลออกมาเชื่อมโยงกันหลายครั้ง 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 ที่ไม่มีเครื่องมือในการติดตาม ไม่มีการสำรองข้อมูลหรือสำรองข้อมูลบางครั้ง ส่งผลให้ผู้ดูแลระบบไม่สามารถรับมือกับความเสี่ยงและตอบสนองได้ทันท่วงที มีความเสี่ยงสูงที่ระบบ Digital ID จะหยุดชะงักได้

ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	
สูง	องค์กรมีกระบวนการและเทคโนโลยีต่างๆ เข้ามาช่วยในการรักษาความมั่นคงปลอดภัยภายในระบบ Digital ID ซึ่งช่วยให้การควบคุมการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ การจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจ เป็นไปอย่างมีประสิทธิภาพ 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
ปานกลาง	องค์กรมีกระบวนการและเทคโนโลยีต่างๆ เข้ามาช่วยในการรักษาความมั่นคงปลอดภัยภายในระบบ Digital ID ทั้งนี้กระบวนการและเทคโนโลยีดังกล่าวสามารถควบคุมการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ และการจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจได้อย่างเพียงพอ ทำให้สามารถควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ แต่ยังสามารถเพิ่มประสิทธิภาพในการควบคุมให้ดียิ่งขึ้นเพื่อให้สามารถรับมือกับการเปลี่ยนแปลงข องภัยคุกคามทางไซเบอร์ นอกจากนั้นองค์กรยังดำเนินการบริหารจัดการช่องโหว่ภายในระบบ Digital ID ทั้งในส่วนของการบริหารจัดการการติดตั้งโปรแกรมสำหรับแก้ไขข้อบกพร่อง (Patch management) โดยมีกระบวนการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง การดำเนินการบริหารจัดการช่องโหว่ของระบบ (Vulnerability management) หรือการจัดให้มีทดสอบการเจาะระบบ (Penetration test) ในระบบ Digital ID โดยผู้เชี่ยวชาญที่เหมาะสม ทั้งนี้ในภาพรวมองค์กรมีการควบคุมเรื่องช่องโหว่ภายในระบบ Digital ID แล้วแต่อาจยังพบเจอช่องโหว่ที่มีระดับผลกระทบสูงบางส่วนที่ยังไม่สามารถแก้ไขได้

ต่ำ	องค์กรยังไม่มีกระบวนการและเทคโนโลยีต่างๆ ในการรักษาความมั่นคงปลอดภัยภายในระบบ Digital ID ที่สามารถควบคุมการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การปกป้องความมั่นคงปลอดภัยของข้อมูลที่ใช้งานในระบบ การควบคุมการเข้าถึงระบบสารสนเทศรวมถึงทางกายภาพ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดการเรื่องการพัฒนาระบบ การจัดการเหตุการณ์ไม่พึงประสงค์ และการจัดการแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจได้ครบถ้วน 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 จาผู้ใช้บริการ 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)	
สูง	องค์กรมีการแจ้งรายละเอียดเกี่ยวกับข้อกำหนดการให้บริการที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตนหรือการแลกเปลี่ยนข้อมูลการพิสูจน์และยืนยันตัวตนอย่างครบถ้วน โดยมีการแจ้งเกี่ยวกับข้อมูลโดยทั่วไปของผู้ให้บริการ วิธีการจัดเก็บและรวบรวมข้อมูล การรักษาความปลอดภัยและความลับของข้อมูล ช่องทางการติดต่อสื่อสาร สิทธิที่ผู้ใช้บริการสามารถปฏิบัติได้ รวมไปถึงข้อกำหนดจากกฎหมายหรือข้อกำหนดอื่นๆ ที่จะมีผลกระทบต่อผู้ใช้บริการ ทั้งนี้ข้อกำหนดการต่างๆ มีการทบทวนอยู่เป็นประจำ นอกจากนี้มีช่องทางรับเรื่องร้องเรียนหรือแจ้งเหตุที่ไม่พึงประสงค์จากผู้ใช้บริการ และมีกระบวนการให้ความช่วยเหลือผู้ใช้บริการจากเหตุการณ์ที่ไม่พึงประสงค์อย่างครบถ้วน ทั้งนี้กระบวนการรับมือต่อเหตุร้องเรียนหรือแจ้งเหตุที่ไม่พึงประสงค์มีการพัฒนาปรับปรุงอย่างสม่ำเสมอ ทำให้กระบวนการดังกล่าวมีประสิทธิภาพที่ดี ส่งผลให้สามารถรับมือจากข้อร้องเรียนหรือเหตุการณ์ไม่พึงประสงค์ได้อย่างทันท่วงที และไม่ส่งผลกระทบต่อชื่อเสียงในการดำเนินงานพิสูจน์และยืนยันตัวตนขององค์กร
ปานกลาง	องค์กรมีการแจ้งรายละเอียดเกี่ยวกับข้อกำหนดการให้บริการที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตนหรือการแลกเปลี่ยนข้อมูลการพิสูจน์และยืนยันตัวตน โดยมีการแจ้งเกี่ยวกับข้อมูลโดยทั่วไปของผู้ให้บริการ วิธีการจัดเก็บและรวบรวมข้อมูล การรักษาความปลอดภัยและความลับของข้อมูล ช่องทางการติดต่อสื่อสาร สิทธิที่ผู้ใช้บริการสามารถปฏิบัติได้ รวมไปถึงข้อกำหนดจากกฎหมายหรือข้อกำหนดอื่นๆ ที่จะมีผลกระทบต่อผู้ใช้บริการ นอกจากนี้มีช่องทางรับเรื่องร้องเรียนหรือแจ้งเหตุที่ไม่พึงประสงค์จากผู้ใช้บริการ และมีกระบวนการให้ความช่วยเหลือผู้ใช้บริการจากเหตุการณ์ที่ไม่พึงประสงค์แต่กระบวนการดังกล่าวยังไม่ได้มีการปรับปรุงให้มีประสิทธิภาพที่ดียิ่งขึ้น ส่งผลให้สามารถรับมือจากข้อร้องเรียนหรือเหตุการณ์ไม่พึงประสงค์ได้ในระดับหนึ่ง อาจส่งผลกระทบเล็กน้อยต่อชื่อเสียงในการดำเนินงานพิสูจน์และยืนยันตัวตนขององค์กร
ต่ำ	องค์กรมีการแจ้งรายละเอียดเกี่ยวกับข้อกำหนดการให้บริการที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตนหรือการแลกเปลี่ยนข้อมูลการพิสูจน์และยืนยันตัวตนไม่ครบถ้วนหรือยังไม่มีข้อกำหนดการให้บริการ 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 รวมถึงมีการแก้ไขติดตามปัญหาที่เป็นประเด็นจากการตรวจสอบอย่างต่อเนื่อง ทำให้มีการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเพียงพอ

สูง	องค์กรมีการทำสัญญากับบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID เพียงบางส่วน และมีบุคคลภายนอกบางส่วนที่ไม่มีการทำสัญญาด้วย รวมถึงยังมีการกำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID แค่บางส่วนเท่านั้น ทำให้อาจมีบางโครงการไม่มีการติดตามผลการปฏิบัติงานของบุคคลภายนอก ทั้งนี้ จำนวนบุคคลภายนอกที่สนับสนุนการให้บริการ Digital ID อาจมีจำนวนมาก ซึ่งทำให้ควบคุมการดำเนินงานจากบุคคลภายนอกได้ยาก ทั้งนี้ องค์กรยังไม่มีการตรวจสอบโดยผู้ตรวจสอบที่มีความเป็นอิสระอย่างครบถ้วน ทำให้ไม่สามารถตรวจสอบประสิทธิภาพในการรักษา ความมั่นคงปลอดภัย การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องได้ ส่งผลกระทบต่อความไม่สอดคล้องต่อกฎหมายและกฎระเบียบ

ความสามารถในการบริหารจัดการความเสี่ยง (Risk management capability)	
สูง	องค์กรมีการศึกษาผลกระทบต่อบริษัทในการดำเนินการตามกฎหมายหรือกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตน ไม่ว่าจะเป็นกฎระเบียบด้านเทคโนโลยีสารสนเทศ กฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล หรือกฎระเบียบอื่นๆ จากหน่วยงานกำกับที่เกี่ยวข้อง รวมถึงมีกระบวนการทบทวนกฎระเบียบและนโยบายบริษัทให้สอดคล้องกับกฎหมายและกฎระเบียบต่างๆ และสื่อสารให้พนักงานรู้และเข้าใจในการเปลี่ยนแปลงของนโยบายต่างๆ โดยมีการวัดผลเพื่อให้มั่นใจได้ว่าการสื่อสารเป็นไปอย่างมีประสิทธิภาพ รวมไปถึงมีการตรวจสอบการปฏิบัติตามกฎหมายและกฎเกณฑ์ โดยผู้ตรวจสอบที่มีความเป็นอิสระและมีความสามารถ ซึ่งครอบคลุมไปถึงระบบและการให้บริการด้านพิสูจน์และยืนยันตัวตน มีกระบวนการในการติดตามและปรับปรุงประเด็นที่ได้จากการตรวจสอบเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างมีประสิทธิภาพ รายงานผลต่อผู้บริหารถึงผลการตรวจสอบทั้งหมดอย่างสม่ำเสมอ
ปานกลาง	องค์กรมีการศึกษาผลกระทบต่อบริษัทในการดำเนินการตามกฎหมายหรือกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตน แต่อาจจะไม่ครบถ้วนในทุกด้าน ซึ่งประกอบด้วยกฎระเบียบด้านเทคโนโลยีสารสนเทศ กฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล หรือกฎระเบียบอื่นๆ จากหน่วยงานกำกับที่เกี่ยวข้อง รวมถึงมีกระบวนการทบทวนกฎระเบียบและนโยบายบริษัทให้สอดคล้องกับกฎหมายและกฎระเบียบต่างๆ แต่อาจจะยังขาดการสื่อสารหรือให้ความรู้กับพนักงานที่เกี่ยวข้องเพื่อให้เข้าใจถึงกฎหมายและกฎระเบียบต่างๆ ที่มีการเปลี่ยนแปลง รวมไปถึงมีการตรวจสอบการปฏิบัติตามกฎหมายและกฎเกณฑ์ โดยผู้ตรวจสอบที่มีความเป็นอิสระและมีความสามารถ แต่ยังไม่ครอบคลุมทุกระบบและการให้บริการด้านพิสูจน์และยืนยันตัวตน ทั้งนี้ องค์กรมีกระบวนการในการติดตามและปรับปรุงประเด็นที่ได้จากการตรวจสอบเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยง รายงานผลต่อผู้บริหารถึงผลการตรวจสอบทั้งหมดแต่ไม่ได้สม่ำเสมอ

ต่ำ	องค์กรไม่มีการศึกษาผลกระทบต่อบริษัทในการดำเนินการตามกฎหมายหรือกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตน รวมถึงไม่มีกระบวนการทบทวนกฎระเบียบและนโยบายบริษัทให้สอดคล้องกับกฎหมายและกฎระเบียบต่างๆ ส่งผลให้นโยบายและแนวทางปฏิบัติขององค์ไม่สอดคล้องกับกฎหมายหรือกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตน และพนักงานไม่สามารถปฏิบัติงานได้ถูกต้องตามกฎหมาย อีกทั้ง องค์กรไม่มีการตรวจสอบการปฏิบัติตามกฎหมายและกฎเกณฑ์ โดยผู้ตรวจสอบที่มีความเป็นอิสระและมีความสามารถ หรือมีการตรวจสอบแต่ไม่มีการติดตามและปรับปรุงประเด็นที่ได้จากการตรวจสอบเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยง ส่งผลให้องค์กรไม่สามารถระบุประเด็นที่ควรจะต้องแก้ไขหรือพัฒนาให้ดียิ่งขึ้นเพื่อให้สอดคล้องกับกับกฎหมายและกฎเกณฑ์ต่างๆ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง
เขตห้วยขวาง กรุงเทพฯ 10310
โทรศัพท์ : 02 123 1234 | โทรสาร : 02 123 1200
: ETDA THAILAND