แผนบริหารความเสี่ยงของ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประจำปีงบประมาณ 2568

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ETDA

สารบัญ

แผนบริหารความเสี่ยงของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ประจำปีงบประมาณ 2568

1. ข้อมูลพื้นฐาน
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อมูลทั่วไป

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) จัดตั้งขึ้นตามพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 ประกาศราชกิจจานุเบกษา เล่ม 136 ตอนที่ 49 ก เมื่อวันที่ 14 เมษายน 2562 มีวัตถุประสงค์เพื่อ “ส่งเสริมและสนับสนุนการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์ของประเทศ เพื่อเป็นกลไกในการขับเคลื่อนนโยบายและแผนของรัฐด้านธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์ให้สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม รวมทั้งส่งเสริมให้เกิดการพัฒนามาตรฐานหรือกฎเกณฑ์ในการใช้งานเทคโนโลยีดิจิทัลเพื่อให้ระบบงานเทคโนโลยีดิจิทัลต่าง ๆ เชื่อมโยงกันได้อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ”

โดย สพธอ. เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น โดยสำนักงานฯ มีภารกิจตามกฎหมายเพื่อให้ดำเนินการได้ตามวัตถุประสงค์ ดังนี้

1. จัดทำแผนยุทธศาสตร์เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์เสนอต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เพื่อพิจารณาให้ความเห็นชอบ
2. จัดทำแผนยุทธศาสตร์การพัฒนาโครงสร้างพื้นฐานด้านมาตรฐานที่สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม
3. ส่งเสริมและสนับสนุนหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและภาคเอกชน ให้มีการดำเนินการด้านธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์เพื่อรองรับการพัฒนาประเทศในด้านต่างๆ ทั้งทางการเงิน การค้า การลงทุน และการนำเข้าส่งออก รวมทั้งการให้บริการประชาชนของภาครัฐให้สอดคล้องกับแผนยุทธศาสตร์เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์
4. ศึกษา วิจัย และพัฒนาเทคโนโลยีดิจิทัลเพื่อรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์ของหน่วยงานทั้งภาครัฐและภาคเอกชน รวมทั้งส่งเสริมการออกแบบสถาปัตยกรรมด้านเทคโนโลยีดิจิทัลเพื่อเสนอแนะต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ในการกำหนดมาตรฐานเรื่องดังกล่าว
5. จัดทำข้อเสนอแนะเกี่ยวกับมาตรฐาน และมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์เพื่อให้หน่วยงานทั้งภาครัฐและภาคเอกชนสามารถใช้เทคโนโลยีดิจิทัลที่สอดคล้องและเชื่อมโยงกันอย่างมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ
6. กำกับดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกาที่ออกตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ รวมถึงการให้การสนับสนุนการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าว
7. วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐานหรือตามมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์
8. เป็นศูนย์กลางในการให้บริการทางวิชาการหรือให้บริการที่เกี่ยวกับการพัฒนาส่งเสริมละสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์แก่หน่วยงานภาครัฐ หน่วยงานเอกชน และประชาชน รวมทั้งเผยแพร่และให้ความรู้ความเข้าใจในการทำธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์

9. ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน
10. ฝึกอบรมเพื่อยกระดับของบุคลากรของสำนักงานและบุคคลภายนอกให้มีทักษะเกี่ยวกับมาตรฐาน ความมั่นคงปลอดภัย และการสร้างความน่าเชื่อถือในระบบและการให้บริการทางธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์
11. ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือคณะกรรมการมอบหมาย หรือตามที่กฎหมายกำหนด

วิสัยทัศน์

เป็นองค์กรที่ร่วมสร้างสังคมดิจิทัลเพื่อเพิ่มมูลค่าทางเศรษฐกิจและยกระดับความสามารถในการแข่งขันของประเทศ

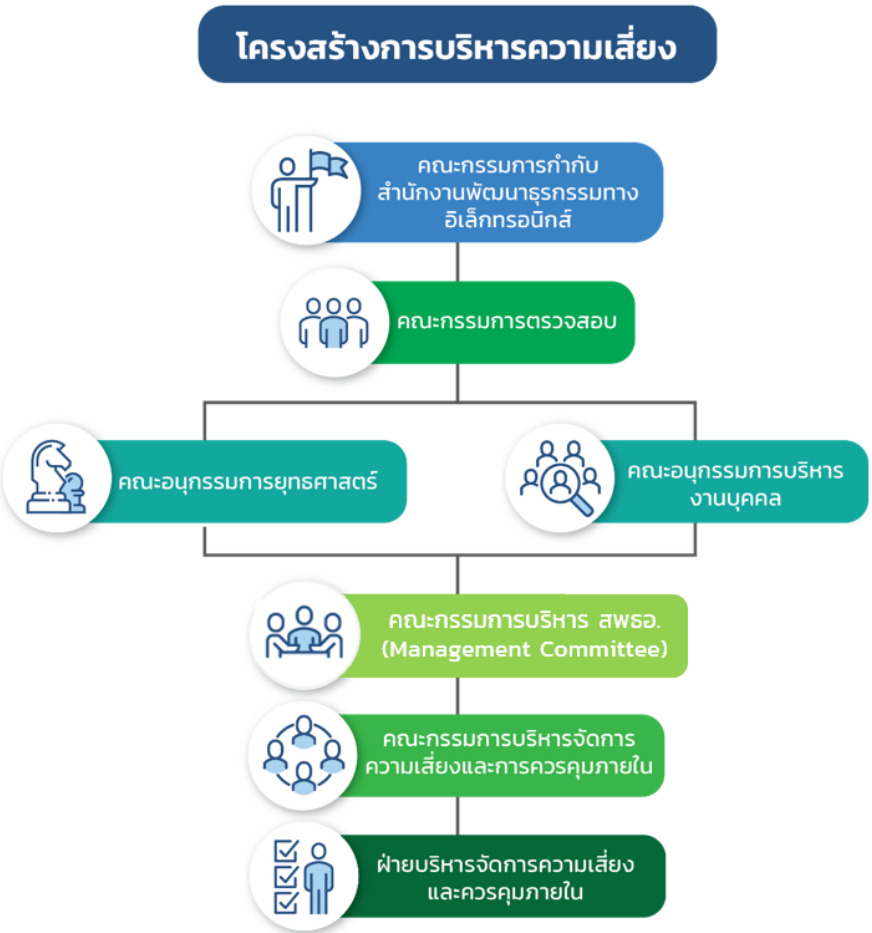
พันธกิจ

1. กำกับดูแลธุรกิจบริการดิจิทัล เพื่อสร้างความน่าเชื่อถือ รองรับการขยายตัวของกิจกรรมทางเศรษฐกิจและสังคมดิจิทัล
2. ส่งเสริมและสนับสนุนให้เกิดการทำธุรกรรมทางอิเล็กทรอนิกส์
3. ร่วมมือกับทุกภาคส่วน เพื่อผลักดันการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างบูรณาการและเชื่อมโยง

ค่านิยม

2. โครงสร้างการบริหารความเสี่ยง

การบริหารความเสี่ยงดำเนินการโดยฝ่ายบริหารความเสี่ยงและควบคุมภายใน โดยมีคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน ของ สพธอ. ช่วยในการจัดวางระบบบริหารความเสี่ยง ติดตาม สอบทาน ประเมินความเพียงพอ ทั้งในด้านประสิทธิภาพและประสิทธิผลของระบบบริหารความเสี่ยง กำกับ ดูแล ทบทวน ให้คำแนะนำต่อผู้ปฏิบัติงานในแต่ละฝ่ายของ สพธอ. โดยขั้นตอนการนำเสนอเพื่อ พิจารณาแผนบริหารความเสี่ยงประจำปีและการรายงานติดตามผล เป็นดังนี้ เมื่อคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน ของ สพธอ. กลั่นกรองข้อมูลแล้ว จะนำเสนอต่อคณะกรรมการบริหาร สพธอ. และเสนอต่อคณะอนุกรรมการที่เกี่ยวข้องในความเสี่ยงแต่ละด้าน ได้แก่ คณะอนุกรรมการยุทธศาสตร์ คณะอนุกรรมการบริหารงานบุคคล และคณะกรรมการตรวจสอบเป็นผู้กลั่นกรองในลำดับสุดท้าย เพื่อให้มีความถูกต้อง สมบูรณ์พร้อมต่อการให้คณะกรรมการกำกับ สพธอ. พิจารณา ซึ่งแสดงขั้นตอนได้ดังรูป



รูปที่ 1 โครงสร้างการบริหารความเสี่ยง

หน้าที่ความรับผิดชอบของแต่ละคณะหรือฝ่ายงาน

1. **งานบริหารความเสี่ยงและควบคุมภายใน**
   วิเคราะห์ข้อมูลเพื่อจัดทำร่างหัวข้อความเสี่ยง แนวทางการจัดการความเสี่ยง โดยพิจารณาจากแผนโครงการต่างๆ ขององค์กรที่จะเกิดขึ้น สาเหตุปัจจัยความเสี่ยง รวมถึงความเสี่ยงต่อเนื่องจากปีก่อน เพื่อนำมาสรุปข้อมูลวิเคราะห์ ประเด็นความเสี่ยง ประเมินมาตรการควบคุม ประชุมหารือกับหน่วยงานเจ้าของความเสี่ยงและหน่วยงานที่เกี่ยวข้อง ในการดำเนินการสัมภาษณ์เชิงลึก สื่อสารสร้างความเข้าใจในกระบวนการทำงาน รวมถึงจัดเตรียมแนวทางในการบริหารจัดการความเสี่ยง ติดตาม ประเมินผล และเสนอร่างแผนบริหารจัดการความเสี่ยงต่อคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน
2. **คณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน**
   ประชุมพิจารณากลั่นกรองประเด็นความเสี่ยง แนวทางการบริหารจัดการความเสี่ยง และพิจารณาให้ความคิดเห็นต่อฝ่ายบริหารความเสี่ยงและควบคุมภายในเจ้าของความเสี่ยง (Risk Owner) ที่เกี่ยวข้อง รวมทั้งนำข้อเสนอแนะจากคณะกรรมการชุดต่าง ๆ ที่เกี่ยวข้องไปปรับปรุงแก้ไข
3. **คณะกรรมการบริหาร สพธอ. (Management Committee-MC)**
   รับทราบประเด็นความเสี่ยงและให้ข้อเสนอแนะต่อแนวทางการบริหารจัดการความเสี่ยงในแต่ละด้าน
4. **คณะอนุกรรมการที่เกี่ยวข้อง**
   4.1 คณะอนุกรรมการยุทธศาสตร์
   รับทราบและให้ข้อเสนอแนะต่อแผนบริหารจัดการความเสี่ยง ซึ่งประกอบด้วยความเสี่ยงด้าน กลยุทธ์ ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกฎระเบียบ และความเสี่ยงด้านชื่อเสียง
   4.2 คณะอนุกรรมการบริหารงานบุคคล
   ประชุมเพื่อพิจารณาประเด็นความเสี่ยงด้านปฏิบัติการเฉพาะที่มีรายละเอียดด้านความเสี่ยงเกี่ยวเนื่องกับการบริหารงานบุคคล เพื่อให้ความคิดเห็นข้อเสนอแนะ เกี่ยวกับประเด็นความเสี่ยงที่เกี่ยวข้อง
5. **คณะกรรมการตรวจสอบ**
   ประชุมเพื่อพิจารณาประเด็นความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกฎระเบียบ ความเสี่ยงด้านชื่อเสียง และความเสี่ยงด้านการเงิน และแนวทางการบริหารจัดการความเสี่ยง โดยช่วยกลั่นกรองข้อมูลก่อนจะมี

นำเสนอวาระการบริหารจัดการความเสี่ยงไปยังคณะกรรมการกำกับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ต่อไป

6. **คณะกรรมการกำกับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์** ประชุมเพื่อพิจารณาประเด็นความเสี่ยงและแนวทางการบริหารจัดการความเสี่ยงในแต่ละด้าน และให้ความเห็นชอบรายงานผลการดำเนินงานด้านการบริหารความเสี่ยงประจำไตรมาส

3. การบริหารความเสี่ยงของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

การเปลี่ยนแปลงอย่างรวดเร็วของสภาพเศรษฐกิจ สังคม เทคโนโลยี รวมถึงการดำเนินงานของ สพธอ. ที่จะต้องดำเนินการให้เป็นไปตามแผนที่วางไว้ องค์กรจึงต้องเผชิญกับความเสี่ยงทั้งจากภายในและภายนอก ผู้บริหารมีหน้าที่กำกับและติดตามโดยตรงในการบริหารจัดการความเสี่ยง ซึ่งหลักการบริหารจัดการความเสี่ยงระดับองค์กรถือเป็นเครื่องมือที่สำคัญของผู้บริหารในการดำเนินงานให้บรรลุวัตถุประสงค์ขององค์กร รวมถึงบุคลากรทุกฝ่ายจะต้องมีความตระหนักและเข้าใจถึงความเสี่ยงในด้านต่างๆ โดยระบบการบริหารจัดการความเสี่ยงที่ดีจะช่วยองค์กรในการวางแผนและจัดการเหตุการณ์ด้านลบที่อาจจะเกิดขึ้นอันเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กร รวมถึงช่วยให้องค์กรได้รับประโยชน์และเกิดการเรียนรู้จากเหตุการณ์ความเสี่ยงที่เกิดขึ้น ส่งผลให้สามารถเพิ่มศักยภาพและขีดความสามารถในการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากขึ้น

แนวทางการบริหารความเสี่ยงของ สพธอ. เป็นการดำเนินการที่นำเอาหลักการประเมินความเสี่ยงอ้างอิงจากประกาศของกระทรวงการคลัง เรื่องหลักการบริหารจัดการความเสี่ยงระดับองค์กร ซึ่งเป็นกรอบแนวทางที่มีการนำแนวคิดการบริหารจัดการความเสี่ยงของ ของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ซึ่งเป็นต้นแบบของระบบการเงินและการบัญชีที่ทั่วโลกใช้อยู่ในปัจจุบัน และ International Organization for Standardization (ISO) รวมถึงการบริหารจัดการความเสี่ยงในภาครัฐของประเทศต่างๆ มากำหนดเป็นแนวทางการบริหารจัดการความเสี่ยง สำหรับหน่วยของรัฐ ไปใช้ในการประเมินความเสี่ยงที่อาจเกิดขึ้นกับองค์กรในด้านต่างๆ เช่น การดำเนินโครงการ ด้านการปฏิบัติงาน เพื่อพิจารณาแนวทางป้องกัน รวมถึงวางระบบการบริหารจัดการความเสี่ยงได้อย่างเหมาะสม โดยการบริหารความเสี่ยงขององค์กรจะใช้หลักการประเมินความเสี่ยงตามหลัก COSO 2017 และยังมีการประเมินการควบคุมภายในตามหลักเกณฑ์ของกระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 เพื่อเป็นแนวทางในการประเมินความเพียงพอของระบบความคุมภายในแต่ละฝ่ายในองค์กร

3.1 กรอบแนวคิดการบริหารจัดการความเสี่ยง

รูปที่ 2 กรอบแนวคิดการบริหารจัดการความเสี่ยง COSO ERM

COSO ERM 2017 เกิดจากการพัฒนาทบทวนปรับปรุงใหม่ จาก COSO ERM ที่ใช้มาตั้งแต่ปี 2004 เนื่องจากการเปลี่ยนแปลงของสภาพแวดล้อมที่ส่งผลให้มีปัจจัยเสี่ยงใหม่ๆ เกิดขึ้นอย่างมากมาย และรวดเร็วขึ้นกว่าเดิม รวมถึงการเปลี่ยนแปลงพฤติกรรมของลูกค้าและผู้มีส่วนได้ส่วนเสียกับองค์กร ที่ทั้งหมดได้แสดงอิทธิพลอย่างยิ่งต่อดำเนินงานขององค์กรต่างๆ ในปัจจุบัน โดยการบริหารจัดการความเสี่ยงดังกล่าวจะต้องเผชิญกับความท้าทายอย่างรอบด้าน ที่ต้องพิจารณาแนวทางใหม่ๆ ในการจัดการความเสี่ยงที่มีประสิทธิผลและประสิทธิภาพมากขึ้น เพื่อรักษาความสามารถและสร้างความยั่งยืนให้กับองค์กรต่อไปได้ เน้นในด้านการดำเนินกลยุทธ์อย่างมีธรรมาภิบาล โดยจากเดิมที่มีองค์ประกอบการบริหารความเสี่ยง 8 องค์ประกอบ ได้ปรับเปลี่ยนให้เหลือเพียง 5 องค์ประกอบ 20 หลักการ ดังรูปด้านบน

3.2 วัตถุประสงค์การบริหารความเสี่ยง

1) เพื่อบริหารจัดการให้ความเสี่ยงขององค์กรให้อยู่ในระดับที่ยอมรับได้
2) เพื่อให้บุคลากรในองค์กรตระหนักถึงภัยคุกคามและลดการสูญเสียที่อาจเกิดขึ้น
3) เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง
4) เพื่อเตรียมความพร้อมและวางแผนรองรับเหตุการณ์เมื่อมีการสูญเสียขึ้น
5) เพื่อให้บุคลากรเข้าใจ ตระหนัก และให้ความสำคัญการบริหารความเสี่ยงตามนโยบายการบริหารความเสี่ยงขององค์กร

3.3 ประโยชน์ของการบริหารความเสี่ยง

1) เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี การบริหารความเสี่ยงจะช่วยให้คณะทำงานบริหารความเสี่ยงและผู้บริหารทุกระดับตระหนักถึงความเสี่ยงที่สำคัญและสามารถทำหน้าที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

2) สร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร โดยการจัดการความเสี่ยงในรูปแบบต่าง ๆ จะเป็นองค์ความรู้ขององค์กรเพื่อการประยุกต์ใช้ในกิจกรรมต่าง ๆ ต่อไปในอนาคต

3) มีภาพรวมของความเสี่ยงต่าง ๆ ที่สำคัญประกอบการกับสื่อสารและการให้ความสำคัญของผู้บริหารจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วน ซึ่งรวมถึงความเสี่ยงตามหลักธรรมาภิบาล

4) เป็นเครื่องมือที่สำคัญในการบริหารงาน ทำให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลาและสามารถปกป้องผลประโยชน์รวมทั้งเพิ่มมูลค่าแก่องค์กร

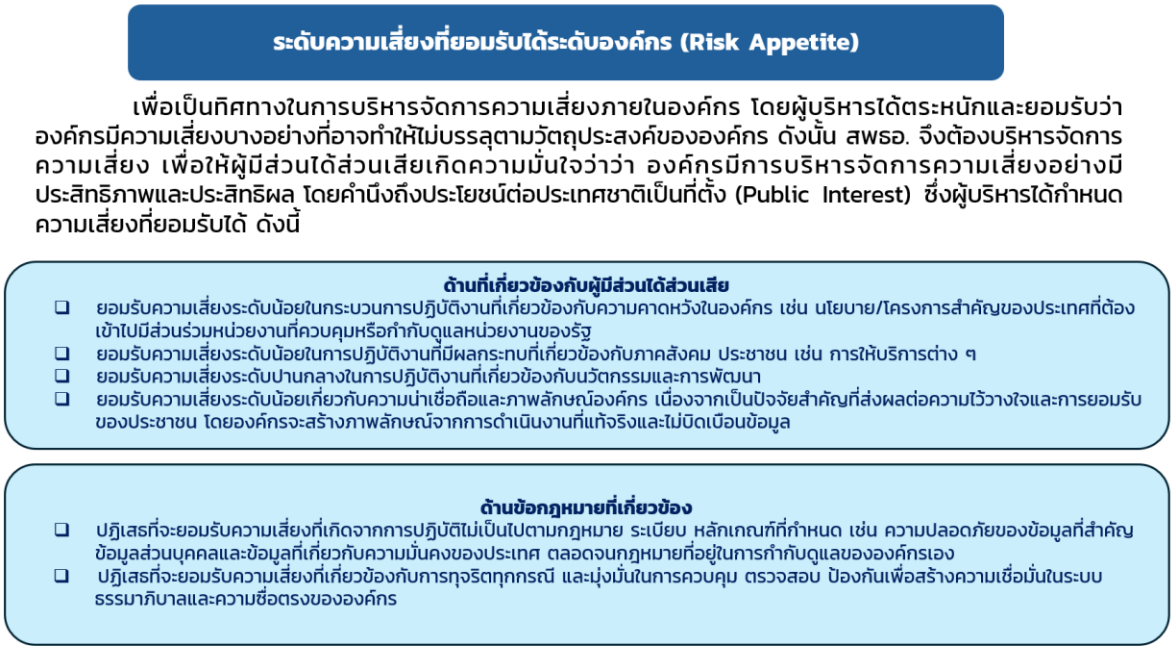
5) ช่วยให้การบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล การจัดสรรทรัพยากรเป็นไปอย่างเหมาะสมตามการจัดการความเสี่ยงที่ถูกเลือกใช้

3.4 ขั้นตอนการบริหารความเสี่ยง

3.4.1 การประเมินสภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมนี้มีอิทธิพลต่อการกำหนดกลยุทธ์และเป้าหมายขององค์กรการกำหนดกิจกรรม การบ่งชี้ประเมินและการจัดการความเสี่ยง สภาพแวดล้อมภายในองค์กรประกอบด้วยหลายปัจจัยเช่น จริยธรรมวิธีการทำงานของผู้บริหารและบุคลากร รวมถึงปรัชญาและวัฒนธรรมในการบริหารความเสี่ยง

ความเสี่ยงที่ยอมรับได้ (Risk Appetite) เป็นส่วนที่สำคัญอย่างหนึ่งของสภาพแวดล้อมภายในองค์กรและมีผลต่อการกำหนดกลยุทธ์เพื่อนำไปดำเนินการให้องค์กรบรรลุเป้าหมายทั้งด้านผลตอบแทนและการเติบโต กลยุทธ์แต่ละแบบนั้นมีความเสี่ยงที่เกี่ยวข้องแตกต่างกัน โดยในปี 2568 ยังคงใช้ระดับความเสี่ยงที่ยอมรับได้ ตามที่คณะกรรมการกำกับ สพธอ. ได้เห็นชอบไว้เมื่อปี 2567 โดยมีรายละเอียด ดังรูป



รูปที่ 3 : ระดับความเสี่ยงที่ยอมรับได้ระดับองค์กร

3.4.2 การกำหนดวัตถุประสงค์ (Objective Setting)

การกำหนดวัตถุประสงค์ที่ชัดเจนทำเพื่อให้องค์กรมั่นใจว่าวัตถุประสงค์ที่กำหนดขึ้นมีความสอดคล้อง กับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ โดยทั่วไปวัตถุประสงค์และกลยุทธ์ควรได้รับการบันทึกเป็นลายลักษณ์อักษรและสามารถพิจารณาได้ในด้านต่าง ๆ ดังนี้ ด้านกลยุทธ์ เกี่ยวข้องกับเป้าหมายและพันธกิจในภาพรวมขององค์กร ด้านปฏิบัติงาน เกี่ยวข้องกับประสิทธิภาพผลการปฏิบัติงานหรือความสามารถในการทำกำไร/บริหาร ด้านการปฏิบัติตามกฎ ระเบียบ เกี่ยวข้องกับการปฏิบัติตามกฎหมายและกฎระเบียบต่างๆ

3.4.3 การบ่งชี้เหตุการณ์ (Event Identification)

องค์กรมีการระบุสถานการณ์ที่อาจเกิดความเสี่ยงซึ่งองค์กรไม่สามารถมั่นใจได้ว่าเหตุการณ์ใดเหตุการณ์หนึ่งจะเกิดขึ้นหรือไม่ หรือมีผลลัพธ์ที่เกิดขึ้นจะเป็นอย่างไร ต้องพิจารณาทั้งปัจจัยภายในและภายนอกองค์กร อาจวิเคราะห์มาจากเหตุการณ์ในอดีตหรือแนวโน้มการเปลี่ยนแปลงในอนาคต

3.4.4 การประเมินความเสี่ยง (Risk Assessment)

ขั้นตอนนี้เน้นการประเมินโอกาสเกิดและผลกระทบของเหตุการณ์ที่อาจเกิดขึ้นต่อวัตถุประสงค์ขณะที่เกิดเหตุกรณ์ใดเหตุการณ์หนึ่งอาจส่งผลกระทบในระดับต่ำ เหตุการณ์ที่เกิดขึ้นอย่างต่อเนื่องอาจมีผลกระทบในระดับสูงต่อวัตถุประสงค์ โดยการระบุความเสี่ยงขององค์กรจึงมีทั้งหมด 5 ประเภทโดยมีนิยามของแต่ละความเสี่ยง ดังนี้

- <u>ความเสี่ยงด้านกลยุทธ์</u> (Strategic Risk) คือความเสี่ยงที่เกิดจากการกำหนดกลยุทธ์หรือนโยบายการบริหารงานทำให้องค์กรไม่สามารถบรรลุกลยุทธ์และไม่สามารถเพิ่มมูลค่าให้แก่องค์กรได้
- <u>ความเสี่ยงด้านปฏิบัติการ</u> (Operational Risk) คือความเสี่ยงที่เกิดจากการปฏิบัติงานโดยเกี่ยวข้องกับกระบวนการในการปฏิบัติงาน อุปกรณ์ เทคโนโลยีสารสนเทศ บุคคลากร ซึ่งส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินธุรกิจขององค์กร
- <u>ความเสี่ยงด้านการเงิน</u> (Financial Risk) คือความเสี่ยงจากการขาดข้อมูลการวิเคราะห์ การวางแผน การควบคุมและการจัดทำรายงานเพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้องเหมาะสม ซึ่งส่งผลต่อสถานะทางการเงินขององค์กร
- <u>ความเสี่ยงด้านกฎระเบียบ</u> (Compliance Risk) คือความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงาน กฎระเบียบหรือกฎหมายที่มีอยู่ไม่เหมาะสมเป็นอุปสรรคต่อการปฏิบัติงาน นโยบายและวิธีการปฏิบัติงานที่องค์กรกำหนดขึ้นไม่สามารถปฏิบัติได้
- <u>ความเสี่ยงด้านชื่อเสียง</u> (Reputation Risk) คือความเสี่ยงอันเนื่องมาจากการดำเนินงานทั้งทางตรงและทางอ้อมที่ก่อให้เกิดความเสียหายต่อชื่อเสี่ยง ตั้งแต่ภาพลักษณ์ในเชิงลบ จนถึงการถูกฟ้องดำเนินคดี ซึ่งอาจส่งผลต่อความน่าเชื่อถือขององค์กร

รูปที่ 4 : แนวทางการประเมินความเสี่ยงและปัจจัยที่ควรต้องพิจารณา

จากนั้นประเมินความเสี่ยงประกอบด้วย 2 มิติ คือ **โอกาสที่อาจเกิดขึ้น (Likelihood)** เหตุการณ์มีโอกาสเกิดขึ้นมาก น้อยเพียงใด **ผลกระทบ (Impact)** หากมีเหตุการณ์เกิดขึ้นองค์กรจะได้รับผลกระทบมากน้อยเพียงใด

เกณฑ์การประเมินระดับความเสี่ยง เป็นหลักเกณฑ์เพื่อให้สามารถระบุระดับโอกาสและระดับผลกระทบว่ามากน้อยโดยเปรียบเทียบเป็นระดับคะแนน สามารถยกตัวอย่างได้ดังต่อไปนี้

เกณฑ์โอกาสจะเกิด (Likelihood) เชิงปริมาณ	
คะแนน	คำนิยาม
5 สูงที่สุด	ไม่เกิดเลยในช่วงเวลา 1 ปี
4 สูง	เกิด 1 ครั้ง/ปี
3 ปานกลาง	เกิด 2 ครั้ง/ปี
2 ต่ำ	เกิด 3 ครั้ง/ปี
1 ต่ำที่สุด	เกิดมากกว่า 3 ครั้ง/ปี

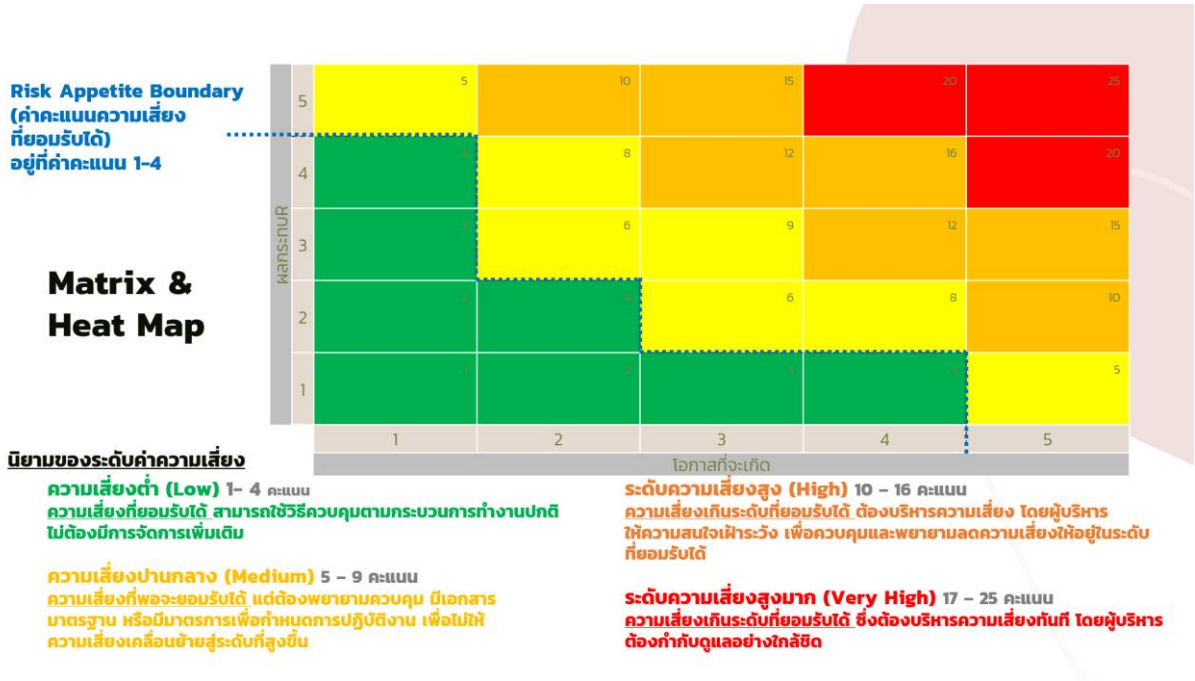
เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน)	
คะแนน	คำนิยาม
5 สูงที่สุด	ดำเนินการได้น้อยกว่าร้อยละ 80
4 สูง	ดำเนินการได้มากกว่าร้อยละ 80-84.9
3 ปานกลาง	ดำเนินการได้มากกว่าร้อยละ 85- 89.9
2 ต่ำ	ดำเนินการได้มากกว่าร้อยละ 90-94.9
1 ต่ำที่สุด	ดำเนินการได้มากกว่าร้อยละ 95

รูปที่ 5 : ตัวอย่างเกณฑ์การประเมินความเสี่ยงองค์กร

เกณฑ์ผลกระทบ (ด้านชื่อเสียง)	
คะแนน	คำนิยาม
5 สูงที่สุด	มีผลพิจารณาโทษทันทีตามกฎหมาย
4 สูง	ถูกฟ้องร้องดำเนินคดี
3 ปานกลาง	ถูกร้องเรียนจากผู้รับบริการและพบว่ามีข้อผิดพลาดจริง
2 ต่ำ	ถูกร้องเรียนจากผู้รับบริการ (ภายใน/ภายนอก)
1 ต่ำที่สุด	ไม่มีการร้องเรียนจากผู้รับบริการ

รูปที่ 5 : ตัวอย่างเกณฑ์การประเมินความเสี่ยงองค์กร (ต่อ)

การจัดลำดับความเสี่ยง โดยการใช้ตารางจัดลำดับความรุนแรงตามปัจจัยเสี่ยง (Risk Ranking) โดยอ้างอิงตามเกณฑ์ที่ผ่านความเห็นชอบของคณะกรรมการกำกับ สพธอ. เมื่อ 2565 โดยกำหนดค่าคะแนนความเสี่ยงที่ยอมรับได้ คือ ระดับค่าความเสี่ยงต่ำ อยู่ที่ค่าคะแนน 1-4 ทั้งนี้หากประเมินความเสี่ยงแล้วมีระดับความเสี่ยงปานกลางจนถึงสูงมาก ต้องมีการบริหารความเสี่ยงตามแนวทางที่ได้กำหนดไว้ในแต่ละระดับ ดังรูป



รูปที่ 6 : ระดับค่าความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้ (Risk Boundary)

3.4.5 การตอบสนองความเสี่ยง (Risk Response)

ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ โดยหลักการตอบสนองความเสี่ยงมี 4 ประการคือ

1. การหลีกเลี่ยง (Avoid) การดำเนินการเพื่อหลีกเลี่ยงเหตุการณีที่ก่อให้เกิดความเสี่ยง
2. การร่วมจัดการ (Share) การร่วมหรือแบ่งความรับผิดชอบกับผู้อื่นในการจัดการความเสี่ยง
3. การลด (Reduce) การดำเนินการเพิ่มเติมเพื่อลดโอกาสที่อาจเกิดขึ้นหรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ ยอมรับได้
4. การยอมรับ (Accept) ความเสี่ยงที่เหลือในปัจจุบันอยู่ภายในระดับที่ต้องการและยอมรับได้แล้ว โดยไม่มีการดำเนิน การเพิ่มเติมเพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก

3.4.6 กิจกรรมควบคุม (Control Activities)

กิจกรรมการควบคุม คือ นโยบายและกระบวนการปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ซึ่งอาจมีการกำหนดกิจกรรม วัตถุประสงค์ที่ทำและการนำไปปฏิบัติที่เป็นเฉพาะของแต่ละองค์กรได้ แต่ควรมอบหมายผู้รับผิดชอบและประเมินประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่เสมอ รวมถึงกำหนดวันแล้วเสร็จให้ชัดเจน

3.4.7 ข้อมูลและการติดต่อสื่อสาร

สารสนเทศและการสื่อสาร จัดเป็นกิจกรรมที่สำคัญสำหรับการบริหารความเสี่ยงในองค์กร เพราะเป็นกระบวนการสื่อสารทั้งที่เป็นทางการ เช่น การรายงานข้อมูลที่สำคัญและจำเป็นต่อการบริหารความเสี่ยงในองค์กรกับผู้ปฏิบัติงานในองค์กร สำหรับการสื่อสารที่ไม่เป็นทางการกับผู้มีส่วนได้เสียก็มีความสำคัญเช่นเดียวกัน เพราะจะมีส่วนช่วยทำให้บุคลากรในองค์กรได้ทราบถึงทิศทางการดำเนินงานด้านการบริหารความเสี่ยง ตลอดจนการเสริมสร้างวัฒนธรรมที่เกี่ยวกับการบริหารความเสี่ยงองค์กรอีกทางหนึ่ง

3.4.8 การติดตามและประเมินผล

สพธอ. มีการติดตามผลตามแผนบริหารความเสี่ยงทุกไตรมาส เสนอต่อคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน และนำเสนอตามลำดับโครงสร้างที่กำหนดไว้ โดยการติดตามและประเมินผลมีวัตถุประสงค์สำคัญเพื่อ

1. ประเมินคุณภาพและความเหมาะสมของการจัดการความเสี่ยง
2. ติดตามผลการจัดการความเสี่ยงที่ได้ดำเนินการไปแล้ว หรืออยู่ระหว่างดำเนินการว่าบรรลุวัตถุประสงค์ของการบริหารความเสี่ยงที่วางไว้หรือไม่
3. ตรวจสอบความคืบหน้าของมาตรการควบคุม ว่าสามารถลดโอกาสหรือผลกระทบต่อเหตุการณ์ความเสี่ยงให้อยู่ในระดับที่ยอมรับได้หรือไม่

4. การจัดทำแผนบริหารจัดการความเสี่ยง ประจำปีงบประมาณ พ.ศ. 2568

ก่อนการชี้บ่งความเสี่ยงในปีงบประมาณใหม่ สพธอ. จะมีการทบทวนความเสี่ยงเดิมประกอบการวิเคราะห์การเปลี่ยนแปลงหรือแนวทางการดำเนินงานในอนาคต ซึ่งการวิเคราะห์เป็นดังนี้

4.1 ผลการบริหารความเสี่ยงตามแผนบริหารจัดการความเสี่ยง ประจำปีงบประมาณ 2567 พบว่า ประเด็นความเสี่ยงทุกด้านมีระดับความเสี่ยงลดลงจากต้นปีงบประมาณ โดยมีระดับค่าความเสี่ยงต่ำ จำนวน 3 หัวข้อ ระดับความเสี่ยงปานกลาง 2 หัวข้อ และ ไม่มีระดับความเสี่ยงสูงหรือสูงมาก รายละเอียดที่หน้า 18-28

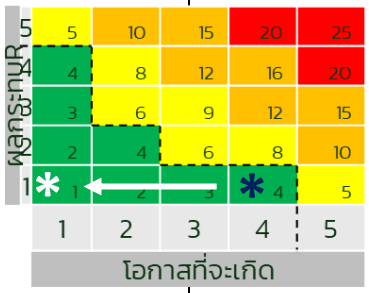
4.2 การดำเนินงานของ สพธอ. ในปีงบประมาณ พ.ศ. 2568 และแผนบริหารจัดการความเสี่ยง ประจำปีงบประมาณ 2568 รายละเอียดที่หน้า 29-50

4.1 ผลการบริหารความเสี่ยงตามแผนบริหารจัดการความเสี่ยง ประจำปีงบประมาณ 2567

หัวข้อความเสี่ยง : R1 การกำกับดูแลพระราชกฤษฎีกา Digital Platform

ปัจจัยความเสี่ยง (Risk Factor) : การกำกับดูแลที่มีผู้มีส่วนได้เสียเกี่ยวข้องจำนวนมาก รวมทั้งการออกมาตรการต่างๆ เพื่อการแก้ไขปัญหาของผู้ใช้บริการบนบริการแพลตฟอร์ม อาจส่งผลให้มีโอกาสได้รับผลกระทบเชิงลบและการดำเนินการทั้งหมด รวมถึงส่งผลต่อระดับความเชื่อมั่นต่อการใช้งาน Digital Platform Services

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน)
คะแนน	คำนิยาม (พิจารณาจากโอกาสที่ไม่มีมาตรการที่เกี่ยวกับ Digital Platform และไม่ถูกนำไปใช้จริง)	คำนิยาม (พิจารณาจากความสำเร็จในการใช้มาตร การไม่เกิดข่าวในเชิงลบ และระดับ ความเชื่อมั่นของประชาชน)
5 สูงที่สุด	นำปัญหาที่พบมากำหนดแนวทางการแก้ไข/มาตรการ เพื่อส่งเสริมให้เกิดความเชื่อมั่น	พบการเผยแพร่ข่าวในเชิงลบเกิน 5 วัน
4 สูง	มี (ร่าง) มาตรฐาน/มาตรการ	พบการเผยแพร่ข่าวในเชิงลบไม่เกิน 4-5 วัน
3 ปานกลาง	มีการประกาศใช้มาตรฐาน/มาตรการ	พบการเผยแพร่ข่าวในเชิงลบไม่เกิน 2-3 วัน หรือผล survey ความเชื่อมั่นในการใช้งาน Digital Service Platform ร้อยละ 70-74.99
2 ต่ำ	มีการประกาศใช้ พร้อมมีผู้ประกอบการแพลตฟอร์มนำไปใช้/ปฏิบัติแล้ว	พบการเผยแพร่ข่าวในเชิงลบไม่เกิน 1 วัน หรือ ผล survey ความเชื่อมั่นในการใช้งาน Digital Platform ร้อยละ 75-79.99
1 ต่ำที่สุด	มีการสื่อสารให้ประชาชนเข้าใจและรับทราบและมีตัวอย่าง Model ที่ใช้งานจริง	ไม่พบการเผยแพร่ข่าวในเชิงลบหรือผลการ survey ความเชื่อมั่นในการใช้งาน Digital Platform มากกว่าร้อยละ 80

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ	ผลการจัดการความเสี่ยง (สิ้นสุดปีงบประมาณ 2567)
- เริ่มมีการศึกษาปัญหาในบริการแพลตฟอร์มจากข้อมูลที่ประกอบการจดแจ้งหรือสถิติต่าง ๆ	**Reduce** - มีการกำหนดMitigation Plan ดังนี้ 1. การกำหนดมาตรการที่ใช้แก้ไขปัญหาได้จริง เช่น คู่มือการพิสูจน์และยืนยันตัวตนเพื่อลงทะเบียนเป็นผู้ใช้บริการบนบริการแพลตฟอร์มดิจิทัล 2. ผลักดันให้เกิด Modelและนำไปสู่การใช้งานเป็นวงกว้าง 3. สื่อสารมาตรการต่างๆ กับประชาชนอย่างสม่ำเสมอ เพื่อเพิ่มการรับรู้และนำไปสู่การเพิ่มความเชื่อมั่น	**- โอกาสที่จะเกิด = ระดับ 4** อยู่ในขั้นตอนศึกษาและ (ร่าง) มาตรการ **- ผลกระทบ = ระดับ 1** เนื่องจากไม่พบข่าวในเชิงลบ  	ศูนย์กำกับดูแลและตรวจสอบธุรกิจ	- **โอกาสจะเกิด = ระดับ 1** เนื่องจากประกาศข้อ เสนอแนะมาตรฐาน COD (Cash on Delivery) ที่มีการดำเนินการร่วมกับ สคบ. ได้มีการประกาศลงในราชกิจจานุเบกษา เมื่อวันที่ 5 กรกฎาคม 2567 และ สพธอ. ได้มีการสื่อสารในการแถลงข่าว “14 ปี ETDA ก้าวที่มั่นคง เพื่อชีวิตดิจิทัลที่มั่นใจ” - **ผลกระทบ = ระดับ 1** เนื่องจากไม่พบการเผยแพร่ข่าวในเชิงลบและระดับความเชื่อมั่นเกี่ยวกับ Digital Platform Services ที่ร้อยละ 86.2

หัวข้อความเสี่ยง : R2 การส่งเสริมการใช้ Digital ID

ปัจจัยความเสี่ยง (Risk Factor) : การไม่มีมาตรการผลักดัน ทำให้ Digital ID ยังไม่เกิดการประยุกต์ที่แพร่หลายและไม่ตอบสนองความคาดหวังของประชาชน

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน)
คะแนน	คำนิยาม (พิจารณาจากโอกาสที่ไม่เกิดการผลักดันการใช้ Digital ID)	คำนิยาม (พิจารณาจากการมีระบบยืนยันตัวตนใน e-service ของภาครัฐเพิ่มขึ้น)
5 สูงที่สุด	สพธอ.มี (ร่าง) แผนการผลักดันการใช้ Digital ID	e-service ภาครัฐที่ผลกระทบสูงเชื่อมต่อ Digital ID สำเร็จน้อยกว่าร้อยละ 35
4 สูง	มีการนำเสนอคณะกรรมการดิจิทัลฯ เพื่อ ให้การสนับสนุนก่อนไปหารือ กับหน่วยงานที่เกี่ยวข้อง	e-service ภาครัฐที่ผลกระทบสูงเชื่อมต่อ Digital ID สำเร็จร้อยละ 35-50
3 ปานกลาง	การหารือจนได้ข้อสรุปความเป็นไปได้กับหน่วยงานที่เกี่ยวข้อง 1 หน่วยงาน เช่น สำนักงบ ประมาณ หรือสำนักงาน กพร.	e-service ภาครัฐที่ผลกระทบสูงเชื่อมต่อ Digital ID สำเร็จร้อยละ 50-65
2 ต่ำ	การหารือจนได้ข้อสรุปความเป็นไปได้กับหน่วยงานที่เกี่ยวข้อง 2 หน่วยงาน	e-service ภาครัฐที่ผลกระทบสูงเชื่อมต่อ Digital ID สำเร็จร้อยละ 65-80
1 ต่ำที่สุด	ครม.เห็นชอบแนวทางการส่งเสริมและสนับสนุนให้หน่วยงานของรัฐใช้ Digital ID และมีการนำมาตรการ/แนวทางไปใช้	e-service ภาครัฐที่ผลกระทบสูงเชื่อมต่อ Digital ID สำเร็จไม่น้อยกว่าร้อยละ 80

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ	ผลการจัดการความเสี่ยง (สิ้นสุดปีงบประมาณ 2567)
มีข้อมูล จำนวน e-service ภาครัฐจาก สำนักงาน ก.พ.ร. และกรมการปกครอง และเบื้องต้นส่วนใหญ่มีความพร้อมในการให้บริการยืนยันตัวตนในปริมาณมาก (หมายเหตุ จำนวน 725 บริการเป็นไปตามข้อมูลของ กพร. ณ ต้นปีงบประมาณ 2567 ที่ภาครัฐมี มี e-service ที่พร้อมใช้งาน)	**Reduce** มีการกำหนดMitigation Plan ดังนี้ 1. การกำหนดบริการที่มี impact สูง เพื่อให้สามารถตอบสนองการใช้ประโยชน์ได้สูงสุดของประชาชน 2. การให้คำปรึกษาเพื่อแก้ปัญหาของแต่ละหน่วยงานเพื่อให้เกิดการเชื่อมต่อได้จริง 3. การสื่อสารคู่มือ เพิ่มกิจกรรมเชิญชวนให้เกิดความสมัครใจของ e-service ภาครัฐทั้งหมดให้มีการเชื่อมต่อ/ใช้ Digital ID	**โอกาสที่จะเกิด = ระดับ 5** เนื่องจากมี (ร่าง) แผนการผลักดันการใช้ Digital ID **ผลกระทบ = ระดับ 5** เนื่องจากอยู่ระหว่างขอข้อมูลและหารือกับหน่วยงานหลัก (ก.พ.ร.) 	หัวหน้าโครงการส่งเสริมและกำกับดูแล Digital ID ของประเทศ	- **โอกาสจะเกิด = ระดับ 2** การหารือด้าน Digital ID กับสำนักงบประมาณและสำนักงาน ก.พ.ร. ได้ดำเนินการแล้วเสร็จตั้งแต่ไตรมาส 1/2567 และ สพธอ. ได้พัฒนากรอบการขับเคลื่อน Thailand Digital ID Framework Phase 2 (พ.ศ. 2568-2570) และเตรียมเสนอคณะกรรมการโครงสร้างพื้นฐานดิจิทัลและคณะกรรมการ DE ในไตรมาส 1/2568 - **ผลกระทบ = ระดับ 3** สพธอ. ได้จัดกิจกรรมส่งเสริมและผลักดันให้เกิดการเชื่อมต่อ Digital ID และ eservice ภาครัฐ จนมีจำนวนเพิ่มขึ้นเป็น 449 บริการ จากจำนวน 725 บริการคิดเป็นร้อยละ 62%

หัวข้อความเสี่ยง : R3 การสนับสนุนยุทธศาสตร์ชาติด้าน AI

ปัจจัยความเสี่ยง (Risk Factor) : สพธอ. อาจดำเนินการไม่สำเร็จตามเป้าหมายที่กำหนดไว้ (สนับสนุนเป้าหมายแผน AI ของประเทศ) โดยเป้าหมายในปี 2567 มีดังนี้ 1) ประชาชนเกิดความรู้และความตระหนักด้าน AI & Governance ไม่น้อยกว่า 20,000 คน 2) AI Governance ไม่น้อยกว่า 1 ฉบับ 3) การประยุกต์ใช้ AI Governance ไม่น้อยกว่า 15 ราย (นับแบบสะสมต่อจากปี 2566)

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน)
คะแนน	คำนิยาม (พิจารณาจากโอกาสที่จะไม่มีธรรมาภิบาลด้านปัญญาประดิษฐ์)	คำนิยาม (พิจารณาจากการถูกนำไปประยุกต์ใช้ของภาครัฐและเอกชน สะท้อนความมีธรรมาภิบาลด้านปัญญาประดิษฐ์ของหน่วยงาน)
5 สูงที่สุด	มี Governance Guideline และ Toolkits ที่ สพธอ.จัดทำและเผยแพร่ แต่ไม่ได้รับการยอมรับหรือถูกนำไปใช้/ขยายผลต่อ	การให้คำปรึกษาการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล 1-2 ราย
4 สูง	มีการให้คำปรึกษา/ต่อยอด AI Governance Guideline และ Toolkits ที่ สพธอ.จัดทำและเผยแพร่ แต่ยังไม่มี Guideline หรือ Toolkits ที่ตอบโจทย์การใช้ AI ในปัจจุบันเพิ่มเติม	การให้คำปรึกษาการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล 3-4 ราย
3 ปานกลาง	มีการให้คำปรึกษา/ต่อยอด AI Governance Guideline และ Toolkits ที่สพธอ.จัดทำและเผยแพร่ และมี (ร่าง) guideline หรือ Toolkits ที่ตอบโจทย์การใช้งาน AI ในปัจจุบัน	การให้คำปรึกษาการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล 5-6 ราย
2 ต่ำ	มีการให้คำปรึกษา/ต่อยอด AI Governance Guideline และ Toolkits ที่สพธอ.จัดทำและเผยแพร่ และมีการนำร่องการใช้งาน guideline หรือ Toolkits ที่ตอบโจทย์การใช้งาน AI ในปัจจุบัน	การให้คำปรึกษาการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล 7-8 ราย
1 ต่ำที่สุด	มีการให้คำปรึกษา/ต่อยอด AI Governance Guideline และ Toolkits ที่สพธอ.จัดทำและเผยแพร่ และมี guideline หรือ Toolkits ใหม่เพิ่มเติมที่ตอบโจทย์การใช้ AI ปัจจุบันและถูกนำไปปรับใช้งาน	การให้คำปรึกษาการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล 9-10 ราย

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ	ผลการจัดการความเสี่ยง (สิ้นสุดปีงบประมาณ 2567)
- มีขั้นตอนที่ชัดเจนในการจัดทำ AI Governance Guideline - มีการหารือความร่วมมือในการดำเนินงานกับบาง Sector หรือในบาง Case study แล้ว	**Reduce** มีการกำหนดMitigation Plan ดังนี้ 1. พัฒนา AI Governance Guideline ที่ตรงกับความต้องการ ณ ปัจจุบัน จะทำให้เกิดประโยชน์สูงสุด (Generative AI) 2. มี toolkits ที่ตอบโจทย์การประยุกต์ใช้ที่หลากหลาย จะเป็นส่วนหนึ่งที่ทำให้เกิดการนำไปใช้เพิ่มขึ้นและช่วยส่งเสริมให้เกิดความเชื่อมั่นของผู้ใช้และผู้รับบริการ	**โอกาสจะเกิด = ระดับ 5** และ**ผลกระทบ = ระดับ 5** เนื่องจากยังไม่มีการนำ AI Guideline ไปใช้เพิ่มเติมและอยู่ระหว่างเตรียมทำ Guideline ฉบับใหม่ 	หัวหน้าโครงการ AI Governance	**-โอกาสจะเกิด = ระดับ 1** มีการนำร่องการใช้งาน AI Governance guideline หรือ toolkits แล้ว และอยู่ระหว่างรับฟังข้อคิดเห็น Generative AI guideline ในวันที่ 3 ก.ค. 2567 และมีหน่วยงานร่วมทดสอบ-ปรับใช้คู่มือฯ ขณะนี้รอการเผยแพร่อย่างเป็นทางการแล้ว **-ผลกระทบ = ระดับ 1** ปี 2567 ดำเนินการให้คำปรึกษาแล้ว 10 ราย ทั้งภาครัฐและเอกชน

หัวข้อความเสี่ยง : R4 การบริหารจัดการทรัพยากรบุคคล

ปัจจัยความเสี่ยง (Risk Factor) : ความไม่ชัดเจนของ career path อาจจะทำให้พนักงานไม่มีการรับรู้เส้นทางการเติบโตในสายงานและอาจจะทำให้ความรักที่จะทำงานอยู่กับองค์กรลดลง

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน)
คะแนน	คำนิยาม (พิจารณาจากโอกาสที่จะทบทวน Career path และการสื่อสารไม่สำเร็จ)	คำนิยาม (พิจารณาจากผล career path survey หมายเหตุ : ผล Career Path จะทำทั้ง deep focus / interview)
5 สูงที่สุด	ร้อยละความสำเร็จตามแผนการทบทวน career path และการสื่อสารที่มีประสิทธิภาพ ดำเนินการได้น้อยกว่าร้อยละ 25	ผล career path survey ลดลงจากปีที่ผ่านมามากกว่าร้อยละ 10
4 สูง	ร้อยละความสำเร็จตามแผนการทบทวน career path และการสื่อสารที่มีประสิทธิภาพ ดำเนินการได้ร้อยละ 25-40	ผล career path survey ลดลงจากปีที่ผ่านมาที่ร้อยละ 5-10
3 ปานกลาง	ร้อยละความสำเร็จตามแผนการทบทวน career path และการสื่อสารที่มีประสิทธิภาพ ดำเนินการได้ร้อยละ 40-55	ผล career path survey มีค่าการเปลี่ยนแปลงจากปีที่ผ่านมา อยู่ระหว่าง +/- ร้อยละ 0-5
2 ต่ำ	ร้อยละความสำเร็จตามแผนการทบทวน career path และการสื่อสารที่มีประสิทธิภาพ ดำเนินการได้ร้อยละ 55-70	ผล career path survey เพิ่มขึ้นจากปีที่ผ่านมาที่ร้อยละ 5-10
1 ต่ำที่สุด	ร้อยละความสำเร็จตามแผนการทบทวน career path และการสื่อสารที่มีประสิทธิภาพ ดำเนินการได้มากกว่าร้อยละ 70	ผล career path survey เพิ่มขึ้นจากปีที่ผ่านมามากกว่าร้อยละ 10

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ	ผลการจัดการความเสี่ยง (สิ้นสุดปีงบประมาณ 2567)
มีแผนการดำเนินงานของฝ่าย HR ที่สนับสนุนการวิเคราะห์ Career Path	**Reduce** มีการกำหนด Mitigation Plan โดยจัดทำ career path ของแต่ละตำแหน่งงาน ประกอบด้วย การขึ้นตำแหน่ง ภาระงาน การพัฒนาตนเอง การประเมิน ความคาดหวังขององค์กรในระดับต่างๆ โดย Q1-Q2 : วางแผนและกำหนดผู้รับผิดชอบหลักและจัดทำ career path พร้อมสื่อสาร Q3 : การสื่อสารกับระดับผู้บริหารและปฏิบัติการ Q4 : สรุปผล career path survey ซึ่ง career path จะทำให้พนักงานสามารถวางแผนการงาน พัฒนางาน/	**โอกาสจะเกิด = ระดับ 5** เนื่องจากเป็นการเริ่มดำเนินงานเทียบตามแผนงานปี 2567 **ผลกระทบ = ระดับ 3** โดยใช้ค่ากลางจากผล career path ของปีที่ผ่านมา 	ฝ่ายอำนวยการและทรัพยากรบุคคล	**โอกาสจะเกิด = ระดับ 1** (มากกว่าร้อยละ 70) 1. Career Path สื่อสารกับทีม Lead ครบแล้วและมีการอัพเดทครบทุกหน่วยงานเกี่ยวกับสถานะปัจจุบันกับอัตรากำลังคน (ร้อยละ 100) 2. ติดตามการประเมินผลการปฏิบัติงาน และติดตามแผนการพัฒนารายบุคคล รวมทั้ง HR เข้าไปช่วยสนับสนุนหาหลักสูตรเพิ่มเติม (on process: ร้อยละ 80) 3. ด้าน Succession Plan ของผู้อำนวยการ (JG9) มีการประชุมคณะทำงานด้าน Succession 2 ครั้ง และมีการจัดลำดับ Successor แล้ว (ร้อยละ 100) **ผลกระทบ = ระดับ 2** ใช้ผลสำรวจปีปัจจุบัน (2567) เทียบผลของการสำรวจ Career Path ปี 2566 (คะแนนเต็ม = 5) เป็นดังนี้ - การได้รับมอบหมายงานทำให้ท่านมีโอกาสพัฒนาความรู้และทักษะใหม่ 4.07 (ปี 2566 = 3.98)

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ	ผลการจัดการความเสี่ยง (สิ้นสุดปีงบประมาณ 2567)
	ตนเองให้ดีขึ้น และสามารถวางแผนอนาคตได้			- ท่านรู้สึกว่าตำแหน่งหน้าที่ของท่านเป็นตำแหน่งที่มีดอกาสก้าวหน้าในอาชีพ 3.70 (ปี 2566 = 3.53) - ท่านมองเห็นตัวเองเติบโตในสายงานของท่านในองค์กรในอีก 2 ปีข้างหน้า 3.52 (ปี 2566 = 3.13) เทียบผลเฉลี่ย 2567 และ 2566 จะได้ (3.76-3.55)/3.55*100 = เพิ่มขึ้นร้อยละ 5.91

หัวข้อความเสี่ยง : R5 การเบิกจ่ายงบประมาณ

ปัจจัยความเสี่ยง (Risk Factor) : การได้รับงบประมาณ 2 รอบ อาจมีผลต่อการใช้งบประมาณไม่บรรลุตามเป้าหมายที่กำหนดไว้

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน)
คะแนน	คำนิยาม (พิจารณาจากการใช้งบประมาณไม่เป็นไปตามแผนของสำนักงบประมาณที่กำหนดไว้ (จ่ายจริง + ผูกพัน))	คำนิยาม (พิจารณาจากการใช้จ่ายงบประมาณประจำปี (งบประมาณแผ่นดิน (จ่ายจริง))
5 สูงที่สุด	ดำเนินการได้น้อยกว่าร้อยละ 25 เทียบกับแผนของสำนักงบประมาณ	มีการใช้จ่ายจริงสำเร็จน้อยกว่า 80% (เทียบแผนรายไตรมาส)
4 สูง	ดำเนินการได้ที่ร้อยละ 25-39.9 เทียบกับแผนของสำนักงบประมาณ	มีการใช้จ่ายจริงสำเร็จน้อยกว่า 85-80% (เทียบแผนรายไตรมาส)
3 ปานกลาง	ดำเนินการได้ที่ ร้อยละ 40-54.9 เทียบกับแผนของสำนักงบประมาณ	มีการใช้จ่ายจริงสำเร็จน้อยกว่า 90-85% (เทียบแผนรายไตรมาส)
2 ต่ำ	ดำเนินการได้ที่ ร้อยละ 55-69.9 เทียบกับแผนของสำนักงบประมาณ	มีการใช้จ่ายจริงสำเร็จน้อยกว่า 95-90% (เทียบแผนรายไตรมาส)
1 ต่ำที่สุด	ดำเนินการได้มากกว่า ร้อยละ 70 เทียบกับแผนของสำนักงบประมาณ	มีการใช้จ่ายจริงตามแผนงบประมาณที่ตั้งไว้สำเร็จมากกว่าเท่ากับ 95% (เทียบแผนรายไตรมาส)

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ	ผลการจัดการความเสี่ยง (สิ้นสุดปีงบประมาณ 2567)
มีแผนการจัดซื้อจัดจ้างและแผนการใช้จ่ายงบประมาณประจำปี 2567	**Reduce** มีการกำหนดMitigation Plan ดังนี้ 1. เร่งรัดการผูกพันสัญญาให้แล้วเสร็จภายในไตรมาส 1 และ 3 2. กำหนดรายการซื้อจ้างของสองไตรมาสสุดท้ายไว้ล่วงหน้า 3. ติดตามสถานะการเบิกจ่ายอยู่เสมอ (รายเดือน) การปรับปรุงแผนเพื่อควบคุมการเบิกจ่ายให้เป็นปัจจุบัน	**ทั้งโอกาสและผลกระทบ = ระดับ 5** เนื่องจากเป็นการเริ่มต้นปีงบประมาณ 	ฝ่ายบริหารกลาง / ฝ่ายนโยบายและแผน	**โอกาสจะเกิด = ระดับ 1** ผลเบิกจ่าย = 586.68/590.54 = 99% เทียบกับแผน สงป. Q4 กำหนดที่ร้อยละ 100 **ผลกระทบ = ระดับ 5** เบิกจ่ายจริงตามแผนรายไตรมาส (Q1-Q4) ต้องไม่น้อยกว่าร้อยละ 90 (531.48 ลบ.) พบว่าดำเนินการได้ 407.11 ลบ. ดังนั้นคิดเป็นร้อยละ 76.6

4.2 การดำเนินงานของ สพธอ. และแผนบริหารจัดการความเสี่ยง ประจำปีงบประมาณ 2568

ในปี 2568 พบว่าบทบาทในการกำกับดูแลทั้งในส่วนธุรกิจบริการ Digital ID และบริการแพลตฟอร์มดิจิทอล ที่มีความชัดเจนเพิ่มมากขึ้นกว่าปีที่ผ่านมา ภายหลังจากการบังคับใช้กฎหมาย พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565 และพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565 สพธอ. ได้มีการประกาศต่าง ๆ เพิ่มเติมทั้งในรูปแบบประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ แนวทาง (Guideline) แนวปฏิบัติที่ดี (Best Practice) และกลไกดูแลตนเองที่เหมาะสม (Self-Regulation) รวมทั้งการมีกระบวนการที่เพิ่มเติมขึ้นมา ได้แก่ การให้ผู้ประกอบธุรกิจบริการแพลตฟอร์มดิจิทัลยื่นรายงานประจำปีและรายงาน Term & Condition ตามที่กฎหมายกำหนด การตรวจประเมินประจำปีสำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตน จึงทำให้หัวข้อความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ยังคงเน้นที่การกำกับดูแลของทั้งสองงานหลัก สำหรับความเสี่ยงด้านการดำเนินงาน (Operational Risk) ยังคงให้ความสำคัญต่อการบริหารทรัพยากรบุคคลอย่างต่อเนื่อง และเพิ่มเติมประเด็นเกี่ยวกับการให้บริการและกระบวนการกำกับดูแลข้อมูลที่อาจส่งผลกระทบต่อภาพลักษณ์ ชื่อเสียงของหน่วยงาน (Reputational Risk) และสุดท้าย ความเสี่ยงด้านการเงิน (Financial Risk) ยังคงเป็นการบริหารการใช้งบประมาณ แต่มีการเพิ่มเติมประเด็นในการบริหารเงินทุนสะสมขององค์กร

โดยแผนบริหารความเสี่ยงประจำปี พ.ศ. 2568 ได้รับความเห็นชอบของคณะกรรมการ เมื่อพฤศจิกายน 2567 และมีการปรับปรุงอีกครั้งในเดือนมีนาคม 2568 ประกอบด้วย

ความเสี่ยง	หัวข้อความเสี่ยงและปัจจัยความเสี่ยง
ความเสี่ยงด้านกลยุทธ์ (Strategic : S) **วัตถุประสงค์ (Objective) :** ประชาชนมีความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์	**SR1-A การกำกับดูแล Digital ID (1)** มาตรฐานหรือหลักเกณฑ์อาจไม่เพียงพอในการปิดความเสี่ยงที่สำคัญของ Digital ID (Misidentification) ด้วยเหตุของการเปลี่ยนแปลงของเทคโนโลยี
	SR1-B การกำกับดูแล Digital ID (2) ผู้ให้บริการที่ สพธอ. กำกับดูแลเกิดปัญหา ด้านมาตรฐานหรือระบบงานที่กระทบต่อผู้ใช้บริการอย่างมีนัยสำคัญ (รวมถึง Cyber incident และ Data protection)

ความเสี่ยง	หัวข้อความเสี่ยงและปัจจัยความเสี่ยง
มีความถูกต้อง ปลอดภัย และน่าเชื่อถือ	**SR2 การกำกับดูแลบริการแพลตฟอร์มดิจิทอล** ปัญหาที่เกิดจากผู้ที่มีพฤติกรรมที่ไม่เหมาะสมในบริการแพลตฟอร์มดิจิทัลอาจนำมาสู่ความไม่เชื่อมั่นในการใช้งาน Digital Platform Services
ความเสี่ยงด้านการดำเนินงาน (Operational : O) **วัตถุประสงค์ (Objective) :** สพธอ. ดำเนินการได้ตามเป้าหมายองค์กรที่กำหนดไว้ มีความพร้อมในการปฏิบัติงานและปฏิบัติตามกฎหมายระเบียบต่าง ๆ ครบถ้วน	**OR1** มีเหตุการณ์ด้านความมั่นคงปลอดภัย (Cyber-attack) เกิดขึ้นกับ e-Service ที่ให้บริการกับคนภายนอก ได้แก่ ระบบจดแจ้ง DPS / ระบบออกใบอนุญาต DID / เว็บไซต์สำนักงาน / Facebook page
	OR2 พนักงานกลุ่ม Team Lead มีความเครียดสูง ซึ่งอาจส่งผลต่อการบริหารงานและทีมงาน รวมถึงความผูกพันต่อองค์กร
	OR3 ระบบสารสนเทศภายในสำนักงาน เกิดข้อผิดพลาดไม่สามารถให้บริการกับพนักงานได้ เช่น ระบบสารบรรณ / ระบบ ERP /ระบบจองทรัพยากรใน Intranet / WIFI / Internet
	OR4 มีข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว รั่วไหลออกจากระบบที่สำคัญเช่น ระบบจดแจ้ง DPS / ระบบออกใบอนุญาต DID ฐานข้อมูลการฝึกอบรม ฐานข้อมูลพนักงานภายใน
ความเสี่ยงด้านการเงิน (Financial : F) **วัตถุประสงค์ (Objective) :** สพธอ. มีความพร้อมในการปฏิบัติงาน และปฏิบัติตามกฎหมาย ระเบียบต่าง ๆ ครบถ้วน	**FR1** การจัดซื้อจัดจ้างในโครงการต่างๆ มีความล่าช้าไม่เป็นไปตามเป้าหมาย
	FR2 เงินทุนสะสมไม่เพียงพอหรือไม่สมดุลเมื่อเทียบกับรายการใช้จ่าย ทำให้ไม่สามารถดำเนินกิจกรรมที่สาคัญได้

หมายเหตุ *SR1-B และ OR4 เกี่ยวข้องกับ Reputation Risk

โดยมีรายละเอียดของแต่ละประเด็นความเสี่ยงดังต่อไปนี้

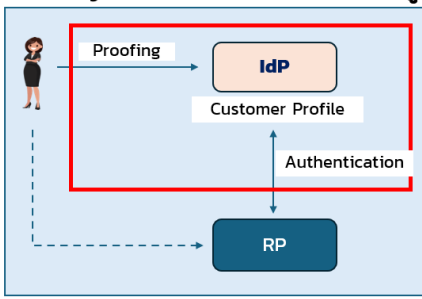
ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : SR)

1) การควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)

กฎหมายที่ สพธอ. มีหน้าที่ในการกำกับดูแล คือ พระราชกฤษฎีกาการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565 ซึ่งมีวัตถุประสงค์ ให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความน่าเชื่อถือ ความปลอดภัย และป้องกันความเสียหายต่อสาธารณะ

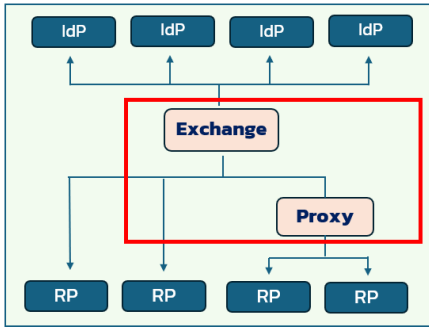
โดยระบบนิเวศน์ของการพิสูจน์และยืนยันตัวตน สามารถแบ่งออกเป็นสองกลุ่ม ได้แก่ กลุ่มที่ 1 – ผู้ให้บริการพิสูจน์และยืนยันตัวตน และกลุ่มที่ 2 – ผู้ให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตน ซึ่งแต่ละกลุ่มมีความเสี่ยงในการดำเนินงานแตกต่างกันและมีการกำหนดวิธีการลดความเสี่ยงไว้แล้ว ดังรูป

Ecosystem ที่สะท้อนการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) และประเด็น Concern



กลุ่มที่ 1 – ผู้ให้บริการพิสูจน์และยืนยันตัวตน

Major concern	Control
1. กระบวนการพิสูจน์ และยืนยันตัวตน สามารถ **Identify บุคคลได้อย่างถูกต้อง**	• การกำหนดมาตรฐานของกระบวนการพิสูจน์และยืนยันตัวตน
2. มีกลไกใน**การดูแลข้อมูลส่วนบุคคล**	• กำหนดกลไกการควบคุมและบริหารจัดการข้อมูล
3. ระบบให้บริการ**มีความมั่นคงปลอดภัย**	• กำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัย



กลุ่มที่ 2 – ผู้ให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตน

Major concern	Control
1. การเชื่อมต่อสามารถ**รับส่งข้อมูลไปยังต้นทาง-ปลายทาง ได้อย่างถูกต้อง**	• กำหนดกลไกการควบคุมและบริหารจัดการข้อมูล
2. ระบบให้บริการมีความมั่นคงปลอดภัย และสามารถ**ให้บริการได้อย่างต่อเนื่อง**	• กำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัย
3. มีกลไกในการดูแล**ข้อมูลส่วนบุคคล**	• กำหนดกลไกการควบคุมและบริหารจัดการข้อมูล

แต่ปัจจัยภายนอกที่ยังไม่อาจควบคุมได้ในการพิสูจน์และยืนยันตัวตนได้ คือ เทคโนโลยีที่ปลอมแปลงอัตลักษณ์ได้ รวมถึงภัยคุกคามที่ส่งผลต่อความปลอดภัยของข้อมูล ซึ่งมีแนวโน้มเพิ่มมากขึ้นในปัจจุบัน จึงเป็นที่มาของการกำหนดประเด็นความเสี่ยง ดังนี้

หัวข้อความเสี่ยง : SR1-A การใช้ Digital ID

ปัจจัยความเสี่ยง (Risk Factor) : มาตรฐานหรือหลักเกณฑ์อาจไม่เพียงพอในการปิดความเสี่ยงที่สำคัญของ Digital ID (Misidentification) ด้วยเหตุของการเปลี่ยนแปลงของเทคโนโลยี

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน)
คะแนน	คำนิยาม (พิจารณาจากโอกาสที่แนวปฏิบัติหรือมาตฐานที่ใช้ในการดำเนินงานด้าน Digital ID ไม่ดีเพียงพอ นำไปสู่เหตุการณ์ไม่พึงประสงค์)	คำนิยาม (พิจารณาจากผลกระทบจากการ Misidentification)
5 สูงที่สุด	สพธอ. มีหลักเกณฑ์ที่ไม่เพียงพอต่อการกำกับดูแลจนทำให้เป็นประเด็นที่มีความเสี่ยงสูงในภายหลัง เช่น ภัยการปลอมแปลงตัวตนจากเทคโนโลยีใหม่	เกิดการปลอมแปลงตัวตนได้แม้ดำเนินการตามหลักเกณฑ์ที่ สพธอ. กำหนดแล้วและเกิดผลกระทบเป็นวงกว้าง เช่น เกิดขึ้นใน IdP หลายราย
4 สูง	สพธอ. มีหลักเกณฑ์ที่เป็นไปตามมาตรฐานโลกในเรื่องสำคัญให้ผู้ประกอบธุรกิจปฏิบัติตาม แต่ผู้ประกอบการอาจยังไม่ Comply โดยทั่วถึง	เกิดความผิดพลาดรุนแรงที่ทำให้บุคคลได้รับผลกระทบด้านกฎหมาย การเงิน หรือชื่อเสียง เช่น - เสียเงินจำนวนมากจากการฉ้อโกง
3 ปานกลาง	สพธอ. มีหลักเกณฑ์ที่เป็นไปตามมาตรฐานโลกในเรื่องสำคัญ และผู้ประกอบธุรกิจส่วนใหญ่ปฏิบัติตามหลักเกณฑ์ที่ สพธอ. มีการกำหนดไว้	เกิดข้อผิดพลาดที่ส่งผลเสียต่อธุรกรรมที่สำคัญ และต้องใช้เวลานานในการแก้ไข เช่น ระบบระบุผิดว่าผู้ใช้เป็นบุคคลต้องสงสัย ทำให้ถูกตรวจสอบเพิ่มเติม
2 ต่ำ	ดำเนินการได้ตามระดับ 3 และสพธอ. มีการหารือร่วมกับ Sector สำคัญ และ Stakeholder เพื่อทบทวนมาตรฐาน/ แนวทางปฏิบัติเพิ่มเติม	เกิดข้อผิดพลาดที่เริ่มส่งผลต่อประสบการณ์ผู้ใช้หรือธุรกรรมเล็กน้อย เช่น ไม่สามารถเข้าถึงบริการทางการเงินหรือสุขภาพได้ในทันที
1 ต่ำที่สุด	ดำเนินการได้ตามระดับ 3 และสพธอ. มีข้อสรุปร่วมกันกับ Sector สำคัญเกี่ยวกับความเพียงพอของมาตรฐาน/แนวปฏิบัติใหม่หรือการปรับปรุงมาตรฐาน	เกิดความไม่สะดวกเล็กน้อยในการใช้งานระบบ เช่น การยืนยันตัวตนใช้เวลานานขึ้นจากปัญหาทางเทคนิค

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
- มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล (มธอ. 11-2566) - ประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 3 หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ และฉบับที่ 4 หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ - การตรวจประเมินผู้ประกอบธุรกิจบริการ DID ตามรอบที่กำหนด	**Reduce** - มีการศึกษา fraud ที่เกี่ยวกับยืนยันตัวตน Biometric เพื่อดูสภาพปัญหาที่เกิดขึ้นในลำดับต้นๆ - การทบทวนหลักเกณฑ์/มาตรการ/แนวทางเกี่ยวกับการยืนยันตัวตน ร่วมกับ Stakeholder - กระบวนการสื่อสารกับ Stakeholder/ Regulator ที่เกี่ยวข้อง เพื่อเกิดการสูญเสียทรัพย์อัพเดทความคืบหน้าของมาตรฐานที่เกี่ยวข้อง - การอัพเดทความรู้เกี่ยวกับมาตรฐานหรือแนวทางการกำกับดูแลที่เกี่ยวข้องผ่านช่องทางต่าง ๆ	**- โอกาสที่จะเกิด = ระดับ 3** สพธอ. มีหลักเกณฑ์ที่เป็นไปตามมาตรฐานโลกในเรื่องสำคัญ และผู้ประกอบธุรกิจส่วนใหญ่ปฏิบัติตามหลักเกณฑ์ที่ สพธอ. มีการกำหนดไว้ **- ผลกระทบ = ระดับ 4** เกิดความผิดพลาดรุนแรงที่ทำให้บุคคลได้รับผลกระทบด้านกฎหมาย การเงิน หรือชื่อเสียง เช่น - เสียเงินจำนวนมากจากการฉ้อโกง 	ศูนย์นโยบาย พัฒนามาตรฐานและหลักเกณฑ์การกำกับดูแลและศูนย์กำกับดูแลและตรวจสอบธุรกิจ

หัวข้อความเสี่ยง : SR1-B การกำกับดูแล Digital ID (2)

ปัจจัยความเสี่ยง (Risk Factor) : ผู้ให้บริการที่ สพธอ. กำกับดูแล เกิดปัญหาด้านมาตรฐานหรือระบบงานที่กระทบต่อผู้ใช้บริการอย่างมีนัยสำคัญ (รวมถึง Cyber incident และ Data protection) (เฉพาะ Digital ID)

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน)	เกณฑ์ผลกระทบ (ด้าน reputation)
คะแนน	คำนิยาม (พิจารณาจากโอกาสที่ผู้ให้บริการเกิดเหตุการณ์/ ปัญหาที่เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตน)	คำนิยาม (พิจารณาจากผลกระทบที่สืบเนื่องจากการเกิด incident)	
5 สูงที่สุด	เกิดปัญหาแต่ไม่สามารถหาสาเหตุหรือแก้ได้	เกิดการปลอมแปลงการพิสูจน์และยืนยันตัวตน	พบการเผยแพร่ข่าวในเชิงลบเกิน 5 วัน
4 สูง	เกิดปัญหาและทราบแนวทางการแก้ไข	เกิดการรั่วไหลของข้อมูลส่วนบุคคล ที่สามารถระบุตัวตนได้ (เช่น ID Card ข้อมูลอัตลักษณ์)	พบการเผยแพร่ข่าวในเชิงลบไม่เกิน 4-5 วัน
3 ปานกลาง	เกิดปัญหาและอยู่ระหว่างการแก้ไข	เกิดการรั่วไหลของข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล	พบการเผยแพร่ข่าวในเชิงลบไม่เกิน 2-3 วัน
2 ต่ำ	สพธอ. ดำเนินการตรวจสอบและปิดประเด็นปัญหาแล้ว	ระบบพิสูจน์และยืนยันตัวตนถูกล็อค เสียโอกาสการทำธุรกรรม	พบการเผยแพร่ข่าวในเชิงลบไม่เกิน 1 วัน
1 ต่ำที่สุด	ไม่พบเหตุการณ์/ปัญหา	ระบบไม่สามารถจดจำใบหน้าหรือลายนิ้วมือได้ต้องทดลองใหม่หลายครั้ง	ไม่พบการเผยแพร่ข่าวในเชิงลบ

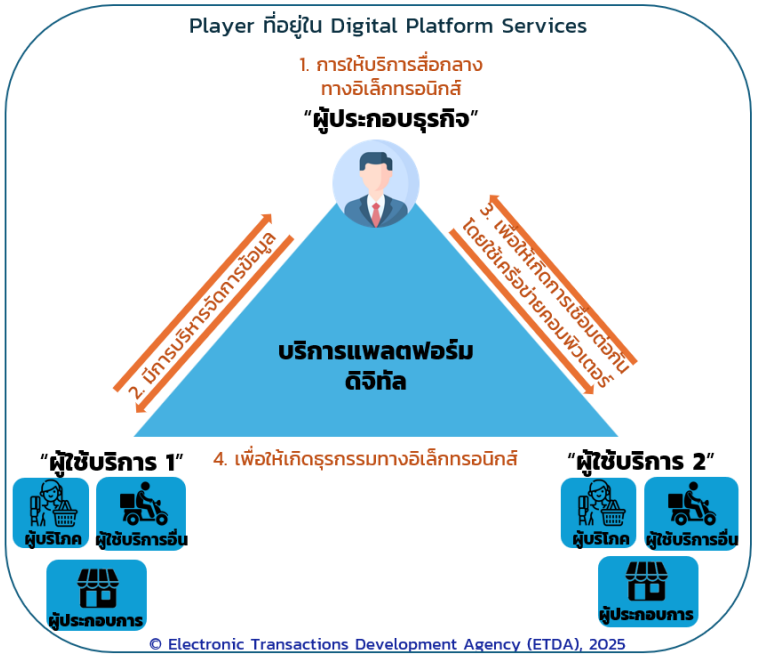
หมายเหตุ กรณีที่เกิดเหตุการณ์ขึ้นจริงมีความเสียหายทั้ง 2 ด้าน ให้ใช้ค่าสูงสุดมาเป็นตัวแทนในการคำนวณระดับความเสี่ยง (Likelihood x Impact)

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
- ประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 5 หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการเกี่ยวกับระบบพิสูจน์และยืนยันตัวตน - ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 7 หลักเกณฑ์การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ	**Reduce** - ผู้ให้บริการมีการดำเนินการตามกฎหมาย มาตรฐาน ที่ สพธอ. กำหนด - ผู้ให้บริการ Digital ID มีการดำเนินการตามมาตรฐาน ISO27001 เป็นอย่างน้อย เพื่อความปลอดภัย มั่นคงด้านสารสนเทศ - สพธอ. มีช่องทางการรับข้อร้องเรียนของผู้ใช้บริการ Digital ID และหากพบปัญหาจาก ผู้ให้บริการ สพธอ. ดำเนินการกำกับให้มีการแก้ไข-ปรับปรุง และติดตามผลการแก้ไข	**- โอกาสที่จะเกิด = ระดับ 1** ไม่พบเหตุการณ์/ปัญหา **- ผลกระทบ = ระดับ 4** อาจเกิดการรั่วไหลของข้อมูลส่วนบุคคล ที่สามารถระบุตัวตนได้ (เช่น ID Card ข้อมูลอัตลักษณ์)  	ศูนย์กำกับดูแลและตรวจสอบธุรกิจ

2) การกำกับดูแลธุรกิจบริการแพลตฟอร์มดิจิทัล (Digital Platform Services)

กฎหมายที่ สพธอ. มีหน้าที่ในการกำกับดูแล คือ พระราชกฤษฎีกาการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัลที่ต้องแจ้งให้ทราบ พ.ศ. 2565 ซึ่งมีวัตถุประสงค์ ให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความน่าเชื่อถือ ผ่านความน่าเชื่อถือของระบบและข้อมูล ทำให้มีความโปร่งใสเป็นธรรมและป้องกันความเสียหายต่อสาธารณะ

โดยระบบนิเวศน์ของการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัล (Digital Platform Services) มีผู้เกี่ยวข้องจำนวน 3 แบบและทำหน้าที่แตกต่างกัน ดังรูป



การกำกับดูแลธุรกิจบริการแพลตฟอร์มดิจิทัล มีประเภทของแพลตฟอร์มดิจิทัลทั้งสิ้น 15 ประเภท ดังนั้น สพธอ. จึงเลือกที่จะให้ความสำคัญไปที่แพลตฟอร์มส่งผลกระทบสูงต่อภาคเศรษฐกิจและสังคม คือ ประเภท e-Market place เนื่องจากมีผู้เข้าถึงเป็นวงกว้าง ทั้งผู้บริโภค ผู้ใช้บริการอื่น และผู้ประกอบการ โดยพบว่าปัญหาหลักที่พบ คือ "การหลอกลวง" ซึ่งนำไปสู่การสูญเสียทรัพย์สิน เช่น สินค้าไม่ตรงปก ไม่ได้รับสินค้า ถูกหลอกให้ลงทุน

เมื่อวิเคราะห์ถึงสาเหตุปัจจัยเสี่ยงจะพบว่าผู้ที่มีพฤติกรรมไม่เหมาะสม กระทำการหลอกลวง (Bad Actor) อาจมาจาก 1. ผู้ที่อยู่ในแพลตฟอร์มตั้งใจหลอกลวง ให้ลงทุน/ ไม่จัดส่งสินค้า/ ขายสินค้าที่ไม่ได้มาตรฐาน/ ไม่ดำเนินการตามข้อกำหนดของแพลตฟอร์ม หรือ 2. ผู้ประกอบธุรกิจบริการแพลตฟอร์มอาจยังไม่มีการกำกับดูแลที่เหมาะสม เช่น ไม่ตรวจสอบ ไม่มีการควบคุมสินค้าที่ไม่ได้มาตรฐาน/ โฆษณาชวนเชื่อ

หัวข้อความเสี่ยง : SR2 การกำกับดูแล Digital Platform Services

ปัจจัยความเสี่ยง (Risk Factor) : ปัญหาที่เกิดจากผู้ที่มีพฤติกรรมที่ไม่เหมาะสมในบริการแพลตฟอร์มดิจิทัลอาจนำมาสู่ความไม่เชื่อมั่นในการใช้งาน Digital Platform Services

เกณฑ์/ คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (เชิงปริมาณ) (Impact)	เกณฑ์ผลกระทบ (เชิงคุณภาพ) (Impact)
คะแนน	คำนิยาม (พิจารณาจากระดับที่มาตรการถูกนำไปใช้โดยแพลตฟอร์ม)	คำนิยาม (พิจารณาจากจำนวนกรณีที่เกิดความเสียหาย (ไตรมาส) *เฉพาะที่รายงานมาที่ 1212ETDA*)	คำนิยาม (พิจารณาจากความเชื่อมั่นของการใช้งาน Digital Platform Services เฉพาะในส่วนที่ ETDA รับผิดชอบ)
5 สูงที่สุด	สพธอ. ไม่มีมาตรการที่ช่วยลดปัญหา	> 600 ราย	มากกว่า ร้อยละ 90
4 สูง	สพธอ. มีการประกาศมาตรการ เพื่อลดการเกิดปัญหา	451-600	ร้อยละ 80.1-90
3 ปานกลาง	สื่อสารมาตรการต่าง ๆ กับผู้บริโภค/ผู้ประกอบการ/เจ้าของแพลตฟอร์ม	301-450 ราย	ร้อยละ 70.1-80
2 ต่ำ	แพลตฟอร์มมีการนำมาตรการไปใช้หรือปรับปรุงการให้บริการ	151-300 ราย	ร้อยละ 60.1-70
1 ต่ำที่สุด	มีการร่วมมือกับหน่วยงานอื่น เพื่อป้องกันปัญหาของแพลตฟอร์ม	0-150 ราย	น้อยกว่าหรือเท่ากับร้อยละ 60

หมายเหตุ กรณีที่เกิดเหตุการณ์ขึ้นจริงมีความเสียหายทั้ง 2 ด้าน ให้ใช้ค่าสูงสุดมาเป็นตัวแทนในการคำนวณระดับความเสี่ยง (Likelihood x Impact)

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
<u>มาตรการสำหรับผู้ประกอบธุรกิจแพลตฟอร์มดิจิทัล</u> - คู่มือการพิสูจน์และยืนยันตัวตน เพื่อลงทะเบียนเป็นผู้ใช้บริการบนบริการแพลตฟอร์มดิจิทัล - คู่มือการดูแลโฆษณาบนบริการแพลตฟอร์มดิจิทัล - คู่มือการดูแลเกี่ยวกับการขายสินค้าที่ต้องมีมาตรฐานของสินค้าบนบริการแพลตฟอร์มดิจิทัล - ต้องรายงานต่อ สพธอ. เกี่ยวกับเรื่องร้องเรียนที่มีจำนวนมากที่สุดห้าลำดับแรก แนวทางการจัดการและระงับข้อพิพาท <u>มาตรการคุ้มครองผู้ใช้บริการ</u> - ประกาศข้อเสนอแนะมาตรฐานฯ บริการเก็บเงินปลายทางสำหรับพาณิชย์อิเล็กทรอนิกส์ - การสื่อสารสร้างความตระหนักรู้ผ่านช่องทางต่าง ๆ	**Reduce** - ส่งเสริม/ขยายผลให้เกิดการใช้คู่มือต่าง ๆ เช่น การหารือกับแพลตฟอร์มขนาดใหญ่ - อาจเพิ่มเติมมาตรการจากการวิเคราะห์ปัญหา เรื่อง Bad actor - การหารือเพื่อ convince กับ Regulator อื่น เพื่อให้เกิดการนำไปขยายผลการใช้งานมากขึ้น	**- โอกาสที่จะเกิด = ระดับ 4** สพธอ. มีมาตรการ/คู่มือ แต่อาจต้องเพิ่มการสื่อสารให้ครบทุก Stakeholder เพื่อรักษาระดับความเชื่อมั่นในการทำธุรกรรมฯ **- ผลกระทบ = ระดับ 5** จำนวนกรณีที่เกิดความเสียหาย (ไตรมาส) เฉพาะที่รายงานมาที่ 1212ETDA ปี 2567 อยู่ที่ประมาณ 650 ราย/ไตรมาส 	งานกำกับแพลตฟอร์มดิจิทัลและฝ่ายดูแลบริการธุรกรรมทางอิเล็กทรอนิกส์

ความเสี่ยงด้านการดำเนินงาน (Operational Risk : OR)

ความเสี่ยงด้านการดำเนินงาน มาจากการพิจารณาความเสี่ยงจากทรัพยากรที่มี กระบวนการทำงานขององค์กร รวมถึงปัจจัยภายนอกที่อาจเกิดขึ้นจนส่งผลกระทบต่อวัตถุประสงค์ของ สพธอ. ที่ต้องการดำเนินการได้ตามเป้าหมายองค์กรที่กำหนดไว้ มีความพร้อมในการปฏิบัติงาน และปฏิบัติตามกฎหมาย ระเบียบต่าง ๆ ครบถ้วน

หัวข้อความเสี่ยง : OR1

ปัจจัยความเสี่ยง (Risk Factor) : มีเหตุการณ์ด้านความมั่นคงปลอดภัย (Cyber-attack) เกิดขึ้นกับ e-Service ที่ให้บริการกับคนภายนอก ได้แก่ ระบบจดแจ้ง DPS / ระบบออกใบอนุญาต DID / เว็บไซต์สำนักงาน / Facebook page

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน) (Impact)
คะแนน	คำนิยาม (พิจารณาจากจำนวนครั้งการเกิดเหตุการณ์ในรายไตรมาส)	คำนิยาม (พิจารณาจากผลกระทบต่อผู้ใช้บริการ)
5 สูงที่สุด	มากกว่า 3 ครั้ง/ไตรมาส	ทำให้ผู้ใช้บริการผิดกฎหมาย (ไม่สามารถยื่นเอกสารได้ทันตามกำหนดเวลา)
4 สูง	3 ครั้ง/ไตรมาส	ทำให้ผู้ใช้บริการเสียสิทธิ์/เสียผลประโยชน์ (ข้อมูลรั่วไหล/ ไม่สามารถตรวจ สอบข้อมูลได้)
3 ปานกลาง	2 ครั้ง/ไตรมาส	ผู้ใช้บริการมีการแจ้งเรื่อง/ข้อร้องเรียนมาที่ สพธอ.
2 ต่ำ	1 ครั้ง/ไตรมาส	ระบบใช้งานไม่ได้ชั่วคราว (ตรวจพบเจอภายใน สพธอ. เอง)
1 ต่ำที่สุด	ไม่เกิดขึ้นเลย	ผู้รับบริการไม่ได้รับผลกระทบ

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
- มีขั้นตอนการปฏิบัติงานในการรักษาความมั่นคงปลอดภัย - มีระบบตรวจสอบการโจมตีจากภายนอก	**Reduce** - การรักษาระบบมาตรฐานด้านสารสนเทศ ISO27001 - การซ้อมแผนการกู้คืนระบบต่าง ๆ	**- โอกาสที่จะเกิด = ระดับ 1** ไม่เกิดขึ้นเลย **- ผลกระทบ = ระดับ 5** ทำให้ผู้ใช้บริการผิดกฎหมาย (ไม่สามารถยื่นเอกสารได้ทันตามกำหนดเวลา) 	ศูนย์ระบบโครงสร้างพื้นฐานด้านสารสนเทศและความมั่นคงปลอดภัย

หัวข้อความเสี่ยง : OR2

ปัจจัยความเสี่ยง (Risk Factor) : พนักงานกลุ่ม Team Lead มีความเครียดสูง อาจทำให้มีความสุขในการทำงานน้อยลง ซึ่งอาจส่งผลต่อการบริหารงานและทีมงาน

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน) (Impact)
คะแนน	คำนิยาม (พิจารณาจากระดับความสุขของ Team Lead โดยเฉลี่ย)	คำนิยาม (พิจารณาจากการบริหารงานและทีมงาน)
5 สูงที่สุด	ไม่มีความสุขมาก (Unhappy) มีคะแนน 0-24.99	ผลการประเมินการบริหารงานและทีมงานจาก Team Lead ทั้งหมดมีค่าเฉลี่ย น้อยกว่า ร้อยละ 50
4 สูง	ไม่มีความสุข (Unhappy) มีคะแนน 25-49.99	ผลการประเมินการบริหารงานและทีมงานจาก Team Lead ทั้งหมดมีค่าเฉลี่ย ร้อยละ 50-59.99
3 ปานกลาง	-	ผลการประเมินการบริหารงานและทีมงานจาก Team Lead ทั้งหมดมีค่าเฉลี่ย ร้อยละ 60-69.99
2 ต่ำ	มีความสุข (Happy) มีคะแนน 50-74.99	ผลการประเมินการบริหารงานและทีมงานจาก Team Lead ทั้งหมดมีค่าเฉลี่ย ร้อยละ 70-79.99
1 ต่ำที่สุด	มีความสุขมาก (very Happy) มีคะแนน 75-100	ผลการประเมินการบริหารงานและทีมงานจาก Team Lead ทั้งหมดมีค่าเฉลี่ย ร้อยละ 80 ขึ้นไป

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
- มีขั้นตอนการปฏิบัติงานในการรักษาความมั่นคงปลอดภัย - มีระบบตรวจสอบการโจมตีจากภายนอก	**Reduce** - มีการประเมินวัดความสุขของพนักงานทั้งองค์กรและจัดกลุ่มโดยใช้เครื่องมือที่ Certify โดยประทรวงสาธารณสุขหรือเทียบเท่า (Q1-2) - ออกแบบกิจกรรมที่ส่งเสริมความสุข/ เพิ่ม Interpersonal Skills / สร้าง Safe-zone Ecosystem และ Social support system (Q1-2) - มีที่ปรึกษา 1-on-1 Sessions พูดคุยเพื่อรับฟังปัญหา รวมทั้ง online consultancy (Q1-4) - Training ด้าน Management Skills และ Communication Skill (Q1-4) หมายเหตุ : การเพิ่มความสุขของ Team Lead ด้วยการส่งเสริมสุขภาพจิตที่ดีขึ้นและการพัฒนาทักษะการบริหารงานและบริหารทีม เช่น การมีที่ปรึกษาช่วยรับฟังปัญหาและให้ข้อเสนอแนะในการปรับปรุง/ แก้ไขสถานการณ์ และการพัฒนาทักษะในการบริหารงานและบริหารทีม อาจส่งผลให้ Team Lead สามารถจัดการปัญหาได้ดียิ่งขึ้น และอาจส่งผลให้มีความสุขในการทำงานมากยิ่งขึ้น	**- โอกาสที่จะเกิด = ระดับ 3** เนื่องจากยังไม่เคยทำการประเมินวัดความสุขของพนักงานทั้งองค์กร **- ผลกระทบ = ระดับ 3** กำหนดให้ใช้ค่าระดับ 3 เป็นค่ากลางเนื่องจากยังไม่มีผลการประเมินดังกล่าวในปีที่ผ่านมา  	ฝ่ายอำนวยการและทรัพยากรบุคคล

หัวข้อความเสี่ยง : OR3

ปัจจัยความเสี่ยง (Risk Factor) : ระบบสารสนเทศภายในสำนักงาน เกิดข้อผิดพลาดไม่สามารถให้บริการกับพนักงานได้ เช่น ระบบสารบรรณ / ระบบ ERP / ระบบจองทรัพยากรใน Intranet / WIFI / Internet

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน) (Impact)
คะแนน	คำนิยาม (พิจารณาจากจำนวนครั้งการเกิดเหตุการณ์ในรายไตรมาส)	คำนิยาม (พิจารณาจากผลกระทบต่อบุคลากรใน สพธอ.)
5 สูงที่สุด	มากกว่า 3 ครั้ง/ไตรมาส	บริการหยุดชะงักเป็นเวลามากกว่า 12 ชั่วโมง หรือข้อมูลลับรั่วไหลและถูกเปิดเผยต่ออสาธารณะ องค์กรเสื่อมเสียชื่อเสียง มีการถูกฟ้องดำ เนินคดีและถูกพิจารณาโทษ
4 สูง	3 ครั้ง/ไตรมาส	บริการหยุดชะงักเป็นเวลา 1-12 ชั่วโมง หรือข้อมูลลับรั่วไหลและถูกเปิดเผยต่อบุคคลที่ไม่เกี่ยวข้อง
3 ปานกลาง	2 ครั้ง/ไตรมาส	บริการหยุดชะงักเป็นเวลา 30-60 นาทีหรือมีการร้องเรียนจากผู้รับบริการและพบว่ามีข้อผิดพลาดจริง
2 ต่ำ	1 ครั้ง/ไตรมาส	บริการหยุดชะงักเป็นเวลา 15-30 นาที หรือมีการร้องเรียนจากผู้รับบริการ
1 ต่ำที่สุด	ไม่เกิดขึ้นเลย	บริการหยุดชะงักไม่เกินเวลา 15 นาทีหรือสามารถแก้ไขได้ด้วยการปฏิบัติงานตามขั้นตอนปกติ

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
- มีแผนในการ Maintenance ระบบ/การจ้างภายนอกเพื่อดูและรักษาระบบ (บางรายการ) และการรับประกัน - มีการกำหนดผู้รับผิดชอบในการดูแลแต่ละระบบ	**Reduce** - การช่องทางในการสื่อสารที่รวดเร็วกับผู้ปฏิบัติงานที่ได้รับผลกระทบ - มีการอัพเดทแนวปฏิบัติเพื่อให้สามารถรับมือต่อเหตุการณ์ต่าง ๆ หรือระบบใหม่ ๆ ได้	**- โอกาสที่จะเกิด = ระดับ 2** ปี 2567 โดยเฉลี่ยเกิดเหตุการณ์จนระบบบริการภายในหยุดชะงักจำนวน 1 ครั้ง/ไตรมาส **- ผลกระทบ = ระดับ 3** ปี 2567 โดยเฉลี่ยการบริการหยุดชะงักเป็นเวลา 30-60 นาที โดยมีพบการร้องเรียนจากผู้รับบริการ 	ศูนย์ระบบโครงสร้างพื้นฐานด้านสารสนเทศและความมั่นคงปลอดภัย

หัวข้อความเสี่ยง : OR4

ปัจจัยความเสี่ยง (Risk Factor) : มีข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว รั่วไหลออกจากระบบที่สำคัญเช่น ระบบจดแจ้ง DPS / ระบบออกใบอนุญาต DID ฐานข้อมูลการฝึกอบรม ฐานข้อมูลพนักงานภายใน

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดผลกระทบที่จะได้รับ) (Impact)
คะแนน	คำนิยาม (พิจารณาจากจำนวนครั้งการเกิดเหตุการณ์รั่วไหลของข้อมูลในรายไตรมาส)	คำนิยาม (พิจารณาจากผลกระทบต่อ สพธอ. กรณีที่เกิดการรั่วไหลของข้อมูล)
5 สูงที่สุด	มากกว่า 3 ครั้ง/ไตรมาส	มีผลพิจารณาโทษทันทีตามกฎหมาย
4 สูง	3 ครั้ง/ไตรมาส	ถูกฟ้องร้องดำเนินคดี
3 ปานกลาง	2 ครั้ง/ไตรมาส	ถูกร้องเรียนจากผู้รับบริการและพบว่ามีข้อผิด พลาดจริง
2 ต่ำ	1 ครั้ง/ไตรมาส	ถูกร้องเรียนจากผู้รับบริการ (ภายใน/ภายนอก)
1 ต่ำที่สุด	ไม่เกิดขึ้นเลย	ไม่มีการร้องเรียนจากผู้รับบริการ

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
- สพธอ. มีนโยบาย วิธีปฏิบัติงานที่เกี่ยวข้องด้าน Data Governance และ PDPA - มีเกณฑ์การประเมินความเสี่ยงใน incident ด้านข้อมูล และแผนการจัดการสำหรับเหตุการณ์ที่ความเสี่ยงสูง	**Reduce** - มีการตรวจสอบการปฏิบัติตามแนวทางที่กำหนด เช่น Data sharing ผู้เข้าถึงข้อมูล - มีเครื่องมือเฝ้าระวังการถูกโจมตีจากภายนอก จัดกิจกรรมสื่อสาร/สร้างความตระหนักแก่พนักงาน	**- โอกาสที่จะเกิด = ระดับ 1** ที่ผ่านมา สพธอ. ไม่เคยเกิดเหตุการณ์รั่วไหลของข้อมูล **- ผลกระทบ = ระดับ 5** หากเกิดเหตุการณ์ อาจเกิดผลกระทบระดับสูงสุด เนื่องจากอาจผิดกฎหมายที่มีการบังคับใช้ 	ทีมธรรมาภิบาลข้อมูล (Data Governance)

หัวข้อความเสี่ยง : FR1

ปัจจัยความเสี่ยง (Risk Factor) : การใช้จ่ายและการเบิกจ่ายงบประมาณไม่เป็นไปตามแผนอาจมีผลต่อการได้รับงบประมาณลดลง

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood) แบ่งตามช่วงเวลา			เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน) (Impact)
คะแนน	คำนิยาม (Q1-พิจารณาจากการติดตามการทำ TOR)	คำนิยาม (Q2-พิจารณาจากการติดตามการลงนามสัญญา (เบิกจ่าย + ผูกพัน))	คำนิยาม (Q3 และ Q4-พิจารณาจากการใช้จ่ายงบประมาณ (เบิกจ่าย + ผูกพัน))	คำนิยาม (ผลการเบิกจ่ายเทียบแผนเบิกจ่ายราย ไตรมาส (Q1-Q4))
5 สูงที่สุด	จัดทำ TOR แล้วเสร็จ น้อยกว่า ร้อยละ 80 ภายในไตรมาส 1	ผลใช้จ่ายเทียบแผนได้ น้อยกว่าร้อยละ 70	ดำเนินการได้ น้อยกว่าร้อยละ 85	ดำเนินการได้ ดีกว่าร้อยละ 95
4 สูง	จัดทำ TOR แล้วเสร็จทั้งหมดร้อยละ 80-89 ภายในไตรมาส 1	ผลใช้จ่าย เทียบแผนได้ ร้อยละ 70-79	ดำเนินการได้ ร้อยละ 85-90	ดำเนินการได้ ร้อยละ 90-94.9
3 ปานกลาง	จัดทำ TOR แล้วเสร็จทั้งหมดร้อยละ 90-99 ภายในไตรมาส 1	ผลใช้จ่ายเทียบแผนได้ ร้อยละ 80-89	ดำเนินการได้ มากกว่าร้อยละ 90	ดำเนินการได้ ร้อยละ 85- 89.9
2 ต่ำ	จัดทำ TOR แล้วเสร็จทั้งหมดร้อยละ 100 ภายในไตรมาส 1	ผลใช้จ่ายเทียบแผนได้ ร้อยละ 90-99	ดำเนินการได้ > ร้อยละ 90 ภายในเดือน ส.ค. 68	ดำเนินการได้ ร้อยละ 80-84.9
1 ต่ำที่สุด	จัดทำ TOR แล้วเสร็จทั้งหมดก่อนขึ้นปีงบประมาณ	ผลใช้จ่าย เทียบแผนได้มากกว่า ร้อยละ 99	ดำเนินการได้ > ร้อยละ 90 ภายในเดือน ก.ค. 68	ดำเนินการได้ น้อยกว่าร้อยละ 80

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
- แผนปฏิบัติการประจำปี 2568 รวมถึงแผนการใช้จ่ายและแผนการเบิกจ่าย - การดำเนินการตามระเบียบ ข้อบังคับของการซื้อจ้าง การใช้งบประมาณ และมาตรการต่าง ๆ ที่ภาครัฐกำหนด	**Reduce** - เร่งรัดการจัดทำ TOR และนำเข้าสู่กระบวนการซื้อจ้าง ภายในเดือน ต.ค. 2567 - การติดตามการดำเนินงานตามแผนเพื่อให้เกิดการเบิกจ่ายเป็นไปตามแผนที่กำหนด - การกำหนดช่วงเวลาของการทบทวนแผนในกรณีที่มีเงินเหลือจ่าย เพื่อให้เกิดการเร่งปรับแผน และมีการสื่อสารไปยังผู้บริหารและหัวหน้าโครงการ - การติดตามผลการดำเนินงานรายไตรมาส วิเคราะห์ปัญหาและมีการนำเสนอประเด็น critical ต่อผู้บริหารเพื่อเร่งดำเนินการในส่วนที่เกี่ยวข้อง	**- โอกาสที่จะเกิด = ระดับ 5** เนื่องจากเป็นการได้รับงบประมาณใหม่และการจัดทำ TOR ยังอยู่ระหว่างดำเนินการ **- ผลกระทบ = ระดับ 5** เนื่องจากเป็นการได้รับงบประมาณใหม่จึงยังไม่เกิดผลการเบิกจ่าย ณ วันที่ 30 กันยายน 2567 	ฝ่ายนโยบายและแผนและฝ่ายอำนวยการ รวมทั้งทุกกลุ่มงานตามสายงานและผู้ดูแลโครงการ

หัวข้อความเสี่ยง : FR2

ปัจจัยความเสี่ยง (Risk Factor) : ในอนาคตเงินทุนสะสมอาจไม่เพียงพอต่อการลดผลกระทบด้านงบประมาณรายจ่ายในกรณีที่ได้รับมาจำกัด

เกณฑ์/คะแนน	เกณฑ์โอกาสจะเกิด (Likelihood)	เกณฑ์ผลกระทบ (วัดประสิทธิภาพการดำเนินงาน) (Impact)
คะแนน	คำนิยาม (พิจารณาจากการบริหารจัดการประจำปี)	คำนิยาม (พิจารณาจากปริมาณเงินทุนคงเหลือ (เทียบอัตราอัตราเฉลี่ยย้อนหลัง 3 ปี))
5 สูงที่สุด	มีการขอใช้เงินทุนสะสมระหว่างปีงบฯ มากกว่า 2 ครั้ง	น้อยกว่า 1 เท่า (คงเหลือน้อยกว่า 48.25 ล้านบาท)
4 สูง	มีการขอใช้เงินทุนสะสมระหว่างปีงบฯ 2 ครั้ง	1-1.5 เท่า (คงเหลือ 48.25 – 72.37 ล้านบาท)
3 ปานกลาง	มีการขอใช้เงินทุนสะสมระหว่างปีงบฯ 1 ครั้ง	1.5-2 เท่า (คงเหลือ 72.38- 96.49 ล้านบาท)
2 ต่ำ	บริหารงานตามแผนการใช้เงินทุนสะสมตามแผน	2-2.5 เท่า (คงเหลือ 96.50- 120.62 ล้านบาท)
1 ต่ำที่สุด	บริหารงานตามแผนการใช้เงินทุนสะสมและมีเงินรายได้	มากกว่า 2.5 เท่า (คงเหลือมากกว่า 120.62 ล้านบาท)

การควบคุมที่มีอยู่ในปัจจุบัน	แผนการจัดการความเสี่ยง	ระดับความเสี่ยง (Inherent Risk)	ผู้รับผิดชอบ
- แผนปฏิบัติการประจำปี 2568 รวมถึงแผนการใช้จ่ายและแผนการเบิกจ่าย - การบริหารงบประมาณแผ่นดิน เพื่อลดการขอใช้ทุนสะสมระหว่างปี	**Reduce** - การบริหารการใช้เงินทุนที่สมทบในแผนปฏิบัติการ - การดำเนินการตามแผนรายได้ขององค์กร	**- โอกาสที่จะเกิด = ระดับ 3** ในช่วงปี 2564-2567 มีการขอใช้เงินทุนสะสมระหว่างปี โดยเฉลี่ยที่ 1 ครั้ง/ปี **- ผลกระทบ = ระดับ 1** ช่วงเดือนกันยายน 2567 สพธอ. มีการขอเงินทุนสะสมเพื่อนำมาใช้สนับสนุนแผนปฏิบัติการประจำปี 2568 ทำให้ทุนสะสมคงเหลือที่ 123 ล้านบาท  	ฝ่ายงบประมาณ

5. การปรับปรุงการดำเนินงานบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง

เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงเป็นระบบและมีความต่อเนื่อง สพธอ. ได้มีการกำหนดผู้รับผิดชอบในแต่ละประเด็นความเสี่ยง รวมถึงเป็นความรับผิดชอบของผู้บริหารในทุกระดับที่จะนำกระบวนการบริหารความเสี่ยงมาปฏิบัติได้อย่างทั่วถึงในองค์กรอย่างสม่ำเสมอ โดยมีการติดตามเพื่อให้เป็นไปตามแผน (Mitigation Plan) อย่างต่อเนื่อง มีการประเมินโอกาสและผลกระทบของเหตุการณ์ที่อาจจะเกิดขึ้นต่อวัตถุประสงค์ มีการติดตามผลและความคืบหน้าการดำเนินงานเป็นรายไตรมาส ตลอดจนทบทวนด้านเทคโนโลยีใหม่ๆ มีการนำข้อบกพร่องในอดีตมาพิจารณาประกอบ เพื่อให้ทราบผลการดำเนินการว่ามีความเหมาะสม และสามารถนำมาใช้ปรับปรุงในการบริหารองค์กรและจัดการความเสี่ยงต่างๆ ทำให้องค์กรสามารถบรรลุเป้าหมาย วัตถุประสงค์ขององค์กรตามยุทธศาสตร์หรือกลยุทธ์เป็นสำคัญให้ได้มากที่สุด

กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ศูนย์ราชการเฉลิมพระเกียรติฯ (อาคารซี)
ชั้นที่ 4 เลขที่ 120 หมู่ที่ 3 ซอยแจ้งวัฒนะ 7 ถนนแจ้งวัฒนะ
แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210