แผนบริหารความเสี่ยงองค์กร
ปีงบประมาณ พ.ศ. 2569

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

ธันวาคม 2568

สารบัญ

หน้า

บทสรุปผู้บริหาร **1**

บทที่ 1 บทนำ **2**

1.1 ข้อมูลทั่วไปขององค์กร 2

1.2 วัตถุประสงค์ของการบริหารความเสี่ยง 4

1.3 เป้าหมายของการบริหารความเสี่ยง 5

1.4 โครงสร้างและบทบาทผู้กำกับดูแลความเสี่ยง 5

บทที่ 2 กรอบแนวคิดและหลักการบริหารความเสี่ยง **8**

2.1 กรอบแนวคิดการบริหารความเสี่ยงองค์กร 8

2.2 หลักการบริหารความเสี่ยงของสถาบัน 9

2.3 ความสัมพันธ์ระหว่างการบริหารความเสี่ยงกับระบบการควบคุมภายใน 9

2.4 ประเภทของความเสี่ยงองค์กร 11

2.5 กระบวนการบริหารความเสี่ยงของสถาบัน (Risk Management Process) 11

บทที่ 3 การประเมินสภาพแวดล้อมและการวิเคราะห์ปัจจัยเสี่ยง **13**

3.1 การประเมินสภาพแวดล้อมภายนอก 13

3.2 การประเมินสภาพแวดล้อมภายใน 16

3.3 การวิเคราะห์สภาพแวดล้อมองค์รวม 17

3.4 ประเด็นความเสี่ยงที่สำคัญขององค์กร (Key Enterprise Risks) 19

บทที่ 4 แผนบริหารจัดการความเสี่ยงองค์กร ประจำปีงบประมาณ พ.ศ. 2569 ..... **22**

4.1 วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง 22

4.2 ระดับความเสี่ยงและเกณฑ์การประเมิน 22

4.3 แผนบริหารความเสี่ยงองค์กรปีงบประมาณ พ.ศ. 2569 24

เอกสารอ้างอิง **36**

สารบัญตาราง

หน้า

ตารางที่ 1 ความสัมพันธ์ระหว่างระบบการบริหารความเสี่ยง และระบบการควบคุมภายใน 10
ตารางที่ 2 กระบวนการบริหารความเสี่ยงของสถาบัน 11
ตารางที่ 3 การประเมินสภาพแวดล้อมภายนอก (PESTEL Analysis) 13
ตารางที่ 4 แสดงผลการประเมินสภาพแวดล้อมภายในของ สขญ. ตามกรอบ 7S McKinsey 16
ตารางที่ 5 ผลการวิเคราะห์ SWOT ของ สขญ. 18
ตารางที่ 6 การทบทวนการบริหารความเสี่ยงปีงบประมาณ พ.ศ. 2568 20
ตารางที่ 7 ประเด็นความเสี่ยงที่สำคัญขององค์กร (Key Enterprise Risks) ปีงบประมาณ พ.ศ. 2569 21
ตารางที่ 8 แผนภูมิความเสี่ยง (Risk map) 23
ตารางที่ 9 การจัดแบ่งระดับความเสี่ยง (Risk Level) และความหมายของแต่ละระดับความเสี่ยง 23
ตารางที่ 10 ประเด็นความเสี่ยงองค์กร ปีงบประมาณ พ.ศ. 2569 และผู้รับผิดชอบ 24

สารบัญรูปภาพ

หน้า

รูปที่ 1 องคประกอบและหลักการของการบริหารความเสี่ยงขององคกร COSO ERM (2017)..... 8
รูปที่ 2 แนวคิด “การบริหารความเสี่ยงแบบบูรณาการ (Integrated Risk Management, IRM)” ของ สขญ. 10

บทสรุปผู้บริหาร

ในปีงบประมาณ พ.ศ. 2569 สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (สขญ.) ยังคงเผชิญสภาพแวดล้อมที่มีความไม่แน่นอนทางการเมือง มีการเลือกตั้งใหม่ ส่งผลให้เกิดการเปลี่ยนแปลงทางนโยบายของภาครัฐ อีกทั้งกฎหมาย/กฎระเบียบที่มอบหมายให้ สขญ. ให้มีภารกิจด้านการเชื่อมโยงข้อมูล อยู่ระหว่างกระบวนการตรากฎหมาย รวมถึง สขญ. ได้มอบหมายภารกิจเร่งด่วนเพิ่มเติมจากรัฐบาล ตลอดจนความท้าทายด้านความมั่นคงปลอดภัยไซเบอร์ ในขณะเดียวกัน สขญ. ยังมีภารกิจที่ต้องขับเคลื่อนให้เกิดการใช้ประโยชน์ด้านข้อมูลเชิงวิเคราะห์ในระดับชาติ โดยกลไกการเชื่อมโยงข้อมูลมายังแพลตฟอร์มข้อมูลขนาดใหญ่แห่งชาติ (D2) จำเป็นต้องอาศัยความร่วมมือจากหลายหน่วยงาน การตีความกฎหมายที่มีหน่วยงานกำกับดูแลด้านข้อมูลหลายหน่วยงาน ซึ่งอาจมีโอกาสในการตีความไม่ตรงกัน

จากการประเมินสถานการณ์ดำเนินงานและผลการบริหารความเสี่ยงองค์กรของ สขญ. ในปีงบประมาณ พ.ศ. 2568 ที่ผ่านมา ชี้ให้เห็นว่า สขญ. มีความก้าวหน้าในการปรับปรุงระบบควบคุมและลดระดับความเสี่ยงหลายประเด็น แต่ยังมีบางด้านที่ต้องติดตามต่อเนื่อง โดยเฉพาะประเด็นกฎหมายด้านข้อมูลและความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีแนวโน้มความสำคัญมากขึ้นในปีงบประมาณ พ.ศ. 2569

จากการวิเคราะห์ปัจจัยทั้งภายนอกและภายใน พร้อมเชื่อมโยงกับผลการดำเนินงานปีที่ผ่านมา สขญ. ได้พิจารณาและกำหนดความเสี่ยงองค์กรที่สำคัญ ปีงบประมาณ พ.ศ. 2569 ใน 5 ประเด็นความเสี่ยง ดังนี้

(1) **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)**: มีความล่าช้าในการเชื่อมโยงขอรับข้อมูลเข้าแพลตฟอร์มข้อมูลขนาดใหญ่แห่งชาติ (D2) เนื่องจาก ยังไม่มีกฎหมาย/กฎระเบียบ ที่มอบหมายภารกิจโดยตรง จึงส่งผลให้ต้องมีกระบวนการด้านเอกสารหลายขั้นตอน

(2) **ความเสี่ยงด้านการปฏิบัติงาน (Operation Risk):** ได้รับมอบหมายงานใหม่เพิ่มเติมอย่างกะทันหันจนส่งผลกระทบต่อการดำเนินงานหลักของสถาบันฯ

(3) **ความเสี่ยงทางด้านการเงิน (Financial Risk):** ไม่มีงบประมาณสำหรับงานใหม่ที่ต้องการการขับเคลื่อน ในช่วงงบประมาณพลางก่อน จนส่งผลกระทบต่อเป้าหมายของสถาบันฯ

(4) **ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk) :** ความเสี่ยงจากความเข้าใจคลาดเคลื่อนในการตีความและการปฏิบัติตามกฎหมายด้านข้อมูล

(5) **ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risk):** ระบบสารสนเทศของสถาบันฯ ถูกโจมตีทางไซเบอร์ จนส่งผลให้ข้อมูลรั่วไหล สูญหาย หรือระบบให้บริการหยุดชะงัก (Ransomware / Data Breach)

ประเด็นความเสี่ยงทั้ง 5 ด้านนี้เป็นปัจจัยสำคัญที่อาจกระทบต่อการดำเนินการที่สำคัญของ สขญ. ในการบรรลุเป้าหมายยุทธศาสตร์ จึงถูกนำไปสู่การจัดทำมาตรการบริหารความเสี่ยงระดับองค์กร เพื่อเสริมความพร้อมและขับเคลื่อนภารกิจของปีงบประมาณ พ.ศ. 2569 ให้เกิดผลอย่างมีประสิทธิภาพ โปร่งใส และสอดคล้องกับมาตรฐานการบริหารความเสี่ยงภาครัฐ

บทที่ 1
บทนำ

ในยุคที่การบริหารจัดการภาครัฐต้องเผชิญกับการเปลี่ยนแปลงทางเทคโนโลยี เศรษฐกิจ และนโยบายที่รวดเร็ว การจัดตั้งระบบบริหารความเสี่ยงองค์กรที่มีประสิทธิภาพจึงมีความจำเป็นอย่างยิ่ง เพื่อให้การดำเนินงานของสถาบันฯ เป็นไปอย่างมีธรรมาภิบาล โปร่งใส และสามารถบรรลุวัตถุประสงค์ตามพันธกิจได้อย่างยั่งยืน สถาบันฯ จึงได้จัดทำ “แผนบริหารจัดการความเสี่ยงองค์กร ประจำปีงบประมาณ พ.ศ. 2569” ขึ้น เพื่อเป็นกรอบแนวทางในการระบุ ประเมิน และจัดการความเสี่ยงที่อาจเกิดขึ้นในทุกระดับขององค์กรให้สอดคล้องกับ มาตรา 79 แห่งพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 รวมถึงมาตรฐานและหลักเกณฑ์การบริหารความเสี่ยงของกระทรวงการคลัง (หนังสือ กค 0409.3/ว36 ลงวันที่ 3 กุมภาพันธ์ 2564) และกรอบมาตรฐานสากล COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017)

แผนบริหารความเสี่ยงองค์กรฉบับนี้ จึงมุ่งเน้นการบูรณาการการบริหารความเสี่ยงให้เป็นส่วนหนึ่งของการดำเนินงานเชิงยุทธศาสตร์ขององค์กร โดยใช้ข้อมูลจากการวิเคราะห์สภาพแวดล้อมภายนอก (PESTEL) และภายใน (7S McKinsey) เพื่อสังเคราะห์เป็นปัจจัยเสี่ยงระดับองค์กร (Enterprise Risks) ที่ครอบคลุมทั้ง 5 ด้าน ได้แก่ ด้านกลยุทธ์ ด้านการปฏิบัติงาน ด้านการเงิน ด้านการปฏิบัติตามกฎระเบียบ และด้านเทคโนโลยีสารสนเทศ พร้อมทั้งกำหนดแผนบริหารจัดการความเสี่ยง (Action Plan) และตัวชี้วัดความเสี่ยงหลัก (KRI) เพื่อใช้ในการติดตาม ประเมินผล และรายงานต่อคณะกรรมการที่เกี่ยวข้องอย่างต่อเนื่อง

1.1 ข้อมูลทั่วไปขององค์กร

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (สขญ.) หรือ Big Data Institute (Public Organization) (BDI) เป็นหน่วยงานของรัฐในกำกับของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จัดตั้งขึ้นในวันที่ 1 มิถุนายน พ.ศ. 2566 ตามพระราชกฤษฎีกาจัดตั้งสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) พ.ศ. 2566 ประกาศในราชกิจจานุเบกษา เพื่อเป็นองค์กรหลักในการส่งเสริมและขับเคลื่อนการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) และเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เพื่อยกระดับประสิทธิภาพภาครัฐ สร้างนวัตกรรมบริการสาธารณะ และพัฒนาเศรษฐกิจ–สังคมของประเทศ

- **วิสัยทัศน์**

  Enabling Data – Driven Nation สถาบันแห่งการส่งเสริมนวัตกรรมด้วยการใช้ข้อมูลขนาดใหญ่ เพื่อการขับเคลื่อนประเทศ สร้างคุณค่าทางสังคม และพัฒนาคุณภาพชีวิตประชาชน

- **พันธกิจ**

  1) วางยุทธศาสตร์การขับเคลื่อนการใช้ประโยชน์จากข้อมูลขนาดใหญ่ เพื่อผลักดันให้เกิดการพัฒนาเศรษฐกิจและสังคม
  2) ส่งเสริม ประสาน และให้บริการแก่ทุกภาคส่วน เพื่อให้เกิดการใช้ประโยชน์ จากข้อมูลขนาดใหญ่ในการเพิ่มประสิทธิภาพการดำเนินงาน และการให้บริการ
  3) ให้บริการวิเคราะห์ข้อมูลขนาดใหญ่ และให้คำปรึกษาด้านข้อมูลขนาดใหญ่ และเทคโนโลยีที่เกี่ยวข้อง

4) ส่งเสริมการสร้างนวัตกรรมด้านข้อมูลขนาดใหญ่ และเทคโนโลยี ที่เกี่ยวข้องให้มีมาตรฐานในระดับสากล
5) ส่งเสริม สนับสนุน และพัฒนาธุรกิจด้านการวิเคราะห์ และใช้ประโยชน์ จากข้อมูลขนาดใหญ่
6) ส่งเสริม สนับสนุน และพัฒนาองค์ความรู้และบุคลากรของประเทศ ด้านการวิเคราะห์ข้อมูลขนาดใหญ่

- **ค่านิยมหลักองค์กร (AGILE)**

A: Agility **ความคล่องตัว**	1. มีความคล่องตัวในการปฏิบัติงาน มุ่งเน้นผลลัพธ์ในการทำงาน 2. รู้จักตนเอง และเชื่อมโยงการทำงานร่วมกับหน่วยงานทั้งภายในและภายนอกองค์กรได้ 3. ปฏิบัติงานโดยใส่ใจถึงคุณภาพ (Quality) ต้นทุน (Cost) และการส่งมอบงาน (Delivery) เพื่อให้ได้ผลงานที่มีคุณภาพ 4. เมื่อเกิดปัญหาในการทำงาน สามารถวิเคราะห์ ปรับปรุง ดำเนินการแก้ไขและพัฒนาการทำงานอย่างต่อเนื่อง เพื่อป้องกันไม่ให้เกิดความผิดพลาดซ้ำๆ ในการทำงาน 5. สร้างให้เกิดการทำงานแบบ Cross-functional เป็นการนำคนที่มีความเชี่ยวชาญจากหลายสายงาน มาทำงานร่วมกัน ซึ่งจะส่งผลให้ทีมสามารถทำความเข้าใจกับรายละเอียดของงานและมีความคล่องตัวมากขึ้น
G: Goal Orientation **มุ่งเน้นเป้าหมาย**	1. คำนึงถึงประโยชน์ และสร้างผลสำเร็จของงานที่สอดคล้องกับนโยบายและเป้าหมายขององค์กร และประเทศชาติเป็นหลัก 2. เน้นคุณภาพทั้งในกระบวนการทำงานของตนเองและหน่วยงาน คุณภาพของชิ้นงาน สภาพแวดล้อมในการทำงาน และบริการ และคุณภาพที่องค์กรมอบหมายให้รับผิดชอบ โดยคำนึงถึงความถูกต้องแม่นยำ ระยะเวลาในการดำเนินการ การปรับปรุงข้อบกพร่องและวงจร PDCA 3. มีความมุ่งมั่นที่จะส่งมอบงานที่มีคุณภาพ ตรงตามวัตถุประสงค์ขององค์กรเพื่อความพึงพอใจของลูกค้าภายในและลูกค้าภายนอก 4. สนับสนุนการทำงานของสมาชิกอย่างสร้างสรรค์เพื่อสร้างความร่วมมือร่วมใจ มุ่งสู่เป้าหมายเดียวกัน
I: Integrity **ยึดมั่นในความถูกต้อง**	1. ตระหนักถึงจริยธรรม ซื่อสัตย์ สุจริต มีคุณธรรม โปร่งใส มีวินัยต่อกฎระเบียบ กติกา และกล้ายืนหยัดและทำในสิ่งที่ถูกต้อง 2. มีความเชื่อมั่นในสิ่งที่ถูกต้อง ประพฤติและปฏิบัติตามจริยธรรมและคุณธรรมแห่งวิชาชีพของตน 3. รักษาความลับและผลประโยชน์ของสำนักงาน ไม่ดำเนินการใดๆ ที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์ขององค์กร และประเทศชาติ 4. มีจิตสำนึกและความรับผิดชอบต่อสังคม มีความเคารพและเชื่อใจเพื่อนร่วมงาน ปรับแนวทางการทำงานให้เกิดพลังการทำงานร่วมกัน 5. มีความเสียสละและเน้นประโยชน์ขององค์กร

L: Lifelong Learning **นักเรียนรู้ตลอดชีวิต**	1. มีความคิดริเริ่ม สร้างสรรค์ ใฝ่เรียนรู้ พัฒนาตนเองเกี่ยวกับงานในหน้าที่ของตนเอง เพื่อพัฒนาขีดความสามารถของตนเองอยู่เสมอ 2. สะสมองค์ความรู้และนำมาใช้อย่างเป็นระบบโดยคำนึงถึงความรู้หลักตามหน้าที่ของตนและองค์กร 3. ตระหนักการเรียนรู้อยู่เสมอ เรียนรู้ข้อผิดพลาดและข้อดีได้อย่างรวดเร็ว เนื่องจากการทำงานเป็นรอบเล็กๆ ทำให้เกิดการเรียนรู้ข้อผิดพลาดที่พบจากครั้งก่อนๆ และสามารถหาข้อบกพร่องตลอดจนข้อดีในการทำงานได้อย่างรวดเร็ว
E: Excellence **ยึดมั่นความเป็นเลิศในงานที่ทำ**	1. สร้างความเป็นเลิศในงานที่รับผิดชอบ เพื่อผลักดันให้เกิดการพัฒนาศักยภาพตนเองและยกระดับองค์กร 2. สามารถวิเคราะห์การทำงาน และนำมาปรับปรุงพัฒนาการทำงานให้เกิดประสิทธิภาพสูงสุด 3. ยึดมั่นในการสร้างความเป็นเลิศในทุกสิ่งที่ทำ อันเกิดจากการใฝ่รู้ ริเริ่มและสร้างสรรค์

1.2 วัตถุประสงค์ของการบริหารความเสี่ยง

การบริหารความเสี่ยงของ สขญ. มีวัตถุประสงค์หลักเพื่อจัดให้มีระบบการบริหารจัดการความเสี่ยงที่มีประสิทธิภาพ โปร่งใส และสามารถรองรับการเปลี่ยนแปลงของสภาพแวดล้อมทางนโยบาย เศรษฐกิจ เทคโนโลยี และสังคม โดยมุ่งให้การดำเนินงานของสถาบัน บรรลุวัตถุประสงค์และเป้าหมายเชิงยุทธศาสตร์ขององค์กรได้อย่างมีประสิทธิผลและยั่งยืน ภายใต้กรอบธรรมาภิบาลและความรับผิดชอบต่อสังคม

วัตถุประสงค์เฉพาะของการบริหารความเสี่ยง ได้แก่

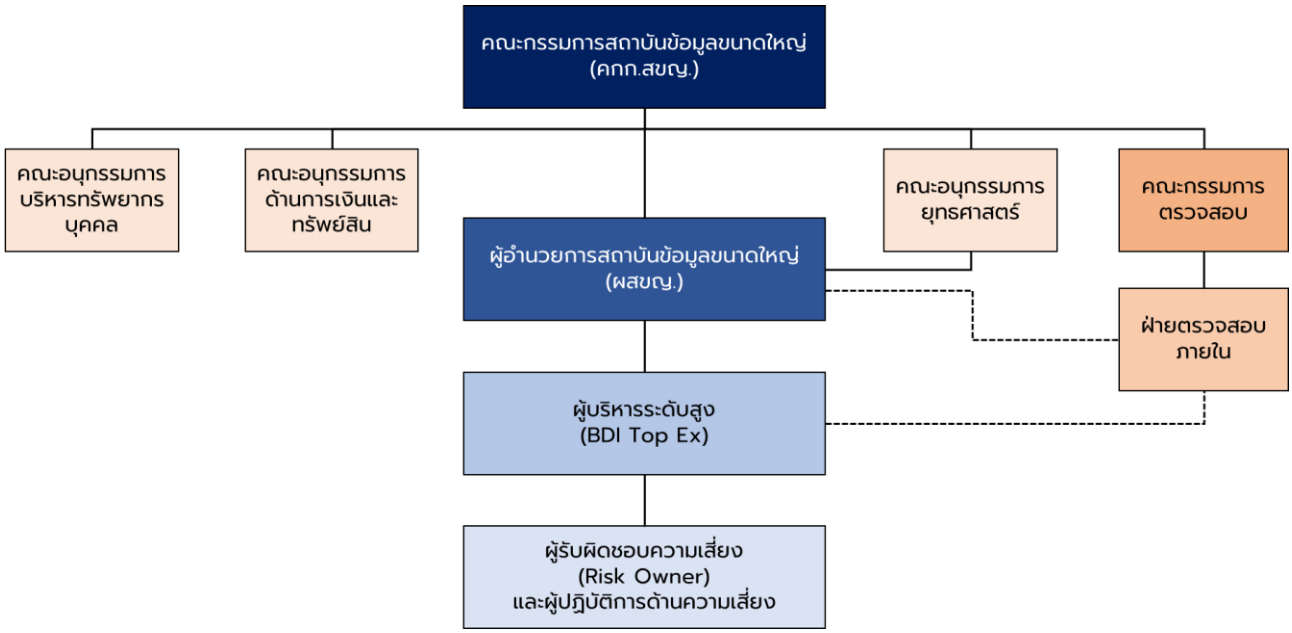
1) เพื่อให้สถาบันฯ มีระบบบริหารจัดการความเสี่ยงที่ครอบคลุมทุกระดับ ทั้งระดับองค์กร ระดับฝ่าย และระดับโครงการ
2) เพื่อระบุ ประเมิน และจัดการความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ของสถาบัน
3) เพื่อให้ผู้บริหารและบุคลากรทุกระดับตระหนักถึงความสำคัญของการบริหารความเสี่ยง และมีส่วนร่วมในการกำหนดแนวทางจัดการความเสี่ยงในส่วนที่ตนรับผิดชอบ
4) เพื่อให้การตัดสินใจเชิงนโยบายและการบริหารของสถาบันฯ มีข้อมูลความเสี่ยงประกอบอย่างเป็นระบบ (Risk–Informed Decision Making)
5) เพื่อเสริมสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้ส่วนเสีย ว่าการดำเนินงานของสถาบันฯ มีระบบบริหารจัดการความเสี่ยงที่เพียงพอ โปร่งใส และตรวจสอบได้
6) เพื่อสนับสนุนการบูรณาการระบบบริหารความเสี่ยงกับระบบการควบคุมภายในและการตรวจสอบภายในของสถาบัน ให้สอดคล้องและเกื้อหนุนกันตามหลัก COSO 2013/2017

1.3 เป้าหมายของการบริหารความเสี่ยง

สขญ. กำหนดเป้าหมายของการบริหารความเสี่ยงองค์กร (Enterprise Risk Management Goals) ให้สอดคล้องกับวิสัยทัศน์ พันธกิจ และยุทธศาสตร์หลักของสถาบัน โดยมีเป้าหมายสำคัญดังนี้

1) **เป้าหมายเชิงกลยุทธ์ (Strategic Objective)** เพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการวางแผนยุทธศาสตร์และการดำเนินงานของสถาบัน โดยมุ่งให้เกิดความเชื่อมโยงระหว่าง “ความเสี่ยง – กลยุทธ์ – ผลการดำเนินงาน” อย่างเป็นระบบ
2) **เป้าหมายเชิงระบบบริหารจัดการ (Management Objective)** เพื่อให้ทุกฝ่ายมีระบบบริหารความเสี่ยงที่เป็นมาตรฐานเดียวกัน มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และตัวชี้วัดความเสี่ยงหลัก (KRI) เพื่อใช้ติดตามและรายงานความเสี่ยงอย่างต่อเนื่อง
3) **เป้าหมายเชิงการดำเนินงาน (Operational Objective)** เพื่อให้การดำเนินภารกิจ โครงการและกิจกรรมของสถาบัน มีการบริหารความเสี่ยงอย่างเหมาะสม สามารถลดโอกาสการเกิดเหตุการณ์ไม่พึงประสงค์ และเพิ่มโอกาสในการบรรลุเป้าหมายที่ตั้งไว้
4) **เป้าหมายเชิงการกำกับดูแลและธรรมาภิบาล (Governance Objective)** เพื่อสร้างวัฒนธรรมองค์กรที่มุ่งเน้นความโปร่งใส ความรับผิดชอบ และการตัดสินใจบนพื้นฐานของข้อมูลและความเสี่ยง รวมถึงสนับสนุนให้เกิดการตรวจสอบ ติดตาม และรายงานผลการบริหารความเสี่ยงต่อคณะกรรมการที่เกี่ยวข้องอย่างเป็นระบบ

1.4 โครงสร้างและบทบาทผู้กำกับดูแลความเสี่ยง



โดยมีบทบาท หน้าที่ และความรับผิดชอบในการบริหารความเสี่ยง ดังนี้

บทบาท	หน้าที่และความรับผิดชอบ
คณะกรรมการ สถาบันข้อมูลขนาดใหญ่	1. พิจารณาเห็นชอบประเด็นความเสี่ยงและแนวทางการบริหารจัดการความเสี่ยงตามแผนบริหารความเสี่ยงองค์กรที่ครอบคลุมภารกิจหลักของ สขญ. 2. รับทราบ ผลการบริหารความเสี่ยงของ สขญ. และให้ข้อเสนอแนะต่อระบบบริหารจัดการความเสี่ยง
คณะกรรมการตรวจสอบ	1. สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุม กระบวนการบริหารจัดการความเสี่ยง และกระบวนการกำกับดูแลที่ดี 2. รายงานความเห็นของคณะกรรมการตรวจสอบเกี่ยวกับการบริหารจัดการความเสี่ยง ในรายงานผลการดำเนินงานของคณะกรรมการตรวจสอบประจำปีต่อคณะกรรมการสถาบันข้อมูลขนาดใหญ่
คณะอนุกรรมการยุทธศาสตร์	1. พิจารณากลั่นกรองและให้ข้อเสนอแนะเกี่ยวกับแผนการบริหารความเสี่ยงของ สขญ. เพื่อให้สอดคล้องกับวัตถุประสงค์การจัดตั้งและภารกิจของสถาบัน 2. พิจารณาให้คำปรึกษาและข้อเสนอแนะสำหรับการจัดทำ การทบทวน และการพัฒนาแผนการบริหารความเสี่ยง 3. กำกับติดตามผลการดำเนินงานและการประเมินผลการบริหารความเสี่ยงของ สขญ. รวมถึงการให้ข้อเสนอแนะแนวทางพัฒนา ปรับปรุงกระบวนการทำงานให้มีประสิทธิภาพมากยิ่งขึ้น
ผู้อำนวยการสถาบัน ข้อมูลขนาดใหญ่	1. ส่งเสริมนโยบายการบริหารความเสี่ยงให้เกิดการนำไปปฏิบัติ เพื่อลดหรือควบคุมโอกาสในการเกิดความเสี่ยงนั้น 2. ติดตามการบริหารจัดการความเสี่ยง และรายงานผลการบริหารความเสี่ยงต่อคณะอนุกรรมการยุทธศาสตร์ และคณะกรรมการสถาบันข้อมูลขนาดใหญ่พิจารณาตามลำดับ
ผู้บริหารระดับสูง สขญ. (BDI Top Ex)	1. กำหนดนโยบาย วัตถุประสงค์ เป้าหมาย และระบบการบริหารความเสี่ยง 2. มอบหมายผู้บริหาร (Risk Owner) และเจ้าหน้าที่เกี่ยวข้องกับการปฏิบัติงานด้านความเสี่ยง เพื่อจัดทำแผนการบริหารความเสี่ยงขององค์กร 3. พิจารณาเห็นชอบแผนบริหารความเสี่ยงของ สขญ. เพื่อนำเสนอต่อคณะอนุกรรมการยุทธศาสตร์ และคณะกรรมการสถาบันข้อมูลขนาดใหญ่พิจารณาตามลำดับ 4. ติดตามความก้าวหน้าการดำเนินงานตามแผนบริหารความเสี่ยง เพื่อให้มั่นใจว่าสามารถจัดการความเสี่ยงได้ตามที่กำหนดไว้
ฝ่ายตรวจสอบภายใน	1. สอบทานกระบวนการบริหารความเสี่ยง 2. รายงานผลการสอบทางกระบวนการบริหารความเสี่ยงต่อคณะกรรมการตรวจสอบรับทราบและให้ข้อเสนอแนะเพื่อเป็นแนวทางการพัฒนาระบบบริหารความเสี่ยง

บทบาท	หน้าที่และความรับผิดชอบ
ผู้บริหาร (Risk Owner) และเจ้าหน้าที่เกี่ยวข้องกับการปฏิบัติงานด้านความเสี่ยง (Assistant Risk Owner)	1. จัดทำแผนบริหารความเสี่ยง โดยกำหนดเกณฑ์การประเมินโอกาส (Likelihood) และผลกระทบ (Impact) เพื่อจัดลำดับความสำคัญ และบ่งชี้ประเด็นความเสี่ยง เพื่อจัดทำเป็นแนวทางการบริหารจัดการความเสี่ยงนั้น 2. กำหนดกิจกรรมควบคุมเพื่อตอบสนองความเสี่ยง และจัดทำแผนปฏิบัติการ (Action Plan) 3. ดำเนินการตามแผนปฏิบัติการ (Action Plan) เพื่อลดและควบคุมความเสี่ยง 4. รายงานผลการดำเนินงานตามแนวทางการจัดการความเสี่ยงต่อผู้บริหารระดับสูง สขญ. (BDI Top Ex) คณะอนุกรรมการยุทธศาสตร์ คณะกรรมการสถาบันข้อมูลขนาดใหญ่ ทุก 3 เดือน

บทที่ 2
กรอบแนวคิดและหลักการบริหารความเสี่ยง

2.1 กรอบแนวคิดการบริหารความเสี่ยงองค์กร

สขญ. ใช้กรอบแนวคิดการบริหารความเสี่ยงองค์กรตามมาตรฐานสากล COSO Enterprise Risk Management (ERM) – Integrating with Strategy and Performance (2017) ดังแสดงในรูปที่ 1 และหลักเกณฑ์ของกระทรวงการคลัง (หนังสือ กค 0409.3/ว36 ลงวันที่ 3 กุมภาพันธ์ 2564) ซึ่งให้ความสำคัญกับการบูรณาการกระบวนการบริหารความเสี่ยงเข้ากับการวางแผนยุทธศาสตร์ และการดำเนินงานขององค์กร เพื่อให้การตัดสินใจเชิงบริหารอยู่บนพื้นฐานของข้อมูลความเสี่ยงที่ครบถ้วนและทันสมัย

รูปที่ 1 องคประกอบและหลักการของการบริหารความเสี่ยงขององคกร COSO ERM (2017)
ที่มา: Enterprise Risk Management: Integrating with Strategy and Performance (2017)

กรอบ COSO ERM 2017 ประกอบด้วยองค์ประกอบสำคัญ 5 ด้าน (Components) ได้แก่

1) **Governance & Culture (การกำกับดูแลและวัฒนธรรมองค์กร)** การกำหนดบทบาท หน้าที่และความรับผิดชอบของผู้บริหารในทุกระดับ รวมถึงการสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับการตระหนักรู้และจัดการความเสี่ยง
2) **Strategy & Objective-Setting (กลยุทธ์และการกำหนดวัตถุประสงค์)** การเชื่อมโยงการบริหารความเสี่ยงเข้ากับการกำหนดวัตถุประสงค์เชิงกลยุทธ์ขององค์กร เพื่อให้แน่ใจว่าความเสี่ยงที่อาจเกิดขึ้นได้รับการพิจารณาในทุกขั้นตอนของการวางแผน
3) **Performance (การปฏิบัติการและผลการดำเนินงาน)** การประเมินความเสี่ยงที่อาจกระทบต่อการบรรลุวัตถุประสงค์ การจัดลำดับความสำคัญของความเสี่ยง และการกำหนดมาตรการตอบสนองที่เหมาะสม เพื่อควบคุมหรือบรรเทาความเสี่ยงให้อยู่ในระดับยอมรับได้

4) **Review & Revision (การทบทวนและปรับปรุง)** การติดตาม ประเมิน และปรับปรุงระบบบริหารความเสี่ยงอย่างต่อเนื่อง เพื่อให้ระบบสามารถตอบสนองต่อการเปลี่ยนแปลงของสภาพแวดล้อมภายในและภายนอก
5) **Information, Communication & Reporting (ข้อมูล การสื่อสาร และการรายงาน)** การจัดให้มีระบบข้อมูลและการสื่อสารที่สนับสนุนการบริหารความเสี่ยง รวมถึงการรายงานผลการบริหารความเสี่ยงต่อผู้บริหารและคณะกรรมการอย่างเป็นระบบและโปร่งใส

2.2 หลักการบริหารความเสี่ยงของสถาบัน

สขญ. กำหนดหลักการบริหารความเสี่ยงองค์กรให้สอดคล้องกับกรอบ COSO ERM 2017 และมาตรฐานภาครัฐ เพื่อให้การบริหารความเสี่ยงของสถาบันเป็นไปอย่างมีประสิทธิภาพและเป็นระบบ โดยมีหลักการสำคัญ ดังนี้

1) **ครอบคลุมทุกระดับ (Enterprise-Wide)** การบริหารความเสี่ยงต้องครอบคลุมทั้งระดับองค์กร ฝ่ายงาน และโครงการ เพื่อให้ทุกหน่วยงานมีส่วนร่วม
2) **สอดคล้องกับยุทธศาสตร์ (Alignment with Strategy)** การประเมินและจัดการความเสี่ยงต้องเชื่อมโยงกับเป้าหมายและยุทธศาสตร์หลักของสถาบัน
3) **มีระบบและกระบวนการชัดเจน (Structured & Systematic)** ใช้กระบวนการระบุ ประเมิน ตอบสนอง และติดตามความเสี่ยงอย่างเป็นระบบ และสามารตรวจสอบย้อนกลับได้
4) **เน้นการบริหารเชิงรุก (Proactive Management)** มุ่งเน้นการคาดการณ์ล่วงหน้า (Predictive) และการเตรียมการรองรับความเสี่ยงก่อนเกิดเหตุ
5) **ใช้ข้อมูลเป็นฐาน (Data-Driven)** การตัดสินใจเกี่ยวกับความเสี่ยงอยู่บนพื้นฐานของข้อมูล วิเคราะห์เชิงประจักษ์ และหลักฐานที่ตรวจสอบได้
6) **ความรับผิดชอบร่วมกัน (Shared Responsibility)** ผู้บริหารและบุคลากรทุกระดับมีหน้าที่ร่วมกันในการบริหารความเสี่ยงในส่วนที่ตนรับผิดชอบ
7) **การสื่อสารและรายงานอย่างโปร่งใส (Transparent Communication)** มีระบบรายงานผลความเสี่ยงที่ชัดเจน สม่ำเสมอ และนำเสนอแก่คณะกรรมการที่เกี่ยวข้องอย่างครบถ้วน
8) **การพัฒนาอย่างต่อเนื่อง (Continuous Improvement)** ระบบบริหารความเสี่ยงต้องได้รับการทบทวนและปรับปรุงอย่างต่อเนื่องให้สอดคล้องกับบริบทองค์กรที่เปลี่ยนแปลง

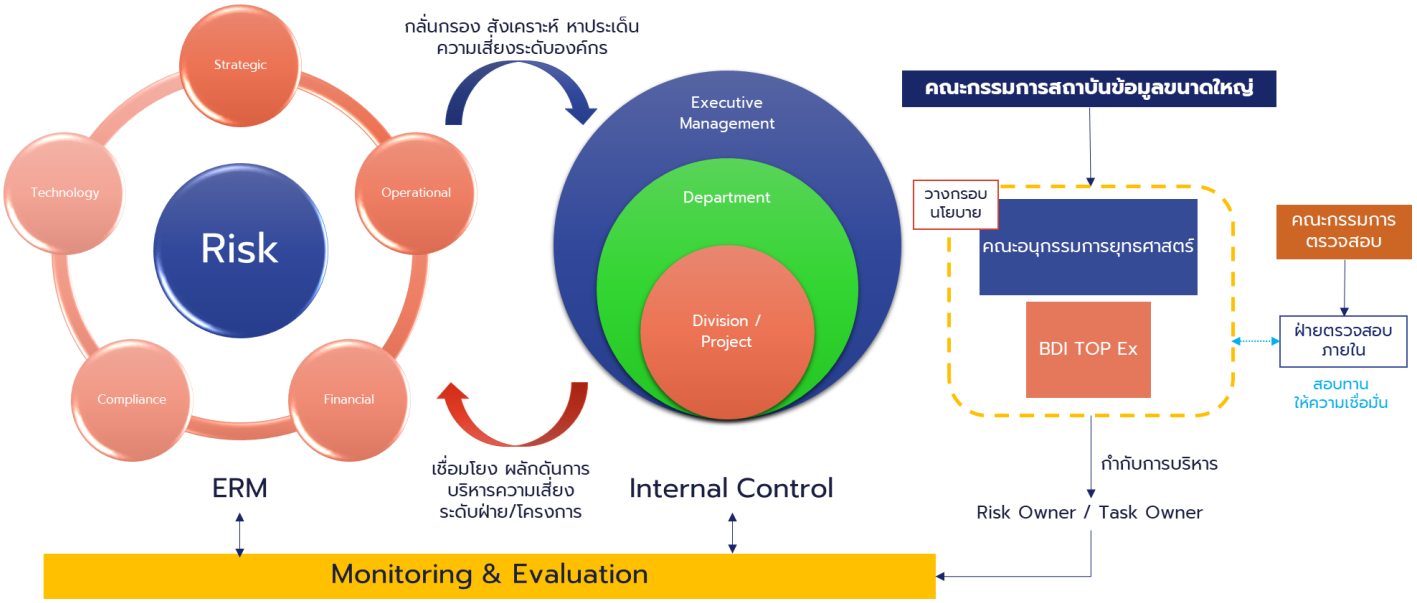
2.3 ความสัมพันธ์ระหว่างการบริหารความเสี่ยงกับระบบการควบคุมภายใน

สขญ. เห็นว่าการบริหารความเสี่ยงและการควบคุมภายในเป็นกระบวนการที่มีความสัมพันธ์และสนับสนุนกันอย่างใกล้ชิด โดย การบริหารความเสี่ยง (Risk Management) เป็น “เครื่องมือเชิงกลยุทธ์” เพื่อระบุและประเมินความเสี่ยงที่อาจส่งผลต่อวัตถุประสงค์ขององค์กร ในขณะที่ การควบคุมภายใน (Internal Control) เป็น “เครื่องมือเชิงปฏิบัติการ”ที่ใช้ในการควบคุม กำกับ และลดโอกาสเกิดความเสี่ยงที่ระบุไว้ให้เหลืออยู่ในระดับที่ยอมรับได้ โดยความสัมพันธ์ระหว่างสองระบบสามารถอธิบายได้ดังตารางที่ 1

ตารางที่ 1 ความสัมพันธ์ระหว่างระบบการบริหารความเสี่ยง และระบบการควบคุมภายใน

ระบบ	วัตถุประสงค์หลัก	ผลลัพธ์ที่คาดหวัง
การบริหารความเสี่ยง (Risk Management, RM)	ระบุและประเมินความเสี่ยงที่อาจกระทบต่อการบรรลุวัตถุประสงค์องค์กร	แผนบริหารความเสี่ยง (Action Plan) และตัวชี้วัดความเสี่ยง (KRI)
การควบคุมภายใน (Internal Control, IC)	กำหนดมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงที่ระบุไว้	ระบบควบคุมภายในที่มีประสิทธิผลและตรวจสอบได้

โดยสรุป การบริหารความเสี่ยงคือ “การมองไปข้างหน้า” เพื่อคาดการณ์สิ่งที่อาจเกิดขึ้น ส่วนการควบคุมภายในคือ “การมองในปัจจุบัน” เพื่อให้แน่ใจว่าการดำเนินงานเป็นไปตามแผนและลดความสูญเสียที่อาจเกิดขึ้น ดังนั้น ทั้งสองกระบวนการนี้จึงต้องดำเนินการควบคู่กัน เพื่อให้ระบบบริหารจัดการของสถาบันมีความครบถ้วนและยั่งยืน ซึ่งจะดำเนินการขับเคลื่อนเพื่อให้เกิดกระบวนการควบคุมภายในและการบริหารความเสี่ยงองค์กรด้วยแนวคิด **“การบริหารความเสี่ยงแบบบูรณาการ (Integrated Risk Management, IRM)”** ดังแสดงในรูปที่ 2 เป็นแนวทางที่องค์กรนำกลยุทธ์ กระบวนการ และบุคลากรมาทำงานร่วมกันเพื่อระบุ ประเมิน และจัดการความเสี่ยงทั้งหมดอย่างเป็นระบบ แทนที่การจัดการความเสี่ยงเป็นส่วน ๆ โดย IRM จะช่วยให้ทุกระดับขององค์กรเข้ามามีส่วนร่วมในการจัดการความเสี่ยง ทำให้การตัดสินใจดีขึ้นและบรรลุเป้าหมายได้ ซึ่งจะนำไปสู่การสร้าง “วัฒนธรรมความเสี่ยง (Risk Culture)”



รูปที่ 2 แนวคิด “การบริหารความเสี่ยงแบบบูรณาการ (Integrated Risk Management, IRM)” ของ สขญ.

2.4 ประเภทของความเสี่ยงองค์กร

สขญ. ได้กำหนดประเภทของความเสี่ยงหลักไว้ 5 ประเภท เพื่อให้การบริหารความเสี่ยงของสถาบันมีทิศทางเดียวกันทั่วทั้งองค์กร ดังนี้

(1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงที่ส่งผลต่อการบรรลุเป้าหมายเชิงยุทธศาสตร์

(2) ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk) ความเสี่ยงจากกระบวนการ บุคลากร หรือระบบ

(3) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงเกี่ยวกับงบประมาณ การใช้จ่าย และแหล่งเงินทุน

(4) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk) ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมายหรือระเบียบ

(5) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risk) ความเสี่ยงเกี่ยวกับระบบเทคโนโลยี ความมั่นคงปลอดภัย และความต่อเนื่องของระบบ

2.5 กระบวนการบริหารความเสี่ยงของสถาบัน (Risk Management Process)

สขญ. ดำเนินการบริหารความเสี่ยงตามกระบวนการ 7 ขั้นตอน ตามมาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ซึ่งได้นำพัฒนาให้สอดคล้องกับมาตรฐาน COSO ERM 2017 โดยมีรายละเอียดดังแสดงในตารางที่ 2

ตารางที่ 2 กระบวนการบริหารความเสี่ยงของสถาบัน

ลำดับ	ขั้นตอน
1. การกำหนดวัตถุประสงค์ (Objective Setting)	กำหนดวัตถุประสงค์ของการดำเนินงานในแต่ละระดับ เพื่อเป็นกรอบในการระบุและบริหารความเสี่ยงให้สอดคล้องกับเป้าหมายองค์กร
2. การระบุความเสี่ยง (Risk Identification)	ระบุเหตุการณ์หรือปัจจัยที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ โดยใช้กรอบวิเคราะห์ PESTEL และ 7S McKinsey ร่วมกับข้อมูลจากทะเบียนความเสี่ยง (Risk Register)
3. การวิเคราะห์ความเสี่ยง (Risk Analysis)	วิเคราะห์สาเหตุและผลกระทบของความเสี่ยง เพื่อทำความเข้าใจบริบทของความเสี่ยงอย่างรอบด้าน
4. การประเมินระดับความเสี่ยง (Risk Assessment)	ประเมินระดับความเสี่ยงโดยใช้เกณฑ์ 2 มิติ (Likelihood × Impact) เพื่อจัดลำดับความสำคัญและพิจารณาระดับความเสี่ยงที่ยอมรับได้
5. การจัดทำแผนบริหารจัดการความเสี่ยง (Risk Management / Response)	กำหนดมาตรการจัดการความเสี่ยงตามหลัก 4T (Tolerate, Treat, Transfer, Terminate) พร้อมระบุผู้รับผิดชอบและระยะเวลา

ลำดับ	ขั้นตอน
6. การติดตามและทบทวนผล (Monitoring & Review)	ติดตามผลการดำเนินการและประเมินประสิทธิผลของมาตรการบริหารความเสี่ยงโดยใช้ตัวชี้วัดความเสี่ยง (KRI) เป็นเครื่องมือหลัก
7. การรายงานผลและปรับปรุงระบบบริหารความเสี่ยง (Reporting & Improvement)	สรุปผลและรายงานต่อคณะกรรมการที่เกี่ยวข้อง รวมทั้งนำข้อเสนอแนะมาปรับปรุงระบบบริหารความเสี่ยงให้เหมาะสมในปีถัดไป

บทที่ 3
การประเมินสภาพแวดล้อมและการวิเคราะห์ปัจจัยเสี่ยง

การบริหารความเสี่ยงองค์กรที่มีประสิทธิภาพจำเป็นต้องอาศัยความเข้าใจเชิงลึกเกี่ยวกับ “สภาพแวดล้อมขององค์กร (Organizational Context)” ทั้งจากภายนอกและภายใน ซึ่งเป็นพื้นฐานสำคัญของการระบุและประเมินความเสี่ยงระดับองค์กรอย่างถูกต้อง ครอบคลุม และสอดคล้องกับยุทธศาสตร์ของสถาบันฯ

สขญ. จึงได้ดำเนินการประเมินสภาพแวดล้อมขององค์กรโดยใช้กรอบวิเคราะห์ที่เป็นมาตรฐานสากล 2 กรอบ ได้แก่

(1) **PESTEL Analysis** สำหรับการวิเคราะห์ปัจจัยภายนอก (External Environment) ที่ส่งผลต่อการดำเนินงานของสถาบันฯ ทั้งในเชิงโอกาสและอุปสรรค

(2) **7S McKinsey Framework** สำหรับการวิเคราะห์ปัจจัยภายใน (Internal Environment) ที่สะท้อนถึงโครงสร้าง กระบวนการ และขีดความสามารถขององค์กร

ผลการประเมินสภาพแวดล้อมทั้งสองด้านนี้จะถูกนำมาสังเคราะห์ร่วมกันในรูปแบบของ SWOT Matrix เพื่อระบุปัจจัยเสี่ยงหลักขององค์กร (Key Enterprise Risks, KR) ใน 5 ประเภทความเสี่ยง ได้แก่ ด้านกลยุทธ์ ด้านการปฏิบัติงาน ด้านการเงิน ด้านการปฏิบัติตามกฎระเบียบ และด้านเทคโนโลยีสารสนเทศ

การวิเคราะห์ดังกล่าวจะเป็นข้อมูลสำคัญในการจัดทำแผนบริหารจัดการความเสี่ยงองค์กร ประจำปีงบประมาณ พ.ศ. 2569 เพื่อให้การบริหารความเสี่ยงของสถาบัน มีทิศทางสอดคล้องกับบริบทการเปลี่ยนแปลงของสภาพแวดล้อมและยุทธศาสตร์องค์กรอย่างยั่งยืน

3.1 การประเมินสภาพแวดล้อมภายนอก

การวิเคราะห์สภาพแวดล้อมภายนอก (External Environment) เป็นขั้นตอนสำคัญในการบริหารความเสี่ยงระดับองค์กร เพื่อให้สถาบันเข้าใจปัจจัยภายนอกที่อาจส่งผลกระทบต่อการดำเนินงานทั้งในเชิงโอกาส (Opportunities) และ อุปสรรค (Threats) ในระยะสั้น–กลาง–ยาว สขญ. ได้ใช้กรอบการวิเคราะห์ PESTEL Framework ซึ่งครอบคลุมปัจจัยด้านการเมือง (Political) เศรษฐกิจ (Economic) สังคม (Social) เทคโนโลยี (Technological) สิ่งแวดล้อม (Environmental) และกฎหมาย (Legal) เพื่อประเมินแนวโน้มและบริบทที่เกี่ยวข้องกับพันธกิจของสถาบัน ดังแสดงในตารางที่ 3

ตารางที่ 3 การประเมินสภาพแวดล้อมภายนอก (PESTEL Analysis)

ปัจจัย PESTEL	สภาพแวดล้อมภายนอก
Political (ด้านการเมือง)	● ความไม่แน่นอนของเสถียรภาพทางการเมืองในประเทศ ● รัฐบาลมีการปรับเปลี่ยนนโยบายด้านดิจิทัลอย่างรวดเร็ว เช่น การผลักดันแพลตฟอร์มข้อมูลภาครัฐ การใช้งานปัญญาประดิษฐ์ภาครัฐ และการเร่งพัฒนาโครงสร้างพื้นฐานข้อมูลระดับชาติ ทำให้สถาบันต้องเตรียมพร้อมปรับตัวอยู่เสมอ

ปัจจัย PESTEL	สภาพแวดล้อมภายนอก
	• โครงสร้างภาครัฐด้านดิจิทัลประกอบด้วยหลายหน่วยงาน (เช่น MDES, DEPA, ETDA, DGA, สกมช.) ซึ่งอาจมีบทบาททับซ้อนกันบางส่วน จำเป็นต้องมีการกำหนดบทบาทและความร่วมมือที่ชัดเจน • การสนับสนุนโครงการเชิงยุทธศาสตร์ของรัฐบาล เช่น Digital ID, Government Cloud, Health Data Exchange อาจเป็นโอกาสในการขับเคลื่อนบทบาทของสถาบัน • ความคาดหวังด้านธรรมาภิบาลข้อมูล (Data Governance) สูงขึ้น ทำให้ต้องยกระดับมาตรฐานข้อมูลและกระบวนการด้านความปลอดภัยอย่างต่อเนื่อง
Economic **(ด้านเศรษฐกิจ)**	• ภาวะเศรษฐกิจชะลอตัวของโลกและไทย รวมถึงภาระงบประมาณแผ่นดินที่สูงขึ้น ส่งผลให้การจัดสรรงบประมาณแก่หน่วยงานรัฐต้องคำนึงถึงข้อจำกัดมากขึ้น • ค่าใช้จ่ายด้านเทคโนโลยี โดยเฉพาะระบบ Cloud, Cybersecurity, Data Platform และการบำรุงรักษาระบบ มีแนวโน้มเพิ่มขึ้นทุกปี ทำให้งบประมาณต้องครอบคลุมค่าใช้จ่ายผันแปร • การเติบโตของเศรษฐกิจข้อมูล (Data Economy) และภาคส่วนเอกชนที่ให้ความสำคัญกับการลงทุนด้านข้อมูล/AI เป็นโอกาสในการร่วมมือเพื่อพัฒนาบริการข้อมูลหรือบริการวิเคราะห์ร่วมกัน • บุคลากรภาครัฐมีข้อจำกัดด้านค่าตอบแทนเมื่อเทียบกับภาคเอกชน ทำให้การแข่งขันในตลาดแรงงานดิจิทัลมีความท้าทาย
Social **(ด้านสังคม)**	• รูปแบบแรงงานใหม่ในระบบ Gig Economy ขยายตัวต่อเนื่อง ทำให้แรงงานมีแนวโน้มเลือกงานแบบอิสระและ on-demand มากขึ้น ส่งผลให้ภาครัฐรวมถึงสถาบันต้องเผชิญความท้าทายในการสรรหาและรักษาบุคลากรที่มีทักษะเฉพาะทาง • ความต้องการแรงงานด้านดิจิทัล เช่น Data Engineer, Data Scientist, AI Specialist, Cybersecurity Specialist สูงขึ้น แต่กำลังผลิตบุคลากรยังไม่เพียงพอกับความต้องการของประเทศ • ประชาชนและองค์กรให้ความสำคัญกับความปลอดภัยข้อมูลส่วนบุคคลเพิ่มขึ้น ส่งผลให้ความคาดหวังต่อความโปร่งใสและการใช้ข้อมูลภาครัฐต้องอยู่ในกรอบจริยธรรมและมาตรฐานสูง • สังคมหันมาใช้บริการออนไลน์มากขึ้น ทำให้ข้อมูลภาครัฐมีความสำคัญต่อการให้บริการประชาชน ส่งผลให้สถาบันต้องสามารถรองรับข้อมูลที่หลากหลายและปริมาณมาก • ความตื่นตัวด้านปัญญาประดิษฐ์ของประชาชนทำให้เกิดความต้องการนำข้อมูลภาครัฐไปสร้างประโยชน์ในรูปแบบใหม่ ๆ มากขึ้น

ปัจจัย PESTEL	สภาพแวดล้อมภายนอก
Technological (ด้านเทคโนโลยี)	• ภัยคุกคามไซเบอร์รุนแรงและซับซ้อนขึ้น โดยเฉพาะ Ransomware, Malware Attack, Data Breach, Zero-day หรือต้นทางข้อมูลภายนอกที่อาจมีความเสี่ยง ทำให้ต้องพัฒนามาตรการป้องกัน–ติดตาม–ตอบสนองอย่างต่อเนื่อง • เทคโนโลยีด้านข้อมูลเปลี่ยนแปลงรวดเร็ว เช่น Generative AI, Large Language Models, Cloud-Native Architecture, Data Lakehouse ทำให้จำเป็นต้องพัฒนาศักยภาพด้านเทคโนโลยีอยู่เสมอ • การพึ่งพาเทคโนโลยีจากผู้ให้บริการรายเดียวอาจสร้างความเสี่ยงด้าน Vendor Lock-in ทำให้เกิดข้อจำกัดด้านงบประมาณและความยืดหยุ่น • ความต้องการด้าน Data Governance, Data Security, Metadata Management และคุณภาพข้อมูลสูงขึ้นตามปริมาณข้อมูลที่เพิ่มขึ้นอย่างรวดเร็ว
Environmental (ด้านสิ่งแวดล้อม)	• การเปลี่ยนแปลงสภาพภูมิอากาศและภัยธรรมชาติอาจกระทบโครงสร้างพื้นฐานดิจิทัลและศูนย์ข้อมูล เช่น ความร้อนสูงในฤดูร้อน น้ำท่วม ไฟฟ้าดับ • แนวโน้มมาตรฐาน Green Data Center ทำให้ต้องเตรียมปรับระบบด้านพลังงาน ประสิทธิภาพ และการใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม • ผู้กำกับด้านสิ่งแวดล้อมเริ่มให้ความสนใจกับข้อมูล ESG มากขึ้น ทำให้ข้อมูลด้านสิ่งแวดล้อมอาจเป็นบริการข้อมูลใหม่ที่สถาบันต้องพัฒนาในอนาคต
Legal (ด้านกฎหมาย)	• มีกฎหมายด้านข้อมูลและเทคโนโลยีจำนวนมาก เช่น PDPA พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ ระเบียบข้อมูลภาครัฐ หรือ กฎหมายว่าด้วย AI ที่อาจประกาศใช้ในอนาคต • การตีความกฎหมายระหว่างหน่วยงานมีความแตกต่างกัน ส่งผลให้การเชื่อมโยงข้อมูลระหว่างส่วนราชการต้องอาศัยการกำกับดูแลและทำความเข้าใจร่วมกัน • ข้อจำกัดด้าน TOR ระเบียบพัสดุ และการจัดซื้อจัดจ้างภาครัฐ ส่งผลต่อความคล่องตัวในการพัฒนาเทคโนโลยีและบริการข้อมูล • ความคาดหวังของผู้ตรวจสอบและหน่วยงานกำกับ (เช่น สำนักงานตรวจเงินแผ่นดิน, สศช. หรือ สกมช.) เพิ่มขึ้น ทำให้ต้องเตรียมข้อมูลและหลักฐานการปฏิบัติที่ครบถ้วน

3.2 การประเมินสภาพแวดล้อมภายใน

การประเมินสภาพแวดล้อมภายในของ สขญ. ดำเนินการโดยใช้กรอบการวิเคราะห์แบบ 7S McKinsey ซึ่งเป็นกรอบการวิเคราะห์ที่มุ่งประเมินองค์ประกอบหลักขององค์กร 7 ด้าน ได้แก่ Strategy, Structure, Systems, Shared Values, Skills, Staff และ Style เพื่อระบุจุดแข็ง (Strengths) และจุดอ่อน (Weaknesses) ขององค์กรในปัจจุบัน โดยการประเมินครั้งนี้พิจารณาจากข้อมูลองค์กร แผนกลยุทธ์ของ สขญ. ปีงบประมาณ พ.ศ. 2569 - 2570 แผนกลยุทธ์การบริหารและพัฒนาบุคลากร พ.ศ. 2567 – 2670 แผนการควบคุมภายในและทะเบียนความเสี่ยง (Risk Register) ระดับฝ่าย/โครงการ ปีงบประมาณ 2569 และผลการดำเนินงานบริหารความเสี่ยงปี 2568 ซึ่งทั้งหมดสะท้อนภาพรวมสภาพแวดล้อมภายในได้อย่างรอบด้านและเป็นปัจจุบัน โดยสามารถวิเคราะห์และแสดงผลการประเมินสภาพแวดล้อมภายในตามกรอบ 7S McKinsey ได้ดังตารางที่ 4

ตารางที่ 4 แสดงผลการประเมินสภาพแวดล้อมภายในของ สขญ. ตามกรอบ 7S McKinsey

กรอบ 7S McKinsey	สภาพแวดล้อมภายใน
Strategy (กลยุทธ์)	• สถาบันมีทิศทางยุทธศาสตร์ที่สอดคล้องกับบทบาทด้านข้อมูลระดับชาติ เช่น การพัฒนาแพลตฟอร์มข้อมูล การวิเคราะห์ข้อมูลเพื่อเชิงนโยบาย การใช้ AI ในภาครัฐ • การขยายภารกิจด้านข้อมูลภาครัฐ เช่น ด้านสาธารณสุข การท่องเที่ยว สิ่งแวดล้อม ทำให้ต้องเพิ่มประสิทธิภาพการบริหารจัดการและการบูรณาการระหว่างฝ่าย • การปรับตัวตามนโยบายรัฐบาลบางส่วนจำเป็นต้องดำเนินการภายในระยะเวลาสั้น ทำให้เกิดแรงกดดันด้านทรัพยากรและบุคลากร
Structure (โครงสร้างองค์กร)	• องค์กรอยู่ในช่วงเติบโต ทำให้บทบาทและความรับผิดชอบของฝ่ายงานหลายส่วนยังต้องมีการจัดวางใหม่ให้รองรับภารกิจที่เพิ่มขึ้น • โครงสร้างงานเชิงเทคนิคและงานเชิงนโยบายต้องทำงานประสานกันมากขึ้น โดยเฉพาะโครงการระดับชาติ • ยังจำเป็นต้องยกระดับรูปแบบการทำงานร่วมกันระหว่างฝ่ายให้เป็นระบบเดียวกันมากขึ้น
Systems (ระบบและกระบวนการทำงาน)	• ระบบงานบางกระบวนการยังต้องพัฒนา SOP ให้ชัดเจนขึ้น โดยเฉพาะการบูรณาการงานข้ามฝ่าย • การกำกับคุณภาพข้อมูล (Data Quality) และ Data Governance ยังอยู่ระหว่างการพัฒนาให้ครอบคลุมทั้งองค์กร • ระบบความมั่นคงปลอดภัยไซเบอร์ต้องการการลงทุนและปรับปรุงต่อเนื่อง เช่น SOC SIEM และ ระบบสำรองข้อมูล

กรอบ 7S McKinsey	สภาพแวดล้อมภายใน
	• การจัดซื้อจัดจ้างมีข้อจำกัดจากกฎหมาย ทำให้ต้องวางแผนและประสานงานอย่างรัดกุม
Shared Values (ค่านิยมและวัฒนธรรมองค์กร)	• บุคลากรมีค่านิยมร่วมด้านการสร้างประโยชน์สาธารณะ การใช้ข้อมูลขับเคลื่อนประเทศ และการทำงานแบบโปร่งใส • มีแรงผลักดันด้านนวัตกรรมและการยกระดับมาตรฐานข้อมูลภาครัฐ
Skills (ทักษะและความเชี่ยวชาญ)	• บุคลากรมีความเชี่ยวชาญด้านข้อมูล แต่บางส่วนยังต้องเสริมทักษะเชิงเทคนิค เช่น Data Architecture Machine Learning หรือ Cloud Computing • งานด้านกฎหมายข้อมูล พัสดุ และการทำ TOR ยังต้องเสริมความเข้าใจให้ครอบคลุมและทันสมัยมากขึ้น
Staff (บุคลากรและศักยภาพ)	• บุคลากรมีความมุ่งมั่นและพร้อมรับผิดชอบงานสูง แต่จำนวนยังไม่เพียงพอเมื่อเทียบกับภารกิจ และหลายฝ่ายต้องรองรับงานใหม่จำนวนมาก • ความต้องการบุคลากรเชิงเทคนิค เช่น Data Engineer Cybersecurity Specialist ยังสูงกว่าจำนวนที่มีอยู่
Style (ภาวะผู้นำและรูปแบบการบริหาร)	• สถาบันมีวัฒนธรรมที่ร่วมมือกันได้ดีและมีความคล่องตัวสูง • ยังจำเป็นต้องเสริมระบบสนับสนุน เช่น ระบบหรือวิธีติดตามผลการดำเนินงาน เพื่อรองรับงานขนาดใหญ่จำนวนมาก

3.3 การวิเคราะห์สภาพแวดล้อมองค์รวม

จากผลการประเมินสภาพแวดล้อมภายนอก (PESTEL) และสภาพแวดล้อมภายใน (7S McKinsey) สขญ. ได้นำข้อมูลทั้งสองส่วนมาสังเคราะห์เพื่อจัดทำการวิเคราะห์ SWOT ในระดับองค์กร โดยมีวัตถุประสงค์เพื่อระบุจุดแข็ง (Strengths) จุดอ่อน (Weaknesses) โอกาส (Opportunities) และอุปสรรค/ความท้าทาย (Threats) ที่มีผลต่อการดำเนินงานในปีงบประมาณ พ.ศ. 2569 และเพื่อใช้เป็นพื้นฐานสำคัญสำหรับระบุประเด็นความเสี่ยงที่สำคัญขององค์กร (Key Enterprise Risks) ซึ่งเป็นฐานของการกำหนดความเสี่ยงระดับองค์กร (Enterprise Risks) สามารถแสดงผลการวิเคราะห์ SWOT ได้ดังตารางที่ 5

ตารางที่ 5 ผลการวิเคราะห์ SWOT ของ สขญ.

Strengths (S) – จุดแข็งภายในองค์กร ● ความเชี่ยวชาญด้านข้อมูลและเทคโนโลยีของบุคลากร ● โครงการระดับชาติที่เป็นที่รู้จัก เช่น Health Link และ Travel Link ● ระบบกำกับดูแลคุณภาพข้อมูลเริ่มชัดเจนขึ้น ● การสนับสนุนจากผู้บริหารระดับสูง	**Opportunities (O) – โอกาสจากสภาพแวดล้อมภายนอก** ● นโยบายรัฐบาลดิจิทัลสนับสนุนบทบาทของ สขญ. ● การเติบโตของเทคโนโลยี AI และ Big Data ● ความต้องการใช้ข้อมูลภาครัฐเพิ่มสูงขึ้น ● โอกาสสร้างความร่วมมือกับหน่วยงานรัฐและเอกชน
Weaknesses (W) – จุดอ่อนภายในองค์กร ● บุคลากรและทักษะเฉพาะทางยังไม่เพียงพอ ● โครงสร้าง บทบาท และความรับผิดชอบบางส่วนยังอยู่ระหว่างการปรับประสานให้เหมาะสมกับภารกิจที่ขยายตัวของสถาบัน ● SOP และ Workflow ระหว่างฝ่ายยังพัฒนาไม่ครบถ้วน ● ระบบรักษาความปลอดภัยข้อมูลต้องขยายให้ครอบคลุมมากขึ้น ● กระบวนการจัดซื้อจัดจ้างยังมีความจำเป็นในการพัฒนาและเพิ่มพูนความเข้าใจให้ครอบคลุมแก่บุคลากรมากขึ้น	**Threats (T) – ความท้าทายจากภายนอก** ● การขับเคลื่อนให้เกิดกฎหมายด้านการแบ่งบันข้อมูล ● ภัยไซเบอร์รุนแรงและซับซ้อนมากขึ้น ● การตีความกฎหมายด้านข้อมูลภาครัฐมีความแตกต่างกัน ● งบประมาณมีข้อจำกัด ● การแข่งขันด้านบุคลากรดิจิทัลกับภาคเอกชนสูงขึ้น

การวิเคราะห์สถานการณ์และคาดการณ์ปัจจัยที่อาจส่งผลต่อการดำเนินงานของสถาบันฯ ได้ดังนี้

(1) การขับเคลื่อนภารกิจเชิงยุทธศาสตร์ด้านข้อมูลขนาดใหญ่

- กฎหมายและกฎระเบียบด้านการแบ่งปันข้อมูล ที่มอบหมายภารกิจให้ สขญ. ต้องขับเคลื่อนให้เกิดขึ้น เพื่อให้หน่วยงานภายนอกมีความมั่นใจในการเชื่อมโยงข้อมูลเข้าสู่แพลตฟอร์มข้อมูลขนาดใหญ่แห่งชาติ (D2)
- สถาบันฯ ต้องเร่งสร้างการรับรู้แพลตฟอร์มข้อมูลขนาดใหญ่แห่งชาติ (D2) เพื่อให้เกิดการเชื่อมโยงข้อมูลระหว่างหน่วยงาน และเกิดการใช้ประโยชน์ข้อมูลเชิงวิเคราะห์จากแพลตฟอร์มฯ

(2) สถานภาพบุคลากรและโครงสร้างงานที่กำลังขยายตัว

- สถาบันฯ ได้เชื่อมั่นในการทำภารกิจที่สำคัญและเร่งด่วนจากภาครัฐ จึงจำเป็นต้องบริหารจัดการกำลังคนให้สอดคล้องกับภาระงานที่เกิดขึ้น

(3) การบริหารงบประมาณภายใต้ข้อจำกัดของงบประมาณพลางก่อน

- การเลือกตั้งใหม่ ทำให้กระบวนการจัดสรรงบประมาณรายจ่าย ในปี 2570 ไม่ทันตามปีงบประมาณ ส่งผลให้งานใหม่ไม่ได้รับการจัดสรรงบประมาณในช่วงพลางก่อน (ช่วงก่อนในช่วงที่อยู่ระหว่างการพิจารณางบประมาณปี 2570)

- สถาบันฯ ต้องบริหารการใช้จ่ายงบประมาณอย่างมีประสิทธิภาพ สามารถส่งมอบผลงานได้ตามเป้าหมายที่กำหนดไว้ อย่างคุ้มค่า และไม่ซ้ำซ้อน เพื่อให้มีเงินคงเหลือสะสมสำหรับดำเนินงานใหม่ ในช่วงงบประมาณพลางก่อน

(4) ความซับซ้อนของกฎหมายกำกับข้อมูลภาครัฐ

- กฎหมายด้านข้อมูลของหน่วยงานรัฐมีหลายฉบับและมีข้อกำหนดไม่เหมือนกัน เช่น การใช้ข้อมูลส่วนบุคคล การเปิดเผยข้อมูล และความมั่นคงทางไซเบอร์ ทำให้การตีความเพื่อใช้ข้อมูลร่วมกันระหว่างหน่วยงานยังไม่เป็นไปในทิศทางเดียวกัน และอาจเป็นข้อจำกัดต่อการนำข้อมูลไปใช้ประโยชน์

(5) ความเสี่ยงด้านเทคโนโลยีและภัยคุกคามทางไซเบอร์

- ระบบสารสนเทศของสถาบันฯ ต้องรองรับข้อมูลสำคัญและบริการแก่หน่วยงานจำนวนมาก จึงเป็นเป้าหมายของการโจมตีไซเบอร์มากขึ้น
- การสูญหายของข้อมูล ระบบหยุดชะงัก หรือการโจมตีแบบ Ransomware/Data Breach อาจส่งผลกระทบต่อความเชื่อมั่น และภารกิจหลักของสถาบันฯ

3.4 ประเด็นความเสี่ยงที่สำคัญขององค์กร (Key Enterprise Risks)

จากผลการประเมินสภาพแวดล้อมทั้งภายนอกและภายในของสถาบันตามกรอบ PESTEL และ McKinsey 7S รวมถึงการวิเคราะห์ SWOT สามารถสรุปได้ว่ามีปัจจัยหลายด้านที่ส่งผลต่อความพร้อม ความท้าทาย และความเสี่ยงเชิงยุทธศาสตร์ของสถาบันอย่างมีนัยสำคัญ ทั้งจากความคาดหวังของหน่วยงานภายนอก นโยบายภาครัฐที่เปลี่ยนแปลงอย่างรวดเร็ว ความก้าวหน้าทางเทคโนโลยี การขยายตัวของภารกิจภายในองค์กร ตลอดจนข้อจำกัดด้านทรัพยากรและกฎหมายข้อมูลภาครัฐที่มีความซับซ้อน

เพื่อนำปัจจัยดังกล่าวไปสู่การกำหนด “ความเสี่ยงระดับองค์กร” (Enterprise Risks) สขญ. ได้ดำเนินการประมวลผลร่วมกับข้อมูลจาก Risk Register รายฝ่าย การทบทวนผลการบริหารความเสี่ยงปีงบประมาณ พ.ศ. 2568 ดังแสดงในตารางที่ 6 และความเห็นเชิงยุทธศาสตร์จากผู้บริหารระดับสูง เพื่อให้สามารถระบุความเสี่ยงที่มีผลกระทบต่อเป้าหมายของสถาบันในภาพรวมได้อย่างถูกต้องและรอบด้าน ผลลัพธ์คือการกำหนด ประเด็นความเสี่ยงที่สำคัญขององค์กรจำนวน 5 ประเด็น ครอบคลุมมิติเชิงกลยุทธ์ การปฏิบัติงาน การเงิน การปฏิบัติตามกฎหมาย และเทคโนโลยี ดังแสดงในตารางที่ 7 ซึ่งเป็นความเสี่ยงที่ต้องติดตามอย่างใกล้ชิดและจัดทำแผนบริหารความเสี่ยงในขั้นตอนต่อไป

ตารางที่ 6 การทบทวนการบริหารความเสี่ยงปีงบประมาณ พ.ศ. 2568

ความเสี่ยงปีงบประมาณ พ.ศ. 2568	การทบทวนผลการบริหารความเสี่ยงปีงบประมาณ พ.ศ. 2568
Strategic Risk (RES): ไม่สามารถสร้างความร่วมมือกับหน่วยงานพันธมิตรในการเชื่อมโยงข้อมูลได้ตามแผนกลยุทธ์ของ สขญ.	ระดับความเสี่ยง สูง (12) ลดลงเหลือ ปานกลาง (9) จากการดำเนินมาตรการสำรวจความพร้อม ประชาสัมพันธ์ และสนับสนุนหน่วยงานต้นทาง พร้อมทั้งขับเคลื่อนร่าง พ.ร.บ.แบ่งปันข้อมูล อย่างไรก็ตาม ยังพบปัญหาที่หลงเหลือ ได้แก่ ขั้นตอนเอกสารที่ใช้เวลานาน กรอบกฎหมายที่ยังไม่สมบูรณ์ ความไม่พร้อมของบางหน่วยงาน และความเชื่อมั่นต่อระบบกลางที่ต้องเสริมต่อเนื่อง จากการประเมินเชิงยุทธศาสตร์ ประเด็นนี้พัฒนาเป็น RES ปี 2569: ความเชื่อมั่นของหน่วยงานภายนอกต่อการเชื่อมโยงข้อมูลกับแพลต์ฟอร์ม D2
Operational Risk (REO): ผู้บริหารระดับต้นยังขาดประสบการณ์ในการบริหาร จนส่งผลให้ไม่สามารถดำเนินงานได้ตามเป้าหมายในปี 2568	ระดับความเสี่ยง สูง (12) ลดลงเหลือ ต่ำ (4) หลังจากมีการอบรมทักษะผู้บริหาร การจัดทำ OKR/PMS การกำหนดตัวชี้วัดชัดเจน และการติดตามใกล้ชิด ทำให้ความสามารถในการบริหารดีขึ้น อย่างไรก็ตาม ภารกิจใหม่ที่สถาบันได้รับในระดับนโยบายมีจำนวนมากขึ้น ส่งผลให้เกิดความกดดันต่อภารกิจหลัก แม้ทักษะผู้บริหารจะดีขึ้นแต่ภาระงานที่เพิ่มขึ้นยังเป็นช่องโหว่สำคัญ ความเสี่ยงดังกล่าวจึงแปรเปลี่ยนเป็นลักษณะเชิงโครงสร้าง นำไปสู่ REO ปี 2569: งานใหม่ที่เพิ่มขึ้นกะทันหัน ส่งผลกระทบต่อภารกิจหลักของสถาบัน
Financial Risk (REF): ไม่มีงบประมาณที่เพียงพอต่อการดำเนินให้เป็นไปตามภารกิจการจัดตั้งสถาบันฯ	ระดับความเสี่ยง ปานกลาง (9) ลดลงเหลือ ต่ำมาก (1) หลังจากสถาบันได้รับการจัดสรรงบประมาณเพิ่มขึ้นกว่า 68% แต่ในทางปฏิบัติ ภารกิจใหม่ที่ได้รับมอบหมายมีจำนวนมากกว่าเดิมอย่างมีนัยสำคัญ ถึงแม้งบประมาณได้รับเพิ่มขึ้น แต่ความต้องการใช้งบเพิ่มขึ้นในอัตราที่สูงกว่า โดยเฉพาะงานเร่งด่วนระดับนโยบาย จึงพัฒนาเป็นความเสี่ยงเชิงโครงสร้าง นำไปสู่ REF ปี 2569: งบประมาณไม่เพียงพอสำหรับการขับเคลื่อนงานใหม่และงานสำคัญของสถาบัน
Compliance Risk (REC): การรับรู้ เข้าใจ ในเรื่องกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้องน้อย จนส่งผลกระทบกับการดำเนินงานของสถาบันฯ	ระดับความเสี่ยง ปานกลาง (6) ลดลงเหลือ ต่ำ (4) เนื่องจากมีการจัดอบรม PDPA, TOR, Digital Workplace, BDI 101 เป็นต้น ทำให้บุคลากรมีความเข้าใจมากขึ้น แต่สิ่งที่ยังคงเป็นปัญหาคงเหลือ คือความหลากหลายและซับซ้อนของกฎหมายด้านข้อมูลภาครัฐที่เพิ่มขึ้น เช่น PDPA, Cybersecurity Act, Data Governance, AI Regulation รวมถึงความแตกต่างของการตีความระหว่างหน่วยงาน ทำให้ประเด็นนี้พัฒนาต่อไปเป็น REC ปี 2569: ความซับซ้อนของกฎหมายด้านข้อมูลภาครัฐที่ส่งผลต่อการใช้ข้อมูลของสถาบัน
Technology Risk (RET): มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไม่ได้รับการปรับปรุงให้ทันสมัยและครบถ้วนตามแผนการดำเนินงานของสถาบันฯ จึงทำให้เกิดภัยคุกคามทางไซเบอร์	ระดับความเสี่ยง สูง (12) ลดลงเหลือ ต่ำมาก (1) จากการออกนโยบายความมั่นคงไซเบอร์ การจัดทำ 6 Domains (ID–GV) การอบรมบุคลากร และการตรวจประเมินภายในครบถ้วน แม้ความเสี่ยงตามแผนจะลดลงอย่างมีนัยสำคัญ แต่สถานการณ์ภัยไซเบอร์ภายนอกประเทศมีความรุนแรงมากขึ้น ข้อมูลภาครัฐกลายเป็นเป้าหมายโจมตีหลัก และยังต้องลงทุนต่อเนื่องใน SOC, DRP และ Incident Response ดังนั้น ประเด็นนี้จึงถูกยกระดับในเชิงยุทธศาสตร์ให้เป็น RET ปี 2569: ภัยคุกคามไซเบอร์ที่อาจทำให้ข้อมูลรั่วไหลหรือระบบหยุดชะงัก

ตารางที่ 7 ประเด็นความเสี่ยงที่สำคัญขององค์กร (Key Enterprise Risks) ปีงบประมาณ พ.ศ. 2569

ประเภทความเสี่ยง	ประเด็นความเสี่ยงที่สำคัญขององค์กร (Key Enterprise Risks)
1. Strategic Risk	RES: มีความล่าช้าในการเชื่อมโยงขอรับข้อมูลเข้าแพลตฟอร์มข้อมูลขนาดใหญ่แห่งชาติ (D2) เนื่องจาก ยังไม่มีกฎหมาย/กฎระเบียบ ที่มอบหมายภารกิจโดยตรง จึงส่งผลให้ต้องมีกระบวนการด้านเอกสารหลายขั้นตอน
2. Operational Risk	REO: ได้รับมอบหมายงานใหม่เพิ่มเติมอย่างกะทันหัน จนส่งผลกระทบต่อการดำเนินงานหลักของสถาบันฯ
3. Financial Risk	REF: ไม่มีงบประมาณสำหรับงานใหม่ที่ต้องการการขับเคลื่อน ในช่วงงบประมาณพลางก่อน จนส่งผลกระทบต่อเป้าหมายของสถาบันฯ
4. Compliance Risk	REC: ความเสี่ยงจากความเข้าใจคลาดเคลื่อนในการตีความและการปฏิบัติตามกฎหมายด้านข้อมูล
5. Technology Risk	RET: ระบบสารสนเทศของสถาบันฯ ถูกโจมตีทางไซเบอร์ จนส่งผลให้ข้อมูลรั่วไหล สูญหาย หรือระบบให้บริการหยุดชะงัก (Ransomware / Data Breach)

บทที่ 4
แผนบริหารจัดการความเสี่ยงองค์กร ประจำปีงบประมาณ พ.ศ. 2569

จากการวิเคราะห์สภาพแวดล้อมภายนอกและภายในของสถาบันตามกรอบ PESTEL และ McKinsey 7S รวมถึงการสังเคราะห์ข้อมูลจากการวิเคราะห์ SWOT นั้น สขญ. ได้ระบุประเด็นความเสี่ยงเชิงยุทธศาสตร์ที่มีผลต่อการบรรลุเป้าหมายของสถาบันในปีงบประมาณ พ.ศ. 2569 อย่างรอบด้าน และเพื่อให้การบริหารความเสี่ยงของสถาบันฯ เป็นไปอย่างเป็นระบบและสอดคล้องกับหลักเกณฑ์ตามระเบียบกระทรวงการคลังและแนวทาง COSO ERM 2017 สขญ. จึงมุ่งจัดทำ “แผนบริหารความเสี่ยงระดับองค์กร” โดยกำหนดระดับความเสี่ยง (Likelihood × Impact) ของแต่ละประเด็น สร้างแนวทางการจัดการความเสี่ยงที่เหมาะสม (Risk Response) ระบุเจ้าของความเสี่ยง (Risk Owner) และผู้ช่วยเจ้าของความเสี่ยง (Assistant Risk Owner) รวมถึงกำหนดตัวชี้วัดความเสี่ยงที่สำคัญ (KRI) เพื่อใช้ในการติดตามผลอย่างต่อเนื่องการติดตามและประเมินผล (Monitoring & Evaluation) เป็นกลไกสำคัญในการสร้างความเชื่อมั่น

4.1 วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

การจัดทำแผนบริหารความเสี่ยงระดับองค์กรมีวัตถุประสงค์เพื่อ

1. กำหนดความเสี่ยงที่สำคัญต่อการบรรลุเป้าหมายยุทธศาสตร์ของสถาบัน
2. จัดลำดับความสำคัญของความเสี่ยงที่ต้องบริหารอย่างเป็นระบบ
3. ระบุผู้รับผิดชอบการบริหารความเสี่ยง ได้แก่ เจ้าของความเสี่ยง (Risk Owner) และผู้ช่วยเจ้าของความเสี่ยง (Assistant Risk Owner) อย่างชัดเจน
4. จัดทำแผนบริหารความเสี่ยงและตัวชี้วัดความเสี่ยงที่สำคัญ (KRI)

4.2 ระดับความเสี่ยงและเกณฑ์การประเมิน

การประเมินความเสี่ยงเป็นการจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เพื่อให้ได้ระดับความเสี่ยง (Risk Level)

- **โอกาสที่จะเกิดหรือความถี่ (Likelihood)** หมายถึง ความถี่ของการเกิดเหตุการณ์ความเสี่ยงว่ามีโอกาสเกิดขึ้นมากน้อยเพียงใด โดยการพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือการคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต
- **ความรุนแรงหรือผลกระทบ (Impact)** หมายถึง ความรุนแรงของเหตุการณ์ความเสี่ยงที่หากเกิดขึ้นแล้วจะส่งผลกระทบในด้านต่างๆ ซึ่งผลกระทบนั้นพิจารณาได้ทั้งเชิงปริมาณ ได้แก่ ผลเสียหายด้านการเงิน และผลกระทบเชิงคุณภาพ ได้แก่ ชื่อเสียงภาพลักษณ์ขององค์กร ความปลอดภัยในชีวิตและทรัพย์สินของบุคลากร และประสิทธิผลของการดำเนินงาน
- **ระดับความเสี่ยง (Risk Level)** กำหนดค่าเท่ากับผลคูณของระดับโอกาสหรือความถี่ที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) และระดับความรุนแรงหรือผลกระทบ (Impact) อันเนื่องมาจากความเสี่ยง

ระดับความเสี่ยง Risk Level =
ระดับโอกาสหรือความถี่ (Likelihood) × ระดับความรุนแรงหรือผลกระทบ (Impact)

โดยสามารถคำนวณออกมาเป็นแผนภูมิความเสี่ยง (Risk map) ได้ดังตารางที่ 8

ตารางที่ 8 แผนภูมิความเสี่ยง (Risk map)

ผลกระทบ (Impact) / โอกาสเกิด (Likelihood)		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
		1	2	3	4	5
เกิดขึ้นสูงมาก	5	5	10	15	20	25
เกิดขึ้นสูง	4	4	8	12	16	20
เกิดขึ้นบ้าง	3	3	6	9	12	15
เกิดขึ้นน้อย	2	2	4	6	8	10
เกิดขึ้นยาก	1	1	2	3	4	5

จากการคำนวณตามแผนภูมิความเสี่ยง (Risk map) สามารถสรุประดับความเสี่ยง (Risk Level) โดยมีคำอธิบายความเสี่ยงได้เป็น 4 ระดับ ดังรายละเอียดในตารางที่ 9

ตารางที่ 9 การจัดแบ่งระดับความเสี่ยง (Risk Level) และความหมายของแต่ละระดับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	ความหมาย
สูงมาก (Extreme)	17 - 25	**ระดับที่ไม่สามารถยอมรับได้** จำเป็นต้องเร่งจัดการความเสี่ยงในทันที เพื่อให้ความเสี่ยงลดลง และอยู่ในระดับที่ยอมรับได้ในที่สุด
สูง (High)	10 - 16	**ระดับที่ไม่สามารถยอมรับได้** โดยต้องเฝ้าระวังและจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
ปานกลาง (Medium)	5 - 9	**ระดับที่พอยอมรับได้** แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงไปอยู่ในระดับที่ยอมรับไม่ได้
น้อย (Low)	1 - 4	**ระดับที่ยอมรับได้** โดยใช้วิธีควบคุมปกติในขั้นตอนการปฏิบัติงานที่กำหนด และติดตามระดับความเสี่ยงตลอดระยะเวลาการปฏิบัติงาน

4.3 แผนบริหารความเสี่ยงองค์กรปีงบประมาณ พ.ศ. 2569

สถาบันฯ ได้พิจารณาระบุประเด็นความเสี่ยงระดับองค์กรที่ต้องได้รับการจัดการในปีงบประมาณ พ.ศ. 2569 พร้อมกำหนดผู้รับผิดชอบของแต่ละประเด็นความเสี่ยง ดังแสดงในตารางที่ 10

ตารางที่ 10 ประเด็นความเสี่ยงองค์กร ปีงบประมาณ พ.ศ. 2569 และผู้รับผิดชอบ

ประเภทความเสี่ยง	ประเด็นความเสี่ยงองค์กร ปีงบประมาณ พ.ศ. 2569	ผู้รับผิดชอบ (Risk Owner)
ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: *S*)	**RES:** มีความล่าช้าในการเชื่อมโยงขอรับข้อมูลเข้าแพลตฟอร์มข้อมูลขนาดใหญ่แห่งชาติ (D2) เนื่องจากยังไม่มีกฎหมาย/กฎระเบียบ ที่มอบหมายภารกิจโดยตรง จึงส่งผลให้ต้องมีกระบวนการด้านเอกสารหลายขั้นตอน	รองผู้อำนวยการกลุ่มงานส่งเสริมธุรกิจและองค์ความรู้
ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk : *C*)	**REC:** ความเสี่ยงจากความเข้าใจคลาดเคลื่อนในการตีความและการปฏิบัติตามกฎหมายด้านข้อมูล	
ความเสี่ยงด้านการปฏิบัติงาน (Operation Risk: *O*)	**REO:** ได้รับมอบหมายงานใหม่เพิ่มเติมอย่างกะทันหัน จนส่งผลกระทบต่อการดำเนินงานหลักของสถาบันฯ	รองผู้อำนวยการกลุ่มงานนโยบายยุทธศาสตร์และบริหาร
ความเสี่ยงด้านการเงิน (Financial Risk: *F*)	**REF:** ไม่มีงบประมาณสำหรับงานใหม่ที่ต้องการการขับเคลื่อน ในช่วงงบประมาณพลางก่อน จนส่งผลกระทบต่อเป้าหมายของสถาบันฯ	
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risk: *T*)	**RET:** ระบบสารสนเทศของสถาบันฯ ถูกโจมตีทางไซเบอร์จนส่งผลให้ข้อมูลรั่วไหล สูญหาย หรือระบบให้บริการหยุดชะงัก (Ransomware / Data Breach)	รองผู้อำนวยการกลุ่มงานบูรณาการและวิเคราะห์ข้อมูล

ประเภทความเสี่ยง: **ด้านกลยุทธ์ (Strategic Risk: S)**

ประเด็นความเสี่ยง: **RES: มีความล่าช้าในการเชื่อมโยงขอรับข้อมูลเข้าแพลตฟอร์มข้อมูลขนาดใหญ่แห่งชาติ (D2) เนื่องจาก ยังไม่มีกฎหมาย/กฎระเบียบที่มอบหมายภารกิจโดยตรง จึงส่งผลให้ต้องมีกระบวนการด้านเอกสารหลายขั้นตอน**

การประเมินความเสี่ยง:

เกณฑ์การประเมินโอกาสหรือความถี่ที่จะเกิด (Likelihood): โอกาสการเชื่อมโยงชุดข้อมูลเข้าสู่แพลตฟอร์ม D2

โอกาสหรือความถี่ที่จะเกิด (Likelihood)	
5	น้อยกว่า 60 ชุดข้อมูล
4	60 - 80 ชุดข้อมูล
3	81 - 100 ชุดข้อมูล
2	101 – 120 ชุดข้อมูล
1	มากกว่า 120 ชุดข้อมูล

เกณฑ์การประเมินความรุนแรงหรือผลกระทบ (Impact): การใช้ประโยชน์ด้านข้อมูลเชิงวิเคราะห์จากแพลตฟอร์ม D2 ในภาคส่วนต่าง ๆ (Sector)

ระดับความรุนแรงหรือผลกระทบ (Impact)	
5	ไม่ถูกนำไปใช้ประโยชน์ด้านการวิเคราะห์ข้อมูลเลย
4	ถูกนำไปใช้ประโยชน์ด้านการวิเคราะห์ข้อมูล 1 ภาคส่วน
3	ถูกนำไปใช้ประโยชน์ด้านการวิเคราะห์ข้อมูล 2 ภาคส่วน
2	ถูกนำไปใช้ประโยชน์ด้านการวิเคราะห์ข้อมูล 3 ภาคส่วน
1	ถูกนำไปใช้ประโยชน์ด้านการวิเคราะห์ข้อมูล มากกว่า 3 ภาคส่วน

โอกาสเกิด (Likelihood) \ ผลกระทบ (Impact)		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
		1	2	3	4	5
เกิดขึ้นสูงมาก	5	5	10	15	20	25
เกิดขึ้นสูง	4	4	8	12	16	20
เกิดขึ้นบ้าง	3	3	6	9	12	15
เกิดขึ้นน้อย	2	2	4	6	8	10
เกิดขึ้นยาก	1	1	2	3	4	5

Risk Score: 4 x 3 = 12

ระดับความเสี่ยง: ระดับสูง

สาเหตุ (Causes)	แนวทางการจัดการความเสี่ยง (Risk Mitigation Tasks)	แผนปฏิบัติการ/กิจกรรมย่อย (Action Plan)	Key Risk Indicator (KRI)
1. ยังไม่มีกฎหมาย/กฎระเบียบ ที่มอบหมายภารกิจให้ สขญ. โดยตรงในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐ	MP 1: ผลักดันให้เกิด กฎหมาย/กฎระเบียบ ที่มอบหมายภารกิจให้ สขญ. โดยตรงในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเพื่อเชื่อมโยงข้อมูลเข้าสู่แพลตฟอร์ม D2	1. <u>ระยะยาว</u> จัดทำ **ร่าง กฎหมายว่าด้วยการแบ่งบันข้อมูลดิจิทัล** และนำเข้าสู่กระบวนการตรากฎหมายในระดับพระราชบัญญัติ 2. <u>ระยะสั้น</u> เพื่อเป็นกลไกชั่วคราวในการกำหนดหลักเกณฑ์ วิธีการ และขั้นตอนการเชื่อมโยงข้อมูลของหน่วยงานของรัฐให้สามารถขับเคลื่อนแพลตฟอร์ม D2 ได้ตามเป้าหมายก่อน จัดทำ **ร่าง ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการแบ่งปันข้อมูลดิจิทัล** และเสนอต่อคณะรัฐมนตรี เพื่อพิจารณาให้มีผลบังคับใช้ในระยะสั้น 3. จัดทำ**เอกสารรองรับการบังคับใช้ของกฎหมาย** เช่น DSA DPA และ NDA, Data Gov Checklist เป็นต้น	ร่าง ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการแบ่งปันข้อมูลดิจิทัล **เข้าสู่กระบวนการพิจารณาของ ครม. ภายในเดือนมีนาคม 69**
2. หน่วยงานภายนอกบางหน่วยงานยังขาดความเข้าใจเกี่ยวกับแพลตฟอร์ม D2 และไม่ทราบถึงความแตกต่างระหว่างแพลตฟอร์ม D2 กับแพลตฟอร์มด้านข้อมูลของหน่วยงาน	MP 2: สร้างการรับรู้แพลตฟอร์ม D2 ต่อหน่วยงานภายนอก	1. รับ**เป็นที่ปรึกษา**ด้านการวิเคราะห์ข้อมูลให้แก่หน่วยงานภาพนอก อย่างน้อย 4 ครั้ง/ปี 2. จัดทำ**สื่อประชาสัมพันธ์**แพลต์ฟอร์ม D2 บนเว็บไซต์ BDI อย่างน้อย 2 ชิ้น/ปี	การเชื่อมโยงข้อมูลเข้าสู่กับแพลตฟอร์ม D2 เพิ่มขึ้น **น้อยกว่า 20 ชุดข้อมูล/ไตรมาส**

สาเหตุ (Causes)	แนวทางการจัดการความเสี่ยง (Risk Mitigation Tasks)	แผนปฏิบัติการ/กิจกรรมย่อย (Action Plan)	Key Risk Indicator (KRI)
อื่น เช่น Exchange Platform ของ สพร.		3. ร่วม**กิจกรรมเผยแพร่** ในรู้แบบประชุม สัมมนา และนิทรรศการ ด้านการบูรณาการข้อมูลเพื่อการวิเคราะห์ อย่างน้อย 2 ครั้ง/ปี	

ประเภทความเสี่ยง: **ด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk : C)**

ประเด็นความเสี่ยง: **REC: ความเสี่ยงจากความเข้าใจคลาดเคลื่อนในการตีความและการปฏิบัติตามกฎหมายด้านข้อมูล**

การประเมินความเสี่ยง:

เกณฑ์การประเมินโอกาสหรือความถี่ที่จะเกิด (Likelihood): โอกาสที่จะเกิดความเข้าใจคลาดเคลื่อนในการตีความหรือปฏิบัติตามกฎหมายด้านข้อมูล

โอกาสหรือความถี่ที่จะเกิด (Likelihood)	
5	ผู้ปฏิบัติงานส่วนใหญ่มีความเข้าใจคลาดเคลื่อนในข้อกฎหมายด้านข้อมูล เกิดความผิดพลาดบ่อยครั้งหรือมีประวัติการปฏิบัติผิดซ้ำ
4	มีการตีความข้อกฎหมายแตกต่างกันระหว่างฝ่ายหรือส่วนงาน ทำให้เกิดการปฏิบัติไม่ตรงกัน หรือผิดเงื่อนไขของกฎหมายด้านข้อมูลเป็นระยะ
3	ผู้ปฏิบัติงานบางส่วนยังไม่เข้าใจข้อกฎหมายอย่างครบถ้วน หรือมีความไม่แน่ใจในการตีความ ทำให้มีข้อผิดพลาดเป็นครั้งคราว
2	มีคู่มือ/แนวปฏิบัติ แต่มีผู้ปฏิบัติงานบางรายที่ยังไม่มั่นใจเกี่ยวกับข้อกฎหมายด้านข้อมูล อาจเกิดข้อผิดพลาดเล็กน้อยในบางโอกาส
1	ผู้ปฏิบัติงานมีความเข้าใจชัดเจน ได้รับการอบรมอย่างสม่ำเสมอ มีคู่มือ/แนวปฏิบัติรองรับ ทำให้เกิดการตีความคลาดเคลื่อนน้อยมาก

เกณฑ์การประเมินความรุนแรงหรือผลกระทบ (Impact): ระดับความเสียหายจากการตีความคลาดเคลื่อนหรือปฏิบัติตามกฎหมายด้านข้อมูลไม่ถูกต้อง

ระดับความรุนแรงหรือผลกระทบ (Impact)	
5	ถูกปรับ/รับโทษตามกฎหมายข้อมูลส่วนบุคคลหรือกฎหมายเฉพาะทาง, เกิดความเสียหายทางการเงินสูง, ถูกสอบสวนโดยหน่วยงานกำกับ, สร้างความเสียหายต่อชื่อเสียงองค์กรอย่างมีนัยสำคัญ
4	เกิดการหยุดชะงัก/ยกเลิกการดำเนินงานด้านข้อมูลของโครงการสำคัญ, ถูกตั้งข้อสังเกตจากหน่วยกำกับ, เกิดความเสี่ยงต่อความเชื่อมั่นของหน่วยงานคู่ความร่วมมือ
3	กระบวนการต้องชะลอ/ล่าช้าเพื่อทบทวนการตีความกฎหมายใหม่, ต้องแก้ไขเอกสารหรือขั้นตอนภายใน
2	เกิดข้อผิดพลาดเล็กน้อยในการปฏิบัติตามกฎหมาย ต้องปรับปรุง/แก้ไขการจัดทำเอกสาร หรือทบทวนขั้นตอนการทำงาน แต่ไม่กระทบโครงการโดยรวม
1	ส่งผลเฉพาะงานภายในเล็กน้อย เช่น ต้องตรวจทานเอกสารเพิ่ม ไม่มีผลต่อเวลา โครงการ หรือการกำกับดูแล

โอกาสเกิด (Likelihood) \ ผลกระทบ (Impact)		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
		1	2	3	4	5
เกิดขึ้นสูงมาก	5	5	10	15	20	25
เกิดขึ้นสูง	4	4	8	12	16	20
เกิดขึ้นบ้าง	3	3	6	9	12	15
เกิดขึ้นน้อย	2	2	4	6	8	10
เกิดขึ้นยาก	1	1	2	3	4	5

Risk Score: 3 x 3 = 9

ระดับความเสี่ยง: ระดับปานกลาง

สาเหตุ (Causes)	แนวทางการจัดการความเสี่ยง (Risk Mitigation Tasks)	แผนปฏิบัติการ/กิจกรรมย่อย (Action Plan)	Key Risk Indicator (KRI)
1. กฎหมายที่กำกับดูแลด้านข้อมูลมีที่เกี่ยวข้องกับข้อมูลหลายฉบับ และมีแนวทางปฏิบัติการกำกับดูแลที่แตกต่างกัน จึงเกิดปัญหาการตีความและเป็นอุปสรรคในการปฏิบัติตามได้ 2. ความรู้ความเข้าใจของผู้ปฏิบัติงานต่อกฎหมายที่เกี่ยวกับข้อมูลยังไม่เพียงพอ	MP 1: สร้างการรับรู้ด้านกฎหมายที่กำกับดูแลด้านข้อมูลให้กับผู้ปฏิบัติงาน	1. จัดทำ**ช่องทางสำหรับรวบรวมกฎหมาย**ที่เกี่ยวข้องกับข้อมูล และข้อพิจารณา/ข้อหารือที่เกี่ยวข้อง จัดทำคู่มือ/แนวปฏิบัติสำหรับผู้ปฏิบัติงานของสถาบัน 2. จัดทำ**สื่อประชาสัมพันธ์**ในรูปแบบที่เข้าถึงง่ายและเหมาะสมกับผู้ปฏิบัติงาน โดยสรุปสาระสำคัญของกฎหมายในรูปแบบ Infographic, Bullet point, คู่มือสรุป (Quick Guide) ทุกไตรมาส 3. จัด**กิจกรรมอบรมความรู้ด้านกฎหมายข้อมูล**แก่ผู้ปฏิบัติงาน อย่างน้อย 1 ครั้ง 4. มี**ช่องทางให้คำปรึกษาหารือข้อกฎหมาย** รวมถึงตรวจสอบเอกสารทางกฎหมายที่เกี่ยวข้องกับการใช้ข้อมูล 5. **หารือกับหน่วยงานที่กำกับดูแล**เมื่อเกิดการตีความข้อกฎหมายที่เกี่ยวข้องกับข้อมูลไม่ตรงกัน	เหตุการณ์ข้อผิดพลาดด้านการตีความหรือการปฏิบัติตามกฎหมายด้านข้อมูลที่ตรวจพบ **มากกว่า 2 ครั้งต่อไตรมาส**

ประเภทความเสี่ยง: **ด้านการปฏิบัติงาน (Operation Risk: O)**
ประเด็นความเสี่ยง: **REO: ได้รับมอบหมายงานใหม่เพิ่มเติมอย่างกะทันหัน จนส่งผลกระทบต่อการดำเนินงานหลักของสถาบันฯ**

การประเมินความเสี่ยง:

เกณฑ์การประเมินโอกาสหรือความถี่ที่จะเกิด (Likelihood): โอกาสงานใหม่เพิ่มเติมอย่างกะทันหัน

โอกาสหรือความถี่ที่จะเกิด (Likelihood)	
5	ได้รับมอบหมายมากกว่า 10 ครั้งต่อปี
4	ได้รับมอบหมาย 7-10 ครั้งต่อปี
3	ได้รับมอบหมาย 4-6 ครั้งต่อปี
2	ได้รับมอบหมาย 1-3 ครั้งต่อปี
1	ได้รับมอบหมาย 1 ครั้งต่อปี (ไม่ได้เป็นผู้รับผิดชอบหลัก)

เกณฑ์การประเมินความรุนแรงหรือผลกระทบ (Impact): การส่งมอบตัวชี้วัดสถาบันฯ

ระดับความรุนแรงหรือผลกระทบ (Impact)	
5	สามารถดำเนินการส่งมอบตัวชี้วัดตามที่สถาบันกำหนดน้อยกว่าร้อยละ 50
4	สามารถดำเนินการส่งมอบตัวชี้วัดตามที่สถาบันกำหนดได้ในช่วงร้อยละ 50-74
3	สามารถดำเนินการส่งมอบตัวชี้วัดตามที่สถาบันกำหนดได้ในช่วงร้อยละ 75-99
2	สามารถดำเนินการส่งมอบตัวชี้วัดตามที่สถาบันกำหนดได้ร้อยละ 100
1	สามารถดำเนินการส่งมอบตัวชี้วัดได้ตามเกณฑ์ที่ กพร. กำหนด

โอกาสเกิด (Likelihood) \ ผลกระทบ (Impact)		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
		1	2	3	4	5
เกิดขึ้นสูงมาก	5	5	10	15	20	25
เกิดขึ้นสูง	4	4	8	12	16	20
เกิดขึ้นบ้าง	3	3	6	9	12	15
เกิดขึ้นน้อย	2	2	4	6	8	10
เกิดขึ้นยาก	1	1	2	3	4	5

Risk Score: 4 x 3 = 12
ระดับความเสี่ยง: ระดับสูง

สาเหตุ (Causes)	แนวทางการจัดการความเสี่ยง (Risk Mitigation Tasks)	แผนปฏิบัติการ/กิจกรรมย่อย (Action Plan)	Key Risk Indicator (KRI)
สขญ. ได้รับมอบหมายภาระงานระดับนโยบายเพิ่มเติมอย่างกะทันหัน โดยมีจำนวนบุคลากรที่จำกัด	MP1: บริหารจัดการกำลังคนให้สอดคล้องกับภาระงาน	1. จัดทำแผนอัตรากำลังคน และระบบ Dashboard ด้านบุคลากร เพื่อให้การบริหารจัดการเป็นไปอย่างมีประสิทธิภาพ 2. มีการกระบวนจ้างบุคลากรชั่วคราว แบบ Fast-track โดยใช้ระยะเวลาดำเนินการจัดจ้างไม่เกิน 30 วัน 3. มีการติดตามการปฏิบัติงานของบุคลากรในระบบ Jira ทุก 2 สัปดาห์ ในกลุ่มที่ตอบโจทย์พันธกิจหลัก	งานที่ได้รับคำสั่งระดับนโยบายเร่งด่วน **มากกว่า 2 ครั้งต่อไตรมาส**
	MP2: พัฒนากำลังคนให้พร้อมปรับตัวตามสถานการณ์ ยืดหยุ่นได้ เมื่อมีสถานการณ์เร่งด่วน โดยไม่ส่งผลต่อการส่งมอบตัวชี้วัดสถาบันฯ	1. การประเมินความพร้อมในการรับมือกับสถานการณ์เร่งด่วน (Pre-test) ให้แก่กลุ่มบุคลากรที่มีศักยภาพสูง (Change Agent) เพื่อออกแบบการอบรม และจัดการอบรมเชิงปฏิบัติการ ในการจัดทำแผนปฏิบัติการ (BCP) 2. ดำเนินการประเมินความพร้อมในการรับมือกับสถานการณ์เร่งด่วน (Post-test) ภายหลังจากการอบรม	ผลการประเมินความพร้อมในการรับมือกับสถานการณ์เร่งด่วน **น้อยกว่า 65 คะแนน**

ประเภทความเสี่ยง: **ด้านการเงิน (Financial Risk: F)**

ประเด็นความเสี่ยง: **REF: ไม่มีงบประมาณสำหรับงานใหม่ที่ต้องการการขับเคลื่อน ในช่วงงบประมาณพลางก่อน จนส่งผลกระทบต่อเป้าหมายของสถาบันฯ**

การประเมินความเสี่ยง:

เกณฑ์การประเมินโอกาสหรือความถี่ที่จะเกิด (Likelihood): โอกาสเงินคงเหลือจากที่ได้รับจัดสรรปี 2569 เพื่อเก็บเป็นเงินสะสมสำหรับงานใหม่ในปีถัดไป

โอกาสหรือความถี่ที่จะเกิด (Likelihood)	
5	ไม่มีเงินคงเหลือ
4	มีเงินคงเหลือ น้อยกว่าหรือเท่ากับ 5%
3	มีเงินคงเหลือ มากกว่า 5 % แต่ไม่เกิน 10%
2	มีเงินคงเหลือ มากกว่า 10 % แต่ไม่เกิน 15%
1	มีเงินคงเหลือ มากกว่า 15%

เกณฑ์การประเมินความรุนแรงหรือผลกระทบ (Impact): ผลการดำเนินงานโครงการใหม่ตามเป้าหมาย

ระดับความรุนแรงหรือผลกระทบ (Impact)	
5	ไม่สามารถดำเนินงานโครงการใหม่ได้เลย
4	ดำเนินการโครงการใหม่ได้บางส่วน โดยใช้บุคลากรภายในของสถาบันดำเนินการเอง โดยไม่มีงบประมาณมาดำเนินการ ล่าช้ากว่าแผน
3	ดำเนินการโครงการใหม่ได้บางส่วน โดยใช้งบประมาณจากเงินสะสมที่มีอยู่อย่างจำกัด ล่าช้ากว่าแผน
2	ดำเนินการโครงการใหม่ได้บางส่วน โดยใช้งบประมาณจากเงินสะสมที่มีอยู่อย่างจำกัด แต่สามารถเร่งดำเนินการได้ทันได้ตามแผน
1	ดำเนินการโครงการใหม่ได้ตามแผน โดยใช้เงินสะสมที่มีดำเนินการได้ตามแผน

โอกาสเกิด (Likelihood) \ ผลกระทบ (Impact)		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
		1	2	3	4	5
เกิดขึ้นสูงมาก	5	5	10	15	20	25
เกิดขึ้นสูง	4	4	8	12	16	20
เกิดขึ้นบ้าง	3	3	6	9	12	15
เกิดขึ้นน้อย	2	2	4	6	8	10
เกิดขึ้นยาก	1	1	2	3	4	5

Risk Score: 3 x 3 = 9

ระดับความเสี่ยง: ระดับปานกลาง

สาเหตุ (Causes)	แนวทางการจัดการความเสี่ยง (Risk Mitigation Tasks)	แผนปฏิบัติการ/กิจกรรมย่อย (Action Plan)	Key Risk Indicator (KRI)
ความไม่แน่นอนทางการเมือง มีแนวโน้มที่จะเลือกตั้งรัฐบาลใหม่ในช่วงปีงบประมาณ พ.ศ. 2569 ส่งผลให้การจัดสรรงบประมาณประจำปีงบประมาณ พ.ศ. 2570 มีความล่าช้า ดังนั้น เพื่อให้หน่วยรับงบประมาณสามารถดำเนินการได้บางส่วน สำนักงบประมาณ จึงจัดสรรเป็นงบพลางก่อนมาให้ก่อน ซึ่งจะไม่ครอบคลุมงานใหม่ในการปฏิบัติตามได้	MP 1: บริหารการใช้จ่ายงบประมาณอย่างมีประสิทธิภาพ เพื่อให้มีเงินคงเหลือสะสมสำหรับโครงการใหม่ในช่วงงบประมาณพลางก่อน	1. **กำหนดนโยบายการใช้จ่ายงบประมาณ** อย่างมีประสิทธิภาพ และเป็นไปตามแผน 2. หัวหน้าโครงการหรือผู้อำนวยการฝ่าย **วางแผนการใช้จ่ายงบประมาณตามนโยบาย** 3. **ติดตามการใช้จ่ายผลเทียบแผน ผ่านระบบ Dashboard** หากไม่เป็นไปตามแผน ให้ หัวหน้าโครงการหรือผู้อำนวยการฝ่าย ดำเนินการปรับแผนให้สอดคล้องกับการใช้จ่ายจริง 4. **ติดตามผลการดำเนินงานทุกไตรมาส** ผ่านการประชุม Management	การใช้จ่ายงบประมาณ **เกินแผนมากกว่า 100%**

ประเภทความเสี่ยง: **ด้านเทคโนโลยีสารสนเทศ (Technology Risk: T)**

ประเด็นความเสี่ยง: **RET: ระบบสารสนเทศของสถาบันฯ ถูกโจมตีทางไซเบอร์ จนส่งผลให้ข้อมูลรั่วไหล สูญหาย หรือระบบให้บริการหยุดชะงัก (Ransomware / Data Breach)**

การประเมินความเสี่ยง:

เกณฑ์การประเมินโอกาสหรือความถี่ที่จะเกิด (Likelihood): เกิดเหตุการณ์ถูกโจมตีทางไซเบอร์ จนส่งผลกระทบต่อการทำงาน (IRP, DRP และ BCP)

โอกาสหรือความถี่ที่จะเกิด (Likelihood)	
5	เกิดขึ้น เท่ากับหรือมากกว่า 5 ครั้ง ในรอบ 1 ปี ที่ส่งผลกระทบต่อการดำเนินงานของสถาบัน
4	เกิดขึ้น 4 ครั้ง ในรอบ 1 ปี ที่ส่งผลกระทบต่อการดำเนินงานของสถาบัน
3	เกิดขึ้น 3 ครั้ง ในรอบ 1 ปี ที่ส่งผลกระทบต่อการดำเนินงานของสถาบัน
2	เกิดขึ้น 2 ครั้ง ในรอบ 1 ปี ที่ส่งผลกระทบต่อการดำเนินงานของสถาบัน
1	เกิดขึ้น 1 ครั้ง หรือไม่เกิดขึ้นเลย ในรอบ 1 ปี ที่ส่งผลกระทบต่อการดำเนินงานของสถาบัน

เกณฑ์การประเมินความรุนแรงหรือผลกระทบ (Impact): ระบบการให้บริการ, ความมั่นคงปลอดภัย, ข้อมูลรั่วไหล

ระดับความรุนแรงหรือผลกระทบ (Impact)	
5	ถูกโจมตีทางไซเบอร์จนเกิดความเสียหายต่อสถาบันฯ ทั้งในด้านกฎหมาย ข้อมูลสำคัญ และการเงิน
4	ถูกโจมตีทางไซเบอร์จนเกิดความเสียหายต่อ ระบบหลักในการให้บริการ และต้องปรับแผน/นโยบาย
3	ถูกโจมตีทางไซเบอร์จนเกิดความเสียหายต่อ ระบบหลักในการให้บริการ ซึ่งแผนปฏิบัติการสามารถรองรับ
2	ถูกโจมตีทางไซเบอร์จนเกิดความเสียหายต่อ ระบบหลักบางส่วน ซึ่งแผนปฏิบัติการสามารถรองรับ
1	ถูกโจมตีทางไซเบอร์ สามารถแก้ไขได้ทันที โดยไม่ส่งผลต่อการดำเนินงานของสถาบันฯ

โอกาสเกิด (Likelihood) \ ผลกระทบ (Impact)		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
		1	2	3	4	5
เกิดขึ้นสูงมาก	5	5	10	15	20	25
เกิดขึ้นสูง	4	4	8	12	16	20
เกิดขึ้นบ้าง	3	3	6	9	12	15
เกิดขึ้นน้อย	2	2	4	6	8	10
เกิดขึ้นยาก	1	1	2	3	4	5

Risk Score: 3 x 4 = 12

ระดับความเสี่ยง: ระดับสูง

สาเหตุ (Causes)	แนวทางการจัดการความเสี่ยง (Risk Mitigation Tasks)	แผนปฏิบัติการ/กิจกรรมย่อย (Action Plan)	Key Risk Indicator (KRI)
1. มีช่องโหว่ทางเทคนิคในระบบสารสนเทศเกิดขึ้นใหม่เสมอ 2. คู่มือการจัดการและปฏิบัติงานยังไม่ครอบคลุมทุกกระบวนการที่สำคัญ ได้แก่ การตรวจหาช่องโหว่, DRP และ BCP (อยู่ระหว่างดำเนินการ) 3. บุคลากรขาดความรู้และทักษะด้าน Cyber Hygiene 4. ระบบเฝ้าระวังและติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศตลอด 24 ชั่วโมง (24/7) ยังไม่ครอบคลุมการทำงานทุกฟังก์ชัน 5. อยู่ระหว่างการศึกษาการใช้อุปกรณ์และเครื่องมือด้านการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพและคุ้มค่า	MP 1: ปฏิบัติตาม พรบ. ไซเบอร์ฯ และมาตรฐาน NIST Cyber Security Framework	1. **ตรวจสอบช่องโหว่ (Vulnerability Assessment)** และ**ทดสอบการเจาะระบบ (Penetration Testing)** อย่างน้อย 1 ครั้ง/ปี พร้อมดำเนินการปรับแก้ไขช่องโหว่ให้อยู่ในเกณฑ์ที่ยอมรับได้ 2. จัดทำ**คู่มือการจัดการและปฏิบัติงาน**ให้ครอบคลุมการตรวจหาช่องโหว่, DRP และ BCP ให้แล้วเสร็จภายในไตรมาส 2 และการ**ซักซ้อมแผน IRP DRP และ BCP** ในช่วงไตรมาส 4 3. จัด**อบรมให้ความรู้**ด้านความมั่นคงปลอดภัยทางไซเบอร์ อย่างน้อย 2 ครั้ง/ปี 4. ศึกษาและพัฒนา**ระบบเฝ้าระวังและติดตามเหตุการณ์**ด้านความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมทุกฟังก์ชัน (SIEM และ SOC) เพื่อนำมาปรับใช้ต่อไป 5. ใช้**อุปกรณ์ เครื่องมือ และระบบ** ได้แก่ DLP, Change Management system, Zero Trust VPN และ EDR/XDR เพื่อการรักษาความมั่นคงปลอดภัย	เกิดเหตุการณ์ถูกโจมตีทางไซเบอร์**จนกระทบต่อการทำงาน (IRP) 1 ครั้ง**

เอกสารอ้างอิง

หมวดที่ 1 : กฎหมาย / ระเบียบ / หนังสือสั่งการ

(1) พระราชกฤษฎีกาจัดตั้งสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) พ.ศ. 2566. ราชกิจจานุเบกษา, เล่ม 140 ตอนที่ 34 ก.

(2) ระเบียบกระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์การควบคุมภายใน พ.ศ. 2561. กรุงเทพฯ: กระทรวงการคลัง.

(3) ระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ. 2544. กรุงเทพฯ: สำนักงานการตรวจเงินแผ่นดิน.

(4) ร่าง แผนยุทธศาสตร์การขับเคลื่อนการใช้ประโยชน์จากข้อมูลขนาดใหญ่ พ.ศ. 2568–2570. กรุงเทพฯ: สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน).

(5) หนังสือกระทรวงการคลัง ที่ กค 0409.4/ว23 ลงวันที่ 19 มีนาคม 2562 เรื่อง มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ. กรุงเทพฯ: กระทรวงการคลัง.หนังสือกระทรวงการคลัง ที่ กค 0409.3/ว36 ลงวันที่ 3 กุมภาพันธ์ 2564 เรื่อง การบริหารจัดการความเสี่ยงของหน่วยงานของรัฐ. กรุงเทพฯ: กระทรวงการคลัง.

หมวดที่ 2 : มาตรฐานสากล / กรอบการบริหารความเสี่ยง

(6) COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017). USA: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

(7) COSO Internal Control – Integrated Framework (2013). USA: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

(8) Global Risks Report 2025. Geneva: World Economic Forum.

หมวดที่ 3 : เอกสารภายใน สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

(9) นโยบายการบริหารความเสี่ยง (SP-007-RSKM Version 2.0). กรุงเทพฯ: สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน).

(10) ผลการดำเนินงานของ สขญ. ปีงบประมาณ พ.ศ. 2568. กรุงเทพฯ: สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน).

(11) แผนกลยุทธ์การบริหารและพัฒนาบุคลากร พ.ศ. 2567–2570. กรุงเทพฯ: สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน).

(12) แผนบริหารความเสี่ยงองค์กร ปีงบประมาณ พ.ศ. 2568. กรุงเทพฯ: สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)