สภาองค์กรของผู้บริโภค
Thailand Consumers Council

คู่มือบริหารความเสี่ยง ปีงบประมาณ พ.ศ. 2568

บทนำ

ในโลกที่เปลี่ยนแปลงอย่างรวดเร็วและไม่แน่นอน การบริหารความเสี่ยงได้กลายเป็นเครื่องมือที่สำคัญต่อความสำเร็จและการเติบโตขององค์กร การเข้าใจและจัดการกับความเสี่ยงในทุกระดับขององค์กรเป็นสิ่งจำเป็นเพื่อให้สามารถบรรลุเป้าหมายเชิงกลยุทธ์ได้อย่างยั่งยืน และลดผลกระทบจากความไม่แน่นอนที่อาจเกิดขึ้นทั้งในด้านการเงิน การปฏิบัติงาน และเทคโนโลยีได้

คู่มือการบริหารความเสี่ยงฉบับนี้ จัดทำขึ้นโดยยึดหลักการบริหารความเสี่ยงแบบบูรณาการ (Enterprise Risk Management: ERM) ตามกรอบการทำงานที่กำหนดโดย COSO (The Committee of Sponsoring Organizations of the Treadway Commission) ปี 2017 โดยมีจุดประสงค์เพื่อให้องค์กรมีเครื่องมือในการระบุ ประเมิน จัดการ และติดตามความเสี่ยงอย่างเป็นระบบ ครอบคลุมทุกมิติและเชื่อมโยงกับเป้าหมายเชิงกลยุทธ์ และมุ่งเน้นการสร้างคุณค่าผ่านการจัดการความเสี่ยงอย่างมีประสิทธิภาพและโปร่งใส

ทั้งนี้คู่มือฉบับนี้เป็นแนวทางที่มีประโยชน์ต่อผู้บริหารและบุคลากรทุกระดับในการทำความเข้าใจถึงกระบวนการบริหารความเสี่ยงและนำไปปรับใช้ในองค์กรอย่างเหมาะสม เพื่อสนับสนุนการตัดสินใจที่ดีขึ้น สร้างความยั่งยืนให้กับองค์กร และเพิ่มมูลค่าให้แก่ผู้มีส่วนได้เสียทุกฝ่าย

ฝ่ายเลขาธิการ
สำนักงานสภาองค์กรของผู้บริโภค
25 กันยายน 2567

สารบัญ

หลักการและเหตุผล

ยุทธศาสตร์การพัฒนาระบบการบริหารองค์กรของรัฐได้กำหนดให้มีการปรับเปลี่ยนกระบวนการและวิธีการทำงาน เพื่อยกระดับขีดความสามารถและมาตรฐานการทำงานของหน่วยงาน ให้อยู่ในระดับสูงเทียบเท่ามาตรฐานสากล โดยยึดหลักการปฏิบัติตามพระราชกฤษฎีกา ว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546 ซึ่งประกอบไปด้วยเป้าหมายสำคัญคือ เพื่อประโยชน์สุขของประชาชน เพื่อผลสัมฤทธิ์ต่อภารกิจของรัฐ มีประสิทธิภาพและเกิดความคุ้มค่าในภารกิจของรัฐ ลดขั้นตอนการปฏิบัติงานที่เกินความจำเป็น รวมทั้งมีการประเมินผลการปฏิบัติงานอย่างสม่ำเสมอ

สำนักงานสภาองค์กรของผู้บริโภคได้ดำเนินการบริหารความเสี่ยง ตามกรอบ COSO ERM 2017 เพื่อบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินการต่างๆ โดยคำนึงถึงการบรรลุวัตถุประสงค์และเป้าหมายตามภารกิจหลักของ พระราชบัญญัติการจัดตั้งสภาองค์กรของผู้บริโภค พ.ศ. 2562 เป็นสำคัญ ทั้งนี้เพื่อช่วยให้สำนักงานสามารถระบุ ป้องกัน และตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการดำเนินงานได้อย่างเป็นระบบ และส่งเสริมการตัดสินใจเชิงกลยุทธ์ที่มีข้อมูลครบถ้วน มุ่งเน้นการสร้างมูลค่าและความยั่งยืนในระยะยาว โดยเฉพาะในยุคที่การเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีและปัจจัยภายนอกที่ไม่สามารถควบคุมได้

วัตถุประสงค์ของการบริหารความเสี่ยง (Risk Management Objectives) คือการช่วยให้สำนักงานสามารถรับมือกับความไม่แน่นอนและจัดการความเสี่ยงต่าง ๆ ที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์เชิงกลยุทธ์และการดำเนินงานหลักของสำนักงาน โดยมีวัตถุประสงค์หลักดังนี้:

1. **ปกป้องและรักษาสินทรัพย์ของสำนักงาน**
   การบริหารความเสี่ยงช่วยปกป้องสินทรัพย์ที่มีมูลค่าทางการเงิน ทรัพยากรบุคคล ทรัพยากรทางกายภาพและทรัพย์สินทางปัญญา ซึ่งสามารถเกิดความเสียหายได้จากความเสี่ยงที่องค์กรเผชิญ เช่น การโจมตีทางไซเบอร์ อุบัติเหตุ หรือการถูกฟ้องร้องทางกฎหมาย
2. **ส่งเสริมการตัดสินใจเชิงกลยุทธ์ที่ดีขึ้น**
   การบริหารความเสี่ยงให้ข้อมูลที่สำคัญเกี่ยวกับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น ทำให้ผู้บริหารสามารถตัดสินใจที่มีความรอบคอบขึ้นและลดโอกาสในการตัดสินใจที่อาจก่อให้เกิดความเสี่ยงเกินขีดความสามารถในการรับได้
3. **เพิ่มความมั่นคงในการดำเนินงานตามพันธกิจ**
   การระบุและจัดการความเสี่ยงที่มีผลกระทบต่อกระบวนการดำเนินงาน ช่วยให้การดำเนินงานของสำนักงานมีความมั่นคงและต่อเนื่อง ลดโอกาสการหยุดชะงักและความเสียหายจากปัจจัยเสี่ยงต่างๆ

4. **ป้องกันการสูญเสียและลดความเสียหาย**
   การบริหารความเสี่ยงมีเป้าหมายในการลดความเสี่ยงที่จะเกิดความเสียหาย เช่น ความสูญเสียทางการเงิน การสูญเสียข้อมูล การสูญเสียทรัพย์สิน หรือความเสียหายต่อชื่อเสียงสำนักงาน
5. **เพิ่มประสิทธิภาพในการใช้ทรัพยากร**
   การบริหารความเสี่ยงช่วยให้องค์กรสามารถจัดสรรทรัพยากรไปยังส่วนที่มีความเสี่ยงสูงหรือต้องการการป้องกันเป็นพิเศษ ช่วยลดความสูญเปล่าของทรัพยากรและปรับปรุงการดำเนินงาน
6. **สร้างความน่าเชื่อถือและความไว้วางใจต่อสาธารณชน**
   การบริหารความเสี่ยงอย่างเป็นระบบช่วยสร้างความเชื่อมั่นให้กับประชาชน และผู้มีส่วนได้เสียอื่น ๆ ว่าสำนักงานสามารถบริหารจัดการความเสี่ยงได้ดีและมีความมั่นคงในการดำเนินงาน
7. **สอดคล้องกับกฎระเบียบและกฎหมาย**
   การบริหารความเสี่ยงช่วยให้สำนักงานปฏิบัติตามกฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง ลดความเสี่ยงในการถูกปรับหรือถูกฟ้องร้อง
8. **สนับสนุนการบรรลุเป้าหมายสำนักงาน**
   การบริหารความเสี่ยงช่วยให้การดำเนินงานเป็นไปตามเป้าหมายที่ตั้งไว้ ลดโอกาสในการเจออุปสรรคที่อาจขัดขวางการบรรลุวัตถุประสงค์เชิงกลยุทธ์

ขอบเขตการบริหารความเสี่ยงของสำนักงาน : การบริหารความเสี่ยงตามแนวทางในคู่มือการบริหารความเสี่ยงฉบับนี้ ใช้เฉพาะการบริหารความเสี่ยงของสำนักงานสภาองค์กรของผู้บริโภคเท่านั้น โดยยึดหลักการแนวทางการบริหารความเสี่ยงตามหลัก COSO ERM (Enterprise Risk Management) ปี 2017

ผู้รับผิดชอบการบริหารความเสี่ยงตามคู่มือฯ ฉบับนี้ :

1) เลขาธิการสำนักงานสภาองค์กรของผู้บริโภค มีหน้าที่รับผิดชอบเป็นผู้บริหารสำนักงานลำดับสูงสุดในการบริหารความเสี่ยงของสำนักงานสภาองค์กรของผู้บริโภค โดยแต่งตั้งคณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในของสำนักงานสภาองค์กรของผู้บริโภค เป็นผู้รับรับผิดชอบการบริหารความเสี่ยงของสำนักงาน ตามคำสั่งของสำนักงานที่แต่งตั้งไว้
2) คณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในของสำนักงานสภาองค์กรของผู้บริโภค เป็นผู้รับรับผิดชอบการบริหารความเสี่ยงของสำนักงาน ตามคำสั่งของสำนักงานที่แต่งตั้งไว้

3) คณะอนุกรรมการบริหาร และคณะกรรมการนโยบายสภาองค์กรของผู้บริโภค (กนย.) มีหน้าที่กำกับดูแลให้การบริหารความเสี่ยงของสำนักงานเป็นไปตามแนวทางการบริหารความเสี่ยงที่สำนักงานกำหนด และเป็นไปอย่างมีประสิทธิผล และประสิทธิภาพ
4) หน่วยตรวจสอบภายในและคณะอนุกรรมการตรวจสอบ ทำหน้าที่ตรวจสอบวิธีการ/ขั้นตอนการบริหารความเสี่ยง แผนบริหารความเสี่ยงประจำปี รายงานความคืบหน้าแผนบริหารความเสี่ยงรายไตรมาส และผลการบริหารความเสี่ยงประจำปี เพื่อตรวจสอบความถูกต้องตามแนวทางปฏิบัติการบริหารความเสี่ยงตามมาตรฐาน และประสิทธิผล ประสิทธิภาพการบริหารความเสี่ยง
5) ฝ่ายต่าง ๆ ที่รับผิดชอบการจัดทำและจัดการตามแผนการบริหารความเสี่ยง และการรายงานความคืบหน้าการจัดการความเสี่ยงรายไตรมาสและผลการบริหารความเสี่ยงประจำปี (Risk Owner)

ความหมายของความเสี่ยง

ตามหลัก COSO ERM (Enterprise Risk Management) ปี 2017 ความเสี่ยง (Risk) หมายถึง เหตุการณ์/ความไม่แน่นอนที่อาจมีผลกระทบ (ทั้งในทางบวกหรือทางลบ) ต่อการบรรลุวัตถุประสงค์ขององค์กร ความเสี่ยงนั้นสามารถเกิดขึ้นได้จากหลายปัจจัย รวมถึงปัจจัยภายในและภายนอกองค์กร ซึ่งอาจส่งผลกระทบต่อการดำเนินงานเชิงกลยุทธ์ การเงิน การปฏิบัติงาน เทคโนโลยีและการปฏิบัติตามกฎหมายหรือข้อบังคับต่างๆ

ภายใต้ COSO ERM ความเสี่ยงไม่ได้ถูกมองเฉพาะในแง่ลบ แต่ยังครอบคลุมถึงความเสี่ยงที่เปิดโอกาสให้กับองค์กรเช่นกัน ดังนั้น การบริหารความเสี่ยงจึงไม่ได้มุ่งเพียงแค่การลดหรือป้องกันความเสียหาย แต่ยังมุ่งใช้ความเสี่ยงเป็นเครื่องมือในการสร้างโอกาสและมูลค่าเพิ่มให้กับองค์กร ซึ่งรวมถึงการปรับใช้กลยุทธ์ที่สามารถรับมือกับความเสี่ยงและใช้ประโยชน์จากโอกาสที่เกิดขึ้น

ความเสี่ยงแต่ละด้าน

ความเสี่ยงแต่ละด้านมีความสำคัญแตกต่างกันขึ้นอยู่กับลักษณะขององค์กรและสภาพแวดล้อมที่องค์กรดำเนินงาน การจำแนกความเสี่ยงจะช่วยให้องค์กรสามารถบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ ลดความสูญเสีย และเพิ่มโอกาสในการสร้างมูลค่าให้กับองค์กรได้อย่างครอบคลุม ทั้งนี้สำนักงานได้จำแนกความเสี่ยงออกดังนี้

1. ความเสี่ยงเชิงกลยุทธ์ (Strategic Risk)

ความหมาย: ความเสี่ยงที่เกิดจากการกำหนดหรือการดำเนินกลยุทธ์ที่ไม่สอดคล้องกับเป้าหมายระยะยาวขององค์กร หรือการที่องค์กรไม่สามารถตอบสนองต่อการเปลี่ยนแปลงในสภาพแวดล้อมภายนอกได้อย่างมีประสิทธิภาพ

2. ความเสี่ยงด้านการดำเนินงาน (Operational Risk)

ความหมาย: ความเสี่ยงที่เกิดจากกระบวนการภายใน การจัดการทรัพยากร บุคลากร หรือเทคโนโลยีที่ใช้ในการดำเนินงาน ซึ่งอาจทำให้กระบวนการทำงานไม่เป็นไปตามที่วางแผนไว้

3. ความเสี่ยงด้านการเงิน (Financial Risk)

ความหมาย: ความเสี่ยงที่เกิดจากปัจจัยทางการเงินหรือสถานการณ์ทางการเงิน หรือการดำเนินการธุรกรรมทางการเงินที่อาจส่งผลกระทบต่อการดำเนินงานหรือความสามารถในการดำเนินกิจกรรมขององค์กร

4. ความเสี่ยงด้านกฎหมายและการปฏิบัติตาม (Compliance and Legal Risk)

ความหมาย: ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย กฎระเบียบ ซึ่งอาจส่งผลให้เกิดการฟ้องร้อง การถูกปรับ หรือการสูญเสียชื่อเสียง หรือสอดคล้องความเสี่ยงที่มีกฎระเบียบ ที่ไม่สอดคล้องต่อการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กร

5. ความเสี่ยงด้านเทคโนโลยี (Technology Risk)

ความหมาย: ความเสี่ยงที่เกิดจากการพึ่งพาเทคโนโลยีในกระบวนการดำเนินงาน ซึ่งหากเทคโนโลยีล้มเหลวหรือไม่ปลอดภัย อาจส่งผลต่อการดำเนินงานหรือการรักษาข้อมูล

ความหมายการบริหารความเสี่ยง

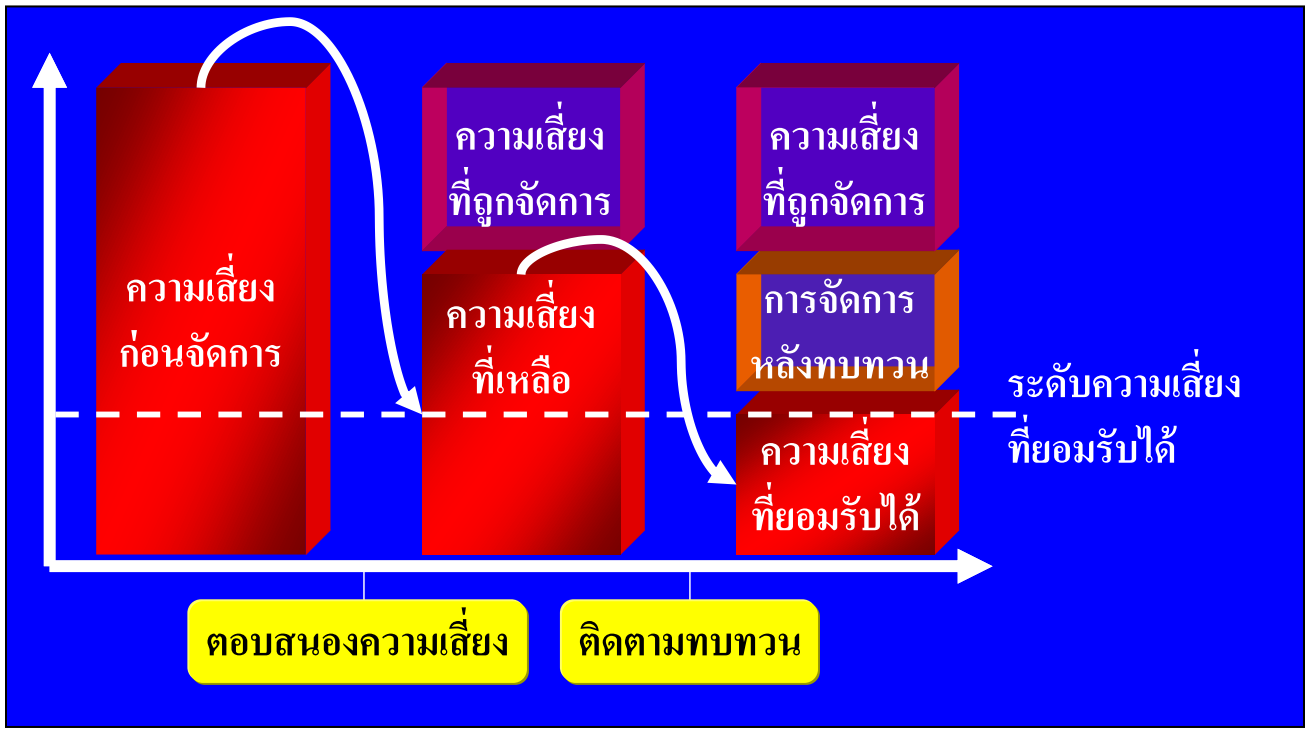
การบริหารความเสี่ยงตามหลัก COSO ERM 2017 (Enterprise Risk Management) เป็นกระบวนการบูรณาการความเสี่ยงเข้ากับทุกระดับและทุกส่วนขององค์กร โดยมีเป้าหมายหลักในการช่วยให้องค์กรสามารถระบุ ประเมิน จัดการ และติดตามความเสี่ยง เพื่อให้สามารถบรรลุวัตถุประสงค์และเป้าหมายเชิงกลยุทธ์ได้อย่างมีประสิทธิภาพ การบริหารความเสี่ยงนี้ไม่ได้จำกัดเฉพาะการป้องกันความเสียหายหรือการลดความสูญเสียเท่านั้น แต่ยังมุ่งเน้นการใช้ความเสี่ยงในการสร้างโอกาสและเพิ่มมูลค่าให้กับองค์กรอีกด้วย

ความเสี่ยงที่รับได้ (Risk Appetite)

หมายถึง ระดับของความเสี่ยงที่คณะกรรมการหรือผู้บริหารกำหนดไว้ในการดำเนินการเพื่อให้บรรลุวัตถุประสงค์หรือนโยบายขององค์กร โดยคณะกรรมการหรือผู้บริหารควรกำหนดยุทธศาสตร์ขององค์กร ที่สอดคล้องกับความเสี่ยงที่ยอมรับได้ โดยมากความเสี่ยงที่ยอมรับได้ (Risk Appetite) จะเป็นตัวเดียวกับเป้าหมายตามวัตถุประสงค์ขององค์กรได้ เช่น การกำหนดเป้าหมายด้านกำไร การกำหนดเป้าหมายด้านเรื่องข้อร้องทุกข์ เป็นต้น

ความเสี่ยงที่เหลืออยู่ (Residual Risk)

หมายถึง ความเสี่ยงที่เหลืออยู่หลังจากที่ดำเนินการจัดการกับความเสี่ยงไปแล้ว พบว่าระดับความเสี่ยงอาจลดลง แต่ยังไม่อยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk Acceptance) ดังรูป



ตัวชี้วัด (Indicator)

ความหมายของตัวชี้วัดในระบบบริหารความเสี่ยง

Key Performance Indicators (KPIs) – Monitor changes in business performance in relation to specific business objective. (หมายถึงตัวชี้วัดที่ใช้ติดตามการเปลี่ยนแปลงความสามารถการดำเนินงานให้บรรลุตามวัตถุประสงค์ของงานที่ตั้งไว้)

Key Risk Indicators (KRIs/KPIs Risk) – Relate to a specific risk and demonstrate a change in likelihood or impact of the risk event occurring. (หมายถึงตัวชี้วัดที่แสดงให้เห็นถึงการเปลี่ยนแปลงผลกระทบหรือโอกาสการเกิดของความเสี่ยง) ตัวชี้วัดความเสี่ยง เป็นเครื่องมือที่สำคัญในการติดตามความเสี่ยง โดยเปรียบเสมือนสัญญาณเตือนล่วงหน้า (Early Warning Signal) เพื่อให้องค์การตระหนักว่าความเสี่ยงที่ได้ระบุขึ้นมีความเปลี่ยนแปลงไปในทิศทางใด เพื่อให้องค์การสามารถเฝ้าระวังระดับโอกาสที่จะเกิดขึ้น หรือผลกระทบของความเสี่ยง และมีการจัดการได้อย่างทันเวลา

Key Control Indicators (KCIs) – Demonstrate a change in a specific control's effectiveness. (หมายถึงตัวชี้วัดที่แสดงให้เห็นถึงการเปลี่ยนแปลงประสิทธิผลของการควบคุมการดำเนินงาน)

แนวคิดการบริหารความเสี่ยงตามหลัก COSO ERM 2017

COSO ERM 2017 ได้รับการปรับปรุงใหม่เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจและมีความยืดหยุ่นมากขึ้น โดยมุ่งเน้นการบูรณาการความเสี่ยงเข้ากับการบริหารองค์กรในทุกระดับ ซึ่งกรอบการทำงานนี้ประกอบด้วย 5 องค์ประกอบหลักและ 20 หลักการย่อยที่ใช้ในการจัดการความเสี่ยง ดังนี้:

1. Governance and Culture (การกำกับดูแลและวัฒนธรรมองค์กร)

Governance: องค์กรต้องมีโครงสร้างการกำกับดูแลที่ชัดเจน ตั้งแต่บทบาทของคณะกรรมการ ผู้บริหาร ไปจนถึงผู้ที่เกี่ยวข้องในการบริหารความเสี่ยง

Culture: การสร้างวัฒนธรรมองค์กรที่เปิดรับการบริหารความเสี่ยง ส่งเสริมให้พนักงานทุกระดับมีความตระหนักและมีส่วนร่วมในการจัดการความเสี่ยง

Core Principles: การกำหนดค่านิยมหลักที่สอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์และทัศนคติที่เหมาะสมต่อความเสี่ยง

2. Strategy and Objective-Setting (การกำหนดกลยุทธ์และวัตถุประสงค์)

Alignment of Risk and Strategy: ความเสี่ยงต้องถูกนำมาพิจารณาในกระบวนการกำหนดกลยุทธ์ขององค์กร เพื่อให้มั่นใจว่าความเสี่ยงที่ยอมรับได้สอดคล้องกับเป้าหมาย

Risk Appetite: องค์กรต้องกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ซึ่งจะถูกใช้เป็นแนวทางในการตัดสินใจ

Business Objectives: ความเสี่ยงต้องถูกประเมินและสอดคล้องกับวัตถุประสงค์ทางธุรกิจในแต่ละระดับขององค์กร

3. Performance (การดำเนินงาน)

Risk Identification: การระบุความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานขององค์กร รวมถึงความเสี่ยงที่เกิดจากปัจจัยภายนอกและภายใน

Risk Assessment: การประเมินความเสี่ยงโดยใช้เครื่องมือที่เหมาะสม เช่น การวิเคราะห์ผลกระทบและความน่าจะเป็น เพื่อจัดลำดับความเสี่ยงตามความสำคัญ

Risk Response: การกำหนดแนวทางการตอบสนองต่อความเสี่ยง เช่น การหลีกเลี่ยงความเสี่ยง การลดความเสี่ยง การโอนย้ายความเสี่ยง หรือการยอมรับความเสี่ยง

Risk Review: การตรวจสอบผลการบริหารความเสี่ยง และปรับปรุงแผนบริหารความเสี่ยงตามสถานการณ์ที่เปลี่ยนแปลง

4. Review and Revision (การตรวจสอบและทบทวน)

Performance Monitoring: การตรวจสอบผลการดำเนินงานที่เกี่ยวข้องกับการบริหารความเสี่ยง เพื่อให้มั่นใจว่ามีการตอบสนองต่อความเสี่ยงอย่างเหมาะสม

Continuous Improvement: การทบทวนและปรับปรุงกระบวนการบริหารความเสี่ยงอย่างต่อเนื่อง เพื่อให้สอดคล้องกับสภาพแวดล้อมทางธุรกิจและปัจจัยที่เปลี่ยนแปลง

5. Information, Communication, and Reporting (ข้อมูล การสื่อสาร และการรายงาน)

Information Quality: การเก็บรวบรวมและใช้ข้อมูลที่ถูกต้องและเหมาะสมในการจัดการความเสี่ยง รวมถึงการนำข้อมูลมาใช้ประกอบการตัดสินใจ

Communication: การสื่อสารเรื่องความเสี่ยงภายในองค์กรอย่างชัดเจนและโปร่งใส เพื่อให้ทุกฝ่ายเข้าใจและร่วมกันจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

Reporting: การรายงานผลการบริหารความเสี่ยงต่อผู้บริหารระดับสูง คณะกรรมการ และผู้มีส่วนได้เสีย เพื่อให้สามารถติดตามความคืบหน้าและปรับปรุงกระบวนการได้ตามความจำเป็น

สรุปกรอบการทำงานของ COSO ERM 2017

กรอบการทำงานของ COSO ERM 2017 มุ่งเน้นการบูรณาการการบริหารความเสี่ยงเข้ากับทุกส่วนขององค์กร ตั้งแต่กระบวนการกำหนดกลยุทธ์ การดำเนินงาน ไปจนถึงการตรวจสอบและปรับปรุงการบริหารความเสี่ยงอย่างต่อเนื่อง ด้วยหลักการนี้ องค์กรจะสามารถตัดสินใจอย่างมีข้อมูลที่ถูกต้อง ลดความไม่แน่นอน และเพิ่มโอกาสในการบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพ

กระบวนการบริหารความเสี่ยงของสำนักงาน (Risk Management Process)

เป็นขั้นตอนในการระบุ ประเมิน และจัดการความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ของสำนักงาน เพื่อให้สามารถควบคุมและจัดการความเสี่ยงได้อย่างมีประสิทธิภาพตามหลัก COSO ERM 2017 ประกอบด้วย 6 ขั้นตอนหลัก ดังนี้:

1. การกำหนดบริบท (Establishing the Context)

ขั้นตอนนี้เป็นขั้นตอนแรกในการบริหารความเสี่ยง สำนักงานดำเนินการวิเคราะห์บริบทหรือสภาพแวดล้อมที่ตนเอง**ดำเนินงานอยู่เป็นประจำทุกปี และทบทวนทุกไตรมาสตามรอบรายงานการบริหารความเสี่ยง** โดยการวิเคราะห์บริบทหรือสภาพแวดล้อมหมายถึงการทำความเข้าใจทั้งปัจจัยภายในและภายนอกที่อาจส่งผลต่อการบริหารความเสี่ยง เช่น วัตถุประสงค์และเป้าหมายขององค์กร ปัจจัยเศรษฐกิจ สังคม การเมือง กฎหมาย สิ่งแวดล้อม และเทคโนโลยี รวมถึงการสถานการณ์ของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง โดยอาจวิเคราะห์ SWOT หรือ PESTEL

ผู้รับผิดชอบ : เลขานุการคณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในของสำนักงานสภาองค์กรของผู้บริโภค เป็นผู้จัดทำรายงานการวิเคราะห์บริบทและสิ่งแวดล้อม

2. การระบุความเสี่ยง (Risk Identification)

เป็นขั้นตอนในการระบุความเสี่ยงที่อาจส่งผลกระทบต่อองค์กร โดยการพิจารณาจากทุกมิติ เช่น ความเสี่ยงทางกลยุทธ์ การเงิน การปฏิบัติงาน กฎหมาย เทคโนโลยี และในการดำเนินการระบุความเสี่ยงควรระบุความเสี่ยงให้ครบ 5 ด้าน เพื่อการมองรอบด้านในการบริหารความเสี่ยง คือ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk),ความเสี่ยงด้านการเงิน (Financial Risk), ความเสี่ยงด้านปฏิบัติการ (Operational Risks), ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) และความเสี่ยงด้านกฎหมายกฎระเบียบ (Compliance and Legal Risk)

สำนักงานดำเนินการระบุความเสี่ยง กำหนดปัจจัยเสี่ยง (สาเหตุความเสี่ยง) และตัวชี้วัดความเสี่ยง (KRIs) เพื่อจัดทำแผนบริหารความเสี่ยงรายปี และทบทวนทุกไตรมาสตามรอบรายงานการบริหารความเสี่ยง (กรณีที่เป็นความเสี่ยงเร่งด่วน Emerging Risk) โดยมีข้อมูลนำเข้ามาเพื่อวิเคราะห์ ได้แก่

- การวิเคราะห์บริบทหรือสภาพแวดล้อมขององค์กร
- แผนยุทธศาสตร์ แผนปฏิบัติงานประจำปี และผลการดำเนินงานต่าง ๆ
- ผลการบริหารความเสี่ยงปีที่ผ่านมา ถึงความเสี่ยงที่เหลืออยู่ (Residual Risk)
- ผลการควบคุมภายใน และรายงานการตรวจสอบภายใน
- ข้อเสนอแนะ หรือข้อร้องเรียนต่าง ๆ ทั้งจากผู้มีส่วนได้ส่วนเสีย และประชาชน
- อื่น ๆ

วิธีการระบุความเสี่ยง อาจใช้การประชุมเชิงปฏิบัติการ การระดมสมอง การสัมภาษณ์ การวิเคราะห์ข้อมูลในอดีต หรือการตรวจสอบกระบวนการทำงานปัจจุบัน

ผู้รับผิดชอบ : คณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในฯ และฝ่ายต่าง ๆ (Risk Owner)

3. การประเมินความเสี่ยง (Risk Assessment)

ขั้นตอนนี้ประกอบด้วยการวิเคราะห์และประเมินผลกระทบของความเสี่ยง โดยจะพิจารณาถึง ความน่าจะเป็น (Likelihood) และ ความรุนแรงของผลกระทบ (Impact) ของความเสี่ยงเหล่านั้น หากเกิดขึ้น การประเมินความเสี่ยงช่วยให้สำนักงานสามารถจัดลำดับความสำคัญของความเสี่ยงเพื่อจัดทำแผนจัดการความเสี่ยงได้อย่างเหมาะสม

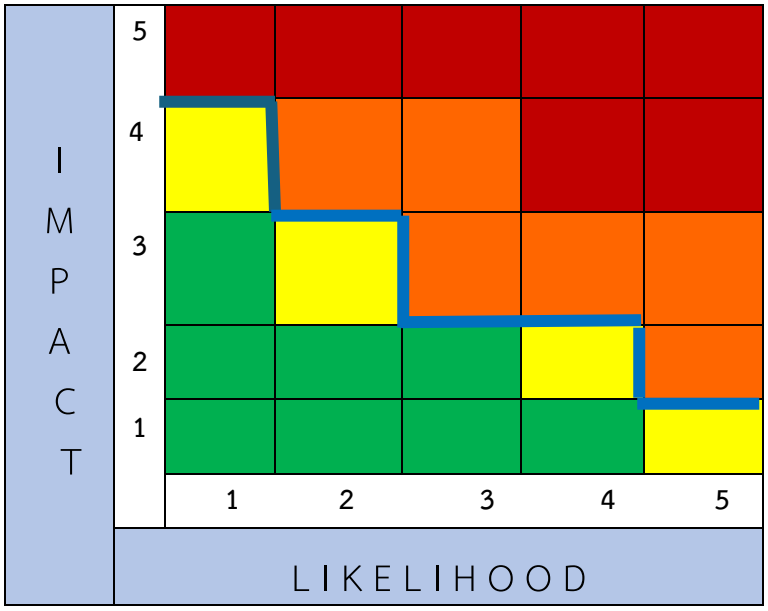
วิธีการประเมินความเสี่ยง อาจใช้การประชุมเชิงปฏิบัติการ การระดมสมอง การสัมภาษณ์ การวิเคราะห์ข้อมูลในอดีต หรือการตรวจสอบกระบวนการทำงานปัจจุบัน โดยดำเนินการพร้อมกับขั้นตอนการระบุความเสี่ยง **สำนักงานดำเนินการประเมินความเสี่ยงเพื่อจัดทำแผนบริหารความเสี่ยงรายปี และทบทวนทุกไตรมาสตามรอบรายงานการบริหารความเสี่ยง**

ผู้รับผิดชอบ : คณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในฯ

3.1 การประเมินระดับความเสี่ยงของสำนักงาน

- การประเมินระดับความเสี่ยงของสำนักงาน จะดำเนินการ**ประเมินระดับความเสี่ยงเป็นประจำทุกปีในช่วงที่ดำเนินการจัดทำแผนบริหารความเสี่ยงประจำปี** โดยความเสี่ยงที่มีระดับความเสี่ยงสูง (สีส้ม) และสูงมาก (สีแดง) จะเป็นความเสี่ยงที่เหลืออยู่ (Residual Risk) ที่จะถูกนำมาจัดทำแผนจัดการความเสี่ยงในปีถัดไป
- การทบทวนระดับความเสี่ยงของสำนักงาน จะดำเนินการ**ทบทวนระดับความเสี่ยงทุกไตรมาสตามรอบรายงานการบริหารความเสี่ยง** เพื่อพิจารณาแนวโน้มของระดับความเสี่ยงที่จะเกิดขึ้น และพิจารณาจัดทำ/ปรับแผนความเสี่ยงในจัดการความเสี่ยง ในระหว่างปีนั้น
- นอกจากนั้นอาจมีความเสี่ยงที่ถูกพิจารณาว่าเพิ่มเป็นความเสี่ยงระหว่างปีที่มีระดับความเสี่ยงสูงถึงสูงมากที่ต้องดำเนินการจัดทำแผนการความเสี่ยงอย่างเร่งด่วน (Emerging Risk)
- ระดับความเสี่ยง = ระดับโอกาส (Likelihood) X ระดับผลกระทบของความเสี่ยงที่จะเกิดขึ้น (Impact) และพล็อตลงในแผนภาพแสดงระดับความเสี่ยง (Heat Map/Matrix)

แผนภาพแสดงระดับความเสี่ยง (Heat Map/ Risk Matrix)



- **เกณฑ์การประเมินโอกาสการเกิดความเสี่ยง (Likelihood)** เป็นการพิจารณาได้จากรูปแบบของความถี่ (Frequency) หรือโอกาสที่จะเกิดความเสี่ยง โดยแบ่งเป็น 5 ระดับ

ตัวอย่างเกณฑ์ประเมินโอกาสการเกิดความเสี่ยง (Likelihood)

ระดับคะแนน	ความถี่โดยเฉลี่ย	โอกาสการเกิดความเสี่ยง	โอกาสการเกิดความเสี่ยงภายในระยะเวลา 12 เดือนข้างหน้า
1	ต่ำมาก/น้อยมาก	มีความเป็นไปได้ที่จะเกิดเหตุการณ์ที่มีความเสี่ยงต่ำมาก หรือในอดีตไม่เคยเกิดขึ้นเลย	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้น้อยมาก หรือแทบไม่มี ความน่าจะเป็นที่จะเกิดเหตุการณ์หรือมีโอกาสเกิดเหตุการณ์ (probability) ไม่เกินร้อยละ 5
2	ต่ำ / น้อย	มีความเป็นไปได้ที่จะเกิดเหตุการณ์ที่มีความเสี่ยงทุก 2 ปี	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้น้อย หรือ มีโอกาสเกิดเหตุการณ์ (probability) มากกว่าร้อยละ 5 แต่ไม่เกินร้อยละ 25

ระดับคะแนน	ความถี่โดยเฉลี่ย	โอกาสการเกิดความเสี่ยง	โอกาสการเกิดความเสี่ยง ภายในระยะเวลา 12 เดือนข้างหน้า
3	ปานกลาง	มีความเป็นไปได้ที่จะเกิดเหตุการณ์ที่มีความเสี่ยง ทุก 1 ปี	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้ในบางครั้ง หรือมีโอกาสเกิดเหตุการณ์ (probability) มากกว่าร้อยละ 25 แต่ไม่เกินร้อยละ 50
4	สูง / บ่อย	มีความเป็นไปได้ที่จะเกิดเหตุการณ์ที่มีความเสี่ยง ทุก 6 เดือน	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้สูง หรือมีโอกาสเกิดเหตุการณ์ (probability) มากกว่าร้อยละ 50 แต่ไม่เกินร้อยละ 75
5	สูงมาก / บ่อยมาก	มีความเป็นไปได้ที่จะเกิดเหตุการณ์ที่มีความเสี่ยง ทุก 1 เดือน	คาดว่าเหตุการณ์นี้มีโอกาสเกิดขึ้นสูงมากในทุกสภาพการณ์ หรือ มีโอกาสเกิดเหตุการณ์ (probability) มากกว่าร้อยละ 75

- **เกณฑ์การประเมินผลกระทบ (Impact) ของความเสี่ยงที่อาจเกิดขึ้นกับสำนักงานมี ดังนี้**

ตัวอย่างเกณฑ์การประเมินผลกระทบ (Impact) แบ่งเป็น 5 ระดับคะแนน โดยสามารถประเมินผลกระทบด้านใดด้านหนึ่งหรือหลายด้านในความเสี่ยงหนึ่งๆ ได้ และถือเอาคะแนนประเมินผลกระทบที่มากที่สุดเป็นสำคัญ

ผลกระทบ	ระดับความรุนแรง				
	ต่ำมาก คะแนน 1	**ต่ำ คะแนน 2**	**ปานกลาง คะแนน 3**	**สูง คะแนน 4**	**สูงมาก คะแนน 5**
ผลกระทบที่ไม่ใช้ตัวเงิน (NON-FINANCIAL)					
ด้านการวางแผนกลยุทธ์และการบริหารจัดการของผู้บริหาร	**ไม่ส่งผลกระทบ** ต่อแผนการบริหารและการดำเนินการตามแผนฯ หรือพันธกิจ **โดยสามารถ**	**ส่งผลกระทบเล็กน้อย** ต่อแผนการบริหาร และการดำเนินงานตามแผนฯ หรือพันธกิจ **โดยผู้บริหารระดับ**	**ส่งผลกระทบปานกลาง**ต่อแผนการบริหาร และการดำเนินงานตามแผนฯ หรือพันธกิจ **โดยผู้บริหาร**	**ส่งผลกระทบอย่างมีนัยสำคัญ**ต่อแผนการบริหาร และการดำเนินงานตามแผนฯ หรือพันธกิจ **โดยผู้บริหาร**	**ส่งผลกระทบรุนแรง** ทำให้ไม่สามารถดำเนินงานตามพันธกิจของสำนักงานได้ **อันมีผลต่อการดำรงอยู่ของสำนักงาน**

ผลกระทบ	ระดับความรุนแรง				
	ต่ำมาก คะแนน 1	**ต่ำ คะแนน 2**	**ปานกลาง คะแนน 3**	**สูง คะแนน 4**	**สูงมาก คะแนน 5**
	ดำเนินงานได้สำเร็จตามเป้าหมาย	**หัวหน้าฝ่ายสามารถจัดการได้**	**ระดับรองเลขาธิการสามารถจัดการได้**	**ระดับเลขาธิการสามารถจัดการได้**	
ด้านภาพลักษณ์และชื่อเสียง	ไม่กระทบต่อภาพลักษณ์และชื่อเสียงของสำนักงานหรือรับรู้เพียง**ภายในสำนักงานเท่านั้น**	ส่งผลกระทบด้านลบเพียงเล็กน้อยต่อภาพลักษณ์และชื่อเสียงของสำนักงานหรือรับรู้เพียง**ภายในวงการสื่อเท่านั้น ซึ่งยังไม่เป็นที่รับรู้ต่อสาธารณชน**	ส่งผลกระทบด้านลบต่อภาพลักษณ์และชื่อเสียงของสำนักงานหรือถูกเผยแพร่ต่อ**สาธารณชนในสื่อระดับประเทศในระยะเวลาสั้น (1-2 วัน)**	ส่งผลกระทบด้านลบต่อภาพลักษณ์และชื่อเสียงของสำนักงานอย่างมีสาระสำคัญหรือถูกเผยแพร่ต่อ**สาธารณชนในสื่อระดับประเทศในระยะเวลาประมาณ 1 สัปดาห์**	ส่งผลกระทบด้านลบต่อภาพลักษณ์และชื่อเสียงของสำนักงานอย่างมีสาระสำคัญหรือถูกเผยแพร่ต่อ**สาธารณชนในสื่อระดับประเทศ และต่างประเทศอย่างต่อเนื่องในระยะยาว**
ด้านการเงิน	อัตราส่วนรายได้ต่อรายจ่าย (รายได้ลบรายจ่าย หารรายจ่าย) **มากกว่าร้อยละ 20** หรือ ไม่มีผลกระทบต่อสภาพคล่องและการบริหารจัดการเงินสด	อัตราส่วนรายได้ต่อรายจ่าย (รายได้ลบรายจ่าย หารรายจ่าย) **มากกว่าร้อยละ 10 แต่ไม่เกินร้อยละ 20** หรือ กระแสเงินสดอาจลดลงเล็กน้อย แต่ยังสามารถเบิกจ่ายเงินได้และรักษาสภาพคล่องได้ตามปกติ	อัตราส่วนรายได้ต่อรายจ่าย (รายได้ลบรายจ่าย หารรายจ่าย) **มากกว่าร้อยละ 5 แต่ไม่เกินร้อยละ 10** หรือ กระแสเงินสดลดลงอย่างชัดเจน แต่ยังสามารถรักษาความสามารถในการเบิกจ่ายเงินได้ มีความจำเป็นต้องจัดทำแผนเพื่อบริหารเงินสดเพิ่มขึ้น	อัตราส่วนรายได้ต่อรายจ่าย (รายได้ลบรายจ่าย หารรายจ่าย) **มากกว่าร้อยละ 0 แต่ไม่เกินร้อยละ 5** หรือ กระแสเงินสดมีปัญหาต้องใช้เงินสำรองจำนวนมาก อาจต้องมีการกู้ยืมหรือหาวิธีเพิ่มสภาพคล่องในระยะสั้น	ขาดความเพียงพอทางการเงิน / อัตราส่วนรายได้ต่อรายจ่าย (รายได้ลบรายจ่าย หารรายจ่าย) **ต่ำกว่า 0** หรือ กระแสเงินสดมีปัญหารุนแรง อาจไม่สามารถเบิกจ่ายเงินได้ตามกำหนด และต้องดำเนินการกู้ยืมเร่งด่วนเพื่อรักษาสภาพคล่อง
ด้านปฏิบัติการ	**ไม่ส่งผลกระทบต่อกระบวนการทำงานหลัก** ไม่มีผลกระทบต่อเป้าหมายหรือการดำเนินงาน	การหยุดชะงักของกระบวนการบางส่วน **แต่สามารถดำเนินการต่อได้โดยไม่ต้องหยุดงานทั้งหมด**	การหยุดชะงักของกระบวนการหลักหรือรองบางส่วน **ทำให้การดำเนินงานล่าช้า แต่สามารถแก้ไขได้ภายในเวลาอันสมควร**	การหยุดชะงักของกระบวนการหลักเป็นระยะเวลานาน **ส่งผลให้ธุรกิจล่าช้าหรือไม่สามารถดำเนินการได้ตามปกติ**	กระบวนการหลักหยุดชะงักเป็นเวลานาน **ทำให้ต้องหยุดการดำเนินการโดยสิ้นเชิง และต้องใช้เวลานานในการฟื้นฟู**

ผลกระทบ	ระดับความรุนแรง				
	ต่ำมาก คะแนน 1	ต่ำ คะแนน 2	ปานกลาง คะแนน 3	สูง คะแนน 4	สูงมาก คะแนน 5
ด้าน เทคโนโลยี	ระบบ IT ที่ใช้ในการสื่อสารภายในองค์กรหยุดทำงานชั่วคราว แต่ไม่กระทบต่อการดำเนินงานหลัก	ความล้มเหลวของระบบบันทึกข้อมูลที่ไม่ได้ใช้งานบ่อย แต่มีผลให้ต้องใช้เวลาในการแก้ไขข้อมูล แต่ไม่มีผลกระทบระยะยาว	ระบบ ERP หยุดทำงาน ทำให้การจัดการทรัพยากรในสำนักงานเกิดความล่าช้า แต่สามารถกลับมาทำงานได้ภายในเวลาอันสมควร	การโจมตีทางไซเบอร์ที่ส่งผลให้ระบบข้อมูลลูกค้าล่มและส่งผลต่อความเชื่อมั่นและการดำเนินงาน ทำให้การหยุดชะงักของกระบวนการหลักที่สำคัญเป็นเวลานาน	การโจมตีทางไซเบอร์ที่ขโมยข้อมูลประชาชนจำนวนมาก ทำให้ประชาชนและผู้มีส่วนได้เสียสูญเสียความเชื่อมั่น และเกิดความเสียหายอย่างมหาศาล กระบวนการหลักขององค์กรหยุดชะงักเป็นเวลานาน
ด้านกฎหมาย	ไม่มีการละเมิดกฎหมายหรือกฎระเบียบที่ชัดเจน หรือเป็นการละเมิดที่มีความรุนแรงต่ำ สามารถแก้ไขได้อย่างรวดเร็ว	ละเมิดกฎระเบียบเล็กน้อย แต่สามารถแก้ไขได้ภายในเวลาที่กำหนดโดยหน่วยงานกำกับ อาจต้องมีการแจ้งรายงาน	ละเมิดกฎระเบียบที่สำคัญ ส่งผลให้ต้องมีการตรวจสอบจากหน่วยงานกำกับดูแล อาจต้องดำเนินการแก้ไขหรือปรับปรุงอย่างรวดเร็ว	การละเมิดกฎหมายหรือกฎระเบียบที่มีความสำคัญมาก ส่งผลให้ต้องมีการตรวจสอบหรือฟ้องร้องจากหน่วยงานกำกับดูแล และอาจต้องดำเนินการแก้ไขในระยะยาว	การละเมิดกฎหมายที่สำคัญอย่างรุนแรง ส่งผลให้เกิดการฟ้องร้องขนาดใหญ่ หรือการสอบสวนจากหน่วยงานภาครัฐและอาจถูกระงับการดำเนินงาน

3.2 การจัดระดับความเสี่ยงของสำนักงาน

หลังจากการประเมินระดับความเสี่ยงแล้ว สำนักงานจะดำเนินการจัดระดับความเสี่ยง โดยจะแบ่งระดับของความเสี่ยงออกเป็น 4 ระดับ และมีค่าความเสี่ยงรวมสูงสุดเท่ากับ 25 คะแนน (Level of Risk) โดยการนำผลที่ได้จากการประเมินระดับโอกาสการเกิดความเสี่ยง (L, Likelihood) และระดับผลกระทบของความเสี่ยงที่จะเกิดขึ้น (I, Impact) มาจัดทำแผนภาพแสดงระดับของความเสี่ยง (Heat Map, Risk Matrix)

ระดับความเสี่ยงรวม = ระดับโอกาสที่จะเกิดความเสี่ยง (L) X ระดับผลกระทบของความเสี่ยง (I)

ระดับความเสี่ยงบนแผนภาพระดับความเสี่ยง (Heat Map, Risk Matrix)

ระดับ ความเสี่ยง	สัญลักษณ์ (แถบสี)	ความหมาย
ต่ำ	เขียว 	ระดับความเสี่ยงที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม
ปานกลาง	เหลือง 	ระดับความเสี่ยงที่พอยอมรับได้ แต่ควรมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ ยังดำเนินการติดตามการควบคุมความเสี่ยงนี้ทุกไตรมาส
สูง	ส้ม 	ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก	แดง 	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
หมายเหตุ : ในกรณีที่ระดับความเสี่ยงที่มีคะแนน =5 ซึ่งมีคะแนนผลกระทบ = 5 และคะแนนโอกาสการเกิด = 1 เป็นความเสี่ยงตาม Black Swan theory ของ Nassim Nicholas Taleb ที่อธิบายถึง เหตุการณ์ที่ไม่ค่อยขึ้น แต่มีผลกระทบสูงมาก อยู่นอกเหนือความคาดหมาย และยากต่อการพยากรณ์ หรือเรียกว่า Silent Risk ควรได้รับการพิจารณาในการจัดทำแผนบริหารความเสี่ยง		

4. การตอบสนองต่อความเสี่ยง (Risk Response)

4.1 เมื่อประเมินและจัดลำดับความเสี่ยงได้แล้ว สำนักงานจะต้องกำหนดมาตรการในการตอบสนองตามระดับของความเสี่ยง ดังนี้

1) **ความเสี่ยงระดับต่ำ (Low Risk) และความเสี่ยงระดับปานกลาง (Meduim Risk) เป็นความเสี่ยงที่ยอมรับได้ (Risk Acceptance)** ไม่ต้องดำเนินการจัดทำแผนจัดการความเสี่ยง แต่จะดำเนินการติดตามและทบทวนระดับความเสี่ยงทุกๆ ไตรมาส ตามรอบการรายงานการบริหารความเสี่ยง

2) **ความเสี่ยงระดับสูง (High Risk) หรือวิกฤติ (Extreme Risk) ต้องมีแผนการจัดการความเสี่ยงอย่างจริงจัง** โดยพิจารณากำหนดมาตรการในแผนจัดการความเสี่ยง ให้สอดคล้องกับปัจจัยเสี่ยง (สาเหตุของความเสี่ยง) ตัวชี้วัดความเสี่ยง (KRI) และสอดคล้องกับแผนยุทธศาสตร์และแผนปฏิบัติการของสำนักงาน สามารถจัดการความเสี่ยงให้เหมาะสมโดยวิธีการเดียวหรือหลายวิธีการในการจัดความเสี่ยงนั้น ๆ ดังนี้

- การลดความเสี่ยง (Risk Reduction, Risk Mitigation): ดำเนินมาตรการจัดทำแผนจัดการความเสี่ยงเพื่อลดความน่าจะเป็นหรือผลกระทบของความเสี่ยง
- การโอนย้ายความเสี่ยง (Risk Transfer): โอนความเสี่ยงไปยังบุคคลที่สาม เช่น การทำประกันภัย
- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance, Risk Terminate): หลีกเลี่ยง/ยกเลิก กิจกรรม/โครงการหรือเหตุการณ์ที่มีความเสี่ยงสูงนั้น

วิธีการกำหนดมาตรการและแผนจัดการความเสี่ยง อาจใช้การประชุมเชิงปฏิบัติการ การระดมสมอง การสัมภาษณ์ การวิเคราะห์ข้อมูลในอดีต หรือการตรวจสอบกระบวนการทำงานปัจจุบัน โดยดำเนินการพร้อมกับขั้นตอนการระบุและประเมินความเสี่ยง **สำนักงานดำเนินการจัดทำแผนบริหารความเสี่ยงรายปี และทบทวนทุกไตรมาสตามรอบรายงานการบริหารความเสี่ยง**

ผู้รับผิดชอบ : คณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในฯ และฝ่ายที่รับผิดชอบการจัดการความเสี่ยงนั้น ๆ (Risk Owner)

4.2 การดำเนินการตามแผนจัดการความเสี่ยง หลังจากที่ได้แผนจัดการความเสี่ยงประจำปีแล้ว เลขานุการคณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในฯ จะดำเนินการแจกจ่ายแผนให้ฝ่ายที่รับผิดชอบ (Risk Owner) การดำเนินการจัดการความเสี่ยงตามแผนจัดการความเสี่ยง

ผู้รับผิดชอบ : เลขานุการคณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในฯ และฝ่ายที่รับผิดชอบ (Risk Owner)

5. การติดตามและตรวจสอบ (Monitoring and Review)

กระบวนการบริหารความเสี่ยงต้องได้รับการติดตามและตรวจสอบอย่างต่อเนื่องทุกไตรมาส สำนักงานประเมินผลว่าการตอบสนองต่อความเสี่ยงที่ได้ดำเนินการนั้นมีประสิทธิผล ประสิทธิภาพหรือไม่ โดยการทบทวนบริบทและสภาพแวดล้อม ความเสี่ยง ระดับความเสี่ยง แผนจัดการความเสี่ยง และกาบรรลุตัวชี้วัดความเสี่ยง

(KRIs) และมีการทบทวนและประเมินความเสี่ยงใหม่เมื่อมีการเปลี่ยนแปลงสถานการณ์ที่มีนัยสำคัญมากกับสำนักงาน

วิธีการติดตามและตรวจสอบความเสี่ยง

- เลขานุการคณะทำงานบริหารจัดการความเสี่ยงฯ ดำเนินการติดตามผลความคืบหน้าการจัดการความเสี่ยงตามแผนจัดการความเสี่ยงจากฝ่ายที่รับผิดชอบ (Risk owner) ทุกไตรมาส เพื่อจัดทำเป็นรายงานความคืบหน้าแผนบริหารความเสี่ยงรายไตรมาส และผลการบริหารความเสี่ยงประจำปี เสนอต่อคณะทำงานบริหารจัดการความเสี่ยงฯ เพื่อเห็นชอบ อนุคณะกรรมการบริหารและ กนย. เพื่อรับทราบต่อไป
- หน่วยตรวจสอบภายใน ดำเนินการตรวจสอบวิธีการบริหารความเสี่ยง แผนบริหารความเสี่ยง และผลการบริหารความเสี่ยง เป็นประจำทุกปี พร้อมให้ข้อเสนอแนะ

ผู้รับผิดชอบ : 1) เลขานุการคณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในฯ

2) หน่วยตรวจสอบภายใน

6. การสื่อสารและการรายงาน (Communication and Reporting)

6.1 การสื่อสารการบริหารความเสี่ยงเป็นขั้นตอนที่สำคัญในการทำให้ทุกคนในองค์กรตระหนักถึงความเสี่ยงและวิธีการจัดการที่เหมาะสม ข้อมูลความเสี่ยงต้องถูกสื่อสารไปยังผู้ที่เกี่ยวข้องทั้งภายในและภายนอกสำนักงาน อาจดำเนินการโดยการจัดสัมมนา/อบรมเรื่องการบริหารความเสี่ยง การแจ้งข่าวสารประชาสัมพันธ์ตามแพลตฟอร์มต่าง ๆของสำนักงาน เช่น Line, website, team เป็นต้น

ผู้รับผิดชอบ : เลขานุการคณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในฯ

6.2 การรายงานการบริหารความเสี่ยง เลขานุการคณะทำงานบริหารจัดการความเสี่ยงฯ เสนอแผนบริหารความเสี่ยงประจำปี รายงานความคืบหน้าแผนบริหารความเสี่ยงรายไตรมาส และผลการบริหารความเสี่ยงประจำปีต่อคณะทำงานบริหารจัดการความเสี่ยงฯ เพื่อเห็นชอบ อนุคณะกรรมการบริหารและ กนย. เพื่อรับทราบต่อไป รวมถึงรายงานต่อหน่วยงานที่กำกับดูแลสำนักงานต่าง ๆ ตามความเหมาะสม

ผู้รับผิดชอบ : เลขานุการคณะทำงานบริหารจัดการความเสี่ยงและประเมินระบบควบคุมภายในฯ

ภาคผนวก

ตัวอย่าง แบบฟอร์ม แผนจัดการความเสี่ยง

แผนบริหารความเสี่ยงสำนักงานสภาองค์กรของผู้บริโภค ประจำปีงบประมาณ พ.ศ....			
ความเสี่ยงลำดับที่ ..			
ประเภทความเสี่ยง			
การประเมินค่าระดับความเสี่ยง	**ค่าโอกาส**	**ค่าผลกระทบ**	**คะแนน**
ประเมินระดับความเสี่ยง ก่อนการจัดการความเสี่ยง			
ประเมินระดับความเสี่ยง ไตรมาสที่			
ตัวชี้วัดความเสี่ยง (KRIs)			
ผลตามตัวชี้วัดความเสี่ยง (KRIs)			
ผู้รับผิดชอบ :			

ปัจจัยความเสี่ยง (สาเหตุความเสี่ยง)	มาตรการการจัดการความเสี่ยงที่มีอยู่เดิม	มาตรการการจัดการความเสี่ยงใหม่	กำหนดเสร็จ
สรุปรายงานความคืบหน้ารายไตรมาส			

ตัวอย่าง แบบรายงานและติดตามผลการจัดการความเสี่ยง ไตรมาส....ปีงบประมาณ....

แบบการรายงานและติดตามผลการจัดการความเสี่ยง ไตรมาส... ปีงบประมาณ ...

ความเสี่ยง :

( ) ด้านกลยุทธ์ ( ) ด้านการการดำเนินงาน ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ ( ) ด้านเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ :

ตัวชี้วัดความเสี่ยง (KRIs) :	
ผลตามตัวชี้วัดความเสี่ยง :	

มาตการจัดการความเสี่ยง	สรุปรายละเอียดการดำเนินการ	กำหนดเสร็จ