แผนบริหารความเสี่ยง
SENATE RISK MANAGEMENT

สำนักงานเลขาธิการ
วุฒิสภา

2567

สำนักนโยบายและแผน

คำนำ

ด้วยหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐจะต้องกำหนดแนวทางการบริหารจัดการความเสี่ยงเพื่อเป็นกรอบแนวทางในการบริหารจัดการความเสี่ยงและวางระบบการบริหารจัดการความเสี่ยงระดับองค์กร ซึ่งการบริหารจัดการความเสี่ยง (Risk Management) ถือเป็นเครื่องมือสำคัญต่อการบริหารเชิงยุทธศาสตร์ เป็นกระบวนการมุ่งเน้นความสำคัญหรือชี้ให้เห็นถึงความเสี่ยงที่จะส่งผลกระทบต่อการดำเนินงานในการบรรลุเป้าหมายที่วางไว้ และเป็นการเตรียมองค์กรไว้ล่วงหน้าอย่างมีเหตุมีผล มีหลักการ โดยจะชี้ให้เห็นถึงโอกาสที่จะเกิดความล้มเหลวในการดำเนินงาน และสามารถบริหารจัดการความเสี่ยงที่เกิดขึ้น อันจะช่วยให้องค์กรสามารถบรรลุจุดมุ่งหมายตามวิสัยทัศน์ ประเด็นยุทธศาสตร์ เป้าประสงค์ และพันธกิจ ที่กำหนดไว้ได้

ทั้งนี้ สำนักงานเลขาธิการวุฒิสภาได้จัดทำแผนบริหารความเสี่ยงมาอย่างต่อเนื่องตั้งแต่ปีงบประมาณ พ.ศ. 2561 เพื่อเป็นกรอบแนวทางการดำเนินงานและการบริหารงานให้สามารถลดสภาพปัญหาหรือหลีกเลี่ยงความเสี่ยงที่อาจส่งผลกระทบหรือสร้างความเสียหายให้แก่สำนักงานเลขาธิการวุฒิสภา โดยใช้แนวคิดของกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (The Committee of Sponsoring Organizations of the Tread way Commission) ซึ่งในเวลาต่อมาได้มีการนำการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM) มาเป็นกรอบแนวทางการดำเนินการ โดยมีจุดมุ่งหมายเพื่อให้ผู้บริหารและบุคลากรของสำนักงานเลขาธิการวุฒิสภาได้ตระหนักถึงความสำคัญในการป้องกัน ควบคุม และบรรเทาความผิดพลาดหรือลดความเสียหาย จากการปฏิบัติงานที่อาจส่งผลกระทบต่อองค์กรในอนาคต

สำนักงานเลขาธิการวุฒิสภา หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. 2567 ฉบับนี้ จะเป็นประโยชน์แก่ผู้บริหารและผู้ปฏิบัติงานทุกท่าน เพื่อให้สามารถนำไปเป็นกรอบแนวทางการดำเนินงานบริหารจัดการความเสี่ยงภายในหน่วยงาน และก่อให้เกิดประโยชน์สูงสุดต่อการบรรลุยุทธศาสตร์ขององค์กรต่อไป

สำนักนโยบายและแผน

กันยายน 2566

สารบัญ

บทที่ 1 บทนำ

CHAPTER 1

สำนักงานเลขาธิการวุฒิสภา เป็นองค์กรหลักของฝ่ายนิติบัญญัติของประเทศ สนับสนุนบทบาทภารกิจของวุฒิสภาตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 รวมถึงกรอบทิศทางการพัฒนาประเทศ ได้แก่ ยุทธศาสตร์ชาติ ระยะ 20 ปี แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนการปฏิรูปประเทศ อาทิ ยุทธศาสตร์ชาติ ระยะ 20 ปี แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนการปฏิรูปประเทศ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ดังนั้น เพื่อให้การดำเนินงานของสำนักงานเลขาธิการวุฒิสภาบรรลุวัตถุประสงค์และเป้าหมาย ตามวิสัยทัศน์ พันธกิจ และแผนปฏิบัติราชการ ได้อย่างมีประสิทธิภาพและประสิทธิผล มีการกำกับดูแลที่ดี สร้างความคุ้มค่าและเพิ่มคุณค่าให้แก่องค์กร ทั้งทางด้านการบริหารงาน งบประมาณ และบุคลากร สำนักงานเลขาธิการวุฒิสภาจึงนำระบบการบริหารความเสี่ยงมาใช้ในการบริหารจัดการองค์กร ซึ่งจะเสริมสร้างความมั่นคงในการดำเนินธุรกิจ และก่อให้เกิดประโยชน์สูงสุดต่อผู้รับบริการ ผู้มีส่วนได้ส่วนเสีย และประชาชน

ประเด็นที่สำคัญในเรื่องความเสี่ยง (Risk) คือ ความไม่แน่นอน (Uncertainty) ของผลลัพธ์ที่อาจเป็นทั้งในเชิงบวกหรือเชิงลบ หากองค์กรสามารถเข้าไปบริหารความเสี่ยงได้อย่างถูกต้อง ภาวะคุกคาม ปัญหา อุปสรรคทั้งหลายที่คาดไว้อาจแปรเปลี่ยนเป็นโอกาส และนำไปสู่การสร้างนวัตกรรมได้ ทั้งยังอาจเป็นโอกาสในการพัฒนาประสิทธิภาพในการทำงาน การบริหารความเสี่ยงเป็นเรื่องประกอบกันระหว่างองค์ประกอบที่สำคัญ 2 ส่วน คือ โอกาสที่น่าจะเกิดขึ้นของสิ่งที่ไม่พึงประสงค์กับผลกระทบที่ตามมา การบริหารความเสี่ยงอย่างเหมาะสม จะเป็นการสนับสนุนกลยุทธ์และแผนงานให้บรรลุเป้าหมายตามที่กำหนด ทำให้เข้าใจภัยคุกคามของการปฏิบัติงานในองค์กรให้มีประสิทธิภาพมากขึ้น สนับสนุนให้มีการปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง มีการสื่อสารในองค์กรมากขึ้น การบริหารความเสี่ยงระดับองค์กรเป็นการบริหารความเสี่ยงโดยพิจารณาจากความเสี่ยงทั้งหมด เป็นกระบวนการเชิงระบบเพื่อระบุ ประเมิน ควบคุม และสื่อสารให้ครอบคลุมทั่วทั้งองค์กร ทำให้มีกระบวนคิดในการที่จะมองไปข้างหน้าโดยได้รับการสนับสนุนและมีส่วนร่วมจากผู้บริหารในทุกระดับ รวมถึงทุกคนในองค์กร

การบริหารจัดการความเสี่ยง (Risk Management) เป็นกระบวนการที่ใช้ในการบริหารจัดการเหตุการณ์ที่อาจจะเกิดขึ้นได้และส่งผลกระทบต่อการบริหารงานของทั้งหน่วยงานภาครัฐและเอกชน ดังนั้น การจัดทำแผนบริหารความเสี่ยงจึงเป็นเครื่องมือที่สำคัญ เพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพช่วยลดปัญหาการดำเนินงาน การเพิ่มโอกาสความสำเร็จผลการดำเนินงานโดยรวม โดยการจัดทำแผนบริหารความเสี่ยงจำเป็นต้องได้รับความร่วมมือจากทุกหน่วยงานภายใน เพื่อให้เป็นกรอบแนวทางให้ผู้ปฏิบัติงานเข้าใจในหลักการ กระบวนการ และขั้นตอนของการบริหารความเสี่ยง ซึ่งจะทำให้การดำเนินงานในการบริหารความเสี่ยงเกิดผลสำเร็จตามแผนที่กำหนดไว้ การบริหารความเสี่ยง

จึงถือเป็นเครื่องมือสำคัญต่อการบริหารเชิงยุทธศาสตร์ในการผลักดันให้มีผลการดำเนินงานที่เป็นเลิศ เป็นองค์กรที่มีสมรรถนะสูง (High Performance Organization : HPO)

ทั้งนี้ สำนักงานเลขาธิการวุฒิสภาได้เริ่มนำการบริหารความเสี่ยงมาใช้ ตั้งแต่ปีงบประมาณ พ.ศ. 2549 ตามบันทึกข้อตกลงการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา โดยเริ่มจากการนำแนวคิดของกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (The Committee of Sponsoring Organizations of the Tread way Commission) เป็นกรอบแนวทางการดำเนินการ และได้ดำเนินการต่อเนื่องเรื่อยมาจนได้มีการจัดทำแผนบริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. 2561 – 2562 ซึ่งได้นำแนวคิดบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM) มาใช้เป็นแนวทางในการจัดทำแผนบริหารความเสี่ยง และในเวลาต่อมาได้มีการจัดทำแผนบริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. 2563 – 2565 รวมถึงฉบับนี้ซึ่งเป็นฉบับล่าสุดโดยยังคงใช้แนวคิดบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM) เช่นเดิม

ข้อมูลพื้นฐานการจัดทำแผนบริหารความเสี่ยง

องค์ประกอบหลักที่นำมาใช้เป็นข้อมูลพื้นฐานในการจัดทำแผนบริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา ได้แก่ แผนปฏิบัติราชการประจำปีงบประมาณ พ.ศ. 2566 - 2570 ของสำนักงานเลขาธิการวุฒิสภา โดยมีสาระสำคัญ ดังนี้

วิสัยทัศน์ (VISION)

มุ่งสู่องค์กรอัจฉริยะ ในการสนับสนุนภารกิจของวุฒิสภา เพื่อประโยชน์ของประเทศชาติ และประชาชน

พันธกิจ (MISSION)

1. สนับสนุนการขับเคลื่อนภารกิจด้านนิติบัญญัติตามบทบัญญัติรัฐธรรมนูญและกฎหมาย
2. ส่งเสริมการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข
3. บริหารจัดการองค์กรให้มีขีดสมรรถนะสูงสู่ความเป็น Smart Digitalization

แผนปฏิบัติราชการ

แผนปฏิบัติราชการเรื่องที่ 1 พัฒนางานและสร้างการมีส่วนร่วมด้านกฎหมาย และวิชาการ เพื่อสนับสนุนงานด้านนิติบัญญัติ

เป้าหมายที่ 1 : ยกระดับการพัฒนางานด้านกฎหมาย และงานด้านวิชาการให้ตอบสนองความต้องการของสมาชิกวุฒิสภา

เป้าหมายที่ 2 : พัฒนาความร่วมมือและสนับสนุนข้อมูลด้านกฎหมายและวิชาการ เพื่อสนับสนุนงานด้านนิติบัญญัติ

แนวทางการพัฒนา

1.1 พัฒนารูปแบบและเนื้อหาที่มีความถูกต้อง รวดเร็ว สะดวกในการเข้าถึงงานด้านกฎหมายและวิชาการที่ตอบสนองความต้องการของผู้รับบริการ มีการออกแบบกระบวนงานที่บูรณาการร่วมกันและนำเทคโนโลยีดิจิทัลมาใช้

1.2 สร้างเครือข่าย และการมีส่วนร่วมงานด้านกฎหมาย และวิชาการ

แผนปฏิบัติการเรื่องที่ 2 พัฒนากลไกการสร้างความรู้และการมีส่วนร่วมในการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

เป้าหมายที่ 1 : ประชาชนมีความรู้ ความเข้าใจ และเล็งเห็นถึงความสำคัญของหน้าที่และอำนาจของวุฒิสภา และในการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

เป้าหมายที่ 2 : สร้างเครือข่ายและการมีส่วนร่วมทางการเมืองตามบทบัญญัติของรัฐธรรมนูญ

แนวทางการพัฒนา

2.1 เสริมสร้างความรู้ ความเข้าใจหน้าที่และอำนาจของวุฒิสภา และสร้างเครือข่ายในการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข

2.2 ส่งเสริมการมีส่วนร่วมต่อการพิจารณาร่างกฎหมาย การควบคุมการบริหารราชการแผ่นดิน และการให้ความเห็นชอบผู้ดำรงตำแหน่งตามรัฐธรรมนูญและกฎหมาย

แผนปฏิบัติราชการเรื่องที่ 3 พัฒนาระบบการบริหารจัดการมุ่งสู่ความเป็น Smart Digitalization

เป้าหมายที่ 1 : พัฒนาระบบบริหารจัดการฐานข้อมูล และโครงสร้างพื้นฐานระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลให้ทันสมัย

เป้าหมายที่ 2 : พัฒนาระบบงานที่มีประสิทธิภาพ และเป็นที่ยอมรับของผู้รับบริการ

เป้าหมายที่ 3 : สร้างและนำนวัตกรรมเพื่อยกระดับการให้บริการ

แนวทางการพัฒนา

3.1 พัฒนาระบบและโครงสร้างฐานข้อมูลเทคโนโลยีดิจิทัลและเชื่อมโยงข้อมูลในแนวทางการบูรณาการข้อมูลภาครัฐ

3.2 พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล

3.3 พลิกโฉมกระบวนการปฏิบัติงานให้มีประสิทธิภาพมากขึ้น

3.4 สร้างนวัตกรรมด้วยเทคโนโลยีดิจิทัล

แผนปฏิบัติราชการเรื่องที่ 4 พัฒนาบุคลากรให้มีขีดสมรรถนะสูง มีคุณธรรม มีความสุขและความผูกพัน

เป้าหมายที่ 1 : พัฒนาศักยภาพระบบการบริหารทรัพยากรบุคคลให้มีประสิทธิภาพและทันสมัย

เป้าหมายที่ 2 : พัฒนาศักยภาพของบุคลากรให้มีความรู้ ความสามารถ และทักษะการคิดวิเคราะห์ให้ทันต่อการเปลี่ยนแปลง

เป้าหมายที่ 3 : บุคลากรมีวัฒนธรรมและค่านิยมที่สอดคล้องกับเป้าหมายขององค์กร

เป้าหมายที่ 4 : พัฒนาคุณภาพชีวิตและสภาพแวดล้อมที่ดีในการปฏิบัติงาน

แนวทางการพัฒนา

4.1 ทบทวนและปรับปรุงระบบการบริหารผลการปฏิบัติงานให้สอดคล้องกับระบบการให้รางวัลและสร้างแรงจูงใจ

4.2 ทบทวนและจัดทำสมรรถนะเชิงเทคนิค (Technical Competency Model) ให้สอดคล้องกับเป้าหมายองค์กร

4.3 พัฒนาบุคลากรให้เป็น Multi-skill worker (Hard & Soft Skill)

4.4 สร้างพื้นที่ปลอดภัยให้กับบุคลากรให้กล้าแสดงความคิดเห็น

4.5 ยกระดับคุณธรรมและความโปร่งใสสู่ความยั่งยืน

4.6 สร้างระบบการค้นหาและส่งเสริมให้บุคลากรเกิดความผูกพัน

วัตถุประสงค์ของแผนบริหารความเสี่ยง

1. เพื่อให้ผู้บริหารและผู้ปฏิบัติงานของสำนักงานเลขาธิการวุฒิสภาเข้าใจหลักการและตระหนักถึงความสำคัญของการบริหารความเสี่ยง

2. เพื่อให้ผู้ปฏิบัติงานได้รับทราบขั้นตอน และกระบวนการในการวางแผนบริหารความเสี่ยงและใช้เป็นแนวทางในการดำเนินงาน เพื่อบริหารจัดการและป้องกันความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา

3. เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

4. เพื่อติดตามและประเมินผลการดำเนินงานตามมาตรการ/กิจกรรมควบคุมความเสี่ยงให้เป็นไปตามเกณฑ์ตัวชี้วัดที่กำหนด และนำผลที่ได้จากการติดตามมาเป็นข้อมูลในการบริหารจัดการความเสี่ยงในปีงบประมาณถัดไป

5. เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจถึงกิจกรรมควบคุมความเสี่ยงในด้านต่าง ๆ ของสำนักงานเลขาธิการวุฒิสภา พร้อมนำแผนงานไปสู่การปฏิบัติอันจะช่วยลดมูลเหตุหรือโอกาสในการเกิดความเสี่ยงที่จะเกิดขึ้นกับองค์กร

เป้าหมายของแผนบริหารความเสี่ยง

1. ผู้บริหารและผู้ปฏิบัติงานของสำนักงานเลขาธิการวุฒิสภาเข้าใจหลักการ และตระหนักถึงความสำคัญของการบริหารความเสี่ยง และสามารถนำไปใช้ในการดำเนินงานตามยุทธศาสตร์ และแผนปฏิบัติงานประจำปีให้บรรลุตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

2. ผู้บริหารและผู้ปฏิบัติงานของสำนักงานเลขาธิการวุฒิสภาสามารถระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความเสี่ยงและจัดการความเสี่ยงให้อยู่ในระดับที่ควบคุมได้ หรืออยู่ในระดับต่ำสุดโดยผ่านกระบวนการสร้างความเข้าใจในการจัดทำแผนบริหารจัดการความเสี่ยง

3. ผู้บริหารและผู้ปฏิบัติงานของสำนักงานเลขาธิการวุฒิสภาสามารถนำแผนบริหารจัดการความเสี่ยงไปปฏิบัติ โดยบูรณาการกับการดำเนินงานตามแผนยุทธศาสตร์และแผนปฏิบัติราชการประจำปี

4. มีการดำเนินการติดตามและประเมินผลการดำเนินงานตามมาตรการ/กิจกรรมควบคุมความเสี่ยงอย่างเป็นระบบ โดยเป็นไปตามเกณฑ์ตัวชี้วัดที่กำหนด และนำผลที่ได้จากการติดตามมาเป็นข้อมูลในการบริหารจัดการความเสี่ยงในปีงบประมาณถัดไป

5. ผู้บริหารและผู้ปฏิบัติงานของสำนักงานเลขาธิการวุฒิสภาสามารถได้รับการสื่อสารและสร้างความเข้าใจถึงกิจกรรมควบคุมความเสี่ยงในด้านต่าง ๆ ของสำนักงานเลขาธิการวุฒิสภา และสามารถนำแผนงานไปสู่การปฏิบัติอันจะช่วยลดมูลเหตุหรือโอกาสในการเกิดความเสี่ยงที่จะเกิดขึ้นกับองค์กร

ประโยชน์ของการบริหารความเสี่ยง

การจัดทำแผนบริหารความเสี่ยงเป็นการวางแผนในการป้องกันหรือบรรเทาความเสียหายของภารกิจงานที่อาจเกิดขึ้นกับองค์กรในอนาคต ซึ่งเป็นการช่วยให้ผู้บริหารได้มีข้อมูลสำคัญสำหรับใช้ในการตัดสินใจเพื่อจัดการปัญหา/อุปสรรคจากสถานการณ์ที่ไม่คาดคิดที่จะเกิดกับองค์กรในอนาคต อันนำไปสู่การวางแผนป้องกันหรือลดความเสียหายต่อเหตุการณ์ที่ส่งผลกระทบทางลบต่อองค์กร ทั้งนี้ ประโยชน์ที่ได้จากการดำเนินการบริหารความเสี่ยง ได้แก่

1. สำนักงานเลขาธิการวุฒิสภามีการบริหารจัดการองค์กรที่ดีตามแนวทางการบริหารกิจการบ้านเมืองที่ดี สามารถกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น พร้อมทั้งยกระดับขีดความสามารถและมาตรฐานการดำเนินงาน
2. สำนักงานเลขาธิการวุฒิสภาสามารถใช้การบริหารความเสี่ยงเป็นเครื่องมือสำคัญในการบริหารงานที่สะท้อนให้เห็นถึงความเสี่ยงตามภารกิจงานด้านต่าง ๆ ที่อาจส่งผลกระทบเสียหายกับองค์กรได้อย่างเหมาะสมและทันเวลา รวมถึงใช้เป็นเครื่องมือสำคัญในการบริหารงานและการตัดสินใจในด้านต่าง ๆ
3. สำนักงานเลขาธิการวุฒิสภาสามารถใช้การบริหารความเสี่ยงเพื่อกำหนดทิศทางในการพัฒนาองค์กรให้มุ่งสู่ทิศทางเดียวกัน และสร้างความร่วมมือของบุคลากรในองค์กรเพื่อป้องกันความเสียหายต่อภารกิจงานที่ได้รับผิดชอบ
4. สำนักงานเลขาธิการวุฒิสภาสามารถใช้การบริหารความเสี่ยงเพื่อการพัฒนาการบริหารและจัดสรรทรัพยากรให้เป็นไปได้อย่างมีประสิทธิภาพและประสิทธิผล โดยมีการจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหารความเสี่ยง

บทที่ 2 การบริหารความเสี่ยง

CHAPTER 2

ความหมายและคำจำกัดความของการบริหารความเสี่ยง

1. ความเสี่ยง (Risk)

ความเสี่ยง หมายถึง เหตุการณ์/การกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายของแผนงาน/โครงการที่สำคัญในแต่ละประเด็นยุทธศาสตร์ตามที่ระบุในแผนปฏิบัติราชการประจำปีของสำนักงานเลขาธิการวุฒิสภา

ลักษณะของความเสี่ยง สามารถแยกเป็น 3 ส่วน ดังนี้

1. ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง
2. เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงาน หรือนโยบาย
3. ผลกระทบของความเสี่ยง คือ ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์ความเสี่ยง

2. ปัจจัยเสี่ยง (Risk Factor)

ปัจจัยเสี่ยง หมายถึง ต้นเหตุ หรือสาเหตุ ที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณนั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

3. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โอกาสที่จะเกิด (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง ผลกระทบ (Impact) หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง

ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

4. การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยง หมายถึง กระบวนการที่เป็นระบบในการบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินการต่าง ๆ เพื่อลดมูลเหตุของโอกาสที่จะทำให้เกิดความเสียหายจากการดำเนินการที่ไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ ควบคุมได้ และตรวจสอบได้อย่างเป็นระบบ ซึ่งการดำเนินการดังกล่าวอาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก ดังนี้

1) การยอมรับ (Take, Accept) หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องดำเนินการใด ๆ เช่น กรณีที่มีความเสี่ยงในระดับไม่รุนแรงและไม่คุ้มค่าที่จะดำเนินการใด ๆ ให้ขออนุมัติหลักการรับความเสี่ยงไว้และไม่ดำเนินการใด ๆ

2) การควบคุม (Treat) หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้ แต่ต้องมีการแก้ไขมีวิธีการควบคุม หรือมีการควบคุมเพิ่มเติม เพื่อให้มีการควบคุมที่เพียงพอและเหมาะสม เช่น การปรับปรุงกระบวนการดำเนินงาน การจัดทำมาตรฐานการควบคุม (Risk Based Internal Control)

3) การยกเลิก (Terminate) หรือหลีกเลี่ยง (Avoid) หมายถึง การที่ความเสี่ยงนั้นไม่สามารถยอมรับได้และต้องจัดการให้ความเสี่ยงนั้นไปอยู่นอกเงื่อนไขของการดำเนินงาน เช่น การหยุดดำเนินงานหรือกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้น การเปลี่ยนแปลงวัตถุประสงค์ในการดำเนินงาน การลดขนาดของงานหรือกิจกรรมลง

4) การโอนย้าย (Transfer) หรือแบ่ง (Share) หมายถึง การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น การจ้างบุคคลภายนอกมาดำเนินการแทน การทำประกันภัย เป็นต้น

COSO : Committee of Sponsoring Organizations

COSO หรือ Committee of Sponsoring Organizations เป็นคณะทำงาน ที่ก่อตั้งขึ้นโดยคณะกรรมาธิการของประเทศสหรัฐอเมริกา ที่ชื่อว่า Treadway Commission ในปี 1985 โดยจัดตั้งขึ้นเพื่อศึกษาและพัฒนาแนวทางการบริหารความเสี่ยง รูปแบบการควบคุมภายในที่มีประสิทธิผลและป้องกันการทุจริตของรายงานทางการเงิน และได้ประกาศใช้กรอบโครงสร้างการควบคุมภายในเชิงบูรณาการ (Internal Control – Integrated Framework) เพื่อช่วยให้ธุรกิจและหน่วยงานต่าง ๆ ประเมินและพัฒนาระบบการควบคุมภายในของตน นับแต่นั้นเป็นต้นมา โดยมาตรฐาน COSO ได้มีการปรับปรุงและพัฒนามาอย่างต่อเนื่อง โดยล่าสุดในปี 2013 ได้มีการจัดทำแนวทางเพิ่มเติมด้านการควบคุมภายใน Internal Control – Integrated Framework : Framework and Appendices ซึ่งยังคงยึดกรอบแนวคิดเดิมของปี 1992 ที่กำหนดให้มีการควบคุมภายในแต่เพิ่มเติมในส่วนอื่น ๆ ให้ชัดเจนขึ้น โดยเฉพาะอย่างยิ่งการเพิ่มเติมเรื่องการสอดส่องในภาพรวมของการกำกับดูแลกิจการ

Enterprise Risk Management : ERM

Enterprise Risk Management : ERM หรือการบริหารความเสี่ยงองค์กร คือ กระบวนการที่ดำเนินการโดยคณะกรรมการ ผู้บริหาร และบุคลากรทุกคนภายในองค์กร ในการร่วมมือกันเพื่อการกำหนดกลยุทธ์และการดำเนินงาน รวมถึงมีการกำหนดกระบวนการบริหารความเสี่ยงซึ่งออกแบบไว้เพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ เพื่อให้ได้รับความมั่นใจว่าการดำเนินการขององค์กรจะสามารถบรรลุวัตถุประสงค์ตามที่องค์กรได้กำหนดไว้ และเพื่อทำให้ขั้นตอนและวิธีการในการบริหารความเสี่ยงเป็นไปอย่างมีระบบและดำเนินไปในทิศทางเดียวกันทั่วทั้งองค์กร โดยมีขั้นตอนสำคัญของกระบวนการบริหารความเสี่ยงองค์กร 8 ขั้นตอน ดังนี้

1. สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมภายในองค์กรเป็นพื้นฐานที่สำคัญสำหรับการบริหารความเสี่ยง ซึ่งเป็นปัจจัยที่มีผลต่อการกำหนดกลยุทธ์และเป้าหมายขององค์กร การกำหนดกิจกรรม การบ่งชี้ ประเมิน และจัดการความเสี่ยงสภาพแวดล้อมภายในองค์กร หมายถึง ปัจจัยต่าง ๆ เช่น จริยธรรม วิธีการทำงานของผู้บริหารและบุคลากร รูปแบบการจัดการของฝ่ายบริหารและวิธีการมอบหมายอำนาจหน้าที่และความรับผิดชอบ ซึ่งผู้บริหารต้องมีการกำหนดร่วมกันกับพนักงานในองค์กร ส่งผลให้มีการสร้างจิตสำนึกการตระหนักและรับรู้เรื่องความเสี่ยง และการควบคุมแก่พนักงานทุกคนในองค์กร

2. การกำหนดวัตถุประสงค์ (Objective Setting)

องค์กรจะต้องมีการกำหนดวัตถุประสงค์ในการดำเนินงานตามภารกิจที่ชัดเจน เพื่อให้มั่นใจว่าวัตถุประสงค์ที่กำหนดนั้นมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ โดยการบริหารจัดการให้อยู่ในกรอบของ Risk Appetite (ค่าความเสี่ยงโดยรวมที่องค์กรยินดีจะยอมรับเพื่อให้องค์กรบรรลุเป้าหมาย) และ Risk Tolerance (ระดับความเบี่ยงเบนจากเกณฑ์ที่ทำให้องค์กรมั่นใจว่าองค์กรได้ดำเนินการบริหารความเสี่ยงอยู่ภายในเกณฑ์ที่ยอมรับได้)

3. การบ่งชี้เหตุการณ์ (Event Identification)

ในกระบวนการบ่งชี้เหตุการณ์ ควรต้องพิจารณาปัจจัยความเสี่ยงทุกด้านที่อาจเกิดขึ้น เช่น ความเสี่ยงด้านกลยุทธ์ การเงินบุคลากร การปฏิบัติงาน กฎหมาย ภาษีอากร ระบบงาน สิ่งแวดล้อม ความสัมพันธ์ระหว่างเหตุการณ์ที่อาจเกิดขึ้นจากแหล่งความเสี่ยงทั้งจากสภาพแวดล้อมภายในและภายนอกองค์กร

4. การประเมินความเสี่ยง (Risk Assessment)

สำหรับการประเมินความเสี่ยงเป็นขั้นตอนที่จะต้องดำเนินการต่อจากการระบุความเสี่ยง โดยการประเมินความเสี่ยงประกอบด้วย 2 กระบวนการหลัก ได้แก่

4.1 การวิเคราะห์ความเสี่ยง

จะพิจารณาสาเหตุและแหล่งที่มาของความเสี่ยง ผลกระทบที่ตามมาทั้งในทางบวกและทางลบ รวมทั้งโอกาสที่อาจเกิดขึ้นของผลกระทบที่อาจตามมา โดยจะต้องมีการระบุถึงปัจจัยที่มีผลต่อผลกระทบและโอกาสที่จะเกิดขึ้น ทั้งนี้ เหตุการณ์หรือสถานการณ์หนึ่ง ๆ อาจจะเกิดผลที่ตามมาและกระทบต่อวัตถุประสงค์/เป้าหมายในหลากหลายด้าน นอกจากนั้นในการวิเคราะห์ควรพิจารณาถึงมาตรการจัดการความเสี่ยงที่ดำเนินการอยู่ในปัจจุบัน รวมถึงประสิทธิผลของมาตรการดังกล่าวด้วย

4.2 การประเมินความเสี่ยง

การประเมินความเสี่ยงจะเปรียบเทียบระหว่างระดับของความเสี่ยงที่ได้จากการวิเคราะห์ความเสี่ยง เทียบกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ในกรณีที่ระดับของความเสี่ยงไม่อยู่ในระดับที่ยอมรับได้ของเกณฑ์การยอมรับความเสี่ยง ความเสี่ยงดังกล่าวจะได้รับการจัดการทันที

5. การตอบสนองความเสี่ยง (Risk Response)

การกำหนดแผนจัดการความเสี่ยงจะมีการนำเสนอแผนจัดการความเสี่ยงที่จะดำเนินการต่อที่ผู้บริหารพิจารณาและขออนุมัติการจัดสรรทรัพยากรที่จำเป็นต้องใช้ดำเนินการ (ถ้ามี) โดยในการคัดเลือกแนวทางในการจัดการความเสี่ยงที่เหมาะสมที่สุดจะคำนึงถึงความเสี่ยงที่ยอมรับได้ (Risk Appetite) กับต้นทุนที่เกิดขึ้นเปรียบเทียบกับประโยชน์ที่จะได้รับ รวมถึงข้อกฎหมาย ระเบียบ กฎเกณฑ์ และข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

6. กิจกรรมการควบคุม (Control Activities)

กิจกรรมการควบคุม คือ นโยบายและกระบวนการปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้เพื่อป้องกันไม่ให้เกิดผลกระทบต่อเป้าหมายขององค์กร เนื่องจากแต่ละองค์กรมีการกำหนดวัตถุประสงค์และเทคนิคการนำไปปฏิบัติเป็นของเฉพาะองค์กร ดังนั้น กิจกรรมการควบคุมจึงมีความแตกต่างกัน ซึ่งอาจแบ่งได้เป็น 4 ประเภท คือ

6.1 การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

6.2 การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อให้ค้นพบข้อผิดพลาดที่ได้เกิดขึ้นแล้วตามกรอบการบริหารความเสี่ยงองค์กร (ERM Framework)

6.3 การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

6.4 การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้น และป้องกันไม่ให้เกิดซ้ำอีกในอนาคต

7. ข้อมูลและการติดต่อสื่อสาร (Information and Communication)

ข้อมูลสารสนเทศเป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ ประเมิน และจัดการความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กร ควรได้รับการบันทึกและสื่อสารไปยังบุคลากรในองค์กรอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อให้สามารถปฏิบัติงานตามหน้าที่และความรับผิดชอบได้ รวมถึงเป็นการรายงานการบริหารจัดการความเสี่ยง เพื่อให้ทุกคนในองค์กรได้รับทราบถึงความเสี่ยงที่เกิดขึ้น และผลของการบริหารจัดการความเสี่ยงเหล่านั้น

8. การติดตาม (Monitoring)

องค์กรควรมีการวิเคราะห์/ติดตามการเปลี่ยนแปลงของสภาพแวดล้อมทั้งภายในและภายนอก รวมถึงการเปลี่ยนแปลงในความเสี่ยงที่อาจเกิดขึ้น ซึ่งอาจส่งผลให้ต้องมีการทบทวนการจัดการความเสี่ยงและการจัดลำดับความสำคัญ รวมถึงอาจนำไปใช้ในการทบทวนกรอบการบริหารความเสี่ยงโดยรวม

หลักการบริหารจัดการความเสี่ยงระดับองค์กรสำหรับหน่วยงานของรัฐ

ตามที่กระทรวงการคลังได้มีการกำหนดหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 (หนังสือกระทรวงการคลัง ที่ กค 0409.4/ว 23 ลงวันที่ 19 มีนาคม 2562 เรื่อง หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562) ซึ่งมีรายละเอียดดังนี้

1. มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

1) หน่วยงานของรัฐต้องจัดให้มีการบริหารจัดการความเสี่ยง เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลแก่ผู้มีส่วนได้ส่วนเสียของหน่วยงานว่าหน่วยงานได้ดำเนินการบริหารจัดการความเสี่ยงอย่างเหมาะสม

2) ฝ่ายบริหารของหน่วยงานของรัฐต้องจัดให้มีสภาพแวดล้อมที่เหมาะสมต่อการบริหารจัดการความเสี่ยงภายในองค์กร อย่างน้อยประกอบด้วย การมอบหมายผู้รับผิดชอบเรื่องการบริหารจัดการความเสี่ยง การกำหนดวัฒนธรรมของหน่วยงานของรัฐที่ส่งเสริมการบริหารจัดการความเสี่ยง รวมถึงการบริหารทรัพยากรบุคคล

3) หน่วยงานของรัฐต้องมีการกำหนดวัตถุประสงค์เพื่อใช้ในการบริหารจัดการความเสี่ยงที่เหมาะสม รวมถึงมีการสื่อสารการบริหารจัดการความเสี่ยงของวัตถุประสงค์ด้านต่าง ๆ ต่อบุคลากรที่เกี่ยวข้อง

4) การบริหารจัดการความเสี่ยงต้องดำเนินการในทุกระดับของหน่วยงานของรัฐ

5) การบริหารจัดการความเสี่ยง อย่างน้อยประกอบด้วย การระบุความเสี่ยง การประเมินความเสี่ยง และการตอบสนองความเสี่ยง

6) หน่วยงานของรัฐต้องจัดทำแผนบริหารจัดการความเสี่ยงอย่างน้อยปีละครั้ง และต้องมีการสื่อสารแผนบริหารจัดการความเสี่ยงกับผู้ที่เกี่ยวข้องทุกฝ่าย

7) หน่วยงานของรัฐต้องมีการติดตามประเมินผลการบริหารจัดการความเสี่ยงและทบทวนแผนการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ

8) หน่วยงานของรัฐต้องมีการรายงานการบริหารจัดการความเสี่ยงของหน่วยงานต่อผู้ที่เกี่ยวข้อง

9) หน่วยงานของรัฐสามารถพิจารณานำเครื่องมือการบริหารความเสี่ยงที่เหมาะสมมาประยุกต์ใช้กับหน่วยงาน เพื่อให้การบริหารจัดการความเสี่ยงของหน่วยงานเกิดประสิทธิภาพสูงสุด

2. หลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

ด้วยพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 มาตรา 79 บัญญัติให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด ดังนั้น เพื่อให้เป็นไปตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 กระทรวงการคลังจึงได้กำหนดหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยง เพื่อให้หน่วยงานของรัฐใช้เป็นกรอบแนวทางในการบริหารจัดการความเสี่ยง โดยมีหลักเกณฑ์ ดังนี้

ข้อ 1 ในหลักเกณฑ์นี้ “หน่วยงานของรัฐ” หมายความว่า

(1) ส่วนราชการ

(2) รัฐวิสาหกิจ

(3) หน่วยงานของรัฐสภา ศาลยุติธรรม ศาลปกครอง ศาลรัฐธรรมนูญ องค์กรอิสระตามรัฐธรรมนูญ และองค์กรอัยการ

(4) องค์การมหาชน

(5) ทุนหมุนเวียนที่มีฐานะเป็นนิติบุคคล

(6) องค์กรปกครองส่วนท้องถิ่น

(7) หน่วยงานอื่นของรัฐตามที่กำหนด

“ผู้กำกับดูแล” หมายความว่า บุคคล หรือคณะบุคคล ผู้มีหน้าที่รับผิดชอบในการกำกับดูแลหรือบังคับบัญชาของหน่วยงานของรัฐ

“หัวหน้าหน่วยงานของรัฐ” หมายความว่า ผู้บริหารสูงสุดของหน่วยงานของรัฐ

“ฝ่ายบริหาร” หมายความว่า ผู้บริหารทุกระดับของหน่วยงานของรัฐ

“ผู้รับผิดชอบ” หมายความว่า คณะบุคคลหรือหน่วยงานที่ได้รับมอบหมายให้ทำหน้าที่เกี่ยวกับการบริหารจัดการความเสี่ยงของหน่วยงานของรัฐที่อยู่ภายใต้การบริหารจัดการของหัวหน้าหน่วยงานของรัฐ

“การบริหารจัดการความเสี่ยง” หมายความว่า กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน รวมถึงเพื่อเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

“ความเสี่ยง” หมายความว่า ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ของหน่วยงาน

ข้อ 2 ให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการความเสี่ยง โดยใช้มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐที่กระทรวงการคลังกำหนดเป็นแนวทางในการบริหารจัดการความเสี่ยง

ข้อ 3 ให้หน่วยงานของรัฐตามข้อ 1 (1) และ (3) – (7) ถือปฏิบัติตามคู่มือหรือแนวทางปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงตามที่กระทรวงการคลังกำหนดและสามารถนำคู่มือหรือแนวทางปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงอื่นมาประยุกต์ใช้กับหน่วยงาน และหน่วยงานของรัฐตามข้อ 1 (2) ถือปฏิบัติตามหลักเกณฑ์หรือแนวปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายในตามที่สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจกำหนด

ข้อ 4 ให้หน่วยงานของรัฐจัดให้มีผู้รับผิดชอบ ซึ่งต้องประกอบด้วยฝ่ายบริหาร และบุคลากรที่มีความรู้ความเข้าใจเกี่ยวกับการจัดทำยุทธศาสตร์และการบริหารจัดการความเสี่ยงของหน่วยงานของรัฐดำเนินการเกี่ยวกับการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ทั้งนี้ ไม่ควรเป็นผู้ตรวจสอบภายในของหน่วยงานของรัฐ

ข้อ 5 ผู้รับผิดชอบมีหน้าที่ ดังนี้

(1) จัดทำแผนการบริหารจัดการความเสี่ยง

(2) ติดตามประเมินผลการบริหารจัดการความเสี่ยง

(3) จัดทำรายงานผลตามแผนการบริหารจัดการความเสี่ยง

(4) พิจารณาทบทวนแผนการบริหารจัดการความเสี่ยง

ข้อ 6 ให้หน่วยงานของรัฐจัดทำแผนบริหารจัดการความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ของหน่วยงานของรัฐ

ข้อ 7 ให้หัวหน้าหน่วยงานของรัฐหรือผู้กำกับดูแลแล้วแต่กรณี กำกับดูแลฝ่ายบริหาร ผู้รับผิดชอบ และบุคลากรที่เกี่ยวข้องให้มีการบริหารจัดการความเสี่ยงให้เป็นไปตามแผนการบริหารจัดการความเสี่ยงที่กำหนดไว้

ข้อ 8 ให้ฝ่ายบริหารและผู้รับผิดชอบต้องจัดให้มีการติดตามประเมินผลการบริหารจัดการความเสี่ยง โดยติดตามประเมินผลอย่างต่อเนื่องในระหว่างการปฏิบัติงานหรือติดตามประเมินผลเป็นรายครั้ง หรือใช้ทั้งสองวิธีร่วมกัน กรณีพบข้อบกพร่องที่มีสาระสำคัญให้รายงานทันที

ข้อ 9 ให้ผู้รับผิดชอบของหน่วยงานของรัฐจัดทำรายงานผลการบริหารจัดการความเสี่ยงและเสนอให้หัวหน้าหน่วยงานของรัฐหรือผู้กำกับดูแลแล้วแต่กรณี พิจารณาอย่างน้อยปีละ 1 ครั้ง

ข้อ 10 หัวหน้าหน่วยงานของรัฐหรือผู้กำกับดูแลแล้วแต่กรณี สามารถกำหนดนโยบาย วิธีการและระยะเวลาการรายงานการบริหารจัดการความเสี่ยง

ข้อ 11 กรณีกรมบัญชีกลางขอให้หน่วยงานของรัฐ ตามข้อ 1 (1) และ (3) – (7) และสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจขอให้หน่วยงานของรัฐ ตามข้อ 1 (2) จัดส่งรายงานแผนการบริหารจัดการความเสี่ยง ตามข้อ 6 และรายงานผลการบริหารจัดการความเสี่ยง ตามข้อ 9 หรือข้อมูลอื่น ๆ

เพิ่มเติม เกี่ยวกับกระบวนการบริหารจัดการความเสี่ยง ให้หน่วยงานของรัฐดังกล่าวดำเนินการตามรูปแบบ วิธีการ และระยะเวลาที่กรมบัญชีกลาง หรือสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจกำหนด

ข้อ 12 กรณีหน่วยงานของรัฐไม่สามารถปฏิบัติตามหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐได้ให้ขอทำความตกลงกับกระทรวงการคลัง

ข้อ 13 หน่วยงานของรัฐที่ได้ดำเนินการหรืออยู่ระหว่างการบริหารจัดการความเสี่ยงให้ดำเนินการต่อไปจนกว่าจะแล้วเสร็จ และให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงฉบับนี้ในรอบระยะเวลาบัญชีถัดไป สำหรับหน่วยงานของรัฐที่ยังไม่ได้ดำเนินการบริหารจัดการความเสี่ยงให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงฉบับนี้ในรอบระยะเวลาบัญชีถัดไป

3. แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

กระทรวงการคลัง ได้กำหนดแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ (หนังสือกระทรวงการคลัง ที่ กค 0409.3/ว 36 ลงวันที่ 3 กุมภาพันธ์ 2564 เรื่อง แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ) ดังนี้

หลักการบริหารจัดการความเสี่ยงระดับองค์กรการบริหารจัดการความเสี่ยงถือเป็นส่วนหนึ่งของการบริหารองค์กรอย่างมีธรรมาภิบาล โดยปัจจัยหลักของการบริหารจัดการความเสี่ยงที่ประสบความสำเร็จเกิดจากการความมุ่งมั่นของหัวหน้าหน่วยงานของรัฐและผู้กำกับดูแล โดยหลักการบริหารจัดการความเสี่ยงระดับองค์กร แบ่งออกเป็น 2 ส่วน ประกอบด้วย

1. กรอบการบริหารจัดการความเสี่ยง เป็นพื้นฐานของการบริหารจัดการความเสี่ยงที่ดีเพื่อให้การบริหารจัดการความเสี่ยงเป็นเครื่องมือช่วยหน่วยงานในการกำหนดแผนระดับองค์กร (Strategic Plans) และการกำหนดวัตถุประสงค์เป็นไปอย่างมีประสิทธิผล รวมถึงการตัดสินใจของผู้บริหารอยู่บนฐานข้อมูลสารสนเทศที่สมบูรณ์ ส่งผลให้หน่วยงานของรัฐสามารถดำเนินงานบรรลุวัตถุประสงค์หลักขององค์กร และเพื่อเพิ่มศักยภาพและขีดความสามารถของหน่วยงาน

2. กระบวนการบริหารจัดการความเสี่ยง เป็นกระบวนการที่เกิดขึ้นอย่างต่อเนื่อง (Routine Processes) ของการบริหารจัดการความเสี่ยง ซึ่งตั้งอยู่บนพื้นฐานของกรอบการบริหารจัดการความเสี่ยงของหน่วยงาน

กรอบการบริหารจัดการความเสี่ยงเป็นพื้นฐานที่สำคัญในการบริหารจัดการความเสี่ยงหน่วยงานของรัฐ ควรพิจารณานำกรอบการบริหารจัดการความเสี่ยงนี้ไปปรับใช้ในการวางระบบการบริหารจัดการความเสี่ยงของหน่วยงาน เพื่อให้หน่วยงานได้รับประโยชน์สูงสุดจากการบริหารจัดการความเสี่ยงอย่างแท้จริง โดยหน่วยงานของรัฐแต่ละแห่งอาจมีศักยภาพที่แตกต่างกันในการนำกรอบการบริหารจัดการความเสี่ยงทั้งหมดไปปรับใช้ ทั้งนี้ ขึ้นอยู่กับความพร้อมของหน่วยงาน กรอบบริหารจัดการความเสี่ยง ประกอบด้วย หลักการ 8 ประการ ดังนี้

1) การบริหารจัดการความเสี่ยงต้องดำเนินการแบบบูรณาการทั่วทั้งองค์กร

2) ความมุ่งมั่นของผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ และผู้บริหารระดับสูง

3) การสร้างและรักษาบุคลากรและวัฒนธรรมที่ดีขององค์กร

4) การมอบหมายหน้าที่ความรับผิดชอบด้วยการบริหารจัดการความเสี่ยง

5) การตระหนักถึงผู้มีส่วนได้ส่วนเสีย

6) การกำหนดยุทธศาสตร์/กลยุทธ์ วัตถุประสงค์ และการตัดสินใจ

7) การใช้ข้อมูลสารสนเทศ

8) การพัฒนาอย่างต่อเนื่อง

<u>การบริหารจัดการความเสี่ยงต้องดำเนินการแบบบูรณาการทั่วทั้งองค์กร</u>

การบริหารจัดการความเสี่ยงแบบบูรณาการควรมีลักษณะ ดังนี้

1) การบริหารจัดการความเสี่ยงต้องมีการบริหารจัดการในภาพรวมมากกว่าแยกเดี่ยว เนื่องจากความเสี่ยงของกิจกรรมหนึ่งอาจมีผลกระทบต่อความเสี่ยงของกิจกรรมอื่น ๆ เช่น ความเสี่ยงของความล่าช้าในระบบการขนส่งวัตถุดิบไม่เพียงกระทบต่อกิจกรรมการผลิต อาจมีผลกระทบด้านการส่งมอบสินค้า ค่าปรับที่อาจจะเกิดขึ้น รวมถึงชื่อเสียงขององค์กร เป็นต้น

2) การบริหารความเสี่ยงควรผนวกเข้าเป็นส่วนหนึ่งของการดำเนินงานขององค์กรรวมถึงกระบวนการจัดทำแผนกลยุทธ์ และกระบวนการประเมินผล

3) การบริหารจัดการความเสี่ยงต้องช่วยสนับสนุนกระบวนการตัดสินใจในทุกระดับขององค์กร

<u>ความมุ่งมั่นของผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ และผู้บริหารระดับสูง</u>

การบริหารจัดการความเสี่ยงจะประสบความสำเร็จขึ้นอยู่กับความมุ่งมั่นของผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ และผู้บริหารระดับสูง หน่วยงานของรัฐบางแห่งมีผู้กำกับดูแลในรูปแบบคณะกรรมการซึ่งมีหน้าที่ในการกำกับฝ่ายบริหารให้มีการบริหารจัดการตามหลักธรรมาภิบาล ผู้กำกับดูแลซึ่งมีหน้าที่ดังกล่าวจะมีหน้าที่ในการกำกับการบริหารจัดการความเสี่ยงด้วย สำหรับหัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงมีหน้าที่ความรับผิดชอบในการบริหารจัดการความเสี่ยง การกำกับการบริหารจัดการความเสี่ยงเป็นกระบวนการที่ทำให้ผู้กำกับดูแลเกิดความมั่นใจว่า หัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงได้บริหารจัดการความเสี่ยงอย่างเหมาะสมเพียงพอ และมีประสิทธิผล หัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงมีหน้าที่โดยตรงในการสร้างระบบบริหารจัดการความเสี่ยงที่มีประสิทธิผล ประกอบด้วย การสร้างสภาพแวดล้อม วัฒนธรรมองค์กร และระบบการบริหารบุคคลที่เหมาะสม การจัดสรรทรัพยากรที่เพียงพอในการบริหารจัดการความเสี่ยง การดำเนินงานตามกระบวนการบริหารจัดการความเสี่ยง การพัฒนาระบบข้อมูลสารสนเทศ การรายงานและการสื่อสาร เป็นต้น

ผู้กำกับดูแล (ถ้ามี) อาจตั้งคณะกรรมการบริหารจัดการความเสี่ยง (หรืออนุกรรมการหรือคณะที่ปรึกษา) ขึ้น ซึ่งประกอบด้วยผู้มีทักษะ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการดำเนินงานของหน่วยงาน เช่น หน่วยงานที่มีการใช้ระบบเทคโนโลยีสารสนเทศเป็นหลัก ในการดำเนินงานอาจจำเป็นต้องมีผู้เชี่ยวชาญอิสระในการกำกับหรือให้ความเห็นเกี่ยวกับความเพียงพอและความเหมาะสมของการบริหารจัดการความเสี่ยงในเรื่องความเสี่ยงทางไซเบอร์ของหัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูง เป็นต้น

การสร้างและรักษาบุคลากรและวัฒนธรรมที่ดีขององค์กร

การขับเคลื่อนหน่วยงานของรัฐต้องอาศัยบุคลากรที่มีศักยภาพ การบริหารทรัพยากรบุคคลเริ่มตั้งแต่การสรรหา การพัฒนาบุคลากรให้มีความรู้ความสามารถ การส่งเสริมและรักษาไว้ซึ่งบุคลากรที่มีความรู้ความสามารถ โดยบุคลากรถือว่าเป็นสินทรัพย์หลักขององค์กรที่ทำให้องค์กรประสบความสำเร็จ การสร้างบุคลากรให้มีความรู้และทักษะในการบริหารจัดการความเสี่ยงถือเป็นส่วนหนึ่งของการบริหารจัดการความเสี่ยง บุคลากรควรมีพฤติกรรมตระหนักถึงความเสี่ยง (Risk-aware behavior) รวมถึงพฤติกรรมการตัดสินใจโดยใช้ข้อมูลสารสนเทศและข้อมูลการบริหารจัดการความเสี่ยง การสร้างพฤติกรรมที่ดี (Desired behaviors) ในการส่งเสริมการบริหารจัดการความเสี่ยงผ่านวัฒนธรรมที่ดีขององค์กรเป็นสิ่งสำคัญ การสร้างวัฒนธรรมที่สนับสนุนการบริหารจัดการความเสี่ยง ประกอบด้วย

1) การสื่อสารและตระหนักถึงนโยบายการบริหารจัดการความเสี่ยงของหน่วยงาน
2) การสร้างความตระหนักถึงหน้าที่ต่อองค์กรในการแจ้งข้อมูลผิดปกติ
3) การสร้างพฤติกรรมการแบ่งปันข้อมูลภายในองค์กร
4) การสร้างพฤติกรรมการตัดสินใจตามนโยบายการบริหารจัดการความเสี่ยง
5) การสร้างพฤติกรรมการตระหนักถึงความเสี่ยงและโอกาส

การมอบหมายหน้าที่ความรับผิดชอบด้วยการบริหารจัดการความเสี่ยง

หน่วยงานควรมีการกำหนดอำนาจ หน้าที่ ความรับผิดชอบในเรื่องของการบริหารจัดการความเสี่ยงอย่างชัดเจนและเหมาะสม ประกอบด้วย เจ้าของความเสี่ยง (Risk Owners) ซึ่งรับผิดชอบในการติดตาม การรายงาน หรือการส่งสัญญาณความเสี่ยง ผู้รับผิดชอบในการตัดสินใจในกรณีที่ความเสี่ยงเกิดขึ้นในระดับที่กำหนดไว้ และผู้ที่มีหน้าที่ในการควบคุมกำกับติดตามให้มีการบริหารจัดการความเสี่ยงตามแผนการบริหารจัดการความเสี่ยง

การตระหนักถึงผู้มีส่วนได้ส่วนเสีย

การบริหารจัดการความเสี่ยงนอกจากจะคำนึงถึงวัตถุประสงค์ขององค์กรเป็นหลักแล้ว ผู้บริหารต้องคำนึงถึงผู้มีส่วนได้ส่วนเสียในการบริหารจัดการความเสี่ยงด้วย โดยเฉพาะความคาดหวังของผู้รับบริการ หรือความคาดหวังของประชาชนที่มีต่อองค์กร รวมถึงผลกระทบที่มีต่อสังคม เศรษฐกิจ และสภาพแวดล้อม

การกำหนดยุทธศาสตร์/กลยุทธ์ วัตถุประสงค์ และการตัดสินใจ

การบริหารจัดการความเสี่ยงเป็นเครื่องมือช่วยผู้บริหารในการกำหนดยุทธศาสตร์/กลยุทธ์ขององค์กร เพื่อให้หน่วยงานมั่นใจว่ายุทธศาสตร์/กลยุทธ์ขององค์กรสอดคล้องกับพันธกิจตามกฎหมายและหน้าที่ความรับผิดชอบของหน่วยงาน ยุทธศาสตร์/กลยุทธ์อาจหมายรวมถึงแผนปฏิบัติราชการระยะยาว แผนปฏิบัติราชการระยะปานกลาง หรือแผนปฏิบัติราชการประจำปีของหน่วยงาน เมื่อหน่วยงานของรัฐกำหนดยุทธศาสตร์/กลยุทธ์โดยสอดคล้องกับความเสี่ยงที่ยอมรับได้ระดับองค์กรแล้ว การบริหารจัดการความเสี่ยงจะถูกใช้เป็นเครื่องมือในการกำหนดทางเลือกของงาน/โครงการ (งานใหม่ ๆ) และการกำหนดวัตถุประสงค์ระดับการปฏิบัติงาน รวมถึงการมอบหมายความรับผิดชอบในการบริหารจัดการความเสี่ยงทั่วทั้งองค์กร โดยอาจกำหนดเป็นส่วนหนึ่งของตัวชี้วัดผลการปฏิบัติงาน (KPI)

การใช้ข้อมูลสารสนเทศ

ในปัจจุบันข้อมูลสารสนเทศเป็นสิ่งสำคัญอย่างยิ่งในการดำเนินงานของหน่วยงาน องค์กรที่มีการบริหารจัดการข้อมูลสารสนเทศอย่างมีประสิทธิภาพส่งผลโดยตรงต่อการบริหารจัดการความเสี่ยง หน่วยงานควรพิจารณาใช้ข้อมูลสารสนเทศในการบริหารจัดการความเสี่ยง เพื่อให้ผู้บริหารสามารถตัดสินใจโดยใช้ข้อมูลความเสี่ยงเป็นพื้นฐาน หน่วยงานควรกำหนดประเภทข้อมูลที่ต้องรวบรวมวิธีการรวบรวมและการวิเคราะห์ข้อมูล และบุคคลที่ควรได้รับข้อมูล

ข้อมูลความเสี่ยง ประกอบด้วย เหตุการณ์ที่เป็นผลกระทบทางลบหรือทางบวกต่อองค์กร สาเหตุความเสี่ยง ตัวผลักดันความเสี่ยง หรือตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators) ข้อมูลสารสนเทศต้องมีความถูกต้อง เชื่อถือได้ เกี่ยวข้องกับการตัดสินใจและทันต่อเวลา ทั้งนี้ หน่วยงานอาจพิจารณาการวบรวม การประมวลผล หรือการวิเคราะห์ความเสี่ยงแบบอัตโนมัติ เพื่อลดข้อผิดพลาดจากบุคคล (Human errors)

การพัฒนาอย่างต่อเนื่อง

การบริหารจัดการความเสี่ยงต้องมีการพัฒนาอย่างต่อเนื่อง ความสมบูรณ์ของระบบบริหารจัดการความเสี่ยงอยู่กับขนาดโครงสร้าง ศักยภาพขององค์กร รวมถึงการใช้ระบบสารสนเทศในการบริหารจัดการความเสี่ยง หน่วยงานอาจพิจารณาทำ Benchmarking เพื่อพัฒนาระบบบริหารจัดการความเสี่ยงขององค์กรอย่างต่อเนื่อง หน่วยงานอาจพัฒนาระบบการบริหารจัดการความเสี่ยงเริ่มต้นจากการบริหารจัดการความเสี่ยงแบบ Silo พัฒนาเป็นการบริหารจัดการความเสี่ยงแบบบูรณาการและพัฒนาต่อเนื่องโดยมีการบริหารจัดการความเสี่ยงเข้าสู่กระบวนการการดำเนินงานโดยปกติของดำเนินงานและการตัดสินใจบนพื้นฐานข้อมูลด้านความเสี่ยง

4. กระบวนการบริหารจัดการความเสี่ยง

กระบวนการบริหารจัดการความเสี่ยงเป็นกระบวนการที่เป็นวงจรต่อเนื่อง ประกอบด้วย

1) การวิเคราะห์องค์กร
2) การกำหนดนโยบายการบริหารจัดการความเสี่ยง
3) การระบุความเสี่ยง
4) การประเมินความเสี่ยง
5) การตอบสนองความเสี่ยง
6) การติดตามและทบทวน
7) การสื่อสารและการรายงาน

การวิเคราะห์องค์กร

ในการวิเคราะห์องค์กรหน่วยงานต้องเข้าใจเกี่ยวกับพันธกิจตามกฎหมาย อำนาจหน้าที่และความรับผิดชอบของหน่วยงาน รวมถึงยุทธศาสตร์ชาติ ยุทธศาสตร์ระดับกระทรวง รวมถึงนโยบายของรัฐบาลที่เกี่ยวข้องกับหน่วยงาน โดยการวิเคราะห์องค์กรต้องวิเคราะห์ทั้งปัจจัยภายในและปัจจัยภายนอกองค์กร หน่วยงานอาจเลือกใช้เครื่องมือการวิเคราะห์องค์กร เช่น 1) SWOT Analysis เป็นการ

วิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค 2) PESTLE Analysis เป็นการวิเคราะห์ด้านการเมือง (Political) ด้านเศรษฐกิจ (Economic) ด้านสังคม (Social) ด้านเทคโนโลยี (Technological) ด้านกฎหมาย (Legal) และด้านสภาพแวดล้อม (Environmental)

การกำหนดนโยบายการบริหารจัดการความเสี่ยง

ผู้บริหารเป็นผู้กำหนดนโยบายบริหารจัดการความเสี่ยง และผู้กำกับดูแลเป็นผู้ให้ความเห็นชอบนโยบายดังกล่าว โดยนโยบายการบริหารจัดการความเสี่ยงอาจระบุถึงวัตถุประสงค์ของการบริหารจัดการความเสี่ยง บทบาทหน้าที่ความรับผิดชอบของการบริหารจัดการความเสี่ยง และความเสี่ยงที่ยอมรับได้ระดับองค์กร ความเสี่ยงที่ยอมรับได้ระดับองค์กร (Risk Appetite) หมายถึง ระดับความเสี่ยงในภาพรวมขององค์กรที่หน่วยงานยอมรับเพื่อดำเนินงานให้บรรลุวัตถุประสงค์ขององค์กร การระบุความเสี่ยงที่ยอมรับได้ระดับองค์กรเป็นการแสดงเจตนารมณ์ของผู้บริหารและผู้กำกับดูแลในการดำเนินงานขององค์กร การกำหนดความเสี่ยงที่ยอมรับได้ควรคำนึงถึงศักยภาพขององค์กรในเรื่องการจัดการความเสี่ยง โดยศักยภาพในการจัดการความเสี่ยงขององค์กร (Risk Capacity) ขึ้นอยู่กับงบประมาณ บุคลากร และความคาดหวังของผู้มีส่วนได้ส่วนเสีย ทั้งนี้ หน่วยงานอาจระบุระดับความเสี่ยงที่ยอมรับได้เป็น 5 ระดับ เช่น ปฏิเสธความเสี่ยง ยอมรับความเสี่ยงได้น้อย ยอมรับความเสี่ยงได้ปานกลาง เต็มใจยอมรับความเสี่ยง และยอมรับความเสี่ยงได้มากที่สุด เป็นต้น หน่วยงานอาจแสดงนโยบายความเสี่ยงที่ยอมรับได้ในแต่ละประเภทความเสี่ยง เพื่อให้ผู้บริหารระดับรองลงมาสามารถนำไปใช้ในการบริหารจัดการความเสี่ยงในระดับสำนัก กอง ศูนย์ สถาบัน กลุ่ม หรือนำไปสู่การระบุระดับความเสี่ยงที่ยอมรับได้สำหรับประเภทความเสี่ยงย่อย

การระบุความเสี่ยง

การระบุความเสี่ยง คือ การระบุเหตุการณ์ที่อาจเกิดขึ้นที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงานทั้งในด้านบวกและด้านลบ ในการระบุความเสี่ยงหน่วยงานอาจทำรายชื่อความเสี่ยงทั้งหมด (Risk Inventory) โดยรายชื่อความเสี่ยงต้องมีการปรับปรุงอย่างสม่ำเสมอโดยอาศัยข้อมูลที่เป็นปัจจุบัน การระบุความเสี่ยงหน่วยงานควรระบุข้อมูลเกี่ยวกับความเสี่ยง ดังนี้

ก. เหตุการณ์ความเสี่ยง

ข. สาเหตุของความเสี่ยง หรือตัวผลักดันความเสี่ยง โดยการวิเคราะห์ถึงสาเหตุที่แท้จริง (Root Cause) ของความเสี่ยง

ค. ผลกระทบทั้งด้านลบและ/หรือด้านบวก

หน่วยงานอาจจัดกลุ่มความเสี่ยงที่มีลักษณะหรือผลกระทบที่เหมือนกันไว้ในประเภทความเสี่ยงเดียวกัน เพื่อให้การพิจารณาและการบริหารจัดการความเสี่ยงประเภทเดียวกันมีมุมมองในภาพรวมชัดเจนมากขึ้น

การประเมินความเสี่ยง

การประเมินความเสี่ยง ประกอบด้วย

1) การกำหนดเกณฑ์การประเมินความเสี่ยง หน่วยงานอาจให้คะแนนความเสี่ยงตามเกณฑ์การประเมินความเสี่ยงด้านต่าง ๆ เช่น ด้านโอกาส ด้านผลกระทบ รวมถึงด้านความสามารถขององค์กรในการจัดการความเสี่ยง และด้านลักษณะของความเสี่ยง โดยช่วงคะแนนอาจกำหนดเป็น 3 ช่วงคะแนน หรือ 5 ช่วงคะแนน

2) การให้คะแนนความเสี่ยง วิธีการให้คะแนนความเสี่ยง เช่น การสัมภาษณ์ การทำแบบสำรวจ การประชุมเชิงปฏิบัติการระหว่างหน่วยงานภายใน การทำ Benchmarking การวิเคราะห์สถานการณ์ (Scenario Analysis) ทั้งนี้ การให้คะแนนความเสี่ยงของแต่ละกองงาน (Silo Thinking) เพียงวิธีเดียวอาจทำให้การให้คะแนนความเสี่ยงมีความคาดเคลื่อนได้

3) การพิจารณาความเสี่ยงในภาพรวม เมื่อหน่วยงานประเมินความเสี่ยงในแต่ละความเสี่ยงที่มีต่อวัตถุประสงค์ของกิจกรรมแล้ว หน่วยงานต้องพิจารณาผลกระทบของความเสี่ยงที่มีต่อวัตถุประสงค์ในระดับกลุ่ม และผลกระทบที่มีต่อหน่วยงานในภาพรวม เช่น ผลกระทบต่อความเสี่ยงที่มีต่อกิจกรรมอาจมีน้อยแต่มีผลกระทบต่อวัตถุประสงค์ระดับกอง หรือความเสี่ยง 2 ความเสี่ยงที่ไม่มีผลกระทบต่อกิจกรรมอาจมีผลกระทบต่อหน่วยงานในภาพรวม เป็นต้น

4) การจัดลำดับความเสี่ยง เมื่อหน่วยงานพิจารณาให้คะแนนความเสี่ยงแล้ว หน่วยงานต้องจัดลำดับความเสี่ยงเพื่อนำไปสู่การพิจารณาจัดสรรทรัพยากรในการตอบสนองความเสี่ยง หน่วยงานอาจใช้คะแนนความเสี่ยง (โอกาส x ผลกระทบ) ในการจัดลำดับความเสี่ยง โดยความเสี่ยงที่เท่ากันอาจพิจารณาปัจจัยอื่นประกอบ เช่น ความสามารถของหน่วยงานในการบริหารจัดการความเสี่ยงด้านนั้น ๆ หรือลักษณะของความเสี่ยงที่มีผลกระทบต่อหน่วยงาน เป็นต้น

การตอบสนองความเสี่ยง

การตอบสนองความเสี่ยง คือ กระบวนการตัดสินใจของฝ่ายบริหารในการจัดการความเสี่ยงที่อาจจะเกิดขึ้น โดยผู้บริหารควรพิจารณาประเด็นดังต่อไปนี้ ในการตัดสินใจเลือกวิธีการตอบสนองความเสี่ยงเพื่อจัดทำแผนบริหารจัดการความเสี่ยงของหน่วยงาน

1. การจัดการต้นเหตุของความเสี่ยง
2. ทางเลือกวิธีการจัดการความเสี่ยง
3. ทรัพยากรที่ต้องใช้ในการบริหารจัดการความเสี่ยง หน่วยงานสามารถพิจารณาเลือกวิธีการจัดการความเสี่ยงวิธีใดวิธีหนึ่งหรือหลายวิธี โดยการพิจารณาวิธีการจัดการความเสี่ยงควรคำนึงถึงต้นทุนกับประโยชน์ที่ได้รับของวิธีการจัดการความเสี่ยงแต่ละวิธี

ตัวอย่างวิธีการจัดการความเสี่ยง ประกอบด้วย

1) ปฏิเสธความเสี่ยงโดยไม่ดำเนินงานในกิจกรรมที่มีความเสี่ยง ได้แก่ กิจกรรมที่มีความเสี่ยงสูงและหน่วยงานไม่สามารถยอมรับความเสี่ยงนั้นได้ หน่วยงานอาจพิจารณาไม่ดำเนินงานในกิจกรรมนั้น ๆ

2) การลดโอกาสของความเสี่ยง เช่น การลดโอกาสของความเสี่ยงการทุจริตด้านการเงิน โดยการวางระบบการควบคุมภายใน ได้แก่ การแบ่งแยกหน้าที่ การตรวจสอบ การสอบทาน และการทบยอด เป็นต้น

3) การลดผลกระทบของความเสี่ยง เช่น การทำประกัน หรือการใช้เครื่องมือป้องกันความเสี่ยงทางการเงิน (Hedging Instruments) เป็นต้น

4) การโอนความเสี่ยง หน่วยงานอาจเลือกใช้วิธีการถ่ายโอนความเสี่ยงของกิจกรรมที่หน่วยงานเห็นว่าควรดำเนินการเพื่อประโยชน์ของประชาชน แต่หน่วยงานมีข้อจำกัดที่ไม่สามารถดำเนินการเองได้หรือไม่สามารถบริหารจัดการความเสี่ยงได้ ได้แก่ การให้ภาคเอกชนดำเนินการโดยมีการโอนความเสี่ยงและผลตอบแทนไปด้วย (Public Private Partnership: PPP) เป็นต้น

5) ยอมรับความเสี่ยงโดยไม่ดำเนินการจัดการความเสี่ยง เนื่องจากความเสี่ยงอยู่ในระดับที่หน่วยงานยอมรับได้ หรือต้นทุนในการบริหารจัดการความเสี่ยงมีมากกว่าประโยชน์ที่ได้รับ

6) ใช้มาตรการการเฝ้าระวัง หน่วยงานต้องกำหนดข้อมูลที่ต้องมีการเก็บรวบรวม การวิเคราะห์ การแจ้งเตือน และการดำเนินการเมื่อเหตุการณ์เกิดขึ้น เช่น ความเสี่ยงของปริมาณน้ำในเขื่อนมากเนื่องจากปริมาณน้ำฝน

7) การทำแผนฉุกเฉิน การจัดทำแผนฉุกเฉินเป็นการระบุขั้นตอนเมื่อเกิดเหตุการณ์ความเสี่ยงขึ้น โดยต้องระบุบุคคลและวิธีการดำเนินการที่ชัดเจน เช่น ความเสี่ยงกรณีที่เจ้าหน้าที่ไม่สามารถเข้าสถานที่ทำงานได้

8) การส่งเสริมหรือผลักดันเหตุการณ์ที่อาจจะเกิดขึ้น เมื่อเหตุการณ์ที่อาจจะเกิดขึ้นส่งผลกระทบเชิงบวกกับองค์กร รวมถึงกำหนดแผนการดำเนินงานเมื่อเหตุการณ์เกิดขึ้น แผนการบริหารจัดการความเสี่ยงอาจประกอบด้วย วิธีการจัดการความเสี่ยง บุคคลที่รับผิดชอบในการบริหารจัดการความเสี่ยง ตัวชี้วัดความเสี่ยงที่สำคัญ วิธีการติดตามและการรายงานความเสี่ยง

<u>การติดตามและทบทวน</u>

การติดตามและทบทวนเป็นกระบวนการที่ให้ความเชื่อมั่นว่าการบริหารจัดการความเสี่ยงที่มีอยู่ยังคงมีประสิทธิผล เนื่องจากความเสี่ยงเป็นสิ่งที่เกิดขึ้นและเปลี่ยนแปลงตลอดเวลา ดังนั้น การติดตามและทบทวนเป็นกระบวนการที่เกิดขึ้นสม่ำเสมอ ปัจจัยที่ทำให้หน่วยงานต้องทบทวนการบริหารจัดการความเสี่ยง ได้แก่ การเปลี่ยนแปลงที่สำคัญซึ่งเกิดจากปัจจัยภายในและภายนอกหรือผลการดำเนินงานไม่เป็นไปตามเป้าหมายที่กำหนดไว้ การติดตามและทบทวนการบริหารจัดการความเสี่ยงสามารถดำเนินการอย่างต่อเนื่อง หรือเป็นระยะซึ่งควรดำเนินการในทุกกระบวนการของการบริหารจัดการความเสี่ยง การติดตาม และทบทวนอาจนำไปสู่การเปลี่ยนแปลงของแผนการปฏิบัติงานขององค์กร การเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ รวมถึงการพัฒนาระบบบริหารจัดการความเสี่ยง

<u>การสื่อสารและการรายงาน</u>

การสื่อสารเป็นการสร้างความตระหนัก ความเข้าใจ และการมีส่วนร่วมของกระบวนการบริหารจัดการความเสี่ยง การสื่อสารเป็นการให้และรับข้อมูล (Two – way Communication) หน่วยงานควรมีช่องทางการสื่อสารทั้งภายในและภายนอก โดยการสื่อสารภายในต้องเป็นการสื่อสาร

แบบจากผู้บริหารไปยังผู้ใต้บังคับบัญชา (Top Down) จากผู้ใต้บังคับบัญชาไปยังผู้บริหาร (Bottom Up) และระหว่างหน่วยงานย่อยภายใน (Across Divisions) หน่วยงานควรกำหนดบุคคลที่ควรได้รับข้อมูล ประเภทของข้อมูลที่ควรได้รับ ความถี่ของการรายงาน รูปแบบและวิธีการรายงาน เพื่อให้ผู้กำกับดูแล ผู้บริหาร และผู้มีส่วนได้ส่วนเสียได้รับข้อมูลสารสนเทศที่ถูกต้อง ครบถ้วน เกี่ยวข้องกับการตัดสินใจและทันต่อเวลา การสื่อสารและรายงานต่อผู้กำกับดูแล เป็นการสื่อสารและการรายงานความเสี่ยงในภาพรวมขององค์กร เพื่อสนับสนุนหน้าที่ของผู้กำกับดูแลในการกำกับการบริหารจัดการความเสี่ยงของฝ่ายบริหาร หน่วยงานอาจพิจารณากำหนดตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators) เพื่อติดตามข้อมูลความเสี่ยงและการรายงานเมื่อระดับความเสี่ยงถึงจุดตัวชี้วัดความเสี่ยงที่สำคัญ

ประเภทความเสี่ยง

1. ความเสี่ยงด้านยุทธศาสตร์/กลยุทธ์ (Strategic Risk : S) เกี่ยวข้องกับการบรรลุเป้าหมายและพันธกิจในภาพรวม โดยความเสี่ยงที่อาจจะเกิดขึ้นเป็นความเสี่ยงเนื่องจากการเปลี่ยนแปลงของสถานการณ์ เหตุการณ์ หรือปัจจัยภายนอก หรือความเสี่ยงจากกลยุทธ์ที่กำหนดไว้ไม่สอดคล้องกับประเด็นยุทธศาสตร์/วิสัยทัศน์ หรือเกิดจากการกำหนดกลยุทธ์ที่ขาดการมีส่วนร่วมจากบุคลากรภายในองค์กร ทำให้กลยุทธ์หรือโครงการขาดการยอมรับ และโครงการไม่ได้นำไปสู่การแก้ไขปัญหาหรือการตอบสนองต่อความต้องการของผู้บริหารหรือผู้มีส่วนได้ส่วนเสียอย่างแท้จริง หรือเป็นความเสี่ยงที่เกิดขึ้นจากการตัดสินใจผิดพลาดหรือนำการตัดสินใจนั้นมาใช้อย่างไม่ถูกต้อง

2. ความเสี่ยงด้านการดำเนินงาน (Operational Risk: O) เกี่ยวข้องกับประสิทธิภาพประสิทธิผลหรือผลการปฏิบัติงาน โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยงเนื่องจากระบบงานภายในขององค์กร/กระบวนการ/เทคโนโลยีหรือนวัตกรรมที่ใช้/บุคลากร/ความเพียงพอของข้อมูล ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินโครงการ

3. ความเสี่ยงด้านการเงิน (Financial Risk: F) เป็นความเสี่ยงเกี่ยวกับการบริหารงบประมาณและการเงิน เช่น การบริหารการเงินไม่ถูกต้อง ไม่เหมาะสม ทำให้ขาดประสิทธิภาพ และไม่ทันต่อสถานการณ์หรือเป็นความเสี่ยงที่เกี่ยวข้องกับการเงินขององค์กร เช่น การประมาณการงบประมาณไม่เพียงพอและไม่สอดคล้องกับขั้นตอนการดำเนินการ เป็นต้น ซึ่งสาเหตุอาจเกิดจากการขาดการจัดหาข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงานเพื่อนำมาใช้ในการบริหารงบประมาณและการเงินดังกล่าว

4. ความเสี่ยงด้านการปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับต่าง ๆ (Compliance Risk : C) เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบต่าง ๆ โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยงเนื่องจากความไม่ชัดเจน ความไม่ทันสมัย หรือความไม่ครอบคลุมของกฎหมาย กฎระเบียบ ข้อบังคับต่าง ๆ

ความหมายองค์ประกอบตามหลักธรรมาภิบาล

ในการวิเคราะห์ความเสี่ยงของสำนักงานเลขาธิการวุฒิสภานั้น ได้มีการพิจารณาปัจจัยความเสี่ยงในด้านต่าง ๆ รวมถึงได้มีการนำแนวคิดเรื่องธรรมาภิบาลที่เกี่ยวข้องในแต่ละด้านมาเป็นปัจจัยในการวิเคราะห์ความเสี่ยงด้วย โดยเป็นความเสี่ยงเรื่องธรรมาภิบาลที่อาจเกิดขึ้นจากการดำเนินแผนงาน/โครงการ เพื่อให้เป็นไปตามหลักธรรมาภิบาล (Good Governance) ประกอบด้วย

1. ประสิทธิผล (Effetiveness)
2. ประสิทธิภาพ (Efficiency)
3. การมีส่วนร่วม (Participation)
4. ความโปร่งใส (Transparency)
5. การตอบสนอง (Responsiveness)
6. ภาระรับผิดชอบ (Accountability)
7. นิติธรรม (Rule of Law)
8. การกระจายอำนาจ (DecentraliZation)
9. ความเสมอภาค (Equity)

หลักประสิทธิผล (Effetiveness) : หมายถึง ผลการปฏิบัติราชการที่บรรลุวัตถุประสงค์และเป้าหมายของแผนปฏิบัติราชการตามที่ได้รับงบประมาณมาดำเนินการ รวมถึงความสามารถเมื่อเทียบเคียงกับส่วนราชการหรือหน่วยงานที่มีภารกิจคล้ายคลึงกัน โดยการปฏิบัติราชการจะต้องมีทิศทาง ยุทธศาสตร์ และเป้าประสงค์ที่ชัดเจน มีกระบวนการปฏิบัติงานและระบบงานที่เป็นมาตรฐาน รวมถึงมีการติดตาม ประเมินผล และพัฒนาปรับปรุงอย่างต่อเนื่องและเป็นระบบ

หลักประสิทธิภาพ (Efficiency) : หมายถึง การบริหารราชการ ตามแนวทางการกำกับดูแลที่ดีที่มีการออกแบบกระบวนการปฏิบัติงานโดยการใช้เทคนิคและเครื่องมือการบริหารจัดการที่เหมาะสม ให้องค์กรสามารถใช้ทรัพยากรทั้งด้านต้นทุน แรงงาน และระยะเวลาให้เกิดประโยชน์สูงสุดต่อการพัฒนาขีดความสามารถในการปฏิบัติราชการตามภารกิจ เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกกลุ่ม

หลักการมีส่วนร่วม (Participation) : หมายถึง กระบวนการที่ข้าราชการและบุคลากรในองค์กรทุกระดับ ประชาชน และผู้มีส่วนได้ส่วนเสียทุกกลุ่ม มีโอกาสได้เข้าร่วมในการรับรู้ เรียนรู้ ทำความเข้าใจ ร่วมแสดงทัศนะ ร่วมเสนอปัญหา/ประเด็นที่สำคัญที่เกี่ยวข้อง ร่วมคิดแนวทาง ร่วมการแก้ไขปัญหา ร่วมในกระบวนการตัดสินใจ และร่วมกระบวนการพัฒนาในฐานะหุ้นส่วนการพัฒนา

หลักความโปร่งใส (Transparency) : หมายถึง กระบวนการเปิดเผยอย่างตรงไปตรงมา ชี้แจงได้เมื่อมีข้อสงสัย และสามารถเข้าถึงข้อมูลข่าวสารอันไม่ต้องห้ามตามกฎหมายได้อย่างเสรี โดยประชาชนสามารถรู้ทุกขั้นตอนในการดำเนินกิจกรรมหรือกระบวนการต่าง ๆ และสามารถตรวจสอบได้

หลักการตอบสนอง (Responsiveness) : หมายถึง การให้บริการที่สามารถดำเนินการได้ภายในระยะเวลาที่กำหนด และสร้างความเชื่อมั่น ความไว้วางใจ รวมถึงตอบสนองความคาดหวัง/ความต้องการของประชาชนผู้รับบริการและผู้มีส่วนได้ส่วนเสีย ที่มีความหลากหลายและมีความแตกต่าง

หลักภาระรับผิดชอบ (Accountability) : หมายถึง การแสดงความรับผิดชอบในการปฏิบัติหน้าที่และผลงานต่อเป้าหมายที่กำหนดไว้ โดยความรับผิดชอบนั้นควรอยู่ในระดับที่สนองต่อความคาดหวังของสาธารณะ รวมทั้งการแสดงถึงความสำนึกในการรับผิดชอบต่อปัญหาสาธารณะ

หลักนิติธรรม (Rule of Law) : หมายถึง การใช้อำนาจของกฎหมาย กฎระเบียบ ข้อบังคับในการบริหารราชการด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของผู้มีส่วนได้ส่วนเสีย

หลักการกระจายอำนาจ (DecentraliZation) : หมายถึง การถ่ายโอนอำนาจการตัดสินใจ ทรัพยากรและภารกิจ รวมถึงการมอบอำนาจและความรับผิดชอบในการตัดสินใจและการดำเนินการให้แก่ผู้ปฏิบัติงาน โดยมุ่งเน้นการสร้างความพึงพอใจในการให้บริการต่อผู้รับบริการและผู้มีส่วนได้ส่วนเสีย การปรับปรุงกระบวนการ และเพิ่มผลิตภาพ เพื่อผลการดำเนินงานที่ดีของส่วนราชการ ทั้งนี้การกระจายอำนาจการตัดสินใจที่ดี บุคลากรต้องมีความรู้ความสามารถและข้อมูลสนับสนุนเพื่อให้เกิดการตัดสินใจที่เหมาะสม

หลักความเสมอภาค (Equity) : หมายถึง การได้รับการปฏิบัติและได้รับบริการอย่างเท่าเทียมกัน โดยไม่มีการแบ่งแยกด้าน ชาย/หญิง ถิ่นกำเนิด เชื้อชาติ ภาษา เพศ อายุ ความพิการ สภาพทางกายและสุขภาพ สถานะของบุคคล ฐานะทางเศรษฐกิจและสังคม ความเชื่อทางศาสนา การศึกษา และอื่น ๆ

บทที่ 3

การจัดทำแผนบริหารความเสี่ยง ของสำนักงานเลขาธิการวุฒิสภา

CHAPTER 3

กระบวนการบริหารความเสี่ยง

เป็นกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organizstion of the Tread Way Commission) ที่มีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์ประเมินและจัดการความเสี่ยงอย่างเหมาะสม โดยกำหนดแนวทางการควบคุมเพื่อป้องกัน/ลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ กระบวนการดังกล่าวจะสำเร็จได้ต้องมีการสื่อสารให้บุคลากรในองค์กรได้มีความรู้ ความเข้าใจในเรื่องการบริหารความเสี่ยงในทิศทางเดียวกันและควรจัดทำระบบสารสนเทศเพื่อการวิเคราะห์ประเมินความเสี่ยง

3.1 หลักเกณฑ์การจัดทำแผนบริหารจัดการความเสี่ยง

การวิเคราะห์องค์กรด้วยการวิเคราะห์ SWOT Analysis ดังนี้

การวิเคราะห์ปัจจัยภายใน (Internal Environment Analysis) ได้แก่ จุดแข็ง (Strength-S) หมายถึง ทรัพยากรด้านต่าง ๆ ที่ได้เปรียบหรือส่วนที่เข้มแข็งภายในองค์กร ที่สามารถใช้ประโยชน์เพื่อผลักดันให้องค์กรสามารถดำเนินงานบรรลุวัตถุประสงค์และภารกิจขององค์กร จุดอ่อน (Weakness-W) หมายถึง ข้อเสียเปรียบ ข้อผิดพลาดในองค์กรที่เป็นข้อด้อยหรือเป็นข้อจำกัดต่าง ๆ ที่ส่งผลทำให้ไม่บรรลุวัตถุประสงค์และภารกิจขององค์กร การวิเคราะห์จุดแข็งและจุดอ่อน เช่น ด้านโครงสร้าง ด้านบุคลากร ด้านบริหารจัดการ ด้านงบประมาณ ด้านวัสดุอุปกรณ์ และด้านกฎหมาย การวิเคราะห์ปัจจัยภายนอก (External Environment Analysis) ได้แก่ โอกาส (Opportunity-O) หมายถึง สถานการณ์หรือปัจจัยที่เกิดจากสภาพแวดล้อมที่มีลักษณะเกื้อกูลต่อการบรรลุวัตถุประสงค์และภารกิจขององค์กร หรือสภาพแวดล้อมภายนอกทั่วไป อุปสรรค (Threat-T) หมายถึง สถานการณ์หรือปัจจัยที่เกิดจากสภาพแวดล้อมภายนอกที่มีลักษณะเป็นอุปสรรค ขัดขวาง หรือทำให้เกิดผลเสียหาย ผลกระทบในทางลบต่อการบริหารงานขององค์กร การวิเคราะห์โอกาสและอุปสรรค เช่น สภาพแวดล้อมภายนอก ได้แก่ ด้านเศรษฐกิจ ด้านสังคม ด้านการเมือง ด้านเทคโนโลยี เป็นต้น

3.2 นโยบายการยอมรับความเสี่ยงระดับองค์กร

นโยบายการยอมรับความเสี่ยงระดับองค์กรเป็นการให้นโยบายเพื่อให้ทิศทางในการบริหารจัดการความเสี่ยงภายในองค์กรโดยผู้บริหารระดับสูง และได้รับความเห็นชอบโดยคณะกรรมการฯ ผู้บริหารได้ตระหนักและยอมรับว่าการดำเนินงานขององค์กรมีความเสี่ยงที่อาจทำให้ไม่บรรลุตามวัตถุประสงค์ขององค์กร การบริหารจัดการความเสี่ยงเป็นหน้าที่ความรับผิดชอบของฝ่ายบริหาร

โดยผู้บริหารทำหน้าที่บริหารจัดการความเสี่ยงอย่างมุ่งมั่นและตั้งใจ เพื่อให้ผู้มีส่วนได้ส่วนเสียมั่นใจว่าองค์กรมีการบริหารจัดการความเสี่ยงอย่างมีประสิทธิภาพและประสิทธิผล เพื่อให้องค์กรสามารถปฏิบัติงานบรรลุตามวัตถุประสงค์ขององค์กร โดยคำนึงถึงประโยชน์ต่อประเทศชาติเป็นที่ตั้ง (Public Interest) ผู้บริหารได้กำหนดความเสี่ยงที่ยอมรับได้ในด้านต่าง ๆ ดังนี้

1) ด้านการปฏิบัติงาน

ผู้บริหารยอมรับความเสี่ยงในระดับปานกลางในกระบวนการการปฏิบัติงานทั่วไปขององค์กร และยอมรับความเสี่ยงระดับน้อยในการปฏิบัติงานมีผลกระทบที่เกี่ยวข้องกับการให้บริการของประชาชน ทั้งนี้ ผู้บริหารจะยอมรับความเสี่ยงระดับสูงในการปฏิบัติงานที่เกี่ยวข้องกับนวัตกรรมและการพัฒนา

2) ด้านการทุจริต

ผู้บริหารปฏิเสธที่จะยอมรับความเสี่ยงที่เกี่ยวข้องกับการทุจริตทุกกรณี

3) ด้านเทคโนโลยีสารสนเทศ

ผู้บริหารปฏิเสธที่จะยอมรับความเสี่ยงในเรื่องของความปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลด้านการเงิน ข้อมูลส่วนบุคคล และข้อมูลที่เกี่ยวข้องกับความมั่นคงของประเทศ และยอมรับความเสี่ยงระดับปานกลางสำหรับระบบสารสนเทศที่เกี่ยวข้องกับเรื่องทั่วไป เช่น แบบความคิดเห็นหรือการเก็บสถิติทั่วไป หน่วยงานยอมรับความเสี่ยงระดับน้อยสำหรับประสิทธิภาพของระบบสารสนเทศในการให้บริการประชาชน

4) ด้านภาพลักษณ์ขององค์กร

ภาพลักษณ์และความน่าเชื่อถือขององค์กรเป็นปัจจัยที่สำคัญในการปฏิบัติงานขององค์กรให้เป็นที่ยอมรับของประชาชนผู้เสียภาษี ซึ่งเป็นผู้มีส่วนได้ส่วนเสียหลักขององค์กร ผู้บริหารยอมรับความเสี่ยงระดับน้อยเกี่ยวกับความเชื่อถือและภาพลักษณ์ขององค์กร อย่างไรก็ตาม ผู้บริหารให้ความสำคัญกับภาพลักษณ์ที่สะท้อนประสิทธิภาพการดำเนินงานที่แท้จริงโดยไม่มีการบิดเบือน เพื่อให้ภาพลักษณ์และความน่าเชื่อถือเกิดจากการปฏิบัติงานขององค์กรและความไว้วางใจของผู้มีส่วนได้ส่วนเสียโดยเนื้อแท้

3.3 การกำหนดประเภทความเสี่ยง (Risk Categories)

การกำหนดประเภทความเสี่ยง โดยระบุความเสี่ยงทั้งหมดที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงาน (Risk Inventory) เมื่อระบุความเสี่ยงทั้งหมดแล้วได้พิจารณาจัดกลุ่มความเสี่ยง โดยความเสี่ยงที่มีลักษณะเหมือนกันจัดกลุ่มเป็นประเภทความเสี่ยงเดียวกันให้ครอบคลุมทุกความเสี่ยง

3.4 การประเมินผลการควบคุมและการจัดการความเสี่ยง

การประเมินผลการควบคุม เป็นการดำเนินการภายหลังจากการที่ได้ระบุระดับความเสี่ยงและจัดลำดับความเสี่ยงแล้ว ให้นำความเสี่ยงมาประเมินผลการควบคุมและการจัดการที่มีอยู่ว่ามีประสิทธิผลเพียงพอหรือไม่ และสามารถลดหรือควบคุมความเสี่ยงและปัจจัยเสี่ยงให้อยู่ในระดับที่ยอมรับได้ พอใช้ ต้องปรับปรุง ดังนี้

1) ยอมรับได้ ลด/ควบคุมความเสี่ยงลงสู่ระดับที่ยอมรับได้
2) พอใช้ ลด/ควบคุมความเสี่ยงได้บางส่วน แต่ยังไม่ถึงระดับที่ยอมรับได้
3) ต้องปรับปรุง หมายถึง ไม่สามารถลด/ควบคุมความเสี่ยงได้

3.5 การจัดการความเสี่ยง

กระบวนการดำเนินการต่าง ๆ ที่ตอบสนองความความเสี่ยง โดยลดมูลเหตุของแต่ละโอกาสที่จะทำให้เกิดความเสียหาย เพื่อให้ระดับความเสี่ยงและผลกระทบของความเสี่ยงที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยพิจารณาต้นทุนการจัดการความเสี่ยงและผลประโยชน์ที่จะได้รับ โดยมีทางเลือกที่จะจัดการกับความเสี่ยงอยู่ด้วยกัน 4 วิธี ดังนี้

1) การยอมรับความเสี่ยง (Risk Retention)

เป็นความเสี่ยงที่ยอมรับให้มีความเสี่ยงได้ เพราะต้นทุนการจัดการความเสี่ยงสูงอาจไม่คุ้มกับผลประโยชน์ที่อาจจะเกิดขึ้น หรือเป็นความเสี่ยงที่มีสาเหตุจากปัจจัยภายนอกที่อยู่เหนือการควบคุม และไม่อาจเลือกใช้วิธีอื่นได้

2) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)

เป็นความเสี่ยงที่ยอมรับไม่ได้ มีผลกระทบกับองค์กรแผนงาน/โครงการ/กิจกรรมหรือกระบวนงานอย่างสูง ซึ่งไม่สามารถจัดการได้ด้วยวิธีอื่น โดยอาจควบคุมได้ด้วย การยกเลิก/ปรับเปลี่ยนเป้าหมาย/โครงการ/งานหรือกิจกรรม

3) การถ่ายโอนความเสี่ยง (Risk Transference)

เป็นความเสี่ยงที่ยอมรับไม่ได้ ต้องดำเนินการถ่ายโอนความเสี่ยงให้ผู้อื่น เช่น การจ้างบุคคลภายนอก เป็นต้น โดยอาจเป็นความเสี่ยงเกี่ยวกับ

- ความเสี่ยงที่มีขนาดความรุนแรงมาก เช่น ความเสี่ยงเกี่ยวกับภัยธรรมชาติ/วินาศภัย
- ความเสี่ยงที่ต้องดำเนินการในเรื่องที่ไม่มีความชำนาญ
- ความเสี่ยงที่ต้องปฏิบัติงานที่มีปริมาณมากในเวลาอันจำกัด เป็นต้น

4) การควบคุม/ลดความเสี่ยง (Risk Control)

- เป็นความเสี่ยงที่ยอมรับไม่ได้ ต้องหาแนวทางการควบคุมทั้งโอกาสและผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งได้รับผลกระทบจากปัจจัยภายในและอยู่ภายใต้การควบคุมขององค์กร ได้แก่ การควบคุมภายใน

- เป็นความเสี่ยงที่ยอมรับไม่ได้ ต้องหาแนวทางการควบคุมทั้งโอกาสและผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งได้รับผลกระทบจากปัจจัยภายนอกและมิได้อยู่ภายใต้การควบคุมขององค์กร ได้แก่ แผนรองรับ/มาตรการ

3.6 การติดตามและทบทวนการบริหารความเสี่ยง

เมื่อดำเนินการจัดทำแผนบริหารจัดการความเสี่ยงเสร็จเรียบร้อยแล้ว จะมีการติดตามโดยการประสานงานกับสำนักงาน โดยวิเคราะห์และประเมินการบริหารจัดการความเสี่ยง หรือการจัดการที่ได้มีการดำเนินการที่ผ่านมาว่ามีประสิทธิผลหรือไม่ ถ้ายังมีความเสี่ยงเหลืออยู่ หรือพบความเสี่ยงที่เกิดขึ้นใหม่ จะดำเนินการปรับแผนบริหารจัดการความเสี่ยงตามข้อเสนอแนะแก้ไขปรับปรุงต่อไป

3.7 การสื่อสารและการรายงาน

การสื่อสารเป็นหัวใจของการบริหารความเสี่ยงในทุก ๆ ขั้นตอน การสื่อสารมีวัตถุประสงค์เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง โดยเข้าใจและมีข้อมูลความเสี่ยง ทางเลือกในการลดปัญหาความเสี่ยง ข้อมูลของความเสี่ยงในลักษณะต่าง ๆ และทำการตัดสินใจได้ดีที่สุดภายใต้ข้อจำกัด ซึ่งการติดต่อสื่อสารและเอกสารที่เกี่ยวข้องนับว่ามีความสำคัญยิ่งต่อความสำเร็จของแต่ละขั้นตอนในกระบวนการบริหารความเสี่ยง โดยการประสานงานกับสำนักเพื่อรวบรวมข้อมูลและเอกสารต่าง ๆ ในการจัดทำแผนบริหารจัดการความเสี่ยง การบริหารความเสี่ยง การติดตาม การทบทวน และการจัดทำรายงานผลการบริหารความเสี่ยง ซึ่งเป็นการรายงานผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง การติดตามผลความคืบหน้าและผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง

การวิเคราะห์องค์กร

สำนักงานเลขาธิการวุฒิสภาได้วิเคราะห์สภาพแวดล้อมที่ส่งผลกระทบต่อสำนักงานเลขาธิการวุฒิสภา วิเคราะห์จากเครื่องมือ SWOT Analysis โดยวิเคราะห์ปัจจัยภายในตามกรอบแนวคิด McKinsey’s 7S และวิเคราะห์ปัจจัยภายนอกตามกรอบแนวคิด PESTEL Analysis

ผลการวิเคราะห์สภาพแวดล้อมของสำนักงานเลขาธิการวุฒิสภา

จุดแข็ง (Strengths)

1. เป็นองค์กรที่มีบทบัญญัติหน้าที่และอำนาจไว้ตามรัฐธรรมนูญ
2. เป็นองค์กรที่สนับสนุนการปฏิบัติหน้าที่ของวุฒิสภาเพียงองค์กรเดียว
3. มีภาพลักษณ์น่าเชื่อถือ ทำให้ได้รับการยอมรับจากการประสานความร่วมมือ รวมทั้งมีเครือข่ายกับหน่วยงานภายนอก
4. มีความเป็นอิสระในการบริหารงานบุคคล การบริหารทั่วไป
5. บุคลากรมีจิตบริการ ความสามารถ ทักษะ ทุ่มเท อดทนในการให้บริการ
6. มีข้อมูลเอกสารที่พร้อมใช้งานและเป็นศูนย์รวมข้อมูลด้านนิติบัญญัติที่สำคัญของประเทศ

จุดอ่อน (Weaknesses)

1. การบริหารจัดการองค์การในภาพรวมของสำนักงานฯ ยังไม่สนับสนุนการทำงานได้อย่างมีประสิทธิภาพ
2. ระบบรักษาความปลอดภัย/สภาพแวดล้อมไม่เอื้อต่อการทำงาน
3. ระบบเทคโนโลยีสารสนเทศ ยังไม่สามารถรองรับการทำงานฝ่ายนิติบัญญัติได้อย่างมีประสิทธิภาพ
4. ระบบบริหารทรัพยากรบุคคล โครงสร้างของบุคลากรและอัตรากำลังยังไม่เหมาะสมกับภารกิจที่มีปริมาณมาก
5. Mind set ของบุคลากรที่ทำงานเชิงรับมากกว่าเชิงรุก ขาดบุคลากรด้านงานวิจัยและการพัฒนาเชิงวิชาการ

โอกาส (Opportunities)

1. รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ยุทธศาสตร์ชาติ ระยะ 20 ปี แผนการปฏิรูปประเทศ ระบบราชการ 4.0 นโยบายต่าง ๆ และมาตรฐานสากลที่เกิดขึ้น ทำให้ส่วนราชการต้องทำงานอย่างมีระบบ มีทิศทางการพัฒนาประเทศอย่างชัดเจนและเป็นไปในทิศทางเดียวกัน

2. การมีรัฐสภาแห่งใหม่ ทำให้มีสถานที่ทำงานแห่งเดียว สามารถสร้างระบบเทคโนโลยีที่ทันสมัย ระบบทรัพยากรที่สนับสนุนการทำงานอย่างมีคุณภาพ

3. การทำงานกับผู้ทรงคุณวุฒิ ทำให้บุคลากรได้รับประสบการณ์ในการทำงานและองค์กรได้รับการสนับสนุนในด้านต่าง ๆ

4. การมีส่วนร่วมทางการเมืองของประชาชนผ่านช่องทางสื่อออนไลน์ในอนาคตเพิ่มมากขึ้น ทำให้เกิดการตรวจสอบการปฏิบัติงานขององค์กร เพื่อผลักดันการปฏิรูปการเมือง และการปฏิรูปประเทศตามเจตนารมณ์ของรัฐธรรมนูญได้ดียิ่งขึ้น

5. ความก้าวหน้าของเทคโนโลยีช่วยให้ได้รับข้อมูลข่าวสารและประชาสัมพันธ์องค์กรทั้งในและต่างประเทศ

6. มีเครือข่ายทุกภาคส่วนที่พร้อมให้ความร่วมมือ อาทิ ด้านการศึกษา ด้านสังคม

ภัยคุกคาม (Threats)

1. ความไม่มีเสถียรภาพทางการเมือง ส่งผลการบริหารงานของสำนักงานเลขาธิการวุฒิสภา

2. ความผันผวนทางเศรษฐกิจ ส่งผลต่อการบริหารงบประมาณที่สำนักงานเลขาธิการวุฒิสภาได้รับในการบริหารจัดการองค์กร

3. ความต้องการ/ความคาดหวังของสมาชิกวุฒิสภา หรือประชาชนที่มีต่ออำนาจหน้าที่ของสำนักงานเลขาธิการวุฒิสภา ส่งผลต่อภาระงาน ทำให้ไม่สามารถพัฒนาตนเองในด้านวิชาการได้ดีเท่าที่ควร

4. การระบาดของโรคอุบัติใหม่ อาทิ ไวรัส Covid - 19 ส่งผลต่อการบริหารจัดการสำนักงานเลขาธิการวุฒิสภาในภาพรวม เช่น รูปแบบการทำงาน (WFH) การรักษาความปลอดภัยในการทำงาน

5. สภาพแวดล้อมเกี่ยวกับภัยธรรมชาติ สภาพภูมิอากาศที่มีการเปลี่ยนแปลงอย่างรวดเร็วและมีผลกระทบที่รุนแรงอันทำให้มนุษยชาติต้องระมัดระวัง

6. ภัยคุกคามด้านเทคโนโลยีดิจิทัล เช่น แฮกเกอร์ ไวรัส สปายแวร์

ความท้าทายที่ส่งผลกระทบต่อสำนักงานเลขาธิการวุฒิสภา

สำนักงานเลขาธิการวุฒิสภา ได้มีการทบทวนแนวทางการพัฒนาสำนักงานเลขาธิการวุฒิสภา และกำหนดประเด็นความท้าทาย ดังนี้

ความท้าทายด้านพันธกิจ

1. สนับสนุนการขับเคลื่อนภารกิจด้านนิติบัญญัติตามบทบัญญัติรัฐธรรมนูญและกฎหมาย
2. ส่งเสริมการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข
3. บริหารจัดการองค์กรให้มีขีดสมรรถนะสูงสู่ความเป็น Smart Digitalization

ความท้าทายด้านปฏิบัติการ

1. การปรับเปลี่ยนให้เป็นองค์กรอัจฉริยะ เป็นระบบราชการ 4.0
2. การบูรณาการการทำงานอย่างเปิดกว้างและเชื่อมโยงกัน
3. การสร้างมาตรฐานในการปฏิบัติราชการ

ความท้าทายด้านบุคลากร

1. พัฒนาศักยภาพระบบการบริหารทรัพยากรให้มีประสิทธิภาพและทันสมัย
2. พัฒนาศักยภาพของบุคลากรให้มีความรู้ ความสามารถ และทักษะการคิดวิเคราะห์ให้ทันต่อการเปลี่ยนแปลง
3. บุคลากรมีวัฒนธรรมและพฤติกรรม ซื่อสัตย์สุจริต
4. พัฒนาคุณภาพชีวิตและสภาพแวดล้อมที่ดีในการปฏิบัติงาน

การจัดทำแผนบริหารความเสี่ยง

แนวทางการบริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดระดับความเสี่ยงที่มีผลกระทบต่อภารกิจของสำนักงานเลขาธิการวุฒิสภา โดยได้กำหนดกิจกรรมเพื่อเป็นการป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยกระบวนการจัดทำแผนบริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภาได้ดำเนินการตามกรอบแนวคิดของการบริหารความเสี่ยง ซึ่งมีแผนการดำเนินงานดังนี้

โครงการจัดทำแผนบริหารความเสี่ยง สำนักงานเลขาธิการวุฒิสภา

- บรรยายเพื่อสร้างความรู้ ความเข้าใจ เกี่ยวกับทฤษฎีและหลักการบริหารความเสี่ยง ตลอดจนแนวทางในการดำเนินการจัดทำแผนบริหารความเสี่ยง
- Workshop ระดมความคิดเห็น เพื่อจัดทำร่างแผนบริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา

+

โครงการพัฒนาคุณภาพการปฏิบัติงานของส่วนราชการสังกัดสำนักงานเลขาธิการวุฒิสภาตามมาตรฐานระบบบริหารคุณภาพ ISO 9001 : 2015 หลักสูตร "เทคนิคการบริหารความเสี่ยง (Risk Management)"

- ระดมความคิดเห็นเพื่อจัดทำแผนบริหารความเสี่ยง
- กำหนดค่าความเสี่ยงและเรียงลำดับในเหตุการณ์ความเสี่ยง
- คัดเลือกเหตุการณ์ความเสี่ยงที่สำคัญ เพื่อกำหนดแนวทางในการจัดการ

- กำหนดกิจกรรมเพื่อควบคุมเหตุการณ์ความเสี่ยง โดยกำหนดขั้นตอน ระยะเวลาดำเนินการ ตลอดจนผู้รับผิดชอบ
- รวบรวม วิเคราะห์ และกำหนดแนวทางในการป้องกันความเสี่ยง

- ประกาศใช้แผนบริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. 2567
- ติดตามความก้าวหน้าการดำเนินงานของกิจกรรมควบคุมความเสี่ยงในแต่ละด้าน
- รวบรวมและรายงานผลการดำเนินงานควบคุมความเสี่ยงแต่ละด้าน
- จัดทำสรุปรายงานผลการดำเนินงานความเสี่ยงประจำปี พ.ศ. 2567
- เผยแพร่ผลรายงานการบริหารความเสี่ยงประจำปีงบประมาณ พ.ศ. 2567 ให้ผู้บริหารและบุคลากรรับทราบ

กระบวนการพิจารณาความเสี่ยง

1. การระบุความเสี่ยง (Event Identification)

1.1 ความเสี่ยง (Risk) หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจเกิดขึ้นในอนาคต และมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านกลยุทธ์ การปฏิบัติงาน การเงิน เวลา และการบริหาร โดยความเสี่ยงนี้จะถูกวัดด้วยผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์ ซึ่งเป็นความเสี่ยงตามความหมายทั่วไป

สำหรับความเสี่ยงของสำนักงานเลขาธิการวุฒิสภานั้น หมายถึง เหตุการณ์/การกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณที่ไม่แนนอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าหมายของแผนงาน/โครงการที่สำคัญในแต่ละประเด็นยุทธศาสตร์ตามที่ระบุในแผนปฏิบัติราชการของสำนักงาน

1.2 ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

1.3 การระบุความเสี่ยง ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยง และปัจจัยเสี่ยง โดยคำนึงถึงปัจจัยภายในและภายนอกที่มีผลกระทบต่อวัตถุประสงค์ และเป้าหมายขององค์กร หรือผลการปฏิบัติงานในระดับองค์กรและกิจกรรม พิจารณาว่ามีเหตุการณ์ใดหรือกิจกรรมใดของกระบวนการปฏิบัติงาน ที่อาจเกิดความผิดพลาด/ความเสียหาย/ไม่บรรลุวัตถุประสงค์ที่กำหนด มีทรัพย์สินใดที่ต้องดูแลป้องกันรักษา

การระบุปัจจัยเสี่ยงเริ่มต้นจากการแจกแจงกระบวนการปฏิบัติงานที่จะทำให้บรรลุวัตถุประสงค์ที่กำหนดไว้ แล้วจึงระบุปัจจัยเสี่ยงที่มีผลกระทบต่อกระบวนการปฏิบัติงานนั้น ๆ โดยสำนักงานเลขาธิการวุฒิสภาได้นำแนวคิดเรื่องหลักธรรมาภิบาลที่เกี่ยวข้องในแต่ละด้านมาเป็นปัจจัยในการวิเคราะห์ด้วย

1.4 การค้นหาความเสี่ยง เริ่มจากการวิเคราะห์ภาระงานที่ต้องรับผิดชอบซึ่งอยู่ภายใต้ภารกิจหลักว่าประกอบด้วยกิจกรรมอะไรบ้าง พร้อมระบุเหตุของความเสี่ยงที่ส่งผลให้กิจกรรมเหล่านั้นไม่ประสบผลสำเร็จโดยแบ่งแยกการวิเคราะห์ออกเป็นสีต่าง ๆ ดังนี้

1) การวิเคราะห์จากภายในองค์กร ได้แก่

- ความเสี่ยงที่เกิดขึ้นจากการดำเนินงานของสำนักเอง (สีเขียว)
- ความเสี่ยงที่เกิดขึ้นจากการปฏิบัติงานตามระเบียบ ข้อบังคับที่หน่วยงานได้กำหนด (สีเหลือง)
- ความเสี่ยงที่เกิดขึ้นจากการดำเนินงานหรือประสานงานข้ามฝ่าย (สีส้ม)

2) การวิเคราะห์จากภายนอกองค์กร ได้แก่ ความเสี่ยงที่เกิดขึ้นจากการดำเนินงานที่เกี่ยวข้องกับสมาชิกวุฒิสภาหรือหน่วยงานภายนอก (สีแดง)

การระบุความเสี่ยงควรเริ่มด้วยการแจกแจงกระบวนการปฏิบัติงานที่จะทำให้บรรลุวัตถุประสงค์ที่กำหนดไว้แล้วจึงระบุปัจจัยเสี่ยงที่มีผลกระทบต่อกระบวนการปฏิบัติงานนั้น ๆ ทำให้เกิดความผิดพลาด ความเสียหายและเสียโอกาส ปัจจัยเสี่ยงนั้นควรจะเป็นต้นเหตุที่แท้จริงเพื่อที่จะสามารถนำไปใช้ประโยชน์ในการหามาตรการลดความเสี่ยงในภายหลังได้ ทั้งนี้ การระบุความเสี่ยงสามารถดำเนินการได้หลายวิธี เช่น จากการวิเคราะห์กระบวนการทำงาน การวิเคราะห์ทบทวนผลการปฏิบัติงานที่ผ่านมา การประชุมเชิงปฏิบัติการ การระดมสมอง การเปรียบเทียบกับองค์กรอื่น การสัมภาษณ์และการสอบถาม เป็นต้น

2. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงประกอบด้วย 2 ขั้นตอน ดังนี้

2.1 การกำหนดเกณฑ์การประเมินมาตรฐาน

เป็นการกำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) โดยผู้บริหารหรือหน่วยงานที่รับผิดชอบด้านการบริหารความเสี่ยงจะต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งสามารถกำหนดเกณฑ์ได้ทั้งเกณฑ์ในเชิงปริมาณและเชิงคุณภาพ ทั้งนี้ ขึ้นอยู่กับข้อมูลสภาพแวดล้อมในหน่วยงานและดุลยพินิจการตัดสินใจของฝ่ายบริหารของหน่วยงาน โดยเกณฑ์ในเชิงปริมาณจะเหมาะกับหน่วยงานที่มีข้อมูลตัวเลข หรือจำนวนเงินมาใช้ในการวิเคราะห์อย่างพอเพียง สำหรับหน่วยงานที่มีข้อมูลเชิงพรรณนาไม่สามารถระบุเป็นตัวเลขหรือจำนวนเงินที่ชัดเจนได้ ก็ให้กำหนดเกณฑ์ในเชิงคุณภาพ ซึ่งได้พิจารณาถึงโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likelihood) และความรุนแรงของเหตุการณ์ต่าง ๆ (Impact) ที่จะเกิดผลกระทบต่อสำนักงานเลขาธิการวุฒิสภา

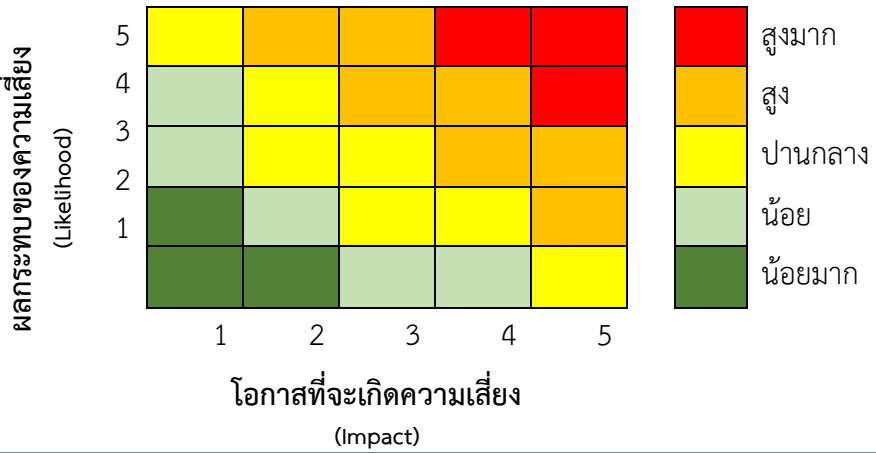
2.2 การประเมินโอกาสและผลกระทบของความเสี่ยง

เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาส (Likelihood) ที่จะเกิดเหตุการณ์ความเสี่ยงต่าง ๆ และประเมินระดับความรุนแรงหรือมูลค่าความเสียหาย (Impact) จากความเสี่ยง เพื่อให้เห็นถึงระดับของความเสี่ยงที่แตกต่างกัน ทำให้สามารถกำหนดการควบคุมความเสี่ยงได้อย่างเหมาะสม ซึ่งจะช่วยให้หน่วยงานสามารถวางแผนและจัดสรรทรัพยากรได้อย่างถูกต้องภายใต้งบประมาณ กำลังคน หรือเวลาที่มีจำกัดโดยอาศัยเกณฑ์มาตรฐานที่กำหนดไว้ข้างตน

3. ระดับของความเสี่ยง (Degree of Risk)

มี 5 ระดับ ได้แก่ สูงมาก สูง ปานกลาง น้อย และน้อยมาก

ตารางระดับของความเสี่ยง (Degree of Risk)



4. การวิเคราะห์ความเสี่ยง (Risk Analysis)

เมื่อพิจารณาโอกาส/ความถี่ที่จะเกิดเหตุการณ์ (Likelihood) และความรุนแรงของผลกระทบ (Impact) ของแต่ละปัจจัยเสี่ยงแล้วให้นำผลที่ได้มาพิจารณาความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงว่าก่อให้เกิดระดับของความเสี่ยงในระดับใด ดังนี้

1) พิจารณาโอกาส/ความถี่ในการเกิดเหตุการณ์ต่าง ๆ (Likelihood) ว่ามีโอกาส/ความถี่ที่จะเกิดนั้นมากน้อยเพียงใดตามเกณฑ์มาตรฐานที่กำหนด

2) พิจารณาความรุนแรงของผลกระทบของความเสี่ยง (Impact) ว่ามีระดับความรุนแรงหรือมีความเสียหายเพียงใดตามเกณฑ์มาตรฐานที่กำหนด

ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood)

ระดับโอกาส	ระดับค่าคะแนน	ความหมาย
ต่ำมาก	1	เกิดขึ้นยาก
ต่ำ	2	เกิดขึ้นน้อย
ปานกลาง	3	เกิดขึ้นบ้าง
สูง	4	เกิดขึ้นบ่อยครั้ง
สูงมาก	5	เกิดขึ้นเป็นประจำ

ระดับผลกระทบ (Impact)

ระดับผลกระทบ	ระดับค่าคะแนน	ความหมาย
ต่ำมาก	1	น้อยมาก
ต่ำ	2	น้อย
ปานกลาง	3	ปานกลาง
สูง	4	รุนแรง
สูงมาก	5	รุนแรงมาก

การประเมินระดับความเสี่ยง (Degree of Risk) จะดำเนินการโดยนำคะแนนระดับโอกาสที่จะเกิดความเสี่ยงคูณด้วยคะแนนระดับความรุนแรงของผลกระทบ และพิจารณาคะแนนความเสี่ยงที่คำนวณได้ว่าอยู่ในระดับความเสี่ยงใด ดังนี้

ตารางแสดงตัวอย่างการคำนวณระดับความเสี่ยง

ความเสี่ยง	ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood)	ระดับผลกระทบ (Impact)	ระดับความเสี่ยง (Degree of Risk)
A	3	4	3 X 4 = 12
B	2	4	2 X 4 = 8
C	5	3	5 X 3 = 15
D	4	2	4 X 2 = 8

5. การจัดลำดับความเสี่ยง (Risk Matrix)

เมื่อได้ค่าระดับความเสี่ยงแล้วจะนำมาจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อสำนักงานเลขาธิการวุฒิสภา เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับของความเสี่ยงที่เกิดจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบของความเสี่ยง (Impact) ที่ประเมินได้ตามตารางการประเมินความเสี่ยง โดยจัดเรียงตามลำดับจากระดับสูงมาก สูง ปานกลาง ต่ำ และเลือกความเสี่ยงที่มีระดับสูงมาก และสูง มาจัดทำแผนการบริหาร/จัดการความเสี่ยงในขั้นตอน ต่อไป

6. การกำหนดแผนภูมิความเสี่ยง (Risk Profile)

ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบที่เกิดขึ้น (Impact) และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite Boundary)

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของเหตุการณ์ต่าง ๆ (Likelihood x Impact)

ซึ่งจัดแบ่งเป็น 5 ระดับ สามารถแสดงเป็น Risk Profile แบ่งพื้นที่เป็น 5 ส่วน (5 Quadrant) ใช้เกณฑ์ในการจัดแบ่งดังนี้

ตารางแสดงระดับความเสี่ยง

ระดับคะแนน	ระดับความเสี่ยง	ความหมาย	ระดับสี
17 - 25	สูงมาก	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งรัดการดำเนินการจัดการความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้ทันที	
10 - 16	สูง	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ โดยต้องดำเนินการจัดการความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้	
5 - 9	ปานกลาง	ระดับความเสี่ยงที่ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยง ไปอยู่ระดับที่ยอมรับไม่ได้	
3 - 4	น้อย	ระดับความเสี่ยงที่ยอมรับได้ โดยใช้วิธีควบคุมปกติ ในขั้นตอนการปฏิบัติงานที่กำหนด	
1 - 2	น้อยมาก	ระดับความเสี่ยงที่ยอมรับได้ บริหารจัดการโดยใช้ วิธีการติดตามระดับความเสี่ยง ตลอดระยะเวลาการปฏิบัติงาน	

ผลกระทบ / โอกาส	น้อยมาก 1	น้อย 2	ปานกลาง 3	สูง 4	สูงมาก 5
เกิดขึ้นเป็นประจำ 5	5	10	15	20	25
เกิดขึ้นบ่อยครั้ง 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

7. เกณฑ์ความเสี่ยง (Risk Level)

ระดับความเสี่ยง	ระดับคะแนน	วิธีการจัดการความเสี่ยง
สูงมาก	17 - 25	**ถ่ายโอนความเสี่ยง**/มีแผนลดและประเมินซ้ำ
สูง	10 - 16	**การควบคุมความสูญเสีย**/มีแผนลดความเสี่ยง
ปานกลาง	5 - 9	**การควบคุมเพื่อป้องกัน**/มีแผนป้องกันความเสี่ยง
น้อย	3 - 4	**การรับความเสี่ยงไว้เอง** /ยอมรับความเสี่ยงแต่มีการควบคุมความเสี่ยง
น้อยมาก	1 - 2	**การหลีกเลี่ยงความเสี่ยง**/ยอมรับความเสี่ยง

8. การจัดทำแผนบริหารความเสี่ยง (Risk Plan)

โดยการนำกลยุทธ์ มาตรการ หรือแผนงาน มาใช้ปฏิบัติในทุกหน่วยงานของสำนักงานเลขาธิการวุฒิสภาเพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือลดความเสียหายของผลกระทบที่อาจเกิดขึ้นจากความเสี่ยง ในการดำเนินงานตามภารกิจต่าง ๆ รวมทั้งโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือที่มีอยู่แต่ยังไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง

โดยมีเป้าหมายการวางแผนจัดการความเสี่ยง คือ

1) ลดโอกาสที่จะเกิดความเสี่ยง

2) ลดความรุนแรงของผลกระทบจากความเสี่ยงนั้น ในกรณีที่ความเสี่ยงนั้นเกิดขึ้น

3) เปลี่ยนลักษณะของผลลัพธ์ที่จะเกิดขึ้นของความเสี่ยงให้เป็นไปในรูปที่องค์กรหรือหน่วยงานต้องการหรือยอมรับได้

<u>ทางเลือกในการจัดการความเสี่ยง</u>

แนวทางการจัดการความเสี่ยงมีหลายวิธี และสามารถปรับเปลี่ยนให้เหมาะสมกับสถานการณ์ขึ้นอยู่กับดุลยพินิจของผู้รับผิดชอบ แต่อย่างไรก็ตาม แนวทางการบริหารจัดการความเสี่ยงต้องคุ้มค่ากับการลดระดับผลกระทบความเสี่ยง

<u>กลยุทธ์ที่ใช้สำหรับจัดการแต่ละความเสี่ยง</u>

1) การหลีกเลี่ยงความเสี่ยง : ปฏิเสธและหลีกเลี่ยงโอกาสที่จะเกิดความเสี่ยง โดยการหยุด ยกเลิก หรือเปลี่ยนแปลงกิจกรรมหรือโครงการที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยง

2) การควบคุมความสูญเสีย : พยายามลดความเสี่ยงโดยการเพิ่มเติม หรือเปลี่ยนแปลงขั้นตอนบางส่วนของกิจกรรมหรือโครงการที่นำไปสู่เหตุการณ์ที่เป็นความเสี่ยง รวมถึงลดความน่าจะเป็นที่เหตุการณ์ที่เป็นความเสี่ยงจะเกิดขึ้น

3) การรับความเสี่ยงไว้เอง : หากทำการวิเคราะห์แล้วเห็นว่าไม่มีวิธีการจัดการความเสี่ยงใดเลยที่เหมาะสมเนื่องจากต้นทุนการจัดการความเสี่ยงสูงกว่าประโยชน์ที่จะได้รับ อาจต้องยอมรับความเสี่ยง แต่ควรมีมาตรการติดตามอย่างใกล้ชิดเพื่อรองรับผลที่จะเกิดขึ้น

4) การถ่ายโอนความเสี่ยง : ยกภาระในการเผชิญหน้ากับเหตุการณ์ที่เป็นความเสี่ยงและการจัดการกับความเสี่ยงให้ผู้อื่น

การจัดทำแผนบริหารความเสี่ยงเพื่อกำหนดมาตรการหรือแผนปฏิบัติการในการจัดการและควบคุมความเสี่ยงที่สูง (High) และสูงมาก (Extreme) นั้นให้ลดลง ให้อยู่ในระดับที่ยอมรับได้ สามารถปฏิบัติได้จริงและให้สามารถติดตามและประเมินผลการจัดการความเสี่ยงนั้นได้ พิจารณาถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุนที่ต้องใช้ลงทุนในการกำหนดมาตรการหรือแผนปฏิบัติการนั้นกับประโยชน์ที่จะได้รับด้วย

9. การรายงานและติดตามผล (Risk Monitoring)

จะต้องมีการรายงานและติดตามผลเป็นระยะ เพื่อให้เกิดความมั่นใจว่าได้มีการดำเนินงานไปอย่างถูกต้องและเหมาะสม โดยมีเป้าหมายในการติดตามผล คือ เป็นการประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการดำเนินการไปแล้วว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่ โดยหน่วยงานต้องสอบทานดูว่าวิธีการบริหารจัดการความเสี่ยงใด มีประสิทธิภาพดีก็ให้ดำเนินการต่อไป หรือวิธีการบริหารจัดการความเสี่ยงใดควรปรับเปลี่ยน และนำผลการติดตามไปรายงานให้ฝ่ายบริหารทราบตามแบบรายงานที่ได้กล่าวไว้ข้างต้น ทั้งนี้ กระบวนการสอบทานหน่วยงานอาจกำหนดข้อมูลที่ต้องติดตาม หรืออาจทำ Check List การติดตาม พร้อมทั้งกำหนดความถี่ในการติดตามผล โดยสามารถติดตามผลได้ใน 2 ลักษณะ คือ

1) การติดตามผลเป็นรายครั้ง (Separate Monitoring) เป็นการติดตามตามรอบระยะเวลาที่กำหนด เช่น ทุก 3 เดือน 6 เดือน 9 เดือน หรือทุกสิ้นปี เป็นต้น

2) การติดตามผลในระหว่างการปฏิบัติงาน (Ongoing Monitoring) เป็นการติดตามที่รวมอยู่ในการดำเนินงานต่าง ๆ ตามปกติของหน่วยงาน

10. การประเมินผลการบริหารความเสี่ยง (Risk Evaluation)

คณะทำงานจัดทำระบบการจัดการความเสี่ยงจะต้องทำสรุปรายงานผลและประเมินผลการบริหารความเสี่ยงประจำปีต่อคณะกรรมการหรือผู้บริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา เพื่อให้มั่นใจว่าสำนักงานเลขาธิการวุฒิสภามีการบริหารความเสี่ยงเป็นไปอย่างเหมาะสม เพียงพอ ถูกต้อง และมีประสิทธิผล มาตรการหรือกลไกการควบคุมความเสี่ยง (Control Activity) ที่ดำเนินการสามารถลดและควบคุมความเสี่ยงที่เกิดขึ้นได้จริง และอยู่ในระดับที่ยอมรับได้ หรือต้องจัดหามาตรการหรือตัวควบคุมอื่นเพิ่มเติม เพื่อให้ความเสี่ยงที่ยังเหลืออยู่หลังมีการจัดการ (Residual Risk) อยู่ในระดับที่ยอมรับได้และให้องค์กรมีการบริหารความเสี่ยงอย่างต่อเนื่องจนเป็นวัฒนธรรมในการดำเนินงาน

11. การทบทวนแผนบริหารความเสี่ยง (Risk Review)

การทบทวนแผนบริหารความเสี่ยง เป็นการทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอน เพื่อการปรับปรุงและพัฒนาแผนงานในการบริหารความเสี่ยงให้ทันสมัยและเหมาะสมกับการปฏิบัติงานจริงเป็นประจำทุกปี

บทที่ 4 ความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา

CHAPTER 4

กระบวนการบริหารความเสี่ยง

จากการวิเคราะห์เพื่อพิจารณาความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา ซึ่งได้ข้อมูลจากการจัดโครงการจัดทำแผนบริหารความเสี่ยงสำนักงานเลขาธิการวุฒิสภา ซึ่งมีการบรรยายเพื่อสร้างความรู้ความเข้าใจเกี่ยวกับทฤษฎีและหลักการบริหารความเสี่ยง ตลอดจนแนวทางในการดำเนินการจัดทำแผนบริหารความเสี่ยง และการ Workshop ระดมความคิดเห็นเพื่อจัดทำร่างแผนบริหารความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา รวมถึงโครงการพัฒนาคุณภาพการปฏิบัติงานของส่วนราชการสังกัดสำนักงานเลขาธิการวุฒิสภาตามมาตรฐานระบบบริหารคุณภาพ ISO 9001 : 2015 หลักสูตร “เทคนิคการบริหารความเสี่ยง (Risk Management)” ซึ่งได้มีการระดมความคิดเห็นเพื่อจัดทำแผนบริหารความเสี่ยง มีการกำหนดค่าความเสี่ยงและเรียงลำดับในเหตุการณ์ความเสี่ยง และการคัดเลือกเหตุการณ์ความเสี่ยงที่สำคัญ เพื่อกำหนดแนวทางในการจัดการตามแนวคิดการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM) นั้น

ทั้งนี้ สำนักเลขาธิการวุฒิสภา ได้พิจารณาประเด็นความเสี่ยงต่าง ๆ ที่มีโอกาสเกิดขึ้น รวมถึงผลกระทบจากความเสี่ยงนั้น ๆ และได้นำข้อมูลในการปฏิบัติภารกิจต่าง ๆ มาดำเนินการระบุความเสี่ยง หรือค้นหาความเสี่ยงด้วยวิธีการระดมความคิดเห็นร่วมกันระหว่างผู้เกี่ยวข้องผ่านการประชุมเชิงปฏิบัติการเพื่อค้นหาและประเมินความเสี่ยง พร้อมทั้งคัดเลือกกระบวนงาน/งานในภารกิจที่มีโอกาส/ความเสี่ยงต่อองค์กรตามกรอบการประเมินความเสี่ยง โดยสามารถคัดเลือกความเสี่ยงที่นำมากำหนดไว้เป็นความเสี่ยงของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. 2567 จำนวน 11 ประเด็นความเสี่ยง ดังตารางความเสี่ยงต่อไปนี้

ตารางระบุความเสี่ยง (Event Identification)

ความเสี่ยง	
ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S) จำนวน 1 ความเสี่ยง ได้แก่	
1	**ประเด็นความเสี่ยงที่ 1** : การขับเคลื่อนแผนปฏิบัติราชการของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง) ไม่สามารถดำเนินได้ตามเป้าหมาย (การดำเนินการในปีงบประมาณ พ.ศ. 2567)

ความเสี่ยง	
ความเสี่ยงด้านการปฏิบัติตามกฎหมาย กฎ ระเบียบ และข้อบังคับต่าง ๆ (Compliance Risk : C) จำนวน **2** ความเสี่ยง ได้แก่	
2	**ประเด็นความเสี่ยงที่ 2** : พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (Personal Data Protection Act : PDPA)
3	**ประเด็นความเสี่ยงที่ 3** : การรั่วไหลของข้อมูลข่าวสารลับในที่ประชุมวุฒิสภา (ภายใต้กฎหมาย 5 ฉบับ)
ความเสี่ยงด้านการดำเนินงาน (Operational Risk : O) จำนวน **8** ความเสี่ยง ได้แก่	
4	**ประเด็นความเสี่ยงที่ 4** : พื้นที่ในส่วนของสำนักงานเลขาธิการวุฒิสภาภายในอาคารรัฐสภา ยังเป็นพื้นที่ก่อสร้างที่ยังไม่สมบูรณ์และยังไม่ได้ส่งมอบ 100%
5	**ประเด็นความเสี่ยงที่ 5** : ความเสี่ยงของภาวะวิกฤติที่มีผลกระทบต่อสำนักงานเลขาธิการวุฒิสภา
6	**ประเด็นความเสี่ยงที่ 6** : บุคลากรขาดองค์ความรู้เฉพาะทางที่เกี่ยวกับกฎหมายเฉพาะด้าน หรือมีความยุ่งยากซับซ้อน
7	**ประเด็นความเสี่ยงที่ 7** : ความไม่เสถียรของระบบเครือข่ายในการประชุมคณะกรรมาธิการ
8	**ประเด็นความเสี่ยงที่ 8** : ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต ขัดข้อง ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) กระแสไฟฟ้าขัดข้องของอุปกรณ์ควบคุมไฟฟ้า
9	**ประเด็นความเสี่ยงที่ 9** : ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware
10	**ประเด็นความเสี่ยงที่ 10** : ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร
11	**ประเด็นความเสี่ยงที่ 11** : ความเสี่ยงจากการถูก Backlist โดย Search Engine หรือ Spamhaus

จากการวิเคราะห์และพิจารณาระบุความเสี่ยง (Event Identification) แล้ว จึงดำเนินการพิจารณาโอกาส/ความถี่ที่จะเกิดเหตุการณ์ (Likelihood) ว่ามีโอกาส/ความถี่ที่จะเกิดนั้นมากน้อยเพียงใด และความรุนแรงของผลกระทบ (Impact) ว่ามีระดับความรุนแรง หรือมีความเสียหายเพียงใดของแต่ละปัจจัยเสี่ยง ต่อมาจึงได้นำผลที่ได้มาพิจารณาความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงว่าก่อให้เกิดระดับของความเสี่ยงในระดับใด เพื่อจะได้นำไปพิจารณาจัดระดับความสำคัญของระดับความเสี่ยง (โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของเหตุการณ์ต่าง ๆ (Likelihood x Impact)) ซึ่งจัดแบ่งเป็น 5 ระดับ สามารถแสดงเป็น Risk Profile แบ่งพื้นที่เป็น 5 ส่วน (5 Quadrant) แสดงสถานะความเสี่ยงที่เกิดขึ้นโดยสัญลักษณ์สีไฟ เขียวเข้ม เขียว เหลือง ส้ม แดง โดยมีรายละเอียดตามตารางสถานะความเสี่ยง

ทั้งนี้ เมื่อได้มีการวิเคราะห์สถานะความเสี่ยงของแต่ละความเสี่ยงแล้ว จะได้นำไปดำเนินการกำหนดแผนบริหารจัดการความเสี่ยงระดับองค์กร ซึ่งจะมีการกำหนดมาตรการตอบสนองความเสี่ยง ระยะเวลาดำเนินการ ตัวชี้วัด และผู้รับผิดชอบ ของความเสี่ยงทั้ง 11 ความเสี่ยง ดังต่อไปนี้

ตารางแสดงสถานะความเสี่ยง (Risk Profile)

ความเสี่ยง	โอกาส	ผลกระทบ	ระดับความเสี่ยง	สถานะ
ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S)				
ประเด็นความเสี่ยงที่ 1 : การขับเคลื่อนแผนปฏิบัติราชการของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง) ไม่สามารถดำเนินได้ตามเป้าหมาย (การดำเนินการในปีงบประมาณ พ.ศ. 2567)	3	5	15	**เสี่ยงสูง**
ความเสี่ยงด้านการปฏิบัติตามกฎหมาย กฎ ระเบียบ และข้อบังคับต่าง ๆ (Compliance Risk : C)				
ประเด็นความเสี่ยงที่ 2 : พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA)	3	5	15	**เสี่ยงสูง**
ประเด็นความเสี่ยงที่ 3 : การรั่วไหลของข้อมูลข่าวสารลับในที่ประชุมวุฒิสภา (ภายใต้กฎหมาย 5 ฉบับ)	1	5	5	**เสี่ยงน้อย**
ความเสี่ยงด้านการดำเนินงาน (Operational Risk: O)				
ประเด็นความเสี่ยงที่ 4 : พื้นที่ในส่วนของสำนักงานเลขาธิการวุฒิสภาภายในอาคารรัฐสภายังเป็นพื้นที่ก่อสร้างที่ยังไม่สมบูรณ์และยังไม่ได้ส่งมอบ 100%	3	3	9	**เสี่ยงปานกลาง**
ประเด็นความเสี่ยงที่ 5 : ความเสี่ยงของภาวะวิกฤติที่มีผลกระทบต่อสำนักงานเลขาธิการวุฒิสภา	4	5	20	**เสี่ยงสูงมาก**
ประเด็นความเสี่ยงที่ 6 : บุคลากรขาดองค์ความรู้เฉพาะทางที่เกี่ยวกับกฎหมายเฉพาะด้านหรือมีความยุ่งยากซับซ้อน	3	5	15	**เสี่ยงสูง**
ประเด็นความเสี่ยงที่ 7 : ความไม่เสถียรของระบบเครือข่ายในการประชุมคณะกรรมาธิการ	2	4	8	**เสี่ยงปานกลาง**
ประเด็นความเสี่ยงที่ 8 : ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) กระแสไฟฟ้าขัดข้องของอุปกรณ์ควบคุมไฟฟ้า	3	3	9	**เสี่ยงปานกลาง**
ประเด็นความเสี่ยงที่ 9 : ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	4	3	12	**เสี่ยงสูง**
ประเด็นความเสี่ยงที่ 10 : ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	3	3	9	**เสี่ยงปานกลาง**
ประเด็นความเสี่ยงที่ 11 : ความเสี่ยงจากการถูก Backlist โดย Search Engine หรือ Spamhaus	4	4	16	**เสี่ยงสูง**

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
1. การขับเคลื่อนแผนปฏิบัติราชการของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง) ไม่สามารถดำเนินได้ตามเป้าหมาย (การดำเนินการในปีงบประมาณ พ.ศ. 2567)	Strategic ความเสี่ยงด้านกลยุทธ์	สำนักงานเลขาธิการวุฒิสภาไม่สามารถขับเคลื่อนแผนงานหรือโครงการต่าง ๆ ที่จะนำไปสู่เป้าหมายของแผนปฏิบัติราชการของสำนักงานเลขาธิการวุฒิสภา โดยเฉพาะประเด็นในการสนับสนุนการขับเคลื่อนภารกิจด้านนิติบัญญัติตามบทบัญญัติรัฐธรรมนูญและกฎหมาย การส่งเสริมการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข และการบริหารจัดการองค์กรให้มีขีดสมรรถนะสูงสู่ความเป็น Smart Digitalization	3	5	15 เสี่ยงสูง	แนวทางการดำเนินการ 1. ติดตามการดำเนินงานตามแผนงาน/โครงการวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้น โดยการคาดการณ์ความเสี่ยงที่ส่งผลกระทบต่อแผนงาน/เป้าประสงค์/ตัวชี้วัด/ผลผลิต/ผลลัพธ์/งบประมาณ ตามแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 - 2570 2. มีระบบสำหรับการติดตามแผนงาน/โครงการที่สามารถประมวลผลการติดตามได้อย่างมีประสิทธิภาพ 3. จัดทำระบบการตรวจสอบเปรียบเทียบผลการดำเนินการและแผนปฏิบัติราชการว่าเป็นไปที่กำหนดไว้หรือไม่	เอกสาร 1. แนวนโยบายในการขับเคลื่อนแผนปฏิบัติราชการ 2. ระบบการตรวจสอบเปรียบเทียบผลการดำเนินการและแผนปฏิบัติราชการ 3. แผนงานหรือแนวทางป้องกันรวมถึงแนวทางในการแก้ไขหากผลการดำเนินการไม่เป็นไปตามเป้าหมาย วิธีการวัด 1. รายงานเปรียบเทียบผลการดำเนินการและแผนปฏิบัติราชการว่าเป็นไปตามที่กำหนดไว้หรือไม่ 2. รายงานการแก้ไขปัญหาหรือการคาดการณ์จากสถานการณ์ที่ส่งผลกระทบต่อเป้าหมาย/ตัวชี้วัดเชิงยุทธศาสตร์ของสำนักงานฯ (ถ้ามี)	1. สำนักนโยบายและแผน 2. ทุกสำนัก

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
						3. จัดทำแนวทางป้องกัน รวมถึงแนวทางในการแก้ไข หากผลการดำเนินการไม่เป็นไปตามเป้าหมาย <u>เป้าหมาย</u> สำนักงานสามารถดำเนินการต่าง ๆ ได้เป็นไปตามแผนปฏิบัติราชการ และสามารถบรรลุเป้าหมายตามที่ได้กำหนดไว้		

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
2. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) เริ่มมีผลใช้บังคับวันที่ 1 มิถุนายน 2565	Compliance ความเสี่ยงด้านการปฏิบัติตามกฎหมาย กฎระเบียบและข้อบังคับต่าง ๆ	อาจมีการรวบรวม การใช้ การเปิดเผย การจัดเก็บ และการทำลายข้อมูลส่วนบุคคลที่ไม่สอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ที่เกิดจากผู้ปฏิบัติไม่ทราบถึงนโยบายและและแนวปฏิบัติในการดูแลข้อมูลฯ ภายในการการทำงานของแต่ละกลุ่มงาน	3	5	15  เสี่ยงสูง	แนวทางการดำเนินการ 1. ดำเนินการแต่งตั้งคณะกรรมการเพื่อพิจารณาดำเนินการเกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ของสำนักงานเลขาธิการวุฒิสภา 2. จัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลฯ ของสำนักงานเลขาธิการวุฒิสภา 3. จัดแผนงานในภาพรวม เป้าหมาย 1. ไม่พบปัญหาข้อร้องเรียนหรือฟ้องร้องจากผู้มีส่วนเกี่ยวข้องอันเกิดจากการไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ 2. ไม่พบปัญหาการไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ จากการตรวจสอบภายใน	เอกสาร 1. คำสั่งแต่งตั้งฯ 2. แนวนโยบายในการคุ้มครองข้อมูลส่วนบุคคลฯ 3. แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลฯ 4. แผนงานดำเนินการเกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ของสำนักงานเลขาธิการวุฒิสภา วิธีการวัด 1. ทะเบียนรับเรื่องร้องเรียนจากผู้มีส่วนได้ส่วนเสีย 2. รายงานผลการตรวจสอบภายในประจำปีงบประมาณ	1. สำนักบริหารงานกลาง (กลุ่มงานวินัย) 2. ทุกสำนัก

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
3. การรั่วไหลของข้อมูลข่าวสารลับในที่ประชุมวุฒิสภา (ภายใต้กฎหมาย 5 ฉบับ กฎหมายที่เกี่ยวข้อง จำนวน 5 ฉบับ ได้แก่ ข้อบังคับการประชุมวุฒิสภา พ.ศ. 2562, ระเบียบวุฒิสภาว่าด้วยการประชุมลับในที่ประชุมวุฒิสภา พ.ศ. 2563, ระเบียบสำนักงานเลขาธิการวุฒิสภาว่าด้วยการบริหารจัดการการประชุมลับและข้อมูลข่าวสารลับของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2563, กฎ ก.ร. ว่าด้วยวินัยข้าราชการรัฐสภาสามัญ พ.ศ. 2555 และประมวลจริยธรรมข้าราชการรัฐสภา พ.ศ. 2554)	<u>Compliance Risk</u> ความเสี่ยงด้านการปฏิบัติตามกฎหมาย กฎระเบียบและข้อบังคับต่าง ๆ	1. ความรับผิดทางกฎหมาย เช่น หน่วยงานอาจถูกฟ้องร้องดำเนินคดี และเจ้าหน้าที่ถูกดำเนินการทางวินัย 2. ความน่าเชื่อถือขององค์กร	1	5	5 เสี่ยงน้อย	<u>แนวทางการดำเนินการ</u> 1. จัดทำข้อพึงปฏิบัติเกี่ยวกับข้อมูลข่าวสารลับในที่ประชุมวุฒิสภา 2. จัดทำคำสั่ง เรื่องแต่งตั้งเจ้าหน้าที่แจกเอกสารรายงานลับและบัตรออกเสียงลงคะแนนลับ 3. ควบคุมการรับและคืนเอกสารลับและจัดทำบัตรลงคะแนนลับการส่งคืนเอกสารลับให้แก่เจ้าของเรื่องหรือสำนักที่รับผิดชอบโดยเร็วที่สุด <u>เป้าหมาย</u> ไม่พบการรั่วไหลของข้อมูลข่าวสารในที่ประชุมวุฒิสภาที่เกิดจากเจ้าหน้าที่	<u>เอกสาร</u> 1. ข้อพึงปฏิบัติเกี่ยวกับข้อมูลข่าวสารลับในที่ประชุมวุฒิสภา 2. คำสั่ง เรื่องแต่งตั้งเจ้าหน้าที่แจกเอกสารรายงานลับและบัตรออกเสียงลงคะแนนลับ <u>วิธีการวัด</u> 1. จำนวนเอกสารลับที่ส่งคืนครบถ้วน 2. ใบควบคุมการรับและคืนเอกสารลับ และบัตรลงคะแนนลับมีจำนวนตรงกัน	สำนักการประชุม

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
4. พื้นที่ในส่วนของสำนักงานเลขาธิการวุฒิสภาภายในอาคารรัฐสภายังเป็นพื้นที่ก่อสร้างที่ยังไม่สมบูรณ์และยังไม่ได้ส่งมอบ 100%	Operational Risk ความเสี่ยงด้านการดำเนินงาน	ปัญหาในพื้นที่ใช้สอยส่วนใหญ่ไม่สามารถดำเนินการใด ๆ ได้เองทันทีที่เกี่ยวกับการดูแลและการให้บริการ เช่น การซ่อมแซมและบำรุงรักษาอาคาร ซึ่งอาจทำให้เกิดความล่าช้าและข้อร้องเรียนที่เกิดจากความไม่พร้อมใช้งานด้านอาคารและสถานที่ได้	3	3	9 เสี่ยงปานกลาง	แนวทางการดำเนินการ 1. ตรวจสอบแก้ไขหากดำเนินการแก้ไขเองได้ก็สามารถดำเนินการทันทีโดยมีการบันทึกและรายงานผล 2. ตรวจสอบแก้ไขเบื้องต้นหากดำเนินการแก้ไขเองไม่ได้ต้องประสานผู้รับเหมาหรือที่ปรึกษาบริหารโครงการก่อสร้างอาคารรัฐสภาแห่งใหม่ซึ่งเป็นผู้รับผิดชอบการสร้างอาคารรัฐสภาและผู้ที่เกี่ยวข้องทราบและให้ดำเนินการผ่านช่อง บันทึก Defect แจ้งซ่อม โทรศัพท์และช่องทาง Line กลุ่มซ่อมระบบไฟฟ้า/เครื่องปรับอากาศ/ประปาห้องน้ำ/ลิฟต์และบันไดเลื่อนรวมถึงงานสถาปัตย์โดยมีการบันทึกและรายงานผล	เอกสาร 1. บันทึกการประชุมข้อหารือและหาแนวปฏิบัติตัวแทนผู้รับเหมาและที่ปรึกษาบริหารโครงการก่อสร้างอาคารรัฐสภาแห่งใหม่ 2. บันทึกรายงานผู้บริหารสำนักงานเลขาธิการวุฒิสภา วิธีการวัด ทะเบียนรับเรื่องร้องเรียนของสำนักงาน	สำนักบริหารงานกลาง (กลุ่มงานอาคารและสถานที่)

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
						<u>เป้าหมาย</u> ข้อร้องเรียนด้านการใช้งานอาคารและสถานที่ ที่เกิดจากความไม่พร้อมใช้งานไม่เกิน 5 ครั้ง/เดือน		

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
5. ความเสี่ยงของภาวะวิกฤติที่มีผลกระทบต่อสำนักงานเลขาธิการวุฒิสภา	Operational Risk ความเสี่ยงด้านการดำเนินงาน	อาจเกิดความไม่สงบจนเกิดเหตุร้ายจนเกิดผลกระทบต่อผู้รับบริการ และประชาชน รวมถึงชีวิตและความปลอดภัยของบุคลากร ทรัพย์สินของสำนักงาน ตลอดจนส่งผลกระทบต่อความไว้วางใจและความน่าเชื่อถือที่มีต่อหน่วยงานที่เกิดจากการหยุดชะงักหรือไม่สามารถให้บริการแก่ประชาชนได้ ทำให้ผู้รับบริการต้องเสียโอกาส เสียเวลาและงบประมาณ อาจก่อให้เกิดความเสียหายในภาพรวม เช่น ด้านเศรษฐกิจ การเงิน สังคม ชุมชน สิ่งแวดล้อม ตลอดจนชีวิต ความปลอดภัยและทรัพย์สินของบุคลากรของสำนักงาน เป็นต้น	4	5	20 เสี่ยงสูงมาก	แนวทางการดำเนินการ 1. ดำเนินการแต่งตั้งคณะกรรมการ และคณะอนุกรรมการแผนบริหารเหตุการณ์พิเศษของสำนักงานเลขาธิการวุฒิสภา 2. จัดทำแผน BCM เพื่อบริหารจัดการเหตุการณ์พิเศษฯ เป้าหมาย ไม่พบการเกิดเหตุร้ายที่กระทบต่อความปลอดภัยของบุคคล และทรัพย์สินของสำนักงานฯ	เอกสาร 1. คำสั่งแต่งตั้งคณะกรรมการและคณะอนุกรรมการ ฯ 2. แผน BCM วิธีการวัด รายงานของคณะกรรมการเหตุการณ์พิเศษฯ	สำนักบริหารงานกลาง

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
6. บุคลากรขาดองค์ความรู้เฉพาะทางที่เกี่ยวกับกฎหมายเฉพาะด้านหรือมีความยุ่งยากซับซ้อน	Operational Risk ความเสี่ยงด้านการดำเนินงาน	1. ด้านคุณภาพ : อาจทำให้การทำงานไม่ถูกต้องครบถ้วน ซึ่งอาจส่งผลทำให้เกิดข้อร้องเรียนได้ (ก.ป. และ อ.พ.) 2. ด้านเวลา : ทำให้ต้องใช้เวลาในการปฏิบัติงานมาก ซึ่งอาจทำให้เกิดความล่าช้าและเสร็จไม่ทันก่อนวันประชุมวุฒิสภา ซึ่งอาจส่งผลทำให้เกิดข้อร้องเรียนได้ (อ.พ.)	3	5	15 เสี่ยงสูง	แนวทางการดำเนินการ 1. สอบถามหน่วยงานที่รับผิดชอบกฎหมายเฉพาะด้านในประเด็นที่ยังมีองค์ความรู้และข้อมูลไม่ครบถ้วน 2. รวบรวมและสืบค้นข้อมูลจากเอกสารข้อมูลซึ่งหน่วยงานที่เกี่ยวข้องได้ดำเนินการรวบรวมไว้และสืบค้นทางเว็บไซต์ เป้าหมาย ไม่พบปัญหาข้อร้องเรียนจากสมาชิกวุฒิสภา และประชาชน ที่เกิดจากขาดองค์ความรู้เฉพาะทางที่เกี่ยวกับกฎหมายเฉพาะด้านหรือมีความยุ่งยากซับซ้อนทั้งปฏิบัติงานล่าช้าข้อมูลไม่ถูกต้องครบถ้วน	เอกสาร ตารางหน่วยงานที่รับผิดชอบกฎหมายเฉพาะด้านหรือมีความยุ่งยากซับซ้อน วิธีการวัด ทะเบียนรับเรื่องร้องเรียนของสำนักงานเลขาธิการวุฒิสภา	สำนักกฎหมาย

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
7. ความไม่เสถียรของระบบเครือข่ายในการประชุมคณะกรรมาธิการ	Operational Risk ความเสี่ยงด้านการดำเนินงาน	เกิดความขัดข้องในการประชุมคณะกรรมาธิการ ทำให้การประชุมไม่ราบรื่น ซึ่งอาจจะส่งผลทำให้เจ้าหน้าที่โดนตำหนิ และอาจทำให้เกิดข้อร้องเรียนได้	2	4	8 เสี่ยงปานกลาง	แนวทางการดำเนินการ 1. ทำการตรวจสอบระบบเครือข่ายทุกครั้ง ก่อนเริ่มการประชุมคณะกรรมาธิการ 2. มีเจ้าหน้าที่ควบคุมภายในห้องประชุมตลอดเวลา เป้าหมาย ไม่พบการร้องเรียนของคณะกรรมาธิการจากปัญหาความขัดข้องในการประชุมที่เกิดจากความไม่เสถียรของระบบเครือข่ายในการประชุมคณะกรรมาธิการ ที่ไม่สามารถแก้ไขได้ทันต่อเวลา จนทำให้การประชุมหยุดชะงักหรือไม่สามารถดำเนินการประชุมต่อไปได้	เอกสาร บันทึกการควบคุมกระบวนการประชุมคณะกรรมาธิการ (FM-BC-02) วิธีการวัด ทะเบียนบันทึกปัญหาการจัดประชุมคณะกรรมาธิการ และทะเบียนรับเรื่องร้องเรียนของสำนักงานเลขาธิการวุฒิสภา	สำนักกรรมาธิการ 1/ สำนักกรรมาธิการ 2/ สำนักกรรมาธิการ 3

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
8. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) กระแสไฟฟ้าขัดข้องของอุปกรณ์ควบคุมไฟฟ้า	Operational Risk ความเสี่ยงด้านการดำเนินงาน	1. ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านเครือข่าย 2. ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่าย	3	3	9 เสี่ยงปานกลาง	แนวทางการดำเนินการ 1. ตรวจสอบ Availability ของ Server ด้วยโปรแกรมตรวจสอบ 2. การจัดทำเส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า 1 เส้นทาง 3. การวาง Web Server ไว้มากกว่า 1 ที่ เช่น ที่ ISP 4. การจัดตั้งศูนย์สำรอง (DR Site) เป้าหมาย - เครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลมีการ Downtime ไม่เกิน 36 ชั่วโมงต่อปี - ร้อยละ 90 ของอุปกรณ์ในโครงการได้รับการแก้ไขปัญหาข้อขัดข้องทันตามเวลาที่สำนักงานเลขาธิการวุฒิสภากำหนด	เอกสาร 1. รายงานผลการตรวจสอบ Availability ของ Server 2. รายงานการบริหารจัดการเครือข่ายอินเทอร์เน็ต (Gateway) 3. สรุปผลการบริหารจัดการ Web Server วิธีการวัด รายงานการรับแจ้งปัญหาการใช้งานในระบบ Helpdesk	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
9. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	Operational Risk ความเสี่ยงด้านการดำเนินงาน	1. ความเสี่ยงต่อการถูกทำลายโปรแกรมหรือข้อมูลใช้คอมพิวเตอร์ไม่ได้ 2. ความเสี่ยงต่อการไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติใช้ระบบงานไม่ได้ 3. ความเสี่ยงต่อการถูกขโมยข้อมูลที่สำคัญข้อมูลที่สำคัญสูญหาย	4	3	12 เสี่ยงสูง	แนวทางการดำเนินการ 1. ใช้ระบบป้องกันไวรัสกับเครื่องแม่ข่ายที่ต้องเสียค่าใช้จ่าย 2. อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ 3. มีการสำรองข้อมูลที่เครื่องลูกข่ายที่จำเป็นไว้อย่างสม่ำเสมอทาง External Hard Disk หรือ DVD เป้าหมาย 1. สามารถป้องกันการโจมตีจากภายนอกเครือข่ายได้ไม่น้อยกว่า ร้อยละ 80 2. ไม่พบข้อมูลสูญหาย/ใช้คอมพิวเตอร์ไม่ได้	เอกสาร 1. บันทึกการใช้โปรแกรมป้องกันไวรัสกับเครื่องแม่ข่าย 2. บันทึกการอัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ 3. มีการสำรองข้อมูลที่เครื่องลูกข่ายที่จำเป็นไว้อย่างสม่ำเสมอทาง External Hard Disk หรือ DVD วิธีการวัด 1. log การป้องกันการโจมตี 2. รายงานการรับแจ้งข้อมูลสูญหาย/ปัญหาการใช้งานในระบบ Helpdesk	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
10. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	Operational Risk ความเสี่ยงด้านการดำเนินงาน	ความเสี่ยงต่อการใช้ช่องโหว่โปรแกรมหรือการซ่อน Script ไว้ในโปรแกรม จนอาจถูกขโมยข้อมูล และนำไปเผยแพร่ ซึ่งการเข้าถึงข้อมูลของสำนักงานฯ กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานฯ	3	3	9 เสี่ยงปานกลาง	แนวทางการดำเนินการ 1. ตั้งมาตรฐานในการพัฒนาซอร์ฟแวร์ตามคำแนะนำของ OWASP-Top 10 Web Application Security Risks เพื่อลดความเสี่ยง 2. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ เป้าหมาย 1. สามารถแก้ไขหากพบการรั่วไหลของข้อมูลจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร ร้อยละ 80 2. ไม่พบปัญหาถูกขโมยข้อมูล	เอกสาร แผนกิจกรรมให้ความรู้มาตรการการกำหนดชั้นความลับ วิธีการวัด 1. รายงานการแก้ไขจากการรั่วไหลของข้อมูลจากช่องโหว่ฯ 2. รายงานการรับแจ้งข้อมูลสูญหายในระบบ Helpdesk	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
11. ความเสี่ยงจากการถูก Backlist โดย Search Engine หรือ Spamhaus	Operational Risk ความเสี่ยงด้านการดำเนินงาน	1. ผู้ใช้งานที่ต้องการข้อมูลของสำนักงานฯ หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน - Web Server - การใช้งานเครือข่าย - การใช้งาน e-mail 2. สำนักงานฯ ขาดความน่าเชื่อถือ อาจส่งผลทำให้เกิดข้อร้องเรียน จากผู้ใช้งานที่ต้องการข้อมูลของสำนักงานฯ หรือประชาชนทั่วไปได้	4	4	16 เสี่ยงสูง	แนวทางการดำเนินการ 1. ติดตั้งโปรแกรมเพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ต โดยเฉพาะจาก SMTP Mail Server ซึ่งมักจะเป็นแหล่งที่ Hacker ชอบใช้ในการส่ง Spam 2. ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server หรือ FTP 3. มีการอัพเดทตัวโปรแกรมและ Signature อย่างสม่ำเสมอ และการทำการบำรุงรักษาทั้งฮาร์ดแวร์และซอร์ฟแวร์ พร้อมทั้ง Update Licenses	เอกสาร 1. ทะเบียนการติดตั้งโปรแกรม 2. แผนกิจกรรมรณรงค์การตรวจสอบข้อมูลก่อนอัพโหลด 3. บันทึกการอัพเดตโปรแกรม วิธีการวัด 1. รายงานการแก้ไขหากพบถูก Blacklist โดย Search Engine หรือ Spamhaus 2. ทะเบียนรับเรื่องร้องเรียน	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

แผนบริหารจัดการความเสี่ยงระดับองค์กร

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง			แผนดำเนินการ		หน่วยงานรับผิดชอบ
			โอกาสเกิด	ผลกระทบ	ระดับคะแนน	การดำเนินการ	เอกสารหลักฐาน	
						<u>เป้าหมาย</u> 1. สามารถแก้ไขหากพบถูก Blacklist โดย Search Engine หรือ Spamhaus ร้อยละ 80 2. ไม่พบเรื่องร้องเรียนที่เกิดจากไม่สามารถเข้าใช้งาน Web Server/การใช้งานเครือข่าย/e-mail ได้		