ประกาศสำนักงานเลขาธิการวุฒิสภา
เรื่อง ให้ใช้แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา
พ.ศ. ๒๕๖๘ – ๒๕๗๐ (ฉบับปรับปรุง)

.....

ตามที่สำนักงานเลขาธิการวุฒิสภาได้มีการประกาศใช้แผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ประจำปี พ.ศ. ๒๕๖๘ - ๒๕๗๐ เมื่อวันที่ ๓๐ กรกฎาคม พ.ศ. ๒๕๖๘ เพื่อใช้เป็นกรอบการดำเนินงานตามมาตรการบริหารความเสี่ยงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา ตามนโยบายเลขาธิการวุฒิสภา ในการรักษามาตรฐานคุณภาพ และความสำเร็จของสำนักงานให้ยั่งยืนและยกระดับการบริหารจัดการองค์กรให้เท่าทันต่อการเปลี่ยนแปลง เพื่อการเป็นองค์กรอัจฉริยะ “I SENATE+” ซึ่งเป็นไปตามแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๖ - ๒๕๗๐ (ฉบับปรับปรุง พ.ศ. ๒๕๖๘) ในแผนปฏิบัติราชการเรื่องที่ ๓ พัฒนาระบบการบริหารจัดการมุ่งสู่ความเป็น Smart Digitalization ตัวชี้วัดที่ ๑๗ ร้อยละความสำเร็จของการป้องกันการถูกบุกรุกโจมตีทางไซเบอร์ ตัวชี้วัดที่ ๑๘ จำนวนชั่วโมงของการหยุดทำงาน (Downtime) ของระบบเทคโนโลยีสารสนเทศของสำนักงานเลขาธิการวุฒิสภา ในแนวทางการพัฒนาที่ ๓.๒ พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล และเป็นไปตามแผนพัฒนารัฐสภาดิจิทัล (Digital Parliament) พ.ศ. ๒๕๖๖ - ๒๕๗๐ ที่มีวัตถุประสงค์การดำเนินการ เพื่อให้มีความทันสมัยและรองรับการดำเนินงานด้านเทคโนโลยีดิจิทัลของส่วนราชการ ในประเด็นพัฒนาที่ ๔ การพัฒนาดิจิทัลที่ยั่งยืน (Digital Development and Sustainability) แผนงานที่ ๑ แผนงานพัฒนาโครงสร้างพื้นฐานดิจิทัล (Digital Infrastructure) และแผนงานที่ ๒ แผนงานความมั่นคงปลอดภัย (Cyber Security) ได้มีการปรับปรุง เพื่อเป็นกรอบในการกำหนดทิศทางการดำเนินงาน ด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา นั้น

บัดนี้ สำนักงานเลขาธิการวุฒิสภาได้จัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๘ – ๒๕๗๐ (ฉบับปรับปรุง) เพื่อใช้แทนแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๘ - ๒๕๗๐ เป็นที่เรียบร้อยแล้ว

ดังนั้น เพื่อให้บรรลุวัตถุประสงค์ของการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา จึงให้ส่วนราชการภายในสังกัดสำนักงานเลขาธิการวุฒิสภา ตลอดจนผู้มีหน้าที่เกี่ยวข้องทุกฝ่าย ได้นำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๘ – ๒๕๗๐ (ฉบับปรับปรุง) เพื่อใช้เป็นแนวทางในการดำเนินงานด้านเทคโนโลยีดิจิทัล ของสำนักงานเลขาธิการวุฒิสภา ต่อไป

ประกาศ ณ วันที่ ๒๕ มิถุนายน พ.ศ. ๒๕๖๙

(นางปัณณิตา สท้านไตรภพ)
เลขาธิการวุฒิสภา

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล ของสำนักงานเลขาธิการวุฒิสภา

พ.ศ. 2568 - 2570 (ฉบับปรับปรุง)

คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล
ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 - 2570

คำนำ

การเปลี่ยนแปลงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ณ อาคารรัฐสภา ได้มีการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัลเพื่อรองรับการพัฒนาตามแผนยุทธศาสตร์ กลยุทธ์ โดยตอบสนองกับนโยบายของเลขาธิการวุฒิสภา “I Senate+” ในการรักษาคุณภาพและความสำเร็จของสำนักงาน และยกระดับการบริหารจัดการองค์กรให้เท่าทันต่อการเปลี่ยนแปลงเพื่อเป็นองค์กรอัจฉริยะ โดยสำนักงานเลขาธิการวุฒิสภาได้มีการจัดทำแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง พ.ศ. 2568) ในส่วนของแผนปฏิบัติราชการเรื่องที่ 3 พัฒนาระบบการบริหารจัดการมุ่งสู่ความเป็น Smart Digitalization เป้าหมายที่ 1 : พัฒนาระบบบริหารจัดการฐานข้อมูลและโครงสร้างพื้นฐานระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลให้ทันสมัย แนวทางการพัฒนา 3.2 พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล การบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล สิ่งที่สำคัญในการสนับสนุนให้องค์กรสามารถดำเนินงานได้บรรลุตามเป้าหมายที่กำหนดแล้ว จึงได้นำกรอบแนวทางการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ (Enterprise Risk Management – Integrated Framework) ตามแนวทาง COSO - ERM มาประยุกต์ใช้เป็นกรอบและแนวทางในการพัฒนาระบบการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงาน ซึ่งมีวัตถุประสงค์ในการให้ผู้บริหาร เจ้าหน้าที่ที่เกี่ยวข้องในองค์กรตระหนักถึงความสำคัญของการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล และการใช้เทคโนโลยีดิจิทัลที่มีความทันสมัย ส่งผลกระทบต่อระบบการปฏิบัติงานที่ปรับเป็นดิจิทัลเต็มรูปแบบได้มีอย่างมีประสิทธิภาพ โดยมีการกำหนดแนวทางดำเนินการการวิเคราะห์ความเสี่ยงของระบบเทคโนโลยีดิจิทัล ในการวางแผนการป้องกันการโจมตีทางไซเบอร์ขององค์กร

ดังนั้น จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2569 – 2570 เพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล โดยมีการระบุความเสี่ยง วิเคราะห์ความเสี่ยง ตอบสนองความเสี่ยง และเลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้น ให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite) โดยมุ่งหวังให้สามารถบรรลุตามเป้าประสงค์ขององค์กร หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 - 2570 ฉบับปรับปรุง จะช่วยให้ผู้รับผิดชอบที่เกี่ยวข้องใช้เป็นแนวทางในการลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ต่อไป

คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล
ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 - 2570
มิถุนายน 2569

สารบัญ

หน้า

1. หลักการและเหตุผล 1
2. วัตถุประสงค์ของการจัดทำบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา 3
3. วิสัยทัศน์ และพันธกิจ ตามแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง พ.ศ. 2568) ที่เกี่ยวข้องด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา 4
4. แผนพัฒนารัฐสภาดิจิทัล (Digital Parliament) พ.ศ. 2566 – 2570 (ฉบับปรับปรุง) 7
5. กระบวนการบริหารความเสี่ยงระบบเทคโนโลยีดิจิทัล 9
   - 5.1 คำนิยาม 9
   - 5.2 ลักษณะของความเสี่ยง 9
   - 5.3 กระบวนการบริหารความเสี่ยง 9
   - 5.4 ประเภทความเสี่ยงด้านเทคโนโลยีดิจิทัล 16
   - 5.5 การตอบสนองความเสี่ยง 18
   - 5.6 ปัจจัยเสี่ยง 18
   - 5.7 การประเมินความเสียหาย 19
   - 5.8 การติดตามและรายงานผล 19
   - 5.9 สถานภาพระบบรักษาความมั่นคงปลอดภัย ICT ของสำนักงานเลขาธิการวุฒิสภา 20
6. การวิเคราะห์การบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา 27
   - 6.1 ขั้นตอนการบริหารความเสี่ยง 28
   - 6.2 กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล 29
   - 6.3 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา 29
   - 6.4 ผลการประเมินแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล 32
7. สรุปผลและข้อเสนอแนะ 56
   - 7.1 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานฯ 56
   - 7.2 สรุป 62
   - 7.3 ข้อเสนอแนะ 62
8. การบริหารจัดการและการติดตามประเมินผลแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 – 2570 (ฉบับปรับปรุง) 63

ภาคผนวก

สารบัญตาราง

ตารางที่		หน้า
1	โอกาสที่จะเกิดความเสี่ยง	13
2	ผลกระทบจากความเสี่ยง	13
3	ฮาร์ดแวร์ ซอฟต์แวร์ ด้านความมั่นคงปลอดภัยของสำนักงานเลขาธิการวุฒิสภา	21
4	เกณฑ์ประเมินความเสี่ยง	28
5	ประเด็นความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของสำนักงานเลขาธิการวุฒิสภา	30
6	ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักงานเลขาธิการวุฒิสภา	32

สารบัญภาพ

ภาพที่		หน้า
1	แผนภาพระบบเครือข่าย (Network Diagram) สำนักงานเลขาธิการวุฒิสภา	25
2	ขั้นตอนการประเมินความเสี่ยง	27
3	กระบวนการจัดทำการบริหารความเสี่ยง	28
4	แผนผังการประเมินความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization)	29

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 – 2570 (ฉบับปรับปรุง)

1 หลักการและเหตุผล

การเปลี่ยนแปลงสภาพแวดล้อมในการดำเนินงานด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ทั้งปัจจัยภายใน อาทิ การปรับเปลี่ยนแผนยุทธศาสตร์ กลยุทธ์ โดยตอบสนองกับนโยบายของเลขาธิการวุฒิสภา I Senate+ ในการรักษาคุณภาพและความสำเร็จของสำนักงานและยกระดับการบริหารจัดการองค์กร ให้เท่าทันต่อการเปลี่ยนแปลงเพื่อเป็นองค์กรอัจฉริยะ โดยสำนักงานเลขาธิการวุฒิสภาได้มีการจัดทำแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง พ.ศ. 2568) และแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. 2569 แผนปฏิบัติราชการเรื่องที่ 3 พัฒนาระบบการบริหารจัดการมุ่งสู่ความเป็น Smart Digitalization เป้าหมายที่ 1 พัฒนาระบบบริหารจัดการฐานข้อมูล และโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลให้ทันสมัย แนวทางการพัฒนาที่ 3.2 พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล รวมถึงการเปลี่ยนแปลงทรัพยากรภายในสำนักงานการเปลี่ยนแปลงวัสดุอุปกรณ์ ระบบงานสารสนเทศที่สนับสนุนในด้านการปฏิบัติงาน รวมถึงปัจจัยภายนอก อาทิ เหตุการณ์ความไม่สงบทางการเมืองภัยธรรมชาติ โรคระบาด เป็นต้น อาจส่งผลกระทบให้การดำเนินงานของสำนักงานไม่เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์ซึ่งจะก่อให้เกิดความเสี่ยงต่อสำนักงานโดยรวม การบริหารความเสี่ยงเป็นส่วนที่สำคัญในการดำเนินตามองค์ประกอบของการกำกับดูแลกิจการที่ดี สนับสนุนให้องค์กร สามารถดำเนินงานได้บรรลุตามเป้าหมายที่กำหนดแล้วจึงได้นำกรอบแนวทางการบริหาร ความเสี่ยงขององค์กรเชิงบูรณาการ (Enterprise Risk Management – Integrated Framework) ตามแนวทาง COSO - ERM มาประยุกต์ใช้เป็นกรอบและแนวทางในการพัฒนาระบบการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงาน ซึ่งมีวัตถุประสงค์ในการให้ผู้บริหาร เจ้าหน้าที่ที่เกี่ยวข้องในองค์กรตระหนักถึงความสำคัญ ของการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล และมีความเข้าใจตรงกันในคำนิยาม เป้าหมายและวัตถุประสงค์ อันจะเป็นการสร้างความรับผิดชอบของผู้ที่เกี่ยวข้อง และเป็นไปในทิศทางเดียวกันในสำนักงานได้อย่างมีประสิทธิภาพ เพื่อใช้เป็นแนวทางให้ผู้บริหาร เจ้าหน้าที่ในส่วนที่เกี่ยวข้องขององค์กร เป็นส่วนหนึ่งของการพัฒนากระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่กำหนดไว้ ในแผนเพื่อให้สำนักงานมีกรอบการดำเนินการตามมาตรการที่อาจส่งผลให้เกิดความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลได้อย่างเป็นระบบรวมทั้งมีการดำเนินการเพื่อสร้างพื้นฐานในการป้องกัน ความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลระยะยาวที่สำคัญให้สำนักงานเพื่อเป็นกลไกในการพัฒนาองค์ความรู้ด้านการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลสำหรับ

ผู้บริหาร เจ้าหน้าที่และสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน มีความตระหนัก และมีความเข้าใจตรงกันถึงเป้าหมาย วัตถุประสงค์ รวมทั้งแนวทางการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงาน เพื่อร่วมกันสร้างความพึงพอใจให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholders) และสร้างมูลค่าเพิ่มให้องค์กรโดยพิจารณาถึงผลกระทบต่อเป้าหมายการดำเนินงานของสำนักงานให้เป็นไปตามหลักการกำกับดูแลกิจการที่ดี

การบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เป็นองค์ประกอบสำคัญของการดำเนินงานด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภาเป็นอย่างมาก จึงมีความจำเป็นในการกำหนดนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา เพื่อบังคับใช้กับทุกหน่วยงานที่เกี่ยวข้องของสำนักงานเลขาธิการวุฒิสภา โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจและตระหนักถึงหน้าที่ความรับผิดชอบต่อการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลอยู่เสมอ และยังสนับสนุนให้เจ้าหน้าที่ทุกระดับชั้นเข้าใจ รวมถึงมีส่วนร่วมในการบริหารและจัดการความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล ปฏิบัติงานที่เกี่ยวข้อง ประกอบด้วยการวางระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลภายในหน่วยงานได้อย่างมีประสิทธิภาพ ควบคุม และลดผลกระทบจากเหตุการณ์ความเสียหายที่อาจเกิดขึ้น โดยกระบวนการดังกล่าว อยู่ภายใต้การดูแลของผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร และมีการกำกับดูแลและสั่งการโดยคณะทำงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล

การบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลจึงเป็นกลไกสำคัญในการวางรากฐานเพื่อป้องกันความเสี่ยงในระยะยาว พัฒนาองค์ความรู้ และส่งเสริมให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรอย่างยั่งยืน ทั้งยังเป็นการตอบสนองต่อแนวนโยบายและแนวปฏิบัติของฝ่ายบริหารมาดำเนินการด้วยหลักการบริหารจัดการภาครัฐแนวใหม่ตามพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546 ที่มุ่งเน้นการพัฒนาระบบราชการไทยให้มีขีดสมรรถนะสูง และสอดคล้องกับ เกณฑ์การประเมิน PMQA 4.0 ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่เน้นการบริหารจัดการข้อมูลสารสนเทศ และระบบดิจิทัลอย่างมีประสิทธิภาพ รวมถึงการวิเคราะห์ความเสี่ยงและการวางแผนรับมือภัยคุกคามทางไซเบอร์และภาวะฉุกเฉิน

ดังนั้น เพื่อรองรับความมั่นคงปลอดภัยด้านระบบเทคโนโลยีดิจิทัลขององค์กร สำนักงานเลขาธิการวุฒิสภาจึงได้จัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2569 – 2570 ขึ้น โดยมุ่งหวังให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจ ตระหนักถึงหน้าที่ความรับผิดชอบ และมีส่วนร่วมในการบริหารจัดการความเสี่ยง เพื่อให้การดำเนินงานด้านเทคโนโลยีดิจิทัลของสำนักงานเป็นไปอย่างมีประสิทธิภาพและสร้างความพึงพอใจให้แก่ผู้มีส่วนได้ส่วนเสียทุกฝ่ายอย่างยั่งยืน

2 วัตถุประสงค์ของการจัดทำบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล ของสำนักงานเลขาธิการวุฒิสภา

2.1 เพื่อให้มีการวิเคราะห์ความเสี่ยงของระบบเทคโนโลยีดิจิทัล กำหนดมาตรการ/กรอบแนวทางการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล การวางแผน ควบคุม และแก้ไขความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล บรรจุในแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 - 2570 (ฉบับปรับปรุง)

2.2 เพื่อให้มีมาตรการ การวางแผน ควบคุม และแก้ไขความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล การโจมตีทางไซเบอร์ ของสำนักงานฯ ได้อย่างเหมาะสมในเวลาที่จำกัดอย่างมีประสิทธิภาพ

2.3 เพื่อช่วยเพิ่มประสิทธิภาพในการบริหารความเสี่ยงอันจะมีผลกระทบต่อการดำเนินงานให้เป็นไปตามแนวนโยบาย และเป้าประสงค์ เพื่อพิจารณาดำเนินการหาแนวทางในการป้องกัน หรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มดำเนินงานหรือดำเนินงานตามแผน

2.4 เพื่อให้ผู้ปฏิบัติงานตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นได้ และดำเนินการจัดการความเสี่ยงที่เกี่ยวข้องให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสาร มีความเข้าใจกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานฯ และนำไปปฏิบัติตามแผน

3 วิสัยทัศน์ และพันธกิจ ตามแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง พ.ศ. 2568) ที่เกี่ยวข้องด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา

3.1 วิสัยทัศน์ ของสำนักงานเลขาธิการวุฒิสภา

กำหนดไว้ว่า “มุ่งสู่องค์กรอัจฉริยะ ในการสนับสนุนภารกิจของวุฒิสภา เพื่อประโยชน์ของประเทศชาติและประชาชน”

3.2 พันธกิจ

กำหนดไว้ว่า

1. สนับสนุนการขับเคลื่อนภารกิจด้านนิติบัญญัติตามบทบัญญัติรัฐธรรมนูญและกฎหมาย

2. ส่งเสริมการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

3. บริหารจัดการองค์กรให้มีขีดสมรรถนะสูงสู่ความเป็น Smart Digitalization

3.3 แผนงานและแนวทางการพัฒนา

3.3.1 แผนปฏิบัติราชการเรื่องที่ 1 พัฒนางานและสร้างการมีส่วนร่วมด้านกฎหมาย และวิชาการ เพื่อสนับสนุนงานด้านนิติบัญญัติ

เป้าหมายที่ 1 : ยกระดับการพัฒนางานด้านกฎหมาย และงานด้านวิชาการให้ตอบสนองความต้องการของสมาชิกวุฒิสภา

เป้าหมายที่ 2 : พัฒนาความร่วมมือและสนับสนุนข้อมูลด้านกฎหมายและวิชาการเพื่อสนับสนุนงานด้านนิติบัญญัติ

<u>แนวทางการพัฒนา</u>

1.1 พัฒนารูปแบบและเนื้อหาที่มีความถูกต้อง รวดเร็ว สะดวกในการเข้าถึงงานด้านกฎหมายและวิชาการที่ตอบสนองความต้องการของผู้รับบริการ มีการออกแบบกระบวนงานที่บูรณาการร่วมกัน และนำเทคโนโลยีดิจิทัลมาใช้

1.2 สร้างเครือข่าย และการมีส่วนร่วมงานด้านกฎหมาย และวิชาการ

3.3.2 แผนปฏิบัติราชการเรื่องที่ 2 พัฒนากลไกการสร้างความรู้และการมีส่วนร่วมในการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

เป้าหมายที่ 1 : ประชาชนมีความรู้ ความเข้าใจ และเล็งเห็นถึงความสำคัญของหน้าที่และอำนาจของวุฒิสภา และในการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

เป้าหมายที่ 2 : สร้างเครือข่ายและการมีส่วนร่วมทางการเมืองตามบทบัญญัติของรัฐธรรมนูญ

<u>แนวทางการพัฒนา</u>

2.1 เสริมสร้างความรู้ ความเข้าใจหน้าที่และอำนาจของวุฒิสภา และสร้างเครือข่ายในการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข

2.2 ส่งเสริมการมีส่วนร่วมต่อการพิจารณาร่างกฎหมาย การควบคุมการบริหารราชการแผ่นดินและการให้ความเห็นชอบผู้ดำรงตำแหน่งตามรัฐธรรมนูญและกฎหมาย

3.3.3 แผนปฏิบัติราชการเรื่องที่ 3 พัฒนาระบบการบริหารจัดการมุ่งสู่ความเป็น Smart Digitalization

เป้าหมายที่ 1 : พัฒนาระบบบริหารจัดการฐานข้อมูล และโครงสร้างพื้นฐานระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลให้ทันสมัย

เป้าหมายที่ 2 : พัฒนาระบบงานที่มีประสิทธิภาพ และเป็นที่ยอมรับของผู้รับบริการ

เป้าหมายที่ 3 : สร้างและนำนวัตกรรมเพื่อยกระดับการให้บริการ

<u>แนวทางการพัฒนา</u>

3.1 พัฒนาระบบและโครงสร้างฐานข้อมูลเทคโนโลยีดิจิทัลและเชื่อมโยงข้อมูลในแนวทางการบูรณาการข้อมูลภาครัฐ

3.2 พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล

3.3 พลิกโฉมกระบวนการปฏิบัติงานให้มีประสิทธิภาพมากขึ้น

3.4 สร้างนวัตกรรมด้วยเทคโนโลยีดิจิทัล

3.3.4 แผนปฏิบัติราชการเรื่องที่ 4 พัฒนาบุคลากรให้มีขีดสมรรถนะสูง มีคุณธรรม มีความสุขและความผูกพัน

เป้าหมายที่ 1 : พัฒนาศักยภาพระบบการบริหารทรัพยากรบุคคลให้มีประสิทธิภาพและทันสมัย

เป้าหมายที่ 2 : พัฒนาศักยภาพของบุคลากรให้มีความรู้ ความสามารถ และทักษะการคิดวิเคราะห์ให้ทันต่อการเปลี่ยนแปลง

เป้าหมายที่ 3 : บุคลากรมีวัฒนธรรมและค่านิยมที่สอดคล้องกับเป้าหมายขององค์กร

เป้าหมายที่ 4 : พัฒนาคุณภาพชีวิตและสภาพแวดล้อมที่ดีในการปฏิบัติงาน

<u>แนวทางการพัฒนา</u>

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

จากวิสัยทัศน์และพันธกิจ แผนงานและแนวทางการพัฒนา โดยสรุปส่วนที่เกี่ยวข้องในแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง พ.ศ. 2568) ในส่วนของแผนปฏิบัติราชการเรื่องที่ 3 พัฒนาระบบการบริหารจัดการมุ่งสู่ความเป็น Smart Digitalization เป้าหมายที่ 1 : พัฒนาระบบบริหารจัดการฐานข้อมูล และโครงสร้างพื้นฐานระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลให้ทันสมัย แนวทางการพัฒนา 3.2 พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภาซึ่งมีหน้าที่หลักในการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานฯ จะเป็นผู้รับผิดชอบดำเนินการ ในการกำหนดแผนการปฏิบัติงานตามแนวทางและแผนในการบริหารความเสี่ยง ด้านเทคโนโลยีดิจิทัล โดยได้พิจารณาจากแนวทางด้านการพัฒนาฐานข้อมูลและสารสนเทศและการสื่อสาร และเครื่องมือด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ที่มีส่วนหลัก ๆ หลายด้าน ได้แก่

1. การพัฒนาโครงสร้างพื้นฐานดิจิทัล (Digital Infrastructure)
   1.1 ด้านคอมพิวเตอร์แม่ข่าย (Server)
   1.2 คอมพิวเตอร์ลูกข่าย และอุปกรณ์ต่อพ่วง (Clients and Peripherals)
   1.3 อุปกรณ์ดิจิทัล Laptop Tablet SmartPhone
   1.4 ด้านเครือข่าย (Networks)
2. งานด้านความมั่นคงปลอดภัย (Cybersecurity)
3. การพัฒนาระบบงานดิจิทัล (Development Digital Systems)
4. การพัฒนาทักษะดิจิทัล (Digital Skill) สำหรับบุคลากร (Human Resources)

การจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภาเป็นสิ่งที่สำคัญในการขับเคลื่อนให้แผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 – 2570 (ฉบับปรับปรุง พ.ศ. 2568) ในการสนับสนุนการพัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล

4 แผนพัฒนารัฐสภาดิจิทัล (Digital Parliament) พ.ศ. 2566 – 2570 (ฉบับปรับปรุง)

4.1 วิสัยทัศน์

"รัฐสภาดิจิทัล (Digital Parliament)" หมายถึง องค์กรที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้อย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อสนับสนุนงานด้านนิติบัญญัติ”

4.2 ประเด็นพัฒนา และแผนงาน

ประเด็นพัฒนาที่ 1 รัฐสภาอัจฉริยะแห่งอนาคต (Advanced Intelligence Parliament)

<u>แผนงาน</u>

1 แผนงานการพัฒนามาตรฐานกระบวนงานดิจิทัล (Digital Process Standard and Improvement)

2) แผนงานระบบบริหารจัดการทรัพยากร (Enterprise Resource Planning)

3) แผนงานเพิ่มศักยภาพระบบสารสนเทศด้านนิติบัญญัติ (Enhancing the Legislation Information System)

ประเด็นพัฒนาที่ 2 การขับเคลื่อนองค์กรด้วยข้อมูล (Data-Driven Organization)

<u>แผนงาน</u>

1) แผนงานมาตรฐานการแลกเปลี่ยนข้อมูล (Data Exchange Standard)

2) แผนงานแพลตฟอร์มข้อมูลขนาดใหญ่ (Big Data Platform)

3) แผนงานระบบอัจฉริยะสนับสนุนการตัดสินใจ (Intelligence Decision Support System)

ประเด็นพัฒนาที่ 3 การขับเคลื่อนการมีส่วนร่วมด้วยนวัตกรรมดิจิทัลและประชาธิปไตย (Digital Participation and Engagement Innovation)

<u>แผนงาน</u>

1) แผนงานการมีส่วนร่วมดิจิทัล (Digital Participation)

2) แผนงานการประชาสัมพันธ์และการสื่อสาร ดิจิทัล (Digital Public Engagement)

ประเด็นพัฒนาที่ 4 การพัฒนาดิจิทัลที่ยั่งยืน (Digital Development and Sustainability)

<u>แผนงาน</u>

1) แผนงานพัฒนาโครงสร้างพื้นฐานดิจิทัล (Digital Infrastructure)

2) แผนงานความมั่นคงปลอดภัย (Cybersecurity)

3) แผนงานระบบสนับสนุนการทำงานนอกที่ตั้ง (Work Anywhere Platform)

ประเด็นพัฒนาที่ 5 พัฒนาด้านวัฒนธรรมดิจิทัล (Digital Culture)

<u>แผนงาน</u>

แผนงานพัฒนาทักษะด้านดิจิทัลของส่วนราชการ สังกัดรัฐสภา มีเป้าหมายเพื่อสนับสนุนการพัฒนาบุคลากรให้มีกระบวนทัศน์ดิจิทัล (Digital Mindset) และทักษะดิจิทัล (Digital Skill)

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร ในฐานะผู้ดูแลระบบเครือข่ายสารสนเทศและการสื่อสาร ซึ่งหมายถึง ผู้ทำหน้าที่รับผิดชอบในการดูแล บำรุงรักษาเครือข่ายสารสนเทศและการสื่อสารของสำนักงานฯ ที่สามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ ระบบการสื่อสารข้อมูล ระบบสารสนเทศและการสื่อสารของสำนักงานฯ เพื่อการบริหารจัดการ นอกเหนือจากนั้นยังเป็นผู้รับผิดชอบ การบริหารจัดการให้เป็นไปตามแผนบริหารความเสี่ยงทางด้านเทคโนโลยีดิจิทัล รวมถึงความเสี่ยงทางด้านระบบเทคโนโลยีดิจิทัล เพราะหากมีการวางแผนที่ดีและมีการจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพแล้วจะลดความเสี่ยงระบบเทคโนโลยีดิจิทัล ที่อาจจะเกิดขึ้นได้ตามสภาวการณ์ต่าง ๆ อีกทั้งยังอำนวยความสะดวกในการดำเนินการ มีแนวทางในการป้องกันและแก้ไขความเสี่ยงที่อาจจะเกิดขึ้นได้ ซึ่งจะช่วยให้การบริหารงานของสำนักงานฯ รวมถึงการให้บริการแก่สมาชิกวุฒิสภา คณะกรรมาธิการ ผู้มีส่วนได้ส่วนเสีย และประชาชนได้อย่างมีประสิทธิภาพสูงสุด และเพื่อเป็นการรองรับการให้บริการตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติการบริหารงาน และการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 เป็นไปตามแผนพัฒนารัฐสภาดิจิทัล (Digital Parliament) พ.ศ. 2566 – 2570 (ฉบับปรับปรุง) ประเด็นพัฒนาที่ 4 การพัฒนาดิจิทัลที่ยั่งยืน (Digital Development and Sustainability) แผนงานความมั่นคงปลอดภัย (Cybersecurity) การจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภาเป็นสิ่งที่สำคัญของแผนงานความมั่นคงปลอดภัย (Cybersecurity) ซึ่งจะช่วยขับเคลื่อนให้การพัฒนารัฐสภาดิจิทัลในประเด็น "การพัฒนาดิจิทัลที่ยั่งยืน" บรรลุผลสำเร็จได้อย่างมั่นคงและปลอดภัย

5 กระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

5.1 คำนิยาม

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ใด ๆ ที่อาจจะเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งจะส่งผลกระทบหรือสร้างความเสียหาย ทั้งที่สามารถตีมูลค่าเป็นตัวเงินได้และที่ไม่สามารถตีมูลค่าเป็นตัวเงินได้ หรือ อาจก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าประสงค์ตามภารกิจหลักและเป็นไปตามแผนปฏิบัติราชการของสำนักงานฯ

การบริหารความเสี่ยง หมายถึง ระบบการบริหารและควบคุม รวมทั้งกระบวนการดำเนินงานต่าง ๆ เพื่อที่จะลดสาเหตุของโอกาสที่จะก่อให้เกิดความเสียหาย เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ สามารถประเมินผล ควบคุม และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าประสงค์ตามภารกิจหลัก และเป้าหมายตามแผนปฏิบัติราชการของสำนักงานฯ เป็นสำคัญ

การบริหารความเสี่ยงมีความจำเป็นที่จะต้องอาศัยขั้นตอนที่ต่อเนื่อง เนื่องจากมีการระบุ ความเสี่ยงอันจะมีผลกระทบจากความเสี่ยง และมาตรการหรือแผนปฏิบัติการในการจัดการความเสี่ยงนั้นได้ถูกดำเนินการตามแผนที่วางไว้

5.2 ลักษณะของความเสี่ยง

ลักษณะของความเสี่ยงสามารถแบ่งออกได้เป็น 3 ลักษณะ ดังนี้

1) ปัจจัยเสี่ยง หมายถึง สาเหตุที่จะทำให้เกิดความเสี่ยง

2) เหตุการณ์เสี่ยง หมายถึง เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงานหรือนโยบาย

3) ผลกระทบของความเสี่ยง หมายถึง ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

5.3 กระบวนการบริหารความเสี่ยง

ปัจจุบันระบบเทคโนโลยีดิจิทัล ได้เข้ามามีบทบาทสำคัญในการดำเนินงานของสำนักงานเลขาธิการวุฒิสภา ในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล ตลอดจนการใช้เครื่องคอมพิวเตอร์แม่ข่าย การจัดทำและพัฒนาระบบเทคโนโลยีดิจิทัลในภาพรวมมุ่งหวังที่จะให้ระบบดิจิทัลมีส่วนช่วยในการปฏิบัติงานรองรับภารกิจของสำนักงานฯ มีความสะดวก รวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น แต่การนำเทคโนโลยีดิจิทัลมาใช้ย่อมมีความเสี่ยง

หลายประการด้วยกัน การวางแผนและการบริหารความเสี่ยงของระบบเทคโนโลยีดิจิทัล จึงเป็นเรื่องสำคัญ และควรมีการเตรียมการที่ดี หากสำนักงานฯ ไม่มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัลที่รัดกุมเพียงพอ อาจส่งผลกระทบต่อการดำเนินงานและสร้างความเสียหายต่อสำนักงานฯ ได้ ทั้งในด้านการพัฒนาสำนักงานฯ การสนับสนุนผู้มีส่วนได้ส่วนเสียการพัฒนาบุคลากรและความคุ้มค่าทางด้านงบประมาณที่ใช้

ดังนั้น การบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล จึงต้องมีทั้งการวางแผนเพื่อขจัดหรือลดความเสี่ยง และการประเมินผลในการบริหารจัดการความเสี่ยง เพื่อลดโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่อาจเกิดขึ้น และสามารถประเมินเป็นเชิงปริมาณหรือเชิงคุณภาพได้ ซึ่งมีกระบวนการบริหารความเสี่ยงตามหลักธรรมาภิบาลมาตรฐาน COSO - ERM (Committee of Sponsoring Organization of the Tread Way Commission – Enterprise Risk Management) เพื่อเตรียมการรองรับการเปลี่ยนแปลงที่อาจเกิดขึ้นและส่งผลกระทบต่อด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ซึ่งต้องมีการวิเคราะห์และบริหารจัดการความเสี่ยงตามประเด็นยุทธศาสตร์ที่เกี่ยวข้องให้ครบถ้วน โดยมีขั้นตอนการดำเนินการหรือเกณฑ์ในการวิเคราะห์ ประเมิน และจัดการความเสี่ยงอย่างเหมาะสมตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO - ERM ซึ่งมีขั้นตอนการดำเนินการ 8 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญ ในการกำหนดกรอบบริหารความเสี่ยง ประกอบด้วยปัจจัยหลายประการ เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงานบุคลากร กระบวนการทำงาน ระบบสารสนเทศ ระเบียบ เป็นต้น สภาพแวดล้อมภายในองค์กรประกอบเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กร

ขั้นตอนที่ 2 การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

เป็นการกำหนดวัตถุประสงค์ของการดำเนินการบริหารจัดการความเสี่ยง ซึ่งจะต้องสอดคล้องกับวิสัยทัศน์ พันธกิจ และยุทธศาสตร์การดำเนินงานขององค์กร ตั้งแต่ระดับองค์กร หน่วยงาน กิจกรรม จนถึงระดับบุคคล เพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าประสงค์ และเพื่อเพิ่มประสิทธิภาพในการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานฯ ที่น่าจะส่งผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย โดยพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้นก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินกิจการตามแผนที่กำหนดไว้ สำหรับวัตถุประสงค์ของการบริหารความเสี่ยงอาจแบ่งออกได้เป็น 2 ระดับ คือ

1) วัตถุประสงค์ระดับองค์กร (Corporate Objective) เป็นวัตถุประสงค์ของการดำเนินงานในภาพรวม ตามแผนยุทธศาสตร์และแผนปฏิบัติราชการประจำปีขององค์กร

2) วัตถุประสงค์ระดับกิจกรรม (Activities Objective) เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจงลงไปสำหรับแต่ละกิจกรรมที่องค์กรกำหนดเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การกำหนดวัตถุประสงค์ที่ชัดเจนช่วยให้การระบุและวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นได้อย่างครบถ้วน ซึ่งวัตถุประสงค์ที่กำหนดขึ้นในแต่ละระดับ ควรมีการกำหนดเป้าหมายและตัวชี้วัดความสำเร็จที่ชัดเจนและสามารถวัดผลได้วัตถุประสงค์ที่ดี (SMART) ควรมีลักษณะ

S : Specific หมายถึง มีการกำหนดเป้าหมายที่ชัดเจน
M : Measurable หมายถึง สามารถวัดผลหรือประเมินผลได้
A : Achievable หมายถึง สามารถปฏิบัติให้บรรลุผลได้
R : Reasonable หมายถึง สมเหตุผล มีความเป็นไปได้
T : Time constrained หมายถึง มีกรอบเวลาที่ชัดเจนและเหมาะสม

ขั้นตอนที่ 3 การระบุความเสี่ยงต่าง ๆ (Event Identification)

นอกจากการกำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารตามแนวทางของ COSO - ERM ออกเป็น 8 ประเภทแล้ว การระบุความเสี่ยง ยังต้องนำหลักธรรมาภิบาลมาเป็นปัจจัยในการวิเคราะห์และระบุความเสี่ยง เพื่อให้เป็นไปตามแนวทางการบริหารกิจการบ้านเมืองที่ดี ประกอบด้วย 10 ประการ ดังนี้

1) หลักประสิทธิผล (Effectiveness) หมายถึง ผลการปฏิบัติราชการที่บรรลุวัตถุประสงค์และเป้าหมายของแผนปฏิบัติราชการตามที่ได้รับงบประมาณมาดำเนินการ โดยการปฏิบัติราชการจะต้องมีทิศทางยุทธศาสตร์ และเป้าประสงค์ที่ชัดเจน มีกระบวนการปฏิบัติงาน และระบบงานที่เป็นมาตรฐาน รวมถึง การติดตาม ประเมินผล และพัฒนาปรับปรุงอย่างต่อเนื่องและเป็นระบบ

2) หลักประสิทธิภาพ (Efficiency) หมายถึง การบริหารราชการตามแนวทางการกำกับดูแลที่ดีที่มีการออกแบบกระบวนการปฏิบัติงาน โดยการใช้เทคนิคและเครื่องมือการบริหารจัดการที่เหมาะสม ให้องค์กรสามารถใช้ทรัพยากรทั้งด้านต้นทุน แรงงาน และระยะเวลาให้เกิดประโยชน์สูงสุดต่อการพัฒนาขีดความสามารถในการปฏิบัติราชการตามภารกิจ เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกกลุ่ม

3) หลักการตอบสนอง (Responsiveness) หมายถึง การให้บริการที่สามารถดำเนินการได้ภายในระยะเวลาที่กำหนดและสร้างความเชื่อมั่น ความไว้วางใจ รวมถึงตอบสนองตามความคาดหวัง/ความต้องการของประชาชนผู้รับบริการ และผู้มีส่วนได้ส่วนเสียที่มีความหลากหลายและมีความแตกต่าง

4) หลักภาระรับผิดชอบ (Accountability) หมายถึง การแสดงความรับผิดชอบในการปฏิบัติหน้าที่ และผลงานต่อเป้าหมายที่กำหนดไว้ โดยความรับผิดชอบนั้นควรอยู่ในระดับที่สนองต่อความคาดหวังของสาธารณะ รวมทั้งการแสดงถึงความสำนึกในการรับผิดชอบต่อปัญหาสาธารณะ

5) หลักความโปร่งใส (Transparency) หมายถึง กระบวนการเปิดเผยอย่างตรงไปตรงมา ชี้แจงได้เมื่อมีข้อสงสัย และสามารถเข้าถึงข้อมูลข่าวสารอันไม่ต้องห้ามตามกฎหมายได้อย่างเสรีโดยประชาชนสามารถรู้ทุกขั้นตอนในการดำเนินกิจกรรมหรือกระบวนการต่าง ๆ และสามารถตรวจสอบได้

6) หลักการมีส่วนร่วม (Participation) หมายถึง กระบวนการที่ข้าราชการประชาชน และผู้มีส่วนได้ส่วนเสียทุกกลุ่มมีโอกาสได้เข้าร่วมรับรู้ เรียนรู้ ทำความเข้าใจ ร่วมแสดงทัศนะ ร่วมเสนอปัญหา/ประเด็นที่สำคัญที่เกี่ยวข้อง ร่วมคิดแนวทาง ร่วมการแก้ไขปัญหา ร่วมในกระบวนการตัดสินใจ และร่วมกระบวนการพัฒนาในฐานะหุ้นส่วนพัฒนา

7) หลักการกระจายอำนาจ (Decentralization) หมายถึง การถ่ายโอนอำนาจการตัดสินใจ การมอบอำนาจและความรับผิดชอบในการตัดสินใจ และการดำเนินการให้แก่บุคลากร โดยมุ่งเน้นการสร้างความพึงพอใจในการให้บริการต่อผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย การปรับปรุงกระบวนการและเพิ่มผลิตภาพ เพื่อผลการดำเนินงานที่ดีของส่วนราชการ

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

9) หลักความเสมอภาค (Equity) หมายถึง การได้รับการปฏิบัติ และได้รับบริการอย่างเท่าเทียมกัน โดยไม่มีการแบ่งแยกด้านชาย/หญิง ถิ่นกำเนิด เชื้อชาติ ภาษา เพศ อายุ ความพิการ สภาพทางกายหรือสุขภาพ สถานะบุคคล ฐานะทางเศรษฐกิจและสังคม ความเชื่อทางศาสนา การศึกษา และอื่น ๆ

10) หลักมุ่งเน้นฉันทามติ (Consensus Oriented) หมายถึง การหาข้อตกลงทั่วไปภายในกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ซึ่งเป็นข้อตกลงที่เกิดจากการใช้กระบวนการ เพื่อหาข้อคิดเห็นจากกลุ่มบุคคลที่รับประโยชน์ และเสียประโยชน์ โดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง ซึ่งต้องไม่มีข้อคัดค้านที่ยุติไม่ได้ในประเด็นที่สำคัญ โดยฉันทามติไม่จำเป็นต้องหมายความว่าเป็นความเห็นพ้องโดยเอกฉันท์

<u>ขั้นตอนที่ 4 การประเมินความเสี่ยง (Risk Assessment)</u>

เป็นขั้นตอนในการใช้หลักเกณฑ์การให้คะแนนจากระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) มาเป็นเครื่องมือในการประเมิน ความเสี่ยง และกำหนดกลยุทธ์ที่ใช้จัดการกับความเสี่ยง โดยแบ่งการจัดระดับความเสี่ยง (Degree of Risk) ออกเป็น 4 ระดับ ตามระดับคะแนน ได้แก่ ระดับความเสี่ยงต่ำ

ระดับความเสี่ยงปานกลาง ระดับความเสี่ยงสูง และระดับความเสี่ยงสูงมาก ซึ่งการจัดทำแผนผังระดับความเสี่ยง (Risk Matrix) จะช่วยในการตัดสินใจในการวางแผนความเสี่ยงได้อย่างเหมาะสม และสามารถจัดลำดับความสำคัญในการจัดการได้ ซึ่งการประเมินความเสี่ยงด้วยวิธีการแบ่งการจัดระดับความเสี่ยงมีขั้นตอนดังนี้

1) การประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood : L) เป็นขั้นตอนการประเมินความเป็นไปได้ ความถี่ หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง แล้วจัดแบ่งระดับของโอกาสที่จะเกิดความเสี่ยง (Likelihood) ออกเป็น 5 ระดับ ตามตารางที่ 1

ตารางที่ 1 โอกาสที่จะเกิดความเสี่ยง

ระดับโอกาส	คำนิยาม
1	นาน ๆ ครั้ง (แทบไม่เกิดขึ้นเลย)
2	ไม่บ่อย (อาจเกิดขึ้นได้ทุก 5 ปี)
3	ปานกลาง (อาจเกิดขึ้นได้ทุกปี)
4	บ่อย (อาจเกิดขึ้นได้ทุกเดือน)
5	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

2) การประเมินความรุนแรงของผลกระทบ (Impact : I) เป็นขั้นตอนการประเมินขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง ซึ่งสามารถจัดแบ่งออกเป็นระดับต่าง ๆ ได้จากผลกระทบที่แตกต่างกันซึ่งแสดงตามตารางที่ 2

ตารางที่ 2 ผลกระทบจากความเสี่ยง

ผลกระทบ	คำนิยาม
1	- เกิดเหตุที่ไม่มีความสำคัญ - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการน้อยมาก (แทบไม่มีผลกระทบเลย)
2	- เกิดเหตุที่แก้ไขได้ - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการน้อย (เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ)
3	- ระบบ IT มีปัญหา และมีความสูญเสียไม่มาก - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)
4	- เกิดปัญหากับระบบ IT ที่สำคัญและระบบความปลอดภัย ซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการมาก (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)

ผลกระทบ	คำนิยาม
5	- เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูล - กระทบต่อความน่าเชื่อถือขององค์กร/ความพึงพอใจของผู้ใช้บริการมากที่สุด (ผู้บริหารถูกลงโทษทางวินัย)

3) การจัดระดับความเสี่ยง (Degree of Risk) เป็นขั้นตอนการนำผลการประเมินความเสี่ยงที่ประมวลจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) เข้าด้วยกัน (ระดับความเสี่ยง = ระดับโอกาส x ระดับผลกระทบ) แล้วจัดทำแผนผังระดับความเสี่ยง (Risk Matrix)

ขั้นตอนที่ 5 กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

เป็นการวิเคราะห์ทางเลือกกลยุทธ์ในการจัดการความเสี่ยง เพื่อช่วยในการตัดสินใจของบุคคลหรือองค์กรใด ๆ ในอันที่จะหาวิธีการที่ดีที่สุดในการตัดสินใจแก้ไขปัญหาต่าง ๆ ที่อาจเกิดขึ้นในอนาคต ทั้งนี้เพื่อลดผลกระทบหรือความเสียหายที่อาจเกิดขึ้นให้น้อยที่สุด โดยมีค่าใช้จ่ายน้อยที่สุด ซึ่งมีวิธีการจัดการ ดังนี้

1) การยอมรับความเสี่ยง (Take/Risk Acceptance) หมายถึง การไม่กระทำใด ๆ เพิ่มเติม กรณีนี้ใช้กับความเสี่ยงที่มีน้อย มีความน่าจะเกิดน้อย หรือเห็นว่ามีต้นทุนในการบริหารความเสี่ยงสูง โดยขออนุมัติหลักการรับความเสี่ยงไว้

2) การลด (Treat/Risk Reduction) หมายถึง การลดโอกาสที่จะเกิดความเสี่ยง การป้องกันการเกิดความสูญเสีย หรือลดผลกระทบจากเหตุการณ์ที่อาจเกิดขึ้นในอนาคต โดยการจัดระบบการควบคุม การกำหนดแผนสำรองในเหตุฉุกเฉิน การวิเคราะห์ข้อมูลในอดีตปัจจุบัน ซึ่งรวมถึงการคาดการณ์ในอนาคตประกอบการตัดสินใจ

3) การหลีกเลี่ยงความเสี่ยง (Terminate/Risk Avoidance) หมายถึง การหยุดหรือการเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น การงดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง หรือการปรับเปลี่ยนรูปแบบการทำงานและลดขอบเขตการดำเนินการ เป็นต้น

4) การกระจาย (Transfer/Risk Sharing) หรือโอนความเสี่ยง (Risk Spreading) หมายถึง การลดโอกาสความน่าจะเกิดหรือลดความเสียหายโดยการแบ่งโอน การหาผู้รับผิดชอบในความเสี่ยง การจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน และการจัดประกันภัย เป็นต้น

ขั้นตอนที่ 6 กิจกรรมการควบคุมความเสี่ยง (Control Activities)

เป็นขั้นตอนดำเนินการกำหนดกิจกรรม หรือมาตรการในการจัดการความเสี่ยงให้หมดไป หรือควบคุมความเสี่ยงให้ลดลงในระดับที่ยอมรับได้ โดยกิจกรรมที่กำหนดต้องเป็นกิจกรรมที่ยังไม่เคยปฏิบัติ หรือเป็นกิจกรรมที่กำหนดขึ้นเพิ่มเติมจากกิจกรรมเดิมที่เคยปฏิบัติอยู่แล้ว แต่กิจกรรมนั้นไม่สามารถควบคุมความเสี่ยงได้ นอกจากนี้ยังต้องกำหนดระยะเวลาที่ใช้ในการดำเนินการแต่ละกิจกรรม ตลอดจนหน่วยงานผู้รับผิดชอบ ดังนั้นกิจกรรมการบริหารความเสี่ยงต่าง ๆ ที่กำหนดขึ้นจึงมีเป้าหมายเพื่อควบคุมความเสี่ยง (Risk Control) ซึ่งสามารถแบ่งประเภทของการควบคุมความเสี่ยงออกเป็น 4 ประเภท ดังนี้

1) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

2) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว

3) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

4) การควบคุมเพื่อแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขใหม่ไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

ทั้งนี้ การดำเนินกิจกรรมการควบคุมควรต้องคำนึงถึงความคุ้มค่าในด้านค่าใช้จ่ายต้นทุนและผลประโยชน์ที่คาดว่าจะได้รับ โดยกิจกรรมการควบคุมควรมีองค์ประกอบดังนี้

1) วิธีการดำเนินงาน ซึ่งประกอบด้วยขั้นตอนและกระบวนการ

2) การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุม ซึ่งควรพิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน และพิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

3) กำหนดระยะเวลาแล้วเสร็จของงาน

ขั้นตอนที่ 7 ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

เป็นขั้นตอนและกระบวนการโดยมีวัตถุประสงค์เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง มีการเปิดช่องทางการสื่อสาร และรับทราบข้อมูลด้านการบริหารความเสี่ยงให้กับผู้บริหารและบุคลากรขององค์กรได้เข้าถึง โดยผ่านช่องทางต่าง ๆ เช่น ระบบอินทราเน็ต หนังสือเวียน การประชุมชี้แจงโดยผู้บริหาร หรือการฝึกอบรม เป็นต้น ซึ่งการสื่อสารที่มีประสิทธิผลนั้น ต้องให้มั่นใจได้ว่า

1) ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา

2) ผู้บริหารสามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่ได้ทันท่วงที

3) มีการติดตามแผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กร และจัดการความเสี่ยงต่าง ๆ เพื่อให้องค์กรมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด

ขั้นตอนที่ 8 การติดตามและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

การติดตาม และเฝ้าระวังความเสี่ยง โดยการกำหนดให้มีการติดตามและประเมินผลว่าแต่ละหน่วยงานมีการประเมินประสิทธิผลของการจัดการความเสี่ยงที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ เพื่อให้เกิดความมั่นใจว่ามาตรการในการปรับปรุงความเสี่ยงที่วางไว้มีความเพียงพอเหมาะสม มีประสิทธิภาพประสิทธิผล และมีการปฏิบัติจริง สามารถลดหรือป้องกันความเสี่ยงที่อาจเกิดขึ้น นับเป็นขั้นตอนสุดท้ายและเป็นปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง ซึ่งควรพิจารณาประเด็นต่อไปนี้

1) การรายงาน และสอบทานขั้นตอนตามกระบวนการบริหารความเสี่ยง เช่น การรายงานและติดตามผลระหว่างการดำเนินงาน (On Going Monitoring) เพื่อสังเกตติดตาม รายงานความคืบหน้า รวมทั้งสอบทานหรือยืนยันผลระหว่างการปฏิบัติงาน

2) ความชัดเจนและสม่ำเสมอของการมีส่วนร่วม และความมุ่งมั่นของผู้บริหารระดับสูง

3) บทบาทของผู้นำในการสนับสนุน และติดตามการบริหารความเสี่ยง

4) การประยุกต์ใช้เกณฑ์การประเมินผลการดำเนินงานที่เกี่ยวกับการบริหารความเสี่ยง เช่น การประเมินผลอิสระ (Independent Evaluation) ซึ่งเป็นการประเมินผลที่เกิดขึ้นในช่วงเวลาที่แล้วแต่จะกำหนด หรือการประเมินโดยผู้ที่ไม่มีส่วนเกี่ยวข้อง หรือการประเมินการควบคุมด้วยตนเอง (Control Self Assessment : CSA) ซึ่งเป็นการจัดประชุมเชิงปฏิบัติร่วมกัน ระหว่างผู้บริหาร ผู้ปฏิบัติงาน ผู้มีความรู้ด้านการควบคุม และผู้อื่นที่มีส่วนเกี่ยวข้อง เป็นต้น

5.4 ประเภทความเสี่ยง

การกำหนดประเภทความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เกิดจากการดำเนินการตามกระบวนการบริหารความเสี่ยง โดยเริ่มจากการกำหนดวัตถุประสงค์ ระบุความเสี่ยงจากแหล่งต่าง ๆ วิเคราะห์ประเมินระดับความสำคัญ และจัดกลุ่มความเสี่ยง ที่คล้ายคลึงกันให้อยู่ในประเภทต่าง ๆ เพื่อให้ง่ายต่อการบริหารจัดการและวางแผนรับมือในอนาคต สอดคล้องกับแผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา พ.ศ. 2563 และประเด็นที่สำคัญของแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐสภา (Parliament Cybersecurity Plan) พ.ศ. 2567-

2570 จึงได้กำหนดความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ซึ่งสามารถแบ่งประเภทความเสี่ยง ออกเป็น 5 ประเภท ดังนี้

1) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความมั่นคงปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

2) ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม

3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ Malware Trojan และ Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

4) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจากความผิดพลาดของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ประสงค์ร้ายเข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งอาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

5) ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสีย รวมถึงประชาชนทั่วไป ดังนั้นการรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากมนุษย์ ภัยจากธรรมชาติหรือเหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

5.5 การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การลดความเสี่ยง (Risk Reduction) เป็นการปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้ง ของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลักคือ การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือ การหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือ สัญญาการบำรุงรักษาหลังการขาย

5.6 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของสำนักงานเลขาธิการวุฒิสภา ได้แก่

5.6.1 ปัจจัยภายนอก ได้แก่

1) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

2) การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

3) การชำรุดเสียหายของตัวเครื่องประมวลผลหลักเสียหายหรือขัดข้อง

4) ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

5) ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

6) การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

5.6.2 ปัจจัยภายใน ได้แก่

1) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2) การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่าง ๆ จากผู้ใช้ภายในองค์กร

3) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดทำงาน

5.7 การประเมินความเสียหาย

1) ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลัก หรือ เครื่องคอมพิวเตอร์แม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

2) ความเสียหายที่เกิดผลเสียหายและต้องหยุดชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

5.8 การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือนและให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

5.9 สถานภาพระบบรักษาความมั่นคงปลอดภัย ICT ของสำนักงานเลขาธิการวุฒิสภา

สถานภาพระบบรักษาความมั่นคงปลอดภัย ICT ของสำนักงานเลขาธิการวุฒิสภา จากการสำรวจและวิเคราะห์สถานภาพปัจจุบันทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีรายละเอียดในด้านต่าง ๆ ประกอบด้วย

5.9.1 สถานภาพด้านฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร

จากการสำรวจสถานภาพปัจจุบันทางด้านเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานเลขาธิการวุฒิสภา สามารถสรุปรายละเอียดของฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร ได้ดังนี้

1) สำนักงานเลขาธิการวุฒิสภามี ฮาร์ดแวร์ ซอฟต์แวร์ ด้านความปลอดภัย ดังนี้

สำนักงานเลขาธิการวุฒิสภาได้ดำเนินการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์จัดเก็บข้อมูลไว้ที่ศูนย์ข้อมูลหลัก (Data Center) บริเวณชั้น B1 ฝั่งสำนักงานเลขาธิการสภาผู้แทนราษฎร อาคารรัฐสภา ซึ่งได้ดำเนินการติดตั้งโดยแบ่งออกเป็น 6 Rack ดังนี้

1. Rack HAD-E สำหรับติดตั้งอุปกรณ์เครือข่ายซึ่งเป็นของศูนย์ข้อมูลหลัก (Data Center)

2. Rack HAD-E1 –E7 สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์จัดเก็บข้อมูล (Storage) สำหรับระบบงานต่าง ๆ ของสำนักงานเลขาธิการวุฒิสภา

โดยสามารถแบ่งแยกเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์จัดเก็บข้อมูล (Storage) ออกตาม Rack โดยมีรายละเอียดตามตารางได้ดังนี้

ตารางที่ 3 ฮาร์ดแวร์ ซอฟต์แวร์ ของสำนักงานเลขาธิการวุฒิสภา

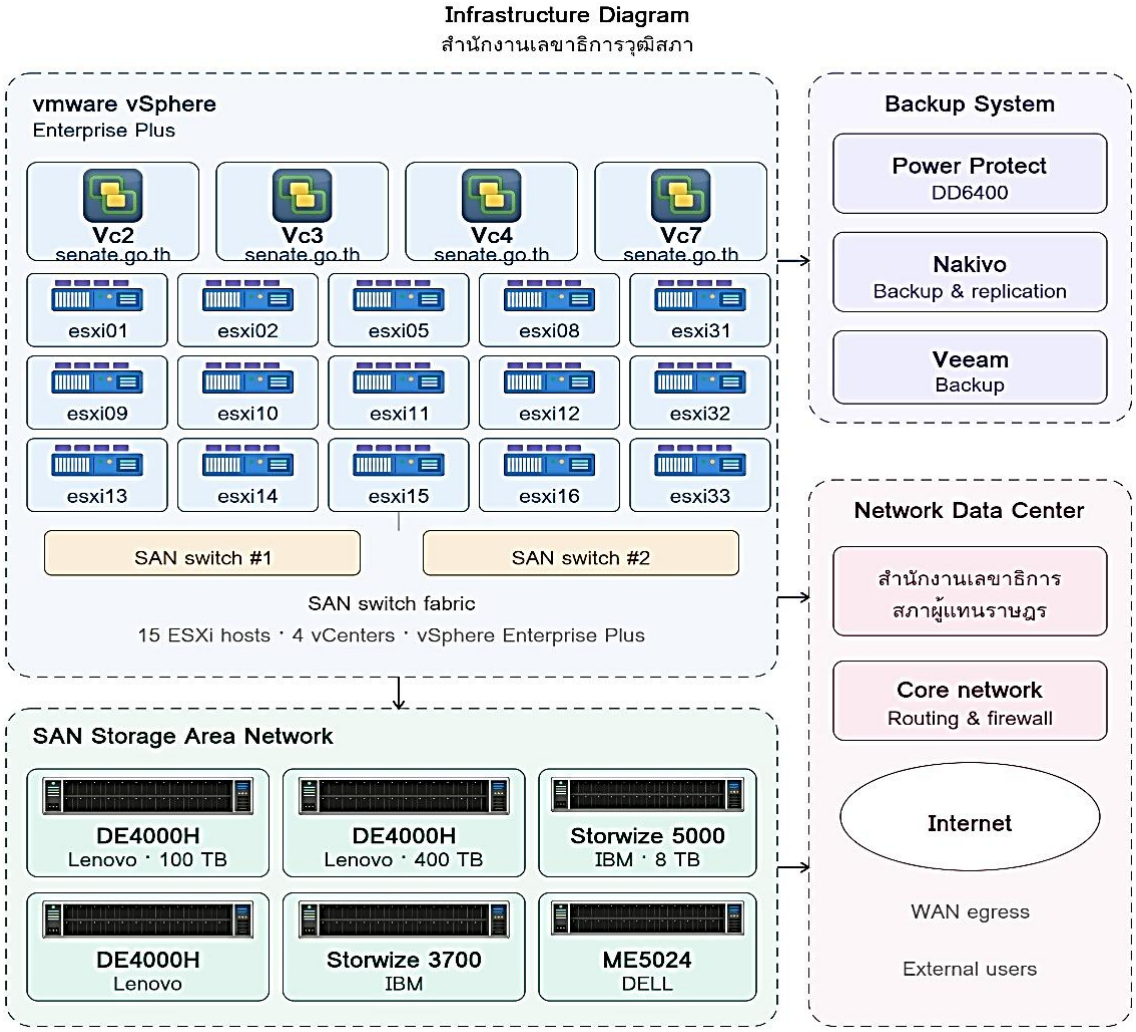
ลำดับที่	Rack Name	อุปกรณ์	หน้าที่	รายละเอียด
1	HAD-E	- Cisco Catalyst 2960-L - Cisco 2560 - PaloAlto PA5050 - Cisco NEXUS N9K - C9332PQ - Cisco NEXUS N9K - C9332PQ	เชื่อมโยงเครือข่ายเข้ากับ Core หลักของสำนักงานเลขาธิการสภาผู้แทนราษฎร	ศูนย์ข้อมูลหลัก Data Center
2	HAD-E1	- Cisco Nexus 2348 UPQ - Cisco Nexus 2348 UPQ - Lenovo SR 650 V3 - Lenovo SR 650 V3 - Lenovo SR 650 V2 - Lenovo SR 650 V2 - Sun Oracle Server X8-2 - Sun Storage Data รุ่น SE6140 - Sun SPARCE Enterprise M4000 - Sun SPARCE Enterprise M5000	- อุปกรณ์สำรองข้อมูล - เครื่องแม่ข่าย - เครื่องแม่ข่าย - สำหรับระบบสารบรรณอิเล็กทรอนิกส์ ระบบ e-office	ศูนย์ข้อมูลหลัก Data Center

ลำดับที่	Rack Name	อุปกรณ์	หน้าที่	รายละเอียด
3	HAD-E2	- Cisco Nexus 2348 TQ -Cisco Nexus 2348 UPQ - Lenovo ThinkSystem SR550 - Sun SPARCE Enterprise T2000 - Sun Storagetek SE6140 - Cyberview - Sun SPARCE Enterprise M4000 - Sun SPARCE Enterprise M5000 - SAN Switch1 - SAN Switch2 -Lenovo ThinkSystem SR550 -SUN StorageTek SL48 -NetApp E2824	- อุปกรณ์เชื่อมโยงเครือข่าย - อุปกรณ์เชื่อมโยงเครือข่าย - เครื่องแม่ข่าย - เครื่องแม่ข่าย - อุปกรณ์เทปสำรองข้อมูล - อุปกรณ์สำรองข้อมูล - เครื่องแม่ข่าย - เครื่องแม่ข่าย สำหรับระบบสารบรรณอิเล็กทรอนิกส์ ระบบ e-office	ศูนย์ข้อมูลหลัก Data Center
4	HAD-E3	- Cisco Nexus 2348TQ - Cisco Nexus 2348TQ - Lenovo ThinkSystem SR530 - IBM System x3550 M4 - IBM System x3550 M4 - Lenovo ThinkSystem SR530 - IBM System x3550 M4 - IBM System x3550 M5 - IBM System x3550 M3	- เครื่องแม่ข่ายสำหรับ esxi06 - เครื่องแม่ข่ายสำหรับ vCloud1 - เครื่องแม่ข่ายสำหรับ vCloud2 - เครื่องแม่ข่ายสำหรับ esxi05 - เครื่องแม่ข่ายสำหรับ esxi02 - เครื่องแม่ข่ายสำหรับ esxi01 - เครื่องแม่ข่ายสำหรับ Webmail	ศูนย์ข้อมูลหลัก Data Center

ลำดับที่	Rack Name	อุปกรณ์	หน้าที่	รายละเอียด
5	HAD-E4	-Cisco Nexus 2348TQ -Cisco Nexus 2348UPQ -IBM SAN Switch 24B#02 -IBM SAN Switch 24B#02 -Lenovo DE2000h#2 -Qnap TS-863U-R -IBM Storwize v3700#2 -IBM Storwize v3700#1 -IBM Storwize v5000e#4 -IBM Storwize v5000e#3 -IBM Storwize v5000e#2 -IBM Storwize v5000e#1 -IBM Storwize v5000e -IBM System Storage DS3512	- อุปกรณ์เชื่อมโยงเครือข่าย - อุปกรณ์เชื่อมโยงเครือข่าย - อุปกรณ์จัดเก็บข้อมูล1 - อุปกรณ์จัดเก็บข้อมูล - อุปกรณ์จัดเก็บข้อมูล - อุปกรณ์ NAS - อุปกรณ์จัดเก็บข้อมูล - อุปกรณ์จัดเก็บข้อมูล - อุปกรณ์จัดเก็บข้อมูล - อุปกรณ์จัดเก็บข้อมูล - อุปกรณ์จัดเก็บข้อมูล - อุปกรณ์จัดเก็บข้อมูล - อุปกรณ์จัดเก็บข้อมูล - เครื่องแม่ข่ายบริหารจัดการ	ศูนย์ข้อมูลหลัก Data Center
6	HAD-E5	- Cisco Nexus 2348TQ - Cisco Nexus 2348TQ - Sun Fire X4170 - Dell PowerEdge R440 - Acer Altos R360 F2 - Symantce Messeging Gateway - HP Proliant DL380G8 - HP Proliant DL380G8 - HP Proliant DL380G6 -HP Proliant DL380G6 -HP Integrity rx2660 - HP Backup -HP Proliant DL380G6 - HP Z420 - HP Z6000	- เครื่องแม่ข่ายระบบ IDP - เครื่องแม่ข่ายจัดเก็บ Log - เครื่องแม่ข่าย DNS - Mail Gateway - ระบบชวเลขประชุมใหญ่ (esxi07) - ระบบชวเลขกรรมาธิการ (esxi03) - เครื่องแม่ข่าย Backup HR - เครื่องแม่ข่ายสิ้นกระแส	ศูนย์ข้อมูลหลัก Data Center

ลำดับที่	Rack Name	อุปกรณ์	หน้าที่	รายละเอียด
7	HAD-E6	- Cisco Nexus 2348UQ - Cisco Nexus 2348UQ - Lenovo SR650 - Lenovo DE4000H - Enclosure DE240S - Lenovo VX Series - Lenovo VX series - Lenovo SR 250 V2 - San Switch DB620S - San Switch DB620S - Lenovo SR 650 V3 - Lenovo SR 650 V3 - Lenovo SR 650 V3 - Lenovo SR 650 V3 - Lenovo DE4000H - Lenovo DE240S - Lenovo DE4000H	- ระบบชวเลขประชุมใหญ่ (esxi08) - เครื่องแม่ข่ายโครงการ Virtualization และอุปกรณ์ Storage	ศูนย์ข้อมูลหลัก Data Center
8	HAD-E7	- Lenovo SR650 V3 - Lenovo SR650 V3 - Lenovo DE4000H - Lenovo SR650 V3 - Lenovo SR650 V3 - Dell Power Edge 750 - Dell Power Edge 750 - Dell Power Protect DD6400 - Dell Power Valut ME5024	- ระบบชวเลขประชุมใหญ่ (esxi16) - อุปกรณ์ Storage - อุปกรณ์ โครงการ Active Directory	ศูนย์ข้อมูลหลัก Data Center

2) แผนภาพระบบเครือข่าย (Network Diagram) สำนักงานเลขาธิการวุฒิสภา ที่ทำการอาคารรัฐสภา แสดงได้ดังภาพที่ 1



ภาพที่ 1 แผนภาพระบบเครือข่าย (Network Diagram) สำนักงานเลขาธิการวุฒิสภา

5.9.2 ด้านบุคลากรของสำนักเทคโนโลยีสารสนเทศและการสื่อสารประกอบด้วย 52 อัตรา ว่าง 4 อัตรา มีการบรรจุข้าราชการ 42 อัตรา พนักงานราชการและพนักงานจ้างเหมา 6 อัตรา รวมบรรจุ 48 อัตรา

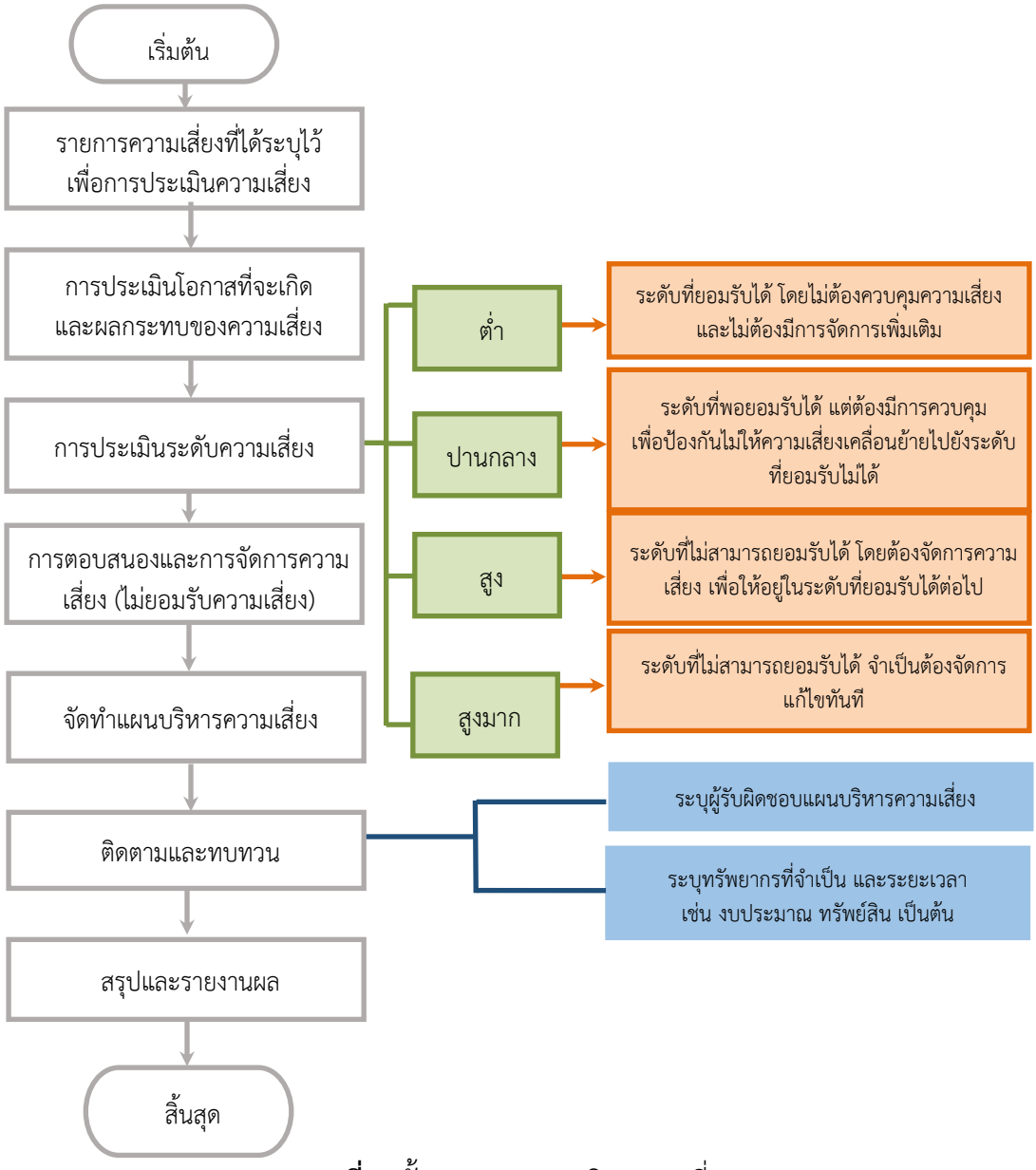
1) บุคลากรข้าราชการทั้งหมด

ประเภทเจ้าหน้าที่	ตำแหน่ง	จำนวน	อัตราว่าง
ข้าราชการ	ผู้อำนวยการสำนัก	1	-
	ผู้บังคับบัญชากลุ่มงาน	4	1
	นักวิชาการคอมพิวเตอร์	21	2
	วิทยากร	2	-
	เจ้าพนักงานเครื่องคอมพิวเตอร์	6	-
	เจ้าพนักงานธุรการ	8	-
พนักงานราชการและพนักงานจ้างเหมา	พนักงานราชการ (นักวิชาการเทคโนโลยีสารสนเทศ)	2	-
	พนักงานจ้างเหมานักวิชาการสารสนเทศและการสื่อสาร	4	-
รวม		48	3

2) บุคลากรด้านความมั่นคงปลอดภัยด้านสารสนเทศสำนักงานเลขาธิการวุฒิสภา ได้มอบหมายให้กลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์ เป็นกลุ่มงานที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ให้ดูแลความมั่นคงปลอดภัยสารสนเทศด้วย ซึ่งทางกลุ่มงานมีบุคลากรในการดูแลระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ การดูแลระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศได้ใช้ตำแหน่งนักวิชาการคอมพิวเตอร์ จำนวน 6 คน เป็นผู้ดูแลหลัก

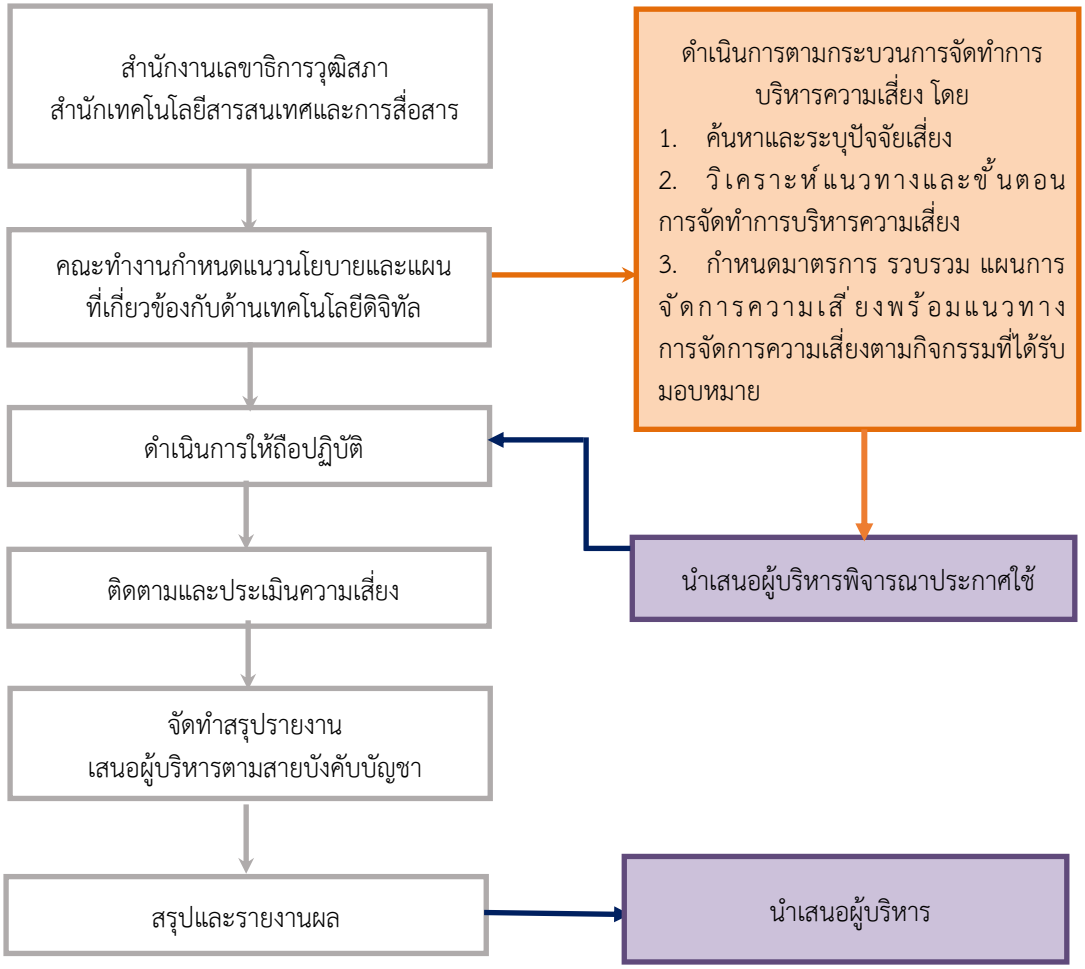
6 การวิเคราะห์การบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา

6.1 ขั้นตอนบริหารความเสี่ยง



ภาพที่ 2 ขั้นตอนการประเมินความเสี่ยง

6.2 กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล



ภาพที่ 3 กระบวนการจัดทำการบริหารความเสี่ยง

6.3 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา

เป็นขั้นตอนการนำผลการประเมินความเสี่ยงที่ประมวลจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) เข้าด้วยกัน (ระดับความเสี่ยง = ระดับโอกาส x ระดับผลกระทบ) แล้วจัดทำแผนผังระดับความเสี่ยง (Risk Matrix) โดยสามารถจัดแบ่งความเสี่ยงออกเป็นความเสี่ยงสูงมาก ความเสี่ยงสูง ความเสี่ยงปานกลาง ความเสี่ยงต่ำ และความเสี่ยงน้อยมาก หรือไม่สำคัญ ซึ่งช่วยในการตัดสินใจในการวางแผนความเสี่ยงได้อย่างเหมาะสม และสามารถจัดลำดับความสำคัญในการจัดการได้ ซึ่งการประเมินความเสี่ยงด้วยแผนผังระดับความเสี่ยง (Risk Matrix) แสดงตามภาพที่ 4

Risk Assessment Matrix			ระดับโอกาส (ความเป็นไปได้)				
			ต่ำมาก/น้อยมาก	ต่ำ/น้อย	ปานกลาง	สูง/บ่อย	สูงมาก/บ่อยมาก
			1	2	3	4	5
ผลกระทบ (ความรุนแรง)	สูงมาก/หายนะ	5	5	10	15	20	25
	สูง/วิกฤต	4	4	8	12	16	20
	ปานกลาง	3	3	6	9	12	15
	ต่ำ/น้อย	2	2	4	6	8	10
	ไม่สำคัญ/น้อยมาก	1	1	2	3	4	5

ระดับความเสี่ยง

ภาพที่ 4 แผนผังการประเมินความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization)

เกณฑ์ในการประเมินความเสี่ยง เป็นการพิจารณาระดับความเสี่ยงที่ประมวลได้ตามภาพที่ 4 จัดแบ่งเป็นเกณฑ์ในการยอมรับความเสี่ยงเป็น 4 ระดับ ดังนี้

ตารางที่ 4 เกณฑ์ประเมินความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วยแถบสี	ความหมาย
ต่ำ	1-3	เขียว	ระดับที่ยอมรับได้โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม (Acceptable or Limited Focus)
ปานกลาง	4-9	เหลือง	ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับได้ (Tolerable but Caution or Management Discretion / Medium Risk)
สูง	10-16	ส้ม	ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป (Intolerable or Attention required/High Risk)
สูงมาก	17-25	แดง	ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ทันที (Intolerable or Immediate attention require /High Risk)

ตารางที่ 5 ประเด็นความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
1	ความเสี่ยงจากข้อมูลรั่วไหล (Data Breach)	5	4	20
2	ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายนอก	5	4	20
3	ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายใน	5	4	20
4	ความเสี่ยงจากการโจมตีทางไซเบอร์สำนักงานฯ ไม่ให้สามารถให้บริการได้ (Denial of Service - DoS)	5	4	20
5	ความเสี่ยงจากไวรัสเรียกค่าไถ่ Ransomware	5	4	20
6	ความเสี่ยงจากการถูก Black List โดย Search Engine หรือ Spamhaus	4	4	16
7	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	5	3	15
8	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	4	3	12
9	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	3	5	15
10	ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	4	3	12
11	ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	2	4	8
12	ความเสี่ยงจากการไม่ทำการสำรองข้อมูลหรือทำการสำรองข้อมูลแต่ขาดการอัพเดทของเครื่องคอมพิวเตอร์แม่ข่าย	2	4	8
13	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย	2	4	8
14	ความเสี่ยงจากการเกิดอัคคีภัย	2	4	8
15	ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart Phone, Tablet, PC) ส่วนบุคคลเข้ามาเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต	2	5	10
16	ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้งาน	2	3	6
17	ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	1	3	3
18	ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1	5	5
19	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์แม่ข่าย	1	5	5
20	ความเสี่ยงจากการเกิดอุทกภัย ห้อง Data Center	1	5	5
21	ความเสี่ยงจากการโจรกรรมฐานข้อมูล	1	5	5
22	ความเสี่ยงจากวินาศภัย/การก่อการร้าย	1	5	5
23	ความเสี่ยงจากแมลง หรือสัตว์ที่ทำให้คอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า /สายสัญญาณ เกิดความชำรุดหรือเสียหาย	1	3	3
24	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่อพ่วง	1	3	3
25	ความเสี่ยงจากแผ่นดินไหว	1	3	3

6.4 ผลการประเมินแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา

ได้มีการประเมินความเสี่ยงตามหลัก COSO ดังนี้

ตารางที่ 6 ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานเลขาธิการวุฒิสภา

ความเสี่ยงสูง

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา 2569	ระยะเวลา 2570	ตัวชี้วัด
1.ความเสี่ยงจากข้อมูลรั่วไหล (Data Breach)	- เสี่ยงด้านข้อมูลภายในหน่วยงานหรือข้อมูลส่วนบุคคลอาจรั่วไหล	1.ถูกโจรกรรมข้อมูลที่เป็นความลับของสำนักงานฯ 2.ถูกโจรกรรมข้อมูลส่วนบุคคล	5	4	สูงมาก 5X4=20	1. มาตรการเร่งด่วนโดยเพิ่มความถี่ในการแจ้งเตือนและสร้างความตระหนักให้เข้มข้น นั้น ดังนี้ 1) แจ้งเวียนให้บุคลากรเปลี่ยนรหัสผ่านให้ยากต่อการคาดเดา ทุก 1 เดือน ตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐสภา 2) สร้างความตระหนักการรักษาความมั่นคงปลอดภัยให้บุคลากรของสำนักงานเลขาธิการวุฒิสภา โดยการซ้อมป้องกันทางไซเบอร์ (Cyber Drill) 3) ยกระดับการสร้างเครือข่ายผู้ใช้งานเพิ่มเติมจากผู้ใช้งานปกติ โดยจัดทำโครงการ Super User เพื่อเป็นการสร้าง	ความเสี่ยงด้านระบบข้อมูล (Database Risk)	✓	✓	ผลผลิต : จัดทำโครงการการยืนยันตัวตนผ่าน MFA (Multi Factor Authentication) เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการยืนยันตัวตนของผู้ใช้งาน ผลลัพธ์ - ร้อยละ 100 ของบุคลากรสำนักงานเลขาธิการวุฒิสภาสามารถยืนยันตัวตนผ่าน MFA (Multi Factor Authentication)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
						เครือข่ายเฝ้าระวังภายในให้ครบทุกสำนัก 2. มาตรการระยะยาว ซึ่งจะดำเนินการยกระดับความปลอดภัยในส่วนของผู้ใช้งานทั่วไป ดังนี้ 1) จัดทำโครงการผ่าน MFA (Multi Factor Authentication) เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการยืนยันตัวตนของผู้ใช้งานผ่านรหัสผ่านที่สร้างขึ้นเฉพาะครั้ง 2) นำโปรแกรม ADSelfService มาใช้ในการบริหารจัดการรหัสผ่านตามแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยรัฐสภา 3) การนำเอาเทคโนโลยี DLP มาใช้ในระดับไฟล์ข้อมูล เพื่อการป้องกันการรั่วไหลของข้อมูล				- ร้อยละ100 ของบุคลากรสำนักงานเลขาธิการวุฒิสภามีการตั้งรหัสผ่านยากต่อการคาดเดาตามแนวนโยบาย

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
2. ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายนอก	เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	1. ทำให้เครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย 2. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูลหรือรูปภาพบน Web Site ของสำนักงานฯ 3. ถูกโจรกรรมข้อมูลที่เป็นความลับของสำนักงานฯ	5	4	สูงมาก 5X4=20	1. ติดตั้งระบบป้องกันและเตือนภัยโปรแกรมประสงค์ร้าย อาทิ Spam ,Virus, Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้น ๆ อยู่เป็นประจำเพื่อที่จะสามารถแก้ไขได้ทันเมื่อถูกโจมตี 2. หมั่นตรวจสอบ Policy และ Log ของ Firewall IPS/IDS อย่างสม่ำเสมอ 3. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับสถานการณ์ได้โดยไม่สับสน 4. ติดตั้ง Firewall และ IDS/IPS เพื่อป้องกันฐานข้อมูลที่มีความสำคัญโดยเฉพาะ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	✓	✓	<u>ผลผลิต</u> : จัดทำโครงการจัดหาลิขสิทธิ์การใช้งาน (license) สำหรับอุปกรณ์เครือข่าย <u>ผลลัพธ์</u> : สามารถป้องกันการโจมตีจากภายนอกเครือข่ายได้ไม่น้อยกว่า ร้อยละ 80

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
3. ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายใน	เสี่ยงต่อการถูกโจมตีผ่านระบบเครือข่ายภายใน	1. ทำให้เครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย 2. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูลหรือรูปภาพบน Web Site ของสำนักงานฯ 3. ถูกโจรกรรมข้อมูลที่เป็นความลับของสำนักงานฯ	5	4	สูงมาก 5X4=20	1. ติดตั้งระบบป้องกันและเตือนภัยโปรแกรมประสงค์ร้าย อาทิ Spam ,Virus, Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้น ๆ อยู่เป็นประจำ เพื่อที่จะสามารถแก้ไขได้ทันเมื่อถูกโจมตี 2. หมั่นตรวจสอบ Policy และ Log ของ Firewall IPS/IDS อย่างสม่ำเสมอ 3. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับสถานการณ์ได้โดยไม่สับสน 4. ติดตั้ง Firewall และ IDS/IPS เพื่อป้องกันฐานข้อมูลที่มีความสำคัญโดยเฉพาะ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	✓	✓	<u>ผลผลิต</u> : จัดทำโครงการจัดหาลิขสิทธิ์การใช้งาน (license) สำหรับอุปกรณ์เครือข่าย <u>ผลลัพธ์</u> : สามารถป้องกันการโจมตีจากภายนอกเครือข่ายได้ไม่น้อยกว่า ร้อยละ 80

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
4. ความเสี่ยงจากการโจมตีทางไซเบอร์สำนักงานฯ ไม่ให้สามารถให้บริการได้ (Denial of Service - DoS)										
4.1 จากภายนอก	เสี่ยงต่อการถูกโจมตีได้จากภายนอก โดยโจมตีทั้งเครื่องแม่ข่ายและ / หรือเครือข่ายภายในทุกรูปแบบ ซึ่งจะมีการพัฒนาวิธีการอยู่ตลอดเวลา	ไม่สามารถใช้งานเครือข่ายได้หรือใช้ได้แต่ช้ามาก	5	4	สูงมาก 5X4=20	1. ติดตั้งระบบป้องกันและเตือนจาก Spam,Virus, Malware,Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้น ๆ อยู่เป็นประจำเพื่อลดหรือสามารถแก้ไขได้ทันเมื่อถูกโจมตี 2.หมั่นตรวจสอบ Policy และ Log ของ Firewall และ IPS/IDS อย่างสม่ำเสมอ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	✓	✓	<u>ผลผลิต</u> : จัดทำแผนตอบสนองภัยคุกคามของรัฐสภา (Incident Response Plan) จำนวน 1 แผน -นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐสภา จำนวน 1 ฉบับ <u>ผลลัพธ์</u> : สามารถดำเนินการตามแผนตอบสนองภัยคุกคามของรัฐสภา (Incident

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
						3.จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับสถานการณ์ใดโดยไม่สับสน				Response Plan) ไม่น้อยกว่า ร้อยละ 80 สามารถดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐสภา
4.2 จากภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่าง ๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ	ไม่สามารถใช้งานเครือข่ายได้หรือใช้ได้แต่ช้ามาก	5	4	สูงมาก 5X4=20	มีมาตรการและกฎระเบียบในการควบคุมมิให้มีการติดตั้ง โปรแกรมต่าง ๆ ลงบนเครื่องลูกข่ายอินทราเน็ตของสำนักงาน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	✓	✓	<u>ผลผลิต</u> : มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐสภา ได้จำนวน 1 ฉบับ -นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐสภา จำนวน 1 ฉบับ <u>ผลลัพธ์</u> : สามารถดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐสภาได้ไม่น้อยกว่าร้อยละ 80

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
										ดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐสภาได้ไม่น้อยกว่า ร้อยละ 80
5. ความเสี่ยงจากไวรัสเรียกค่าไถ่ Ransomware	เสี่ยงต่อการถูกโจมตีจากไวรัสเรียกค่าไถ่ Ransomware	ไม่สามารถใช้งานเครือข่ายได้หรือใช้ได้แต่ช้ามาก	5	4	สูง 5X4=20	1. มีการ Update software ให้เป็นปัจจุบัน 2. มีการสำรองข้อมูลไว้มากกว่า 1แห่ง 3. ให้ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์กับบุคลากรสำนักงานเลขาธิการวุฒิสภา	ความเสี่ยงด้านบุคลากร (Human Risk) และ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	✓	✓	ผลผลิต : จัดทำแผนตอบสนองภัยคุกคามของรัฐสภา (Incident Response Plan) จำนวน 1 แผ่น -นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐสภา จำนวน 1 ฉบับ ผลลัพธ์ : ประชาสัมพันธ์สื่อสารการให้ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์กับบุคลากรสำนักงานเลขาธิการวุฒิสภา

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
6. ความเสี่ยงจากการถูก Black List โดย Search Engine หรือ Spamhaus (http://www.spamhaus.org)	1. ผู้ใช้งานที่ต้องการข้อมูลของสำนักงานฯ หรือประชาชนทั่วไปสามารถเข้าใช้งาน Web Server ได้ 2. ไม่สามารถใช้งานเครือข่ายหรือ e-mail ได้	1. ลดความน่าเชื่อถือต่อสำนักงานฯ หรือข้อมูลของสำนักงานฯ 2. สำนักงานฯ อาจถูกฟ้องร้องโดยมีส่วนได้ส่วนเสีย	4	4	สูง 4X4=16	1. ติดตั้งโปรแกรม เพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ตโดยเฉพาะจาก SMTP Mail Server ซึ่งมักจะเป็นแหล่งที่ Hacker ชอบใช้ในการส่ง Spam 2. ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server หรือ FTP เช่น Symantec Web Gateway ,Symantec Endpoint Protection 3. มีการอัพเดทตัวโปรแกรมและ Signature อย่างสม่ำเสมอและการทำการบำรุงรักษา (Maintenance) ทั้งฮาร์ดแวร์และซอฟต์แวร์ พร้อมทั้ง Update Licenses	ความเสี่ยงด้านบุคลากร (Human Risk) และความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	✓	✓	ผลผลิต : มีการติดตั้ง Symantec Brightmail Gateway เพื่อป้องกันติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server หรือ FTP ผลลัพธ์ : สามารถแก้ไขหากพบถูก Black List โดย Search Engine หรือ Spamhaus ร้อยละ 85

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
7. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	1. เสี่ยงต่อการสูญหายของข้อมูล 2. เสี่ยงต่อการถูกฟ้องร้องและเสื่อมเสียชื่อเสียงและความน่าเชื่อถือของสำนักงานฯ	1. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้น ๆ 2. สำนักงานฯ อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้น ๆ 3. ความไม่สะดวกหากไปใช้งานด้วยซอฟต์แวร์ ที่ไม่จำเป็นต้องมีลิขสิทธิ์ (Open Source)	5	3	สูง 5x3=15	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2. ทำสัญญา หรือข้อตกลง/สนับสนุนการใช้โปรแกรม SaaS เช่น www.docs.com แทน Microsoft Office 3. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	✓	✓	<u>ผลผลิต</u> : จัดทำโครงการจัดหาลิขสิทธิ์การใช้งาน (license) สำหรับอุปกรณ์เครือข่าย และมีโครงการการจัดซื้ออุปกรณ์คอมพิวเตอร์ที่มีซอฟต์แวร์ที่มีลิขสิทธิ์ <u>ผลลัพธ์</u> : ร้อยละ 100 มีซอฟต์แวร์ที่มีลิขสิทธิ์จากการจัดซื้อเครื่องคอมพิวเตอร์

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
8. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	1.เสี่ยงต่อการถูกทำลายโปรแกรมหรือข้อมูล 2. เสี่ยงต่อการไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3. เสี่ยงต่อการถูกขโมยข้อมูลที่สำคัญ	1.ใช้คอมพิวเตอร์ไม่ได้ 2. ใช้ระบบงานไม่ได้ 3. ข้อมูลที่สำคัญสูญหาย	4	3	สูง 4 x3= 12	1. ใช้ระบบป้องกันไวรัสกับเครื่องแม่ข่ายที่ต้องเสียค่าใช้จ่าย เช่น Symantec Endpoint Protection ที่สำนักงานฯ ใช้อยู่ที่สามารถควบคุมการโจมตีและการบุกรุกเครือข่ายจากสาเหตุต่าง ๆ เช่น การระบาดของ Virus และ Worm, การโจมตีเพื่อปฏิเสธกาให้บริการ (Denial of Server-DoS) การบุกรุกแบบ Vulnerability Exploit, Network Reconnaissance และเทคนิคการหลบซ่อนการโจมตีแบบ Traffic Normalization , IP Defragmentation Reassemble ได้ 2. อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ 3. มีการสำรองข้อมูลที่เครื่องลูกข่ายที่จำเป็นไว้อย่างสม่ำเสมอทาง External Hard Disk หรือ Cloud	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	✓	✓	<u>ผลผลิต</u> : จัดทำโครงการจัดหาลิขสิทธิ์การใช้งาน (license) สำหรับอุปกรณ์เครือข่าย <u>ผลลัพธ์</u> : สามารถป้องกันการโจมตีจากภายนอกเครือข่ายได้มากกว่าร้อยละ 80

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
9.ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	1.ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านระบบเครือข่าย 2.ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่าย	1.ขัดขวางการทำงานของเจ้าหน้าที่และผู้บริหาร 2. บุคคลภายนอกไม่สามารถเข้าใช้ Web Server หรือค้นหาข้อมูลที่ต้องการ	3	5	สูง 3x5=15	1. ตรวจสอบ Availability ของ Server ด้วยโปรแกรมตรวจสอบ เช่น โปรแกรม zabbix จาก http://zabbix.senate.go.th/zabbix เป็นต้น 2. การจัดทำเส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า 1 เส้นทาง หากสำนักงานฯ มีงบประมาณเพียงพออาจ พิจารณาในการจัด Gateway ที่ผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISP) ต่างออกไป จะทำให้ระบบเครือข่ายอินเทอร์เน็ต (ISP) ต่างออกไป จะทำให้ระบบเครือข่ายอินเทอร์เน็ต มีเสถียรภาพมากขึ้น 3. การวาง Web Server ไว้มากกว่า 1 ที่ เช่น ที่ ISP เป็นต้น 4. การจัดตั้งศูนย์สำรอง (DR Site)	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	✓	✓	<u>ผลผลิต</u> : **1.** จัดทำโครงการเพิ่มประสิทธิภาพการบำรุงรักษาระบบเครือข่ายและซ่อมแซมเครื่องคอมพิวเตอร์ 2. มีการจัดทำโครงการบำรุงรักษาเว็บไซต์สำรอง 3. เส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า 1 เส้นทาง <u>ผลลัพธ์</u> : - เครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลมีการ Downtime ไม่เกิน 36 ชั่วโมงต่อปี - ร้อยละ 90 ของอุปกรณ์ในโครงการได้รับการแก้ไขปัญหา

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
										ข้อขัดข้องทันตามเวลาที่สำนักงานเลขาธิการวุฒิสภากำหนด
10. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1. เสี่ยงต่อการถูกขโมยข้อมูล 2. เสี่ยงต่อการทำความเสียหายแก่โปรแกรม 3.เสี่ยงต่อการใช้ช่องโหว่โปรแกรมหรือการซ่อน Script ไว้ในโปรแกรมเพื่อวัตถุประสงค์แอบแฝง	1. ลดความน่าเชื่อถือต่อสำนักงานฯ หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ 2. กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานฯ เป็นอย่างยิ่ง	~~3~~4	3	สูง 4x3= 12	1. ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP-Top 10 Web Application Security Risks เพื่อลดความเสี่ยง 2. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ 3.มีมาตรการในการเข้ารหัสข้อมูลที่เป็นความลับ เช่น RSA256 4.มีการประเมินช่องโหว่ของระบบโปรแกรมประยุกต์ภายในองค์กร	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	✓	✓	<u>ผลผลิต</u> : มีการกำหนดมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับของการพัฒนาโปรแกรมประยุกต์ภายในองค์กร มีการประเมินช่องโหว่ของระบบโปรแกรมประยุกต์ภายในองค์กร <u>ผลลัพธ์</u> : สามารถแก้ไขหากพบการรั่วไหลของข้อมูลจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร ร้อยละ 80

ความเสี่ยงปานกลาง

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
11. ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	1. เสี่ยงต่อการถูกขโมยข้อมูล 2. เสี่ยงต่อการทำความเสียหายแก่โปรแกรม 3. ไม่สามารถแก้ไขข้อบกพร่องได้เอง 4. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูลทำให้ไม่สามารถใช้งานได้ในระยะยาว	1. ลดความน่าเชื่อถือต่อสำนักงานฯ หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ 2. กรณีเป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานฯ เป็นอย่างยิ่ง 3. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลพร้อมกับการทำการบำรุงรักษา	2	4	ปานกลาง 2x4=8	1. ออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) level 2 2. การออกแบบโดยการอ้างอิงด้วยแผนผังแสดงความสัมพันธ์ระหว่างกลุ่มข้อมูล (Entity)-ER Diagram 3. ให้มีการส่งมอบ Source Code ในรูปแบบ External Memory เช่น ฮาร์ดดิสก์ไดรฟ์ภายนอก (external hard drive), แฟลชไดรฟ์ (flash drive), การ์ดหน่วยความจำ (memory card) ในฟอร์แมตที่ไม่เข้ารหัสใด ๆ และสามารถปรับปรุงแก้ไขได้ 4. หากมีการพัฒนา Library ด้วยตนเองต้องส่ง Source Code Library ที่สามารถแก้ไขได้	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	✓	✓	ผลผลิต : เอกสารการจ้างงานแสดงถึงการพัฒนาโปรแกรมโดยผู้รับจ้างภายนอก ต้องปฏิบัติตามมาตรฐานการออกแบบ ผลลัพธ์ : สามารถดำเนินการตามมาตรฐานร้อยละ 80

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
		เครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการอัพเดทอยู่เสมอ				5. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ 6. มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม 7. มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึง การแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดทเมื่อมี Version หรือ Release ใหม่การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น				
12. ความเสี่ยงจากการไม่ทำการสำรองข้อมูลหรือทำ	1.เสี่ยงต่อการสูญหายข้อมูลในขั้นเล็กน้อย	1. เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือ	2	4	ปานกลาง 2x4=8	1.มีการบริหารจัดการในการทำสำรองข้อมูล (Backup) เป็นประจำอยู่เสมอ	ความเสี่ยงด้านระบบ	✓	✓	ผลผลิต : มีการบริหารจัดการในการทำสำรองข้อมูล (Backup) เป็นประจำอยู่เสมอ

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
การสำรองข้อมูลแต่ขาดการอัพเดทของเครื่องคอมพิวเตอร์แม่ข่าย	หรือมากจนไม่สามารถดำเนินงานได้ตามปกติ 2. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	การจัดทำขึ้นมาใหม่ 2. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้เนื่องจากขาดความมั่นใจในข้อมูล				2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) เพื่อความแน่ใจในข้อมูลที่เก็บไว้ปัจจุบัน การจัดเก็บสำรองข้อมูลของสำนักงานฯ ที่มีอุปกรณ์และระบบบริหาร 3. การจัดการเชื่อมโยงเครื่องแม่ข่ายอื่นเข้าสู่ระบบการสำรองข้อมูลโดยอัตโนมัติ	ข้อมูล (Database Risk)			<u>ผลลัพธ์</u> : สามารถกู้คืนระบบสารสนเทศภายใน 12 ชั่วโมง (RPO)
13. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย	1. เสี่ยงต่อการไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ 2. เสี่ยงต่อความเสียหายต่อความเสียหายของข้อมูล	การใช้งานระบบไม่สามารถใช้งานตามปก	2	4	ปานกลาง 2x4=8	1.การป้องกันระบบเครื่องแม่ข่ายฐานข้อมูลหลักเสียหายด้วยการเพิ่มประสิทธิภาพ การทำงานในแบบ Hot Standby หรือ Clustering ทุกส่วนของเครื่องแม่ข่ายฐานข้อมูลหลัก 2. การจัดเก็บฐานข้อมูลสำรอง (Backup) และที่พร้อมใช้งานได้โดยอาจประสานงานกับบริษัทผู้ให้บริการในลักษณะ Application Service Provider หรือหน่วยงานอื่น ในความตกลงที่จะใช้เครื่องของหน่วยงานอื่น เพื่อใช้งาน	ความเสี่ยงด้านระบบข้อมูล (Database Risk)	✓	✓	<u>ผลผลิต</u> : มีการจัดทำโครงการบำรุงรักษาเว็บไซต์สำรอง <u>ผลลัพธ์</u> : เครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลมีการ Downtime ไม่เกิน 36 ชั่วโมงต่อปี

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
						ทดแทนในกรณีที่เกิดความเสียหายต่อเครื่องแม่ข่ายฐานข้อมูลหลักของสำนักงานฯ 3. การจัดตั้งศูนย์สำรองข้อมูล (Backup Site)				
14 .ความเสี่ยงจากการเกิดอัคคีภัย	1. การถูกทำลายทรัพย์สินระบบคอมพิวเตอร์และเครือข่าย 2. การถูกทำลายข้อมูล 3. การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร	1.เสียงบประมาณในการจัดหาระบบทดแทน 2. การไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน	2	4	ปานกลาง 2x4=8	1.ติดตั้งระบบตรวจจับควันที่สามารถตรวจจับควันได้ก่อนล่วงหน้า (High Sensitivity Smoke Detector) ซึ่งปัจจุบันรัฐสภา ได้ติดตั้งระบบนี้ใช้งานอยู่ในศูนย์ข้อมูลข้างต้นแล้ว 2. ติดตั้งระบบดับเพลิงแบบ Novec 1230 4. จัดตั้งศูนย์สำรองในกรณีที่เกิดอัคคีภัยขึ้น 5. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	✓	✓	ผลผลิต : จัดทำแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 1 แผน ผลลัพธ์ : สามารถดำเนินงานตามแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ได้ไม่น้อยกว่าร้อยละ 80

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
15. ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart Phone, Tablet, PC) ส่วนบุคคลเข้ามาเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต	เสี่ยงต่อผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลเข้าใช้เครือข่ายอินเทอร์เน็ต	ข้อมูลที่เป็นความลับถูกนำออกเผยแพร่หรือนำไปใช้ประโยชน์ อันจะนำมาซึ่งการขาดความน่าเชื่อถือในการจัดเก็บข้อมูลของสำนักงานฯ	2	~~3~~ 5	ปานกลาง 2x5= 10	1.ควบคุมการเข้าใช้เครือข่ายด้วย Radius และ Directory เช่น AD หรือ LDAP ร่วมกันในการควบคุมการเข้าใช้งานเครือข่าย 2. เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดยติดตั้งระบบยืนยันตน (Authentication)	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	✓	✓	ผลผลิต : มีการจัดทำระบบบริหารจัดการบัญชีผู้ใช้งาน (Ldap Server) จำนวน 1 ระบบ ผลลัพธ์ : ระบบสารสนเทศของสำนักงานฯ มีการพิสูจน์ตัวตนก่อนการเข้าใช้งานระบบสารสนเทศ ได้ไม่น้อยกว่าร้อยละ 90
16. ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้งาน	ข้อมูลที่สำคัญมีการรั่วไหลจากการโอนสิทธิ์เปลี่ยนผู้ถือครอง การมอบสิทธิ์ และ	1. ข้อมูลที่อยู่ในชั้นความลับรั่วไหลทำให้เสียหายต่อความ	2	3	ปานกลาง 2X3=6	มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard disk ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้น ๆ ทิ้งแล้ว หากทำได้	ความเสี่ยงด้านระบบข้อมูล (Database Risk)	✓	✓	ผลลัพธ์ : จัดทำมาตรการการดำเนินการในการนำส่งเครื่องคืนเพื่อเปลี่ยนมือผู้ใช้งาน หรือส่งบริษัทซ่อมหรือจำหน่ายต่อไปตามนโยบายในการรักษา

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
	การบำรุงรักษา	น่าเชื่อถือของสำนักงานฯ 2. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้				อุปกรณ์ Notebook Tablet Smart Phone มีมาตรการในการโอนสิทธิ์เปลี่ยนผู้ถือครอง การมอบสิทธิ์ และการบำรุงรักษา				ความมั่นคงปลอดภัยด้านสารสนเทศ ผลผลิต : มีการปฏิบัติการมาตรการการดำเนินการในการนำส่งเครื่องคืนเพื่อเปลี่ยนมือผู้ใช้งาน หรือส่งบริษัทซ่อมหรือจำหน่าย หรือทำลาย ต่อไปตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
17. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	1. ไม่สามารถใช้งานเครื่องแม่ข่ายและเครือข่ายได้ 2. ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่ายทั้งส่วนระบบปฏิบัติการ	1.ข้อมูลเสียหาย 2..ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเสียหาย ต้องมีการติดตั้งใหม่ 3.เสียเวลาการใช้งาน 3 ถึง 6	1	3	ปานกลาง 1X3=3	1. มีระบบไฟฟ้า 2 แห่งจ่าย A / B ให้ server และอุปกรณ์สามารถใช้ระบบไฟฟ้าที่ศูนย์ข้อมูลหลักได้ครบทั้ง 2 แหล่งจ่าย 2. มีเครื่องกำเนิดไฟฟ้า 3. มีระบบไฟฟ้าสำรอง UPS	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	✓	✓	ผลผลิต : มีอุปกรณ์รองรับแหล่งจ่ายไฟฟ้าของศูนย์ข้อมูลหลัก (อุปกรณ์ต้องมี power supply จำนวน 2 แหล่งจ่าย) ผลลัพธ์ : ร้อยละ 90 ของอุปกรณ์ได้รับการแก้ไขปัญหาข้อขัดข้องทันตามเวลาที่

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
	(Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ shutdown อย่างเหมาะสม	ชั่วโมงเป็นอย่างน้อย								สำนักงานเลขาธิการวุฒิสภากำหนด
18. ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1. เสี่ยงต่อการใช้ Resource ของสำนักงานฯ ในทางที่ผิดหรือ เปล่าประโยชน์ เช่น การฟังวิทยุหรือดูโทรทัศน์ออนไลน์ การโหลด Bit	1.สูญเสีย Bandwidth ในเครือข่ายทำให้สำนักงานฯ ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี 2. สำนักงานฯ อาจถูก	1	5	ปานกลาง 1X5=5	1. บริหารจัดการในการกำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น 2. บริหารจัดการในการกำหนด Policy ของอุปกรณ์ Bandwidth Management เพื่อกำจัดหรือปิดกั้นการใช้ resources ในทางที่ผิด	ความเสี่ยงด้านบุคลากร (Human Risk)	✓	✓	ผลผลิต : มีการติดตั้งระบบ Bandwidth ผลลัพธ์ : สามารถบริหารจัดการ Bandwidth ได้ไม่น้อยกว่า ร้อยละ 80

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
	Torrent การดูเว็บไซต์ที่ลามกอนาจาร ผิดศีลธรรม เป็นต้น 2.การใช้ resource ของสำนักงานฯ ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม หรือ เพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	ร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก				3.การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์หรือ Resources ต่าง ๆ ของสำนักงานฯ ไปใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา				
19. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์แม่ข่าย	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	1. เสียงบประมาณในการจัดหาเครื่องคอมพิวเตอร์แม่	1	5	ปานกลาง 1X5=5	1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุม การเข้า-ออก ห้องคอมพิวเตอร์ แม่ข่าย 2. ตู้ RACK ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and	✓	✓	<u>ผลผลิต</u> : มีอุปกรณ์รักษาความปลอดภัยในการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย จำนวน 1 ระบบ

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
		ข่ายทดแทนที่มีมูลค่าสูง 2. เสียเวลาในการกู้ระบบ 3. เสียภาพลักษณ์ของสำนักงานฯ				จัดเก็บข้อมูล (Disk Array) และอุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจตลอดเวลา 3. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน การนำติดตัวไปด้วยตลอดเวลา หรือติดตั้งอุปกรณ์ล็อค เช่น Kensington Lock เป็นต้น เพื่อป้องกันการสูญหาย	Environment Risk)			ผลลัพธ์ : สามารถป้องกันการสูญหายของอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย
20. ความเสี่ยงจากการเกิดอุทกภัย ห้อง Data Center	ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	เสียงบประมาณในการซ่อมแซมหรือจัดหาใหม่ทดแทน	1	5	ปานกลาง 1X5=5	1. ติดตั้งเครื่องตรวจจับระดับน้ำรั่วไหลพื้นที่ที่มีความไวต่อน้ำ 2. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	✓	✓	ผลผลิต : จัดทำแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร 1 แผน ผลลัพธ์ : สามารถดำเนินงานตามแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
										ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ได้ไม่น้อยกว่าร้อยละ 80
21. ความเสี่ยงจากการโจรกรรมฐานข้อมูล	ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ	1. เสียชื่อเสียงและความน่าเชื่อถือที่มีต่อสำนักงานฯ 2. การสูญหายหรือถูกทำลายข้อมูล	1	5	ปานกลาง 1X5=5	1.มีการบริหารจัดการด้านการป้องกันข้อมูล 2. มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) ตามความสำคัญของข้อมูลโดยสามารถทำงานร่วมกับ Active Directory (AD) หรือ Lightweight Directory Access Protocol (LDAP) Server และ Syslog ได้	ความเสี่ยงด้านระบบข้อมูล (Database Risk)	✓	✓	<u>ผลลัพธ์</u> : สามารถดำเนินการตามนโยบายในการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐสภาได้ไม่น้อยกว่าร้อยละ 80 <u>ผลผลิต</u> : จัดทำนโยบายในการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐสภาจำนวน 1 ฉบับ
22. ความเสี่ยงจากวินาศภัย/การก่อการร้าย	เสี่ยงต่อการสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	1	5	ปานกลาง 1X5=5	1. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไรและจะใช้เครื่องทดแทนจากที่ใดเพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง 2. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data	✓	✓	<u>ผลผลิต</u> : จัดทำแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 1 แผน

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
						3. จัดทำศูนย์สำรอง (Backup Site)	Communication Risk)			ผลลัพธ์ : สามารถดำเนินงานตามแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ได้ไม่น้อยกว่าร้อยละ 80

ความเสี่ยงต่ำ

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
23.ความเสี่ยงจากแมลงหรือสัตว์ที่ทำให้คอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า / สายสัญญาณเกิดความชำรุดหรือเสียหาย	เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน	1	3	ต่ำ 1X3=3	1. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ RACK 2. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	✓	✓	ผลผลิต : มีการห่อหุ้มสายไฟฟ้า/สายสัญญาณ เพื่อป้องกันการชำรุดเสียหายของสายไฟฟ้า/สายสัญญาณ ผลลัพธ์ : ระบบอินเทอร์เน็ตสามารถให้บริการได้อย่างต่อเนื่องโดยมีการ Downtime ไม่เกิน 36 ชั่วโมงต่อปี

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสเกิด (Likelihood)	ระดับผลกระทบสูงสุด	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ประเภทความเสี่ยง	ระยะเวลา		ตัวชี้วัด
								2569	2570	
24. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	1.เสียงบประมาณในการจัดหาอุปกรณ์ทดแทน 2. เสียภาพลักษณ์ของสำนักงานฯ	1	3	ต่ำ 1X3=3	1. ควบคุมการเข้าออกอาคาร 2. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-ออกอาคารตลอดเวลา 3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมที่ๆ มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	✓	✓	ผลผลิต : มีระบบปลอดภัยติดตั้งกล้องวงจรปิดให้ครอบคลุมที่ๆ มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่ในการเข้าออกเข้า-ออกอาคารตลอดเวลา (Access Control) ผลลัพธ์ : ป้องกันการสูญหายของอุปกรณ์เครื่องลูกข่ายและอุปกรณ์ต่อพ่วง
25. ความเสี่ยงจากแผ่นดินไหว	ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	1	3	ต่ำ 1X3=3	1. ทำการสำรองข้อมูลไว้ต่างสถานที่ 2. จัดทำแผนสำรองฉุกเฉินเพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไรและจะใช้เครื่องทดแทนจากที่ใด เพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง 3. จัดทำศูนย์สำรอง (Backup Site)	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	✓	✓	ผลผลิต : จัดทำแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร 1 แผน ผลลัพธ์ : สามารถดำเนินงานตามแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ได้ไม่น้อยกว่าร้อยละ 80

7 สรุปผลและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแลตรวจสอบ และควบคุมความเสี่ยงกับกิจกรรม หน้าที่ และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกในการขับเคลื่อน การดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กร จึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลจำนวนมากถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงาน ของทุกหน่วยงานภายในสำนักงานเลขาธิการวุฒิสภา และภายนอก ซึ่งในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาล มีความเสี่ยงตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหาย และถูกนำไปใช้ในทางที่ผิดทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น การแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือการจัดการความเสี่ยงในองค์กร

7.1. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่ผลคะแนนสูงสุด ดังนี้

7.1.1 ความเสี่ยงจากข้อมูลรั่วไหล (Data Breach) มีแนวทางปฏิบัติดังนี้

1) มาตรการเร่งด่วนโดยเพิ่มความถี่ในการแจ้งเตือนและสร้างความตระหนักให้เข้มข้น นั้น ดังนี้

1. แจ้งเวียนให้บุคลากรเปลี่ยนรหัสผ่านให้ยากต่อการคาดเดาทุก 1 เดือน ตามแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยรัฐสภา

2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยให้บุคลากรของสำนักงานเลขาธิการวุฒิสภา โดยการซ้อมป้องกันทางไซเบอร์ (Cyber Drill)

3. ยกระดับการสร้างเครือข่ายผู้ใช้งานเพิ่มเติมจากผู้ใช้งานปกติ โดยจัดทำโครงการ Super User เพื่อเป็นการสร้างเครือข่ายเฝ้าระวังภายในให้ครบทุกสำนัก

2) มาตรการระยะยาว ซึ่งจะดำเนินการยกระดับความปลอดภัยในส่วนของผู้ใช้งานทั่วไป ดังนี้

1. จัดทำโครงการการยืนยันตัวตน ผ่าน MFA (Multi Factor Authentication) เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการยืนยันตัวตนของผู้ใช้งานผ่านรหัสผ่านที่สร้างขึ้นเฉพาะครั้ง

2. นำโปรแกรม ADSelfService มาใช้ในการบริหารจัดการรหัสผ่านตามแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยรัฐสภา

3) การนำเอาเทคโนโลยี DLP มาใช้ในระดับไฟล์ข้อมูล เพื่อการป้องกันการรั่วไหลของข้อมูล

7.1.2 ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายนอก ซึ่งมีการกำหนดมาตรการ ดังนี้

1) ติดตั้งระบบป้องกันและเตือนภัยโปรแกรมประสงค์ร้าย อาทิ Spam, Virus, Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้น ๆ อยู่เป็นประจำเพื่อที่จะสามารถแก้ไขได้ทันเมื่อถูกโจมตี

2) หมั่นตรวจสอบ Policy และ Log ของ Firewall IPS/IDS อย่างสม่ำเสมอ

3) จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับสถานการณ์ได้โดยไม่สับสน

4) ติดตั้ง Firewall และ IDS/IPS เพื่อป้องกันฐานข้อมูลที่มีความสำคัญโดยเฉพาะ

7.1.3 ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายใน ซึ่งมีการกำหนดมาตรการ ดังนี้

1) ติดตั้งระบบป้องกันและเตือนภัยโปรแกรมประสงค์ร้าย อาทิ Spam, Virus, Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้น ๆ อยู่เป็นประจำเพื่อที่จะสามารถแก้ไขได้ทันเมื่อถูกโจมตี

2) หมั่นตรวจสอบ Policy และ Log ของ Firewall IPS/IDS อย่างสม่ำเสมอ

3) จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับสถานการณ์ได้โดยไม่สับสน

4) ติดตั้ง Firewall และ IDS/IPS เพื่อป้องกันฐานข้อมูลที่มีความสำคัญโดยเฉพาะ

1.7.4. ความเสี่ยงจากการโจมตีทางไซเบอร์สำนักงานฯ ไม่ให้สามารถให้บริการได้ (Denial of Service - DoS) มีแนวทางปฏิบัติ ดังนี้

1) ติดตั้งระบบป้องกันและเตือน จาก Spam,Virus, Malware,Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้นๆ อยู่เป็นประจำ เพื่อลดหรือสามารถแก้ไขได้ทันเมื่อถูกโจมตี

2) หมั่นตรวจสอบ Policy และ Log ของ Firewall และ IPS/IDS อย่างสม่ำเสมอ

3) จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับสถานการณ์ใดโดยไม่สับสน

4) มีมาตรการและกฎระเบียบในการควบคุมมิให้มีการติดตั้ง โปรแกรมต่าง ๆ ลงบนเครื่องลูกข่ายอินทราเน็ตของสำนักงาน

7.1.5 ความเสี่ยงจากไวรัสเรียกค่าไถ่ Ransomware มีแนวทางปฏิบัติ ดังนี้

1) มีการ Update software ให้เป็นปัจจุบัน

2) มีการสำรองข้อมูลไว้มากกว่า 1 แห่ง

3) ให้ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์กับบุคลากรสำนักงานเลขาธิการวุฒิสภา

7.1.6 ความเสี่ยงจากการถูก Black List โดย Search Engine หรือ Spamhaus (http://www.spa mhaus.org) มีแนวทางปฏิบัติ ดังนี้

1) ติดตั้งโปรแกรม เพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ตโดยเฉพาะจาก SMTP Mail Server ซึ่งมักจะเป็นแหล่งที่ Hacker ชอบใช้ในการส่ง Spam

2) ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server หรือ FTP เช่น Symantec Web Gateway,Symantec Endpoint Protection

3) มีการอัพเดทตัวโปรแกรมและ Signature อย่างสม่ำเสมอและการทำการบำรุงรักษา (Maintenance) ทั้งฮาร์ดแวร์และซอฟต์แวร์ พร้อมทั้ง Update Licenses

7.1.7 ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ มีแนวทางปฏิบัติดังนี้

1) การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น

2) ทำสัญญา หรือข้อตกลง/สนับสนุนการใช้โปรแกรม SaaS เช่น www.docs.com แทน Microsoft Office

3) การรณรงค์ขอความร่วมมือ เจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย

7.1.8 ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware แนวทางปฏิบัติ ดังนี้

1) ใช้ระบบป้องกันไวรัสกับเครื่องแม่ข่ายที่ต้องเสียค่าใช้จ่าย เช่น Symantec Endpoint Protection ที่สำนักงานฯ ใช้อยู่ที่สามารถควบคุมการโจมตีและการบุกรุกเครือข่ายจากสาเหตุต่างๆ เช่น การระบาดของ Virus และ Worm, การโจมตีเพื่อปฏิเสธการให้บริการ (Denial of Server-DoS) การบุกรุกแบบ Vulnerability Exploit, Network Reconnaissance และเทคนิคการหลบซ่อนการโจมตีแบบ Traffic Normalization, IP Defragmentation Reassemble ได้

2) อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ

3) มีการสำรองข้อมูลที่เครื่องลูกข่ายที่จำเป็นไว้อย่างสม่ำเสมอทาง External Hard Disk หรือ Cloud

7.1.9 ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง มีแนวทางปฏิบัติ ดังนี้

1) ตรวจสอบ Availability ของ Server ด้วยโปรแกรม ตรวจสอบ เช่น โปรแกรม zabbix จากhttp://zabbix.senate.go.th/zabbix เป็นต้น

2) การจัดทำเส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า 1 เส้นทาง หากสำนักงานฯ มีงบประมาณเพียงพออาจ พิจารณาในการจัด Gateway ที่ผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISP) ต่างออกไป จะทำให้ระบบเครือข่ายอินเทอร์เน็ต (ISP) ต่างออกไป จะทำให้ระบบเครือข่ายอินเทอร์เน็ต มีเสถียรภาพมากขึ้น

3) การวาง Web Server ไว้มากกว่า 1 ที่ เช่น ที่ ISP เป็นต้น

4) การจัดตั้งศูนย์สำรอง (DR Site)

7.1.10 ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร มีแนวทางปฏิบัติดังนี้

1) ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP-Top 10 Web Application Security Risks เพื่อลดความเสี่ยง

2) มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ

3) มีมาตรการในการเข้ารหัสข้อมูลที่เป็นความลับ เช่น RSA256

4) มีการประเมินช่องโหว่ของระบบโปรแกรมประยุกต์ภายในองค์กร

7.1.11 ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง มีแนวทางปฏิบัติ ดังนี้

1) ออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) level 2

2) การออกแบบโดยการอ้างอิงด้วยแผนผังแสดงความสัมพันธ์ระหว่างกลุ่มข้อมูล (Entity)-ER Diagram

3) ให้มีการส่งมอบ Source Code ในรูปแบบ External Memory เช่น ฮาร์ดดิสก์ไดรฟ์ภายนอก (external hard drive), แฟลชไดรฟ์ (flash drive), การ์ดหน่วยความจำ (memory card) ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้

4) หากมีการพัฒนา Library ด้วยตนเองต้องส่ง Source Code Library ที่สามารถแก้ไขได้

5) มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่

6) มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม

7) มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึง การแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดท เมื่อมี Version หรือ Release ใหม่การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น

7.1.12 ความเสี่ยงจากการไม่ทำการสำรองข้อมูลหรือทำการสำรองข้อมูลแต่ขาดการอัพเดทของเครื่องคอมพิวเตอร์แม่ข่าย มีแนวทางปฏิบัติ ดังนี้

1) มีการบริหารจัดการในการทำสำรองข้อมูล (Backup) เป็นประจำอยู่เสมอ

2) มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) เพื่อความแน่ใจในข้อมูลที่เก็บไว้ ปัจจุบัน การจัดเก็บสำรองข้อมูลของสำนักงานฯ ที่มีอุปกรณ์และระบบบริหาร

3) การจัดการเชื่อมโยงเครื่องแม่ข่ายอื่นเข้าสู่ระบบการสำรองข้อมูลโดยอัตโนมัติ

7.1.13 ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหายมีแนวทางปฏิบัติ ดังนี้

1) การป้องกันระบบเครื่องแม่ข่ายฐานข้อมูลหลักเสียหายด้วยการเพิ่มประสิทธิภาพ การทำงานในแบบ Hot Standby หรือ Clustering ทุกส่วนของเครื่องแม่ข่ายฐานข้อมูลหลัก

2) การจัดเก็บฐานข้อมูลสำรอง (Backup) และที่พร้อมใช้งานได้โดยอาจประสานงานกับบริษัทผู้ให้บริการในลักษณะ Application Service Provider หรือหน่วยงานอื่น ในความตกลงที่จะใช้เครื่องของหน่วยงานอื่น เพื่อใช้งานทดแทนในกรณีที่เกิดความเสียหายต่อเครื่องแม่ข่ายฐานข้อมูลหลักของสำนักงานฯ

3) การจัดตั้งศูนย์สำรองข้อมูล (Backup Site)

7.1.14 ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหายมีแนวทางปฏิบัติ ดังนี้

1) ติดตั้งระบบตรวจจับควันที่สามารถตรวจจับควันได้ก่อนล่วงหน้า (High Sensitivity Smoke Detector) ซึ่งปัจจุบันรัฐสภา ได้ติดตั้งระบบนี้ใช้งานอยู่ในศูนย์ข้อมูลข้างต้นแล้ว

2) ติดตั้งระบบดับเพลิงแบบ Novec 1230

4) จัดตั้งศูนย์สำรองในกรณีที่เกิดอัคคีภัยขึ้น

5) มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ

7.1.15 ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart Phone, Tablet, PC) ส่วนบุคคลเข้ามาเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต มีแนวทางปฏิบัติดังนี้

1) ควบคุมการเข้าใช้เครือข่ายด้วย Radius และ Directory เช่น AD หรือ LDAP ร่วมกันในการควบคุมการเข้าใช้งานเครือข่าย

2) เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดยติดตั้งระบบยืนยันตน (Authentication)

7.1.16 ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้งาน มีแนวทางปฏิบัติดังนี้

1) มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard disk ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้อุปกรณ์ Notebook Tablet Smart Phone

2) มีมาตรการในการโอนสิทธิ์เปลี่ยนผู้ถือครอง การมอบสิทธิ์ และการบำรุงรักษา

7.1.17 ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง มีแนวทางปฏิบัติ ดังนี้

1) มีระบบไฟฟ้า 2 แห่งจ่าย A / B ให้ server และอุปกรณ์ สามารถใช้ระบบไฟฟ้าที่ศูนย์ข้อมูลหลักได้ครบทั้ง 2 แหล่งจ่าย

2) มีเครื่องกำเนิดไฟฟ้า

3) มีระบบไฟฟ้าสำรอง UPS

7.1.18 ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์ มีแนวทางปฏิบัติ ดังนี้

1) บริหารจัดการในการกำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น

2) บริหารจัดการในการกำหนด Policy ของอุปกรณ์ Bandwidth Management เพื่อกำจัดหรือปิดกั้นการใช้ resources ในทางที่ผิด

3) การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์หรือ Resources ต่างๆ ของสำนักงานฯ ไปใช้ในทางที่ผิดรวมถึงการบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา

7.1.19 ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์แม่ข่าย มีแนวทางปฏิบัติ ดังนี้

1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุม การเข้า-ออก ห้องคอมพิวเตอร์ แม่ข่าย

2. ตู้ RACK ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์จัดเก็บข้อมูล (Disk Array) และอุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจตลอดเวลา

3. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน การนำติดตัวไปด้วยตลอดเวลา หรือติดตั้งอุปกรณ์ล็อค เช่น Kensington Lock เป็นต้น เพื่อป้องกันการสูญหาย

7.1.20 ความเสี่ยงจากการเกิดอุทกภัยห้อง Data Center มีแนวทางปฏิบัติ ดังนี้

1) ติดตั้งเครื่องตรวจจับระดับน้ำรั่วไหลพื้นที่ที่มีความไวต่อน้ำ

2) มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ

7.1.21 ความเสี่ยงจากการโจรกรรมฐานข้อมูล มีแนวทางปฏิบัติ ดังนี้

1) มีการบริหารจัดการด้านการป้องกันข้อมูล

2) มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) ตามความสำคัญของข้อมูลโดยสามารถทำงานร่วมกับ Active Directory (AD) หรือ Lightweight Directory Access Protocol (LDAP) Server และ Syslog ได้

7.1.22 ความเสี่ยงจากวินาศภัย/การก่อการร้าย มีแนวทางปฏิบัติ ดังนี้

1) จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไร และจะใช้เครื่องทดแทนจากที่ใด เพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง

2) ทำการสำรองข้อมูลไว้ต่างสถานที่กัน

3) จัดทำศูนย์สำรอง (Backup Site)

7.2 สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ได้ดำเนินการจัดทำเพื่อ

7.2.1 เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

7.2.2 เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

7.2.3 ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

7.3 ข้อเสนอแนะ

7.3.1 การควบคุมนโยบายและการบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่า ได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

1) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

2) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

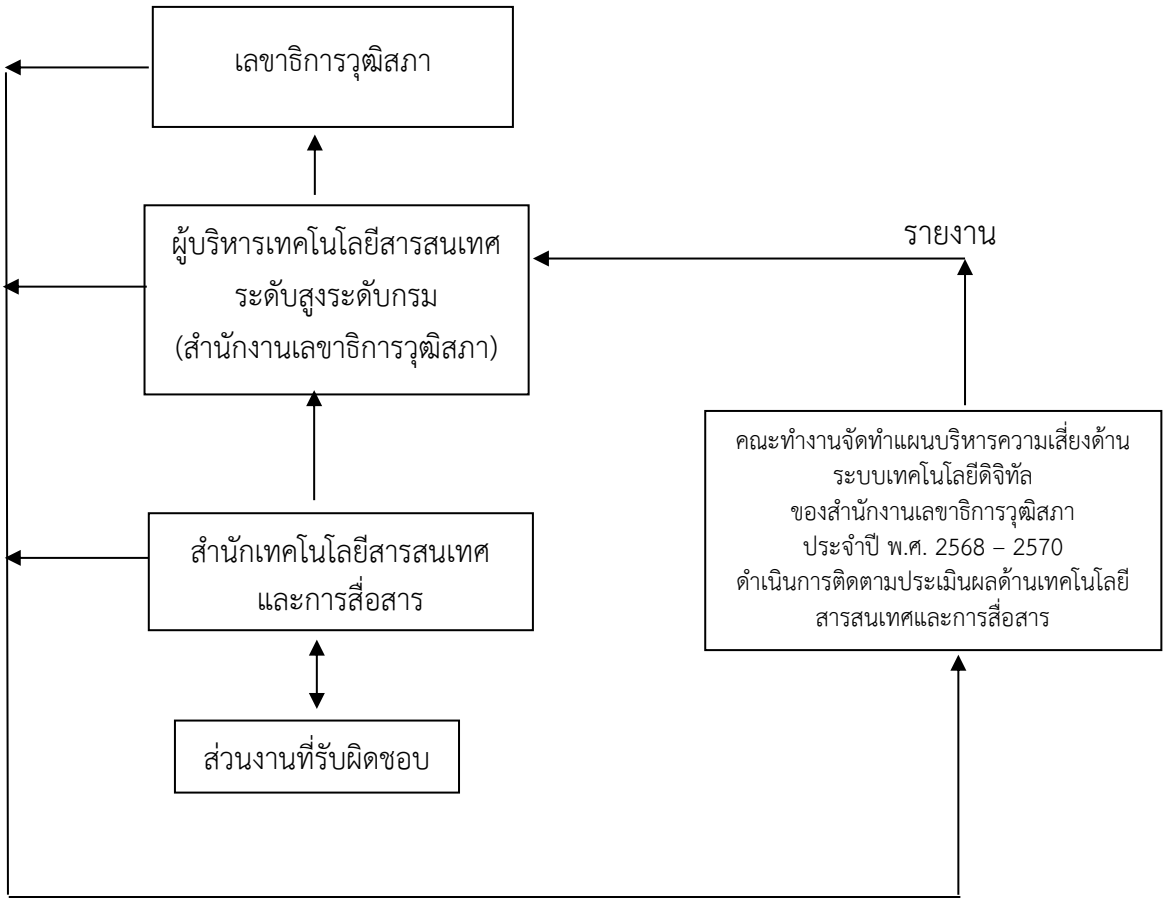
3) กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

7.3.2 การติดตามการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ

8 การบริหารจัดการและการติดตามประเมินผลแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 – 2570 (ฉบับปรับปรุง)

สำนักงานเลขาธิการวุฒิสภา กำหนดโครงสร้างการบริหารจัดการและแนวทางการติดตามประเมินผล เพื่อเป็นเครื่องวัดความสำเร็จของแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 – 2570 (ฉบับปรับปรุง) ดังนี้

โครงสร้างการบริหารจัดการ แต่งตั้งคณะทำงานติดตามประเมินผลแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เพื่อทำการวิเคราะห์และวางระบบติดตามประเมินผล และรายงานผลการทำงานต่อผู้บริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา ตามลำดับชั้น



รูปที่ 3 ผังโครงสร้างการบริหารจัดการและติดตามประเมินผลแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

<u>ตัวอย่าง</u> แบบรายงานติดตามประเมินผล

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

ปี .....

ความเสี่ยง	ผลกระทบ	มาตรการ/ แผนปฏิบัติการ	ผลการ ดำเนินงาน	ระยะเวลา ในการ ดำเนินการ	ผู้รับผิดชอบ/ ผู้ดำเนินงาน
1.....					
2.....					
3.....					
4.....					

บรรณานุกรม

สำนักงานเลขาธิการวุฒิสภา, แผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2566 - 2570 (ฉบับปรับปรุง พ.ศ. 2568). กรุงเทพฯ: สำนักการพิมพ์ สำนักงานเลขาธิการวุฒิสภา, 2568.

สำนักงานเลขาธิการวุฒิสภา, แผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. 2569 กรุงเทพฯ: สำนักการพิมพ์ สำนักงานเลขาธิการวุฒิสภา, 2569.

สำนักงานเลขาธิการวุฒิสภา, แผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 - 2570, (กรุงเทพฯ: สำนักเทคโนโลยีสารสนเทศและการสื่อสาร, 2568).

สำนักงานเลขาธิการวุฒิสภา, แผนบริหารความเสี่ยงสำนักงานเลขาธิการวุฒิสภา 2569 - 2570 กรุงเทพฯ: สำนักนโยบายและแผน สำนักงานเลขาธิการวุฒิสภา, 2569

สำนักงานเลขาธิการสภาผู้แทนราษฎร, แผนพัฒนารัฐสภาดิจิทัล (Digital Parliament) พ.ศ. 2566 – 2570 (ฉบับปรับปรุง), (กรุงเทพฯ: สำนักการพิมพ์ สำนักงานเลขาธิการสภาผู้แทนราษฎร), 2568.

Committee of Sponsoring Organization of the Treadway Commission. (2013). COSO Internal Control Integrated Framework (Online) http://www.coso.org เข้าสืบค้นเมื่อ 2566

ภาคผนวก

คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล
ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 - 2570

คำสั่งสำนักเทคโนโลยีสารสนเทศและการสื่อสาร
ที่ ๑๐/๒๕๖๘
เรื่อง แต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล
ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๘ - ๒๕๗๐

.....

ตามนโยบายเลขาธิการวุฒิสภาในการรักษามาตรฐานคุณภาพและความสำเร็จของสำนักงานให้ยั่งยืนและยกระดับการบริหารจัดการองค์กร ให้เท่าทันต่อการเปลี่ยนแปลงเพื่อการเป็นองค์การอัจฉริยะ โดยสำนักงานเลขาธิการวุฒิสภามีการจัดทำแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๖ - ๒๕๗๐ (ฉบับปรับปรุง พ.ศ. ๒๕๖๘) โดยประกาศไปแล้ว ณ วันที่ ๒๘ พฤษภาคม พ.ศ. ๒๕๖๘ แผนปฏิบัติราชการเรื่องที่ ๓ พัฒนาระบบการบริหารจัดการมุ่งสู่ความเป็น Smart Digitalization ตัวชี้วัดที่ ๑๗ ร้อยละความสำเร็จของการป้องกันการถูกบุกรุกโจมตีทางไซเบอร์ ตัวชี้วัดที่ ๑๘ จำนวนชั่วโมงของการหยุดทำงาน (Downtime) ของระบบเทคโนโลยีสารสนเทศของสำนักงานเลขาธิการวุฒิสภา แนวทางการพัฒนาที่ ๓.๒ พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล และเป็นไปตามแนวทางแผนพัฒนารัฐสภาดิจิทัล (Digital Parliament) ส่วนของสำนักงานเลขาธิการวุฒิสภา เพื่อให้มีกรอบการดำเนินงานตามมาตรการการบริหารความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา นั้น

เพื่อให้สำนักงานเลขาธิการวุฒิสภาดำเนินการเตรียมความพร้อมในการพัฒนาระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา สามารถรองรับภารกิจของวุฒิสภาและสำนักงานเลขาธิการวุฒิสภา ให้มีการบริหารจัดการข้อมูลสารสนเทศและระบบการทำงานที่ปรับเป็นดิจิทัลเต็มรูปแบบ มีประสิทธิภาพและใช้งานได้ เพื่อพัฒนาไปในแนวทางเดียวกับแผนพัฒนารัฐสภาดิจิทัล ต้องอยู่บนความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัล ดังนั้น เพื่อให้เกิดประสิทธิภาพในการดำเนินงาน จึงขอยกเลิกคำสั่งสำนักเทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๖/๒๕๖๗ ลงวันที่ ๑๖ พฤษภาคม พ.ศ. ๒๕๖๗ และแต่งตั้งคณะทำงานจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๘ – ๒๕๗๐ โดยมีองค์ประกอบและอำนาจหน้าที่ ดังนี้

๑. องค์ประกอบ

๑.๑ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร	ที่ปรึกษาคณะทำงาน
๑.๒ ผู้บังคับบัญชากลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์	หัวหน้าคณะทำงาน
๑.๓ ผู้บังคับบัญชากลุ่มงานวิทยาการคอมพิวเตอร์	คณะทำงาน
๑.๔ ผู้บังคับบัญชากลุ่มงานพัฒนาระบบงานคอมพิวเตอร์	คณะทำงาน

๑.๕ ผู้บังคับบัญชา...

๑.๕	ผู้บังคับบัญชากลุ่มงานบริการระบบคอมพิวเตอร์	คณะทำงาน
๑.๖	นายประจักษ์ เพ็ญเลี้ยง	คณะทำงาน
๑.๗	นายสุวิทย์ น้อยอยู่	คณะทำงาน
๑.๘	นายสุรชัย เตชมี	คณะทำงาน
๑.๙	นางสาวพนมวัน อินรีย์	คณะทำงาน
๑.๑๐	นางสาวสุดารัตน์ พงษ์เฉลียว	คณะทำงาน
๑.๑๑	นางสาวกนกกร โพธิ์สุนทร	คณะทำงาน
๑.๑๒	นางสาวกัลยา แพงสาย	คณะทำงาน
๑.๑๓	นายสิทธิชัย สุนทร	คณะทำงาน
๑.๑๔	นายสาโรจน์ ภคุโล	คณะทำงาน
๑.๑๕	นางสาวสุดารัตน์ ใจอุดม	คณะทำงานและเลขานุการ
๑.๑๖	นางสาวพัทธกานต์ วุฒิอัครวัฒน์	คณะทำงานและผู้ช่วยเลขานุการ
๑.๑๗	จ่าโท เชิดศักดิ์ เพิ่มทรัพย์	คณะทำงานและผู้ช่วยเลขานุการ
๑.๑๘	นางสาวเบญจมาศ สำเนียงสูง	คณะทำงานและผู้ช่วยเลขานุการ

๒. อำนาจหน้าที่

๒.๑ ศึกษา วิเคราะห์ แผนพัฒนา กฎระเบียบที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารของภาครัฐ ทบทวนแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล และที่เกี่ยวข้องของสำนักงานเลขาธิการวุฒิสภา และทบทวนแผนรายปี

๒.๒ ศึกษา วิเคราะห์ และจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๘ - ๒๕๗๐ ให้สอดคล้องกับแผนพัฒนารัฐสภาดิจิทัล (Digital Parliament) พ.ศ. ๒๕๖๖ – ๒๕๗๐

๒.๓ จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๘ - ๒๕๗๐ เพื่อรองรับความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา

๒.๔ กำกับดูแล ตรวจสอบติดตามผลการดำเนินงาน ประสานการดำเนินงานที่เกี่ยวข้องตามแผนฯ ที่กำหนดไว้ รายงานผลการดำเนินงานให้ผู้บังคับบัญชาตามสายการบังคับบัญชาทราบเป็นระยะเพื่อพิจารณาดำเนินการต่อไป และรายงานต่อหัวหน้าส่วนราชการ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๘ กรกฎาคม พ.ศ. ๒๕๖๘

(นางทุติยาพร ทวนทอง)
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 - 2570 (ฉบับปรับปรุง)

คณะทำงานจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล
ของสำนักงานเลขาธิการวุฒิสภา พ.ศ. 2568 - 2570