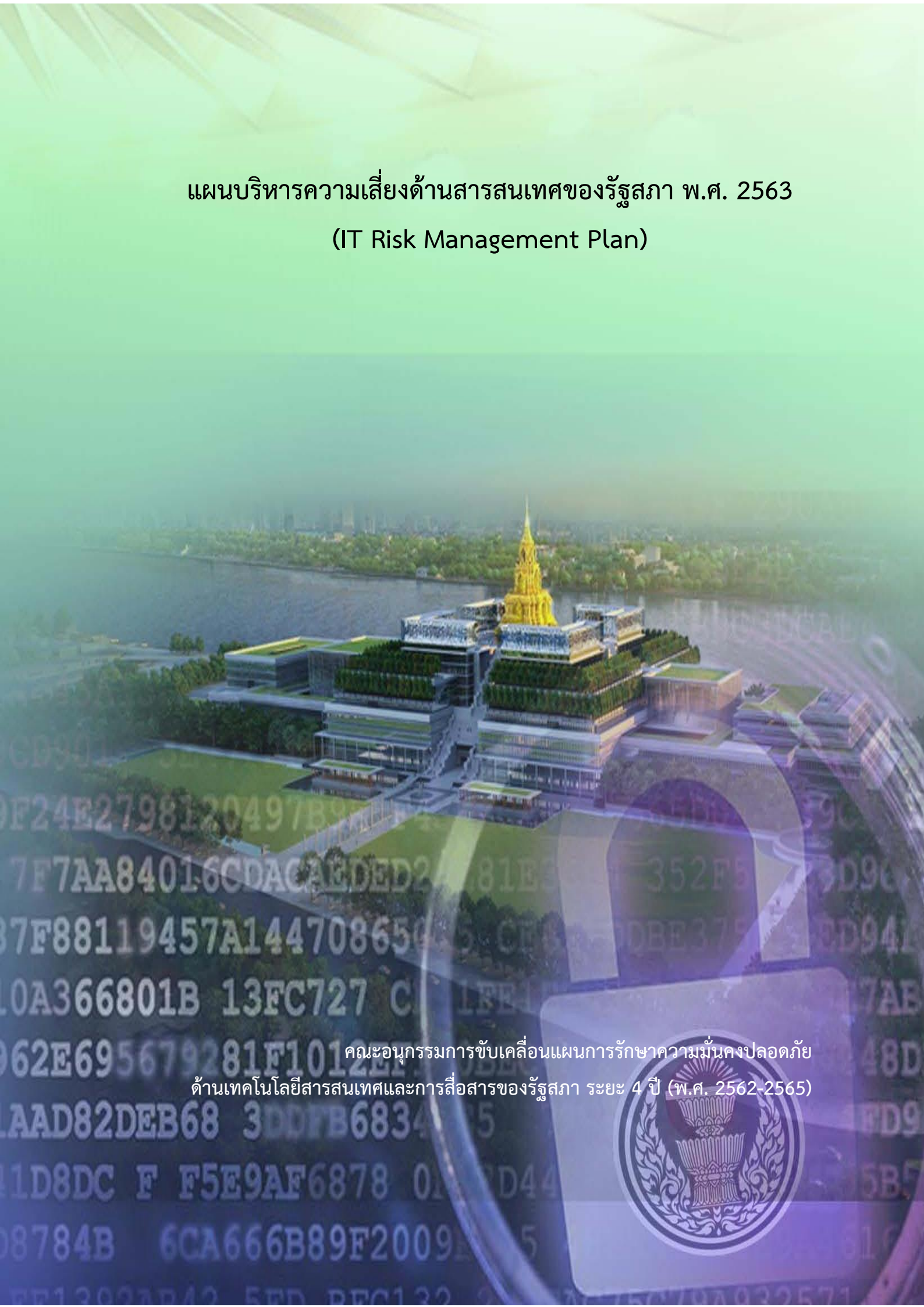
แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา พ.ศ. 2563

(IT Risk Management Plan)



คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ 4 ปี (พ.ศ. 2562-2565)

คำนำ

แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา พ.ศ. 2563 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง ตอบสนองความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้ยอมรับได้ โดยมุ่งหวังให้รัฐสภาสามารถบรรลุตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม รัฐสภาจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite) คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ 4 ปี (พ.ศ. 2562 - 2565) หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของรัฐสภา ต่อไป

คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา
ระยะ 4 ปี (พ.ศ. 2562 - 2565)
มิถุนายน 2563

สารบัญ

สารบัญตาราง

สารบัญภาพ

แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา พ.ศ. 2563

1. หลักการและเหตุผล

การเปลี่ยนแปลงสภาพแวดล้อมในการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งปัจจัยภายใน อาทิ การปรับเปลี่ยนแผนยุทธศาสตร์ กลยุทธ์ การเปลี่ยนแปลงทรัพยากรภายในสำนักงาน การเปลี่ยนแปลงสถานที่และด้านการปฏิบัติงาน รวมถึงปัจจัยภายนอก อาทิ เหตุการณ์ความไม่สงบทางการเมือง ภัยธรรมชาติ เป็นต้น อาจส่งผลกระทบให้การดำเนินงานของรัฐสภาไม่เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนการดำเนินงานและแผนกลยุทธ์ ซึ่งจะก่อให้เกิดความเสี่ยงต่อรัฐสภาโดยรวม

การบริหารความเสี่ยงเป็นองค์ประกอบของการกำกับดูแลกิจการที่ดี ซึ่งนอกจากจะสนับสนุนให้องค์กรสามารถดำเนินงานได้บรรลุตามเป้าหมายที่กำหนดแล้ว ยังสามารถสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้ส่วนเสียขององค์กร (Stakeholders) ได้อีกทางหนึ่ง รัฐสภาจึงได้นำกรอบแนวทางการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ (Enterprise Risk Management–Integrated Framework) ตามแนวทาง COSO ERM ซึ่งมีวัตถุประสงค์ในการให้ผู้บริหาร เจ้าหน้าที่ที่เกี่ยวข้องในองค์กรตระหนักถึงความสำคัญของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของรัฐสภา และมีความเข้าใจตรงกันในคำนิยาม เป้าหมาย และวัตถุประสงค์ อันจะเป็นการสร้างความรับผิดชอบอย่างทั่วถึงและเป็นไปในทิศทางเดียวกันทั้งรัฐสภาได้อย่างมีประสิทธิภาพ เพื่อใช้เป็นแนวทางให้ผู้บริหาร เจ้าหน้าที่ทั่วทั้งองค์กร เป็นส่วนหนึ่งของการพัฒนากระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผน เพื่อให้รัฐสภามีกรอบการดำเนินการที่ตอบสนองต่อเหตุการณ์ที่อาจส่งผลให้เกิดความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลและเทคโนโลยีสารสนเทศและการสื่อสารได้อย่างเป็นระบบ และมีมาตรฐาน รวมทั้งมีการดำเนินการเพื่อสร้างพื้นฐานในการป้องกันความเสี่ยงระยะยาวที่สำคัญให้รัฐสภา อีกทั้งเป็นกลไกในการพัฒนาองค์ความรู้ด้านการบริหารความเสี่ยงสำหรับผู้บริหาร เจ้าหน้าที่ และสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน มีความตระหนักและมีความเข้าใจตรงกันถึงเป้าหมาย วัตถุประสงค์ รวมทั้งแนวทางการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา เพื่อร่วมกันสร้างความพึงพอใจให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholders) และสร้างมูลค่าเพิ่มให้องค์กร โดยพิจารณาถึงผลกระทบต่อเป้าหมายการดำเนินงานของรัฐสภาให้เป็นไปตามหลักการกำกับดูแลกิจการที่ดี

การบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลและเทคโนโลยีสารสนเทศและการสื่อสาร เป็นองค์ประกอบสำคัญของการดำเนินงานด้านระบบเทคโนโลยีดิจิทัลและเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภาเป็นอย่างมาก จึงมีความจำเป็นในการกำหนดนโยบายบริหารความเสี่ยงด้าน

ระบบเทคโนโลยีดิจิทัลและเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา เพื่อบังคับใช้กับทุกหน่วยงานที่เกี่ยวข้องของรัฐสภา โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจและตระหนักถึงหน้าที่ความรับผิดชอบต่อการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลและเทคโนโลยีสารสนเทศและการสื่อสารอยู่เสมอ และยังสนับสนุนให้เจ้าหน้าที่ทุกระดับชั้นเข้าใจ รวมถึงมีส่วนร่วมในการบริหารและจัดการความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลและเทคโนโลยีสารสนเทศและการสื่อสารในทุกขั้นตอนปฏิบัติงาน แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลเทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วย การวางระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลและเทคโนโลยีสารสนเทศและการสื่อสารภายในรัฐสภาได้อย่างมีประสิทธิภาพ และการป้องกัน ควบคุม และลดผลกระทบจากเหตุการณ์ความเสียหายที่อาจเกิดขึ้น โดยกระบวนการดังกล่าวจะอยู่ภายใต้การดูแลของหัวหน้าส่วนงาน ผู้อำนวยการ และมีการกำกับ ดูและสั่งการโดยคณะทำงานด้านการบริหารความเสี่ยง

2. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา

2.1 เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ

2.2 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

2.3 เพื่อดำเนินการจัดการความเสี่ยงที่เกี่ยวข้องให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีความเข้าใจกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภาอย่างถ่องแท้

2.4 เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับแผนงานด้านเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสาร ให้ได้รับการยอมรับและมีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและมีความต่อเนื่อง

2.5 เพื่อช่วยเพิ่มประสิทธิภาพในการบริหารความเสี่ยงอันจะมีผลกระทบต่อการดำเนินงานให้เป็นไปตามแนวนโยบาย และเป้าประสงค์ เพื่อพิจารณาดำเนินการหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มดำเนินงานหรือดำเนินงานตามแผน

3. แผนพัฒนา Digital Parliament ของรัฐสภา ระยะ 5 ปี (พ.ศ. 2561–2565)

3.1 วิสัยทัศน์

รัฐสภาดิจิทัล (Digital Parliament) หมายถึง องค์การที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้อย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อสนับสนุนงานด้านนิติบัญญัติ

3.2 พันธกิจ

จากการกำหนดยุทธศาสตร์ของแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ 5 ปี (พ.ศ. 2561–2565) มีพันธกิจ 2 ด้าน ดังนี้

1) พัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้ผู้รับบริการและประชาชนได้รับข้อมูลสารสนเทศของรัฐสภาที่ถูกต้อง รวดเร็ว และทันสมัย ตรงกับความต้องการ

2) พัฒนาและส่งเสริมสมาชิกรัฐสภา และบุคคลในวงงานรัฐสภาให้รู้เท่าทันการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสร้างสรรค์

3.3 เป้าประสงค์เชิงยุทธศาสตร์

เป้าประสงค์เชิงยุทธศาสตร์ของแผนพัฒนา Digital Parliament ของรัฐสภาระยะ 5 ปี (พ.ศ. 2561–2565) มีดังนี้

1) ระบบข้อมูลและสารสนเทศของรัฐสภา มีการเชื่อมโยงและบูรณาการเพื่อให้บริการอย่างมีประสิทธิภาพ

2) ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีประสิทธิภาพและมีความมั่นคงปลอดภัยเป็นไปตามมาตรฐานสากล

3) สมาชิกรัฐสภาและบุคคลในวงงานรัฐสภารู้เท่าทันสามารถใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างสร้างสรรค์

4) ผู้รับบริการและประชาชนได้รับข้อมูลสารสนเทศของรัฐสภาที่ถูกต้อง รวดเร็ว และทันสมัยตรงกับความต้องการ

3.4 ยุทธศาสตร์ของแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ 5 ปี (พ.ศ. 2561–2565)

1) พัฒนาระบบและบูรณาการข้อมูลมุ่งสู่การเป็น Digital Parliament

2) พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามมาตรฐานสากล

3) ส่งเสริมและสนับสนุน ให้สมาชิกรัฐสภา และบุคคลในวงงานรัฐสภา มีความรู้ความสามารถและทักษะในการประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ

4. กระบวนการบริหารความเสี่ยงด้านสารสนเทศ

4.1 คำนิยาม

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายองค์กร ทั้งในด้านกลยุทธ์ ด้านการดำเนินงาน ด้านการเงิน และด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

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

4.2 กระบวนการบริหารความเสี่ยง

แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา เป็นกระบวนการบริหารความเสี่ยงตามหลักธรรมาภิบาลมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread Way Commission) เพื่อเตรียมการรองรับการเปลี่ยนแปลงที่อาจเกิดขึ้นและส่งผลกระทบต่อด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ซึ่งต้องมีการวิเคราะห์ และบริหารจัดการความเสี่ยงตามประเด็นยุทธศาสตร์ที่เกี่ยวข้องให้ครบถ้วน โดยมีขั้นตอนการดำเนินการหรือเกณฑ์ในการวิเคราะห์ ประเมิน และจัดการความเสี่ยงอย่างเหมาะสมตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO ซึ่งมีขั้นตอนการดำเนินการ 7 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

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

1) วัตถุประสงค์ระดับองค์กร (Corporate Objective) เป็นวัตถุประสงค์ของการดำเนินงานในภาพรวม ตามแผนยุทธศาสตร์และแผนปฏิบัติราชการประจำปีขององค์กร

2) วัตถุประสงค์ระดับกิจกรรม (Activities Objective) เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจงลงไปสำหรับแต่ละกิจกรรมที่องค์กรกำหนดเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การกำหนดวัตถุประสงค์ที่ชัดเจนช่วยให้การระบุและวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นได้อย่างครบถ้วน ซึ่งวัตถุประสงค์ที่กำหนดขึ้นในแต่ละระดับ ควรมีการกำหนดเป้าหมายและตัวชี้วัดความสำเร็จที่ชัดเจนและสามารถวัดผลได้วัตถุประสงค์ที่ดี (SMART) ควรมีลักษณะดังนี้

S :Specific หมายถึงมีการกำหนดเป้าหมายที่ชัดเจน

M :Measurable หมายถึงสามารถวัดผลหรือประเมินผลได้

A :Achievable หมายถึงสามารถปฏิบัติให้บรรลุผลได้

R :Reasonable หมายถึงสมเหตุผล มีความเป็นไปได้

T :Time constrained หมายถึง มีกรอบเวลาที่ชัดเจนและเหมาะสม

ขั้นตอนที่ 2 การระบุความเสี่ยงต่างๆ (Event Identification)

นอกจากการกำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารตามแนวทางของ COSO ออกเป็น 8 ประเภทแล้ว การระบุความเสี่ยงยังต้องนำหลักธรรมาภิบาลมาเป็นปัจจัยในการวิเคราะห์และระบุความเสี่ยง 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 รวมถึง ตอบสนองตามความคาดหวัง/ความต้องการของประชาชนผู้รับบริการ และผู้มีส่วนได้ส่วนเสียที่มีความหลากหลายและมีความแตกต่าง

4) หลักภาระรับผิดชอบ (Accountability) หมายถึง การแสดงความรับผิดชอบในการปฏิบัติหน้าที่ และผลงานต่อเป้าหมายที่กำหนดไว้ โดยความรับผิดชอบนั้นควรอยู่ในระดับที่สนองต่อความคาดหวังของสาธารณะ รวมทั้งการแสดงถึงความสานึกในการรับผิดชอบต่อปัญหาสาธารณะ

5) หลักความโปร่งใส (Transparency) หมายถึง กระบวนการเปิดเผยอย่างตรงไปตรงมา ชี้แจงได้เมื่อมีข้อสงสัย และสามารถเข้าถึงข้อมูลข่าวสารอันไม่ต้องห้ามตามกฎหมายได้อย่างเสรีโดยประชาชนสามารถรู้ทุกขั้นตอนในการดำเนินกิจกรรม หรือกระบวนการต่างๆ และสามารถตรวจสอบได้

6) หลักการมีส่วนร่วม (Participation) หมายถึง กระบวนการที่ข้าราชการ ประชาชนและผู้มีส่วนได้ส่วนเสียทุกกลุ่มมีโอกาสได้เข้าร่วมรับรู้ เรียนรู้ ทาความเข้าใจ 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 กฎระเบียบข้อบังคับในการบริหารราชการด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของผู้มีส่วนได้ส่วนเสีย

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

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

<u>ขั้นตอนที่ 3 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	นานๆ ครั้ง (แทบไม่เกิดขึ้นเลย)
2	ไม่บ่อย (อาจเกิดขึ้นได้ทุก 5 ปี)
3	ปานกลาง (อาจเกิดขึ้นได้ทุกปี)
4	บ่อย (อาจเกิดขึ้นได้ทุกเดือน)
5	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

2) การประเมินความรุนแรงของผลกระทบ (Impact : I) เป็นขั้นตอนการประเมินขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง ซึ่งสามารถจัดแบ่งออกเป็นระดับต่างๆ 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)
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 4 กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

เป็นการวิเคราะห์ทางเลือกกลยุทธ์ในการจัดการความเสี่ยง เพื่อช่วยในการตัดสินใจของบุคคลหรือองค์กรใดๆ ในอันที่จะหาวิธีการที่ดีที่สุดในการตัดสินใจแก้ไขปัญหาต่างๆ ที่อาจเกิดขึ้นในอนาคต ทั้งนี้เพื่อลดผลกระทบหรือความเสียหายที่อาจเกิดขึ้นให้น้อยที่สุด โดยมีค่าใช้จ่ายน้อยที่สุด ซึ่งมีวิธีการจัดการ ดังนี้

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

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

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

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

<u>ขั้นตอนที่ 5 กิจกรรมการควบคุมความเสี่ยง (Control Activities)</u>

เป็นขั้นตอนดำเนินการกำหนดกิจกรรม หรือมาตรการในการจัดการความเสี่ยงให้หมดไป หรือควบคุมความเสี่ยงให้ลดลงในระดับที่ยอมรับได้ โดยกิจกรรมที่กำหนดต้องเป็นกิจกรรมที่ยังไม่เคยปฏิบัติ หรือเป็นกิจกรรมที่กำหนดขึ้นเพิ่มเติมจากกิจกรรมเดิมที่เคยปฏิบัติอยู่แล้ว แต่กิจกรรมนั้นไม่สามารถควบคุมความเสี่ยงได้ นอกจากนี้ยังต้องกำหนดระยะเวลาที่ใช้ในการดำเนินการแต่ละกิจกรรม ตลอดจนหน่วยงานผู้รับผิดชอบ ดังนั้นกิจกรรมการบริหารความเสี่ยงต่างๆ 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) การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น ซึ่งควรพิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน และพิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

3) กำหนดระยะเวลาแล้วเสร็จของงาน

ขั้นตอนที่ 6 ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

เป็นขั้นตอนและกระบวนการโดยมีวัตถุประสงค์เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง มีการเปิดช่องทางการสื่อสาร และรับทราบข้อมูลด้านการบริหารความเสี่ยงให้กับผู้บริหารและบุคลากรขององค์กรได้เข้าถึง โดยผ่านช่องทางต่างๆ เช่น ระบบอินทราเน็ต หนังสือเวียน การประชุมชี้แจงโดยผู้บริหาร หรือการฝึกอบรม เป็นต้น ซึ่งการสื่อสารที่มีประสิทธิผลนั้น ต้องให้มั่นใจได้ว่า

1) ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา

2) ผู้บริหารสามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่ได้ทันท่วงที

3) มีการติดตามแผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กร และจัดการความเสี่ยงต่าง ๆ เพื่อให้องค์กรมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด

ขั้นตอนที่ 7 การติดตามและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

การติดตาม และเฝ้าระวังความเสี่ยง โดยการกำหนดให้มีการติดตาม และประเมินผลว่าแต่ละหน่วยงานมีการประเมินประสิทธิผลของการจัดการความเสี่ยงที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ เพื่อให้เกิดความมั่นใจว่ามาตรการในการปรับปรุงความเสี่ยงที่วางไว้มีความเพียงพอเหมาะสม มีประสิทธิภาพประสิทธิผล และมีการปฏิบัติจริง สามารถลดหรือป้องกันความเสี่ยงที่อาจเกิดขึ้น นับเป็นขั้นตอนสุดท้ายและเป็นปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง ซึ่งควรพิจารณาประเด็นต่อไปนี้

1) การรายงาน และสอบทานขั้นตอนตามกระบวนการบริหารความเสี่ยง เช่น การรายงานและติดตามผลระหว่างการดำเนินงาน (On Going Monitoring) เพื่อสังเกต ติดตาม 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

4.3 ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

รัฐสภาได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ออกได้เป็น 5 ประเภท

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

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

3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ 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 ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจากความผิดพลาดของซอฟต์แวร์นั้นๆ หรือการถูกผู้ประสงค์ร้ายเข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งอาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

5) ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูล

ถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไข เปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสีย รวมถึงประชาชนทั่วไป ดังนั้นการรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากมนุษย์ ภัยจากธรรมชาติหรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

4.4 การตอบสนองความเสี่ยง

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

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นไว้เอง โดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสี่ยหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่

พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือ การหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือ สัญญาการบำรุงรักษาหลังการขาย

4.5 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของรัฐสภา ได้แก่

4.5.1 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

4.5.2 ปัจจัยภายใน ได้แก่

1) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2) การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

3) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอร์ฟแวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดทำงาน

4.6 การประเมินความเสียหาย

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

2) ความเสียหายที่เกิดผลเสียหายและต้องหยุดชั่วขณะได้แก่การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

4.7 การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือนและให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

4.8 สถานภาพระบบรักษาความมั่นคงปลอดภัย ICT ของรัฐสภา

สถานภาพระบบรักษาความมั่นคงปลอดภัย ICT ของรัฐสภา จากการสำรวจและวิเคราะห์สถานภาพปัจจุบันทางด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการสภาผู้แทนราษฎร และสำนักงานเลขาธิการวุฒิสภา มีรายละเอียดในด้านต่าง ๆ ประกอบด้วย

4.8.1 สถานภาพด้านฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร

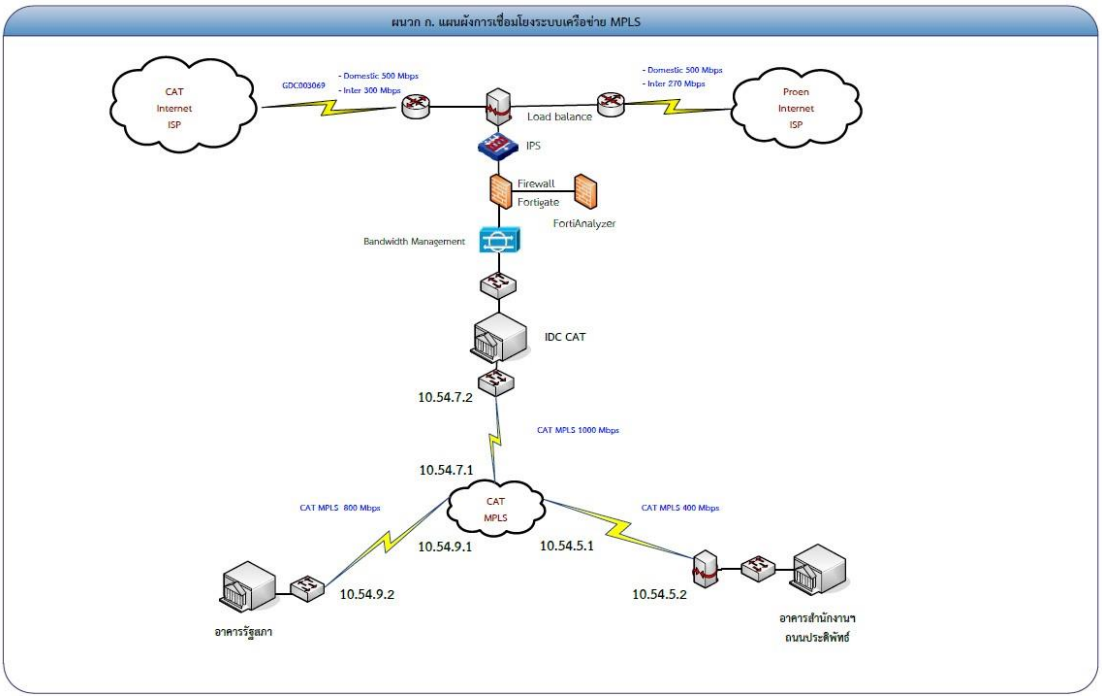
จากการสำรวจสถานภาพปัจจุบันทางด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการสภาผู้แทนราษฎร และสำนักงานเลขาธิการวุฒิสภา สามารถสรุปรายละเอียดของฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร ได้ดังนี้

1) สำนักงานเลขาธิการสภาผู้แทนราษฎรมี ฮาร์ดแวร์ ซอฟต์แวร์ ด้านความปลอดภัย ดังนี้

ตารางที่ 3 ฮาร์ดแวร์ ซอฟต์แวร์ ด้านความปลอดภัยของสำนักงานเลขาธิการสภาผู้แทนราษฎร

ลำดับ	รายการอุปกรณ์	ยี่ห้อ/รุ่น	สถานที่ติดตั้ง	จำนวน (ชุด)	ปีที่จัดหา	หมายเหตุ
1	อุปกรณ์ระบบป้องกันไวรัสคอมพิวเตอร์ (Virus Wall)	McAfee EWS3200 Appliance	อาคารกษาปณ์	3	2554	
2	Firewall	FortiGate600D	ศูนย์ IDC	1	2560	
3	Firewall Log Analyzer	FortiAnalyzer400E	ศูนย์ IDC	1	2556	
4	ระบบยืนยันตัวบุคคล พร้อมตรวจจับพฤติกรรมที่น่าสงสัยและป้องกันการบุกรุกระบบเครือข่ายจากภายใน(Network Access Control)	ForescoutCT 2000	ศูนย์ IDC	1	2556	
5	ระบบยืนยันตัวบุคคล พร้อมตรวจจับพฤติกรรมที่น่าสงสัยและป้องกันการบุกรุกระบบเครือข่ายจากภายใน(Network Access Control)	ForescoutCT 1000	อาคารกษาปณ์ , ศูนย์ IDC	3	2556	
6	Antivirus server	Nod Server	อาคารกษาปณ์	2	2556	
7	ระบบเฝ้าระวัง SERVER แบบ 24x7	SIEM SYSTEM ,rapid7	บริษัท กสท	1	2561	จ้างบริการ
8	ระบบวิเคราะห์ LOG	SIEM SYSTEM	บริษัท กสท	1	2561	จ้างบริการ
9	ระบบเฝ้าระวังและแจ้งเตือนสถานะเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ระบบเครือข่าย	Forerunner	อาคารกษาปณ์	1	2559	พัฒนาเอง
10	Mail gateway	บริษัท กสท	ศูนย์ IDC	1	2561	จ้างบริการ
11	ระบบสแกนลายนิ้วมือสำหรับห้อง server	HIP		2	2560	
12	ระบบป้องกันการทำ DDOS PROTECTION	Nexus Guard	บริษัท กสท	1	2561	จ้างบริการ
13	LDAP	ใช้ OpenSource และ implement เอง	ศูนย์ IDC	2	2552	
14	Radius	ใช้ Open Source และ implement เอง	ศูนย์ IDC	2	2552	

แผนผัง network สำนักงานเลขาธิการสภาผู้แทนราษฎรแสดงได้ดังภาพที่ 1



ภาพที่ 1 ไดอะแกรม network สำนักงานเลขาธิการสภาผู้แทนราษฎร

ในด้านบุคลากรด้านความมั่นคงปลอดภัยด้านสารสนเทศสำนักงานเลขาธิการสภาผู้แทนราษฎร ได้มอบหมายให้กลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นกลุ่มงานที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ให้ดูแลความมั่นคงปลอดภัยสารสนเทศด้วย ซึ่งทางกลุ่มงานมีบุคลากรในการดูแลระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ดังนี้

ตำแหน่ง	จำนวน/คน
ผู้บังคับบัญชากลุ่มงาน	1
นักวิชาการคอมพิวเตอร์	11
เจ้าพนักงานธุรการ	1

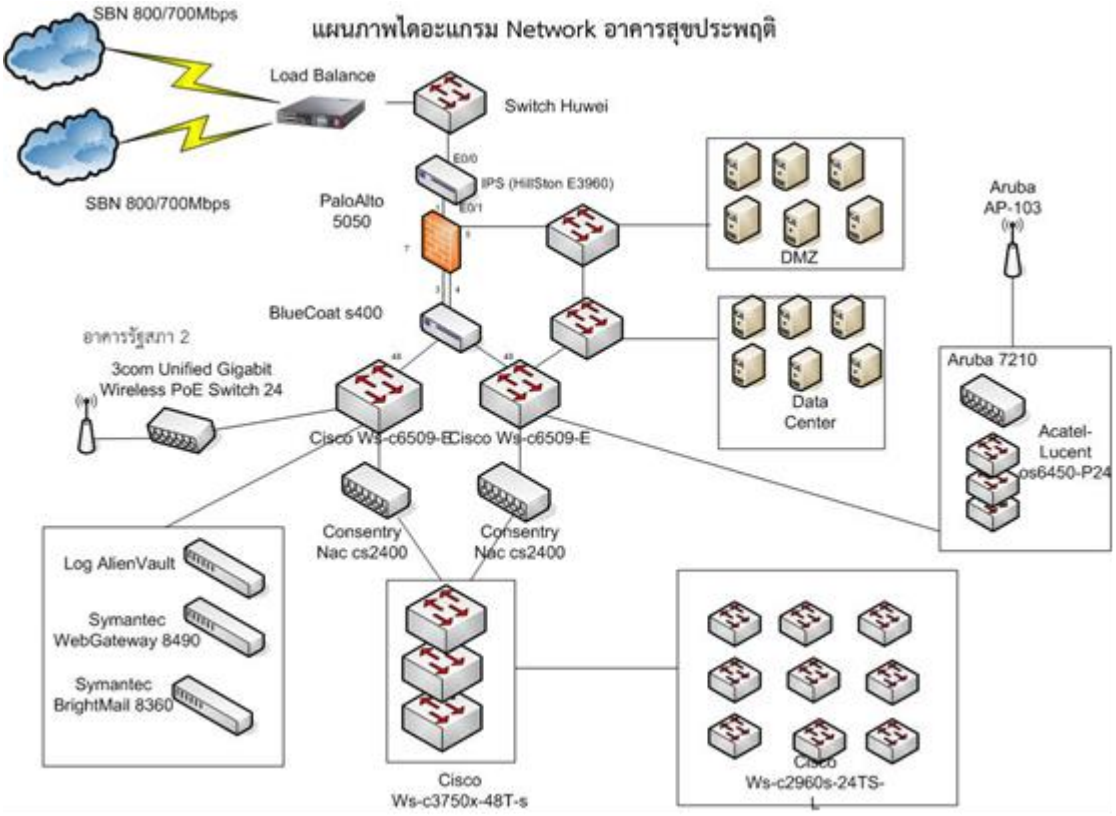
ทั้งนี้ การดูแลระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศได้ใช้ตำแหน่งนักวิชาการคอมพิวเตอร์ จำนวน 11 คน เป็นผู้ดูแล

4.8.2 สำนักงานเลขาธิการวุฒิสภามี ฮาร์ดแวร์ ซอฟต์แวร์ ด้านความปลอดภัย ดังนี้

ตารางที่ 4 ฮาร์ดแวร์ ซอฟต์แวร์ ด้านความปลอดภัยของสำนักงานเลขาธิการวุฒิสภา

ลำดับ	รายการอุปกรณ์	ยี่ห้อ/รุ่น	สถานที่ติดตั้ง	จำนวน (ชุด)	ปีที่จัดหา
1	Firewall ชนิด NGFW	PaloAlto 5050	อาคารสุขประพฤติ	1	2557
2	Firewall ชนิด NGFW	PaloAlto 5020	อาคารสุขประพฤติ	1	2557
3	Firewall	Cisco ASA 5080	อาคารสุขประพฤติ	1	2552
4	IPS	Cisco ASA 5585–X IPS sSP–20	อาคารสุขประพฤติ	1	2554
5	IPS	Hilstone SG–6000	อาคารสุขประพฤติ	1	2559
6	ระบบบริหารจัดการ Bandwidth	BlueCoat S400	อาคารสุขประพฤติ	1	2556
7	ระบบบริหารจัดการ Bandwidth	Packerteer PacketShaper 7500	อาคารสุขประพฤติ	1	2550
8	Web Gateway	Symantec Web Gateway 8450	อาคารสุขประพฤติ	1	2553
9	Mail Gateway	Symantec Messaging Gateway 8360	อาคารสุขประพฤติ	1	2553
10	Antivirus Server (Management)	Symantec Endpoint Protection	อาคารสุขประพฤติ	1	2554
11	Antivirus Server (Update Signature)	Symantec Endpoint Protection	อาคารสุขประพฤติ	1	2554
12	Log Management	AlientVault 5.2.2	อาคารสุขประพฤติ	1	2559
14	Radius	Cisco insigst nat	อาคารสุขประพฤติ	1	2553
15	ระบบยืนยันตัวบุคคล	Concentry cs 2400	อาคารสุขประพฤติ	2	2553
16	ระบบยืนยันตัวบุคคล	Concentry cs 2400	อาคารสุขประพฤติ	1	2553
16	ระบบยืนยันตัวบุคคล	Concentry cs 2400	อาคารสุขประพฤติ	1	2553
18	Ldap	Openldap	อาคารสุขประพฤติ	1	2550

แผนผัง network สำนักงานเลขาธิการวุฒิสภา อาคารสุขประพฤติ แสดงได้ดังภาพที่ 2



ภาพที่ 2 ไดอะแกรม network สำนักงานเลขาธิการวุฒิสภา

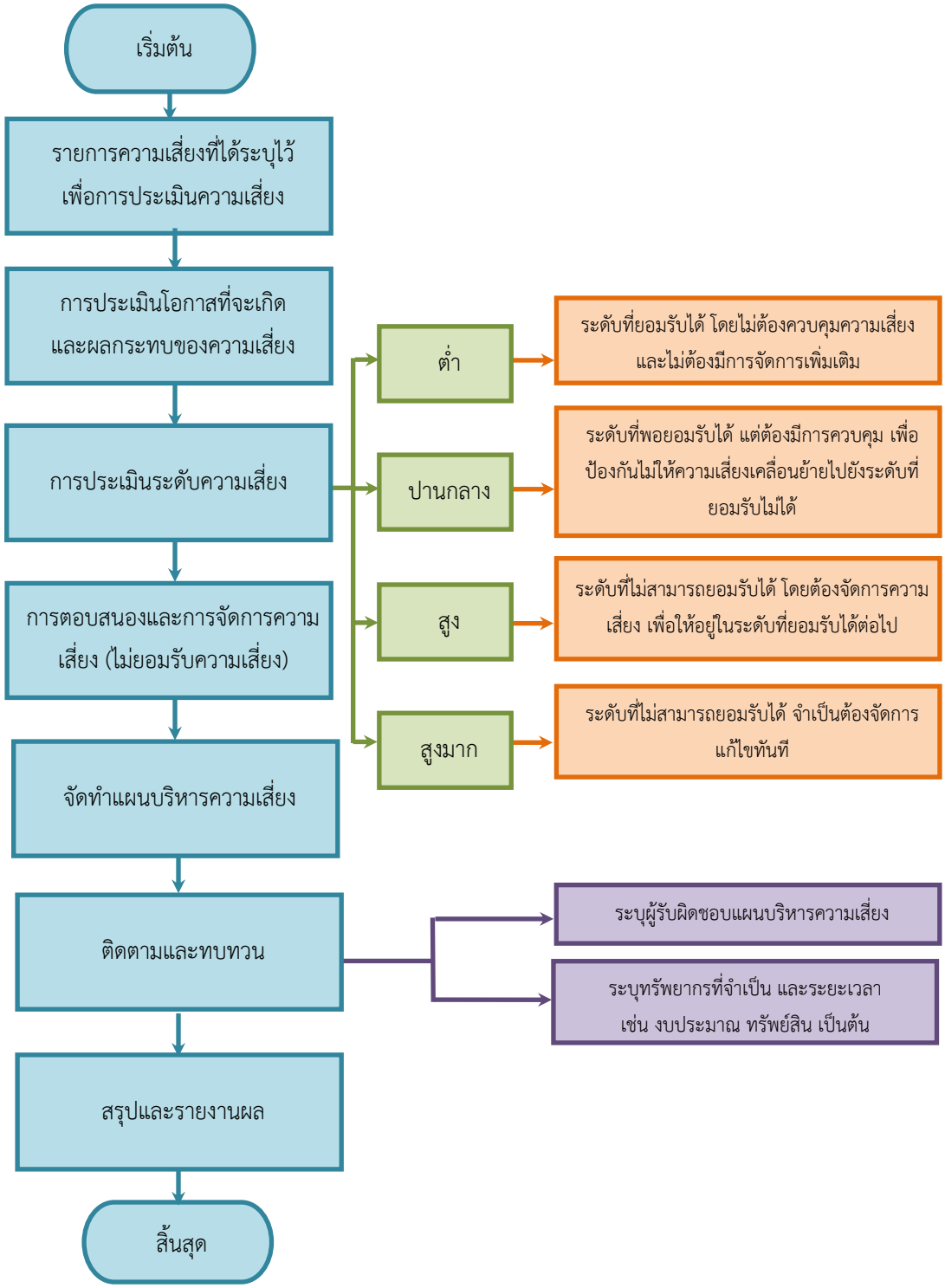
ในด้านบุคคลากรด้านความมั่นคงปลอดภัยด้านสารสนเทศสำนักงานเลขาธิการวุฒิสภา ได้มอบหมายให้กลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นกลุ่มงานที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ให้ดูแลความมั่นคงปลอดภัยสารสนเทศด้วย ซึ่งทางกลุ่มงานมีบุคลากรในการดูแลระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ดังนี้

ตำแหน่ง	จำนวน/คน
ผู้บังคับบัญชากลุ่มงาน	1
นักวิชาการคอมพิวเตอร์	5
เจ้าพนักงานธุรการ	1

ทั้งนี้ การดูแลระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศได้ใช้ตำแหน่งนักวิชาการคอมพิวเตอร์ จำนวน 5 คน เป็นผู้ดูแล

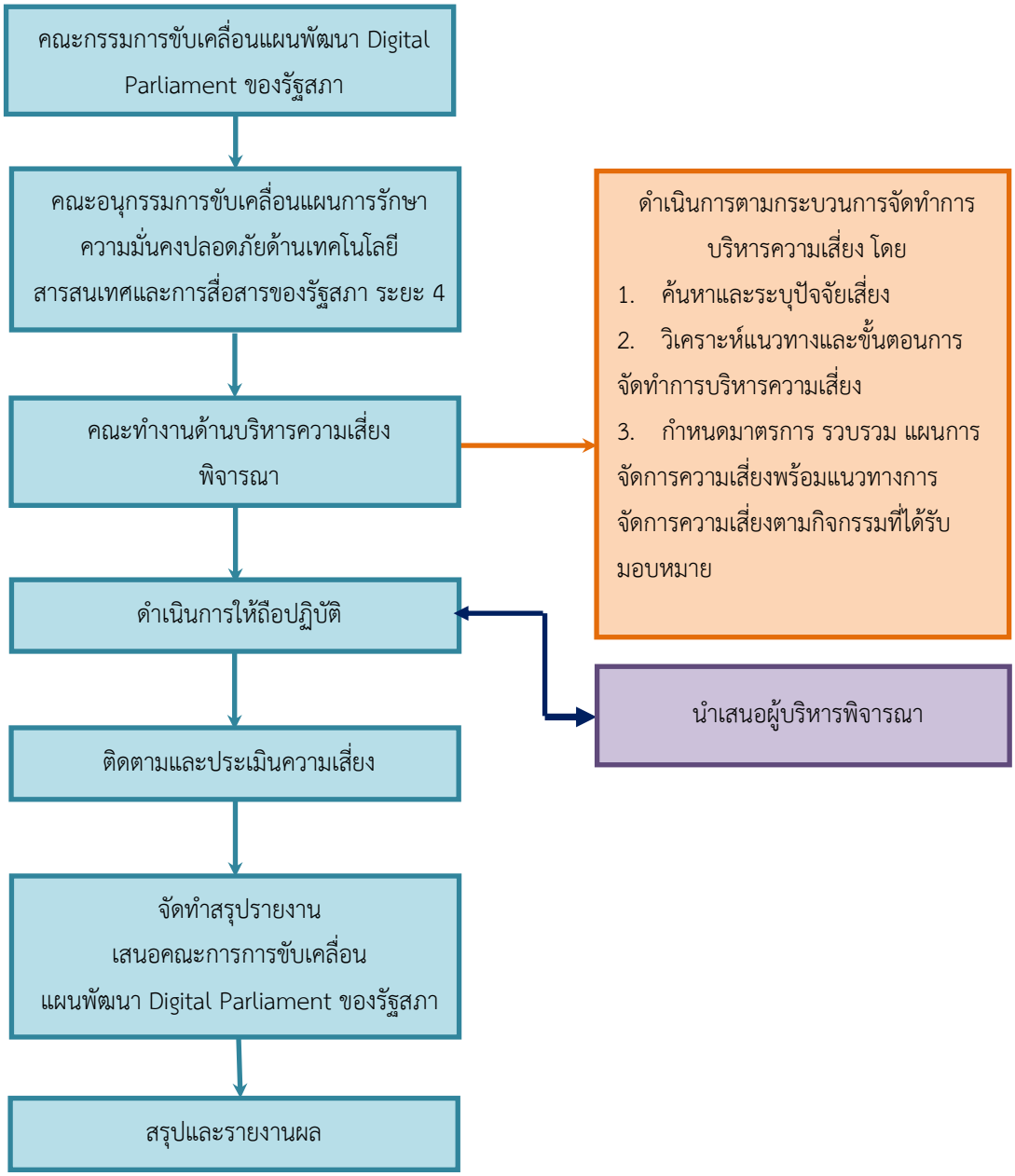
5. การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของรัฐสภา

5.1 ขั้นตอนบริหารความเสี่ยง



ภาพที่ 3 ขั้นตอนการประเมินความเสี่ยง

5.2 กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



ภาพที่ 4 กระบวนการจัดทำการบริหารความเสี่ยง

5.3 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของรัฐสภา

เป็นขั้นตอนการนำผลการประเมินความเสี่ยงที่ประมวลจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) เข้าด้วยกัน (ระดับความเสี่ยง = ระดับโอกาส x ระดับผลกระทบ) แล้วจัดทำแผนผังระดับความเสี่ยง (Risk Matrix) โดยสามารถจัดแบ่งความเสี่ยงออกเป็นเป็น 4 ระดับ คือ ความเสี่ยงสูงมาก ความเสี่ยงสูง ความเสี่ยงปานกลาง และความเสี่ยงต่ำ ซึ่งช่วยในการตัดสินใจในการวางแผนความเสี่ยงได้อย่างเหมาะสม และสามารถจัดลำดับความสำคัญในการจัดการได้ ซึ่งการประเมินความเสี่ยงด้วยแผนผังระดับความเสี่ยง (Risk Matrix) แสดงตามภาพที่ 5

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 5 แผนผังการประเมินความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization)

เกณฑ์ในการประเมินความเสี่ยง เป็นการพิจารณาระดับความเสี่ยงที่ประมวลได้ตามภาพที่ 5 จัดแบ่งเป็นเกณฑ์ในการยอมรับความเสี่ยงเป็น 4 ระดับ ดังนี้

ตารางที่ 5 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 6 ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศของรัฐสภา

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
1	ความเสี่ยงจากการใช้ซอร์ฟแวร์ที่ไม่มีลิขสิทธิ์	5	5	25
2	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	5	3	15
3	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	5	3	15
4	ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายใน	5	3	15
5	ความเสี่ยงจากการถูก Black List โดย Search Engine หรือ spamhaus	5	3	15
6	ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	3	4	12
7	ความเสี่ยงจากอัคคีภัย	2	5	10
8	ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	2	5	10
9	ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	2	4	8
10	ความเสี่ยงจากการเกิดอุทุกภัย	2	3	6
11	ความเสี่ยงจากแมลง หรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์หรือ สายไฟฟ้า /สายสัญญาณ	3	2	6
12	ความเสี่ยงจากการโจรกรรม อุปกรณ์ คอมพิวเตอร์แม่ข่ายหรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	3	2	6

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
13	ความเสี่ยงจากการไม่ทำการสำรองข้อมูลหรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	3	2	6
14	ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายนอก	2	3	6
15	ความเสี่ยงจากการโจมตีทางไซเบอร์สำนักงานฯ ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)	2	3	6
16	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย	2	3	6
17	ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต	1	5	5
18	ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1	5	5
19	ความเสี่ยงจากวินาศภัย/การก่อการร้าย	1	5	5
20	ความเสี่ยงจาก ความชื้น อุณหภูมิ	1	5	5
21	ความเสี่ยงจากแผ่นดินไหว	3	5	15
22	ความเสี่ยงจากการโจรกรรมฐานข้อมูล	2	2	4

5.4 ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

ได้มีการประเมินความเสี่ยงตามหลัก COSO ดังนี้

ตารางที่ 7 ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของรัฐสภา

ความเสี่ยงสูง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
1. ความเสี่ยงจากการใช้ซอร์ฟแวร์ที่ไม่มีลิขสิทธิ์	1. เสี่ยงต่อการสูญหายของข้อมูล 2. เสี่ยงต่อการถูกฟ้องร้องและเสื่อมเสียชื่อเสียงและความน่าเชื่อถือของสำนักงานฯ	1. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอร์ฟแวร์นั้นๆ 2. สำนักงานฯ อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ 3. ความไม่สะดวกหากไปใช้งานด้วยซอร์ฟแวร์ ที่ไม่จำเป็นต้องมีลิขสิทธิ์ (Open Source)	5	5	สูงมาก 5x5=25	1. การจัดหาซอร์ฟแวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2. ทำสัญญา หรือข้อตกลง/สนับสนุนการใช้โปรแกรม SaaS เช่น www.docs.com แทน Microsoft Office 3. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอร์ฟแวร์ที่ถูกกฎหมาย	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)
2.ความเสี่ยงจาก การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	1.ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านเครือข่าย	1.ขัดขวางการทำงานของเจ้าหน้าที่และผู้บริหารสำนักงานฯ 2. บุคคลภายนอกไม่สามารถเข้าใช้ Web	5	3	สูง 5x3=15	1. ตรวจสอบ Availability ของ Server ด้วยโปรแกรม ตรวจสอบ เช่น Montastic จาก http://www.montatic.com เป็นต้น	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication

ความเสี่ยงสูง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
	2.ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่าย	Server หรือค้นหาข้อมูลที่ต้องการ				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 ที่อาคารสุขประพฤติ หรือ ISP 4. การจัดตั้งศูนย์สำรอง (Backup Site) 5. การปรับปรุงเครือข่ายหลักภายใน (Backbone Networks) อุปกรณ์ป้องกันการโจมตี เช่น Firewall,IPS/IDS ,NAC,Router	Risk)

ความเสี่ยงสูง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
						และ Switch ต่างๆใหม่ ให้เป็นแบบ Redundancy 6. การจัดหา Bandwidth Management เพื่อควบคุมการใช้งานเครือข่ายให้มีประสิทธิภาพ เพื่อให้การใช้งานระบบงานของสำนักงานฯ ได้รับ Bandwidth สูงกว่าการใช้งานด้านอื่นๆ	
3. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	1.เสี่ยงต่อการถูกทำลายโปรแกรมหรือข้อมูล 2. เสี่ยงต่อการไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3. เสี่ยงต่อการถูกขโมยข้อมูลที่สำคัญ	1.ใช้คอมพิวเตอร์ไม่ได้ 2. ใช้ระบบงานไม่ได้ 3. ข้อมูลที่สำคัญสูญหาย	5	3	สูง 5x3=15	1. ใช้ระบบป้องกันไวรัสกับเครื่องแม่ข่ายที่ต้องเสียค่าใช้จ่าย เช่น Symantec Endpoint Protection ที่สำนักงานฯ ใช้อยู่ที่สามารถควบคุมการโจมตีและการบุกรุกเครือข่ายจากสาเหตุต่างๆ เช่น การระบาดของ Virus และ Worm,การโจมตีเพื่อห้ามการบริการ (Denial of Server-DoS) การบุกรุกแบบ Vulnerabilty Exploit,Network Reconnaissance และเทคนิคการ	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

ความเสี่ยงสูง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
						หลบซ่อนการโจมตีแบบ Traffic Normalization , IP Defragmentation,TCP Reassemble ได้ 2. อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ 3. มีการสำรองข้อมูลที่เครื่องลูกข่ายที่จำเป็นไว้อย่างสม่ำเสมอทาง External Hard Disk หรือ DVD	
4. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1. เสี่ยงต่อการถูกขโมยข้อมูล 2. เสี่ยงต่อการทำความเสียหายแก่โปรแกรม 3.เสี่ยงต่อการใช้ช่องโหว่โปรแกรมหรือการซ่อน Scriptไว้ในโปรแกรมเพื่อวัตถุประสงค์แอบแฝง	1. ลดความน่าเชื่อถือต่อสำนักงานฯ หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ 2. กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานฯ เป็นอย่างยิ่ง	5	3	สูง 5X3=15	1. ตั้งมาตรฐานในการพัฒนาซอร์ฟแวร์ตามคำแนะนำของ OWASP-Top 10 Web Application Security Risks เพื่อลดความเสี่ยง 2. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

ความเสี่ยงสูง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
5. 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 อาจถูกฟ้องร้อง โดยมีส่วนได้ส่วนเสีย	5	3	สูง 5X3=15	1. ติดตั้งโปรแกรม เพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ตโดยเฉพาะจาก SMTP Mail Server ซึ่งมักจะเป็นแหล่งที่ Hacker ชอบใช้ในการส่ง Spam ปัจจุบันสำนักงานฯ ได้ทำการติดตั้ง Symantec Brightmail Gateway เพื่อป้องกันแล้ว แต่ต้องมีตารางในการตรวจสอบที่เข้มงวด 2. ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server หรือ FTP เช่น Symantec Web Gateway ,Symantec Endpoint Protection ที่สำนักงานฯใช้อยู่เป็นต้น 3. มีการอัพเดทตัวโปรแกรมและ Signature อย่างสม่ำเสมอและการทำการบำรุงรักษา (Maintenance)	ความเสี่ยงด้านบุคลากร (Human Risk) และความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

ความเสี่ยงสูง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
						ทั้งฮาร์ดแวร์และซอร์ฟแวร์ พร้อมทั้ง Update Licenses	
6. ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	1. เสี่ยงต่อการถูกขโมยข้อมูล 2. เสี่ยงต่อการทำความเสียหายแก่โปรแกรม 3. ไม่สามารถแก้ไขข้อบกพร่องได้เอง 4. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว	1. ลดความน่าเชื่อถือต่อสำนักงานฯ หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ 2. กรณีเป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานฯ เป็นอย่างยิ่ง 3. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูล พร้อมกับการทำการบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการอัพเดทอยู่เสมอ	3	4	สูง 3x4=12	1. ออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) level 2 2. การออกแบบโดยการอ้างอิงด้วยแผนผังแสดงความสัมพันธ์ระหว่างกลุ่มข้อมูล (Entity)-ER Diagram 3. ให้มีการส่งมอบ Source Code ในรูปแบบ DVD ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้ 4. หากมีการพัฒนา Library ด้วยตนเองต้องส่ง Source Code Library ที่สามารถแก้ไขได้ 5. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

ความเสี่ยงสูง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
						6. มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม 7. มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึง การแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดทเมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น	
7 .ความเสี่ยงจากการเกิดอัคคีภัย	1. การถูกทำลายทรัพย์สิน ระบบคอมพิวเตอร์และเครือข่าย 2. การถูกทำลายข้อมูล 3. การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร	1.เสียงบประมาณในการจัดหาระบบทดแทน 2. การไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน	2	5	สูง 2X5 =10	1.ติดตั้งระบบตรวจจับควันที่สามารถตรวจจับควันได้ก่อนล่วงหน้า (Very Early Smoke Detection Apparatus – VESDA) 2. ติดตั้งระบบดับเพลิงแบบ Aerosol ซึ่งปัจจุบันสำนักงานฯ ได้ติดตั้งระบบนี้ใช้งานอยู่ในศูนย์สารสนเทศทั้ง 3 ระบบข้างต้นแล้ว	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

ความเสี่ยงสูง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
						4. จัดตั้งศูนย์สำรองในกรณีที่เกิดอัคคีภัยขึ้น 5. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	
8.ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้งาน	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรือ ม้วยเทป (Cartridge Tape) แผ่น DVD/CD	1. ข้อมูลที่อยู่ในชั้นความลับ รั่วไหลทำให้เสียหายต่อความน่าเชื่อถือของสำนักงานฯ 2. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	2	5	สูง 2X5=10	มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk ม้วนเทป (Cartridge Tape) แผ่น DVD/CD ให้แน็ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้วหากทำได้	ความเสี่ยงด้านระบบข้อมูล (Database Risk)

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
1. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	1. ไม่สามารถใช้งานเครื่องแม่ข่ายและเครือข่ายได้ 2. ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่ายทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ shutdown อย่างเหมาะสม	1.ข้อมูลเสียหาย 2.ระบบปฏิบัติการ โปรแกรม หรือฐานข้อมูล เสียหาย ต้องมีการติดตั้งใหม่ 3.เสียเวลาการใช้งาน 3 ถึง 6 ชั่วโมงเป็นอย่างน้อย	2	4	ปานกลาง 2X4=8	1. ติดตั้งระบบ UPS ที่สามารถสำรองไฟฟ้าเพียงพอสำหรับเครื่องแม่ข่ายและสามารถทำการ shutdown เครื่องแม่ข่ายทั้งหมดกรณีไฟฟ้าดับเกินกว่าที่ UPS จะสามารถจ่ายไฟได้ 2. วางแผนจัดการยุบรวมเครื่องแม่ข่ายต่างๆ ที่กระจัดกระจายเป็นจำนวนมากและมีหลายระบบปฏิบัติการให้เป็นในที่มีระบบสำรอง (Redundancy) โดยใช้เทคโนโลยี Virtualization มาบริหารจัดการ 3. วางแผนการจัดหาและติดตั้งเครื่องกำเนิดไฟฟ้า (Electrical Generator) สำหรับศูนย์สารสนเทศอาคารรัฐสภาแห่งใหม่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)
2. ความเสี่ยงจากการเกิดอุทกภัย	ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	เสียงบประมาณในการซ่อมแซมหรือจัดหาใหม่ทดแทน	2	3	ปานกลาง 2X3=6	1. ติดตั้งเครื่องตรวจจับระดับน้ำรั่วไหลพื้นที่ที่มีความไวต่อน้ำ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
						2. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	(Physical and Environment Risk)
3.ความเสี่ยงจากแมลง หรือสัตว์กัดแทะคอมพิวเตอร์อุปกรณ์หรือสายไฟฟ้า/สายสัญญาณ	เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน	3	2	ปานกลาง 3X2=6	1. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ RACK 2. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)
4.ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายหรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง							
4.1 เครื่องคอมพิวเตอร์แม่ข่าย	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	1. เสียงบประมาณในการจัดหาเครื่องคอมพิวเตอร์แม่ข่ายทดแทนที่มีมูลค่าสูง 2. เสียเวลาในการกู้ระบบ	2	3	ปานกลาง 2X3=6	1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุม การเข้า-ออก ห้องคอมพิวเตอร์แม่ข่าย 2. ตู้ RACK ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์จัดเก็บข้อมูล (Disk Array) และ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
		3. เสียภาพลักษณ์ของสำนักงานฯ				อุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจตลอดเวลา 3. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน การนำติดตัวไปด้วยตลอดเวลา หรือติดตั้งอุปกรณ์ล็อค เช่น Kensington Lock เป็นต้น เพื่อป้องกันการสูญหาย	
4.2 เครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	1.เสียงบประมาณในการจัดหาอุปกรณ์ทดแทน 2. เสียภาพลักษณ์ของสำนักงานฯ	2	3	ปานกลาง 2X3=6	1. ควบคุมการเข้าออกอาคาร 2. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-ออกอาคารตลอดเวลา 3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมที่ๆ มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)
5. ความเสี่ยงจากการไม่ทำการสำรองข้อมูลหรือ	1.เสี่ยงต่อการสูญหายข้อมูลในขั้นเล็กน้อยหรือมากจนไม่	1. เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือ การจัดทำขึ้นมาใหม่	2	3	ปานกลาง 2X3=6	1.มีการบริหารจัดการในการทำสำรองข้อมูล (Backup) เป็นประจำอยู่เสมอ	ความเสี่ยงด้านระบบข้อมูล (Database Risk)

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
ทำการสำรองข้อมูลแต่ขาดการอัพเดท	สามารถดำเนินงานได้ตามปกติ 2. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	2. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้เนื่องจากขาดความมั่นใจในข้อมูล				2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ(Restore) เพื่อความแน่ใจในข้อมูลที่เก็บไว้ ปัจจุบัน การจัดเก็บสำรองข้อมูลของสำนักงานฯ ที่มีอุปกรณ์และระบบบริหารจัดการสำรองข้อมูลโดยอัตโนมัติ มีเฉพาะระบบเครื่องในโครงการเพิ่มประสิทธิภาพการบริหารราชการของสำนักงานเลขาธิการวุฒิสภา ระยะที่ 1 และโครงการจัดตั้งห้องสมุดอิเล็กทรอนิกส์ 3. การจัดการเชื่อมโยงเครื่องแม่ข่ายอื่นเข้าสู่ระบบการสำรองข้อมูลโดยอัตโนมัติ	
6. ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายนอก	เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	1. ทำให้เครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆทั้งหมดในเครือข่าย	1	5	ปานกลาง 1X5=5	1. ติดตั้งระบบป้องกันและเตือนภัย Anti Spam ,Antivirus , Malware,Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้นๆ อยู่เป็น	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
		2. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูลหรือรูปภาพบน Web Site ของสำนักงานฯ 3. ถูกโจรกรรมข้อมูลที่เป็นความลับของสำนักงานฯ				ประจำเพื่อที่จะสามารถแก้ไขได้ทันเมื่อถูกโจมตี 2. หมั่นตรวจสอบ Policy และ Log ของ Firewall IPS/IDS อย่างสม่ำเสมอ 3. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับสถานการณ์ได้โดยไม่สับสน 4. ติดตั้ง Firewall และ IDS/IPS เพื่อป้องกันฐานข้อมูลที่มีความสำคัญโดยเฉพาะ	
7. ความเสี่ยงจากการโจมตีทางไซเบอร์สำนักงานฯ ไม่ให้สามารถให้บริการได้ (Denial of Service- DoS)							

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
7.1 จากภายนอก	เสี่ยงต่อการถูกโจมรีได้จากภายนอก โดยโจมตีทั้งเครื่องแม่ข่ายและ / หรือเครือข่ายภายในทุกรูปแบบ ซึ่งจะมีการพัฒนาวิธีการอยู่ตลอดเวลา	ไม่สามารถใช้งานเครือข่ายได้หรือใช้ได้แต่ช้ามาก	1	5	ปานกลาง 1X5=5	1. ติดตั้งระบบป้องกันและเตือน ภัย Spam,Virus,Malware,Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้นๆ อยู่เป็นประจำ เพื่อลดหรือสามารถแก้ไขได้ทันเมื่อถูกโจมตี 2.หมั่นตรวจสอบ Policy และ Log ของ Firewall และ IPS/IDS อย่างสม่ำเสมอ 3.จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับสถานการณ์ใดโดยไม่สับสน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)
7.2 จากภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดย	ไม่สามารถใช้งานเครือข่ายได้ หรือใช้ได้แต่ช้ามาก	1	5	ปานกลาง 1X5=5	มีมาตรการและกฎระเบียบในการควบคุมมิให้มีการติดตั้ง โปรแกรมต่างๆ ลงบนเครื่องลูกข่ายอินทราเน็ตของสำนักงาน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
	ผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ						
8.ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย	1. เสี่ยงต่อการไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ 2. เสี่ยงต่อความเสียหายต่อความเสียหายของข้อมูลหบ	การใช้งานระบบไม่สามารถใช้งานตามปก	1	5	ปานกลาง 1x5=5	1.การป้องกันระบบเครื่องแม่ข่ายฐานข้อมูลหลักเสียหายด้วยการเพิ่มประสิทธิภาพ การทำงานในแบบ Hot Standby หรือ Clustering ทุกส่วนของเครื่องแม่ข่ายฐานข้อมูลหลัก 2. การจัดเก็บฐานข้อมูลสำรอง (Backup) และที่พร้อมใช้งานได้โดยอาจประสานงานกับบริษัทผู้ให้บริการในลักษณะ Application Service Provider หรือหน่วยงานอื่น ในความตกลงที่จะใช้เครื่องของหน่วยงานอื่น เพื่อใช้งานทดแทนในกรณีที่เกิดความเสียหายต่อเครื่องแม่ข่ายฐานข้อมูลหลักของสำนักงานฯ 3. การจัดตั้งศูนย์สำรองข้อมูล (Backup Site)	ความเสี่ยงด้านระบบข้อมูล (Database Risk)

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
9.ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	เสี่ยงต่อผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลเข้าใช้เครือข่ายอินทราเน็ตผ่านทาง WiFi	ข้อมูลที่เป็นความลับถูกนำออกเผยแพร่หรือนำไปใช้ประโยชน์ อันจะนำมาซึ่งการขาดความน่าเชื่อถือในการจัดเก็บข้อมูลของสำนักงานฯ			ปานกลาง 3X5=5	1.ควบคุมการเข้าใช้เครือข่ายด้วย NAC ,Radius และ Directory เช่น AD หรือ LDAP ร่วมกันในการควบคุมการเข้าใช้งานเครือข่าย ซึ่งในปัจจุบันสำนักงานฯ ได้เริ่มมีการนำระบบดังกล่าวเข้ามาติดตั้งใช้งานอยู่ 2. เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดยติดตั้งระบบยืนยันตน (Authentication)	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)
10. ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1. เสี่ยงต่อการใช้ Resource ของสำนักงานฯ ในทางที่ผิด หรือ เปล่าประโยชน์ เช่น การฟังวิทยุหรือดูโทรทัศน์ออนไลน์ การโหลด Bit Torrent การดูเว็บไซต์ที่ลามก	1.สูญเสีย Bandwidth ในเครือข่ายทำให้สำนักงานฯ ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี 2. สำนักงานฯ อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	2	2	ปานกลาง 2X2=4	1. บริหารจัดการด้วยข้อแนะนำ Ten Ways to Protect Your Network From Insier Threats (www.enterprisenetworkingplAnet.com) เพื่อลดความเสี่ยง 2. บริหารจัดการในการกำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น 3. บริหารจัดการในการกำหนด Policy ของอุปกรณ์ Bandwidth	ความเสี่ยงด้านบุคลากร (Human Risk)

ความเสี่ยงปานกลาง							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
	อนาจาร ผิดศีลธรรม เป็นต้น 2.การใช้ Resource ของสำนักงานฯ ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม หรือ เพลงที่ไม่มีลิขสิทธิ์ เป็นต้น					Management เพื่อกำจัดหรือปิดกั้นการใช้ resources ในทางที่ผิด 4.การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์หรือ Resources ต่างๆ ของสำนักงานฯ ไปใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา	

ความเสี่ยงต่ำ							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
1. ความเสี่ยงจากวินาศภัย/การก่อการร้าย	เสี่ยงต่อการสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	1	3	ต่ำ 1X3=3	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน 2. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไร และจะใช้เครื่องทดแทนจากที่ใด เพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง 3. จัดทำศูนย์สำรอง (Backup Site)	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)
2. ความเสี่ยงจากความชื้น อุณหภูมิ	เครื่องมีประสิทธิภาพ (Performance) และความเชื่อถือได้ (Stability) ลดลง และเครื่องอาจหยุดทำงานได้	อายุของเครื่องและอุปกรณ์สั้นลง ทำให้สิ้นเปลืองงบประมาณในการจัดการซ่อมแซมหรือจัดหาทดแทน	2	1	ต่ำ 2X1=2	1. บำรุงรักษาระบบปรับอากาศชนิด Precision ที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้ ซึ่งปัจจุบันสำนักงานฯ ได้ติดตั้งระบบนี้ ที่ศูนย์สารสนเทศ ชั้น 13 อาคารสุขประพฤติแล้ว 2. สำนักงานฯ ควรมีการวางแผนในการจัดทำระบบที่เหมาะสมสำหรับศูนย์สารสนเทศอาคารรัฐสภาแห่งใหม่ด้วย โดยประสานงานกับผู้ออกแบบ และสอดคล้องกับ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

ความเสี่ยงต่ำ							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
						นโยบายของสำนักงานฯ เพื่อลดความเสี่ยงด้านการบริหารจัดการและความเสี่ยงด้านการเงิน เนื่องจากต้องใช้งบประมาณสูงและอาจมีข้อจำกัดหลายๆ ด้าน	
3. ความเสี่ยงจากแผ่นดินไหว	ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	1	1	ต่ำ 1X1=1	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน 2. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไรและจะใช้เครื่องทดแทนจากที่ใด เพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง 3. จัดทำศูนย์สำรอง (Backup Site)	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)
4. ความเสี่ยงจากการโจรกรรมฐานข้อมูล	ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ	1. เสียชื่อเสียงและความน่าเชื่อถือที่มีต่อสำนักงานฯ 2. การสูญหายหรือถูกทำลายข้อมูล	1	1	ต่ำ 1X1=1	1.มีการบริหารจัดการด้านการป้องกันข้อมูล 2. มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) ตามความสำคัญของข้อมูลโดยสามารถทำงานร่วมกับ Network Access Control (NAC) Radius, Active Directory (AD) หรือ Lightweight Directory	ความเสี่ยงด้านระบบข้อมูล (Database Risk)

ความเสี่ยงต่ำ							
ความเสี่ยง	**ปัจจัยเสี่ยง**	**ผลกระทบ**	**โอกาสเกิด (Likelihood)**	**ระดับผลกระทบสูงสุด**	**ระดับความเสี่ยง**	**มาตรการ/แผนปฏิบัติการ**	**ประเภทความเสี่ยง**
						Access Protocol (LDAP) Server และ Syslog ได้ 3.มีการบริหารสื่อจัดเก็บข้อมูล เช่น Hard Disk ม้วนเทป (Cartridge Tape) แผ่น DVD/CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์หรือสื่อเก็บข้อมูลนั้นๆ ทิ้งแล้วหากทำได้	

6. สรุปผลและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแลตรวจสอบ และควบคุมความเสี่ยงกับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อน การดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงานภายในรัฐสภา ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือการจัดการความเสี่ยงในองค์กร นั่นเอง

6.1. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่ผลคะแนนสูงสุด ดังนี้

6.1.1 ความเสี่ยงจากการใช้ซอร์ฟแวร์ที่ไม่มีลิขสิทธิ์ มีแนวทางปฏิบัติดังนี้

1) การจัดหาซอร์ฟแวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น

2) ทำสัญญา หรือ ข้อตกลง/สนับสนุนการใช้โปรแกรม Saas แทน Microsoft Office

3) รณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอร์ฟแวร์ที่ถูกกฎหมาย

6.1.2 ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง มีแนวทางปฏิบัติดังนี้

1) ตรวจสอบ Availability ของ Server ด้วยโปรแกรมตรวจสอบ เช่น Montastic จาก http://www.montatic.com

2) การจัดทำเส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า 1 เส้นทาง

3) การวาง Web Server ไว้มากกว่า 1 ที่ เช่น ที่ให้บผู้บริการอินเทอร์เน็ต (ISP)

4) การจัดตั้งศูนย์สำรอง (Backup Site)

5) การปรับปรุงเครือข่ายหลักภายใน (Backbone Networks)

6) การจัดหา Bandwidth Management

6.1.3 ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware มีแนวทางปฏิบัติดังนี้

1) ใช้ระบบป้องกันไวรัสกับเครื่องแม่ข่ายที่ต้องเสียค่าใช้จ่าย

2) อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ

3) มีการสำรองข้อมูลที่เครื่องลูกข่ายที่จำเป็นไว้อย่างสม่ำเสมอทาง External Hard Disk

6.1.4 ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร มีแนวทางปฏิบัติดังนี้

1) ตั้งมาตรฐานในการพัฒนาซอร์ฟแวร์ตามคำแนะนำของ OWASP–Top 10

2) มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ

6.1.5 ความเสี่ยงจากการถูก Black List โดย Search Engine หรือ spamhaus มีแนวทางปฏิบัติดังนี้

1) ติดตั้งโปรแกรมเพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ต

2) ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server

6.1.6 ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง มีแนวทางปฏิบัติดังนี้

1) การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) level2

2) การออกแบบโดยการอ้างอิงด้วยแผนผัง ER Diagram

3) ให้มีการส่งมอบ Source Code ในรูปแบบ DVD

4) หากมีการพัฒนา Library ด้วยตนเองต้องส่ง Source Code Library ที่สามารถแก้ไขได้

5) มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่

6) มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม

7) มีแผนการบำรุงรักษาระบบงาน

6.1.7 ความเสี่ยงจากอัคคีภัย มีแนวทางปฏิบัติดังนี้

1) ติดตั้งระบบตรวจจับควันที่สามารถตรวจจับควันได้ก่อนล่วงหน้า (Very Early Smoke Detection Appatus–VESDA)

2) ติดตั้งระบบดับเพลิงแบบ Aerosol

3) จัดตั้งศูนย์สำรองในกรณีที่เกิดอัคคีภัยขึ้น

4) มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ

6.1.8 ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้ มีแนวทางปฏิบัติดังนี้ มีการบริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk ม้วนเทป

6.2 สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

6.2.1 เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

6.2.2 เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

6.2.3 ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

6.3 ข้อเสนอแนะ

6.3.1 การควบคุมนโยบายและการบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

1) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

2) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

3) กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

6.3.2 การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ

ภาคผนวก

คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย

ด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ 4 ปี (พ.ศ. 2562-2565)

คำสั่งคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา
ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕)
ที่ ๒ /๒๕๖๑
เรื่อง แต่งตั้งคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕)

ตามที่ ได้มีคำสั่งสภานิติบัญญัติแห่งชาติ ที่ ๑๘๓/๒๕๖๐ ลงวันที่ ๑๒ ธันวาคม ๒๕๖๐ เรื่อง แต่งตั้งคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕) และคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ได้มีคำสั่งที่ ๓/๒๕๖๐ ลงวันที่ ๑๘ ธันวาคม ๒๕๖๐ เรื่อง แต่งตั้งคณะอนุกรรมการจัดทำแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕) โดยคณะอนุกรรมการฯ ได้จัดทำแผนการรักษาความมั่นคงปลอดภัยฯ ตามอำนาจหน้าที่กำหนดไว้เสร็จสิ้นเรียบร้อยแล้ว นั้น

เพื่อให้การขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕) ดำเนินการต่อไปอย่างมีประสิทธิภาพ จึงเห็นสมควรแต่งตั้งคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕) ประกอบด้วย

๑. นายวีรชาติ มัตติทานนท์	ที่ปรึกษาและอนุกรรมการ
๒. ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา	ประธานอนุกรรมการ
๓. ผู้อำนวยการสำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร	รองประธานอนุกรรมการ
๔. ผู้บังคับบัญชากลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์ สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร	อนุกรรมการ
๕. ผู้บังคับบัญชากลุ่มงานบริการระบบคอมพิวเตอร์ สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร	อนุกรรมการ
๖. ผู้บังคับบัญชากลุ่มงานวิทยาการคอมพิวเตอร์ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา	อนุกรรมการ
๗. นายสุธี ยืนแน่นอน สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร	อนุกรรมการ

๘. นางณัชชา ศรเพลิง สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร	อนุกรรมการ
๙. นางสมคิด แช่ว่อง สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร	อนุกรรมการ
๑๐. นายประจักษ์ เพ็ญเลี้ยง สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา	อนุกรรมการ
๑๑. นายทวีศักดิ์ น้อยภาษี สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา	อนุกรรมการ
๑๒. นางสาวพัทธกานต์ วุฒิอัครวัฒน์ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา	อนุกรรมการ
๑๓. นายสมหวัง เรืองพรชัย สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา	อนุกรรมการและเลขานุการ
๑๔. นายสุวิทย์ น้อยอยู่ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา	อนุกรรมการและผู้ช่วยเลขานุการ
๑๕. นายชัยวัฒน์ ปันต่า สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร	อนุกรรมการและผู้ช่วยเลขานุการ
๑๖. นายธนาเทพ มัฆนาโส สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร	อนุกรรมการและผู้ช่วยเลขานุการ

ให้คณะอนุกรรมการ มีอำนาจหน้าที่ ดังต่อไปนี้

๑. กำกับ ดูแล และขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒ - ๒๕๖๕) ให้เป็นไปตามเป้าหมายของแผนการรักษาความมั่นคงปลอดภัยฯ ที่กำหนดไว้แต่ละปีงบประมาณ

๒. กำหนดระเบียบ ข้อปฏิบัติ และแนวทางการดำเนินการที่เกี่ยวข้อง เพื่อให้รองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

๓. ติดตาม ประเมินผลและรายงานผลการดำเนินงานต่อคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕) ทราบเป็นระยะ ๆ

๔. แต่งตั้งคณะทำงานเพื่อดำเนินการตามที่คณะอนุกรรมการเห็นสมควร

๕. ดำเนินการอื่นตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๙ พฤศจิกายน พ.ศ. ๒๕๖๑

(นางพรรษมนต์ ไทยวัฒนานุกูล)
ประธานคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament
ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕)