EGA
e-Government Agency

นโยบายและคู่มือบริหารความเสี่ยง
(Risk Management Policy and Manual)

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

คำนิยม

การเปลี่ยนแปลงของสภาวะเศรษฐกิจ สังคม ธุรกิจ และวิวัฒนาการด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่เกิดขึ้นในปัจจุบันนี้ เป็นสิ่งที่ทุกภาคส่วนในธุรกิจและทุกประเทศจำเป็นจะต้องตระหนักและพิจารณาอย่างเข้าใจและเลี่ยงไม่ได้ที่จะต้องให้ความสำคัญและปรับรูปแบบการดำเนินธุรกิจรวมถึงกลยุทธ์ต่าง ๆ เพื่อให้องค์กรสามารถอยู่รอดและแข่งขันได้ การปรับเปลี่ยนใด ๆ ก็ตามภายในองค์กรไม่ว่าจะปรับเปลี่ยนในรูปแบบใดตั้งแต่ระดับกลยุทธ์องค์กร จนถึงการปรับเปลี่ยนในระดับกระบวนการดำเนินงาน สิ่งเหล่านี้เป็นสิ่งที่ผู้มีบทบาทในการบริหารองค์กรจะมองข้ามไม่ได้ และจำเป็นจะต้องตระหนักและให้ความสำคัญในเรื่องการบริหารการเปลี่ยนแปลง (Change Management)

ภายใต้การบริหารความเปลี่ยนแปลงต่าง ๆ ที่เกิดจากปัจจัยทั้งภายในและภายนอกที่มากระทบกับองค์กร แน่นอนที่สุดที่ทุกคนต้องยอมรับและต้องตระหนักควบคู่กันไปด้วยคือ “การบริหารความเสี่ยง” ซึ่งองค์กรที่มีความพร้อมรับมือการเปลี่ยนแปลงและให้ความสำคัญกับการบริหารจัดการและควบคุมความเสี่ยงให้อยู่ในระดับการยอมรับได้เท่านั้นที่จะทำให้ธุรกิจสามารถรับมือกับการเปลี่ยนแปลงและดำเนินภารกิจได้ประสบความสำเร็จ การบริหารความเสี่ยงเป็นองค์ประกอบของการกำกับดูแลกิจการที่ดี ซึ่งนอกจากจะสนับสนุนให้องค์กรสามารถดำเนินงานได้บรรลุตามเป้าหมายที่กำหนดแล้ว ยังสามารถสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้ส่วนเสียขององค์กร (Stakeholders) ได้อีกทางหนึ่ง

จากการที่ผมได้อ่านนโยบายและคู่มือบริหารความเสี่ยงเล่มนี้ ผมมีความรู้สึกประทับใจที่คณะผู้จัดทำได้นำเสนอรายละเอียดการบริหารความเสี่ยงในแต่ละด้านได้อย่างชัดเจน และง่ายต่อการเข้าใจ ซึ่งได้กล่าวถึงกระบวนการบริหารความเสี่ยงโดยเริ่มจากการระบุความเสี่ยง (Risk Identified) การประเมินความเสี่ยง (Risk Assessment) การควบคุมและบรรเทาความเสี่ยง (Risk Control) การรายงานความเสี่ยง (Risk Reporting) และการติดตามความเสี่ยง (Risk Monitoring) อีกทั้งมีการกล่าวถึงตัวอย่างเพื่อประกอบการอธิบายอย่างชัดเจนในแต่ละขั้นตอน ซึ่งจะช่วยให้ผู้อ่านมีความเข้าใจและสามารถนำเนื้อหาในนโยบายและคู่มือฯ เล่มนี้ไปใช้ประโยชน์ได้อย่างแท้จริง

ผมหวังเป็นอย่างยิ่งว่านโยบายและคู่มือบริหารความเสี่ยงเล่มนี้ จะเป็นประโยชน์ต่อสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) เพื่อใช้เป็นแนวทางและหลักปฏิบัติในการบริหารความเสี่ยงขององค์กร ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และนำไปสู่เป้าหมายที่กำหนดไว้

รศ. ดร. วรากรณ์ สามโกเศศ
ประธานกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์

คำนิยม

ความเสี่ยง เป็นสิ่งที่ทุกองค์กรจะต้องบริหารจัดการ ไม่ว่าองค์กรนั้นจะเป็นหน่วยงานขนาดเล็ก หรือขนาดใหญ่เป็นหน่วยงานที่มีภารกิจ หรือบทบาทที่เกี่ยวข้อง หรือมีผลกระทบต่อหน่วยงานอื่นมาก หรือน้อยเพียงใดก็ตามความพยายามที่จะบริหารจัดการความเสี่ยงจะไม่บรรลุผลสำเร็จได้เลย หากผู้ที่เกี่ยวข้องในองค์กรไม่มีความรู้ ความเข้าใจ หรือไม่ตระหนักในปัจจัยเสี่ยงที่มีอยู่ รวมทั้งไม่มีวิธีการที่ชัดเจน ปฏิบัติได้ในการจัดการกับความเสี่ยง ที่มิใช่การขจัดความเสี่ยงให้หมดสิ้นไปซึ่งเป็นสิ่งที่เป็นไปไม่ได้ ดังนั้น การลดความเสี่ยงในด้านต่างๆ ให้อยู่ในระดับที่ยอมรับได้ จึงเป็นเป้าหมายของคู่มือฉบับนี้ของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ซึ่งนับว่าเป็นคู่มือที่มีความครบถ้วน สมบูรณ์ อันจะนำไปสู่การบริหารจัดการความเสี่ยงในการปฏิบัติภารกิจของ สรอ. ได้อย่างมีประสิทธิผล

อย่างไรก็ตาม การมีคู่มือบริหารความเสี่ยงเพียงอย่างเดียวไม่ได้ทำให้ สรอ. มีการบริหารจัดการความเสี่ยงที่ดีได้ การปฏิบัติตามคู่มือฉบับนี้อย่างเคร่งครัด เป็นเงื่อนไขสำคัญยิ่งที่จะนำไปสู่ความสำเร็จในการควบคุมความเสี่ยงทุกด้านของ สรอ. ฉะนั้น การสร้างความตระหนัก และการทำความเข้าใจกับผู้บริหารและพนักงานทุกคนจึงเป็นสิ่งแรกที่ควรกระทำเพื่อให้คู่มือฉบับนี้ได้ถูกนำไปใช้กับทุกปัจจัยเสี่ยงซึ่งจะทำให้ สรอ. สามารถปฏิบัติภารกิจ และบรรลุเป้าหมายขององค์กรได้อย่างมีความเสี่ยงน้อยที่สุด

นางสาววลัยรัตน์ ศรีอรุณ
ที่ปรึกษา สำนักงานรัฐบาลอิเล็กทรอนิกส์

คำนิยม

การเปลี่ยนแปลงของสภาวะแวดล้อมในปัจจุบัน เป็นความจริงที่ไม่สามารถหลีกเลี่ยงได้ ไม่เว้นแม้แต่วิวัฒนาการด้านเทคโนโลยีสารสนเทศ การจับกระแสทิศทางการเปลี่ยนแปลงของโลกยุคใหม่เพื่อปรับเปลี่ยนให้ทันหรือสอดรับต่อเหตุการณ์ที่เปลี่ยนผันตลอดเวลานั้น อาจส่งผลให้การดำเนินงานของหลายๆ องค์กรไม่เป็นไปตามเป้าหมายที่ได้กำหนดไว้ตามแผนการดำเนินงาน เนื่องจากต้องเผชิญหน้ากับการเปลี่ยนแปลงตลอดเวลา อีกทั้งความเสี่ยงที่อาจเกิดขึ้นได้จากสภาพแวดล้อมทั้งภายในและภายนอกองค์กร อาจส่งผลกระทบ สร้างความเสียหายหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ที่กำหนดไว้ หากองค์กรละเลยในการดูแลและจัดการกับ "การบริหารความเสี่ยง"

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ตระหนักถึงความสำคัญของการบริหารความเสี่ยง ซึ่งถือได้ว่าเป็นองค์ประกอบของการกำกับดูแลกิจการที่ดี (Good Governance) จึงได้จัดทำนโยบายบริหารความเสี่ยงขึ้น เพื่อให้เป็นกรอบแนวทางในการดำเนินการและการพัฒนาระบบการบริหารความเสี่ยงที่มีคุณภาพและมีมาตรฐานตามแนวทางการกำกับดูแลของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และสำนักงานคณะกรรมการพัฒนาระบบราชการ โดยเล็งเห็นว่าหากสำนักงานมีการบริหารความเสี่ยงที่มีประสิทธิภาพจะเป็นส่วนสำคัญอย่างยิ่งในการเพิ่มศักยภาพขององค์กร จึงได้กำหนดนโยบายการบริหารความเสี่ยง (Enterprise Risk Management Policy) ของสำนักงานให้ครอบคลุม ๕ ด้าน ได้แก่ ด้านนโยบายและกลยุทธ์ ด้านการเงินและงบประมาณ ด้านการปฏิบัติงาน ด้านกฎหมาย กฎระเบียบ และด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

การบริหารความเสี่ยงภายในองค์กรของสำนักงาน นับเป็นองค์ประกอบที่สำคัญยิ่งในการบริหารจัดการองค์กร ซึ่งเป็นสิ่งที่ทุกคนในองค์กรจำเป็นต้องให้ความร่วมมือในการปฏิบัติอย่างจริงจัง และต่อเนื่องจนเกิดเป็นวัฒนธรรมองค์กร เพื่อให้ความเสี่ยงที่เหลืออยู่ในระดับที่ยอมรับได้ อีกทั้งต้องร่วมกันมองหาโอกาสที่เกิดขึ้นนำมาสร้างมูลค่าเพิ่มให้แก่องค์กร (Value Creation) ตลอดจนปรับปรุง เปลี่ยนแปลงกระบวนการจัดการให้สอดคล้องกับสถานการณ์ตลอดเวลา ซึ่งนอกจากจะทำให้องค์กรสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้แล้ว ยังจะเป็นประโยชน์ต่อองค์กรในภาพรวมตามนโยบายและหลักการกำกับดูแลที่ดี ผมหวังเป็นอย่างยิ่งว่านโยบายและคู่มือการบริหารความเสี่ยงของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) เล่มนี้ จะเป็นประโยชน์ต่อบุคลากรของสำนักงาน ในการพัฒนากระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานของสำนักงานให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงานและแผนกลยุทธ์องค์กรต่อไป

ดร.ศักดิ์ เสกขุนทด
ผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์

โครงสร้างเนื้อหา

ความเสี่ยงระดับองค์กร
(Enterprise Risk)

ประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
ที่ ๔๙ /๒๕๕๕
เรื่อง นโยบายการบริหารความเสี่ยง สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

.....

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ตระหนักถึงความสำคัญของการบริหารความเสี่ยง จึงได้จัดทำนโยบายบริหารความเสี่ยง (Enterprise Risk Management Policy) ขึ้น เพื่อให้เป็นกรอบแนวทางในการดำเนินการและการพัฒนาระบบการบริหารความเสี่ยง โดยมุ่งเน้นให้กรรมการ ผู้อำนวยการ ผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กรตระหนักถึงความสำคัญของการจัดการและควบคุมความเสี่ยงในการดำเนินงาน เพื่อให้บรรลุวิสัยทัศน์ พันธกิจ และกลยุทธ์ขององค์กร พร้อมทั้งมีการดำเนินการเพื่อสนองตอบต่อเหตุการณ์อันอาจส่งผลให้เกิดความเสี่ยงทุกๆ ด้านได้อย่างเคร่งครัดและทันท่วงที

ทั้งนี้ นโยบายการบริหารความเสี่ยง (Enterprise Risk Management Policy) ของ สรอ. ครอบคลุมถึงการบริหารความเสี่ยง ๕ ด้าน ดังนี้ ด้านนโยบายและกลยุทธ์ ด้านการเงินและงบประมาณ ด้านการปฏิบัติงาน ด้านกฎหมาย กฎระเบียบ และด้านระบบเทคโนโลยีสารสนเทศ ทั้งนี้ สรอ. ตระหนักดีว่าความต่อเนื่องของการบริหารงานของ สรอ. เป็นปัจจัยสำคัญต่อหน่วยงานอื่น ๆ เป็นจำนวนมาก

ซึ่งการดำเนินการบริหารความเสี่ยงภายในองค์กรของ สรอ. ได้คำนึงถึงการสร้างความพึงพอใจ ให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholders) และการสร้างมูลค่าเพิ่มให้กับองค์กร (Value Creation) โดยพิจารณาถึงผลกระทบต่อเป้าหมายการดำเนินการ เพื่อให้เป็นไปตามหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance) โดยมีการบูรณาการความเสี่ยงกับการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี เพื่อเป็นการสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรอย่างยั่งยืน มีระบบบริหารความเสี่ยงที่เป็นมาตรฐาน พร้อมตอบสนองต่อเหตุการณ์เสี่ยงได้อย่างทันท่วงที

ดังนั้น เพื่อให้การบริหารความเสี่ยงของ สรอ. เป็นไปด้วยความเรียบร้อยอย่างมีประสิทธิภาพและประสิทธิผลอาศัยอำนาจตามมาตรา ๒๖ และ ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ.๒๕๕๔ ประกอบกับมติคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ ในคราวประชุมครั้งที่ ๗/๒๕๕๕ เมื่อวันที่ ๑๘ กรกฎาคม ๒๕๕๕ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) จึงกำหนดนโยบายการบริหารความเสี่ยงตามรายละเอียดแนบท้ายประกาศนี้ เพื่อให้ปฏิบัติตามอย่างเคร่งครัดโดยทั่วกัน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๒ สิงหาคม พ.ศ. ๒๕๕๕

(นายศักดิ์ เสกขุนทด)
ผู้อำนวยการ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

คู่มือบริหารความเสี่ยงสำนักงานรัฐบาลอิเล็กทรอนิกส์
(Enterprise Risk Management Manual)

สารบัญ

หน้าที่

๑. บทสรุปผู้บริหาร

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ตระหนักถึงความสำคัญของการบริหารความเสี่ยง จึงได้จัดทำนโยบายบริหารความเสี่ยง (Enterprise Risk Management Policy) ขึ้น เพื่อให้เป็นกรอบแนวทางการพัฒนาระบบการบริหารความเสี่ยงให้มีคุณภาพและมาตรฐานตามแนวทางการกำกับดูแลของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และสำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) รวมถึงแนวทางปฏิบัติที่ดี โดยคำนึงถึงความสอดคล้องกับวัตถุประสงค์และเป้าหมายการดำเนินงานของสำนักงาน ทั้งนี้เพื่อให้นโยบายบริหารความเสี่ยงสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) มีประสิทธิภาพและประสิทธิผลในการบริหารจัดการความเสี่ยงของสำนักงาน ตลอดจนสร้างความมั่นใจว่า สำนักงานมีการบูรณาการกระบวนการทำงานเกี่ยวกับการกำกับดูแลกิจการ (Corporate Governance) การบริหารความเสี่ยง (Risk Management) และการปฏิบัติตามกฎหมาย ระเบียบ ประกาศ คำสั่ง และมาตรฐานที่ดี (Compliance) เพื่อให้บรรลุถึงผลการดำเนินงานที่เกิดจากการมีส่วนร่วมของหน่วยงานและบุคลากรทุกระดับในสำนักงาน

๒. หลักการและวัตถุประสงค์

การเปลี่ยนแปลงสภาพแวดล้อมในการดำเนินงานของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ทั้งปัจจัยภายใน อาทิ การปรับเปลี่ยนกลยุทธ์ โครงสร้างสำนักงาน การเปลี่ยนแปลงทรัพยากรภายในสำนักงาน รวมถึงปัจจัยภายนอก อาทิ เหตุการณ์ความไม่สงบทางการเมือง ภัยธรรมชาติ เป็นต้น อาจส่งผลกระทบให้การดำเนินงานของสำนักงานไม่เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์ ซึ่งจะก่อให้เกิดความเสี่ยงต่อสำนักงานโดยรวม

การบริหารความเสี่ยงเป็นองค์ประกอบของการกำกับดูแลกิจการที่ดี ซึ่งนอกจากจะสนับสนุนให้องค์กรสามารถดำเนินงานได้บรรลุตามเป้าหมายที่กำหนดแล้ว ยังสามารถสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้ส่วนเสียขององค์กร (Stakeholders) ได้อีกทางหนึ่ง สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) จึงได้นำกรอบการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ (Enterprise Risk Management – Integrated Framework) ตามแนวทาง COSO ERM มาประยุกต์ใช้เป็นกรอบและแนวทางในการพัฒนาระบบการบริหารความเสี่ยงของสำนักงาน ซึ่งมีวัตถุประสงค์ในการให้ผู้บริหาร เจ้าหน้าที่และลูกจ้างในองค์กรตระหนักถึงความสำคัญของการบริหารความเสี่ยง และมีความเข้าใจตรงกันในคำนิยาม เป้าหมายและวัตถุประสงค์ อันจะเป็นการสร้างความรับผิดชอบอย่างทั่วถึงและเป็นไปในทิศทางเดียวกันทั่วทั้งสำนักงานได้อย่างมีประสิทธิภาพ

นโยบายการบริหารความเสี่ยง (Enterprise Risk Management Policy) จัดทำขึ้นเพื่อวัตถุประสงค์ ดังนี้

๑) เพื่อใช้เป็นแนวทางให้กับผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กร ในการเป็นส่วนหนึ่งของการพัฒนากระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์

๒) เพื่อให้สำนักงานมีกรอบการดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่อาจส่งผลให้เกิดความเสี่ยงทุกด้านได้อย่างเป็นระบบและมีมาตรฐาน รวมทั้งมีการดำเนินการเพื่อสร้างพื้นฐานในการป้องกันความเสี่ยงระยะยาวให้กับสำนักงานที่สำคัญ

๓) เพื่อเป็นกลไกในการพัฒนาองค์ความรู้ด้านการบริหารความเสี่ยงให้เกิดขึ้นกับผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งสำนักงาน และสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน

๔) เพื่อให้ผู้บริหาร เจ้าหน้าที่และลูกจ้าง ตระหนักและมีความเข้าใจตรงกันถึงเป้าหมายวัตถุประสงค์รวมทั้งแนวทางการบริหารความเสี่ยงของสำนักงาน เพื่อร่วมกันสร้างความพึงพอใจให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholders) และสร้างมูลค่าเพิ่มให้กับองค์กร โดยพิจารณาถึงผลกระทบต่อเป้าหมายการดำเนินงานของสำนักงานให้เป็นไปตามหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance) และข้อกำหนดของหน่วยงานที่กำกับดูแลสำนักงาน

ตามคู่มือการบริหารและกำกับดูแลของคณะกรรมการองค์การมหาชน (หน้า ๔๑) กำหนดให้องค์การมหาชนควรดำเนินการวิเคราะห์และประเมินความเสี่ยงขององค์กรให้ครอบคลุมอย่างน้อย ๔ ด้าน ได้แก่ ด้านนโยบายและกลยุทธ์ ด้านการเงินและงบประมาณ ด้านการปฏิบัติงาน และด้านกฎหมาย กฎระเบียบ และสามารถเพิ่มนโยบายการบริหารความเสี่ยงด้านอื่น ๆ ได้ เพื่อให้ครอบคลุมกับการดำเนินงานขององค์กร สรอ. จึงจัดแบ่งประเภทความเสี่ยงของสำนักงานเป็น ๕ ด้าน ดังนี้

๑) ด้านนโยบายและกลยุทธ์

๒) ด้านการเงิน

๓) ด้านการปฏิบัติงาน

๔) ด้านกฎหมาย กฎระเบียบ

๕) ด้านระบบเทคโนโลยีสารสนเทศ

ซึ่งสามารถจัดทำเป็นนโยบายที่เกี่ยวข้องด้านการบริหารความเสี่ยง ๕ นโยบาย ประกอบด้วย

๑) นโยบายด้านนโยบายและกลยุทธ์ หมายถึง ความเสี่ยงที่เกิดจากการกำหนดนโยบายต่าง ๆ เช่น นโยบายระดับรัฐจนถึงนโยบายในระดับผู้บริหาร แผนกลยุทธ์ แผนดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับสภาพแวดล้อมภายใน และปัจจัยภายนอก เป็นต้น ทำให้มีโอกาสที่จะไม่ประสบความสำเร็จตามทิศทางที่กำหนดไว้ ซึ่งจะส่งผลกระทบต่อตัวชี้วัดผลการปฏิบัติงานของสำนักงาน

๒) นโยบายด้านการเงิน หมายถึง ความเสี่ยงทางการเงินในภาพรวม ทั้งในด้านการบริหารจัดการด้านการเงิน การวางแผนทางการเงิน ซึ่งต้องเป็นไปในทิศทางเดียวกับกลยุทธ์ของสำนักงาน และกฎหมาย กฎระเบียบต่าง ๆ ที่เกี่ยวข้อง

๓) นโยบายด้านการปฏิบัติงาน หมายถึง ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากบุคลากร ระบบงาน และระบบสารสนเทศ รวมถึงการขาดระบบการควบคุมที่เกี่ยวข้องกับกระบวนการปฏิบัติงานทั้งหมด โดยเฉพาะการไม่ได้ประเมินความเสี่ยงของโครงการของสำนักงาน

๔) นโยบายด้านกฎหมาย กฎระเบียบ หมายถึง ความเสี่ยงต่าง ๆที่เกี่ยวข้องกับกฎหมาย ระเบียบ ประกาศ คำสั่ง มติคณะรัฐมนตรี หรือมาตรฐานที่ดี ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงกฎระเบียบ เป็นต้น

๕) นโยบายด้านระบบเทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่ครอบคลุมการบริหารจัดการ และประสิทธิภาพการดำเนินงานด้านเทคโนโลยีสารสนเทศ ซึ่งเกี่ยวข้องกับความมั่งคงปลอดภัย (Security) ความถูกต้องเชื่อถือได้ของข้อมูล (Integrity) และความพร้อมใช้งานของระบบงานและข้อมูล (Availability)

๓. แนวทางการกำหนดกลยุทธ์การบริหารความเสี่ยง

สำนักงานต้องกำหนดกลยุทธ์ในการบริหารความเสี่ยงโดยคำนึงถึงสาระสำคัญ ดังนี้

๑) ความเหมาะสมกับขอบเขตและลักษณะการดำเนินงานของสำนักงาน ตลอดจนสภาพแวดล้อมที่เปลี่ยนแปลงไป โดยจะต้องมีความสอดคล้องกับนโยบาย/กลยุทธ์/เป้าหมาย/แผนงาน/โครงการต่าง ๆ ของสำนักงาน

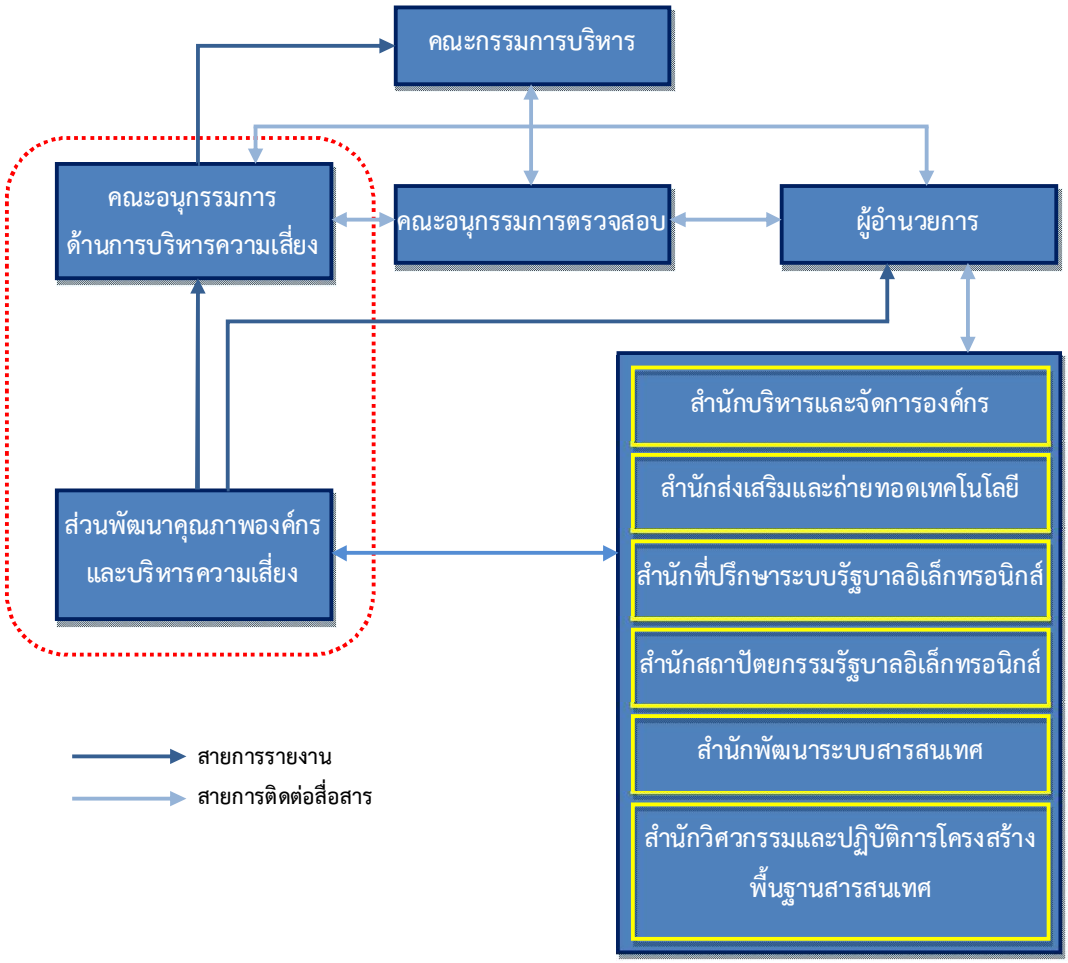
๒) ความสอดคล้องกับแนวทางมาตรฐานของหน่วยงานกำกับดูแล ข้อกำหนดของกฎหมาย ระเบียบประกาศ หลักเกณฑ์ และแนวทางปฏิบัติที่ดี

๓) สำนักงานจะต้องทบทวนกลยุทธ์การบริหารความเสี่ยงอย่างน้อยปีละ ๑ ครั้งตามแผนประจำปี หรือทบทวนทันทีที่มีเหตุการณ์เปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้ทราบถึงปัญหา อุปสรรค ที่ส่งผลต่อการบรรลุเป้าหมายการบริหารความเสี่ยง และเพื่อสร้างความมั่นใจถึงการบรรลุเป้าหมายโดยรวมของสำนักงาน

๔. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงและบทบาทหน้าที่รับผิดชอบการบริหารความเสี่ยง

สำนักงานต้องจัดให้มีโครงสร้างหน้าที่ของคณะอนุกรรมการและหน่วยงาน เพื่อกำกับดูแลและรับผิดชอบด้านการบริหารความเสี่ยง โดยโครงสร้างหน้าที่ต้องมีความชัดเจน สอดคล้องกับการบริหารความเสี่ยงของสำนักงาน และเหมาะสมกับการดำเนินงานขององค์กร รวมถึงมีความเป็นอิสระและมีการถ่วงดุลอำนาจอย่างเหมาะสม ดังนี้



๕. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการที่เกี่ยวข้องกับการบริหารความเสี่ยง

คณะกรรมการ	บทบาท หน้าที่ และความรับผิดชอบ
คณะกรรมการบริหาร สำนักงานรัฐบาลอิเล็กทรอนิกส์	๑) อนุมัตินโยบาย และกลยุทธ์การบริหารความเสี่ยงเพื่อประกาศใช้ ๒) กำกับดูแลให้มีการดำเนินงานที่เป็นไปตามหลักเกณฑ์ของทางการและเป็นไปตามหลักการกำกับดูแลกิจการที่ดี มีความโปร่งใส เป็นธรรมต่อทุกหน่วยงานที่เกี่ยวข้อง
คณะอนุกรรมการด้านบริหารความเสี่ยง	๑) เสนอแนะนโยบายการบริหารความเสี่ยงและกรอบของการบริหารความเสี่ยงต่อคณะกรรมการ ๒) ให้คำปรึกษาและเสนอแนะการจัดทำแผนบริหารความเสี่ยงเพื่อให้บรรลุเป้าหมายตามแผนปฏิบัติงานของสำนักงาน เพื่อเสนอต่อคณะกรรมการ ๓) เสนอแนะแนวทาง ในการบริหารจัดการหรือการดำเนินงาน เพื่อลดผลกระทบและความเสี่ยงที่อาจจะเกิดขึ้นกับสำนักงาน ๔) พิจารณาผลการประเมินและติดตามความมีประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงเพื่อรายงานต่อคณะกรรมการ ๕) ในกรณีการพิจารณากลั่นกรอง ให้คำปรึกษา ประเมินหรือวิเคราะห์ในเรื่องใดที่จำเป็นต้องมีผู้เชี่ยวชาญเฉพาะด้านในสาขาที่เกี่ยวข้องเข้าร่วมพิจารณาในรายละเอียด ให้คณะอนุกรรมการเชิญบุคคลดังกล่าวเข้าร่วมพิจารณากับคณะอนุกรรมการเป็นคราวๆ ไป โดยให้บุคคลดังกล่าวได้รับค่าตอบแทนตามระเบียบสำนักงาน ๖) ปฏิบัติงานอื่นใดตามที่ประธานกรรมการ หรือคณะกรรมการมอบหมาย
คณะอนุกรรมการตรวจสอบ	๑) สอบทานให้สำนักงานมีระบบการควบคุมภายในระบบการตรวจสอบภายในและระบบการบริหาร ความเสี่ยงที่เหมาะสมและมีประสิทธิผล

คณะกรรมการ	บทบาท หน้าที่ และความรับผิดชอบ
	๒) ให้คำปรึกษาและเสนอแนะแนวทางการพัฒนา ปรับปรุงระบบการควบคุมภายใน ระบบการตรวจสอบภายในและระบบการบริหารความเสี่ยงที่สำคัญและจำเป็น เพื่อให้มีความทันสมัยอยู่เสมอ ๓) กำกับดูแลการปฏิบัติให้สอดคล้องตามนโยบาย ข้อบังคับ กฎระเบียบ ประกาศ คำสั่ง มติคณะรัฐมนตรี และกฎหมายอื่นๆ ที่เกี่ยวข้อง

บทบาท หน้าที่และความรับผิดชอบของผู้บริหาร หน่วยงาน และเจ้าหน้าที่ที่เกี่ยวข้องกับการบริหารความเสี่ยง

หน่วยงาน/ผู้บริหาร/คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
ผู้อำนวยการ เจ้าหน้าที่ และลูกจ้างทุกคนในสำนักงาน	๑) เป็นเจ้าของความเสี่ยง (Risk Owner) มีหน้าที่ลูกจ้างทุกคนในสำนักงานรับผิดชอบการวิเคราะห์ ระบุ และประเมินความเสี่ยง กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือแผนบริหารความเสี่ยงของหน่วยงาน/โครงการ หรืองานที่อยู่ในความรับผิดชอบ ๒) ติดตามและรายงานความเสี่ยงให้ผู้บังคับบัญชาทราบตามลำดับชั้นตลอดจนคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อให้การบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ
ผู้บริหาร	ผู้บริหารตั้งแต่ระดับผู้จัดการขึ้นไปมีหน้าที่กำกับ ดูแล หน่วยงาน/โครงการให้มีการบริหารและจัดการความเสี่ยง และเป็นเจ้าของความเสี่ยง (Risk Owner)
คณะทำงานการบริหารความเสี่ยงด้าน/เรื่อง ต่าง ๆ	มีหน้าที่ตามที่ได้รับมอบหมายจากคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ หรือคณะอนุกรรมการด้านการบริหารความเสี่ยง
ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง	๑) จัดและทบทวนนโยบายและกลยุทธ์ในการดำเนินงานด้านการบริหารความเสี่ยงเพื่อนำเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยง ๒) จัดทำและทบทวนเครื่องมือในการวัด ติดตามและควบคุมความเสี่ยงเพื่อเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง ๓) ติดตามและรายงานสถานะความเสี่ยงต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

หน่วยงาน/ผู้บริหาร/คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
ส่วนตรวจสอบภายใน	๑) สอบทานและประเมินความเพียงพอ ความมีประสิทธิภาพและประสิทธิผลของบริหารความเสี่ยง ระบบการควบคุมภายใน และระบบที่ส่งเสริมการกำกับดูแลกิจการที่ดี ๒) ตรวจสอบการดำเนินงานตามแผนงานหรือโครงการเพื่อสอดคล้องกับวัตถุประสงค์ และเป้าหมายที่กำหนดไว้อย่างมีประสิทธิภาพและประสิทธิผล
สำนัก/ส่วน	๑) ควบคุมดูแลการปฏิบัติงานในสำนัก/ส่วน ให้เป็นไปตามนโยบายและกลยุทธ์การบริหารความเสี่ยง รวมทั้งจัดให้มีระบบบริหารความเสี่ยงที่มีประสิทธิภาพ ๒) สร้างความมั่นใจว่าการปฏิบัติงานรายวันมีการประเมินจัดการและรายงานความเสี่ยงอย่างเพียงพอ ๓) ส่งเสริมเจ้าหน้าที่ในสำนักและส่วนงานให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง ๔) สร้างความมั่นใจว่าแผนการบริหารความเสี่ยงได้รับการปฏิบัติอย่างครบถ้วน
Risk – Internal Control Officer (RICO)	๑) รับผิดชอบในการประสานงาน การประเมินความเสี่ยง การควบคุมภายใน และการปฏิบัติตามกฎเกณฑ์ รวมทั้งเผยแพร่ความรู้ที่เกี่ยวข้องแก่เจ้าหน้าที่ในหน่วยงานของตนเอง ๒) ให้คำปรึกษา พร้อมทั้งประสานงานให้หน่วยงานตนเอง ดำเนินการตามกระบวนการบริหารความเสี่ยงโดยมีการระบุ ประเมิน และจัดการความเสี่ยงด้านต่างๆ ที่อาจเกิดขึ้น เพื่อป้องกันหรือลดระดับความเสี่ยง ๓) ช่วยเหลือและสนับสนุนการจัดประชุมเชิงปฏิบัติการเพื่อจัดทำแผนจัดการความเสี่ยงทุกระดับ ๔) บันทึก ติดตาม และรายงานความก้าวหน้าของแผนจัดการความเสี่ยงระดับสำนักและส่วนงาน ๕) ประสานงานกับส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง

๖. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

ความหมายของความเสี่ยง

การดำเนินงานในองค์กรโดยทั่วไป มีเป้าหมายเพื่อเพิ่มมูลค่าให้แก่ผู้มีส่วนได้ส่วนเสีย ทำให้ทุกองค์การต้องเผชิญกับความไม่แน่นอน ที่อาจเกิดขึ้นจากปัจจัยภายในและภายนอกหลายประการ เช่น การเปลี่ยนแปลงของกฎ ระเบียบ และนโยบายของรัฐบาล การบริหารงานด้านความปลอดภัยในชีวิตและทรัพย์สินอันเนื่องมาจากการเปลี่ยนแปลงปัจจัยต่างๆ ภัยจากการก่อการร้าย ภัยธรรมชาติ และความเสี่ยงอื่นๆ เป็นต้น ผู้บริหารจึงต้องพิจารณาว่าควรจัดการกับความไม่แน่นอนที่เกิดขึ้นอย่างไร เพื่อให้องค์การสามารถรักษาหรือเพิ่มมูลค่าของผู้มีส่วนได้ส่วนเสียได้

“ความไม่แน่นอน” ที่อาจเกิดขึ้นสามารถส่งผลต่อองค์กรได้ทั้งเชิงลบและเชิงบวก ซึ่งหมายความถึง “ความเสี่ยง” ที่อาจทำให้องค์กรเสียหาย หรือ “โอกาส” ที่เพิ่มมูลค่าให้กับองค์กร การบริหารความเสี่ยงควรเริ่มต้นจากการทำความเข้าใจต่อคำนิยามของความเสี่ยง เพื่อให้ทุกคนมีแนวปฏิบัติเดียวกันในการบ่งชี้ความเสี่ยงและโอกาส

นิยามการบริหารความเสี่ยง

ความหมายของการบริหารความเสี่ยง การบริหารความเสี่ยง คือ การกำหนดนโยบาย โครงสร้าง และกระบวนการ เพื่อให้คณะกรรมการ ผู้บริหารและบุคลากรขององค์กรนำไปปฏิบัติในการกำหนดกลยุทธ์และปฏิบัติงานทั่วทั้งองค์กร กระบวนการบริหารความเสี่ยงได้รับการออกแบบให้สามารถบ่งชี้เหตุการณ์ที่เกิดขึ้น ประเมินผลกระทบต่อองค์กร และกำหนดวิธีการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อให้เกิดความเชื่อมั่นในระดับหนึ่งว่าการดำเนินการในองค์กรจะบรรลุตามวัตถุประสงค์ที่กำหนดไว้

การบริหารความเสี่ยงที่มีประสิทธิผล มีข้อดีดังต่อไปนี้

- เพิ่มมูลค่าขององค์กรที่มีต่อผู้มีส่วนได้ส่วนเสีย
- ทำให้เกิดความมั่นใจต่อการปฏิบัติตามกฎหมายและข้อบังคับต่างๆ
- เพิ่มประสิทธิภาพการทำงานของเจ้าหน้าที่
- ป้องกันและดูแลทรัพย์สินต่างๆ
- ทำให้การดำเนินงานเป็นไปอย่างยั่งยืน
- เพิ่มความน่าเชื่อถือของการเปิดเผยข้อมูลต่อบุคลากรภายนอก

ศัพท์เฉพาะ/คำนิยาม

ศัพท์เฉพาะ	คำนิยาม
ความเสี่ยง (Risk)	เหตุการณ์ที่มีความไม่แน่นอน อาจเกิดขึ้นและมีผลกระทบในเชิงลบต่อการบรรลุวัตถุประสงค์และเป้าหมาย
ระดับความเสี่ยงก่อนการบริหาร (Inherent Risk)	ระดับความเสี่ยงที่เกิดขึ้นก่อนที่จะมีการควบคุม/จัดการ
ระดับความเสี่ยงหลังการบริหาร (Residual Risk)	ระดับความเสี่ยงที่คงเหลืออยู่หลังจากที่ได้ควบคุม/จัดการแล้ว
โอกาส (Likelihood)	โอกาสหรือความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้น
ผลกระทบ (Impact/Consequence)	ผลกระทบจากเหตุการณ์ที่เกิดขึ้นทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน
การระบุปัจจัยเสี่ยง (Risk Identification)	การระบุปัจจัยเสี่ยง เป็นขั้นตอนในการค้นหาว่าปัจจัยเสี่ยงใดบ้างที่ส่งผลกระทบต่อเป้าหมาย
ผู้รับผิดชอบความเสี่ยง (Risk Owner)	ผู้รับผิดชอบความเสี่ยง หรือผู้ที่ใกล้ชิดความเสี่ยงโดยตรง มีความสามารถในการจัดการเพื่อลดระดับความเสี่ยง
Degree of Acceptance	ระดับของการยอมรับความเสี่ยง
Risk Map	แผนภาพแสดงความสัมพันธ์ของปัจจัยเสี่ยงและผลกระทบทั้งในเชิงปริมาณและเชิงคุณภาพที่ส่งผลเชื่อมโยงกันต่อเป้าหมายของหน่วยงานต่างๆ ภายในองค์กร Risk Map สามารถช่วยในการจัดทำแผนการบริหารความเสี่ยงให้มีประสิทธิภาพมากขึ้นและครอบคลุมถึงปัจจัยเสี่ยงต่างๆ ครบถ้วน
Risk Profile	กลุ่ม (set) ของความเสี่ยง ที่แสดงให้เห็นถึงความเสี่ยงต่างๆ ที่อาจส่งผลกระทบต่อเป้าหมายของหน่วยงานต่างๆ โดยจะมีข้อมูลที่บ่งบอกลักษณะของความเสี่ยง ประเภทของความเสี่ยง ผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงนั้น ตลอดจนข้อมูลต่างๆ ที่เกี่ยวข้องกับความเสี่ยงนั้น สามารถแสดงด้วยแผนภูมิ (Risk Map) ๒ มิติ ขนาด ๕*๕ ประกอบด้วยแกนด้านผลกระทบ และแกนด้านโอกาสเกิดแต่ละแกนแบ่งระดับความรุนแรงเป็น ๕ ระดับมีวัตถุประสงค์เพื่อเป็นการวัดระดับความเสี่ยง
Risk Appetite	ระดับความเสี่ยงโดยรวมที่องค์กรยอมรับได้เพื่อมุ่งไปสู่พันธกิจหรือวิสัยทัศน์ขององค์กร
Risk Tolerance	ระดับความเบี่ยงเบนที่องค์กรยอมรับได้จากเกณฑ์หรือดัชนีวัดผลการดำเนินงานที่เกี่ยวข้องกับการบรรลุวัตถุประสงค์
KRI (Key Risk Indicator)	ตัวชี้วัดเชิงปริมาณ กิจกรรม หรือเหตุการณ์ ที่บ่งบอกถึงการเปลี่ยนแปลงของความเสี่ยงสำคัญที่ส่งผลกระทบต่อเป้าหมายได้ โดยสามารถใช้ประโยชน์ในการบริหารความเสี่ยง เพื่อติดตามผลการบริหารความเสี่ยงว่าเป็นไปตามเป้าหมายหรือไม่ เพื่อจะได้ปรับปรุง/เปลี่ยนแปลงแผนการบริหารความเสี่ยงให้มีประสิทธิภาพมากยิ่งขึ้น

ศัพท์เฉพาะ	คำนิยาม
	และในกรณีตัวชี้วัดมีลักษณะเป็นดัชนีชี้นำ (Leading Indicator) สามารถนำไปใช้ประโยชน์ในการวางแผนการบริหารความเสี่ยงให้มีระบบเตือนล่วงหน้า (Early Warning System) ได้
Value Driver Diagram	แผนภาพแสดงปัจจัยที่ส่งผลกระทบต่อเป้าหมายทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ใช้หลักการเดียวกับ Cause-and–Effect Analysis โดย Value Driver Diagram เป็นเครื่องมือที่สำคัญในขั้นตอนการระบุปัจจัยเสี่ยง
Risk Factor	ปัจจัยเสี่ยงหมายถึง สิ่งที่เกิดขึ้นจากเหตุการณ์ หรือรายละเอียดของเหตุการณ์ที่ทำให้ทราบว่าความเสี่ยงเกิดจากอะไร
Risk Driver	เหตุแห่งความเสี่ยง ซึ่งอาจเป็นเหตุเกิดจากปัจจัยภายในองค์กร เช่น วัฒนธรรมองค์กร โครงสร้างองค์กร บุคลากร หรือเหตุที่เกิดจากปัจจัยภายนอก เช่น การเมือง คู่แข่ง สภาวะเศรษฐกิจ เป็นต้น
Cost & Benefit Analysis	การวิเคราะห์ถึงผลประโยชน์เปรียบเทียบกับต้นทุนทั้งที่เป็นตัวเงินและไม่สามารถวัดเป็นตัวเงิน เพื่อใช้ในการตัดสินใจ เลือกใช้วิธีการที่เหมาะสม โดยการตัดสินใจเลือกใช้การจัดการความเสี่ยงวิธีใดนั้นควรคำนึงถึงประโยชน์ทั้งในด้านของการลดผลกระทบหรือโอกาสเกิด โดยเปรียบเทียบกับต้นทุนหรือค่าใช้จ่ายที่เกิดจากการจัดการความเสี่ยงนั้นๆ แล้วพิจารณาเลือกวิธีการจัดการความเสี่ยงที่ได้รับประโยชน์มากกว่าต้นทุนหรือค่าใช้จ่ายที่ต้องใช้
ความมั่นคงปลอดภัย (Security)	การจัดการป้องกันการเข้าถึง การเข้าไปแก้ไขเปลี่ยนแปลง การทำลาย การเปิดเผยข้อมูล การรักษาความลับ (Confidential) ทั้งระหว่างที่กำลังพัฒนาระบบงาน หรือในการจัดส่งข้อมูลการประมวลผล หรือการจัดเก็บรักษาข้อมูลในระบบงาน การจัดเก็บระบบงาน โดยจัดการป้องกันให้มีความเหมาะสมและความสำคัญของข้อมูลรวมถึงระบบงานด้วย
ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)	ข้อมูลที่จะส่งมอบให้กับผู้ใช้ข้อมูล (End User) เป็นข้อมูลที่มีความสมบูรณ์ ถูกต้องครบถ้วน ซึ่งจะทำให้การดำเนินงานและการบริหารงานขององค์กรมีประสิทธิภาพ
ความพร้อมใช้งานของระบบงานและข้อมูล (Availability)	เรื่องของการจัดส่งข้อมูลไปให้ผู้ที่ต้องการใช้ข้อมูลได้รวดเร็วทันเวลา และสามารถให้ข้อมูลได้อย่างต่อเนื่องในเวลาที่เหมาะสม เพื่อสนับสนุนการดำเนินงานขององค์กร ทั้งนี้องค์กรต้องมีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ซึ่งเป็นแผนการดำเนินงานหลักขององค์กร และมีแผนงานรองประกอบแผนงานหลักได้แก่ แผนการกู้ระบบกลับคืน (Disaster Recovery Plan) แผนสำรองฉุกเฉิน (Contingency Plan) และแผนรองรับเหตุการณ์ไม่คาดว่าจะเกิดขึ้น (Incident Response Plan)

ดังนั้น การบริหารความเสี่ยงขององค์กรโดยรวม (Enterprise-Wide Risk Management) หมายถึง การบริหารความเสี่ยงโดยเชื่อมโยงการบริหารความเสี่ยงจากเหตุที่เกิดจากปัจจัยภายใน เช่น โครงสร้างองค์กร กระบวนการในการดำเนินงานต่าง ๆ บุคลากร วัฒนธรรมองค์กร และจากปัจจัยภายนอก เช่น การเมือง คู่แข่ง ภาวะเศรษฐกิจ เข้าด้วยกัน โดยมีลักษณะสำคัญ ได้แก่

- ผสมผสานและเป็นส่วนหนึ่งของธุรกิจ โดยการบริหารความเสี่ยงควรสอดคล้องกับแผนธุรกิจ วัตถุประสงค์ การตัดสินใจ และสามารถนำไปใช้กับองค์ประกอบอื่น ๆ ในการบริหารองค์กร
- พิจารณาความเสี่ยงทั้งหมด โดยครอบคลุมความเสี่ยงทั่วทั้งองค์กร ได้แก่ ความเสี่ยงเกี่ยวกับกลยุทธ์ การดำเนินงาน การเงิน และการปฏิบัติตามกฎระเบียบ ซึ่งความเสี่ยงเหล่านี้อาจทำให้เกิดความเสียหาย ความไม่แน่นอน และโอกาส รวมถึงการมีผลกระทบต่อวัตถุประสงค์ และความต้องการของผู้มีส่วนได้ส่วนเสีย
- ระบุความเสี่ยงโดยการคาดการณ์ในอนาคต โดยองค์กรต้องสามารถระบุว่าความเสี่ยงอะไรที่อาจเกิดขึ้นบ้าง และเมื่อเกิดขึ้นจริงจะมีผลกระทบต่อวัตถุประสงค์อย่างไร เพื่อให้องค์กรได้จัดเตรียมการบริหารความเสี่ยง
- ได้รับการสนับสนุนและมีส่วนร่วม จากทุกคนในองค์กรตั้งแต่ระดับกรรมการ ผู้บริหารทุกระดับ และเจ้าหน้าที่ทุกคน

๗. องค์ประกอบการบริหารความเสี่ยง

การบริหารความเสี่ยง เป็นกระบวนการที่ดำเนินการอย่างต่อเนื่องภายในองค์การ และควรถูกรวมกับกิจกรรมปกติทางธุรกิจ เพื่อให้องค์การสามารถดำเนินการตามกลยุทธ์ที่กำหนด เพื่อให้บรรลุพันธกิจและวัตถุประสงค์ที่ต้องการ

กระบวนการ ๘ ขั้นตอนหลักประกอบด้วย

๑. สภาพแวดล้อมภายในองค์กร แนวนโยบายโดยทั่วไปของสำนักงาน ซึ่งเป็นพื้นฐานที่สำคัญของกรอบการบริหารความเสี่ยง และการจัดการกับความเสี่ยง

๒. การกำหนดวัตถุประสงค์และเป้าหมาย ที่สอดคล้องกับกลยุทธ์ สรอ.

๓. การระบุเหตุการณ์ การบ่งชี้และเข้าใจความเสี่ยงทั้งหมดที่มีผลกระทบต่อวัตถุประสงค์ที่กำหนดไว้

๔. การประเมินความเสี่ยง โดยพิจารณาถึงผลกระทบและโอกาสเกิดความเสี่ยง

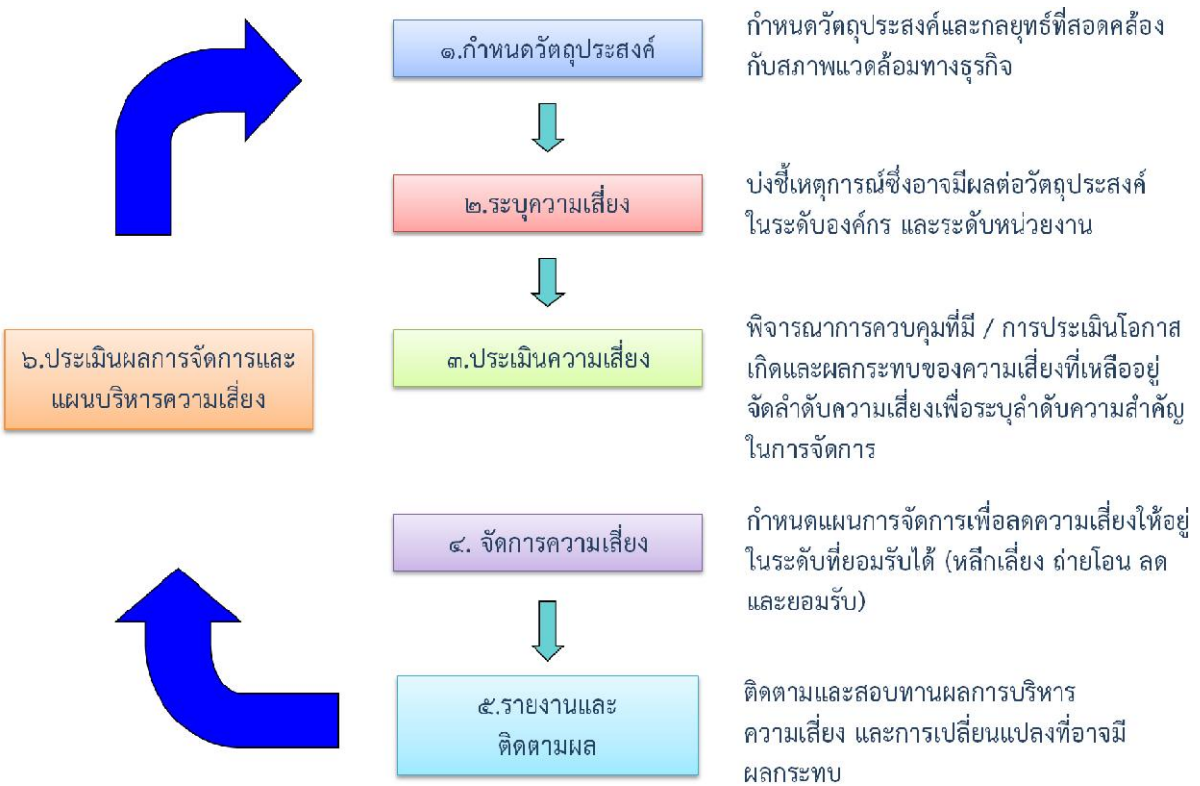
๕. การตอบสนองความเสี่ยง กำหนดการจัดการความเสี่ยงที่ปฏิบัติอยู่ในปัจจุบัน

๖. กิจกรรมการควบคุม โดยพิจารณาถึงการควบคุมเพิ่มเติมรวมทั้งความสัมพันธ์ของต้นทุนและผลประโยชน์ที่เกิดขึ้น ผู้บริหารควรนำวิธีการจัดการความเสี่ยงไปปฏิบัติและติดตาม เพื่อให้มั่นใจได้ว่ามีการดำเนินการตามวิธีการที่กำหนดไว้ กิจกรรมการควบคุม คือนโยบายและขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง

๗. สารสนเทศและการสื่อการ การสื่อสารเพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่ มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง

๘. การติดตามผลและรายงานความมีประสิทธิผลของกระบวนการและระบบการบริหารความเสี่ยง

ทั้งนี้ กระบวนการของการบริหารความเสี่ยง ๘ ขั้นตอน เพื่อการนำเอาขั้นตอนทั้ง ๘ ไปปฏิบัติ มีรายละเอียดดังนี้



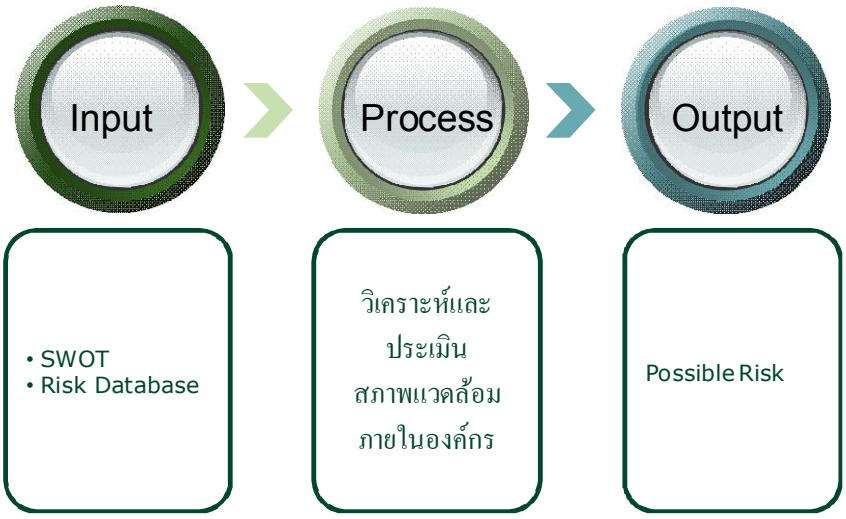
๗.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมภายในองค์กรครอบคลุมถึงแนวนโยบายโดยทั่วไปของสำนักงาน ซึ่งเป็นพื้นฐานที่สำคัญของกรอบการบริหารความเสี่ยง และการจัดการกับความเสี่ยงโดยผู้บริหาร เจ้าหน้าที่และลูกจ้างทั้งหมดในสำนักงาน ซึ่งมีอิทธิพลต่อความตระหนักถึงความเสี่ยงของบุคลากรของสำนักงาน และช่วยก่อให้เกิดแนวทางการบริหารความเสี่ยงของสำนักงาน

สภาพแวดล้อมภายในองค์กร เป็นพื้นฐานสำคัญขององค์ประกอบอื่นของการบริหารความเสี่ยงองค์กร และช่วยก่อให้เกิดแนวทางปฏิบัติและโครงสร้างของการบริหารความเสี่ยงขององค์กร โดยการวิเคราะห์สภาพแวดล้อมภายในองค์กร จะมีผลต่อการประเมินและการดำเนินการในการกำหนดกลยุทธ์และวัตถุประสงค์ขององค์กร การกำหนดกิจกรรมทางธุรกิจ และการระบุความเสี่ยง

การวิเคราะห์และประเมินสภาพแวดล้อมภายในองค์กร ควรครอบคลุมถึงแนวนโยบายทั่วไปขององค์กร ซึ่งเป็นพื้นฐานของการพิจารณาความเสี่ยงและการจัดการความเสี่ยงโดยบุคลากรทั้งหมดในองค์กร องค์ประกอบสำคัญที่มีผลต่อสภาพแวดล้อมในองค์กร ได้แก่ ค่านิยมและความเชื่อ ศักยภาพและการพัฒนาของบุคลากร รูปแบบการบริหารจัดการของฝ่ายบริการ วิธีการมอบอำนาจหน้าที่ความรับผิดชอบ ลักษณะโครงสร้างขององค์กร ตลอดจนพฤติกรรมที่คนในองค์กรยึดถือเพื่อเป็นแนวทางในการปฏิบัติงาน

สามารถแสดงองค์ประกอบที่เกี่ยวข้องในการวิเคราะห์และประเมินสภาพแวดล้อมภายในองค์กร ได้ดังนี้



จากแผนภาพดังกล่าว เพื่อให้การวิเคราะห์สภาพแวดล้อมภายในองค์กร สะท้อนการดำเนินธุรกิจได้ชัดเจนขึ้น จึงควรพิจารณาให้ครอบคลุมถึงปัจจัยภายในและภายนอกที่อาจมีผลกระทบต่อองค์กร ตลอดจนวิเคราะห์จากฐานข้อมูลความเสี่ยงองค์กร ดังนี้

- ปัจจัยภายใน เช่น โครงสร้างองค์กร กระบวนการและวิธีปฏิบัติงาน วัฒนธรรมองค์กร ความสามารถในการแข่งขัน ปรัชญาการบริหารความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้ของผู้บริหาร

- ปัจจัยภายนอก เช่น ภาวะเศรษฐกิจ การเมืองทั้งในประเทศและต่างประเทศ การแข่งขันทางธุรกิจ ลักษณะของตลาดและความสามารถของคู่เทียบ ความก้าวหน้าทางเทคโนโลยี กฎเกณฑ์การกำกับดูแลของหน่วยงานที่เกี่ยวข้อง

๗.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

สำนักงานต้องกำหนดให้หน่วยงานทุกระดับมีการกำหนดวัตถุประสงค์และเป้าหมายการดำเนินงานที่สอดคล้องกับวิสัยทัศน์ พันธกิจ กลยุทธ์ และเป้าหมายโดยรวมของสำนักงาน โดยต้องมีความชัดเจน สามารถวัดหรือประเมินผลได้

ในการกำหนดวัตถุประสงค์ ควรกำหนดให้ครอบคลุมแต่ละประเภทของวัตถุประสงค์ ดังต่อไปนี้

- วัตถุประสงค์ด้านกลยุทธ์ คือ วัตถุประสงค์ระดับนโยบายขององค์กร โดยสอดคล้องกับวิสัยทัศน์และพันธกิจขององค์กรโดยรวม ซึ่งมุ่งสู่การบรรลุเป้าหมายขององค์กรในภาพรวม

- วัตถุประสงค์ด้านปฏิบัติการ คือ วัตถุประสงค์ที่เกี่ยวข้องกับประสิทธิภาพและประสิทธิผลของการปฏิบัติการ

- วัตถุประสงค์ด้านการเงิน คือ วัตถุประสงค์ที่เกี่ยวข้องกับการบริหารการเงินขององค์กรในทุกด้าน ได้แก่ ประสิทธิภาพในการเบิกจ่ายงบลงทุน ประสิทธิภาพในการบริหารค่าใช้จ่ายความน่าเชื่อถือและความทันเวลาของการรายงานข้อมูลทางการเงินและข้อมูลที่ไม่ใช่ทางการเงิน ทั้งจากภายในและภายนอกองค์กร

- วัตถุประสงค์ด้านการปฏิบัติตามกฎระเบียบ คือ วัตถุประสงค์ที่เกี่ยวข้องกับการปฏิบัติตามกฎหมายและกฎระเบียบต่างๆการปฏิบัติตามกฎระเบียบเกี่ยวข้อง

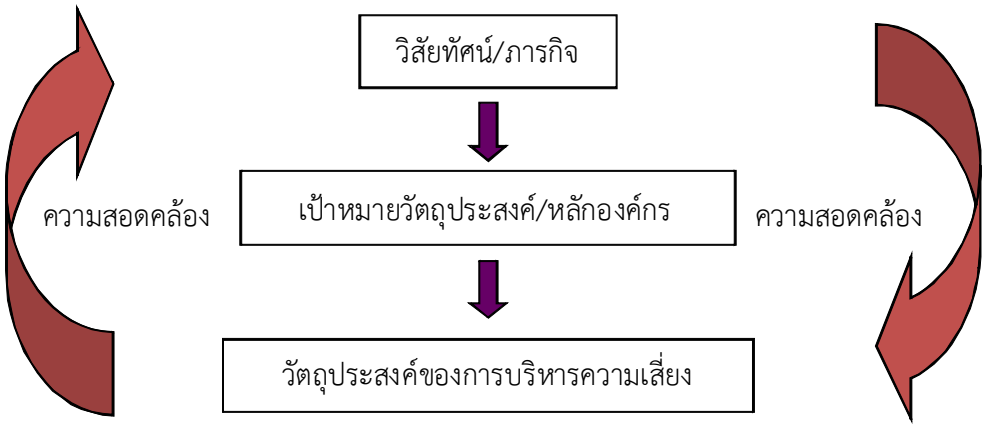
<u>ความสอดคล้องของวัตถุประสงค์</u>

วัตถุประสงค์ต้องมีความสอดคล้องทั่วทั้งองค์กร เพื่อให้เกิดความมั่นใจว่า หน่วยงาน ผู้บริหาร และเจ้าหน้าที่ ดำเนินการเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

วิสัยทัศน์เป็นจุดเริ่มต้นในการกำหนดทิศทางขององค์กร ผู้บริหารระดับสูงจะทำการกำหนดวัตถุประสงค์ระดับองค์กรขึ้นในการจัดทำแผนประจำปี แต่ละหน่วยงานดำเนินการกำหนดวัตถุประสงค์ของหน่วยงานให้

สอดคล้องกับวัตถุประสงค์ที่องค์กรได้กำหนดไว้ และการกำหนดวัตถุประสงค์ของกระบวนการและโครงการต่างๆ ต้องคำนึงถึงความสอดคล้องกับวัตถุประสงค์ของหน่วยงานและระดับองค์กร

วัตถุประสงค์อาจเกี่ยวข้องกับองค์การในหลายๆ ด้าน รวมไปถึง ทรัพยากร เทคโนโลยีสารสนเทศ ผลการดำเนินการ ด้านปฏิบัติการ เป็นต้น



๗.๓ การระบุเหตุการณ์ (Event Identification)

คือ การระบุเหตุการณ์ความเสี่ยงหรือความไม่แน่นอนที่อาจเกิดขึ้น โดยพิจารณาจากปัจจัยทั้งภายในและภายนอกสำนักงาน ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของสำนักงาน

ประเภทความเสี่ยง ความเสี่ยงแบ่งออกเป็น ๔ ด้าน ดังนี้

๑. **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)** เป็นความเสี่ยงที่เกิดจากการกำหนดกลยุทธ์ หรือนโยบายการบริหารงาน ทำให้องค์กรไม่สามารถบรรลุกลยุทธ์และเพิ่มมูลค่าให้องค์กรได้ เช่น นโยบายไม่สอดคล้องกับความต้องการของตลาด โครงสร้างองค์กรที่ปรับเปลี่ยน ผลงานวิจัยไม่สามารถนำมาใช้ประโยชน์ได้ เป็นต้น

๒. **ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)** เป็นความเสี่ยงที่เกิดจากการปฏิบัติงานปกติในทุก ๆ ขั้นตอนโดยเกี่ยวข้องกับ กระบวนการในการปฏิบัติงาน อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากร ซึ่งส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินธุรกิจขององค์กร เช่น โครงการล่าช้า ขาดอุปกรณ์หรือเครื่องมือที่มีประสิทธิภาพ ขาดการติดตามการบริหารสัญญา บุคลากรขาดแรงจูงใจในการปฏิบัติงาน เป็นต้น

๓. **ความเสี่ยงด้านการเงิน (Financial Risk)** เป็นความเสี่ยงจากการขาดข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงานเพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้อง เหมาะสม ส่งผลต่อสถานะทางการเงินขององค์กร เช่น แผนการลงทุนไม่มีความชัดเจนเพียงพอ ที่จะนำไปใช้ในการวิเคราะห์เพื่อคาดการณ์ด้านการเงินได้ สภาพคล่องทางการเงิน อัตราแลกเปลี่ยน ดอกเบี้ย ไม่มีแหล่งรายได้ใหม่ เป็นต้น

๔. ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk) เป็นความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงานได้ กฎระเบียบหรือกฎหมายที่มีอยู่ไม่เหมาะสมเป็นอุปสรรคต่อการปฏิบัติงาน นโยบายและวิธีการปฏิบัติงานที่องค์กรกำหนดขึ้นไม่สามารถปฏิบัติได้ เช่น ความสับสนในการเลือกกฎระเบียบหรือกฎหมายที่จะบังคับใช้ เนื่องจากกฎระเบียบหรือกฎหมายหลายฉบับที่สามารถอ้างถึงและบังคับใช้ในกรณีหนึ่งๆ เป็นต้น

ความเสี่ยงของแผนงาน/โครงการ ตามมติคณะรัฐมนตรีวันที่ ๒๒ เมษายน ๒๕๕๑ ได้เห็นชอบในหลักเกณฑ์และแนวทางคัดเลือกแผนงาน/โครงการที่สำคัญตามนโยบายรัฐบาล เพื่อให้มีการวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล เพื่อให้ส่วนงาน รัฐวิสาหกิจ และหน่วยงานอื่น ของรัฐใช้เป็นมาตรฐานเดียวกันทุกหน่วยงาน

โดยได้กำหนดแนวทางการวิเคราะห์ความเสี่ยงของแผนงาน/โครงการตามหลักธรรมาภิบาล มี ๑๐ ประเภท ได้แก่

๑. **ความเสี่ยงต่อหลักประสิทธิผล (Effectiveness)** ต้องมีวิสัยทัศน์เชิงยุทธศาสตร์ เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกฝ่าย ปฏิบัติตามหน้าที่ตามพันธกิจให้บรรลุวัตถุประสงค์ขององค์กร มีการวางเป้าหมายการปฏิบัติงานที่ชัดเจน และอยู่ในระดับที่ตอบสนองต่อความคาดหวังของประชาชน สร้างกระบวนการปฏิบัติงานอย่างเป็นระบบและมีมาตรฐาน มีการ

จัดการความเสี่ยงและมุ่งเน้นผลการปฏิบัติงานที่เป็นเลิศ รวมถึงมีการติดตามประเมินผล และพัฒนาปรับปรุงการปฏิบัติงานให้ดีขึ้นอย่างต่อเนื่อง

๒. **ความเสี่ยงต่อหลักประสิทธิภาพ (Efficiency)** ในการปฏิบัติงานต้องมีการใช้ทรัพยากรอย่างประหยัด เกิดผลิตภาพ คุ้มค่าการลงทุนและบังเกิดประโยชน์สูงสุดต่อส่วนรวม รวมทั้งต้องมีการลดขั้นตอนและระยะเวลาในการปฏิบัติงาน เพื่ออำนวยความสะดวกและลดภาระค่าใช้จ่าย ตลอดจนยกเลิกภารกิจที่ล้าสมัย และไม่มีความจำเป็น

๓. **ความเสี่ยงต่อหลักการมีส่วนร่วม (Participation)** ต้องรับฟังความคิดเห็นของประชาชน รวมทั้งเปิดให้ประชาชนมีส่วนร่วมในการรับรู้ เรียนรู้ ทำความเข้าใจ รวมทั้งแสดงทัศนะ ร่วมเสนอปัญหา/ประเด็นสำคัญที่เกี่ยวข้อง ร่วมคิดแก้ไขปัญหา ร่วมในกระบวนการตัดสินใจและการดำเนินงาน และร่วมตรวจสอบผลการปฏิบัติงาน

๔. **ความเสี่ยงต่อหลักความโปร่งใส (Transparency)** ต้องปฏิบัติงานด้วยความซื่อสัตย์สุจริต ตรงไปตรงมา ร่วมทั้งต้องมีการเปิดเผยข้อมูลข่าวสารที่จำเป็นและเชื่อถือได้ ให้ประชาชนได้รับทราบอย่างสม่ำเสมอ ตลอดจนวางระบบให้การเข้าถึงข้อมูลข่าวสารเป็นไปโดยง่าย

๕. **ความเสี่ยงต่อหลักการตอบสนอง (Responsivenss)** ต้องสามารถให้บริการได้อย่างมีคุณภาพ สามารถดำเนินการแล้วเสร็จภายในระยะเวลาที่กำหนด สร้างความเชื่อมั่นไว้วางใจ รวมถึงตอบสนองตามความคาดหวัง/ความต้องการของประชาชนผู้รับบริการ และผู้มีส่วนได้ส่วนเสียที่มีความหลากหลายและมีความแตกต่างกันได้อย่างเหมาะสม

๖. **ความเสี่ยงต่อหลักภาระรับผิดชอบ (Acountability)** ในการปฏิบัติงานต้องสามารถตอบคำถามและชี้แจงได้เมื่อมีข้อสงสัย รวมทั้งต้องมีการจัดวางระบบการรายงานความก้าวหน้า และผลสัมฤทธิ์ตามเป้าหมายที่กำหนดไว้ต่อสาธารณะ เพื่อประโยชน์ในการตรวจสอบและการให้คุณให้โทษ ตลอดจนมีการจัดเตรียมระบบการแก้ไขหรือบรรเทาปัญหา และผลกระทบใดๆ ที่อาจจะเกิดขึ้น

๗. **ความเสี่ยงต่อหลักนิติธรรม (Rule of Law)** ต้องใช้อำนาจของกฎหมาย กฎระเบียบ ข้อบังคับในการปฏิบัติงานอย่างเคร่งครัด ด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของประชาชน และผู้มีส่วนได้ส่วนเสียฝ่ายต่างๆ

๘. **ความเสี่ยงต่อหลักการกระจายอำนาจ (Decentralization)** ในการปฏิบัติงานควรมีการมอบอำนาจและกระจายความรับผิดชอบในการตัดสินใจและการดำเนินการให้แก่ผู้ปฏิบัติงานในระดับต่างๆ ได้อย่างเหมาะสม รวมทั้งมีการโอนถ่ายบทบาท และภารกิจให้แก่องค์กรปกครองส่วนท้องถิ่นหรือภาคส่วนอื่นๆ ในสังคม

๙. **ความเสี่ยงต่อหลักความเสมอภาค (Equity)** ต้องให้บริการอย่างเท่าเทียมกัน ไม่มีการแบ่งแยกด้านชาย/หญิง ถิ่นกำเนิด เชื้อชาต ภาษา เพศ อายุ สภาพทางกายหรือสุขภาพ สถานะของบุคคล ฐานะทางเศรษฐกิจและสังคม ความเชื่อทางศาสนา การศึกษาอบรม และอื่นๆ นอกจากนี้ยังต้องคำนึงถึงโอกาสความทัดเทียมกันของการเข้าถึงบริการสาธารณะ ของกลุ่มบุคลลผู้ด้อยโอกาสในสังคม

๑๐. **ความเสี่ยงต่อหลักการมุ่งเน้นฉันทามติ (Consensus Oriented)** ในการปฏิบัติงานต้องมีกระบวนการในการแสวงหาฉันทามติ หรือข้อตกลงร่วมกัน ระหว่างกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องโดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง จะต้องไม่มีข้อคัดค้าน ที่หาข้อยุติไม่ได้ ในประเด็นที่สำคัญ

จากแนวคิดธรรมภิบาลที่เกี่ยวข้อง สามารถแสดงความเชื่อมโยง ต่อปัจจัยในการวิเคราะห์ความเสี่ยง เช่น

- ด้านนโยบายและกลยุทธ์ โครงการที่คัดเลือกมานั้น อาจมีความเสี่ยงต่อเรื่องประสิทธิผลและการมีส่วนร่วม
- ด้านปฏิบัติงาน อาจมีความเสี่ยงต่อเรื่องประสิทธิภาพและความโปร่งใส
- ด้านการเงิน อาจมีความเสี่ยงต่อเรื่องนิติธรรมและภาระรับผิดชอบ
- ด้านกฎหมาย กฎระเบียบ อาจมีความเสี่ยงต่อเรื่องนิติธรรมและความเสมอภาค

ทั้งนี้สามารถอธิบายความสัมพันธ์ ตามตารางด้านล่างได้ดังนี้

	หลักประสิทธิผล Effectiveness	หลักประสิทธิภาพ Efficiency	หลักการมีส่วนร่วม Participation	หลักความโปร่งใส Transparency	หลักการตอบสนอง Responsiveness	หลักภาระรับผิดชอบ Accountability	หลักนิติธรรม Rule of Law	หลักการกระจายอำนาจ Decentralization	หลักความเสมอภาค Equity	หลักการมุ่งเน้นฉันทามติ Consensus Oriented
Strategic Risk	✓		✓		✓	✓				
Operational Risk	✓	✓	✓	✓	✓				✓	✓
Financial Risk	✓	✓		✓		✓	✓			
Compliance Risk	✓	✓			✓		✓		✓	

๗.๔ การประเมินความเสี่ยง (Risk Assessment)

สำนักงานต้องกำหนดให้หน่วยงานทุกระดับประเมินความเสี่ยงของทุกปัจจัยเสี่ยงที่ได้ระบุไว้ โดยอ้างอิงจากเกณฑ์วัดระดับความเสี่ยง โอกาสและผลกระทบ ที่สำนักงานกำหนดไว้ โดยอาจใช้ฐานข้อมูลในอดีตหรือการคาดการณ์ในอนาคตเพื่อประกอบการประเมินระดับความเสี่ยง

การประเมินความเสี่ยงควรพิจารณาถึงความไม่แน่นอนของเหตุการณ์หรือเงื่อนไขต่างๆ ใน ๒ ปัจจัย ดังต่อไปนี้

- ผลกระทบ ที่อาจจะเกิดขึ้นจากความเสี่ยง
- โอกาสเกิด ของความเสี่ยง

ผลกระทบ (Impact)

การประเมินความเสี่ยงควรพิจารณาถึงผลกระทบทั้งทางด้านการเงิน และที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ผลกระทบสามารถวัดได้ในเชิงของการสูญเสียทางการเงินทั้งทางตรงและทางอ้อม การวัดผลการดำเนินงานที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ความพึงพอใจของผู้มีส่วนได้ส่วนเสีย สภาพแวดล้อมและสังคม เป็นต้น

การประเมินผลกระทบของปัจจัยเสี่ยง ควรครอบคลุมทั้งการกำหนดผลกระทบในเชิงการเงินและผลกระทบที่มิใช่ทางการเงิน อย่างไรก็ตาม บางปัจจัยเสี่ยงอาจไม่สามารถกำหนดผลกระทบในเชิงการเงินที่ชัดเจนได้ ดังนั้นในการประเมินความเสี่ยงเบื้องต้นจึงพิจารณาผลกระทบที่เกิดจากความเสี่ยงในเชิงคุณภาพเป็นส่วนใหญ่ โดยเมื่อพิจารณาระดับความรุนแรงของผลกระทบแล้วนั้น ความเสี่ยงที่มีผลกระทบมากหรือมีโอกาสเกิดสูง จำเป็นต้องได้รับการพิจารณาจากผู้บริหารระดับสูงมาก และทันท่วงที โดยกำหนดแผนการบริหารความเสี่ยงที่ท้าทาย และติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ

ตารางด้านล่างแสดงถึงตัวอย่างของผลกระทบที่เกิดจากความเสี่ยงในแบบต่างๆ

ประเภทของผลกระทบ	ตัวอย่าง
การเงิน	การลดลงหรือความล่าช้าในการบรรลุเป้าหมายทางรายได้ กำไร สุทธิ กระแสเงินสด หรือสินทรัพย์รวม
กลยุทธ์	การไม่บรรลุวัตถุประสงค์ขององค์การหรือสายงาน
ทรัพยากรบุคคล	การลาออกของเจ้าหน้าที่ การสูญเสียเจ้าหน้าที่หลัก หรือปัญหาด้านจริยธรรม
ชื่อเสียง	การเผยแพร่ข่าวที่เสียหายขององค์การในสื่อต่างๆ เช่น หนังสือพิมพ์ โทรทัศน์ เป็นต้น

ประเภทของผลกระทบ	ตัวอย่าง
ระบบเทคโนโลยีและสารสนเทศ	ระบบเทคโนโลยีและสารสนเทศล้มเหลว หรือการละเมิดความปลอดภัยของข้อมูล องค์การ
กฎระเบียบ ข้อบังคับ	การละเมิดกฎระเบียบ
การต่อเนื่องของการดำเนินธุรกิจ	การหยุดชะงักของกระบวนการและการดำเนินการทางธุรกิจ

โอกาสเกิด (Likelihood)

การประเมินโอกาสเกิดของความเสี่ยง โดยทั่วไปการหาข้อมูลมาทำการสนับสนุนการประมาณการที่ถูกต้องเป็นไปได้ยาก ในกรณีที่สามารถหาข้อมูลที่เกี่ยวกับเหตุการณ์ความล้มเหลวหรือความถี่ที่เกิดขึ้นในอดีต ต้องมีความมั่นใจในฐานข้อมูลดังกล่าวว่าสามารถบ่งชี้ถึงความเป็นไปได้ของเหตุการณ์ในอนาคตได้

การประเมินโอกาสเกิดขึ้นอยู่กับระยะเวลาที่นำมาพิจารณา ดังนั้นแล้ว เมื่อทำการประเมินโอกาสเกิด ผู้บริหารต้องมีความชัดเจนในการกำหนดระยะเวลาที่จะใช้ในการพิจารณา โดยไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นได้ในระยะยาว

ประโยชน์ของผู้บริหารที่ได้จากการประเมินความเสี่ยงมีดังต่อไปนี้

- การเปรียบเทียบความเสี่ยงกับกลยุทธ์และนโยบายขององค์กร
- กลยุทธ์และนโยบายขององค์กรจัดอยู่ในทิศทางใด กลยุทธ์และนโยบายดังกล่าวยอมรับความเสี่ยงที่เกิดขึ้นได้มากน้อยเพียงใด รวมถึงความเสี่ยงที่สามารถระบุได้นั้น มีความสอดคล้องกับกลยุทธ์และนโยบายขององค์กรเพียงใด
- การบ่งชี้ถึงความเสี่ยงที่ไม่เป็นที่ยอมรับ
- องค์กรสามารถกำหนดระดับความเสี่ยงที่ยอมรับได้ และระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้หรือไม่ และการกำหนดดังกล่าว เป็นการกำหนดโดยภาพรวมหรือเป็นการกำหนดในรายปัจจัยเสี่ยง
- การคัดเลือกและจัดลำดับการดำเนินการที่เหมาะสมในการลดความเสี่ยง

จากประเด็นดังกล่าว แสดงให้เห็นถึงความสำคัญของการกำหนดระดับความเสี่ยงที่ยอมรับได้ และระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ขององค์กร ซึ่ง

ความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้ โดยธุรกิจยังคงดำเนินการได้บรรลุตามเป้าหมาย

ความเสี่ยงที่ยอมรับได้กำหนดขึ้นเพื่อใช้เป็นแนวทางกำหนดกลยุทธ์ขององค์กร ทั้งนี้ความเสี่ยงที่ยอมรับได้ควรได้รับการกำหนดโดยผู้บริหารและอนุมัติโดยคณะกรรมการ การกำหนดความเสี่ยงที่ยอมรับได้ควรพิจารณาถึงความสมดุลระหว่างการเติบโต ความเสี่ยงและผลตอบแทนขององค์กร ในขณะเดียวกันองค์กรควรบริหารความเสี่ยงที่เกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้

ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) คือ ระดับความเบี่ยงเบนจากวัตถุประสงค์ที่ยอมรับได้

การดำเนินธุรกิจภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ทำให้ผู้บริหารมั่นใจได้ว่า การดำเนินงานขององค์กร อยู่ภายในเกณฑ์หรือประเภทของความเสี่ยงที่ยอมรับได้ (Risk Appetite) ซึ่งมีผลให้คณะกรรมการและผู้บริหารขององค์กรมีความมั่นใจมากขึ้นว่าการดำเนินการขององค์กร จะสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ได้

<u>การจัดลำดับความเสี่ยง</u>

ผู้บริหารระดับสูงควรกำหนดเงื่อนไขที่ใช้ในการจัดลำดับความเสี่ยง และควรมีการสอบทานการจัดลำดับความเสี่ยงเป็นประจำ เพื่อให้สอดคล้องกับเงื่อนไขทางธุรกิจที่เปลี่ยนไป ขั้นตอนในการจัดลำดับความเสี่ยงมีดังต่อไปนี้

<u>การกำหนดระดับของผลกระทบ</u>

- กำหนดเงื่อนไขที่จะใช้ในการพิจารณา

  - พิจารณาทั้งเงื่อนไขทางการเงินและเงื่อนไขอื่นๆ ที่ไม่เกี่ยวข้องกับการเงิน เช่น ยอดขาย ผลตอบแทนทางการเงิน ผลกำไร ชื่อเสียง ความสามารถในการบรรลุวัตถุประสงค์ อัตราการลาออกของเจ้าหน้าที่ ความปลอดภัยในชีวิตและทรัพย์สิน และระบบเทคโนโลยีสารสนเทศ

  - ทำให้มั่นใจได้ว่าเงื่อนไขนั้นสอดคล้องกับวัตถุประสงค์ขององค์กร

- กำหนดมูลค่าของผลกระทบให้กับระดับคะแนน ๑, ๒, ๓, ๔ และ ๒๕ ในการจัดลำดับ โดยระดับคะแนนนี้อาจมีการเปลี่ยนแปลงได้ ขึ้นอยู่กับความเหมาะสมกับสถานการณ์ในขณะนั้น

- ทำให้มั่นใจว่ามูลค่าต่างๆ ที่กำหนดเพื่อใช้ในการจัดลำดับสำหรับเงื่อนไขที่ต่างกันมีความสอดคล้องกัน ดังตัวอย่าง ระดับผลกระทบ ๓ ของผลกระทบทางการเงิน สามารถเทียบเท่ากับระดับคะแนน ๓ ของเงื่อนไขด้านสิ่งแวดล้อม เป็นต้น

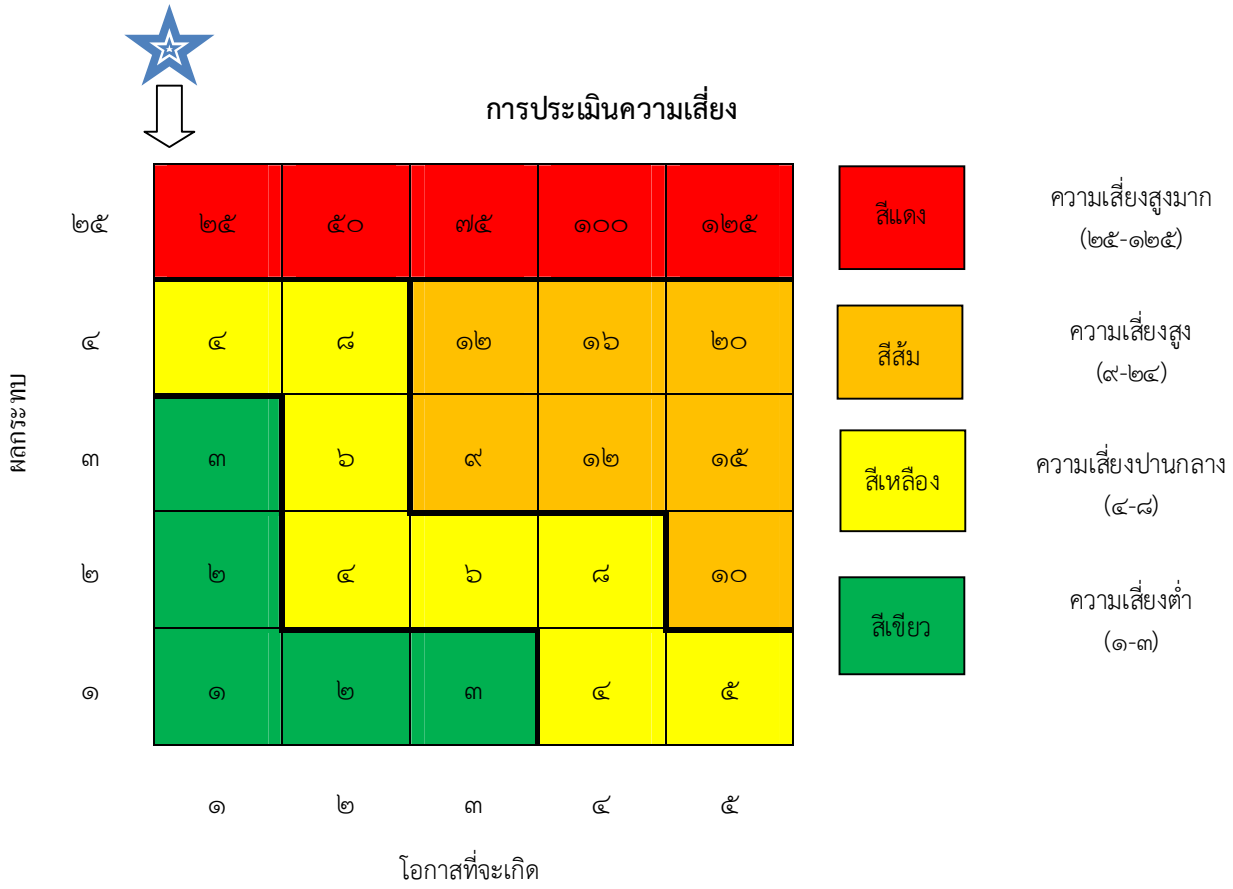
การกำหนดระดับของโอกาสเกิด

- กำหนดช่วงเวลาที่ชัดเจนสำหรับการพิจารณาโอกาสเกิด อย่างไรก็ตาม ไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นในระยะยาว

- ประยุกต์คำอธิบายในแต่ละคะแนน โดยระดับคะแนนนี้สามารถเปลี่ยนแปลงได้เช่นเดียวกับระดับคะแนนของผลกระทบ ขึ้นอยู่กับความเหมาะสมกับสถานการณ์ในขณะนั้น

แนวทางการพิจารณาความมีนัยสำคัญของความเสี่ยง

การประเมินความเสี่ยง สามารถทำได้โดยการอ้างอิงกับตารางแสดงการจัดลำดับความเสี่ยง การพิจารณาว่าความเสี่ยงใดมีนัยสำคัญ ที่ต้องนำมาดำเนินการก่อนหลัง โดยทั่วไปอาจใช้การกำหนดค่าลำดับความเสี่ยงทั้งในด้านของผลกระทบและโอกาสเกิด ทั้งนี้ การกำหนดนัยสำคัญของความเสี่ยงขององค์กร ควรได้รับการพิจารณาจากผู้บริหารระดับสูงและผ่านความเห็นชอบจากคณะกรรมการบริหารความเสี่ยงองค์กร หลังจากการประเมินความมีนัยสำคัญของความเสี่ยงเพื่อนำมาใช้ในการกำหนดกลยุทธ์การจัดการความเสี่ยงต่างๆ ควรคำนึงถึงประสิทธิผลของต้นทุนที่ต้องใช้ในการจัดการความเสี่ยงนั้นๆ กับระดับความสำคัญของความเสี่ยงที่ลดลงว่าเหมาะสมเพียงใด ทั้งนี้ความมีประสิทธิผลของการจัดการความเสี่ยงอาจประเมินได้ในเชิงของการลดลงของโอกาสเกิดและผลกระทบ



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

๗.๕ การตอบสนองความเสี่ยง (Risk Response)

เป็นการระบุว่ามีทางเลือกใดบ้างที่สามารถใช้ในการจัดการความเสี่ยง มีความเหมาะสม และนำไปปฏิบัติเป็นส่วนหนึ่งของการบริหารความเสี่ยงของสำนักงาน ซึ่งจะต้องประเมินผลกระทบที่มีต่อโอกาสที่จะเกิดรวมทั้งต้นทุนและประโยชน์ที่ได้รับ เพื่อให้ความเสี่ยงที่เหลืออยู่ภายในช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ ทั้งนี้ การตอบสนองต่อความเสี่ยงแบ่งเป็น ๔ ประการ คือ การยอมรับ (Accept) การลด (Reduce) การหลีกเลี่ยง/ยกเลิก (Avoid/Terminate) และการโอนความเสี่ยง (Transfer)

สำนักงานต้องจัดให้มีการควบคุมความเสี่ยงและเพดานความเสี่ยงที่เพียงพอและเหมาะสมตามแต่ละประเภทความเสี่ยงและต้องอยู่ภายใต้ระดับความเสี่ยงที่สำนักงานยอมรับได้ รวมทั้งสอดคล้องกับมาตรฐานและหลักเกณฑ์ของหน่วยงานกำกับดูแล แนวทางปฏิบัติที่ดี ตลอดจนนโยบายบริหารความเสี่ยงกับทิศทางและกลยุทธ์

การดำเนินงานของสำนักงาน พร้อมทั้งกำหนดกระบวนการปฏิบัติตามการควบคุมความเสี่ยงและเพดานความเสี่ยงที่กำหนดไว้ แนวทางการอนุมัติข้อยกเว้นกรณีจำเป็นหรือเหตุการณ์ไม่ปกติต่าง ๆ รวมถึงการทบทวนการควบคุมความเสี่ยงและเพดานความเสี่ยงดังกล่าวเป็นระยะ เพื่อให้มีประสิทธิภาพในการควบคุมและป้องกันความเสี่ยงให้กับสำนักงาน

ผู้บริหารต้องประเมินว่าปัจจุบันการจัดการความเสี่ยงเพียงพอหรือไม่ ทั้งประสิทธิภาพในการลดโอกาสเกิดความเสี่ยง และผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงต่างๆ หากไม่มีการจัดการความเสี่ยง หรือการจัดการในปัจจุบันไม่เพียงพอ ควรมีการพิจารณากิจกรรมอื่นๆ เพิ่มเติมให้เหมาะสมและนำไปปฏิบัติ

<u>วัตถุประสงค์ของการจัดการความเสี่ยง</u>

- ลดโอกาสในการเกิดและผลกระทบของความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้โดยการจัดการสาเหตุของความเสี่ยงอย่างมีประสิทธิภาพ หรือโดยการจัดการผลกระทบที่อาจจะเกิดขึ้นของความเสี่ยง เช่น การมีเจ้าหน้าที่ปฏิบัติการที่พร้อมซ่อมแซมความเสียหายที่เกิดขึ้น เป็นต้น

- การลดผลกระทบของความเสี่ยง ซึ่งโดยมากมักใช้ระบบการเตือนภัย หรือระบบการบริหาร พร้อมด้วยการจัดทำแผนฉุกเฉิน หรือแผนฟื้นฟู

- การเพิ่มโอกาสในการเกิด หรือผลกระทบจากความเสี่ยงที่เป็นโอกาสให้มากที่สุด โดยการปฏิบัติเพื่อสร้างหรือหาโอกาส หรือการจัดการเพื่อให้ได้ผลลัพธ์ที่ดีขึ้น

<u>กลยุทธ์ในการบริหารความเสี่ยง</u>

การยอมรับความเสี่ยง (Accept) ความเสี่ยงหลังการควบคุมอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใดๆ เพิ่มเติมที่มีผลต่อโอกาสเกิด หรือผลกระทบของความเสี่ยง

- ตั้งใจที่จะดำเนินการต่อไป
- ยอมรับทั้งหมด
- กำหนดรางวัล/เป้าหมายความเสียหาย และระดับการยอมรับ
- กำหนด และติดตามตัวบ่งชี้ความเสี่ยงที่สำคัญ
- คิดราคาสูงขึ้น
- กิจกรรมการตรวจสอบและติดตาม
- จัดหาเงินทุนสำรองเพื่อรองรับผลที่อาจเกิดขึ้น
- จัดเตรียมแผนรองรับการเสื่อมถอย (fall-back)

การลดความเสี่ยง (Reduction) การดำเนินการเพิ่มเติมเพื่อลดโอกาสเกิด หรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ตัวอย่างเช่น

- ดำเนินกิจกรรมในเชิงรุกหรือการควบคุมเพื่อลดโอกาสเกิดและผลกระทบ
- การดำเนินการด้านกลยุทธ์ กระบวนการและระบบ
- การพัฒนาบุคลากร ความชำนาญ และโครงสร้างองค์กร
- จัดทำแผนฉุกเฉิน
- พัฒนาแผนฟื้นฟู
- จัดเตรียมแผนรองรับการเสื่อมถอย (fall-back)

การหลีกเลี่ยงความเสี่ยง (Avoid) การดำเนินการเพื่อยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง ทั้งนี้ หากทำการใช้กลยุทธ์นี้อาจต้องทำการพิจารณาวัตถุประสงค์ว่าสามารถบรรลุได้หรือไม่ เพื่อทำการปรับเปลี่ยนต่อไป

- หยุดกิจกรรม
- ออกจากตลาด หรือลดการเสียส่วนแบ่งตลาด
- การลดขนาดการลงทุน
- เปลี่ยน หรือปรับเป้าหมาย
- การออกแบบใหม่ เช่น กระบวนการทางธุรกิจ ระบบ เครื่องมือ

การโอนย้ายความเสี่ยง (Sharing) การโอนย้าย หรือการแบ่งความเสี่ยงบางส่วนกับบุคคลหรือองค์การอื่น

- การประกันภัย
- การร่วมทุน พันธมิตรทางธุรกิจ หุ้นส่วนทางธุรกิจ
- การจ้างบุคคลภายนอก
- การกระจายความเสี่ยง
- การป้องกัน (Hedge)

<u>แนวทางในการกำหนดกลยุทธ์การจัดการความเสี่ยง</u>

กลยุทธ์การจัดการความเสี่ยงถูกกำหนดขึ้นเพื่อลดระดับของความเสี่ยง ทั้งผลกระทบและโอกาสเกิดให้เป็นไปตามระดับความเสี่ยงที่ยอมรับได้ ในบางกรณีการรวมกลยุทธ์การจัดการความเสี่ยง อาจทำให้เกิดผลที่มี

ประสิทธิภาพมากขึ้นทั้งทางด้านต้นทุนและการปฏิบัติงาน ดังนั้น ควรต้องมีการพิจารณาการจัดการความเสี่ยงต่างๆ ที่อาจมีความเกี่ยวข้องกัน และอาจดำเนินการโดยหลายหน่วยงาน รวมทั้งคำนึงถึงต้นทุนที่อาจเกิดขึ้น ในการจัดให้มีการจัดการความเสี่ยงสำหรับกำหนดเป็นกลยุทธ์ในการจัดการความเสี่ยงโดยรวมเพื่อให้เกิดการจัดการความเสี่ยงอย่างเป็นบูรณาการ

ผู้บริหารอาจทำการพิจารณาปัจจัยในการกำหนดกลยุทธ์การจัดการความเสี่ยง ต่อไปนี้

- การประเมินผลกระทบและโอกาสเกิดจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง

ในการประเมินทางเลือกของแต่ละกลยุทธ์การจัดการความเสี่ยง ผู้บริหารต้องมีความเข้าใจว่ากิจกรรมการจัดการความเสี่ยงอาจส่งผลต่อผลกระทบและโอกาสเกิดของความเสี่ยงต่างกัน ดังนั้นแล้ว การประเมินผลกระทบและโอกาสเกิดของความเสี่ยงที่อาจเปลี่ยนแปลงจากการดำเนินการตามกิจกรรมการจัดการความเสี่ยง จึงควรพิจารณาก่อนการตัดสินใจเลือกกลยุทธ์ เพื่อให้ระดับความเสี่ยงสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ขององค์กร ทั้งนี้ การประเมินผลกระทบและโอกาสเกิดหลังจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยงสามารถอ้างอิงข้อมูลได้จากเหตุการณ์ในอดีต แนวโน้มของเหตุการณ์ที่อาจเกิดขึ้น และวิเคราะห์การเปลี่ยนแปลงที่อาจเกิดขึ้นในอนาคต ความเสี่ยงสามารถถูกระบุได้ทั้งอันตรายหรือโอกาสที่อาจเกิดขึ้น การกำหนดกลยุทธ์การจัดการความเสี่ยงจึงสามารถทำได้จากการประเมินปัจจัยหลัก ๒ ประการ ดังนี้

๑. ประเมินต้นทุนและผลตอบแทนของการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง

เนื่องจากทรัพยากรองค์กรมีจำกัด จึงมีความจำเป็นต้องประเมินต้นทุนและผลตอบแทนที่เกิดขึ้นหากมีการดำเนินการตามกิจกรรมการจัดการความเสี่ยง ในกรณีที่พบว่าผลตอบแทนที่ได้จากการดำเนินการที่ได้ไม่คุ้มกับต้นทุนส่วนเพิ่ม ผู้บริหารอาจพิจารณาถึงแนวทางในการโอนย้ายความเสี่ยง (Sharing) เพื่อทำการแบ่งต้นทุนให้หน่วยงานภายนอกรับผิดชอบ เช่น การทำประกันภัย หรือการร่วมทุน เป็นต้น

๒. การประเมินความเป็นไปได้ที่จะประสบผลสำเร็จในการจัดการความเสี่ยง

เนื่องจากกิจกรรมการจัดการความเสี่ยงที่องค์กรจะกำหนดขึ้นนั้น ต้องประกอบด้วยปัจจัยหลายประเภทที่สนับสนุนให้การดำเนินการประสบความสำเร็จ ดังนั้น การประเมินความเป็นไปได้ที่กิจกรรมการจัดการความเสี่ยงจะประสบความสำเร็จจึงมีความจำเป็น โดยควรพิจารณาถึงปัจจัยต่างๆ เช่น ความรู้ความเข้าใจของบุคลากร งบประมาณที่ใช้ในการจัดการ ระยะเวลาแล้วเสร็จ เป็นต้น หากพิจารณาแล้วพบว่ากิจกรรมดังกล่าวมีแนวโน้มที่จะไม่ประสบความสำเร็จ ควรพิจารณาถึงกลยุทธ์การจัดการความเสี่ยงด้วยวิธีการอื่นเพื่อใช้เป็นทางเลือกหรือปรับปรุงแผนการจัดการความเสี่ยงที่มีอยู่ให้เหมาะสมยิ่งขึ้น

หลังจากได้ทำการประเมินเพื่อกำหนดกลยุทธ์การจัดการความเสี่ยงที่มีประสิทธิผลจากแนวทางที่ได้กล่าวมาแล้วข้างต้น ผู้บริหารต้องทำการกำหนดแผนการปฏิบัติงาน (Implementation Plan) หรือขั้นตอนใน

การปฏิบัติ (Procedure) โดยต้องระบุระยะเวลาแล้วเสร็จเพื่อให้มั่นใจได้ว่าจะมีการดำเนินงานตามกลยุทธ์เพื่อให้เกิดโอกาสตามที่คาดหวังไว้จริง และได้รับการดำเนินการโดยเจ้าของความเสี่ยง

- ความรับผิดชอบในการบริหารความเสี่ยง หรือ “การเป็นเจ้าของความเสี่ยง” (Risk Owner) คือ หน่วยงาน หรือบุคคลที่รับผิดชอบให้การดำเนินการจัดการความเสี่ยงบรรลุวัตถุประสงค์หรือประสบความสำเร็จ โดยทั่วไปเจ้าของความเสี่ยงจะต้องรับผิดชอบในการตัดสินใจ เกี่ยวกับแผนการบริหารความเสี่ยง และแผนการปรับปรุงที่เหมาะสมสำหรับความเสี่ยงที่ไม่สามารถยอมรับได้ เมื่อแผนได้ถูกอนุมัติและเห็นชอบแล้วเจ้าของความเสี่ยงจะต้องรับผิดชอบต่อการนำแผนไปปฏิบัติและติดตามผลการดำเนินงานของแผนนั้น และต้องแสดงให้ผู้บริหารเห็นความสำเร็จในการทำหน้าที่ของตนเกี่ยวกับการบริหารความเสี่ยง

- การพัฒนาการจัดการความเสี่ยงสำหรับความเสี่ยงที่ซับซ้อนอาจเกี่ยวข้องกับผู้บริหารระดับสูงและเจ้าหน้าที่ของหลายหน่วยงาน ดังนั้น การสื่อสารที่ดีจึงเป็นสิ่งจำเป็นเพื่อให้แน่ใจว่าบุคคลที่เกี่ยวข้องภายในองค์กรได้ตระหนักถึงสิ่งที่กำลังดำเนินการ และบทบาทที่ต้องเกี่ยวข้องหรือปฏิบัติ

๗.๖ กิจกรรมการควบคุม (Control Activities)

เมื่อมีการเลือกวิธีในการตอบสนองความเสี่ยงที่เหมาะสมแล้ว กิจกรรมการควบคุมความเสี่ยง จะถูกกำหนดขึ้น เพื่อให้มั่นใจได้ว่ามีการจัดการความเสี่ยงอย่างเหมาะสม ซึ่งกิจกรรมการควบคุมเป็นกิจกรรมที่มีอยู่ในทุกหน้าที่ และทุกระดับของการปฏิบัติงานของ สรอ. ซึ่งในการปฏิบัติงานทุกด้านนั้นต้องจัดให้มีกิจกรรมการควบคุมที่เหมาะสมเพียงพอกับระดับความเสี่ยงต่อความผิดพลาดหรือความเสียหายที่อาจเกิดขึ้น ทั้งนี้ประเภทของการควบคุม สามารถจัดกลุ่มได้ดังนี้

การควบคุมแบบป้องกัน (Preventive control) เป็นการควบคุมแบบป้องกันหรือลดความเสี่ยงจากความผิดพลาด ความเสียหาย เช่น การแบ่งแยกหน้าที่ การติดอุปกรณ์เพื่อป้องกันเหตุ

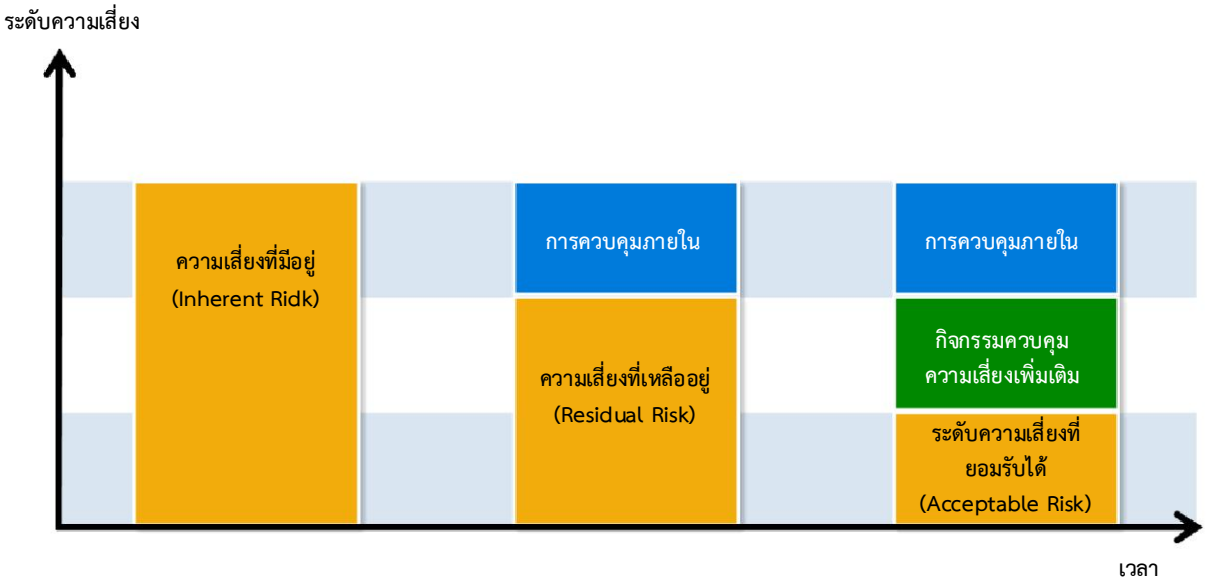
การควบคุมแบบค้นหา (Detective control) เป็นการควบคุมเพื่อค้นหาความผิดพลาดหรือความเสียหายที่เกิดขึ้นแล้ว เช่น การตรวจนับ การสอบทานงาน

การควบคุมแบบแก้ไข (Corrective control) เป็นวิธีควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เคยเกิดขึ้นแล้วให้ถูกต้อง หรือไม่ให้เกิดซ้ำในอนาคต เช่น แผนจูงใจลูกค้าไม่ให้ยกเลิกบริการ แผนรองรับกรณีเกิดเหตุสุดวิสัย/ภัยพิบัติ หรือ การจัดหาระบบคอมพิวเตอร์สำรอง

การควบคุมแบบส่งเสริม (Directive control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสาเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การประกวดหรือให้รางวัลแก่ผู้ที่มีผลงานดี

ดังนั้น กิจกรรมการควบคุมจึงเป็นวิธีการต่าง ที่นามาใช้ในการปฏิบัติงาน เพื่อให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล โดยอาจกำหนดเป็นมาตรการ หรือขั้นตอนต่าง ๆ เป็นแผนปฏิบัติการจัดการความเสี่ยง โดยแผนดังกล่าวต้องได้รับความเห็นชอบจากผู้บริหารในระดับที่เกี่ยวข้อง เพื่อให้การสนับสนุนทรัพยากรที่จำเป็นตามที่กำหนดไว้ในแผน เช่น บุคลากร งบประมาณ เป็นต้น ซึ่งจะประกอบด้วย

- กิจกรรมแสดงขั้นตอนและวิธีการดำเนินงาน
- ระยะเวลา / วันที่ดำเนินการแล้วเสร็จ
- เป้าหมาย
- ผู้รับผิดชอบ
- ตัวชี้วัดความเสี่ยง (KRI) เพื่อใช้ในการติดตามผลหรือเป็นสัญญาณเตือนภัยล่วงหน้า



ตารางแสดงความสัมพันธ์ของความสี่ยงและกิจกรรมการควบคุม

การเลือกกิจกรรมการควบคุม ควรมีการพิจารณาความเกี่ยวข้อง เหมาะสมของกิจกรรมควบคุมที่มีต่อการตอบสนองความเสี่ยง และ การนามาใช้เพื่อให้บรรลุวัตถุประสงค์เป็นสำคัญ ไม่ใช่เพื่อให้เห็นว่าต้องมีกิจกรรมการควบคุมเท่านั้น กิจกรรมการควบคุมบางอย่างที่กำหนดอาจช่วยให้องค์กรบรรลุวัตถุประสงค์มากกกว่าหนึ่งวัตถุประสงค์

๗.๗ สารสนเทศและการสื่อสาร (Information and Communication)

สารสนเทศ หมายถึง ข้อมูลที่ได้ผ่านการประมวลผลและถูกจัดให้อยู่ในรูปแบบที่เหมาะสม มีความหมายและเป็นประโยชน์ต่อการใช้งาน ซึ่งข้อมูลสารสนเทศหมายรวมถึงข้อมูลทางการเงิน(Financial Information) และการดำเนินงานในด้านอื่นๆ (Non-Financial Information) โดยเป็นข้อมูลทั้งจากแหล่งภายในของ สรอ. และภายนอก สรอ.

สารสนเทศที่ใช้ในการปฏิบัติงาน ได้มาจากแหล่งภายในและภายนอก ทั้งในรูปแบบเชิงปริมาณ และคุณภาพ ทั้งที่เป็นสารสนเทศทางการเงิน และที่มิใช่การเงิน ที่มีความเกี่ยวข้องกับวัตถุประสงค์ขององค์กรหลาย ๆ ประเภท

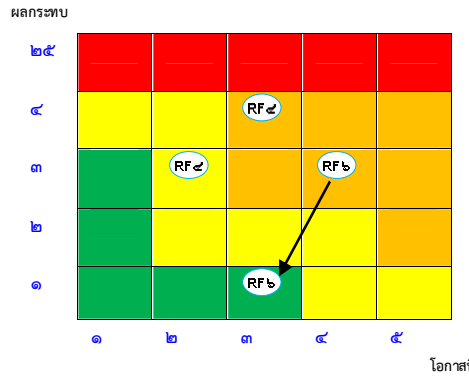
การมีสารสนเทศที่ถูกต้อง ตรงเวลา และถูกสถานที่ เป็นสิ่งจำเป็นที่จะมีผลต่อการบริหารความเสี่ยงขององค์กร ทุกระดับขององค์กรต้องการสารสนเทศ เพื่อใช้ในการกำหนดกลยุทธ์ ระบุ ประเมิน ตอบสนอง ควบคุม และติดตามรายงานผล ความเสี่ยง เพื่อให้การดำเนินงานบรรลุวัตถุประสงค์ขององค์กร

การสื่อสาร เป็นการสื่อสารข้อมูลที่จัดทำไว้แล้ว ส่งไปถึงผู้ที่ควรจะได้รับ หรือมีไว้พร้อมสำหรับผู้ที่ควรใช้สารสนเทศนั้น เพื่อให้ผู้ที่ได้รับใช้ข้อมูลดังกล่าวให้เกิดประโยชน์ในการตัดสินใจด้านต่าง ๆ และเพื่อสนับสนุนให้เกิดความเข้าใจ ตลอดจนมีการดำเนินงานตามวัตถุประสงค์ โดยระบบการสื่อสารต้องประกอบด้วยการสื่อสารภายในองค์กรและระบบการสื่อสารภายนอกองค์กร ซึ่งการสื่อสารแบ่งเป็น

- การสื่อสารภายในองค์กร ควรเป็นการสื่อสารหลายทาง เพื่อให้มีการดำเนินงานตามวัตถุประสงค์ของการควบคุมภายใน กระบวนการ และความรับผิดชอบในทุกระดับขององค์กร เช่น การสื่อสารจากระดับบนลงล่าง (Top-Down) หรือจากล่างขึ้นบน (Bottom-up) การสื่อสารในระดับเดียวกัน (Horizontal) โดยมีเทคนิคหรือเครื่องมือที่นำมาใช้สื่อสารระหว่างกัน ได้แก่ ระบบ Intranet ,Video/Telephone Conference เป็นต้น

- สื่อสารภายนอกองค์กร เป็นการสื่อสารกับแหล่งข้อมูลภายนอกโดยทำอย่างเป็นทางการ เป็นระยะ ๆ อย่างสม่ำเสมอหรืออาจทำเป็นมีเหตุจำเป็นเป็นครั้งคราวก็ได้ เช่น การติดต่อทางโทรศัพท์ การเชิญพบปะสังสรรค์ เป็นต้น

- แสดงผลการบริหารความเสี่ยงของแต่ละปัจจัยเสี่ยง เทียบกับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite)
- แสดงระดับความเสียหายของแต่ละปัจจัยเสี่ยง ทั้งก่อนและหลังบริหารปัจจัยเสี่ยงนั้นๆ โดยใช้แผนภูมิความเสี่ยง (Risk Profile) ในการอธิบาย



การจัดทำผลการบริหารความเสี่ยง ควรรายงานระดับความรุนแรงในแต่ละปัจจัยเสี่ยง โดยครอบคลุมทั้ง ๔ ปัจจัย ดังนี้

๑. ระดับความรุนแรงก่อนการบริหารความเสี่ยง
๒. ระดับความรุนแรงตามเป้าหมายที่องค์กรคาดหวัง
๓. ระดับความรุนแรงหลังการบริหารความเสี่ยง
๔. ระดับความรุนแรงที่องค์กรยอมรับได้

ทุกระดับที่ลดลงไม่ว่าจะเป็นโอกาสหรือผลกระทบก็ตาม องค์กรควรแสดงผลการวิเคราะห์อย่างชัดเจนเปรียบเทียบกับเกณฑ์ที่กำหนด

ผลการบริหารความเสี่ยง : ปัจจัยเสี่ยง A

ความรุนแรงก่อนการบริหารความเสี่ยง		เป้าหมายที่คาดหวัง		ความรุนแรงหลังการบริหารความเสี่ยง		ความรุนแรงที่องค์กรยอมรับได้	
โอกาส	ผลกระทบ	โอกาส	ผลกระทบ	โอกาส	ผลกระทบ	โอกาส	ผลกระทบ

ทั้งนี้ องค์กรจะต้องมีการสื่อสารเพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่ มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง นอกจากนี้ควรมีการประเมินประสิทธิภาพ และประสิทธิผลของการสื่อสาร เป็นระยะ ๆ เพื่อให้การสื่อสารเป็นส่วนหนึ่งของการควบคุมภายใน ที่เป็นประโยชน์สูงสุดต่อองค์กร

๗.๘ การติดตามและประเมินผล (Monitoring)

การติดตามและการรายงานผลเป็นกิจกรรมที่ใช้เพื่อติดตามและสอบทานแผนการจัดการความเสี่ยง เพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงมีประสิทธิภาพและเหมาะสม หรือควรปรับเปลี่ยน หากแผนนั้นไม่มีประสิทธิภาพเพียงพอ โดยกำหนดข้อมูลที่ต้องติดตาม และความถี่ในการสอบทาน และควรกำหนดให้มีการประเมินความเสี่ยงซ้ำอย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้วหรือมีความเสี่ยงใหม่เพิ่มขึ้น

การติดตามผลโดยทั่วไปมักจะดำเนินการโดยผู้บริหารและบุคลากรภายในองค์กรเอง อย่างไรก็ตามอาจให้บุคคลภายนอก เช่น ที่ปรึกษา หรือผู้เชี่ยวชาญอิสระ ช่วยในการติดตามการจัดการความเสี่ยงเป็นครั้งคราวได้ ความเสี่ยงและการจัดการต่อความเสี่ยงอาจมีการเปลี่ยนแปลงตลอดเวลา การจัดการต่อความเสี่ยงที่เคยมีประสิทธิผล อาจเปลี่ยนเป็นกิจกรรมที่ไม่เหมาะสม กิจกรรมการควบคุมอาจมีประสิทธิผลน้อยลง หรือไม่ควรดำเนินการต่อไป หรืออาจ มีการเปลี่ยนแปลงในวัตถุประสงค์หรือกระบวนการต่างๆ ดังนั้นแล้ว ผู้บริหารควรประเมินกระบวนการบริหารความเสี่ยง เป็นประจำเพื่อให้มั่นใจว่าการบริหารความเสี่ยงมีประสิทธิผลเสมอ

<u>ลักษณะหลักของการติดตามความเสี่ยง คือ</u>

- การประเมินควรมีประสิทธิผลและความต่อเนื่องของกิจกรรมการควบคุม และกิจกรรมอื่นที่ใช้จัดการความเสี่ยง
- การกำหนดระดับความเสี่ยงที่ยอมรับได้ที่เหมาะสมและสอดคล้องกับกลยุทธ์ทางธุรกิจ
- การรวบรวมและบันทึกข้อมูลอย่างครบถ้วน ถูกต้อง ทันเวลา
- การติดต่อสื่อสารเกี่ยวกับความเสี่ยงและกระบวนการต่างๆ อย่างสม่ำเสมอและเปิดเผยทั้งแบบเป็นทางการและไม่เป็นทางการ

<u>แนวทางการรายงานผลการดำเนินงาน มีดังนี้</u>

๘.๑ คณะอนุกรรมการด้านการบริหารความเสี่ยง

๘.๑.๑ รายงานต่อคณะกรรมการบริหาร สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

- รายงานแผนการบริหารความเสี่ยงประจำปี รวมทั้งแผนปฏิบัติการเพื่อการจัดการความเสี่ยง ปีละ ๑ ครั้ง
- รายงานผลการดำเนินการและความคืบหน้าการจัดการความเสี่ยงที่สำคัญระดับองค์กรต่อคณะกรรมการบริหาร สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) อย่างน้อยไตรมาศละ ๑ ครั้ง

๘.๑.๒ รายงานต่อคณะกรรมการตรวจสอบ

- รายงานผลการดำเนินงานอย่างน้อยปีละ ๑ ครั้ง

๘.๒ ผู้จัดการความเสี่ยงและการควบคุมภายใน (ของแต่ละสำนัก)

- รายงานต่อ คณะอนุกรรมด้านการบริหารความเสี่ยง /ผู้อำนวยการ สรอ. / รองผู้อำนวยการ สรอ. /สำนักที่เกี่ยวข้อง
- รายงานความเสี่ยงระดับองค์กรในส่วนที่รับผิดชอบและแผนปฏิบัติการการจัดการความเสี่ยงตลอดจนความคืบหน้าในการจัดการความเสี่ยงตามแผน พร้อมทั้งปัญหาและอุปสรรค เดือนละ ๑ ครั้ง

๘.๓ ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง

๘.๓.๑ รายงานต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

- รายงานความเสี่ยงที่สำคัญระดับองค์กร รวมทั้งรายละเอียดการจัดการความเสี่ยงตลอดจนความคืบหน้าของแผนปฏิบัติการและประเด็นสำคัญเพื่อการพิจารณาของ คณะอนุกรรมการด้านการความเสี่ยงทุกครั้ง ที่มีการประชุมคณะอนุกรรมการด้านการความเสี่ยง

- รายงานเหตุการณ์ที่เกิดขึ้นใหม่ทั้งที่เป็นโอกาสและความเสี่ยงที่มีผลต่อสำนักงานจากสภาพแวดล้อมที่เปลี่ยนแปลงไปเป็นการเฉพาะกิจ

- รายงานกรณีฉุกเฉินภายใน ๓ วันทำการ ในการประชุมเป็นกรณีพิเศษ เมื่อดัชนีชี้วัดความเสี่ยงมีการเปลี่ยนแปลงและอาจมีผลกระทบอย่างรุนแรงต่อการบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร

สรอ. ต้องสนับสนุนให้เกิดการสื่อสารในเชิงรุกและให้มีการสื่อสารอย่างสม่ำเสมอ ช่องทางในการสื่อสารอย่างเป็นทางการที่ใช้ในการพิจารณาความเสี่ยง การควบคุม และแผนการดำเนินการ ได้แก่ การประชุมทั่วไปผู้บริหาร การประชุมคณะทำงาน รายงานประจำเดือนสำหรับผู้บริหาร การประชุมคณะกรรมการบริหารความเสี่ยงเป็นต้น การสื่อสาร อย่างต่อเนื่องจะช่วยให้มีข้อมูลความเสี่ยงที่เพียงพอและได้รับการนำเสนอเพื่อใช้ในการตัดสินใจอย่างทันท่วงที ในบางกรณีการจัดการกับความเสี่ยงด้วยวิธีการที่เร่งด่วน จากการพูดคุยทางโทรศัพท์เกิดขึ้น อาจมีความเหมาะสมกว่ารอการจัดทำรายงานอย่างเป็นทางการผู้ที่เกี่ยวข้องต้องรายงานความเสี่ยงที่มีระดับความเสี่ยงสูง ให้แก่ผู้บังคับบัญชาทราบอย่างสม่ำเสมอและทันท่วงที พร้อมทั้งอธิบายวิธีการจัดการความเสี่ยงเหล่านั้นนอกจากนี้ ผู้บริหารในแต่ละหน่วยงานควรพิจารณาและนำเสนอความเสี่ยงที่มีระดับความเสี่ยงสูงของหน่วยงาน หรือความเสี่ยงที่ควรจะต้องได้รับการจัดการในระดับที่สูงกว่าขึ้นไปยังผู้บริหารในสายบังคับบัญชาเพื่อทำการพิจารณา ความเสี่ยงและหาแนวทางการจัดการความเสี่ยงในระดับงานที่สูงขึ้นต่อไป

๘. Governance Risk management & Compliance (GRC)

GRC คือ แนวคิดในการเชื่อมโยงและบูรณาการนิยามของสามองค์ประกอบ ได้แก่

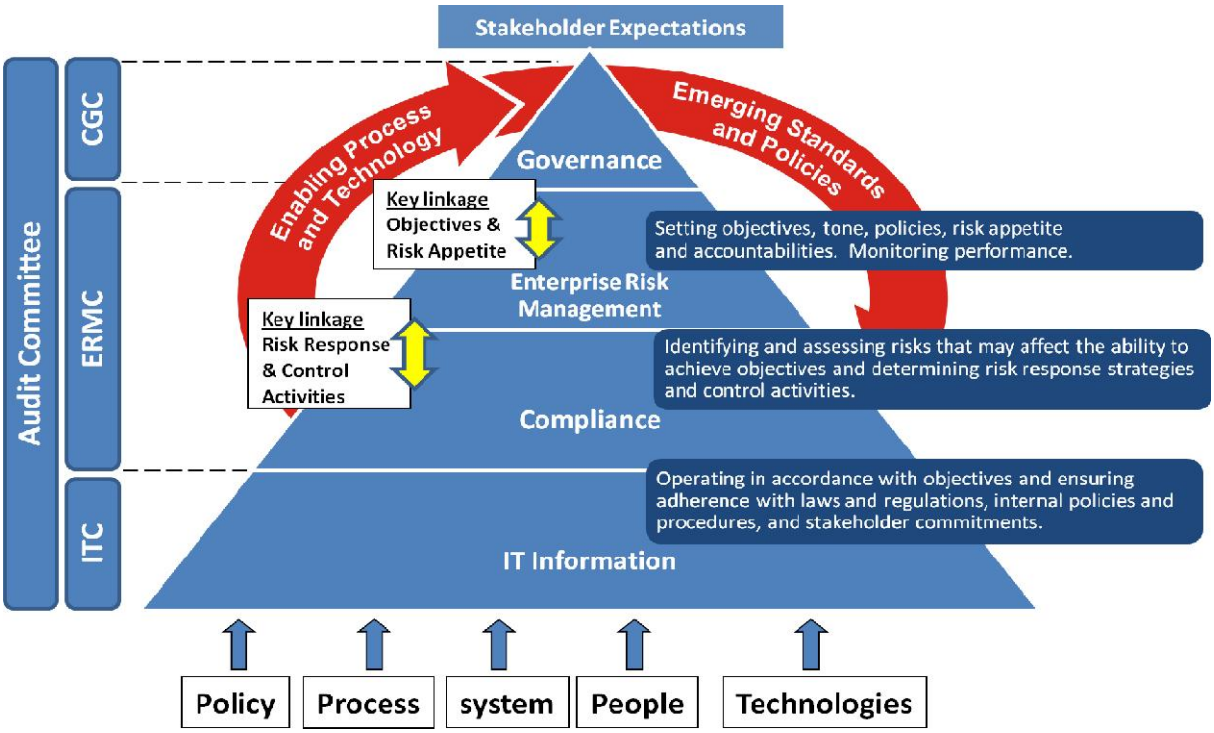
Governance หมายถึง นโยบาย วัฒนธรรมองค์กร กระบวนการขั้นตอนการปฏิบัติงานที่ถูกกำหนดออกมาอย่างชัดเจนในการบริหารจัดการและกำกับดูแลองค์กรโดยผู้บริหารระดับสูงเพื่อการบริหารองค์กรที่โปร่งใส ซึ่งรวมถึงความสัมพันธ์และบทบาทของทุกคนในองค์กร ตลอดจนกำหนดเป้าหมายหลักที่เน้นเรื่องความโปร่งใสในการบริหารจัดการของผู้บริหารระดับสูงในองค์กร

Risk Management หมายถึง การบริหารจัดการความเสี่ยงที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ที่ตั้งไว้ โดยใช้กระบวนการเชิงระบบของการประเมินสถานะและระดับของความเสี่ยงที่เกี่ยวข้องกับธุรกิจ ในลักษณะที่ทำให้การดำเนินงานไม่บรรลุผลตามเป้าหมาย โดยจะต้องหาทางค้นหาระบุความเสี่ยง จัดลำดับความเสี่ยงตามความสำคัญ และบริหารจัดการหรือป้องกันหรือลดโอกาสเกิดและผลกระทบของปัจจัยเสี่ยงที่ไม่คาดหวัง (Risk) ด้วยทางเลือกที่เหมาะสม ทบทวนระดับความเสี่ยงที่หลงเหลือและดำเนินการบริหารจัดการเพิ่มเติม จนกระทั่งความเสี่ยงลดระดับลงมาอยู่ในเกณฑ์ที่ยอมรับได้ขององค์กร และรวมถึงใช้ประโยชน์จากเหตุการณ์ในเชิงบวก (Opportunity) ได้อย่างรวดเร็วและมีประสิทธิภาพเพื่อสร้างมูลค่าเพิ่มให้องค์กร

Compliance หมายถึง การดำเนินงานกำกับให้มั่นใจว่า การปฏิบัติการทุกอย่างอยู่ภายใต้กฎเกณฑ์อย่างเหมาะสม ไม่เกิดการฝ่าฝืนใดๆ เกิดขึ้น โดยกฎเกณฑ์ที่ว่านี้รวมทั้งระเบียบ ข้อบังคับ กฎหมาย คำสั่งภายในองค์กร พันธะที่ผูกพันไว้กับผู้มีส่วนได้เสีย คู่สัญญาทุกภาคส่วน ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความปลอดภัยขององค์กรอย่างถูกต้องตามมาตรฐาน การปฏิบัติตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์ เป็นต้น การดำเนินงานในส่วนของการปรับปรุงประสิทธิภาพและประสิทธิผลในการกำกับการปฏิบัติตามกฎเกณฑ์ ในลักษณะที่ติดตาม เฝ้าระวังการเปลี่ยนแปลงในด้านกฎเกณฑ์และระเบียบเพื่อทำความเข้าใจ การศึกษาผลกระทบของกฎเกณฑ์ภายนอกต่อการดำเนินงานภายในและความจำเป็นในการปรับนโยบาย ระเบียบ ประกาศ กระบวนการปฏิบัติงานและสื่อสารเพื่อมิให้เกิดการฝ่าฝืน ซึ่งถือเป็นส่วนหนึ่งของการกำกับดูแลที่ดี

การพัฒนาแนวคิดจากการบริหารแบบ Silo มาเป็นกรอบแนวคิดที่บูรณาการ GRC เข้าด้วยกัน โดยแนวคิด GRC นั้นไม่ได้เป็นการพยายามที่จะรวบเอางาน ๓ ด้าน มาไว้ที่ศูนย์กลางเพียงจุดเดียว หากแต่ต้องการที่จะนำองค์ประกอบทั้ง ๓ มาปฏิบัติร่วมกันในรูปแบบของการทำงานเป็นทีม เป็นการแสวงหาแนวทาง การเชื่อมโยงบูรณาการงาน ๓ ด้านเข้าด้วยกันในเชิงนโยบาย กระบวนการดำเนินงาน ขั้นตอนการปฏิบัติและระบบการควบคุม แบ่งปันข้อมูลซึ่งกันและกัน มีการเปิดกว้างทางความคิดที่จะปรับปรุงองค์กรจากข้อมูลและแนวทางจากผู้บริหาร

ของหลายๆ ฝ่าย โดยต้องได้รับการสนับสนุนจากองค์ประกอบพื้นฐานหลัก ๕ ประการขององค์กร ได้แก่ กลยุทธ์ กระบวนการ ระบบ บุคลากร เทคโนโลยี ดังรูปความสัมพันธ์และความเชื่อมโยงตามภาพ ตัวอย่าง เช่น



- การรณรงค์ปลูกฝัง ปรับเปลี่ยนวัฒนธรรมขององค์กร เพื่อนำบุคคลภายในองค์กรไปสู่วัตถุประสงค์และเป้าหมายด้านวัฒนธรรมองค์กรที่คาดหวังเพื่อเพิ่มประสิทธิภาพ สนับสนุนหรือผลักดันให้การดำเนินงานขององค์กรบรรลุตามวัตถุประสงค์ได้ดีขึ้น ทั้งยังทำให้เกิดผลลัพธ์เชิงวัฒนธรรมองค์กรที่พึงประสงค์ด้วย

- กลยุทธ์/กระบวนการ/ระบบ : การส่งเสริมให้คณะกรรมการสามารถกำกับดูแลองค์กรและให้คำแนะนำแก่ผู้บริหารเพื่อดำเนินงานให้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องได้อย่างมั่นใจ โดยผู้บริหารต้องจัดให้มีการบริหารความเสี่ยงที่เป็นระบบ มุ่งเน้นความเสี่ยงที่ตรงประเด็น และสามารถจัดกระบวนการทำงานเพื่อให้มีการปฏิบัติตามระเบียบหรือการควบคุมภายในได้อย่างเหมาะสม ภายใต้ต้นทุนการดำเนินงานที่สมเหตุสมผล รวมถึงการนำเทคโนโลยีมาสนับสนุนการทำงานให้มีประสิทธิภาพ และการสื่อสารข้อมูลอย่างถูกต้องเหมาะสมทันเวลาต่อผู้เกี่ยวข้องทุกระดับ

- การที่บุคลากรมีความมุ่งมั่น ยึดถือและส่งเสริมวัฒนธรรมของการดำเนินธุรกิจอย่างมีศักดิ์ศรีและคุณค่าทางจริยธรรม รับผิดชอบในผลงานของตน มีมุมมองที่เป็นหนึ่งเดียวกับองค์กรและต่อต้านการทำกิจกรรมที่ต่างคนต่างทำตามอำนาจหน้าที่เฉพาะตัว เน้นการทำงานเป็นทีมโดยคำนึงถึงประโยชน์ขององค์กรเป็นหลัก

- การควบคุมภายในที่เพียงพอในการลดความเสี่ยงของบุคคล ช่วยกำกับคนมากขึ้น เช่น การกำกับติดตาม (Monitoring) การใช้ระบบควบคุมการตรวจสอบคุณภาพงานและการทดสอบผลงานว่าใช้งานได้จริงอย่างสม่ำเสมอและมีประสิทธิผล หรือกระบวนการฝึกอบรมบุคลากร เพื่อให้เหมาะสมกับความรับผิดชอบในภารกิจการกำหนดให้มีมาตรฐานการทำงานที่ชัดเจน

- การใช้เทคโนโลยี หรือ ไอทีภิบาล (IT Governance) มาช่วยในการกำกับดูแลที่ดี ด้วยการนำ IT มาทำหน้าที่เป็นระบบเฝ้าระวัง เป็นเครื่องเตือนภัยล่วงหน้า เป็นระบบอัตโนมัติที่กำกับการปฏิบัติในลักษณะที่ฝ่าฝืนกฎเกณฑ์ หรือเป็นระบบรายงานความผิดปกติ

- การประสานงานและเชื่อมโยงเครื่องมือ ระบบงาน และคน

โดย GRC จะช่วยทำให้องค์กรเกิดความสามารถในการแข่งขันในระยะยาว เพิ่มความโปร่งใสในการเปิดเผยข้อมูล เสริมภาพลักษณ์ที่ดีให้กับองค์กร ตลอดจนคณะผู้บริหารระดับสูง รวมทั้งการสร้างจิตสำนึกในการปฏิบัติงานที่ดีให้กับเจ้าหน้าที่ทุกคน ส่งผลให้ลูกค้าเกิดความเชื่อถือและความมั่นใจในการใช้บริการต่างๆ ของ องค์กร

ความเสี่ยงด้านนโยบายและกลยุทธ์
(Strategic Risk)

ประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
ที่ ๗/๒๕๕๕
นโยบายบริหารความเสี่ยงด้านนโยบายและกลยุทธ์
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

เพื่อให้การดำเนินการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ (Strategic Risk Management) ของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) มีความสอดคล้องตามนโยบายบริหารความเสี่ยงของ สรอ. (Enterprise Risk Management Policy)

โดย สรอ. ตระหนักถึงความสำคัญในการบริหารจัดการความเสี่ยงในการดำเนินงาน จึงได้จัดทำนโยบายบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ (Strategic Risk Management Policy) ให้เป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยง (Enterprise Risk Management Policy) โดยกำหนดให้ สรอ. มีการประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามประเมินผล และการรายงานความเสี่ยงด้านนโยบายและกลยุทธ์ และจัดให้มีระบบการควบคุมภายใน เพื่อใช้ในการควบคุมดูแลการดำเนินงานภายในของ สรอ. เพื่อให้คณะกรรมการ ผู้อำนวยการ ผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กร มีส่วนร่วม สร้างความคุ้นเคยและผลักดันให้การบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ของ สรอ. อยู่ในทุกกระบวนการทำงาน และให้ยึดถือเป็นกลไกหนึ่งในการส่งเสริมให้การดำเนินการของ สรอ. มีประสิทธิภาพ อันจะเป็นส่วนหนึ่งของวัฒนธรรมองค์กรอย่างยั่งยืน และสามารถสร้างมูลค่าเพิ่มให้กับองค์กรและประเทศชาติ

ดังนั้น เพื่อให้การบริหารความเสี่ยงของ สรอ. ด้านนโยบายและกลยุทธ์เป็นไปด้วยความเรียบร้อยอย่างมีประสิทธิภาพและประสิทธิผล อาศัยอำนาจตามมาตรา ๒๖ และ ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ.๒๕๕๔ ประกอบกับมติคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ ในคราวประชุมครั้งที่ ๘/๒๕๕๕ เมื่อวันที่ ๑๕ สิงหาคม ๒๕๕๕ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) จึงกำหนดให้ยึดถือนโยบายการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ตามคู่มือการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์อย่างเคร่งครัดโดยทั่วกัน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๑ กันยายน พ.ศ. ๒๕๕๕

(นายศักดิ์ เสกขุนทด)
ผู้อำนวยการ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

คู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์
(Strategic Risk Management Manual)

สารบัญ

หน้าที่

๑. บทนำ

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ให้ความสำคัญต่อการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ (Strategic Risk Management) เป็นอย่างมาก โดยมีคณะกรรมการบริหาร สรอ. แนะนำและติดตามการรายงานผ่านคณะอนุกรรมการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อหาแนวทางแก้ไขปัญหาที่เกิดจากปัจจัยเสี่ยงต่างๆ นอกจากนี้ยังกำหนดให้มีการดูแลและทบทวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์อย่างต่อเนื่อง เพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ สรอ. ยอมรับได้

การบริหารความเสี่ยงด้านนโยบายและกลยุทธ์จึงเป็นกระบวนการสำคัญที่จะลดโอกาสของความเสี่ยงที่อาจเกิดขึ้นและบรรเทาผลกระทบที่องค์กรจะได้รับในทุกหน่วยงานของ สรอ. ดังนั้น กระบวนการบริหารความเสี่ยงจะช่วยลดความสูญเสียที่อาจจะเกิดขึ้นให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้รวมทั้งเป็นองค์ประกอบสำคัญในการกำกับดูแล สรอ. ให้บรรลุผลสำเร็จตามเป้าหมายที่กำหนด

สรอ. ได้กำหนดกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ เพื่อให้หน่วยงานต่างๆ ของ สรอ. ได้ใช้เป็นแนวทางในการพิจารณาแผนกลยุทธ์และแผนธุรกิจที่สอดคล้องกับกลยุทธ์หลักของ สรอ. โดยการระบุความเสี่ยงที่อาจเกิดขึ้นแล้วทำการประเมินความเสี่ยงถึงโอกาสที่จะเกิดขึ้นรวมทั้งผลกระทบที่จะได้รับ พร้อมทั้งจัดหาแนวทางหรือมาตรการควบคุมที่เหมาะสมมาดำเนินการหรือจัดการกับความเสี่ยงนั้น โดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่ สรอ. กำหนด

ดังนั้นคู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ของ สรอ.นี้ จึงมุ่งเน้นถึงการสร้างความตระหนักให้เกิดแก่ทุกคนที่เกี่ยวข้องในสำนักงาน ในการที่จะช่วยสอดส่องดูแล ระมัดระวัง เพื่อลดความเสี่ยง หรือ บรรเทาผลกระทบจากความเสี่ยงด้านนโยบายและกลยุทธ์ อันเกิดจากความเสี่ยงที่ไม่สามารถบรรลุเป้าหมายตามนโยบายและกลยุทธ์ ของ สรอ. เช่น การไม่สามารถดำเนินโครงการ GIN หรือ MailGoThai ได้ตามแผนงาน เป็นต้น ความเสี่ยงที่เกิดขึ้นดังกล่าวข้างต้นเป็นความเสี่ยงด้านนโยบายและกลยุทธ์ ที่ส่งผลต่อนโยบายที่ได้รับมอบหมายจากกระทรวงเทคโลยีสารสนเทศและการสื่อสาร หรือนโยบายภาครัฐได้ตามกำหนด รวมทั้งอาจส่งผลต่อภาพลักษณ์ขององค์กรและทำให้องค์กรไม่สามารถดำเนินการได้ครบถ้วนสมบูรณ์ตามวัตถุประสงค์และภารกิจที่กำหนดไว้ ดังนั้นการส่งเสริมให้ทุกคนตระหนักถึงความสำคัญและมีส่วนร่วมในการการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ (Strategic Risk Management) โดยคณะกรรมการบริหาร สรอ. จะให้คำแนะนำและติดตามการรายงานการบริหารความเสี่ยงฯ ผ่านคณะอนุกรรมการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อวางแนวทางแก้ไขปัญหาที่เกิดจากปัจจัยเสี่ยงต่างๆ นอกจากนี้ยังกำหนดให้มีการดูแลและทบทวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ อย่างต่อเนื่อง เพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ สรอ. ยอมรับได้

สรอ. ได้กำหนดกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ เพื่อให้หน่วยงานต่างๆ ของ สรอ. ใช้เป็นแนวทางในการจัดทำแผนกลยุทธ์และแผนธุรกิจที่สอดคล้องกับกลยุทธ์หลักของ สรอ. โดยการระบุความเสี่ยงที่อาจเกิดขึ้น แล้วทำการประเมินถึงโอกาสที่จะเกิดความเสี่ยงขึ้นรวมทั้งผลกระทบที่จะได้รับ พร้อมทั้งจัดทำแนวทางหรือมาตรการควบคุมที่เหมาะสมเพื่อจัดการกับความเสี่ยงนั้น โดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่ สรอ. กำหนด

คู่มือการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ โดยจะกล่าวถึงวัตถุประสงค์ ขอบเขต โครงสร้างและบทบาทหน้าที่ของผู้รับผิดชอบกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ และรายละเอียดของกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ เพื่อเป็นแนวทางในการปฏิบัติงานของ สรอ. และเพื่อให้หน่วยงานต่างๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ตนเองตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

แนวทางการบริหารความเสี่ยงที่นำมาใช้

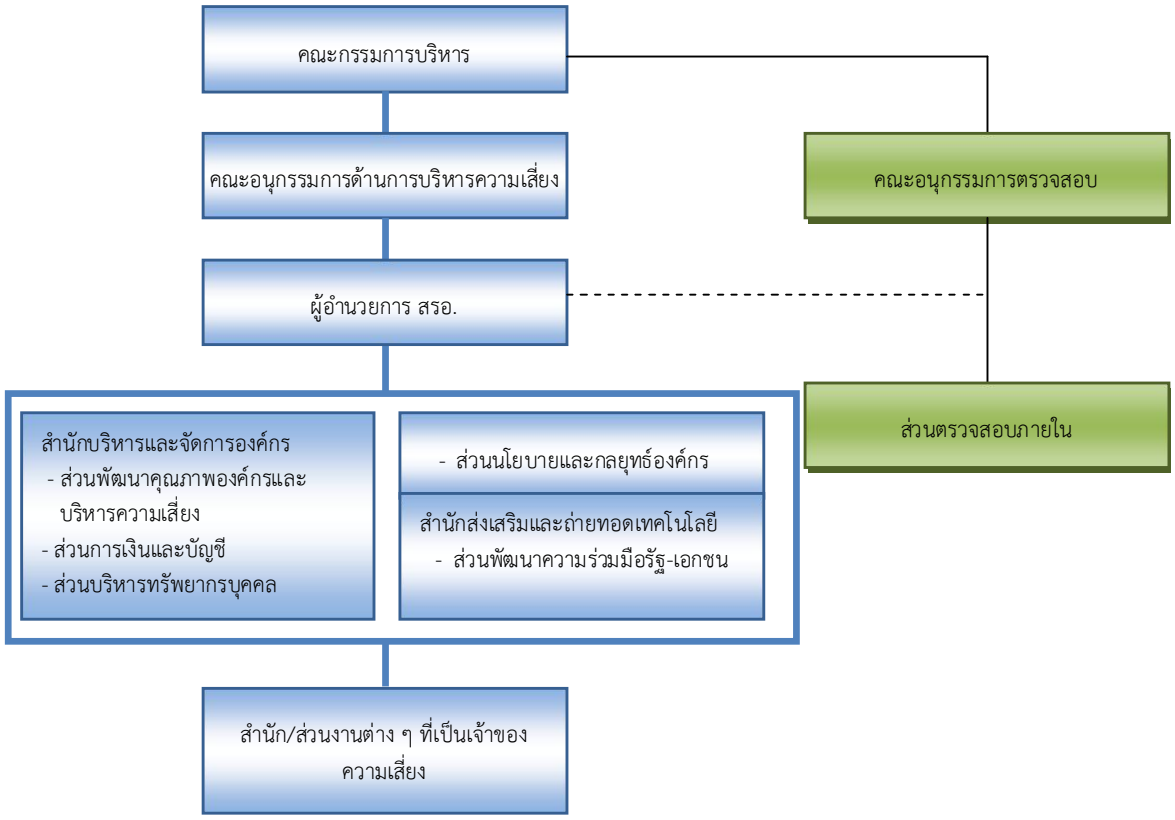
สรอ. กำหนดกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ตามแนวทางการปฏิบัติงานของ สรอ. และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Tread way Commission (COSO) โดยครอบคลุมความเสี่ยงธุรกิจ (Business Risk) ที่เกี่ยวกับการจัดทำและการกำหนดแผนงานของแผนกลยุทธ์ (Strategic Risk) และการจัดการ (Management Risk) ให้อยู่ในระดับที่เหมาะสมกับความซับซ้อนของธุรกิจ

ขอบเขตของคู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ซึ่งครอบคลุมถึงความเสี่ยงอันเกิดจากการดำเนินงานที่ไม่เป็นไปตามแผนกลยุทธ์ สรอ. รวมทั้งนโยบายที่ได้รับจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งนโยบายภาครัฐ ตั้งแต่การกำหนดแผนงานที่รองรับนโยบายไม่ครบถ้วน การดำเนินงานไม่ได้ตามเป้าหมายแผนกลยุทธ์ของโครงการหลัก เช่น โครงการ GIN Cloud หรือ Mail.Go.Thai เป็นต้น รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นปัจจัยภายนอก เช่น การเปลี่ยนแปลงนโยบายภาครัฐ เป็นต้น โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ เพื่อให้หน่วยงานต่างๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ของตนเอง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบดังนี้

๑. กำหนดกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ และนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๓. จัดทำคู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ และเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๔. ประสานงานกับส่วนนโยบายและกลยุทธ์องค์กร และบัญชี ส่วนพัฒนาความร่วมมือรัฐเอกชน และส่วนนโยบายและกลยุทธ์องค์กรองค์กร เพื่อจัดให้หน่วยงานต่างๆ ดำเนินการพิจารณา Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของหน่วยงานต่างๆ รวมถึงแนวทางการจัดการความเสี่ยงที่เหมาะสม

๕. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่างๆ ให้เข้าใจถึงแนวทาง ความสำคัญ และความรับผิดชอบในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๖. ดูแลให้มีการปฏิบัติตามกระบวนการในการออก/ปรับปรุงผลิตภัณฑ์ตามแนวทางที่ สรอ. กำหนดและมีส่วนร่วมพิจารณาให้ความเห็นในการออกผลิตภัณฑ์ในประเด็นที่เกี่ยวข้องกับความเสี่ยง รวมทั้งปรับปรุงหรือแก้ไขข้อบกพร่องที่เกี่ยวกับความเสี่ยงด้านต่างๆ ที่เกิดขึ้นภายหลังการออก/ปรับปรุงผลิตภัณฑ์ โดยดำเนินการร่วมกับหน่วยงานเจ้าของผลิตภัณฑ์นั้นๆ

๗. ร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) สำหรับสถานการณ์ที่ไม่ปกติ เพื่อรองรับการเปลี่ยนแปลงสภาพแวดล้อมที่ไม่เป็นไปตามที่คาดไว้

๘. ร่วมกับส่วนการเงินและบัญชี ส่วนพัฒนาความร่วมมือรัฐเอกชน และส่วนนโยบายและกลยุทธ์องค์กร เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนนโยบายและกลยุทธ์ และงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

(๑) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับสรอ. พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Risk Likelihood) และผลกระทบ (Risk Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือก พร้อมทั้งระบุการควบคุมอย่างชัดเจน

(๒) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้นๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหาร ควบคุม และจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนการเงินและบัญชี สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดทำแผนการเงิน ให้สอดคล้องกับแผนกลยุทธ์ แผนธุรกิจในภาพรวมของ สรอ. รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๓. ติดตามและวิเคราะห์ผลการดำเนินงานของ สรอ. เปรียบเทียบกับแผนการเงิน และอื่นๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมายและแนวทางการจัดการความเสี่ยง (Mitigation)

๔. ร่วมกับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนพัฒนาความร่วมมือรัฐเอกชน และส่วนนโยบายและกลยุทธ์องค์กร เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนการเงินและงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

(๑) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับ สรอ. พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Risk Likelihood) และผลกระทบ (Risk Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือกพร้อมทั้งระบุการควบคุมอย่างชัดเจน

(๒) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้นๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหาร ควบคุม และจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนนโยบายและกลยุทธ์องค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดทำแผนนโยบายและกลยุทธ์ ให้สอดคล้องกับแผนกลยุทธ์ แผนธุรกิจในภาพรวมของ สรอ. รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๓. ติดตามและวิเคราะห์ผลการดำเนินงานของ สรอ. เปรียบเทียบกับแผนนโยบายและกลยุทธ์ และอื่นๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมายและแนวทางการจัดการความเสี่ยง (Mitigation) เพื่อให้การปฏิบัติงานเป็นไปอย่างประสิทธิภาพและเกิดประสิทธิผล กรณีที่มีการเบี่ยงเบนไปจากแผนให้เสนอแนวทางแก้ไขให้ทันท่วงที

๔. ร่วมกับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนพัฒนาความร่วมมือรัฐเอกชน และส่วนการเงินและบัญชี เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนนโยบายและกลยุทธ์ และงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

(๑) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับ สรอ. พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Risk Likelihood) และผลกระทบ (Risk Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือกพร้อมทั้งระบุการควบคุมอย่างชัดเจน

(๒) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวน

ระดับความเสี่ยงนั้นๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหาร ควบคุม และจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนพัฒนาความร่วมมือรัฐเอกชน สำนักส่งเสริมและถ่ายทอดเทคโนโลยี มีหน้าที่รับผิดชอบ ดังนี้

๑. ศึกษาความเป็นไปได้ตามแผนกลยุทธ์ แผนธุรกิจในภาพรวมของ สรอ. รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๓. ติดตามและวิเคราะห์ผลการดำเนินงานของ สรอ. เปรียบเทียบกับแผนพัฒนาความร่วมมือรัฐเอกชน และอื่นๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมาย และแนวทางการจัดการความเสี่ยง (Mitigation)

๔. ร่วมกับส่วนนโยบายและกลยุทธ์องค์กร ส่วนการเงินและบัญชี และส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนนโยบายและกลยุทธ์ และงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

(๑) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับ สรอ. พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Risk Likelihood) และผลกระทบ (Risk Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือกพร้อมทั้งระบุการควบคุมอย่างชัดเจน

(๒) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator : KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้นๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหาร ควบคุม และจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนบริหารทรัพยากรบุคคล สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดองค์กร และกำหนดวิธีการปฏิบัติงานที่เอื้อต่อการปฏิบัติตามแผนกลยุทธ์ โดยจัดให้มีการสอบยันและถ่วงดุลอำนาจ (Check and Balance) อย่างเหมาะสม รวมถึงกำหนดสายการบังคับบัญชาที่ชัดเจนและเปิดเผย เพื่อการสั่งการที่รวดเร็วและมีประสิทธิภาพ

๒. จัดอัตรากำลังให้เหมาะสมกับคุณสมบัติและหน้าที่ตำแหน่งงานที่รับผิดชอบ รวมทั้งกำหนดระบบการสรรหา การฝึกอบรม และการกำหนดผลตอบแทนที่เหมาะสม เพื่อสนับสนุนเจ้าหน้าที่ให้ปฏิบัติตามแผนกลยุทธ์เพื่อบรรลุเป้าหมายของ สรอ.

๓. สร้างเสริมให้เกิดการกำกับดูแลกิจการที่ดีภายใน สรอ. เพื่อให้การดำเนินธุรกิจของ สรอ. มีความเจริญเติบโตอย่างต่อเนื่องและมั่นคง บริหารงานอย่างมีประสิทธิภาพ โปร่งใส และเป็นธรรม ซึ่งจะสร้างความเชื่อมั่นให้กับทุกหน่วยงาน

ส่วนตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

ตรวจสอบและสอบทานการควบคุมภายในด้านต่างๆ ของ สรอ. ก่อนนำเสนอคณะอนุกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

สำนัก และส่วนงานต่างๆ ของ สรอ. มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกลยุทธ์และแผนปฏิบัติการของสำนัก และส่วนงานต่างๆ ให้สอดคล้องกับแผนกลยุทธ์หลักของ สรอ.

๒. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับสำนัก และส่วนงานต่าง ๆ

๓. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนกลยุทธ์สำนัก และส่วนงานต่างๆ ให้กับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง เพื่อนำไปจัดทำแผนภาพความเสี่ยงด้านนโยบายและกลยุทธ์และภาพความเสี่ยงแบบบูรณาการ ตามลำดับต่อไป

๔. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของสำนักให้กับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเป็นรายไตรมาส

๕. บริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงาน ในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๖. ดูแล ติดตามการจัดการความเสี่ยง และประเมินผลการจัดการความเสี่ยงเป็นประจำ เพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับ รวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติม เพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๗. แต่งตั้งผู้ประสานงานด้านความเสี่ยง (Risk Officer) เพื่อประสานงานกับส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงในการจัดทำ Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของส่วนงานและสำนัก

๘. สื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๔.๑ ความเสี่ยงด้านนโยบายและกลยุทธ์ (Policy and Strategic Risk)

ความเสี่ยงด้านนโยบายและกลยุทธ์ (Policy and Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดนโยบายต่างๆ เช่น นโยบายระดับรัฐจนถึงนโยบายในระดับผู้บริหาร แผนกลยุทธ์ แผนดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับสภาพแวดล้อมภายใน และปัจจัยภายนอก ทำให้มีโอกาสที่จะไม่ประสบความสำเร็จตามทิศทางที่กำหนดไว้ ซึ่งจะส่งผลกระทบต่อตัวชี้วัดผลการปฏิบัติงานของสำนักงาน

แผนยุทธศาสตร์ หมายถึง แผนที่แสดงทิศทางการดำเนินงานและสะท้อนวิสัยทัศน์หรือเป้าหมายหรือนโยบายของ สรอ. โดยทั่วไปจะมีระยะเวลา ๓ ถึง ๕ ปี ซึ่งแผนกลยุทธ์ที่ดี จะต้องมีความชัดเจนสอดคล้องกับเป้าหมาย ยืดหยุ่น และสามารถปรับเปลี่ยนให้สอดคล้อง กับสภาวการณ์ที่เปลี่ยนแปลงได้

แผนธุรกิจ (Business Plan) หมายถึง แผนที่กำหนดกรอบการดำเนินงานโดยรวมของ สรอ. เพื่อสนับสนุนการปฏิบัติงานให้สำเร็จตามแผนกลยุทธ์ และเป็นแนวทางให้แก่ หน่วยงานต่างๆ ในการกำหนดแผนปฏิบัติการ (Action Plan) โดยทั่วไปจะเป็นแผนระยะสั้นไม่เกิน ๑ ปี ประกอบด้วย เป้าหมาย ผลดำเนินการ หน่วยงานที่รับผิดชอบ ปริมาณทรัพยากรที่ใช้ กรอบเวลาการดำเนินงาน และเกณฑ์ในการติดตามผลการปฏิบัติงาน ซึ่งควรสอดคล้องกับงบประมาณของ สรอ. ด้วย

๔.๒ ที่มาของความเสี่ยงด้านนโยบายและกลยุทธ์ สามารถจำแนกได้ ๒ ประเภท ดังนี้

๔.๒.๑ ปัจจัยความเสี่ยงภายนอก หมายถึง ปัจจัยที่ สรอ. ไม่สามารถควบคุมได้ หรือควบคุมได้ยาก ซึ่งจะส่งผลกระทบหรือเป็นอุปสรรคต่อการจัดทำแผนกลยุทธ์ แผนดำเนินงานของ สรอ. และการปฏิบัติ เพื่อให้บรรลุเป้าหมายที่วางไว้ของ สรอ.

(๑) การได้รับนโยบายต่าง ๆ จากหน่วยงานภายนอกที่กำกับดูแล สรอ. นั้น ทาง สรอ. จะต้องสามารถสื่อสารสู่เจ้าหน้าที่ได้อย่างถูกต้องตามที่ได้รับนโยบายมา เพื่อที่หน่วยงานต่าง ๆ ของ สรอ. จักได้นำไปกำหนดในแผนกลยุทธ์และแผนดำเนินงานได้อย่างสอดคล้องตามนโยบายที่ได้รับ

(๒) การเปลี่ยนแปลงนโยบายระดับรัฐ อาจทำให้สภาวะการทำงานหยุดชะงัก หรือต้องวางกลยุทธ์และแผนการดำเนินงานใหม่

(๓) การเปลี่ยนแปลงพฤติกรรมของกลุ่มลูกค้าเป้าหมาย การเปลี่ยนแปลงของโครงสร้างประชากรและความต้องการของลูกค้า จะมีผลต่อฐานลูกค้าของ สรอ. ซึ่ง สรอ. ต้องมีการ

กำหนดกลุ่มลูกค้าเป้าหมายที่มีศักยภาพ และวิธีการเสนอบริการที่ดีให้แก่ลูกค้าเหล่านั้น เพื่อป้องกันความเสี่ยงที่จะสูญเสียส่วนแบ่งตลาด

(๔) การเลือกใช้เทคโนโลยีเป็นความเสี่ยงที่มีความสำคัญต่อการดำเนินงานของ สรอ. อย่างมาก ดังนั้น สรอ. ต้องมีการจัดการความเสี่ยงจากการเลือกใช้เทคโนโลยีเพื่อตอบสนองต่อนโยบายที่ได้รับ และสนับสนุนต่อแผนกลยุทธ์ แผนดำเนินงานของ สรอ.

(๕) การเกิดภัยพิบัติจากธรรมชาติ เช่น น้ำท่วมปี พ.ศ. ๒๕๕๔ เป็นต้น ภัยจากการประท้วงจนก่อให้เกิดการจลาจล แต่ระดับความรุนแรงของผลกระทบดังกล่าวขึ้นอยู่กับขอบเขตการดำเนินงานที่เกี่ยวข้องกับเหตุการณ์หรือภัยพิบัติ และความสามารถในการปรับตัวของ สรอ.

(๖) กฎหมาย มติคณะรัฐมนตรี ข้อบังคับ ระเบียบ ประกาศ และคำสั่ง ตลอดจนระเบียบของหน่วยงานที่กำกับดูแล อาจเป็นอุปสรรคในการดำเนินงานอันส่งผลกระทบต่อการปฏิบัติตามแผนกลยุทธ์และแผนดำเนินงานให้บรรลุเป้าหมายและจำเป็นต้องปรับเปลี่ยนแผนกลยุทธ์และแผนดำเนินงานให้สอดคล้องกับกฎหมาย ฯลฯ

๔.๒.๒ ปัจจัยความเสี่ยงภายใน หมายถึง ปัจจัยที่ สรอ. สามารถควบคุมได้ แต่สามารถส่งผลกระทบหรือเป็นอุปสรรคต่อการดำเนินงานตามแผนกลยุทธ์เพื่อให้บรรลุเป้าหมาย ได้แก่

(๑) สรอ. ต้องจัดให้มีกระบวนการสื่อสารองค์กรในเรื่องแผนกลยุทธ์ และแผนดำเนินงานขององค์กรสู่เจ้าหน้าที่อย่างทั่วถึงทุกระดับ และต่อเนื่อง

(๒) โครงสร้างองค์กร การจัดโครงสร้างองค์กร มีความสำคัญต่อการปฏิบัติตามแผนกลยุทธ์และแผนดำเนินงานให้บรรลุเป้าหมายและมีประสิทธิภาพ หาก สรอ. ไม่มีการทบทวนการแบ่งแยกหน้าที่ความรับผิดชอบตามนโยบายหรือภารกิจที่ได้รับจากรัฐบาลเป็นรายปี หรือรายเฉพาะกิจจะทำให้เกิดปัญหาในการจัดการเพื่อบรรลุต่อเป้าหมายที่ต้องการ

(๓) กระบวนการและวิธีปฏิบัติงาน หาก สรอ. มิได้กำหนดกระบวนการและวิธีปฏิบัติงานที่ชัดเจน หรือกำหนดความรับผิดชอบที่ซับซ้อนกัน อาจส่งผลให้การปฏิบัติตามแผนการดำเนินงานและแผนปฏิบัติการล่าช้าและผิดพลาดได้ง่าย ยากแก่การติดตามและรายงานผลการปฏิบัติงานได้ถูกต้องและทันกาล

(๔) ความเพียงพอและคุณภาพของบุคลากร การดำเนินงานตามแผนกลยุทธ์และแผนดำเนินงานในทุกระดับของ สรอ. จะบรรลุเป้าหมายได้หรือไม่นั้นขึ้นอยู่กับปริมาณและคุณภาพของบุคลากร จำนวนบุคลากรที่เพียงพอจะช่วยรองรับปริมาณงานและธุรกรรมได้ครบถ้วน บุคลากรควรมีความเชี่ยวชาญและได้รับการฝึกอบรมที่จำเป็นเพื่อให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผล

(๕) ความเพียงพอของข้อมูล ผู้บริหารของ สรอ. จะต้องได้รับข้อมูลที่เหมาะสมเพื่อใช้ในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ การได้รับข้อมูลไม่เพียงพอ ไม่เหมาะสม ไม่ถูกต้องและไม่ทันกาลจะเป็นอุปสรรคต่อการเข้าใจสภาวการณ์ และส่งผลต่อการวางแผนกลยุทธ์และแผนดำเนินงานการกำหนดเป้าหมายและการบริหารงานของ สรอ.

(๖) เทคโนโลยี สรอ. จะต้องมีเทคโนโลยีที่สามารถแข่งขันและตอบสนองความต้องการของลูกค้าได้ โดยเฉพาะธุรกรรมที่ซับซ้อน พร้อมทั้งต้องปรับปรุงระบบเทคโนโลยีสารสนเทศให้สามารถแข่งขันและรองรับปริมาณธุรกรรมใหม่ได้

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
หน่วยงานภาครัฐระดับกระทรวงและกรม ไม่มีการบูรณาการและเชื่อมโยงในเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ได้ตามเป้าหมาย ร้อยละ ๕๐	การประสานความต้องการของหน่วยงานภาครัฐเพื่อให้เพิ่มประสิทธิภาพการดำเนินของหน่วยงานภาครัฐ ไม่สามารถดำเนินการได้ตามแผนงาน	✓	
	จำนวนหน่วยงานภาครัฐที่เข้าร่วมการทำ Focus Group เพื่อสร้างการมีส่วนร่วมในการพัฒนา GIN มีจำนวนไม่เป็นไปตามเป้าหมาย		✓
การพัฒนาระบบเว็บไซต์กลางบริการอิเล็กทรอนิกส์ภาครัฐ (e-Portal) ไม่เป็นไปตามเป้าหมาย	ไม่สามารถปรับข้อมูลใน e-Portal เพื่อให้ตรงตามความต้องการของแต่ละพื้นที่ได้แล้วเสร็จ	✓	
	จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการไม่เป็นไปตามเป้าหมาย	✓ อาจเป็นปัจจัยภายในหากการวางแผนการตลาดไม่ดีพอ	✓ อาจเป็นปัจจัยภายนอกหากงบประมาณของหน่วยงานภาครัฐที่ใช้บริการถูกจำกัด
จำนวนหน่วยงานที่ให้บริการ Cloud แก่หน่วยงานภาครัฐไม่เป็นไปตามเป้าหมาย	การพัฒนา Data Center Consolidation ล่าช้ากว่าแผนงานที่กำหนด	✓	

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
ไม่สามารถสร้าง เครือข่ายความร่วมมือในการพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์ได้ตามแผนงาน	ไม่สามารถดำเนินกิจกรรมพัฒนาความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนเพื่อส่งเสริมการพัฒนารัฐบาลอิเล็กทรอนิกส์ (Public-Private Partnership) ได้ล่าช้ากว่าแผนงาน	✓	
	จำนวนหน่วยงานภาครัฐที่มาเข้าร่วมโครงการไม่เป็นไปตามเป้าหมาย		✓

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

การวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงทางนโยบายและกลยุทธ์ นั้น จากการที่สำนักงานเป็นหน่วยงานกลางของประเทศในการผลักดันและขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ โดยมีพันธกิจคือ การพัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์ โดยมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงทางนโยบายและกลยุทธ์ เพื่อให้การดำเนินงานในขั้นตอนต่างๆ ของการจัดทำแผนธุรกิจและแผนกลยุทธ์มีประสิทธิภาพ รวมทั้งมีประโยชน์สำหรับตัดสินใจในการดำเนินธุรกิจของ สรอ. ผู้บริหารและหน่วยงานที่เกี่ยวข้องกับความเสี่ยงด้านนโยบายและกลยุทธ์จะต้องร่วมกันกำหนดและทบทวนกลยุทธ์อย่างสม่ำเสมอ เพื่อใช้กำหนดแผนปฏิบัติการ (Action Plan) ในการพัฒนางานเพื่อป้องกันและลดความเสียหายที่อาจจะเกิดขึ้นรวมถึงช่วยให้สามารถบรรลุเป้าหมายและวัตถุประสงค์ของแผนดำเนินงานโดยแผนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่จัดทำขึ้นจะต้องมีรายละเอียดของวัตถุประสงค์ ขอบเขตงาน ผู้มีหน้าที่รับผิดชอบ งบประมาณรองรับ หรือทรัพยากรที่ต้องการผลที่จะได้รับ รวมถึงระยะเวลา การดำเนินงานของแผนที่ชัดเจน เพื่อประโยชน์ในการบริหารและติดตามการดำเนินงานตามแผนการบริหารความเสี่ยงที่กำหนดไว้

ทั้งนี้ การวิเคราะห์สภาพแวดล้อมต้องคำนึงถึงปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อ สรอ. หรือหน่วยงานที่เกี่ยวข้องกับนโยบายหลัก เนื่องจากการวิเคราะห์ถึงสภาพแวดล้อมทั้งภายในและภายนอก (SWOT Analysis) จะทำให้ สรอ. ทราบถึงปัจจัยเสี่ยงที่จะส่งผลกระทบต่อความสำเร็จของ สรอ. ช่วยให้ สรอ. ทราบว่าต้องบริหารจัดการอย่างไร เพื่อสร้างข้อได้เปรียบทางการแข่งขันเมื่อต้องเผชิญกับสภาพการแข่งขันที่รุนแรง

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านนโยบายและกลยุทธ์ อันมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามแผนกลยุทธ์ แผนปฏิบัติการประจำปี และการปฏิบัติตามกฎหมาย กฎระเบียบต่างๆ ที่จะส่งผลต่อการดำเนินงานด้านนโยบายและกลยุทธ์ ต่างๆ ของหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร คณะกรรมการกิจการการจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เป็นต้น

๕.๓ การระบุเหตุการณ์ (Event Identification)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร สามารถระบุเหตุการณ์ความเสี่ยงได้เบื้องต้นตามกระบวนการกำหนดยุทธศาสตร์ของ สรอ. ดังนี้

๑. ความเสี่ยงด้านการกำหนดแผนยุทธศาตร์ หรือแผนการดำเนินงานไม่เหมาะสม สอดคล้องกันของนโยบาย กลยุทธ์ โครงสร้างองค์กร

๒. ความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงาน ไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณา ไม่สามารถติดตามเป้าหมายได้

๓. ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์ หรือแผนปฏิบัติการประจำปี

<u>ความเสี่ยงด้านการกำหนดแผนยุทธศาตร์ หรือแผนการดำเนินงานไม่เหมาะสม สอดคล้องกัน ของนโยบาย กลยุทธ์ โครงสร้างองค์กร</u>

การระบุความเสี่ยง แนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อความสอดคล้องกันของแผนงานต่างๆ ที่จะสนับสนุนยุทธศาสตร์หลักของ สรอ. รวมทั้งความสอดคล้องหรือข้อจำกัดของทรัพยากรที่เกี่ยวข้องกับการดำเนินยุทธศาสตร์ ทั้งทรัพยาการด้านงบประมาณ ด้านบุคลากร หรือระบบสนับสนุนอื่นๆ เช่น ระบบสารสนเทศ โครงสร้างองค์กร เป็นต้น เพื่อให้เกิดการใช้ทรัพยากรอย่างคุ้มค่าและลดความซ้าซ้อน สามารถพิจารณาได้จากความถี่ในการเปลี่ยนแปลง การปรับปรุงแผนปฏิบัติการที่ได้รับอนุมัติจากคณะกรรมการบริหารแล้วในระหว่างปี รวมทั้งปัจจัยภายนอกต่างๆ เช่นนโยบายหน่วยงานกำกับ นโยบายรัฐบาล ที่มีผลต่อการดำเนินกำหนดแผนยุทธศาสตร์ รวมทั้งกำหนดกิจกรรมในการดำเนินโครงการหลักของ สรอ.

<u>ความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงาน ไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณา ไม่สามารถติดตามเป้าหมายได้</u>

การระบุความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงาน ไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณา ไม่สามารถติดตามเป้าหมายได้ เป็นการระบุปัจจัยเสี่ยง แนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อการปฏิบัติงาน ที่ดำเนินการแล้วไม่สามารถทำให้ภาพรวม สรอ. บรรลุเป้าหมายที่แท้จริงได้ตามนโยบายและกลยุทธ์ และแผนงานประจำปี รวมทั้งปัจจัยเสี่ยงของกระบวนการกำหนดหรือการจัดทำเป้าหมายของตัวชี้วัดที่ได้กำหนดไว้ของยุทธศาสตร์ไม่ชัดเจนได้ ซึ่งจะส่งผลต่อการดำเนินกิจกรรมหลักของ สรอ.

<u>ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์ หรือแผนปฏิบัติการประจำปี)</u>

การระบุความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์ หรือแผนปฏิบัติการประจำปี ให้ระบุจากเป้าหมายของ สรอ. ในการกำหนดเป้าหมาย รวมทั้งกิจกรรมตามแผน

ยุทธศาสตร์ ที่อาจไม่บรรลุได้ตามกำหนด หรือความเสี่ยงที่อาจเกิดจากความล่าช้าในการดำเนินกิจกรรมตามแผนยุทธศาตร์ และแผนปฏิบัติการประจำปี รวมทั้งปัจจัยที่จะส่งผลกระทบการการดำเนินกิจกรรมตามแผนงาน เช่น กิจกรรมพัฒนาเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) กิจกรรมพัฒนาระบบเว็บไซต์กลางบริการอิเล็กทรอนิกส์ภาครัฐ (e-Portal) กิจกรรมพัฒนาความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนเพื่อส่งเสริมการพัฒนารัฐบาลอิเล็กทรอนิกส์ (Public-Private Partnership) กิจกรรมยกระดับขีดความสามารถและพัฒนาฐานข้อมูลบุคลากร ICT ภาครัฐ (ICT Training) เป็นต้น

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนนโยบายและกลยุทธ์องค์กร ส่วนการเงินและบัญชี และส่วนพัฒนาความร่วมมือรัฐเอกชน สำนักส่งเสริมและถ่ายทอดเทคโนโลยี ส่วนบริหารทรัพยากรบุคคล สำนัก และส่วนงานต่างๆ ของ สรอ. ที่เกี่ยวข้องกับกลยุทธ์ของ สรอ. จะร่วมกันพิจารณา วิเคราะห์ และกำหนดปัจจัยต่างๆที่มีผลกระทบต่อความสี่ยงด้านนโยบายและกลยุทธ์ ในแต่ละช่วงเวลา ทำให้ประเมินได้ว่าในอนาคต สรอ. จะมีการดำเนินงานตามแผนกลยุทธ์ หรือแผนงานโครงการหลักในช่วงใด

อย่างไรก็ตามส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนนโยบายและกลยุทธ์องค์กร และบัญชี และส่วนวางแผนนโยบายและกลยุทธ์ ยังมีการร่วมพิจารณาถึงความเสี่ยงที่เกิดจากการดำเนินโครงการหลักของ สรอ. ที่ไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการ และของ สรอ.

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงจะพิจารณาปัจจัยการประเมินความเสี่ยง ๒ ด้าน คือ การประเมินโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) จากการเกิดเหตุการณ์ความเสี่ยงเพื่อทราบระดับความรุนแรงของความเสี่ยง ทั้งนี้ความเสี่ยงด้านนโยบายและกลยุทธ์ สามารถประเมินด้วยเครื่องมือเป้าหมายการดำเนินงานที่กำหนดไว้ รวมทั้งการประเมินจากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือ โอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านนโยบายและกลยุทธ์ เหล่านั้นขึ้น เป็นแต่ละเหตุการณ์ เช่น หน่วยงานภาครัฐระดับกระทรวงและกรม ไม่มีการบูรณาการและเชื่อมโยงในเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ได้ตามเป้าหมาย ร้อยละ ๕๐ เกิดจากสาเหตุจำนวนหน่วยงานภาครัฐที่เข้าร่วมการทำ Focus Group เพื่อสร้างการมีส่วนร่วมในการพัฒนา GIN มีจำนวนไม่เป็นไปตามเป้าหมาย เป็นต้น และควรมีการจัดทำ Sensitivity and Simulation Analysis ด้วย

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

<u>ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์ หรือแผนปฏิบัติการประจำปีประสิทธิภาพในการบริหารงบประมาณ</u>

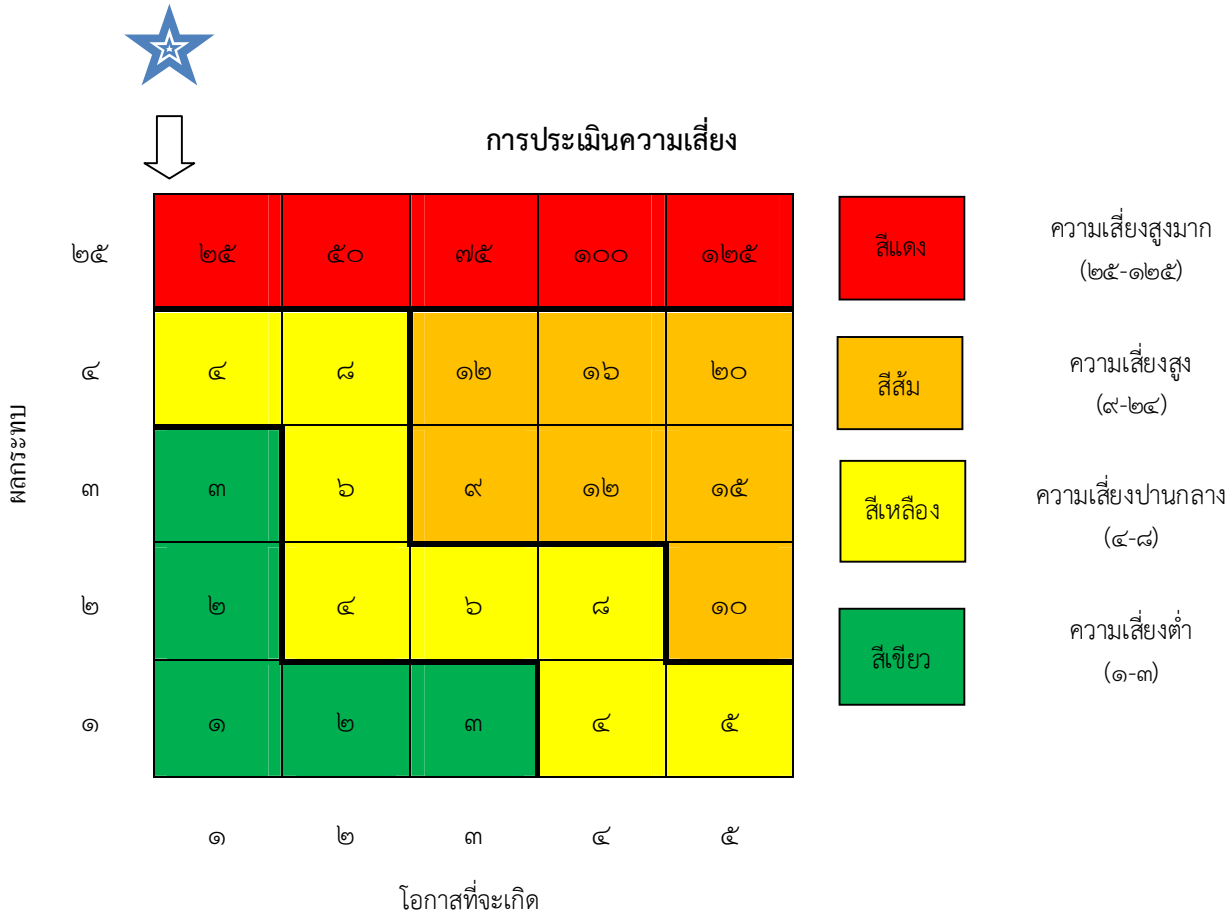
ชื่อปัจจัยเสี่ยง หน่วยงานภาครัฐระดับกระทรวงและกรม ไม่มีการบูรณาการและเชื่อมโยงในเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ได้ตามเป้าหมาย ร้อยละ ๕๐

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	แจ้งหน่วยงานภาครัฐที่เข้าร่วมและยืนยันการเข้าร่วมได้ก่อน ๒ เดือนในทุกครั้งที่มีการจัด Focus Group	แจ้งหน่วยงานภาครัฐที่เข้าร่วมและยืนยันการเข้าร่วมได้ก่อน ๑ เดือนในทุกครั้งที่มีการจัด Focus Group	แจ้งหน่วยงานภาครัฐที่เข้าร่วมและยืนยันการเข้าร่วมได้ก่อน ๒ สัปดาห์ในทุกครั้งที่มีการจัด Focus Group	สามารถแจ้งหน่วยงานภาครัฐที่เข้าร่วมและยืนยันการเข้าร่วมได้ก่อนการจัด ในบางครั้งที่มีการจัด Focus Group	ไม่สามารถแจ้งหน่วยงานภาครัฐที่เข้าร่วมและได้รับยืนยันการเข้าร่วมได้ก่อนการจัดงานในทุกครั้งที่มีการจัด Focus Group
ผลกระทบ	จำนวนหน่วยงานภาครัฐที่เข้าร่วมการทำ Focus Group เพื่อสร้างการมีส่วนร่วมในการพัฒนา GIN มีจำนวนเป็นไปตามเป้าหมาย	จำนวนหน่วยงานภาครัฐที่เข้าร่วมการทำ Focus Group เพื่อสร้างการมีส่วนร่วมในการพัฒนา GIN มีจำนวนเป็นน้อยกว่าเป้าหมายร้อยละ ๕	จำนวนหน่วยงานภาครัฐที่เข้าร่วมการทำ Focus Group เพื่อสร้างการมีส่วนร่วมในการพัฒนา GIN มีจำนวนเป็นน้อยกว่าเป้าหมายร้อยละ ๑๐	จำนวนหน่วยงานภาครัฐที่เข้าร่วมการทำ Focus Group เพื่อสร้างการมีส่วนร่วมในการพัฒนา GIN มีจำนวนเป็นน้อยกว่าเป้าหมายร้อยละ ๑๕	จำนวนหน่วยงานภาครัฐที่เข้าร่วมการทำ Focus Group เพื่อสร้างการมีส่วนร่วมในการพัฒนา GIN มีจำนวนเป็นน้อยกว่าเป้าหมายร้อยละ ๒๐

ชื่อปัจจัยเสี่ยง จำนวนหน่วยงานที่ให้บริการ Cloud แก่หน่วยงานภาครัฐไม่เป็นไปตามเป้าหมาย

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	ดำเนินกิจกรรมตามแผนพัฒนา Data Center Consolidation ได้ครบถ้วนร้อยละ ๑๐๐ ตามแผนงาน	ดำเนินกิจกรรมตามแผนพัฒนา Data Center Consolidation ได้ร้อยละ ๙๕	ดำเนินกิจกรรมตามแผนพัฒนา Data Center Consolidationได้ร้อยละ ๙๐	ดำเนินกิจกรรมตามแผนพัฒนา Data Center Consolidation ได้ร้อยละ ๘๕	ดำเนินกิจกรรมตามแผนพัฒนา Data Center Consolidation ได้ร้อยละ ๘๐
ผลกระทบ	จำนวนหน่วยงานที่ให้บริการ Cloud แก่หน่วยงานภาครัฐเป็นไปตามเป้าหมาย	จำนวนหน่วยงานที่ให้บริการ Cloud แก่หน่วยงานภาครัฐน้อยกว่าเป้าหมายร้อยละ ๕	จำนวนหน่วยงานที่ให้บริการ Cloud แก่หน่วยงานภาครัฐน้อยกว่าเป้าหมายร้อยละ ๑๐	จำนวนหน่วยงานที่ให้บริการ Cloud แก่หน่วยงานภาครัฐน้อยกว่าเป้าหมายร้อยละ ๑๕	จำนวนหน่วยงานที่ให้บริการ Cloud แก่หน่วยงานภาครัฐน้อยกว่าเป้าหมายร้อยละ ๒๐

เมื่อประเมินระดับความเสี่ยงได้แล้ว ขั้นต่อไปคือ การจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญและจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของ สรอ. หรือหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดย สรอ. ได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น ๔ ระดับ ตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้นๆ ได้แก่ ระดับสูงมาก ระดับสูง ระดับปานกลาง ระดับต่ำ ตามลำดับ โดยใช้ตารางแสดงระดับวัดความเสี่ยงเป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมิน ซึ่งตารางจะแสดงข้อมูลเป็น ๒ แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact) ตามตารางแสดงระดับวัดความเสี่ยง



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

ระดับความเสี่ยงด้านนโยบายและกลยุทธ์

	สีเขียวเข้ม	:	ความเสี่ยงด้านนโยบายและกลยุทธ์อยู่ในระดับต่ำ
	สีเหลือง	:	ความเสี่ยงด้านนโยบายและกลยุทธ์อยู่ในระดับปานกลาง
	สีส้ม	:	ความเสี่ยงด้านนโยบายและกลยุทธ์อยู่ในระดับสูง
	สีแดง	:	ความเสี่ยงด้านนโยบายและกลยุทธ์อยู่ในระดับสูงมาก

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้นๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าวที่เหมาะสม เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบ ที่เกิดจากความเสี่ยงนั้นๆ จะทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้นๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าว เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
หน่วยงานภาครัฐระดับกระทรวงและกรม ไม่มีการบูรณาการและเชื่อมโยงในเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ได้ตามเป้าหมาย ร้อยละ 50	๑. เป้าหมายและแผนปฏิบัติการในการบูรณาการและเชื่อมโยงในเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ต้องมีการทบทวนและปรับปรุงอย่างสม่ำเสมอ ๒. สื่อสารทำความเข้าใจกับหน่วยงานที่เกี่ยวข้องเพื่อร่วมกับกำหนดมาตรการเพิ่มเติมในกรณีที่ผลการดำเนินงานไม่บรรลุเป้าหมาย	การลดความเสี่ยง (Treat)

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
จำนวนหน่วยงานที่ให้บริการ Cloud แก่หน่วยงานภาครัฐไม่เป็นไปตามเป้าหมาย	๑. กำหนดให้ฝ่ายงานที่เกี่ยวข้องรายงานความก้าวหน้าการจัด Focus Group ให้ผู้บริหารที่เกี่ยวข้องทราบ ๒. ทบทวนการกำหนดกลุ่มเป้าหมายที่เป็นหน่วยงานภาครัฐเมื่อมีการดำเนินงานในระหว่างปีที่ไม่เป็นไปตามเป้าหมาย ๓. กำหนดแผนงานหรือกิจกรรมเพิ่มเติมเพื่อส่งเสริมให้หน่วยงานภาครัฐเข้าร่วมโครงการให้บริการ Cloud	การลดความเสี่ยง (Treat)

๕.๖ กิจกรรมการควบคุม (Control Activities)

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนการเงินและบัญชี ส่วนโยบายและกลยุทธ์องค์กร มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านนโยบายและกลยุทธ์ โดยจะควบคุมความเสี่ยงทางด้านสภาพคล่องด้านการบริหารเงินลงทุน และอื่นๆ ให้สอดคล้องกับเพดานความเสี่ยง (Risk Limit) หรือตัวบ่งชี้ความเสี่ยงด้านนโยบายและกลยุทธ์ ที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านนโยบายและกลยุทธ์ ของสำนักงานให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการบริหาร สรอ. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

๕.๗ สารสนเทศและการสื่อสาร (Information and Communication)

<u>แหล่งที่มาของข้อมูล</u>

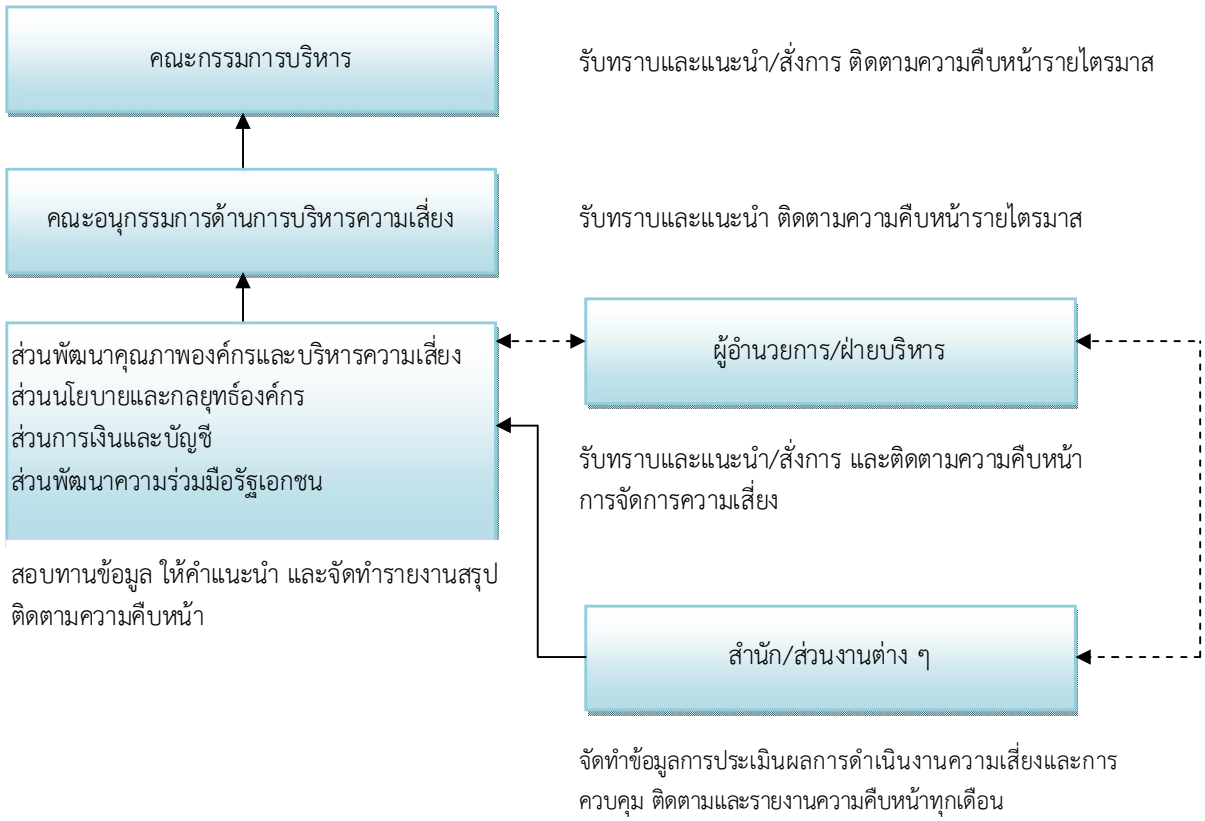
ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนนโยบายและกลยุทธ์องค์กร ส่วนการเงินและบัญชี สำนักบริหารและจัดการองค์กร จัดเก็บข้อมูลซึ่งมีรายละเอียดดังนี้

ข้อมูล	แหล่งที่มา	หมายเหตุ
● แผนนโยบายและกลยุทธ์ ระยะยาว ● แผนนโยบายและกลยุทธ์ประจำปี ● การปรับปรุงแผนการดำเนินงาน	● ส่วนนโยบายและกลยุทธ์องค์กร ● ส่วนการเงินและบัญชี	● พิจารณาจากการจัดทำงบประมาณตามแผนงานทั้งระยะสั้น และระยะยาว ● รายละเอียดกิจกรรมตามแผนงานที่กำหนด
● สถานะการดำเนินงานตามแผนงานทั้งระยะสั้นและระยะยาว ● สถานะการดำเนินงานตามตัวชี้วัดตามยุทธศาสตร์ สรอ.	● ส่วนนโยบายและกลยุทธ์องค์กร	● พิจารณาจากการรายงานความคืบหน้าการติดตามโครงการตามแผนยุทธศาตร์ ● พิจารณาจากการรายงานความคืบหน้าของตัวชี้วัดตามยุทธศาสตร์ ● รายงานปัญหาอุปสรรคและแนวทางแก้ไขของการดำเนินโครงการที่สำคัญ รวมทั้งตามแผนงาน

๕.๘ การติดตามและประเมินผล (Monitoring)

ส่วนนโยบายและกลยุทธ์องค์กร ส่วนการเงินและบัญชี มีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการสรอ. และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านนโยบายและกลยุทธ์ ที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านนโยบายและกลยุทธ์ ในภาพรวมต่อคณะอนุกรรมการบริหารความเสี่ยง เพื่อคณะกรรมการบริหาร สรอ. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่อง ต่อไป

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติ ส่วนนโยบายและกลยุทธ์องค์กรต้องรายงานให้ผู้บริหาร สรอ. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สรอ. / ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการบริหาร
ปานกลาง หรือเตือน (Warning)	รับทราบ/แนะนำ และสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำ และสั่งการ
สูง หรือรุนแรง (Severe)	รับทราบ/แนะนำ และสั่งการรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ
สูงมาก หรือรุนแรงมาก (High Severe)	รับทราบ/แนะนำ/สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ

ความเสี่ยงด้านปฏิบัติงาน
(Operational Risk)

ประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
ที่ ๖ /๒๕๕๕
เรื่อง นโยบายการบริหารความเสี่ยงด้านการปฏิบัติงาน
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

.....

เพื่อให้การดำเนินการบริหารความเสี่ยงด้านการปฏิบัติงาน (Operational Risk Management Policy) ของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) มีความสอดคล้องตามนโยบายการบริหารความเสี่ยงของ สรอ. (Enterprise Risk Management Policy)

โดย สรอ. ตระหนักถึงความสำคัญในการบริหารจัดการความเสี่ยงในการดำเนินงาน จึงได้จัดทำนโยบายการบริหารความเสี่ยงด้านการปฏิบัติงาน (Operational Risk Management Policy) ให้เป็นส่วนหนึ่งของนโยบายการบริหารความเสี่ยง (Enterprise Risk Management Policy) โดยกำหนดให้ สรอ. มีการประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามประเมินผล และการรายงานความเสี่ยงด้านการปฏิบัติงานและจัดให้มีระบบการควบคุมภายในเพื่อใช้ในการควบคุมดูแลการดำเนินงานภายในของ สรอ. ให้คณะกรรมการ ผู้อำนวยการ ผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กร มีส่วนร่วม สร้างความคุ้นเคยและผลักดันให้การบริหารความเสี่ยงด้านการปฏิบัติงานของ สรอ. อยู่ในทุกกระบวนการทำงาน และให้ยึดถือเป็นกลไกหนึ่งในการส่งเสริมให้การดำเนินการของ สรอ. มีประสิทธิภาพ อันจะเป็นส่วนหนึ่งของวัฒนธรรมองค์กรอย่างยั่งยืน และสามารถสร้างมูลค่าเพิ่มให้กับองค์กรและประเทศชาติ

ดังนั้น เพื่อให้การบริหารความเสี่ยงของ สรอ. ด้านการปฏิบัติงานเป็นไปด้วยความเรียบร้อยอย่างมีประสิทธิภาพและประสิทธิผลอาศัยอำนาจตามมาตรา ๒๖ และ ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ.๒๕๕๔ ประกอบกับมติคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ ในคราวประชุมครั้งที่ ๗/๒๕๕๕ เมื่อวันที่ ๑๘ กรกฎาคม ๒๕๕๕ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) จึงกำหนดให้ยึดถือนโยบายการบริหารความเสี่ยงด้านการปฏิบัติงาน ตามคู่มือการบริหารความเสี่ยงด้านการปฏิบัติงานอย่างเคร่งครัดโดยทั่วกัน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๖ สิงหาคม พ.ศ. ๒๕๕๕

(นายศักดิ์ เสกขุนทด)
ผู้อำนวยการ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

คู่มือบริหารความเสี่ยงด้านปฏิบัติงาน
(Operational Risk Management Manual)

สารบัญ

หน้าที่

๑. บทนำ

เพื่อให้การบริหารความเสี่ยงด้านการปฏิบัติงานของสำนักงานรัฐบาลอิเล็กทรอนิกส์(องค์การมหาชน) (สรอ.) เป็นไปในแนวทางเดียวกัน สรอ. จึงได้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านการปฏิบัติงาน (Operational Risk Management Policy) เพื่อบังคับใช้กับทุกหน่วยงานของ สรอ. โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจและตระหนักถึงหน้าที่ความรับผิดชอบต่อการบริหารความเสี่ยงด้านการปฏิบัติงานอยู่เสมอ นับเป็นการสนับสนุนให้ทุกหน่วยงานของ สรอ. มีการบริหารความเสี่ยงด้านการปฏิบัติงานอย่างเป็นระบบ และยังเป็นการส่งเสริมให้มีกระบวนการควบคุมภายในที่ดีอีกทางหนึ่งด้วย และเพื่อให้เจ้าหน้าที่ทุกระดับสามารถเข้าใจต่อการบริหารความเสี่ยงด้านการปฏิบัติงาน สรอ. จึงได้จัดทำคู่มือการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงด้านการปฏิบัติงาน (คู่มือฯ) โดยจะใช้ประกอบในการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งคู่มือฯจะกล่าวลงไปในรายละเอียดเพื่อให้หน่วยงานสามารถวางระบบการบริหารความเสี่ยงด้านการปฏิบัติงานภายในหน่วยงานของตนเองได้อย่างมีประสิทธิภาพ มีกระบวนการการป้องกัน การควบคุมความเสี่ยงด้านการปฏิบัติงานให้ความเสี่ยงอยู่ในระดับที่ สรอ. สามารถยอมรับได้ (Risk Appetite) และระดับความเสี่ยงที่ทนได้ (Risk Tolerance) สามารถลดผลกระทบจากเหตุการณ์ความเสียหายที่อาจเกิดขึ้นต่อ สรอ. และสอดคล้องกับการบริหารความเสี่ยงองค์กร (Enterprise Risk Management)

แนวทางการบริหารความเสี่ยงที่นำมาใช้

สรอ. กำหนดกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานตามแนวทางการปฏิบัติงานของ สรอ. และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Tread way Commission (COSO) โดยการบริหารความเสี่ยงด้านการปฏิบัติงานจะอยู่บนพื้นฐานของการควบคุมภายใน ซึ่งเป็นกระบวนการที่เป็นขั้นตอนที่ต่อเนื่องและแทรกอยู่ในการปฏิบัติงานตามปกติของทุกหน่วยงาน ทั้งนี้เจ้าหน้าที่ในทุกหน่วยงานของ สรอ. มีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งมีผู้บริหารเป็นผู้รับผิดชอบให้มีระบบการบริหารความเสี่ยงด้านการปฏิบัติงาน ตามที่ สรอ. กำหนด คือ มีการระบุ ประเมิน ติดตาม ควบคุม และรายงานความเสี่ยง

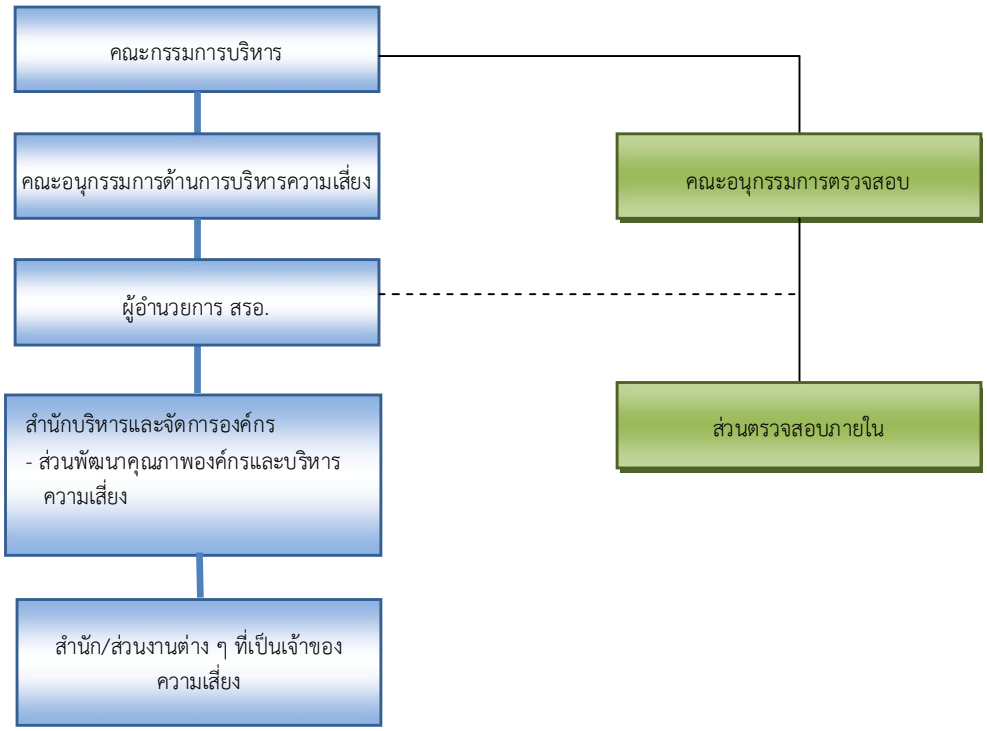
การบริหารความเสี่ยงด้านการปฏิบัติงานควรให้ความมั่นใจอย่างสมเหตุสมผลว่าหน่วยงานจะบรรลุตามเป้าหมายที่ได้กำหนดไว้ กล่าวคือ แม้ว่าจะมีการวางระบบการบริหารความเสี่ยงด้านการปฏิบัติงานไว้ดีเพียงใดก็ไม่สามารถรับรองได้ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้อย่างสมบูรณ์ เพราะมีข้อจำกัดจากปัจจัยอื่นนอกเหนือการควบคุมของหน่วยงาน เช่น ผลกระทบจากปัจจัยภายนอก เป็นต้น

ขอบเขตของคู่มือบริหารความเสี่ยงด้านการปฏิบัติงาน

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งครอบคลุมถึงความเสี่ยงอันเกิดจากการดำเนินงานที่ไม่เป็นไปตามแผนกลยุทธ์ สรอ. รวมทั้งนโยบายที่ได้รับจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งนโยบายภาครัฐ ตั้งแต่การกำหนดแผนงานที่รองรับนโยบายไม่ครบถ้วนการดำเนินงานไม่ได้ตามเป้าหมายแผนกลยุทธ์ของโครงการหลัก รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นปัจจัยภายนอก เช่น การเปลี่ยนแปลงนโยบายภาครัฐ เป็นต้น โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานเพื่อให้หน่วยงานต่างๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านการปฏิบัติงานของตนเอง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านการปฏิบัติงาน



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบดังนี้

๑. กำหนดกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงาน และนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านการปฏิบัติงาน ให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานที่กำหนดในกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงาน

๓. จัดทำคู่มือบริหารความเสี่ยงด้านการปฏิบัติงานและเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๔. ประสานงานกับส่วนปฏิบัติงานและบัญชี ส่วนพัฒนาความร่วมมือรัฐเอกชน และส่วนนโยบายและกลยุทธ์องค์กร เพื่อจัดให้หน่วยงานต่างๆ ดำเนินการพิจารณา Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของหน่วยงานต่างๆ รวมถึงแนวทางการจัดการความเสี่ยงที่เหมาะสม

๕. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่างๆ ให้เข้าใจถึงแนวทาง ความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านการปฏิบัติงาน

๖. ดูแลให้มีการปฏิบัติตามกระบวนการในการออก/ปรับปรุงผลิตภัณฑ์ตามแนวทางที่ สรอ. กำหนดและมีส่วนร่วมพิจารณาให้ความเห็นในการออกผลิตภัณฑ์ในประเด็นที่เกี่ยวข้องกับความเสี่ยง รวมทั้งปรับปรุงหรือแก้ไขข้อบกพร่องที่เกี่ยวกับความเสี่ยงด้านต่างๆ ที่เกิดขึ้นภายหลังการออก/ปรับปรุงผลิตภัณฑ์ โดยดำเนินการร่วมกับหน่วยงานเจ้าของผลิตภัณฑ์นั้นๆ

๗. ร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) สำหรับสถานการณ์ที่ไม่ปกติ เพื่อรองรับการเปลี่ยนแปลงสภาพแวดล้อมที่ไม่เป็นไปตามที่คาดไว้

ผู้ประสานงานความเสี่ยง (Risk Internal Control Officer: RICO)

ทุกหน่วยงานต้องกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็น RICO ประจำหน่วยงาน ซึ่งจะดูแลรับผิดชอบในการประสานงานกับส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงที่จะนำเครื่องมือต่างๆ ที่ใช้ในการบริหารความเสี่ยงด้านการปฏิบัติงานไปใช้บริหารความเสี่ยงด้านการปฏิบัติงานภายในหน่วยงานตนเอง และรายงานข้อมูลที่

เกี่ยวข้องให้ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงตามกำหนดเวลา รวมไปถึงให้ความรู้ที่เกี่ยวกับการบริหารความเสี่ยงด้านการปฏิบัติงานแก่เจ้าหน้าที่ในหน่วยงานของตนเอง ทั้งนี้ เพื่อให้เจ้าหน้าที่ทุกระดับในหน่วยงานตนเองรับทราบถึงความเสี่ยงด้านการปฏิบัติงานโดยรวมและแนวทางแก้ไขที่ได้กำหนดไว้ ดังนั้น RICO จึงควรเป็นบุคคลที่มีความเข้าใจในกระบวนการในการปฏิบัติงานต่างๆของหน่วยงานตนเองเป็นอย่างดี เพื่อจะได้สามารถระบุและประเมินความเสี่ยงด้านการปฏิบัติงานของหน่วยงานตนเองได้อย่างถูกต้องพร้อมทั้งรายงานข้อมูลที่เกี่ยวกับความเสี่ยงด้านการปฏิบัติงานได้อย่างครบถ้วน ถูกต้อง

ผู้จัดการความเสี่ยง (Risk Manager)

ผู้จัดการความเสี่ยง (Risk Manager) หมายถึง หัวหน้าหน่วยงานนั้นๆ โดยเป็นบุคคลที่ทำหน้าที่รับผิดชอบในการบริหารจัดการความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานที่อยู่ภายใต้ความรับผิดชอบของตนเองในฐานะเจ้าของความเสี่ยง (Risk owner) รวมถึงมีหน้าที่ดูแลให้การปฏิบัติงานเป็นไปตามนโยบายและกรอบการบริหารความเสี่ยงด้านการปฏิบัติงานตามที่ สรอ. กำหนด พร้อมทั้งให้ความเห็นชอบต่อข้อมูลที่เกี่ยวกับการบริหารความเสี่ยงด้านการปฏิบัติงานที่ RICO รายงานให้แก่ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง

เจ้าหน้าที่ทุกคน (Employees)

มีหน้าที่ในการปฏิบัติตามนโยบายและกรอบการบริหารความเสี่ยงด้านการปฏิบัติงานตามที่ สรอ. กำหนด รวมไปถึงรับผิดชอบในการบริหารความเสี่ยงด้านการปฏิบัติงานภายใต้ขอบเขตความรับผิดชอบของตน โดยมีหน้าที่ทำความเข้าใจหลักการของความเสี่ยงภายใต้กรอบการบริหารความเสี่ยงของ สรอ. เพื่อให้แน่ใจว่าการบริหารความเสี่ยงด้านการปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพ ส่งผลให้เกิดมูลค่าเพิ่มแก่หน่วยงานและ สรอ. สอดคล้องกับแผนงาน วัตถุประสงค์ และกลยุทธ์ที่กำหนดไว้

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๔.๓ ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)

ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk) คือ ความเสี่ยงที่ทำให้เกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดี หรือขาดธรรมาภิบาลในองค์กร และขาดการควบคุมดูแลที่เหมาะสม โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน คน (เจ้าหน้าที่ บุคคลภายนอก หรือลูกค้า) ระบบงาน หรือเหตุการณ์ภายนอก ซึ่งส่งผลกระทบต่อการดำเนินงานของ สรอ.

ความเสี่ยงด้านการปฏิบัติงาน ยังครอบคลุมถึงเหตุการณ์ความเสียหาย (Loss Incidents) ที่อาจเกิดขึ้นเนื่องจากการดำเนินงานผิดพลาดของหน่วยงาน (Business Unit) ใดๆ ใน สรอ. และสามารถเกิดขึ้นได้กับการปฏิบัติงานในทุกระดับชั้น นอกจากนี้ ความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานหนึ่ง อาจส่งผลกระทบและก่อให้เกิดความเสียหายแก่หน่วยงานอื่นๆ ต่อเนื่องกันไปได้ ดังนั้น จึงมีความจำเป็นที่ในแต่ละหน่วยงานของ สรอ. ต้องมีระบบการบริหารความเสี่ยงด้านการปฏิบัติงานที่มีประสิทธิภาพและเหมาะสมกับสภาวะแวดล้อมในการดำเนินธุรกิจ เพื่อให้มั่นใจว่า สรอ. สามารถจัดการความเสี่ยงด้านการปฏิบัติงานได้ และลดความสูญเสียให้อยู่ในระดับต่ำที่สุด

๔.๔ ที่มาของความเสี่ยงด้านการปฏิบัติงาน สามารถจำแนกได้ ๗ ประเภท ดังนี้

๔.๒.๑. ความเสี่ยงจากการทุจริตจากภายใน (Internal fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายใน สรอ. เพื่อให้ผลประโยชน์ที่เกิดขึ้นจากการทุจริตดังกล่าวตกแก่พวกพ้องของตนเอง

๔.๒.๒. ความเสี่ยงจากการทุจริตจากภายนอก (External Fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายนอก แต่ก่อให้เกิดความเสียหายโดยตรงต่อ สรอ.

๔.๒.๓. ความเสี่ยงจากการจ้างงาน และความปลอดภัยในสถานที่ปฏิบัติงาน (Employment practices and workplace safety) ความเสี่ยงจากการจ้างงานสามารถเกิดขึ้นจากกระบวนการต่าง ๆ ที่เกี่ยวกับการจ้างงาน เช่น การจ่ายค่าตอบแทน การปฏิบัติต่อเจ้าหน้าที่อย่างไม่เป็นธรรม เป็นต้น ซึ่งอาจก่อให้เกิดการลาออก การฟ้องร้อง หรือการหยุดงานประท้วงได้ และสำหรับความปลอดภัยในสถานที่ปฏิบัติงาน หากไม่มีการกำหนดมาตรการการรักษาความปลอดภัยในการปฏิบัติงาน หรือการควบคุมสภาพแวดล้อมในการปฏิบัติงานที่ไม่เพียงพอ อาจส่งผลกระทบต่อสุขภาพของเจ้าหน้าที่ อันเนื่องมาจากโรคภัย หรือได้รับบาดเจ็บจากอุบัติเหตุอันเนื่องมาจากการปฏิบัติงานได้

๔.๒.๔. ความเสี่ยงจากลูกค้า ผลิตภัณฑ์ และวิธีปฏิบัติในการดำเนินธุรกิจ (Clients, Products and Business practices) เป็นความเสี่ยงที่เกิดขึ้นจากวิธีปฏิบัติในการดำเนินธุรกิจ กระบวนการออกแบบพัฒนาผลิตภัณฑ์ และการเข้าถึงข้อมูลลูกค้าที่ไม่เหมาะสม ไม่เป็นไปตามกฎหมาย ระเบียบและข้อบังคับที่ทางการกำหนด เช่น การทำธุรกรรมที่ละเมิดกฎหมาย และการที่ สรอ. นำข้อมูลความลับของลูกค้าไปหาผลประโยชน์ เป็นต้น

๔.๒.๕. ความเสี่ยงด้านความปลอดภัยของทรัพย์สิน (Damage to physical assets) เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ทรัพย์สินของ สรอ. อันเนื่องมาจากภัยต่างๆที่เกิดขึ้น เช่น อุทกภัย วาตภัย อัคคีภัย การก่อการร้าย ความไม่สงบทางการเมือง การก่อวินาศภัย เป็นต้น

๔.๒.๖. ความเสี่ยงจากการขัดข้องหรือการหยุดชะงักของระบบงานและระบบคอมพิวเตอร์ (Business disruption and system failures) เป็นความเสี่ยงที่เกิดขึ้นจากระบบงานที่ผิดปกติ หรือการหยุดทำงานของระบบงานด้านต่างๆ เช่น ความไม่สอดคล้องกันหรือความแตกต่างของระบบงาน ความบกพร่องของระบบงานคอมพิวเตอร์หรือระบบเครือข่าย รวมถึงการใช้เครื่องมือและเทคโนโลยีที่ไม่เหมาะสม ล้าสมัย และไม่มีประสิทธิภาพ เป็นต้น

๔.๒.๗. ความเสี่ยงจากกระบวนการทำงาน (Execution, Delivery and Process management) เป็นความเสี่ยงที่เกิดขึ้นจากความผิดพลาดในวิธีปฏิบัติงาน (Methodology) ความผิดพลาดของระบบการปฏิบัติงาน หรือความผิดพลาดจากการปฏิบัติงานของเจ้าหน้าที่ภายใน สรอ. และเจ้าหน้าที่หรือผู้รับจ้างจากการจ้างงานภายนอก เช่น การบันทึกข้อมูลเข้าระบบผิดพลาด ผู้รับจ้างจากภายนอกไม่ปฏิบัติตามสัญญาการจ้างงาน การขาดความรู้ความเข้าใจในการปฏิบัติงานและการใช้งานระบบคอมพิวเตอร์ของเจ้าหน้าที่ การปรับปรุงกระบวนการทำงานที่ไม่เหมาะสม รวมถึงการจัดทำนิติกรรมสัญญาและเอกสารทางกฎหมายที่ไม่สมบูรณ์ทำให้ไม่สามารถใช้บังคับได้ตามกฎหมาย เป็นต้น

ประเภทความเสี่ยงด้านการปฏิบัติงาน (Risk Event Type)

Operational Risk	People ความเสี่ยงที่เกิดจากบุคลากร	ความเสี่ยงที่เกิดจากการทุจริตภายใน ความเสี่ยงที่เกิดจากการทุจริตภายนอก
	Process ความเสี่ยงที่เกิดจากกระบวนการภายใน	ความเสี่ยงที่เกิดจากการจ้างงานและความปลอดภัยในสถานที่ปฏิบัติงาน
	Systems ความเสี่ยงที่เกิดจากระบบงาน	ความเสี่ยงจากการขัดข้องและหยุดชะงักของระบบงานและระบบคอมพิวเตอร์
	External Events ความเสี่ยงเกิดจากเหตุการณ์ภายนอก	ความเสี่ยงด้านความปลอดภัยของทรัพย์สิน ความเสี่ยงที่เกิดจากกระบวนการทำงาน

ตัวอย่างปัจจัยเสี่ยงด้านการปฏิบัติงาน

ตัวอย่างปัจจัยเสี่ยงด้านการปฏิบัติงาน	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
ไม่สามารถเผยแพร่ผลการศึกษามาตรฐานและ Success Case ได้ตามเป้าหมาย	การจัดทำเล่มและจัดส่งเล่มมาตรฐานเว็บไซต์ให้หน่วยงานที่เกี่ยวข้องล่าช้า	✓	
	จำนวนหน่วยงานภาครัฐที่เข้าร่วมอบรมและสัมมนาเผยแพร่ความรู้สถาปัตยกรรมและมาตรฐานรัฐบาลอิเล็กทรอนิกส์ ของหน่วยงานภาครัฐ		✓
ระบบสนับสนุนการแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ (e-Sarabun) ปรับปรุงให้เป็นแบบ Cloud ล่าช้า ส่งผลให้ทำให้ระบบสารบรรณอิเล็กทรอนิกส์ไม่เกิดความเสถียรมั่นคงปลอดภัย และมีเครื่องมือช่วยในการพัฒนาระบบที่สมบูรณ์	การปรับปรุงเรื่องระบบสถาปัตยกรรมให้เป็นแบบ Cloud มีความล่าช้ากว่าแผนงานมาก	✓	
	จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการไม่เป็นไปตามเป้าหมาย	✓ อาจเป็นปัจจัยภายในหากการวางแผนการตลาดไม่ดีพอ	✓ อาจเป็นปัจจัยภายนอกหากงบประมาณของหน่วยงานภาครัฐที่ใช้บริการถูกจำกัด
ไม่สามารถให้ข้อเสนอแนะเชิงนโยบาย (Policy Recommendation) เกี่ยวกับแนวทางในการพัฒนารัฐบาลอิเล็กทรอนิกส์ จากการดำเนินงาน	หน่วยงานภายใน สรอ. ไม่สามารถประสานงานกับหน่วยงานภายนอกหรือบุคคลภายนอกเพื่อสร้าง Strategic Partners ที่สามารถร่วมวิจัย ให้ข้อมูล รวมถึง ร่วมผลักดันให้งานวิจัยเชิงนโยบายที่เกิดขึ้นได้ถูกนาไปปฏิบัติ	✓	
	ไม่สามารถดำเนินกิจกรรมในการร่วมกับกลุ่มสังคมออนไลน์เพื่อทำให้เกิดการวิจัยนโยบายผ่าน e-Participation ได้ตามแผนงาน	✓	

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

การวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงทางปฏิบัติงานนั้น จากการที่สำนักงานเป็นหน่วยงานกลางของประเทศในการผลักดันและขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ โดยมีพันธกิจคือ การพัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์ โดยมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงทางปฏิบัติงานเพื่อให้มีกระบวนการในการบริหารความเสี่ยงด้านการปฏิบัติงานให้เป็นไปตามหลักมาตรฐานสากลและเป็นมาตรฐานเดียวกันทั่วทั้ง สรอ. เช่นเดียวกับกระบวนการบริหารความเสี่ยงด้านอื่นๆ โดยจะครอบคลุมการปฏิบัติงานในทุกระดับชั้นของแต่ละหน่วยงานใน สรอ. เพื่อช่วยให้การดำเนินงานเกิดผลดีและปฏิบัติงานได้ตามกฎระเบียบที่เกี่ยวข้อง โดยแผนการบริหารความเสี่ยงด้านการปฏิบัติงานที่จัดทำขึ้นจะต้องมีรายละเอียดของวัตถุประสงค์ ขอบเขตงาน ผู้มีหน้าที่รับผิดชอบ งบประมาณรองรับ หรือทรัพยากรที่ต้องการผลที่จะได้รับ รวมถึงระยะเวลา การดำเนินงานของแผนที่ชัดเจน เพื่อประโยชน์ในการบริหารและติดตามการดำเนินงานตามแผนการบริหารความเสี่ยงที่กำหนดไว้

ทั้งนี้การวิเคราะห์สภาพแวดล้อมต้องคำนึงถึงระบบงานที่รองรับการปฏิบัติงานในทุกขั้นตอนของ สรอ. ได้แก่ กระบวนการ เทคโนโลยี สารสนเทศ อุปกรณ์ บุคลากรความเพียงพอของข้อมูล ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินงานที่มีผลกระทบต่อ สรอ.

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านการปฏิบัติงานอันมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามกระบวนการหรือขั้นตอนการปฏิบัติงาน รวมทั้งการปฏิบัติตามกฎหมาย กฎระเบียบต่างๆ ที่จะส่งผลต่อการดำเนินงานด้านการปฏิบัติงาน ต่างๆ ของหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ก.พ.ร. เป็นต้น

๕.๓ การระบุเหตุการณ์ (Event Identification)

การระบุเหตุการณ์ความเสี่ยง จะเริ่มด้วยการแจกแจงกระบวนการปฏิบัติงาน (Work flow) เพื่อให้ได้ทราบขั้นตอนงานที่มีอยู่และจะทำให้บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยหน่วยงานต้องมีการระบุจุด/พื้นที่ ที่มี

ความเสี่ยง (Key Risk Area) และสาเหตุหรือปัจจัยของความเสี่ยง (Risk Factor) ในแต่ละผลิตภัณฑ์/บริการ หรือในแต่ละระบบงานก่อนที่จะมีกิจกรรมการควบคุม (Control Activities) เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่ (Inherent Risk) ผ่านระบบการควบคุมภายในและการประเมินการควบคุมความเสี่ยงด้วยตนเอง (Risk and Control Self Assessment หรือ RCSA) โดยการระบุความเสี่ยงของหน่วยงานนั้น ควรดำเนินการในทุกระดับตั้งแต่ระดับปฏิบัติงานขึ้นไปจนถึงระดับบริหาร และครอบคลุมในทุกกิจกรรมของหน่วยงานทั้งนี้ หน่วยงานควรมีการทบทวนการระบุความเสี่ยงด้านการปฏิบัติงานที่มีอยู่อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงของปัจจัยความเสี่ยงต่างๆ ที่ส่งผลกระทบต่อกระบวนการในการปฏิบัติงาน เช่น ระบบหรือขั้นตอนที่ในการปฏิบัติงานเปลี่ยนไป มีการเปลี่ยนแปลงโครงสร้างองค์กร การเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ การออกผลิตภัณฑ์ใหม่ ๆ การเปลี่ยนแปลงทางกฎหมาย และกฎระเบียบข้อบังคับต่างๆ เป็นต้น ทั้งนี้ ในการระบุความเสี่ยงเบื้องต้น หน่วยงานสามารถระบุความเสี่ยงได้จากแผนผังกระบวนการทำงานหรือขั้นตอนการปฏิบัติงาน (Working Process/Work Flow) หรือข้อมูลเหตุการณ์ความเสียหายที่เคยเกิดขึ้นกับหน่วยงาน (Loss Incidents)

<u>ความเสี่ยงด้านกระบวนการทำงานหรือขั้นตอนในการปฏิบัติงาน</u>

ในการระบุความเสี่ยงนั้นหน่วยงานเจ้าของความเสี่ยง (Risk Owner) จะต้องทำความเข้าใจเกี่ยวกับกระบวนการทำงานหรือขั้นตอนการปฏิบัติงานของตนเอง เพื่อสามารถระบุจุดที่อาจเกิดความเสี่ยง (Key Risk Area) ซึ่งวิธีที่นิยมในการระบุจุดความเสี่ยงนั้น จะสร้างแผนผังกระบวนการทำงานหรือขั้นตอนการปฏิบัติงาน ซึ่งมีการระบุถึงปัจจัยความเสี่ยง เอกสาร ระบบงาน และผู้รับผิดชอบที่เกี่ยวข้องในแต่ละกระบวนการทำงานอย่างชัดเจน และการจัดทำแผนผังกระบวนการทำงานและสัญลักษณ์ที่ใช้ของแต่ละหน่วยงาน ควรกำหนดใช้สัญลักษณ์แทนในแต่ละกระบวนการทำงานที่เป็นมาตรฐานเดียวกันทั้ง สรอ.

<u>ความเสี่ยงด้านข้อมูลเหตุการณ์ความเสียหาย</u> (Loss Incidents)

ในการระบุความเสี่ยงนั้น สามารถนำข้อมูลจากเหตุการณ์ความเสียหายของหน่วยงานที่เคยเกิดขึ้นในอดีต ซึ่งจะช่วยให้หน่วยงานทราบถึงความรุนแรง (Severity) และโอกาส (Likelihood) ที่จะเกิดความเสี่ยงเหล่านั้นอีก นอกจากนี้ ยังช่วยให้หน่วยงานสามารถคาดคะเนหรือระบุความเสี่ยงที่อาจจะเกิดขึ้นในอนาคตได้ หากปัจจัยแวดล้อมต่างๆ ของหน่วยงานไม่ได้เปลี่ยนแปลงไปอย่างมีนัยสำคัญ

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง และหน่วยงานต่างๆ ของ สรอ. ที่เกี่ยวข้องกับกระบวนการดำเนินงานที่สำคัญจะร่วมกันพิจารณา วิเคราะห์ และกำหนดปัจจัยต่างๆที่มีผลกระทบต่อความสี่ยงด้านการปฏิบัติงานในแต่ละกระบวนการ หรือกระบวนการ/โครงสร้างองค์กร/เทคโนโลยี ที่มีการเปลี่ยนแปลงอย่างเป็นนัยสำคัญ

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

เมื่อหน่วยงานได้มีการระบุจุดที่อาจก่อให้เกิดความเสี่ยง (Key Risk Area) และสาเหตุ/ปัจจัยที่ก่อให้เกิดความเสี่ยง (Risk Factor) ในแต่ละกระบวนการทำงานแล้ว หน่วยงานต้องมีการประเมินความเสี่ยงด้านการปฏิบัติงานในแต่ละจุดที่มีความเสี่ยงในแต่ละขั้นตอนการปฏิบัติงาน ซึ่งต้องอาศัยดุลยพินิจและประสบการณ์ของผู้ปฏิบัติงานในหน่วยงาน รวมถึงข้อมูลความเสี่ยงที่เคยเกิดขึ้นในอดีตเป็นสำคัญ โดยจะพิจารณาจาก ๒ ปัจจัย คือ

- โอกาสที่จะเกิดความเสี่ยง (Likelihood) โดยพิจารณาจากความถี่ของเหตุการณ์ที่เกิดขึ้นในอดีตและประมาณโอกาสที่จะเกิดขึ้นในอนาคต

- ระดับความรุนแรงของผลกระทบ (Severity of Impact) ที่เกิดจากความเสี่ยงนั้นๆ พิจารณาจากความรุนแรงของเหตุการณ์ในอดีตและประมาณความรุนแรงของเหตุการณ์ที่อาจเกิดขึ้นในอนาคตเพื่อหน่วยงานจะได้ทราบถึงระดับความเสี่ยงที่มีอยู่ (Inherent Risk) และยังเป็นข้อมูลสำหรับการจัดลำดับความสำคัญในการดำเนินการปรับปรุง ควบคุม และลดความเสี่ยงต่อไป

ทั้งนี้ ในขั้นตอนของการระบุและการประเมินความเสี่ยงของหน่วยงานนั้น จะต้องพิจารณาถึงปัจจัยเสี่ยงทั้งภายในและภายนอกหน่วยงานประกอบด้วย เช่น คุณภาพของบุคลากร อัตราการหมุนเวียนของเจ้าหน้าที่ กระบวนการในการปฏิบัติงาน สภาพการแข่งขัน ความก้าวหน้าของเทคโนโลยี กฎหมายหรือกฎระเบียบข้อบังคับต่างๆ และสภาวะเศรษฐกิจ เป็นต้น นอกจากนี้ การระบุและประเมินความเสี่ยงของหน่วยงานควรดำเนินการอย่างต่อเนื่องและทบทวนความเหมาะสมเป็นระยะ

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ชื่อปัจจัยเสี่ยง ไม่สามารถเผยแพร่ผลการศึกษา, มาตรฐาน และ Success Case ได้ตามเป้าหมาย

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	การจัดทำเล่มและจัดส่งเล่มมาตรฐานเว็บไซต์ให้หน่วยงานที่เกี่ยวข้องได้เร็วกว่าแผนงานมากกว่า ๑ เดือน	การจัดทำเล่มและจัดส่งเล่มมาตรฐานเว็บไซต์ให้หน่วยงานที่เกี่ยวข้องได้เร็วกว่าแผนงาน ๑ เดือน	การจัดทำเล่มและจัดส่งเล่มมาตรฐานเว็บไซต์ให้หน่วยงานที่เกี่ยวข้องได้ตามแผน	การจัดทำเล่มและจัดส่งเล่มมาตรฐานเว็บไซต์ให้หน่วยงานที่เกี่ยวข้องได้ล่าช้ากว่าแผนงาน ๑ เดือน	การจัดทำเล่มและจัดส่งเล่มมาตรฐานเว็บไซต์ให้หน่วยงานที่เกี่ยวข้องได้ล่าช้ากว่าแผนงานมากกว่า ๑ เดือน

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
ผลกระทบ	จำนวนหน่วยงานภาครัฐที่เข้าร่วมอบรมและสัมมนาเผยแพร่ความรู้สถาปัตยกรรมและมาตรฐานรัฐบาลอิเล็กทรอนิกส์ ของหน่วยงานภาครัฐมากกว่าเป้าหมายร้อยละ ๒๐	จำนวนหน่วยงานภาครัฐที่เข้าร่วมอบรมและสัมมนาเผยแพร่ความรู้สถาปัตยกรรมและมาตรฐานรัฐบาลอิเล็กทรอนิกส์ ของหน่วยงานภาครัฐมากกว่าเป้าหมายร้อยละ ๑๐	จำนวนหน่วยงานภาครัฐที่เข้าร่วมอบรมและสัมมนาเผยแพร่ความรู้สถาปัตยกรรมและมาตรฐานรัฐบาลอิเล็กทรอนิกส์ ของหน่วยงานภาครัฐได้ตามเป้าหมาย	จำนวนหน่วยงานภาครัฐที่เข้าร่วมอบรมและสัมมนาเผยแพร่ความรู้สถาปัตยกรรมและมาตรฐานรัฐบาลอิเล็กทรอนิกส์ ของหน่วยงานภาครัฐน้อยกว่าเป้าหมายร้อยละ ๑๐	จำนวนหน่วยงานภาครัฐที่เข้าร่วมอบรมและสัมมนาเผยแพร่ความรู้สถาปัตยกรรมและมาตรฐานรัฐบาลอิเล็กทรอนิกส์ ของหน่วยงานภาครัฐน้อยกว่าเป้าหมายร้อยละ ๒๐

ชื่อปัจจัยเสี่ยง ระบบสนับสนุนการแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ (e-Sarabun) ปรับปรุงให้เป็นแบบ Cloud ล่าช้าส่งผลให้ทำให้ระบบสารบรรณอิเล็กทรอนิกส์ไม่เกิดความเสถียร มั่นคงปลอดภัย และมีเครื่องมือช่วยในการพัฒนาระบบที่สมบูรณ์

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	การปรับปรุงเรื่องระบบสถาปัตยกรรมให้เป็นแบบ Cloud ได้แล้วเสร็จเร็วกว่าแผนงานมากกว่า ๑ เดือน	การปรับปรุงเรื่องระบบสถาปัตยกรรมให้เป็นแบบ Cloud ได้แล้วเสร็จเร็วกว่าแผนงาน ๑ เดือน	การปรับปรุงเรื่องระบบสถาปัตยกรรมให้เป็นแบบ Cloud แล้วเสร็จตามแผนงาน	การปรับปรุงเรื่องระบบสถาปัตยกรรมให้เป็นแบบ Cloud แล้วเสร็จล่าช้ากว่าแผนงาน ๑ เดือน	การปรับปรุงเรื่องระบบสถาปัตยกรรมให้เป็นแบบ Cloud แล้วเสร็จล่าช้ากว่าแผนงานมากกว่า ๑ เดือน
ผลกระทบ	จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการมากกว่าเป้าหมาย ร้อยละ ๒๐	จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการมากกว่าเป้าหมาย ร้อยละ ๑๐	จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการไม่เป็นไปตามเป้าหมาย	จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการน้อยกว่าเป้าหมาย ร้อยละ ๑๐	จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการน้อยกว่าเป้าหมาย ร้อยละ ๒๐

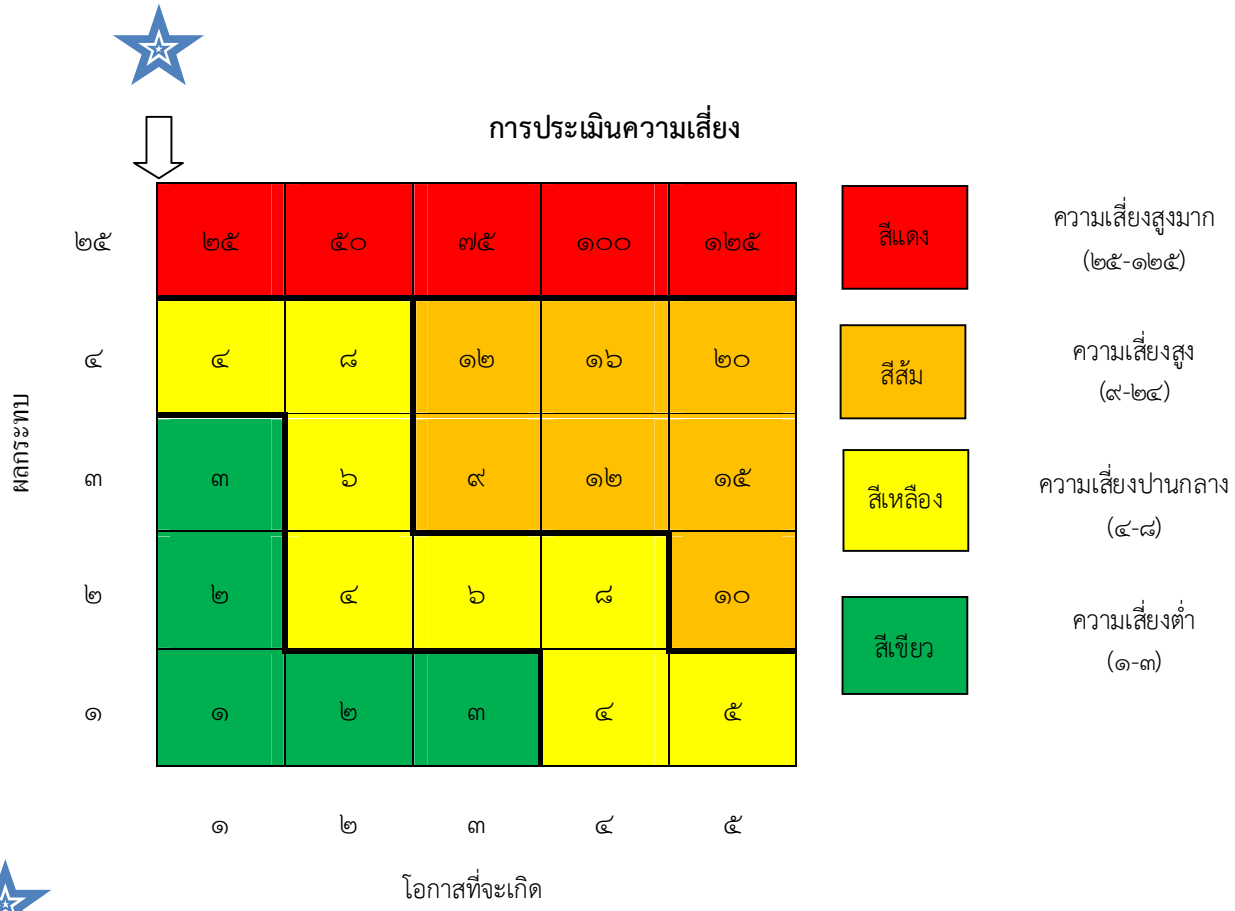
เมื่อประเมินระดับความเสี่ยงได้แล้ว ขั้นต่อไปคือ การจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญและจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของ สรอ. หรือหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดย สรอ. ได้แยกระดับความสำคัญหรือความ

รุนแรงของความเสี่ยงออกเป็น ๔ ระดับ ตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้นๆ ได้แก่ ระดับสูงมาก ระดับสูง ระดับปานกลาง ระดับต่ำ ตามลำดับ โดยใช้ตารางแสดงระดับวัดความเสี่ยงเป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมิน ซึ่งตารางจะแสดงข้อมูลเป็น ๒ แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact) ตามตารางแสดงระดับวัดความเสี่ยง

สรอ. ได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น ๔ โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
๑-๓	ต่ำ	ระดับความเสี่ยงที่องค์กรยอมรับ (Acceptable) ซึ่งอาจมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
๔-๘	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ แต่ต้องมีมาตรการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงมีค่าสูงขึ้นไปยังระดับที่ไม่สามารถยอมรับได้
๙-๒๔	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้ (มีแผนควบคุมความเสี่ยง)
๒๕ ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจำเป็นต้องเร่งจัดการความเสี่ยงจนกระทั่งให้อยู่ในระดับที่สามารถยอมรับได้ทันที หรืออาจมีการถ่ายโอนความเสี่ยง

โดยแสดงเป็นตาราง ๒ มิติ แสดงการแบ่งระดับความเสี่ยงทั้ง ๔ โซน ดังนี้



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้นๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าวที่เหมาะสม เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบ ที่เกิดจากความเสี่ยงนั้นๆ จะทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้นๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยง

ดังกล่าว เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
ไม่สามารถเผยแพร่ผลการศึกษา, มาตรฐาน และ Success Case ได้ตามเป้าหมาย	๑. ประสานงานกับหน่วยงานที่ต้องรายงานผลการศึกษามาตรฐาน และ Success Case เพื่อนำจัดทำเล่มคู่มือ และเตรียมหลักสูตรในการจัดอบรมเป็นรายเดือน และประสานงานกับโรงพิมพ์ เพื่อให้การจัดทำคู่มือแล้วเสร็จได้ตามแผนงาน ๒. สื่อสารทำความเข้าใจกับหน่วยงานภาครัฐในการประชาสัมพันธ์ /แจ้งกำหนดการอบรม สัมมนาล่วงหน้า ในการเผยแพร่ความรู้สถาปัตยกรรมและมาตรฐานรัฐบาลอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ	การลดความเสี่ยง (Treat)

๕.๖ กิจกรรมการควบคุม (Control Activities)

ระบบการควบคุมภายในที่มีประสิทธิภาพนับเป็นกลไกพื้นฐานสำคัญในการควบคุมและป้องกันความเสียหายที่อาจเกิดขึ้นแก่หน่วยงาน ดังนั้น เมื่อหน่วยงานได้ทำการระบุและประเมินความเสี่ยงด้านการปฏิบัติงานแล้วควรดำเนินการจัดอันดับของความเสี่ยงตามลำดับความสำคัญหรือตามความรุนแรงของผลกระทบของความเสี่ยงนั้นๆ เพื่อหน่วยงานสามารถวางระบบการควบคุมความเสี่ยงในแต่ละประเภท ซึ่งวัตถุประสงค์หลักของระบบควบคุม คือ การควบคุมความเสี่ยงด้านการปฏิบัติงานให้อยู่ในระดับที่หน่วยงานและ สรอ. สามารถยอมรับได้ และเพื่อให้มั่นใจว่าการดำเนินงานเป็นไปตามวัตถุประสงค์ที่หน่วยงานหรือ สรอ. ได้วางไว้ รวมถึงต้องมีการติดตามและรายงานต่อคณะกรรมการบริหาร สรอ. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

อย่างไรก็ตาม การพัฒนาระบบการควบคุมความเสี่ยงด้านการปฏิบัติงานที่เหมาะสมของหน่วยงานนั้นหน่วยงานควรพิจารณาถึงปัจจัยต่างๆ เหล่านี้ด้วย

• ความมีประสิทธิภาพของระบบการควบคุมความเสี่ยง จะต้องสามารถลดความเสี่ยงด้านการปฏิบัติงานได้อย่างชัดเจนและมีความเกี่ยวข้องโดยตรงกับสาเหตุหลักของความเสี่ยง

• ผลกระทบต่อประสิทธิภาพของการดำเนินงาน โดยระบบการควบคุมความเสี่ยงที่เหมาะสมนั้นควรสร้างผลกระทบที่น้อยที่สุดต่อระยะเวลาที่ใช้ในการปฏิบัติงาน ต้นทุน/ค่าใช้จ่าย บุคลากร และคุณภาพของงาน

• ความยากง่ายในการนำไปปฏิบัติ โดยควรมีต้นทุนของการนำไปปฏิบัติต่ำ และสามารถนำไปปฏิบัติได้ในเวลาที่รวดเร็ว

๕.๗ สารสนเทศและการสื่อสาร (Information and Communication)

<u>แหล่งที่มาของข้อมูล</u>

ส่วนพัฒนาองค์กรและบริหารความเสี่ยง เป็นหน่วยงานกลางในตามติดตามเพื่อจัดเก็บข้อมูลตามปัจจัยเสี่ยงด้านการปฏิบัติงาน ซึ่งมีรายละเอียดเช่น ตัวอย่างดังนี้

ข้อมูล	แหล่งที่มา	หมายเหตุ
● โครงสร้างองค์กรที่มีการเปลี่ยนแปลง ● ระบบหรือขั้นตอนที่ใช้ในการปฏิบัติงาน	● ส่วนบริหารทรัพยากรบุคคล	● พิจารณาจากการจัดทำโครงสร้างองค์กรฉบับปรับปรุง ● รายละเอียดระบบหรือขั้นตอนการปฏิบัติงานที่สำคัญโดยเฉพาะโครงการหลัก
● การเปลี่ยนแปลงทางกฎหมาย และกฎระเบียบข้อบังคับต่างๆ	● ส่วนนิติการ	● พิจารณาจากการรายงานการเปลี่ยนแปลงทางกฎหมาย และกฎระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้อง กับสรอ.

๕.๘ การติดตามและประเมินผล (Monitoring)

ส่วนงานที่เกี่ยวข้องและเป็นหน่วยงานเจ้าของความเสี่ยงมีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการ สรอ. และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านการปฏิบัติงานที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านการปฏิบัติงานใน

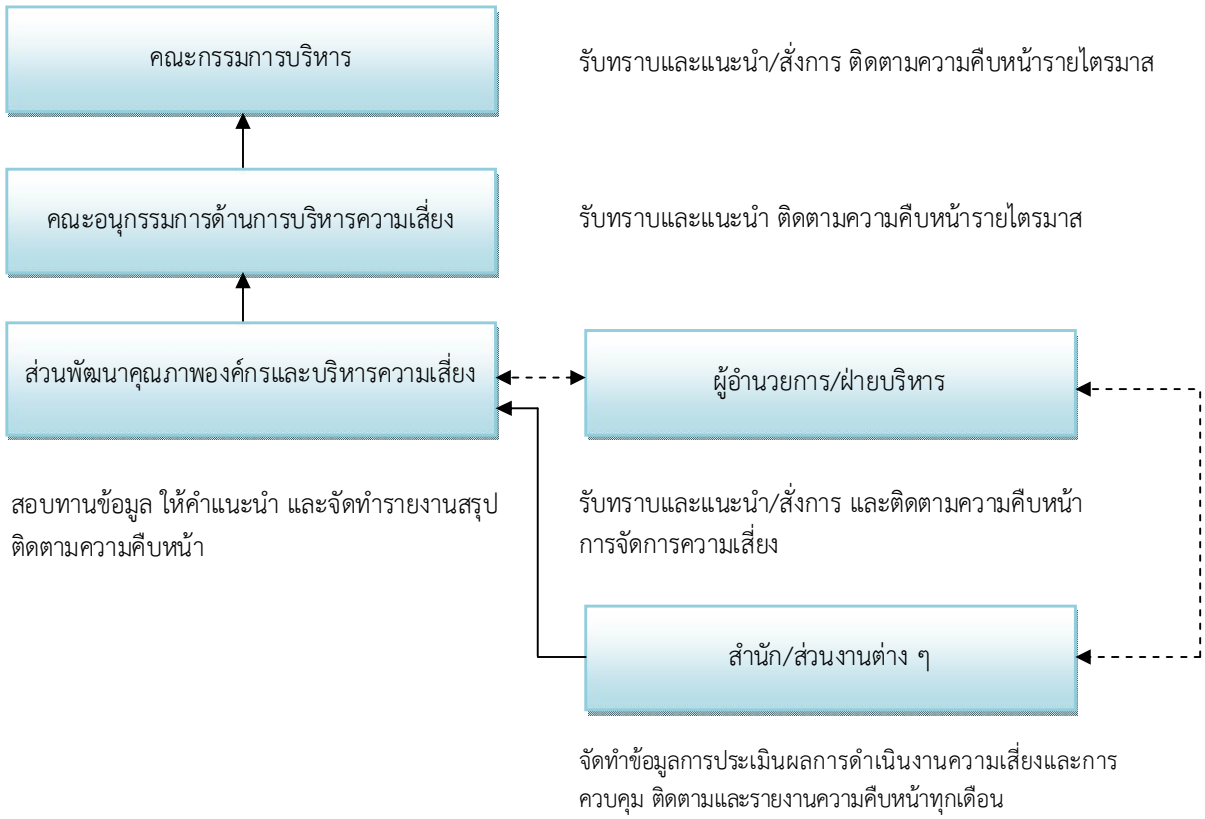
ภาพรวมต่อคณะอนุกรรมการบริหารความเสี่ยง เพื่อคณะกรรมการบริหาร สรอ. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่อง ต่อไป

ทั้งนี้หน่วยงานต้องรายงานเหตุการณ์ความเสียหายที่เกิดจากความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานทันทีหรือภายในวันทำการถัดไป และในกรณีที่ไม่มีเหตุการณ์ความเสียหายฯ หน่วยงานก็ต้องรายงานให้ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงทราบด้วย เพื่อให้มั่นใจว่าส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงได้รับข้อมูลที่ถูกต้องและครบถ้วน โดยข้อมูลทั้งหมดนั้นส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงจะรวบรวมสรุปผล พร้อมวิเคราะห์จุดที่เกิดความเสี่ยง (Risk Area) เพื่อหาแนวทางในการป้องกันแก้ไข และนำเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง หรือคณะอนุกรรมการที่เกี่ยวข้องต่อไป ทั้งนี้ หากมีความเสียหายฯ ที่มีนัยสำคัญเกิดขึ้นกับหน่วยงาน หน่วยงานจะต้องมีการจัดทำ ActionPlan เพื่อลดหรือป้องกันไม่ให้เกิดความเสียหายดังกล่าวขึ้นกับ สรอ. ได้อีกในอนาคต

สรุปความสัมพันธ์ของการบริหารความเสี่ยงด้านการปฏิบัติงาน
กับเครื่องมือบริหารความเสี่ยงด้านการปฏิบัติงาน

เครื่องมือบริหารความเสี่ยง	กระบวนการบริหารความเสี่ยงที่เกี่ยวข้อง	การนำเครื่องมือบริหารความเสี่ยงมาใช้ในหน่วยงาน
Risk Control Self Assessment : RCSA	- การระบุ - การประเมิน - การควบคุม - การรายงาน - การติดตาม	กำหนดให้หน่วยงานจัดทำปีละ ๑ ครั้ง เป็นอย่างน้อย
Operational Loss Data	- การระบุ - การรายงาน - การติดตาม	กำหนดให้หน่วยงานรายงานเป็นรายเดือน โดยต้องรายงานทั้งในกรณีที่มีความเสียหาย และไม่มีความเสียหาย
Key Risk Indicator : KRIs	- การรายงาน - การติดตาม	ความถี่ในการติดตามและรายงาน KRIs มีทั้งรายสัปดาห์ รายเดือน รายไตรมาส รายครึ่งปี และรายปี ขึ้นอยู่กับ KRIs แต่ละตัว

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติ ส่วนนโยบายและกลยุทธ์องค์กรต้องรายงานให้ผู้บริหาร สรอ. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สรอ. / ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการบริหาร
ปานกลาง หรือเตือน (Warning)	รับทราบ/แนะนำ และสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำ และสั่งการ
สูง หรือรุนแรง (Severe)	รับทราบ/แนะนำ และสั่งการรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ
สูง หรือรุนแรงมาก (High Severe)	รับทราบ/แนะนำ/ สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ

ความเสี่ยงด้านการเงิน
(Financial Risk)

EGA
e-Government Agency

ประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

ที่ ๑๐ /๒๕๕๕

เรื่อง นโยบายบริหารความเสี่ยงด้านการเงิน

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

.....

เพื่อให้การบริหารความเสี่ยงด้านการเงินของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) มีการวางแผน ควบคุม เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับ สรอ. ภายใต้ความเปลี่ยนแปลงของสิ่งแวดล้อมต่างๆ ทั้งภายในและภายนอก โดยเฉพาะสิ่งแวดล้อมภายนอกด้านการเงินที่ไม่อาจจะควบคุมได้ เช่น ภาวะเศรษฐกิจตกต่ำ ภาวะเงินเฟ้อเกินระดับปกติ ความผันผวนของอัตราดอกเบี้ย อัตราแลกเปลี่ยน ราคาน้ำมัน ตลอดจนการล่มสลายของเศรษฐกิจในบางประเทศ ซึ่งล้วนแล้วแต่เป็นปัจจัยเสี่ยงจากภายนอกที่มีผลกระทบต่อความเสี่ยงด้านการเงินตั้งแต่ระดับมหภาคสู่ระดับจุลภาคในแต่ละประเทศที่รวมถึง สรอ. ด้วย เนื่องจาก สรอ. เป็นหน่วยงานรัฐที่ได้รับการจัดสรรงบประมาณจากรัฐบาล และจัดหารายได้ได้เองเป็นบางส่วนภายใต้วัตถุประสงค์ตามพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ จึงย่อมได้รับผลกระทบจากปัจจัยเสี่ยงด้านการเงินจากภายนอกที่กล่าวข้างต้น อีกทั้ง สรอ. ยังมีปัจจัยเสี่ยงด้านการเงินที่อาจเกิดขึ้นภายในสำนักงานเองด้วย เช่น นโยบายและกลยุทธ์ระดับองค์กรที่ต้องเปลี่ยนแปลงให้สอดคล้องกับสถานการณ์แวดล้อมทุกด้าน ซึ่งส่งผลต่อการบริหารจัดการงบประมาณ การจัดทำแผนประมาณการงบการเงิน งบกระแสเงินสด การบริหารโครงสร้างเงินทุน การบริหารการลงทุน นโยบายการดำรงเงินสดขั้นต่ำให้เพียงพอเพื่อใช้ในการดำเนินงาน รวมถึงการเกิดเหตุการณ์วิกฤติ ฉุกเฉินต่างๆ หรือแม้แต่การปฏิบัติและไม่ปฏิบัติตามนโยบาย กฎหมาย ข้อบังคับ ระเบียบต่างๆที่เกี่ยวข้องทางด้านการเงิน เป็นต้น ทั้งหมดนี้ล้วนแล้วแต่เป็นความเสี่ยงด้านการเงินที่ต้องบริหารจัดการและกำหนดไว้ในแผนการบริหารความเสี่ยงทางการเงินทั้งระยะสั้นและระยะยาว ที่ต้องสอดคล้องกับแผนธุรกิจ แผนกลยุทธ์ ของ สรอ.

ทั้งนี้ สรอ. ตระหนักถึงความสำคัญในการบริหารความเสี่ยงในการดำเนินงาน จึงได้จัดทำนโยบายบริหารความเสี่ยงด้านการเงิน (Financial Risk Management Policy) ซึ่งเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยง (Enterprise Risk Management Policy) โดยได้กำหนดกระบวนการบริหารความเสี่ยงด้านการเงินให้ครอบคลุมทุกสถานการณ์ เพื่อเป็นแนวทางปฏิบัติ ตั้งแต่การระบุความเสี่ยง การประเมินความเสี่ยง การวัดความเสี่ยง การควบคุมความเสี่ยง การติดตาม และการรายงานความเสี่ยงด้านการเงิน เพื่อให้คณะกรรมการ ผู้อำนวยการ ผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กร จะต้องมีส่วนร่วม สร้างความคุ้นเคยและผลักดันให้การบริหารความเสี่ยงด้านการเงินของ สรอ. อยู่ในทุกกระบวนการทำงาน และยึดถือเป็นกลไกหนึ่งในการส่งเสริมให้การดำเนินการของ สรอ. มีประสิทธิภาพ เพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของวัฒนธรรมองค์กรยั่งยืนต่อไป

ดังนั้น เพื่อให้การบริหารความเสี่ยงของ สรอ. ด้านการเงินเป็นไปด้วยความเรียบร้อยอย่างมีประสิทธิภาพและประสิทธิผล อาศัยอำนาจตามมาตรา ๒๖ และ ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ.๒๕๕๔ ประกอบกับมติคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ ในคราวประชุมครั้งที่ ๙/๒๕๕๕ เมื่อวันที่ ๑๙ กันยายน ๒๕๕๕ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) จึงกำหนดให้ยึดถือนโยบายบริหารความเสี่ยงด้านการเงิน ตามคู่มือการบริหารความเสี่ยงด้านการเงินอย่างเคร่งครัดโดยทั่วกัน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๒ ตุลาคม พ.ศ. ๒๕๕๕

(นายศักดิ์ เสกขุนทด)

ผู้อำนวยการ

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

คู่มือบริหารความเสี่ยงด้านการเงิน
(Financial Risk Management Manual)

สารบัญ

หน้าที่

๑. บทนำ

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) มีภารกิจดำเนินงานภายใต้ พรฎ.จัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งต้องดำเนินงานและบริหารความเสี่ยงภายใต้ความเปลี่ยนแปลงและปรับตัวต่อผลกระทบจากสิ่งแวดล้อมภายนอก ทั้งที่มาจากปัจจัยภายในประเทศและภายนอกประเทศ ทำให้ สรอ. ต้องตระหนักและระมัดระวังในการบริหารจัดการความเสี่ยง โดยเฉพาะความเสี่ยงด้านการเงินที่มีความผันผวนและมีความอ่อนไหวต่อการเปลี่ยนแปลงจากสภาพแวดล้อมทั้งภายในและภายนอก

สรอ. เป็นหน่วยงานของรัฐที่ได้รับการจัดสรรงบประมาณเพื่อใช้ดำเนินการตามภารกิจ อีกทั้งยังสามารถจัดหารายได้เองบางส่วนจากการให้บริการด้านระบบเทคโนโลยีสารสนเทศต่างๆ ที่สอดคล้องตามวัตถุประสงค์ใน พ.ร.ฎ. จัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

ดังนั้นคู่มือบริหารความเสี่ยงด้านการเงินของ สรอ. นี้ จึงมุ่งเน้นถึงการสร้างความตระหนักให้เกิดแก่ทุกคนที่เกี่ยวข้องในสำนักงาน ในการที่จะช่วยสอดส่องดูแล ระมัดระวัง เพื่อลดความเสี่ยง หรือ บรรเทาผลกระทบจากความเสี่ยงด้านการเงิน อันเกิดจากความเสี่ยงด้านงบประมาณที่ส่งผลให้เกิดความไม่สอดคล้องกับแผนที่กำหนด เช่น การไม่ได้รับการจัดสรรงบประมาณตามแผนงานประจำปี และการบริหารการใช้จ่ายงบประมาณที่ไม่มีประสิทธิภาพ อีกทั้งความเสี่ยงด้านการเงินยังครอบคลุมถึงการดำเนินการที่ไม่เป็นไปตามแผนรายได้ประจำปี เช่น รายได้ที่ไม่เป็นไปตามแผน การบริหารลูกหนี้การค้าที่ไม่มีประสิทธิภาพ การจัดเก็บค่าบริการที่ไม่เป็นตามแผนการจัดหารายได้ ความเสี่ยงที่เกิดขึ้นดังกล่าวข้างต้นเป็นความเสี่ยงด้านการเงินที่ส่งผลต่อกระแสเงินสดรับเข้าเพื่อใช้จ่ายในการดำเนินการตามภารกิจ และอาจจะส่งผลต่อเนื่องทำให้เกิดความเสี่ยงทางด้านสภาพคล่องในการดำเนินการของ สรอ. ทำให้ สรอ.ไม่สามารถชำระหนี้สิน และภาระผูกพันต่างๆได้ ท้ายที่สุดอาจจะส่งผลต่อภาพลักษณ์ขององค์กรและทำให้องค์กรไม่สามารถดำเนินการได้ครบถ้วนสมบูรณ์ตามวัตถุประสงค์และภารกิจที่กำหนดไว้ สรอ. ส่งเสริมให้ทุกคนตระหนักถึงความสำคัญและมีส่วนร่วมในการการบริหารความเสี่ยงด้านการเงิน (Financial Risk Management) โดยคณะกรรมการบริหาร สรอ. จะให้คำแนะนำและติดตามการรายงานการบริหารความเสี่ยง ผ่านคณะอนุกรรมการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อวางแนวทางแก้ไขปัญหาที่เกิดจากปัจจัยเสี่ยงต่างๆ นอกจากนี้ยังกำหนดให้มีการดูแลและทบทวนการบริหารความเสี่ยงด้านการเงินอย่างต่อเนื่อง เพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ สรอ. ยอมรับได้

สรอ. ได้กำหนดกระบวนการบริหารความเสี่ยงด้านการเงินเพื่อให้หน่วยงานต่างๆ ของ สรอ. ใช้เป็นแนวทางในการจัดทำแผนกลยุทธ์และแผนธุรกิจที่สอดคล้องกับกลยุทธ์หลักของ สรอ. โดยการระบุความเสี่ยงที่อาจเกิดขึ้น แล้วทำการประเมินถึงโอกาสที่จะเกิดความเสี่ยงขึ้นรวมทั้งผลกระทบที่จะได้รับ พร้อมทั้งจัดทำแนวทางหรือมาตรการควบคุมที่เหมาะสมเพื่อจัดการกับความเสี่ยงนั้น โดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่ สรอ. กำหนด

คู่มือการบริหารความเสี่ยงด้านการเงินฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายการบริหารความเสี่ยงด้านการเงิน โดยจะกล่าวถึงวัตถุประสงค์ ขอบเขต โครงสร้างและบทบาทหน้าที่ของผู้รับผิดชอบกระบวนการบริหารความเสี่ยงด้านการเงิน และรายละเอียดของกระบวนการบริหารความเสี่ยงด้านการเงินเพื่อเป็นแนวทางในการปฏิบัติงานของ สรอ. และเพื่อให้หน่วยงานต่างๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านการเงินตนเองตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

แนวทางการบริหารความเสี่ยงที่นำมาใช้

สรอ. กำหนดกระบวนการบริหารความเสี่ยงด้านการเงินตามแนวทางการปฏิบัติงานของ สรอ. และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Tread way Commission (COSO)

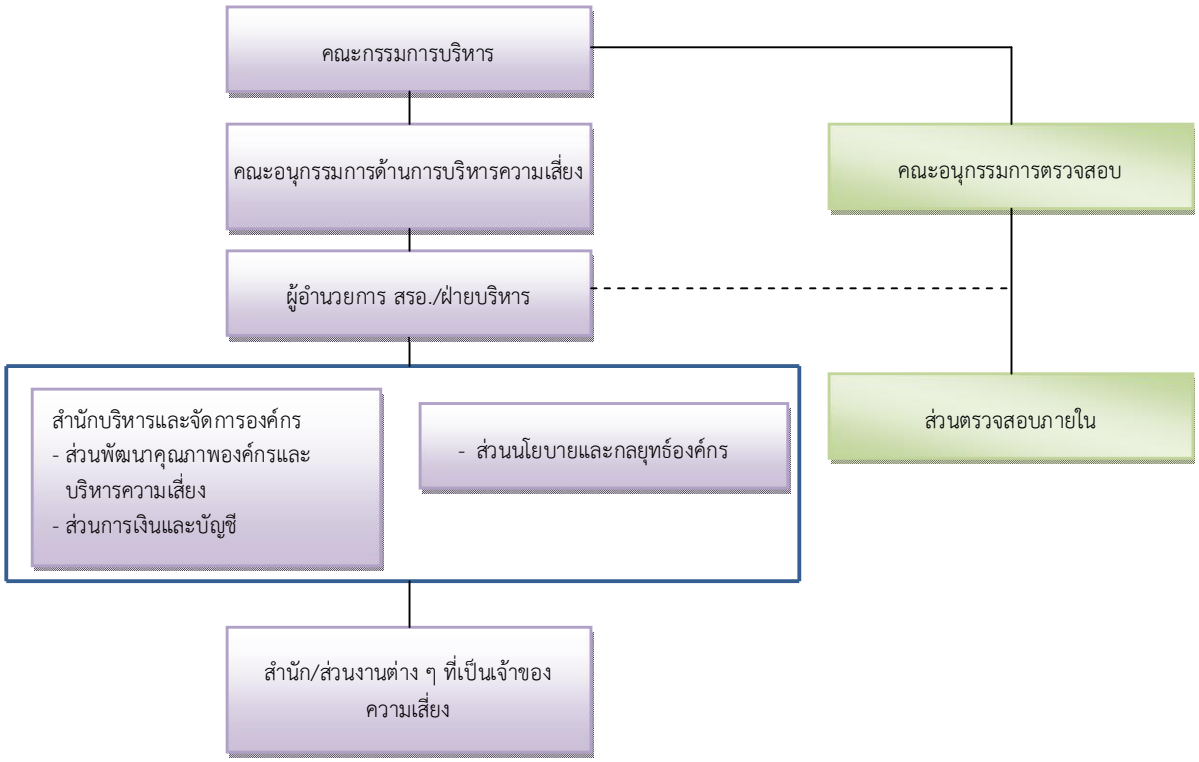
ขอบเขตของคู่มือบริหารความเสี่ยงด้านการเงิน

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านการเงิน ซึ่งครอบคลุมถึงความเสี่ยงอันเกิดจากการปฏิบัติที่ไม่เป็นไปตามแผนงบประมาณประจำปี ตั้งแต่การวางแผนงบประมาณ การของบประมาณ การได้รับอนุมัติงบประมาณจากรัฐบาล การเบิกจ่ายงบประมาณ รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้จ่ายงบประมาณที่ไม่มีประสิทธิภาพการปฏิบัติที่ไม่สอดคล้องกับกฎหมาย หรือกฎระเบียบที่เกี่ยวข้องทั้งภายในและภายนอกที่กำหนดไว้

อีกทั้งยังครอบคลุมถึง ความเสี่ยงที่เกิดจากความผันผวนของอัตราแลกเปลี่ยน ความเสี่ยงที่ทำให้ สรอ. ไม่สามารถชำระหนี้และภาระผูกพันต่างๆ เมื่อถึงกำหนดชำระ การไม่สามารถจัดหาเงินทุนได้เพียงพอเพื่อใช้จ่ายตามภารกิจในการดำเนินการประจำปีหรือเมื่อเกิดภาวะวิกฤติ ฉุกเฉิน ความเสี่ยงที่ทำให้ สรอ. ไม่สามารถรับชำระหนี้จากการให้บริการลูกค้าอันส่งผลต่อสภาพคล่องเนื่องจากกระแสเงินสดรับเข้าไม่เป็นไปตามแผน รวมทั้งความเสี่ยงอันเกิดจากการบริหารจัดการเงินทุนที่ไม่มีประสิทธิภาพ ส่งผลให้ สรอ. เสียผลประโยชน์ต่างๆที่ควรจะได้รับ ทั้งที่เป็นไปหรือไม่เป็นไปตามแผน

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านการเงิน



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบดังนี้

๑. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการเงิน และนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านการเงินให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. จัดทำและทบทวนเพดาน หรือตัวบ่งชี้ (Trigger) ความเสี่ยงด้านการเงิน ที่เกี่ยวกับเพดานของสภาพคล่องและหลักเกณฑ์การขออนุมัติกรณีมีการเกินเพดานหรือตัวบ่งชี้ของสภาพคล่องที่กำหนดไว้ เพื่อนำเสนอขออนุมัติต่อคณะกรรมการบริหาร สรอ.

๓. รายงานความเสี่ยงด้านการเงิน ที่แสดงถึงการปฏิบัติหรือไม่ปฏิบัติตามแนวทาง สตง. หรือ ก.พ.ร. ที่กำหนดไว้ หรือความเสี่ยงที่เกิดจากการดำเนินทางการเงิน ไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการ และของ สรอ. และแสดงถึงความเสี่ยงด้านการเงินเปรียบเทียบกับเพดาน หรือตัวบ่งชี้ที่ได้รับอนุมัติต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

๔. จัดทำตัวแบบ Risk Model และ Stress Testing และรายงานสรุปผลเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

๕. ประเมิน ติดตาม และควบคุมความเสี่ยงด้านการเงิน ที่เกี่ยวกับสภาพคล่อง เพื่อให้มีการปฏิบัติตามนโยบายที่กำหนด

๖. จัดทำคู่มือบริหารความเสี่ยงด้านการเงิน และเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๗. ประสานงานกับส่วนการเงินและบัญชี และส่วนนโยบายและกลยุทธ์องค์กร เพื่อจัดให้หน่วยงานต่างๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการเงินที่กำหนด

๘. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่างๆ ให้เข้าใจถึงแนวทางความสำคัญ และความรับผิดชอบในการบริหารความเสี่ยงด้านการเงิน

๙. ร่วมกับส่วนการเงินและบัญชี และส่วนนโยบายและกลยุทธ์องค์กร เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนการเงินและงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

(๑) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านการเงินในระดับ สรอ. พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Risk Likelihood) และผลกระทบ (Risk Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสม

(๒) ติดตามผลการบริหารความเสี่ยงด้านการเงินโดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้นๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหาร ควบคุม และจัดการความเสี่ยงด้านการเงินในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

(๔) จัดทำแผนฉุกเฉินด้านการเงิน รวมถึงทบทวนแผนปีละ ๑ ครั้ง หรือตามความเหมาะสม

ส่วนการเงินและบัญชี สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดทำแผนการเงิน ให้สอดคล้องกับแผนกลยุทธ์ แผนธุรกิจในภาพรวมของ สรอ. รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์ รวมถึงทบทวนแผนปีละ ๑ ครั้ง หรือตามความเหมาะสม

๒. รับผิดชอบในการบริหารสภาพคล่อง การบริหารโครงสร้างเงินทุน การบริหารอัตราแลกเปลี่ยนต่างๆที่เกี่ยวข้อง และรายงานสถานะการเงินด้านต่างๆของ สรอ. ต่อคณะกรรมการบริหาร

๓. รับผิดชอบในการดูแลและจัดทำแผนการลงทุนด้านการเงิน ปฏิบัติตามนโยบายการบริหารเงินลงทุนเพื่อให้เกิดผลตอบแทนและประโยชน์สูงสุดแก่องค์กร และรายงานการลงทุนด้านการเงินต่อคณะอนุกรรมการบริหารการลงทุน เพื่อรายงานคณะกรรมการบริหารต่อไป

๔. จัดทำรายงานและจัดหาข้อมูลที่เพียงพอให้แก่ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง เพื่อประโยชน์ในการประเมินและควบคุมความเสี่ยงด้านการเงินของ สรอ.

๕. ร่วมกับส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง เสนอแนะวิธีการลดหรือปิดความเสี่ยงด้านการเงินให้อยู่ในระดับที่เหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ และสอดคล้องกับการปฏิบัติงานด้านการเงินและการงบประมาณที่มีอยู่ หรือที่จะได้รับต่อไป

๖. รวบรวมข้อมูล วิเคราะห์พฤติกรรมที่เกิดขึ้นจริงในอดีต (Behavioral Maturity) เพื่อจัดทำรายงานพร้อมวิเคราะห์สถานะสภาพคล่องของ สรอ. จัดทำข้อเสนอแนะ และนำเสนอต่อคณะกรรมการบริหาร สรอ.

๗. ร่วมกับส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง จัดทำแผนฉุกเฉินด้านการเงิน รวมถึงทบทวนแผนปีละ ๑ ครั้ง หรือตามเหมาะสม

ส่วนนโยบายและกลยุทธ์องค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับการงบประมาณที่กำหนดไว้ในกระบวนการบริหารความเสี่ยงด้านการเงิน

๒. ร่วมกับส่วนการเงินและบัญชีและส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเชื่อมโยงการบริหารความเสี่ยงด้านการเงินที่เกี่ยวข้องกับการงบประมาณเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนการเงินและแผนงบประมาณรวมของ สรอ.

๓. ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านการเงินที่เกี่ยวกับการงบประมาณในระดับ สรอ. พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Risk Likelihood) และผลกระทบ (Risk Impact) ที่ได้ระบุไว้เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสม

๔. ติดตามผลการบริหารความเสี่ยงด้านการเงินที่เกี่ยวข้องกับการงบประมาณโดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้นๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

๕. บริหาร ควบคุม และจัดการความเสี่ยงด้านการเงินที่เกี่ยวกับการงบประมาณในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

สอบทานการควบคุมภายในด้านต่างๆ ของ สรอ. ก่อนนำเสนอคณะอนุกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

สำนัก และส่วนงานต่างๆ ของ สรอ. มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกลยุทธ์และแผนปฏิบัติการของสำนัก และส่วนงานต่างๆ ให้สอดคล้องกับแผนการเงินและการงบประมาณของ สรอ.

๒. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับสำนัก และส่วนงานต่าง ๆ

๓. พิจารณาและประเมิน Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนการเงินและแผนงบประมาณของสำนัก และส่วนงานต่างๆ ให้กับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง เพื่อนำไปจัดทำความเสี่ยงด้านการเงินและภาพความเสี่ยงแบบบูรณาการตามลำดับต่อไป

๔. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของสำนักให้กับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเป็นรายเดือนหรือรายไตรมาสตามความเหมาะสม

๕. บริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงาน ในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๖. ดูแล ติดตามการจัดการความเสี่ยง และประเมินผลการจัดการความเสี่ยงเป็นประจำ เพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับ รวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติม เพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๗. แต่งตั้งผู้ประสานงานด้านความเสี่ยง (Risk Officer) เพื่อประสานงานกับส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงในการจัดทำ Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของส่วนงานและสำนัก

๘. สื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๔.๑ ความเสี่ยงด้านการเงิน (Financial Risk)

ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงทางการเงินในภาพรวม ทั้งในด้านการบริหารจัดการด้านการเงิน การวางแผนทางการเงิน ซึ่งต้องเป็นไปในทิศทางเดียวกับกลยุทธ์ของสำนักงาน และกฎหมาย กฎระเบียบต่าง ๆ ที่เกี่ยวข้อง

หากพิจารณาความเสี่ยงด้านการเงินที่เกี่ยวข้องกับสำนักงานแล้ว อาจแยกเป็นประเภทหลักๆ ของความเสี่ยงด้านการเงิน ได้ดังนี้

- การไม่ตระหนักหรือความจำกัดของงบประมาณของประเทศ ทำให้ได้รับจัดสรรงบประมาณไม่สอดคล้องกับความจำเป็น และแผนงานที่จะทำให้สามารถบรรลุเป้าหมาย
- รายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย เนื่องมาจากจำนวนหน่วยงานภาครัฐที่มาขอใช้บริการไม่เป็นไปตามเป้าหมาย หรือขาดการวางแผนที่เหมาะสมในการคาดการณ์และวางแผนทางการเงิน
- การไม่สามารถควบคุมการเบิกใช้งบประมาณให้เป็นไปตามแผนที่กำหนดไว้
- การขาดสภาพคล่อง เนื่องมาจากการวางแผนทางการเงินที่ไม่รัดกุม โดยไม่สามารถบริหารเงินทุนหมุนเวียนให้มีสภาพคล่องเพื่อให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่อง

โดยรายงานทางการเงินที่มีส่วนสนับสนุนในการวิเคราะห์ความเสี่ยงทางด้านการเงิน ได้แก่

งบดุล (Balance Sheet) หมายถึง งบแสดงฐานะของสำนักงาน ณ วันสิ้นรอบระยะเวลาบัญชี (วันสิ้นงวดบัญชี) โดยจัดทำขึ้นทุกๆ รอบระยะเวลาที่กำหนดไว้ เช่น ๑ เดือน ๓ เดือน ๖ เดือน หรือ๑ ปี โดยในส่วนของงบดุลนั้นจะแสดงความสัมพันธ์ของทรัพย์สิน หนี้สินและส่วนของทุน

งบรายได้ค่าใช้จ่าย/งบกำไรขาดทุน (Profit and Loss Statement) หมายถึง งบที่แสดงผลการดำเนินงานของกิจการในช่วงเวลาใดเวลาหนึ่ง เช่น รอบปีบัญชี โดยจะแสดงรายได้ ค่าใช้จ่าย และ กำไรหรือขาดทุนสุทธิ ช่วยให้ผู้ใช้ทราบว่าผลกำไรหรือขาดทุนของกิจการนั้นมาส่วนใด เพื่อปรับปรุงการดำเนินงาน และคาดการณ์ผลการดำเนินงานในอนาคต

งบกระแสเงินสด(Cash Flow Statement) หมายถึง งบที่แสดงการเปลี่ยนแปลงเงินสดของกิจการในช่วงเวลาใดเวลาหนึ่ง เช่น รอบปีบัญชี โดยจะแสดงการได้มาและใช้ไปของเงินสดและรายการเทียบเท่าเงินสด

ของ ๓ กิจกรรมหลักคือ กิจกรรมดำเนินงาน กิจกรรมลงทุน และ กิจกรรมจัดหาเงิน ช่วยให้ผู้ใช้สามารถประเมินสภาพคล่องของกิจการ โดยเฉพาะความสามารถในการชำระหนี้

อัตราส่วนทางการเงิน(Financial Ratio) หมายถึง การนำตัวเลขที่อยู่ในงบการเงินมาหาอัตราส่วน เพื่อใช้ในการวิเคราะห์เปรียบเทียบ โดยผลลัพธ์ที่ได้อาจแสดงอยู่ในรูปร้อยละ สัดส่วน ระยะเวลา จำนวนรอบ หรือจำนวนครั้ง ซึ่งจะช่วยให้ผู้วิเคราะห์ประเมินผลการดำเนินงาน แนวโน้ม และความเสี่ยงของกิจการได้ดียิ่งขึ้น

๔.๒ ที่มาของความเสี่ยงด้านการเงิน สามารถจำแนกเป็นปัจจัยเสี่ยงได้ ๒ ประเภท ดังนี้

๔.๒.๑ ปัจจัยความเสี่ยงภายนอก ได้แก่

(๑) ความเสี่ยงจากการที่ ความไม่ตระหนักถึงความสำคัญของภารกิจของ สรอ. หรือการที่งบประมาณของประเทศมีจำกัด ทำให้ สรอ. ได้รับจัดสรรงบประมาณไม่สอดคล้องกับความจำเป็น และแผนงานที่กำหนดไว้

(๒) ความเสี่ยงจากการเปลี่ยนแปลงกฎระเบียบ กฎหมาย หรือกฎเกณฑ์ด้านการเงินต่างๆของรัฐบาล ที่มีผลกระทบต่อการปฏิบัติงานด้านการเงินและงบประมาณของ สรอ.

(๓) ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของสิ่งแวดล้อมภายนอกต่างๆ ทั้งภายในประเทศและภายนอกประเทศ ที่ทำให้เกิดความผันผวนของค่าเงิน อัตราแลกเปลี่ยน อัตราดอกเบี้ย ฯลฯ ที่มีผลกระทบต่อการบริหารด้านการเงินของ สรอ.

๔.๒.๒ ปัจจัยความเสี่ยงภายใน ได้แก่

(๑) การเปลี่ยนแปลง และความไม่ชัดเจนของนโยบายและกลยุทธ์ระดับองค์กร ซึ่งส่งผลต่อกลยุทธ์ในระดับปฏิบัติการและมีผลกระทบทั้งทางตรงและทางอ้อมต่อแผนการปฏิบัติงานด้านการเงิน และงบประมาณ

(๒) การเปลี่ยนแปลงโครงสร้างองค์กร อาจทำให้มีผลกระทบต่อค่าใช้จ่ายทางการเงินและการใช้จ่ายเงินงบประมาณของ สรอ.

(๓) การปฏิบัติและไม่ปฏิบัติตามนโยบายด้านการเงิน การงบประมาณและการลงทุนต่างๆที่กำหนดไว้ และการที่ข้อมูลไม่เป็นปัจจุบัน (Up to date) ส่งผลให้การบริหารจัดการด้านการเงินของ สรอ. ไม่มีประสิทธิภาพ เช่น การกำหนดโครงสร้างของเงินทุนที่ไม่สอดคล้องตามหลักการบริหารการเงินที่ทำให้ต้นทุนทางการเงินต่ำ หรือการสร้างผลตอบแทนทางการเงินเพื่อให้เกิดประโยชน์สูงสุด โดยไม่ส่งผลต่อสภาพคล่องทางการเงินของ สรอ.

ตัวอย่างปัจจัยเสี่ยงทางด้านการเงิน

ตัวอย่างปัจจัยเสี่ยงทางด้านการเงิน	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การไม่ตระหนักหรือความจำกัดของงบประมาณของประเทศ ทำให้ได้รับจัดสรรงบประมาณไม่สอดคล้องกับความจำเป็น และแผนงานที่จะทำให้สามารถบรรลุเป้าหมาย	การคาดการณ์แผนผิดพลาดส่งผลต่อการขอใช้งบประมาณในแต่ละปี	✓	
	การเปลี่ยนแปลงกฎระเบียบ กฎหมาย หรือกฎเกณฑ์ด้านการเงินต่างๆของรัฐบาล		✓
รายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย	จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการไม่เป็นไปตามเป้าหมาย	✓ อาจเป็นปัจจัยภายในหากการวางแผนการตลาดไม่ดีพอ	✓ อาจเป็นปัจจัยภายนอกหากงบประมาณของหน่วยงานภาครัฐที่ใช้บริการถูกจำกัด
	ขาดการวางแผนที่เหมาะสมการคาดการณ์และวางแผนทางการเงิน	✓	
การไม่สามารถควบคุมการเบิกใช้งบประมาณให้เป็นไปตามแผนที่กำหนดไว้	การกำหนด รายละเอียดคุณลักษณะเฉพาะของครุภัณฑ์ ไม่ตรงกับความต้องการ และการเสนอขายในท้องตลาด ปัจจุบัน	✓	
	แผนงานไม่ได้ตามเป้าหมายทำให้เบิกจ่ายงบลงทุนไม่ได้	✓	
การขาดสภาพคล่อง	ถึงความเพียงพอของการดำรงเงินสดขั้นต่ำเพื่อใช้ในการหมุนเวียนในสำนักงานทั้งในภาวะปกติและภาวะเกิดเหตุการณ์ไม่ปกติ	✓	

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงทางการเงินนั้น จากการที่สำนักงานเป็นหน่วยงานกลางของประเทศในการผลักดันและขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ โดยมีพันธกิจคือ การพัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์ โดยมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงทางการเงิน จึงมุ่งเน้นไปที่การบริหารงบประมาณให้มีประสิทธิภาพ รวมถึงการวางแผนทางการเงินให้เหมาะสมกับการกำหนดกลยุทธ์ในแต่ละปี

อย่างไรก็ตาม มีบางส่วนงานของสำนักงานที่มีหน้าที่สร้างรายได้นอกเหนือจากรายได้ตามงบประมาณ ดังนั้นความเสี่ยงทางการเงินในอีกมุมมองหนึ่งคือ รายได้นอกงบประมาณดังกล่าวไม่เป็นไปตามเป้าหมายที่กำหนด

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านการเงินอันมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามแผนบริหารงบประมาณและเงินรายได้นอกงบประมาณ การบริหารสภาพคล่อง การบริหารเงินลงทุน การกำหนดและบริหารโครงสร้างของเงินทุน การป้องกันความเสี่ยงด้านอัตราแลกเปลี่ยน และการปฏิบัติตามกฎหมาย กฎระเบียบทางด้านการเงิน การงบประมาณต่างๆของทางการ

๕.๓ การระบุเหตุการณ์ (Event Identification)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร สามารถระบุเหตุการณ์ความเสี่ยงได้เป็น ๓ ประเภทหลัก ดังนี้

๑. ความเสี่ยงด้านประสิทธิภาพในการบริหารงบประมาณ

๒. ความเสี่ยงด้านการเงินและการวางแผนทางการเงิน

๓. ความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย

<u>ความเสี่ยงด้านประสิทธิภาพในการบริหารงบประมาณ</u>

การระบุความเสี่ยง แนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อการปฏิบัติที่ไม่เป็นไปตามแผนดำเนินงานด้านการเงินและงบประมาณประจำปี สามารถพิจารณาได้จากความถี่ในการเปลี่ยนแปลง การปรับปรุงแผนงบประมาณ

ที่ได้รับอนุมัติจากคณะกรรมการบริหารแล้วในระหว่างปี สัดส่วนประสิทธิภาพการเบิกจ่าย การผูกพันงบประมาณต่อแผนงบประมาณรวมทั้งปี และปัจจัยต่างๆ ที่มีผลต่อการไม่ได้รับการจัดสรรงบประมาณจากภาครัฐตามแผนที่วางไว้

ความเสี่ยงด้านการเงินและการวางแผนทางการเงิน

การระบุความเสี่ยงด้านการบริหารสภาพคล่อง ให้ระบุประเมินจากความสามารถในการจ่ายชำระหนี้ และภาระผูกพันต่างๆ ความสามารถในการบริหารงบประมาณ และการบริหารลูกหนี้การค้า และโอกาสเสี่ยงที่จะเกิดหนี้สูญจากการเรียกเก็บเงินจากลูกหนี้การค้าไม่ได้ วิเคราะห์ถึงความเพียงพอของการดำรงเงินสดขั้นต่ำเพื่อใช้ในการหมุนเวียนในสำนักงานทั้งในภาวะปกติและภาวะเกิดเหตุการณ์ไม่ปกติ รวมถึงปัจจัยความเสี่ยงที่อาจส่งผลกระทบต่อกระแสเงินสดในช่วงระยะเวลาต่างๆ เพื่อให้ สรอ. มีการบริหารความเสี่ยงด้านการเงินที่เหมาะสม มีสภาพคล่องเพียงพอสามารถจ่ายหนี้สินและภาระผูกพันเมื่อถึงกำหนดชำระได้

การระบุความเสี่ยงที่เกิดจากการบริหารโครงสร้างของเงินทุนและการบริหารเงินลงทุน ควรวิเคราะห์และระบุปัจจัยเสี่ยงที่ส่งผลกระทบต่อแหล่งที่มาและใช้ไปของเงินทุน การระบุและประเมินสัดส่วนโครงสร้างเงินทุนที่เหมาะสม การจัดทำประมาณการงบการเงิน และงบกระแสเงินสด เพื่อวิเคราะห์ประเมินสถานะการเงิน สถานะเงินสดส่วนเกินจากการใช้หมุนเวียนในสำนักงานตามรอบระยะเวลาบัญชีนั้นๆ และการวิเคราะห์เพื่อระบุปัจจัยต่างๆ ที่ส่งผลให้การบริหารการลงทุนไม่เป็นไปตามนโยบายและแผนการบริหารการลงทุนทางทั้งในระยะสั้นและระยะยาว

ความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย

การระบุความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย ให้ระบุประเมินจากเป้าหมายของสำนักงานในการสร้างรายได้นอกงบประมาณ รวมถึงแผนการตลาดที่จะรองรับในการกำหนดกลยุทธ์ในการหาหน่วยงานภาครัฐที่เป็นกลุ่มเป้าหมาย รวมถึงวิเคราะห์ถึงความต้องการของลูกค้าที่เหมาะสม พร้อมกับกำหนดทรัพยากรของสำนักงานที่ต้องการในการสนับสนุนถึงการบรรลุเป้าหมายดังกล่าว

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนการเงินและบัญชี และส่วนนโยบายและกลยุทธ์องค์กร จะร่วมกันพิจารณา วิเคราะห์ และกำหนดปัจจัยต่างๆ ที่มีผลกระทบต่อความเสี่ยงด้านการเงินในแต่ละช่วงเวลา ทำให้ประเมินได้ว่าในอนาคต สรอ. จะมีสภาพคล่องส่วนเกินหรือขาดในช่วงใด ซึ่งสะท้อนถึงความเสี่ยงด้านการเงินของ สรอ.

อย่างไรก็ตามส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนการเงินและบัญชี และส่วนนโยบายและกลยุทธ์องค์กร ยังมีการร่วมพิจารณาถึงความเสี่ยงที่เกิดจากการใช้งบประมาณที่ไม่เป็นไปตามแนวทางของ สตง. กรมบัญชีกลาง หรือ ก.พ.ร. ที่กำหนดไว้ หรือความเสี่ยงที่เกิดจากการดำเนินงานทางการเงิน และงบประมาณไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการ และของ สรอ.

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยงด้านการเงิน สามารถวัดได้จากประมาณการกระแสเงินสดรับและจ่าย เพื่อดูฐานะสภาพคล่องในแต่ละช่วงเวลาต่างๆ หรือการวิเคราะห์อัตราส่วนทางการเงิน เช่น อัตราส่วนเงินทุนหมุนเวียนหรืออัตราส่วนสภาพคล่อง (Current Ratio) อัตราส่วนเงินทุนหมุนเร็ว (Quick Ratio) อัตราส่วนเงินสด (Cash Ratio) เป็นต้น เพื่อทราบถึงแนวโน้มสภาพคล่องทางการเงินหรือความเป็นไปได้ที่ สรอ. จะขาดสภาพคล่องในอนาคต

ความเสี่ยงด้านการบริหารโครงสร้างเงินทุน สามารถวัดประเมินได้ด้วยการวิเคราะห์สัดส่วนระหว่างหนี้สินและทุน (Debt/Equity Ratio) เพื่อให้ทราบถึงนโยบายการจัดหาแหล่งที่มาของเงินทุนมาเพื่อใช้ในสำนักงาน ซึ่งต้องดูให้สอดคล้องกับนโยบายด้านการเงินเพื่อให้เกิดประสิทธิภาพในการบริหารงานสูงสุด

ความเสี่ยงด้านการบริหารเงินทุน สามารถวัดประเมินจากการพิจารณาอัตราส่วนผลตอบแทนจากการลงทุน ด้วยเครื่องมือทางการเงินต่างๆ เพื่อวิเคราะห์ความสามารถในการทำกำไรของการลงทุนด้านการเงินแต่ละประเภท ทั้งนี้จะต้องสอดคล้องตามแผนและนโยบายการบริหารการลงทุนด้านการเงิน เช่น การใช้อัตราผลตอบแทนจากการลงทุน (Return on Investment, ROI), อัตราผลตอบแทนต่อสินทรัพย์รวม (Return on Asset, ROA) และ Risk adjusted return on Control Capital

ทั้งนี้ความเสี่ยงด้านการเงินอื่นๆ ที่ไม่สามารถประเมินด้วยเครื่องมือทางการเงิน สามารถประเมินได้จากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือ โอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านการเงินเหล่านั้นขึ้น เป็นแต่ละเหตุการณ์ เช่น ความเสี่ยงที่เกิดจากการวิเคราะห์ข้อมูลหรือการนำข้อมูลด้านประมาณการงบการเงินไปใช้ไม่ถูกต้อง เกิดจากสาเหตุความผิดพลาดในการประมาณการตัวเลขจากเรื่องอะไร ให้วิเคราะห์และกำหนดเป็นตัวประเมินความเสี่ยงทีละเหตุการณ์ไป เป็นต้น และควรมีการจัดทำ Sensitivity and Simulation Analysis ด้วย

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ความเสี่ยงด้านประสิทธิภาพในการบริหารงบประมาณ
ชื่อปัจจัยเสี่ยง การเบิกจ่ายงบประมาณไม่ได้ตามเป้าหมาย

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	การเบิกจ่ายต่ำกว่าเป้าหมายมากกว่า ๑๐% ในรอบระยะเวลา ๑-๖ เดือน	การเบิกจ่ายต่ำกว่าเป้าหมายมากกว่า ๕% ในรอบระยะเวลา ๖ เดือน	การเบิกจ่ายต่ำกว่าเป้าหมายมากกว่า ๑๐% ในรอบระยะเวลา ๑-๓ เดือน	การเบิกจ่ายต่ำกว่าเป้าหมายมากกว่า ๑๐% ในรอบระยะเวลา ๓-๕ เดือน	การเบิกจ่ายต่ำกว่าเป้าหมายมากกว่า ๑๐% ในรอบระยะเวลา ๖ เดือน

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
ผลกระทบ	การเบิกจ่ายงบประมาณได้ร้อยละ ๑๐๐	การเบิกจ่ายงบประมาณได้ร้อยละ ๙๕	การเบิกจ่ายงบประมาณได้ร้อยละ ๙๐	การเบิกจ่ายงบประมาณได้ร้อยละ ๘๕	การเบิกจ่ายงบประมาณได้ร้อยละ ๘๐

ความเสี่ยงด้านการเงินและการวางแผนทางการเงิน

ชื่อปัจจัยเสี่ยง อัตราส่วนทุนหมุนเวียนต่ำกว่าระดับที่ยอมรับได้

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	ไม่มีเหตุการณ์ที่สินทรัพย์หมุนเวียนน้อยกว่าหนี้สินหมุนเวียน	ในช่วง ๑-๓ เดือน มีเหตุการณ์ที่สินทรัพย์หมุนเวียนน้อยกว่าหนี้สินหมุนเวียน	ในช่วง ๓-๕ เดือน มีเหตุการณ์ที่สินทรัพย์หมุนเวียนน้อยกว่าหนี้สินหมุนเวียน	ในช่วง ๓-๕ เดือน มีเหตุการณ์ที่สินทรัพย์หมุนเวียนน้อยกว่าหนี้สินหมุนเวียนอย่างมีนัยสำคัญ	ในช่วง ๖ เดือน มีเหตุการณ์ที่สินทรัพย์หมุนเวียนน้อยกว่าหนี้สินหมุนเวียน
ผลกระทบ	อัตราส่วนทุนหมุนเวียนมากกว่า ๑.๒๕ เท่า	อัตราส่วนทุนหมุนเวียนมากกว่า ๑ เท่า แต่ไม่เกิน ๑.๒๕ เท่า	อัตราส่วนทุนหมุนเวียนเท่ากับ ๑ เท่า	อัตราส่วนทุนหมุนเวียนเท่ากับ ๐.๗-๐.๙๙ เท่า	อัตราส่วนทุนหมุนเวียนต่ำกว่า ๐.๗ เท่า

ความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย

ชื่อปัจจัยเสี่ยง รายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	จำนวนลูกค้าที่เป็นหน่วยงานภาครัฐสูงกว่าเป้าหมายร้อยละ ๒๐	จำนวนลูกค้าที่เป็นหน่วยงานภาครัฐสูงกว่าเป้าหมายร้อยละ ๑๐	จำนวนลูกค้าที่เป็นหน่วยงานภาครัฐเป็นไปตามเป้าหมาย	จำนวนลูกค้าที่เป็นหน่วยงานภาครัฐต่ำกว่าเป้าหมายร้อยละ ๑๐	จำนวนลูกค้าที่เป็นหน่วยงานภาครัฐต่ำกว่าเป้าหมายร้อยละ ๒๐
ผลกระทบ	รายได้นอกงบประมาณเท่ากับ ๒๐๐ ล้านบาท	รายได้นอกงบประมาณเท่ากับ ๑๕๐ ล้านบาท	รายได้นอกงบประมาณเท่ากับ ๑๐๐ ล้านบาท	รายได้นอกงบประมาณเท่ากับ ๘๐ ล้านบาท	รายได้นอกงบประมาณเท่ากับ ๕๐ ล้านบาท

<u>การประเมินตัวบ่งชี้ (Trigger) ความเสี่ยงด้านการเงิน</u>

ตัวบ่งชี้ความเสี่ยงด้านการเงินของ สรอ. ได้มีการกำหนดและประเมินไว้ให้สอดคล้องตามนโยบายด้านการเงิน การลงทุน และการงบประมาณต่างๆ โดยความเห็นชอบจากคณะกรรมการบริหาร สรอ. เช่น

การกำหนดตัวบ่งชี้ความเสี่ยงด้านการเงิน โดยการดำรงเงินสดหมุนเวียนขั้นต่ำไว้เพื่อใช้จ่ายสำหรับค่าใช้จ่ายดำเนินงานประจำเดือนอย่างน้อย ๑ เดือน เป็นต้น

เมื่อประเมินระดับความเสี่ยงได้แล้ว ขั้นต่อไปคือ การจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญและจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของ สรอ. หรือหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดย สรอ. ได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น ๔ ระดับ ตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้นๆ ได้แก่ ระดับสูงมาก ระดับสูง ระดับปานกลาง ระดับต่ำ ตามลำดับ โดยใช้ตารางแสดงระดับวัดความเสี่ยงเป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมิน ซึ่งตารางจะแสดงข้อมูลเป็น ๒ แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact) ตามตารางแสดงระดับวัดความเสี่ยง

การประเมินความเสี่ยง

ผลกระทบ					
๒๕	๒๕	๕๐	๗๕	๑๐๐	๑๒๕
๔	๔	๘	๑๒	๑๖	๒๐
๓	๓	๖	๙	๑๒	๑๕
๒	๒	๔	๖	๘	๑๐
๑	๑	๒	๓	๔	๕
	๑	๒	๓	๔	๕

โอกาสที่จะเกิด

สีแดง	ความเสี่ยงสูงมาก (๒๕-๑๒๕)
สีส้ม	ความเสี่ยงสูง (๙-๒๔)
สีเหลือง	ความเสี่ยงปานกลาง (๔-๘)
สีเขียว	ความเสี่ยงต่ำ (๑-๓)

ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

ระดับความเสี่ยงด้านการเงิน

	สีเขียวเข้ม	:	ความเสี่ยงด้านการเงินอยู่ในระดับต่ำ
	สีเหลือง	:	ความเสี่ยงด้านการเงินอยู่ในระดับปานกลาง
	สีส้ม	:	ความเสี่ยงด้านการเงินอยู่ในระดับสูง
	สีแดง	:	ความเสี่ยงด้านการเงินอยู่ในระดับสูงมาก

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบ ที่เกิดจากความเสี่ยงนั้นๆ จะทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้นๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าว เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
ความเสี่ยงด้านประสิทธิภาพในการบริหารงบประมาณ	๑. เป้าหมายและแผนปฏิบัติการในการเบิกจ่ายงบประมาณต้องมีการทบทวนและปรับปรุงอย่างสม่ำเสมอ ๒. ระบบการติดตามต้องมีความถี่ที่เพียงพอ และรายงานผลต่อผู้บริหารระดับสูงกรณีที่เกิดปัญหาและอุปสรรค ๓. สื่อสารทำความเข้าใจกับหน่วยงานที่เกี่ยวข้องเพื่อร่วมกับกำหนดมาตรการเพิ่มเติมในกรณีที่ผลการดำเนินงานไม่บรรลุเป้าหมาย	การลดความเสี่ยง (Treat)
ความเสี่ยงด้านการเงินและการวางแผนทางการเงิน	๑. กำหนดให้ฝ่ายงานที่เกี่ยวข้องรายงานความเพียงพอของการดำรงเงินสดขั้นต่ำเพื่อใช้ในการหมุนเวียนในสำนักงานทั้งในภาวะปกติและภาวะเกิดเหตุการณ์ไม่ปกติ	การลดความเสี่ยง (Treat)

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
	๒. จัดทำแผนสำรองกรณีเกิดเหตุการณ์ไม่ปกติ โดยการหาแหล่งที่มาของเงินทุนที่เหมาะสม	
ความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย	๑. ทบทวนแผนการตลาดเชิงรุก และกำหนดหน่วยงานรับผิดชอบโดยตรง ๒. หาพันธมิตรที่เชี่ยวชาญเรื่องการตลาดและกำหนดเป้าหมายร่วมกัน	การลดความเสี่ยง (Treat) / การโอนย้ายความเสี่ยง (Transfer)

๕.๖ กิจกรรมการควบคุม (Control Activities)

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนบัญชีและการเงิน และส่วนนโยบายและกลยุทธ์องค์กร มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านการเงินโดยจะควบคุมความเสี่ยงทางด้านการเงิน ด้านการบริหารเงินลงทุน และอื่นๆ ให้สอดคล้องกับเพดานความเสี่ยง (Risk Limit) หรือตัวบ่งชี้ความเสี่ยงด้านการเงินที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านการเงินของสำนักงานให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการบริหาร สรอ. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

๕.๗ สารสนเทศและการสื่อสาร (Information and Communication)

<u>แหล่งที่มาของข้อมูล</u>

ส่วนพัฒนาองค์กรและบริหารความเสี่ยง จัดเก็บข้อมูลซึ่งมีรายละเอียดดังนี้

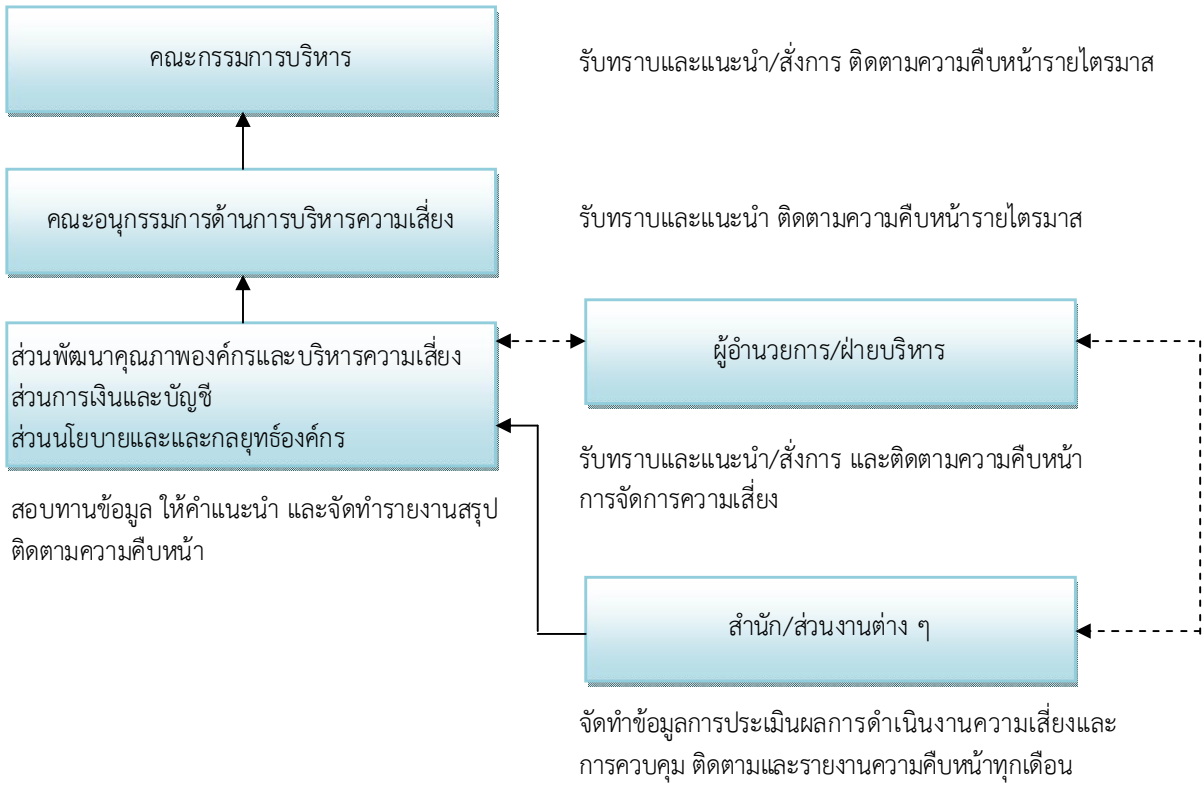
ข้อมูล	แหล่งที่มา	หมายเหตุ
สถานะสภาพคล่องสุทธิ ● ประมาณการกระแสเงินสด ● Current Ratio ● อัตราส่วนทางการเงิน	● ส่วนการเงินและบัญชี	● พิจารณาจากการจัดทำงบประมาณกระแสเงินสดด้วยวิธีทางอ้อม ● อัตราส่วนต่างๆ พิจารณาจากงบแสดงสถานะการเงิน (งบดุล) และงบรายได้ค่าใช้จ่าย (งบกำไรขาดทุน)

ข้อมูล	แหล่งที่มา	หมายเหตุ
สถานะการเบิกจ่ายงบประมาณ	• ส่วนการเงินและบัญชี	• พิจารณาจากการรายงานการเบิกจ่ายงบประมาณรายเดือน • พิจารณาจากการรายงานความคืบหน้าการติดตามโครงการที่ต้องมีการเบิกจ่ายเงินงบประมาณ
ผลการดำเนินงานของรายได้นอกงบประมาณ	• ส่วนที่ปรึกษาการให้บริการ	• ความคืบหน้าการให้บริการหน่วยงานภาครัฐ • การรายงานผลการดำเนินงานของรายได้นอกงบประมาณเทียบกับเป้าหมายแต่ละเดือน พร้อมรายงานถึงปัญหาอุปสรรคและแนวทางแก้ไข

๕.๘ การติดตามและประเมินผล (Monitoring)

ส่วนการเงินและบัญชี ส่วนนโยบายและและกลยุทธ์องค์กร มีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการ สรอ. และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านการเงินที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านการเงินในภาพรวมต่อคณะอนุกรรมการบริหารความเสี่ยง เพื่อคณะกรรมการบริหาร สรอ. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่อง ต่อไป

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติ ส่วนการเงินและบัญชีต้องแจ้งข้อมูลให้ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง พร้อมทั้งรายงานให้ผู้บริหาร สรอ. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สรอ. / ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการบริหาร
ต่ำ	รับทราบ/แนะนำ	รับทราบ	รับทราบ
ปานกลาง หรือเตือน (Warning)	รับทราบ/แนะนำ และสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำ และสั่งการ
สูง หรือรุนแรง (Severe)	รับทราบ/แนะนำ และสั่งการ/รายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ
สูงมาก หรือรุนแรงมาก (High Severe)	รับทราบ/แนะนำ/สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ

ความเสี่ยงด้านกฎหมาย กฎระเบียบ
(Compliance Risk)

ประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
ที่ ๙ /๒๕๕๕
นโยบายบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

เพื่อให้การดำเนินการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ (Compliance Risk Management) ของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) มีความสอดคล้องตามนโยบายบริหารความเสี่ยงของ สรอ. (Enterprise Risk Management Policy)

โดย สรอ. ตระหนักถึงความสำคัญในการบริหารจัดการความเสี่ยงในการดำเนินงาน จึงได้จัดทำนโยบายบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ (Compliance Risk Management Policy) ให้เป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยง (Enterprise Risk Management Policy) โดยกำหนดให้ สรอ. มีการประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามประเมินผล และการรายงานความเสี่ยงด้านกฎหมาย กฎระเบียบ และจัดให้มีระบบการควบคุมภายในเพื่อใช้ในการควบคุมดูแลการดำเนินงานภายในของ สรอ. เพื่อให้คณะกรรมการ ผู้อำนวยการ ผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กร มีส่วนร่วม สร้างความคุ้นเคยและผลักดันให้การบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบของ สรอ. อยู่ในทุกกระบวนการทำงาน และให้ยึดถือเป็นกลไกหนึ่งในการส่งเสริมให้การดำเนินการของ สรอ. มีประสิทธิภาพ อันจะเป็นส่วนหนึ่งของวัฒนธรรมองค์กรอย่างยั่งยืน และสามารถสร้างมูลค่าเพิ่มให้กับองค์กรและประเทศชาติ

ดังนั้น เพื่อให้การบริหารความเสี่ยงของ สรอ. ด้านกฎหมาย กฎระเบียบเป็นไปด้วยความเรียบร้อยอย่างมีประสิทธิภาพและประสิทธิผล อาศัยอำนาจตามมาตรา ๒๖ และ ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ.๒๕๕๔ ประกอบกับมติคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ ในคราวประชุมครั้งที่ ๘/๒๕๕๕ เมื่อวันที่ ๑๕ สิงหาคม ๒๕๕๕ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) จึงกำหนดให้ยึดถือนโยบายการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ตามคู่มือการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบอย่างเคร่งครัดโดยทั่วกัน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๑ กันยายน พ.ศ. ๒๕๕๕

(นายศักดิ์ เสกขุนทด)
ผู้อำนวยการ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

คู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ
(Compliance Risk Management Manual)

สารบัญ

หน้าที่

๑. บทนำ

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ได้ตระหนักถึงการดำเนินธุรกรรมต่างๆ เพื่อให้อยู่ภายใต้กฎหมาย มติคณะรัฐมนตรี ข้อบังคับ ระเบียบ ประกาศ และคำสั่ง ตลอดจนระเบียบของหน่วยงานที่กำกับดูแล เช่น คณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) สำนักงานการตรวจเงินแผ่นดิน (สตง.) เป็นอย่างมาก สรอ. จึงให้ความสำคัญต่อการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ (Compliance Risk) โดยมีคณะกรรมการบริหาร สรอ. แนะนำและติดตามการรายงานผ่านคณะอนุกรรมการบริหารความเสี่ยงอย่างสม่ำเสมอ

กระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ เป็นกระบวนการที่สำคัญมาก โดยเฉพาะความเสี่ยงด้านกฎหมาย ซึ่งถ้า สรอ. มีการดำเนินธุรกรรมที่ขัดต่อกฎหมายนั้น อาจเป็นสาเหตุให้ สรอ. ถูกระงับการดำเนินงานตามภารกิจลงได้ ดังนั้นกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ จึงเป็นกระบวนการที่ช่วยให้การดำเนินการของ สรอ. มีการควบคุมการดำเนินการหรือจัดการความเสี่ยงโดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่ สรอ. กำหนด

คู่มือการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ โดยจะกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ เพื่อใช้เป็นแนวทางในการปฏิบัติงานของ สรอ.

แนวทางการบริหารความเสี่ยงที่นำมาใช้

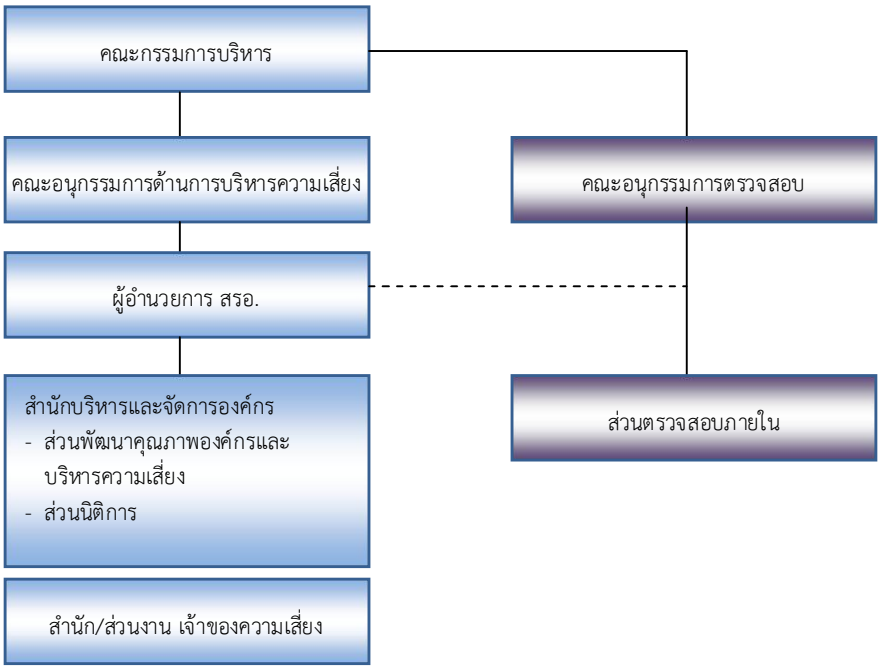
สรอ. กำหนดกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบตามแนวทางการปฏิบัติงานของ สรอ. และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Tread way Commission (COSO)

ขอบเขตของคู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบเท่านั้น โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ เพื่อให้หน่วยงานต่างๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบของตนเอง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านกฎหมาย และกฎระเบียบ



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบดังนี้

๑. กำหนดกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ และนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. ประสานงานกับหน่วยงานต่าง ๆ เพื่อให้หน่วยงานต่างๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบที่กำหนดในกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

๓. จัดทำคู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ และเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๔. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่างๆ ให้เข้าใจถึงแนวทาง ความสำคัญ และความรับผิดชอบในการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

๕. รวบรวมข้อมูลความเสี่ยงด้านกฎหมาย กฎระเบียบ และรายงานคณะอนุกรรมการด้านการบริหารเสี่ยง

ส่วนนิติการ สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบดังนี้

๑. พิจารณากฎระเบียบภายในต่าง ๆ ให้สอดคล้องและอยู่ภายใต้กฎหมายที่เกี่ยวข้อง

๒. ให้คำปรึกษาหน่วยงานต่าง ๆ ของ สรอ. ในการดำเนินการเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบ

ส่วนตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

ตรวจสอบและสอบทานการควบคุมภายในด้านต่างๆ ของ สรอ. ก่อนนำเสนอคณะอนุกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

สำนัก และส่วนงานต่าง ๆ ของ สรอ. มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดแผนปฏิบัติการของสำนัก และส่วนงานต่างๆ โดยดำเนินการตามกรอบนโยบาย และกระบวนการบริหารความเสี่ยงที่กำหนดในกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

๒. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับสำนัก และส่วนงานต่าง ๆ

๓. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนปฏิบัติงานสำนัก และส่วนงานต่างๆ ให้กับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง เพื่อนำไปจัดทำแผนภาพบริหารความเสี่ยง (Risk Map) ต่อไป

๔. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของสำนักให้กับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเป็นรายไตรมาส

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

ความเสี่ยงด้านกฎหมาย กฎระเบียบ (Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการหรือการปฏิบัติงานที่เป็นไปตามและไม่เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง ทำให้มีผลกระทบต่อธรรมาภิบาลและหรือต่อ สรอ. และเจ้าหน้าที่ ทั้งนี้ ความเสี่ยงด้านกฎหมาย กฎระเบียบ ยังรวมถึงความเสี่ยงจากการตีความกฎหมาย การไม่ทราบ การไม่เข้าใจกฎระเบียบ ที่ไม่สอดคล้องตรงกันของหน่วยงานต่าง ๆ

(๑) แผนปฏิบัติงาน (Action Plan) หมายถึง กรอบการดำเนินงานประจำปี ที่หน่วยงานต่าง ๆ จัดทำขึ้นเพื่อใช้ในการปฏิบัติงานประจำปี โดยแผนปฏิบัติงานจะต้องสนับสนุนแผนธุรกิจ (Business Plan) ของ สรอ.

(๒) โอกาสที่จะเกิดความเสี่ยง (Risk Likelihood) หมายถึง ความเป็นไปได้ที่จะเกิดความเสี่ยงด้านกฎหมาย กฎระเบียบ

(๓) ผลกระทบของเหตุการณ์จากความเสี่ยง (Risk Impact) หมายถึง ผลกระทบหรือความเสียหายที่เกิดขึ้นกับ สรอ. อันเนื่องมาจากการเกิดขึ้นของความเสี่ยงด้านกฎหมาย กฎระเบียบ

(๔) ดัชนีชี้วัดความเสี่ยง (Key Risk Indicators) หมายถึง เครื่องมือที่จะช่วยให้ผู้บริหาร สรอ. ทราบถึงระดับความเสี่ยงที่มีอยู่ในช่วงเวลาใดเวลาหนึ่ง โดยอาศัยการชี้วัดจากปัจจัยเสี่ยงต่างๆ ที่กำหนดขึ้น

(๕) ความเสี่ยงตั้งต้น (Inherent Risk) เป็นความเสี่ยงด้านกฎหมาย กฎระเบียบที่มีอยู่ทันทีที่มีการกระทำกิจกรรมหรือการดำเนินงาน เช่น การดำเนินการด้านเทคโนโลยีสารสนเทศ ต้องสอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๖) ระดับความเสี่ยงที่ทนได้หรือความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ความเสี่ยงที่เกินจากความเสี่ยงที่ยอมรับได้ แต่อยู่ในช่วงกำหนดที่ทน ซึ่งจะต้องมีการจัดการทันที

(๗) ปัจจัยเสี่ยง (Risk Factor) หมายถึง เหตุการณ์หรือปัจจัยที่เป็นสาเหตุของความเสี่ยง ควรเป็นสาเหตุที่แท้จริง (Root Cause) เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในอนาคตได้อย่างถูกต้อง

(๘) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ระดับของความเสี่ยงที่ สรอ. จะยอมรับได้ ซึ่งในความเป็นจริงนั้น ความเสี่ยงด้านกฎหมายเกิดได้สองด้าน ได้แก่ การที่ทำตามกฎหมายแต่ไม่บรรลุวัตถุประสงค์ของแผนงานที่กำหนดไว้ กับการไม่ทำตามกฎหมายซึ่งไม่ควรมี สำหรับด้านกฎระเบียบต้องพิจารณาว่าเป็นกฎระเบียบภายใน หรือกฎระเบียบภายนอก และระดับของ

ผลกระทบต่อ สรอ. และเจ้าหน้าที่ผู้ปฏิบัติงาน โดยจักต้องจัดทำแผนจัดการความเสี่ยงที่มีอยู่ในปัจจุบันให้ครอบคลุมความเสี่ยงทั้งหมด รวมถึงความเสี่ยงด้านธรรมาภิบาลด้วย

(๙) ความเสี่ยงคงเหลือ (Residual Risk) เป็นความเสี่ยงที่เหลืออยู่หลังจากที่ได้มีการจัดการ หรือควบคุมความเสี่ยงนั้นแล้ว ความเสี่ยงคงเหลือจะเป็นจุดเริ่มต้นของการกำหนดระดับความเสี่ยงที่ยอมรับได้

สำหรับ สรอ. เพื่อช่วยให้องค์กรสามารถเผชิญกับความเสี่ยงจากการดำเนินกิจกรรมหรือธุรกิจได้อย่างมีประสิทธิภาพยิ่งขึ้น

การดำเนินการของ สรอ. เกี่ยวกับการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ต้องเริ่มตั้งแต่การ จัดทำแผนธุรกิจ แผนกลยุทธ์ของ สรอ. และเมื่อหน่วยงานต่าง ๆ ได้รับทราบแผนธุรกิจ สรอ. แล้วนำมาวิเคราะห์ ทำให้ทราบว่า หน่วยงานของตนสามารถที่จะสนับสนุนแผนธุรกิจได้อย่างไร จึงจัดทำแผนปฏิบัติงาน (Action Plan) ของหน่วยงานตนเอง ซึ่งในการจัดทำแผนปฏิบัติงานของหน่วยงานนั้น ต้องมีการจัดกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ไปพร้อมกัน

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

การวิเคราะห์และประเมินสภาพแวดล้อมการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ต้องคำนึงถึงปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อ สรอ. หรือหน่วยงานนั้นๆ ในการวิเคราะห์ดังกล่าวจะทำให้สามารถระบุได้ว่า แผนงาน/โครงการ นั้นๆ จะสามารถดำเนินงานต่อไปได้หรือไม่ หรือจักต้องปรับปรุงแผนงาน/โครงการ อย่างไร เพื่อไปสู่เป้าหมายที่กำหนดไว้

ตัวอย่างตารางรายงานการตรวจสอบความเสี่ยงด้านกฎหมาย กฎระเบียบ ปี.....

สำนัก/โครงการ.....

วัตถุประสงค์เป้าหมายที่ต้องการ.....

แผนปฏิบัติงาน (Action plan) สำนัก/โครงการ		กฎหมาย กฎระเบียบ ที่เกี่ยวข้อง		ธรรมาภิบาลที่เกี่ยวข้อง
ลำดับ	งาน/โครงการ	ภายนอก	ภายใน	
๑.				
๒.				
๓.				
๔.				
๕.				
๖.				
๗.				
๘.				
๙.				
๑๐.				
๑๑.				

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

ส่วนนิติการเป็นผู้รับผิดชอบหลักในการกำหนดระดับความเสี่ยงด้านกฎหมาย กฎระเบียบ รวมถึงธรรมาภิบาลของ สรอ. องค์กร และส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเป็นผู้รับผิดชอบหลักในการกำหนดวัตถุประสงค์ของการบริหารความเสี่ยงในภาพรวมของ สรอ.

สำนัก ส่วนงาน หรือโครงการต่างๆ เป็นผู้รับผิดชอบในการจัดการความเสี่ยงด้านกฎหมาย กฎระเบียบ เพื่อให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ที่ได้ร่วมกับส่วนนิติการ และส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง กำหนดไว้สำหรับงานหรือโครงการที่รับผิดชอบ พร้อมทั้งมีการรายงานความเสี่ยงตามระยะเวลาตามแต่ระดับความเสี่ยงที่ได้กำหนดไว้

๕.๓ การระบุเหตุการณ์ (Event Identification)

การระบุเหตุการณ์ความเสี่ยง จะเริ่มด้วยการแจกแจงกระบวนการปฏิบัติงาน (Work flow) เพื่อให้ได้ทราบขั้นตอนงานที่มีอยู่และจะทำให้บรรลุวัตถุประสงค์ที่กำหนดไว้ แล้วจึงระบุปัจจัยเสี่ยงด้านกฎหมาย กฎระเบียบที่มีผลกระทบในแต่ละขั้นตอนการปฏิบัติงานนั้นๆ ที่อาจส่งผลต่อวัตถุประสงค์/เป้าหมายของงาน/โครงการ ทั้งทางตรงและทางอ้อมต่อ สรอ.

หน้าที่ ๑

ตัวอย่างการระบุและประเมินความเสี่ยงประจำปี.....

งาน/โครงการ.....

สำนัก/หน่วยงาน.....

กระบวนการปฏิบัติงาน	สาเหตุความเสี่ยง (Risk Factors)	ปัจจัยเสี่ยง (Risk driver)	การประเมินความเสี่ยงก่อนจัดการ (Risk Assessment)				ระดับความเสี่ยงก่อนจัดการ (Inherent Risk)
			ความเสี่ยงภายนอก/ภายใน			ผลกระทบ	
			ภายนอก	ภายใน	โอกาสเกิด		

ผู้รายงาน.....

ตำแหน่ง.....

วันที่ .....

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย กฎระเบียบ

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย กฎระเบียบ	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การฟ้องร้องดำเนินคดีตามกฎหมาย	ความผิดพลาดจากเอกสาร	✓	
	การไม่ปฏิบัติตามคำแนะนำของฝ่ายนิติการ	✓	
การไม่ปฏิบัติตามกฎหมายและกฎระเบียบ	ความไม่เข้าใจในกฎหมายและกฎระเบียบ	✓	
การบริหารจัดการสัญญา	ไม่มีหน่วยงานในการติดตามสัญญาเป็นการเฉพาะ	✓	
	เปลี่ยนบุคลากรที่ทำหน้าที่ติดตามสัญญา	✓	

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

ทั้งนี้ ความเสี่ยงด้านกฎหมาย และกฎระเบียบ สามารถประเมินได้จากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือ โอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านกฎหมายและกฎระเบียบเหล่านั้นขึ้นเป็นแต่ละเหตุการณ์ โดยทั่วไป ความเสี่ยงด้านกฎหมายและกฎระเบียบ จะมีลักษณะการกำหนดผลกระทบที่ท้าทายมาก นั่นคือ มีเพียงระดับ ๕ ซึ่งหมายถึงการมีเหตุการณ์ที่ไม่ปฏิบัติตามกฎหมายกฎระเบียบเกิดขึ้น แม้เพียง ๑ ครั้ง และระดับ ๑ คือ ทุกธุรกรรมขององค์กรเป็นไปตามกฎหมาย และกฎระเบียบที่เกี่ยวข้อง

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ชื่อปัจจัยเสี่ยง การไม่ปฏิบัติตามกฎหมายและกฎระเบียบ

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	จากการอบรมเรื่องกฎหมายกฎระเบียบพนักงานมีความรู้ ความเข้าใจสูงกว่าร้อยละ ๙๘	จากการอบรมเรื่องกฎหมายกฎระเบียบพนักงานมีความรู้ ความเข้าใจ ร้อยละ ๙๖-๙๘	จากการอบรมเรื่องกฎหมายกฎระเบียบพนักงานมีความรู้ ความเข้าใจ ร้อยละ ๙๑-๙๕	จากการอบรมเรื่องกฎหมายกฎระเบียบพนักงานมีความรู้ ความเข้าใจ ร้อยละ ๗๑-๙๐	จากการอบรมเรื่องกฎหมายกฎระเบียบพนักงานมีความรู้ ความเข้าใจไม่ถึงร้อยละ ๗๐

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
ผลกระทบ	ทุกธุรกรรมขององค์กรเป็นไปตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง	-	-	-	การมีเหตุการณ์ที่ไม่ปฏิบัติตามกฎหมาย กฎระเบียบเกิดขึ้นแม้เพียง ๑ ครั้ง

เมื่อประเมินระดับความเสี่ยงได้แล้ว ขั้นต่อไปคือ การจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญและจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของ สรอ. หรือหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดย สรอ. ได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น ๔ ระดับ ตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้นๆ ได้แก่ ระดับสูงมาก ระดับสูง ระดับปานกลาง ระดับต่ำ ตามลำดับ โดยใช้ตารางแสดงระดับวัดความเสี่ยงเป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมิน ซึ่งตารางจะแสดงข้อมูลเป็น ๒ แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact) ตามตารางแสดงระดับวัดความเสี่ยง

การประเมินความเสี่ยง

ผลกระทบ					
๒๕	๒๕	๕๐	๗๕	๑๐๐	๑๒๕
๔	๔	๘	๑๒	๑๖	๒๐
๓	๓	๖	๙	๑๒	๑๕
๒	๒	๔	๖	๘	๑๐
๑	๑	๒	๓	๔	๕
	๑	๒	๓	๔	๕

โอกาสที่จะเกิด

สีแดง	ความเสี่ยงสูงมาก (๒๕-๑๒๕)
สีส้ม	ความเสี่ยงสูง (๙-๒๔)
สีเหลือง	ความเสี่ยงปานกลาง (๔-๘)
สีเขียว	ความเสี่ยงต่ำ (๑-๓)

ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

ระดับความเสี่ยงด้านกฎหมาย กฎระเบียบ

	สีเขียวเข้ม	:	ความเสี่ยงด้านกฎหมาย กฎระเบียบอยู่ในระดับต่ำ
	สีเหลือง	:	ความเสี่ยงด้านกฎหมาย กฎระเบียบอยู่ในระดับปานกลาง
	สีส้ม	:	ความเสี่ยงด้านกฎหมาย กฎระเบียบอยู่ในระดับสูง
	สีแดง	:	ความเสี่ยงด้านกฎหมาย กฎระเบียบอยู่ในระดับสูงมาก

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบ ที่เกิดจากความเสี่ยงนั้นๆ จะทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้นๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าว เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
ความเสี่ยงด้านการไม่ปฏิบัติตามกฎหมายและกฎระเบียบ	๑. ศึกษา ติดตาม และวิเคราะห์กฎหมาย กฎระเบียบที่เปลี่ยนแปลงไป ๒. สื่อสารทำความเข้าใจกับพนักงานถึงกฎหมาย และกฎระเบียบที่เกี่ยวข้องโดยมีความถี่ที่เหมาะสม	การลดความเสี่ยง (Treat)

๕.๖ กิจกรรมการควบคุม (Control Activities)

การควบคุมเป็นเครื่องมือที่ใช้ในการจัดการกับความเสี่ยงที่มีอยู่ ดังนั้นหน่วยงานควรดำเนินการระบุการควบคุมที่มีอยู่ และประเมินประสิทธิผลและความเพียงพอของการควบคุม หากไม่เพียงพอให้หน่วยงานดังกล่าวจัดทำแผนจัดการความเสี่ยงเพิ่มเติม โดยการประเมินการควบคุมสามารถจัดทำตามตาราง

หน้าที่ ๑

ตัวอย่างการบริหารความเสี่ยงและปรับปรุงการควบคุมภายใน ประจำปี .....
งาน/โครงการ.....
สำนัก/หน่วยงาน.....

กระบวนการปฏิบัติงาน งาน/ โครงการ	ระดับความเสี่ยงก่อนจัดการ (Inherent Risk)	การควบคุมที่มีอยู่ (Control)	ผลการประเมินการควบคุม	ความเสี่ยงที่เหลืออยู่/ จุดอ่อน (Residual Risk)	การปรับปรุงการควบคุม	วันที่เสร็จ/ ต้องการให้เสร็จ	สำนัก/ หน่วยงานที่รับผิดชอบ	หมายเหตุ

ผู้รายงาน.....

ตำแหน่ง.....

วันที่ .....

๕.๗ สารสนเทศและการสื่อสาร (Information and Communication)

ระดับความเสี่ยงของความเสี่ยงด้านกฎหมาย กฎระเบียบ

ระดับความรุนแรงและการรายงาน	กฎหมาย กฎระเบียบที่เกี่ยวข้อง	ผู้อำนวยการ สรอ. / ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการบริหาร
ปานกลาง หรือเตือน (Warning)	ข้อบังคับ ระเบียบ ประกาศ และคำสั่งภายใน	รับทราบ/แนะนำ และสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำ และสั่งการ
สูง หรือรุนแรง (Severe)	ระเบียบของหน่วยงานที่กำกับดูแล	รับทราบ/แนะนำ และสั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ
สูงมาก หรือรุนแรงมาก (High Severe)	กฎหมาย มติคณะรัฐมนตรี	รับทราบ/แนะนำ/สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ

๕.๘ การติดตามและประเมินผล (Monitoring)

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ส่วนนิติการ ต้องรายงานความเสี่ยงด้านกฎหมาย กฎระเบียบต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง และคณะกรรมการบริหาร สรอ. เพื่อให้ทราบผลการดำเนินงาน ปัญหาที่เกิดขึ้น และตรวจสอบสาเหตุของปัญหา ตลอดจนหาแนวทางแก้ไขเพื่อป้องกัน ควบคุมและลดความเสี่ยงด้านกฎหมาย กฎระเบียบตามที่กำหนด ซึ่งในรายงานความเสี่ยงต้องแสดงถึงความเสี่ยงด้านกฎหมาย กฎระเบียบที่มีอยู่ และแนวทางแก้ไข ระยะเวลาแล้วเสร็จอย่างชัดเจน

หน้าที่ ๑

รายงานการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ประจำปี.....

สำหรับงวดตั้งแต่ วันที่ ... เดือน.....พ.ศ. ..... ถึง วันที่ ... เดือน.....พ.ศ. .....

งาน/โครงการ.....

สำนัก/หน่วยงาน.....

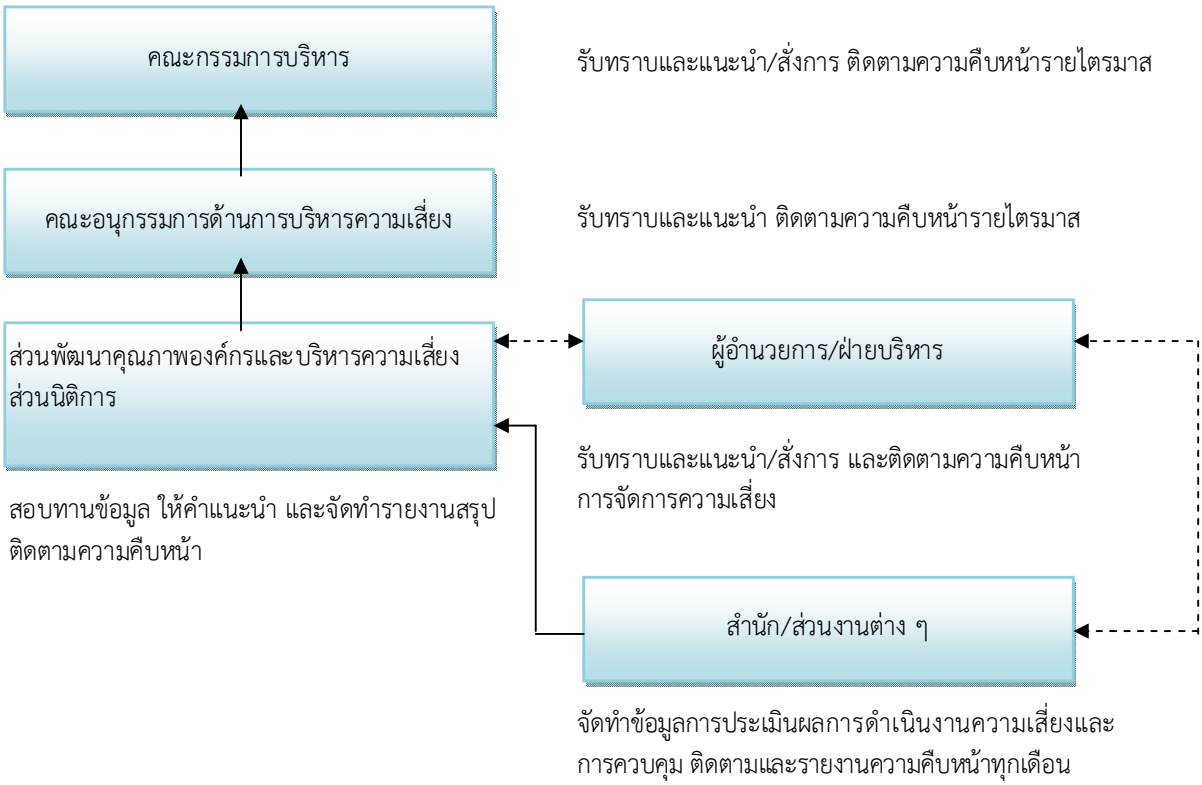
งาน/ โครงการ	ความเสี่ยง ที่มีอยู่	ระดับความ เสี่ยง	โอกาส เกิด	ผลกระทบ	การปรับปรุงการ ควบคุม	กำหนด เสร็จ	หน่วยงาน/ ผู้รับผิดชอบ

ผู้รายงาน.....

ตำแหน่ง.....

วันที่ .....

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

(Information Technology Risk)

EGA
e-Government Agency

ประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

ที่ ๙ /๒๕๕๕

เรื่อง นโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

.....

เพื่อให้การดำเนินการด้านระบบเทคโนโลยีสารสนเทศของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) มีการวางแผน ควบคุม เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับ สรอ. พร้อมทั้งมีการดำเนินการเพื่อสนองตอบต่อเหตุการณ์อันอาจส่งผลให้เกิดความเสี่ยงทุกๆ ด้านได้อย่างเคร่งครัดและทันท่วงที

ทั้งนี้ สรอ. ตระหนักดีว่าความต่อเนื่องของการบริหารงานของ สรอ. เป็นปัจจัยสำคัญต่อหน่วยงานอื่น ๆ เป็นจำนวนมาก จึงได้จัดทำนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management Policy) ให้เป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยง (Enterprise Risk Management Policy) โดยกำหนดให้ สรอ. มีการประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามประเมินผล และการรายงานความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและจัดให้มีระบบการควบคุมภายในเพื่อใช้ในการควบคุมดูแลการดำเนินงานภายในของ สรอ. เพื่อให้คณะกรรมการ ผู้อำนวยการ ผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กร มีส่วนร่วม สร้างความคุ้นเคยและผลักดันให้การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สรอ. อยู่ในทุกกระบวนการทำงาน และให้ยึดถือเป็นกลไกหนึ่งในการส่งเสริมให้การดำเนินการของ สรอ. มีประสิทธิภาพ อันจะเป็นส่วนหนึ่งของวัฒนธรรมองค์กรอย่างยั่งยืน และสามารถสร้างมูลค่าเพิ่มให้กับองค์กรและประเทศชาติ

ดังนั้น เพื่อให้การบริหารความเสี่ยงของ สรอ. ด้านระบบเทคโนโลยีสารสนเทศเป็นไปด้วยความเรียบร้อยอย่างมีประสิทธิภาพและประสิทธิผล อาศัยอำนาจตามมาตรา ๒๖ และ ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ.๒๕๕๔ ประกอบกับมติคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ ในคราวประชุมครั้งที่ ๙/๒๕๕๕ เมื่อวันที่ ๑๙ กันยายน ๒๕๕๕ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) จึงกำหนดให้ยึดถือนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ตามคู่มือการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัดโดยทั่วกัน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๒ ตุลาคม พ.ศ. ๒๕๕๕

(นายศักดิ์ เสกขุนทด)
ผู้อำนวยการ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

คู่มือการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

(Information Technology Risk Management Manual)

สารบัญ

หน้าที่

๑. บทนำ

การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) เป็นองค์ประกอบสำคัญของการดำเนินงานของ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) เป็นอย่างมาก จึงได้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management Policy) เพื่อบังคับใช้กับทุกหน่วยงานของ สรอ. โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจและตระหนักถึงหน้าที่ความรับผิดชอบต่อการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศอยู่เสมอ และยังสนับสนุนให้เจ้าหน้าที่ทุกระดับชั้นเข้าใจ รวมถึงมีส่วนร่วมในการบริหารและจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศในทุกขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

คู่มือการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศซึ่งจะใช้ประกอบกับคู่มือเฉพาะของแต่ละเครื่องมือที่ใช้ในการบริหารความเสี่ยง ซึ่งจะกล่าวลงไปในรายละเอียดเพื่อให้หน่วยงานสามารถวางระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศภายในหน่วยงานของตนเองได้อย่างมีประสิทธิภาพ และเป็นการป้องกัน ควบคุม และลดผลกระทบจากเหตุการณ์ความเสียหายที่อาจเกิดขึ้นต่อ สรอ. โดยกระบวนการดังกล่าวจะอยู่ภายใต้การดูแลของหัวหน้าหน่วยงาน ฝ่ายบริหาร และมีการกำกับ ดูแลและสั่งการโดยคณะกรรมการบริหาร สรอ. ผ่านทางคณะอนุกรรมการด้านการบริหารความเสี่ยง

แนวคิดเกี่ยวกับการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๑. การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศจะอยู่บนพื้นฐานของการควบคุมภายใน ซึ่งเป็นกระบวนการที่เป็นขั้นตอนที่ต่อเนื่องและแทรกอยู่ในการปฏิบัติงานตามปกติของทุกหน่วยงาน

๒. เจ้าหน้าที่ในทุกหน่วยงานของ สรอ. มีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ซึ่งมีผู้บริหารเป็นผู้รับผิดชอบให้มีระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ตามที่ สรอ. กำหนด คือ มีการระบุ ประเมิน ติดตาม ควบคุม และรายงานความเสี่ยง

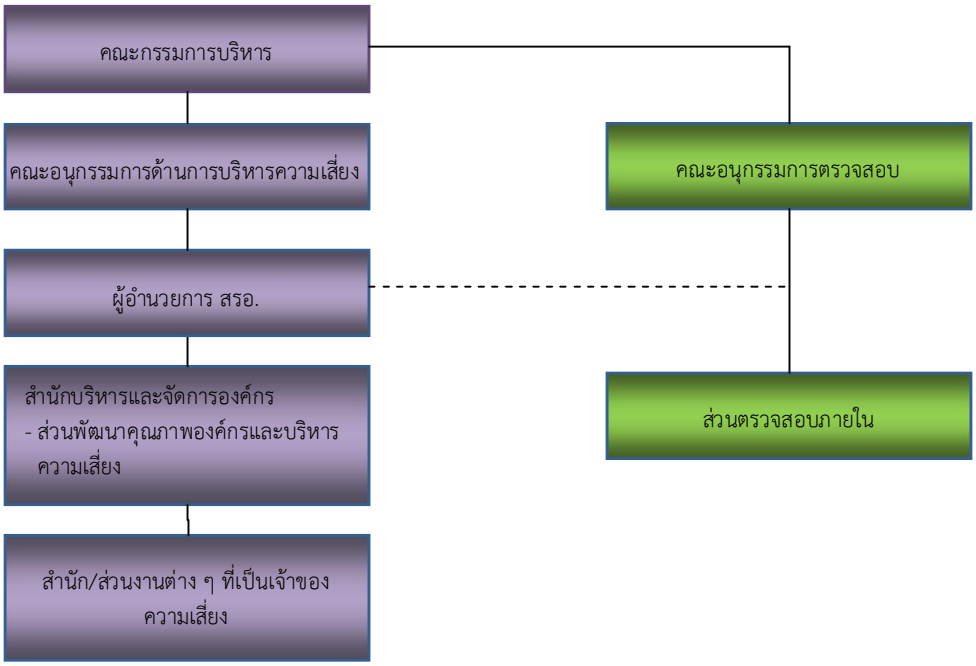
๓. การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศควรให้ความมั่นใจอย่างสมเหตุสมผลว่าหน่วยงานจะบรรลุตามเป้าหมายที่ได้กำหนดไว้ กล่าวคือ แม้ว่าจะมีการวางระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศไว้ดีเพียงใด ก็ไม่สามารถรับรองได้ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้อย่างสมบูรณ์ เพราะมีข้อจำกัดจากปัจจัยอื่นนอกเหนือการควบคุมของหน่วยงาน เช่น ผลกระทบจากปัจจัยภายนอก เป็นต้น

ขอบเขตของคู่มือบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยง สรอ. โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ เพื่อให้หน่วยงานต่างๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของตนเอง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง สำนักบริหารและจัดการองค์กร มีหน้าที่รับผิดชอบดังนี้

๑. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. รายงานความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ที่แสดงถึงการปฏิบัติหรือไม่ปฏิบัติตามนโยบายที่กำหนดไว้

๓. ประเมิน ติดตาม และควบคุมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ที่เกี่ยวกับสภาพคล่อง เพื่อให้มีการปฏิบัติตามนโยบายที่กำหนด

๔. ประสานงานกับหน่วยงานต่าง ๆ ที่เป็นเจ้าของความเสี่ยง เพื่อให้หน่วยงานต่าง ๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่กำหนด

๕. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่างๆ ให้เข้าใจถึงแนวทาง ความสำคัญ และความรับผิดชอบในการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๖. บริหาร ควบคุม และจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

๗. ร่วมกับหน่วยงานต่าง ๆ จัดทำแผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (Business Continuity Plan) รวมถึงทบทวนแผนปีละ ๑ ครั้ง หรือตามความเหมาะสม

สำนัก และส่วนงานต่างๆ ของ สรอ. มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกลยุทธ์และแผนปฏิบัติงานของสำนัก และส่วนงานต่างๆ ให้สอดคล้องกับนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๒. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับสำนัก และส่วนงานต่าง ๆ

๓. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance ให้กับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง เพื่อนำไปจัดทำความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและภาพความเสี่ยงแบบบูรณาการ ตามลำดับต่อไป

๔. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของสำนักให้กับส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงเป็นรายเดือนหรือรายไตรมาศตามความเหมาะสม

๕. จัดทำแผนจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Treatment Plan) ของสำนัก และส่วนงานต่างๆ และบริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงาน ในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๖. ดูแล ติดตามการจัดการความเสี่ยง และประเมินผลการจัดการความเสี่ยงเป็นประจำ เพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับ รวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติม เพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๗. แต่งตั้งผู้ประสานงานด้านความเสี่ยง (Risk Internal Control Officer: RICO) เพื่อประสานงานกับส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงในการจัดทำ Risk Factor, Risk Appetite และ Risk Tolerance จากแผนธุรกิจ แผนกลยุทธ์ หรือแผนปฏิบัติงานของสำนักและส่วนงาน

๘. สื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

ส่วนตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

สอบทานการควบคุมภายในด้านต่างๆ ของ สรอ. ก่อนนำเสนอคณะอนุกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ การสอบทานความเสี่ยงควรพิจารณาแผนจัดการความเสี่ยงของสำนักและส่วนงานต่างๆ ว่ามีความเหมาะสมหรือไม่ และให้ข้อคิดไว้ในการปรับปรุงหรือแก้ไขตามสมควร

การสอบทานควรรวมถึงการติดตามว่ามีการดำเนินตามแผนการจัดการความเสี่ยงหรือไม่ และสถานการณ์ดำเนินการว่าอยู่ในระดับใด

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้มีการนำมาตรฐาน ISO/IEC 27001:2005 ซึ่งเป็นมาตรฐานที่กำลังได้รับความนิยมอย่างแพร่หลายในปัจจุบัน และกล่าวถึงข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS (Information Security Management) ให้กับองค์กร ซึ่งวัตถุประสงค์ของมาตรฐานนี้เพื่อให้องค์กรสามารถบริหารจัดการทางด้านความปลอดภัยได้อย่างมีระบบ และเพียงพอเหมาะสมต่อการดำเนินธุรกิจขององค์กร มาร่วมกำหนดเป็นประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วย โดยสามารถกำหนดกรอบการบริหาร ดังนี้

๔.๑ ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk)

ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk) คือ ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำระบบเทคโนโลยีสารสนเทศมาใช้ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน ทั้งนี้ ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ จะมีองค์ประกอบที่สำคัญ ๓ ประการ ได้แก่ แผนงานการใช้ระบบเทคโนโลยีสารสนเทศ การตัดสินใจในการนำเทคโนโลยีสารสนเทศมาใช้ และการวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน ระบบงาน เหตุการณ์ภายนอก หรือคน (เจ้าหน้าที่ บุคคลภายนอก หรือลูกค้า) ซึ่งส่งผลกระทบต่อการดำเนินงานของ สรอ.

๔.๒ ประเภทของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Type of Risk) สามารถจำแนกออกได้เป็น ๗ ประเภทดังนี้

๔.๒.๑ ความเสี่ยงด้านข้อมูล (Information Risk) หมายถึง ความเสี่ยงที่เกิดจากข้อมูลต่างๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาดโดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้เกิดการฟ้องร้องได้ หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้โดยความเสี่ยงนี้อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ยังรวมไปถึงความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back Up) ที่สำคัญคือ เพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูลสำรอง (Information back-Up) การกู้คืนข้อมูล (Information Recovery) ซึ่งเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่อง (Business Continuity Plan) และแผนกู้คืนข้อมูล (Disaster Recovery Plan)

๔.๒.๒ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ความเสี่ยงในเรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงาน และขององค์กร ที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการและเหมาะสมกับงบประมาณ หรือความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงจากการที่เทคโนโลยีสารสนเทศหมดอายุไปเอง ความเสี่ยงจากการไม่ได้กำหนดหรือกำหนดกระบวนการอนุมัติใช้อุปกรณ์เทคโนโลยีสารสนเทศไม่ชัดเจน

๔.๒.๓ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึงความเสี่ยงที่เกิดจากการเลือกใช้หรือความเสี่ยงจากการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ไม่หวังดีทำลายระบบ (Hacker) การควบคุมการ Reversion software ไม่เพียงพอ การที่ Software ที่ใช้อยู่ Out of date ความเสี่ยงที่เกิดจากการเลือกใช้ Software platforms ความเสี่ยงที่เกิดจากควบคุมการเปลี่ยนแปลง (Change control) ไม่เหมาะสมเพียงพอ ความเสี่ยงที่ไม่ได้กำหนดขั้นตอนการอนุมัติการใช้งาน Software การไม่ได้จัดทำขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Document operating procedures) ความเสี่ยงจากการไม่แยกระบบสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน (Separation of development, test and operation facilities) เป็นต้น

๔.๒.๔ ความเสี่ยงด้านบุคลากร (People Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศ ในเรื่องของการกำหนดโครงสร้าง การมอบหมายงานในหน้าที่ให้แก่บุคลากรด้านระบบเทคโนโลยีสารสนเทศ ที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดระบบเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ และความเสี่ยงจากการว่าจ้างหรือจัดจ้างบุคลากรภายนอก (Information Technology Outsourcing) เพื่อจัดทำโครงการด้านระบบเทคโนโลยีสารสนเทศต่าง ๆ ทั้งนี้ ยังรวมถึงการที่ขาดแผนการฝึกอบรมด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่ของ สรอ. อย่างทั่วถึง ทั้งในส่วนของผู้ดูแลระบบ (Administration) ผู้พัฒนาระบบ (Developer/Programmer) และผู้ใช้งานทั่วไป (User) อย่างสม่ำเสมอ

๔.๒.๕ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย และการก่อการร้าย เป็นต้น

๔.๒.๖ ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบเครือข่ายสื่อสารขัดข้อง ไม่มีระบบเครือข่ายสื่อสารสำรอง ความเสี่ยงที่เกิดจากไม่ได้กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดในการบริหารจัดการสำหรับบริหารเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริหารเครือข่ายโดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก การบำรุงรักษาอุปกรณ์เครือข่ายสื่อสารไม่สม่ำเสมอ การไม่มีรายชื่อและข้อมูลสำหรับติดต่อหน่วยงานอื่นกรณีมีความจำเป็น เช่น บมจ. ทศท คอร์เปอเรชั่น บมจ. กสท. โทรคมนาคม ผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) ความเสี่ยงที่ผู้ดูแลระบบไม่มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่าง ๆ ที่ส่งผ่านทางเครือข่าย เป็นต้น

๔.๒.๗ ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) หมายถึง ความเสี่ยงที่เกิดจากกระบวนการทำงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ซึ่งส่งผลให้ขาดการนำ Best Practice ที่ดีต่างๆ มาใช้งาน COBIT 5 ได้กำหนดกระบวนการที่เป็นมาตรฐานที่ดีต่างๆ ไว้จำนวน ๓๗ กระบวนการ และ กำหนด Best Practice ของกระบวนการต่างๆ ไว้ให้ เช่นกัน

การขาดการนำ Best Practice เหล่านั้นมาใช้งานจะทำให้องค์กรไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่มาตรฐานดังกล่าวได้กำหนดไว้ COBIT 5 ได้กำหนดเป้าหมายทางธุรกิจสำหรับการนำเทคโนโลยีสารสนเทศมาใช้งานไว้จำนวน ๑๗ เป้าหมาย

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

สรอ. ได้จัดให้มีกระบวนการในการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศให้เป็นไปตามหลักมาตรฐานสากลและเป็นมาตรฐานเดียวกันทั่วทั้ง สรอ. เช่นเดียวกับกระบวนการบริหารความเสี่ยงด้านอื่นๆ โดยจะครอบคลุมการปฏิบัติงานในทุกระดับชั้นของแต่ละหน่วยงานใน สรอ. เพื่อช่วยให้การดำเนินงานเกิดผลดีและปฏิบัติงานได้ตามกฎระเบียบที่เกี่ยวข้อง ซึ่งการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ โดยการวิเคราะห์สภาพแวดล้อมภายในองค์กร และภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงในเทคโนโลยีสารสนเทศ จากการที่สำนักงานเป็นหน่วยงานกลางของประเทศในการผลักดันและขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ โดยมีพันธกิจคือ การพัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์

ดังนั้น การวิเคราะห์ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินงานที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศที่ให้บริการกับลูกค้า และระบบเทคโนโลยีสารสนเทศภายในของ สรอ. มีเสถียรภาพ และความมั่นคงของระบบ รวมทั้งมีประโยชน์สำหรับตัดสินใจในการดำเนินธุรกิจอิเล็กทรอนิกส์ของ สรอ. ผู้บริหารและหน่วยงานที่เกี่ยวข้องกับความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศจะต้องร่วมกันกำหนดและทบทวนกลยุทธ์อย่างสม่ำเสมอ เพื่อใช้กำหนดแผนปฏิบัติการ (Action Plan) ในการพัฒนางานเพื่อป้องกันและลดความเสียหายที่อาจจะเกิดขึ้นรวมถึงช่วยให้สามารถบรรลุเป้าหมายและวัตถุประสงค์ของแผนดำเนินงาน

ทั้งนี้การวิเคราะห์สภาพแวดล้อมต้องคำนึงถึงปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อ สรอ. หรือหน่วยงานที่เกี่ยวข้องกับนโยบายหลัก เนื่องจากการวิเคราะห์ถึงสภาพแวดล้อมทั้งภายในและภายนอก (SWOT Analysis) จะทำให้ สรอ. ทราบถึงปัจจัยเสี่ยงที่จะส่งผลกระทบต่อความสำเร็จของ สรอ. ช่วยให้ สรอ. ทราบว่าต้องบริหารจัดการอย่างไร เพื่อสร้างเสถียรภาพ ความมั่นคง และความน่าเชื่อถือของระบบเทคโนโลยีสารสนเทศเมื่อต้องเผชิญกับสภาพการเปลี่ยนแปลงที่รวดเร็ว

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านระบบเทคโนโลยีสารสเนทศ มีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามแผนงานโครงการของระบบสารสนเทศ หรือการปฏิบัติตามกฎหมาย กฎระเบียบต่างๆ ที่จะส่งผลต่อการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงเทคโนโลยี

สารสนเทศและการสื่อสาร คณะกรรมการกิจการการจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ มาตรฐานความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นต้น

๕.๓ การระบุเหตุการณ์ (Event Identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องกับโครงการและกิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อ สรอ. ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

การระบุความเสี่ยงประกอบด้วยคำศัพท์พื้นฐาน ๒ คำ ได้แก่

๑. ภัยคุกคาม (Threat) หมายถึง ภัยที่มีผลในทางลบต่อสินทรัพย์สารสนเทศ และการดำเนินธุรกิจขององค์กรในลักษณะใดลักษณะหนึ่ง เช่น ไวรัสซึ่งเป็นภัยชนิดหนึ่ง เมื่อภัยนี้เกิดขึ้นจริง จะทำให้ธุรกิจขององค์กรเกิดการหยุดชะงักได้

๒. จุดอ่อนหรือช่องโหว่ (Vulnerability) หมายถึง สภาพหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ และหากถูกใช้ให้เป็นประโยชน์โดยภัยคุกคามก็อาจทำให้สินทรัพย์สารสนเทศขององค์กรได้รับความเสียหายได้

โดยในบริบท เมื่อมีการระบุความเสี่ยงหนึ่ง เช่น ความเสี่ยงเรื่องของไวรัส จะมีความเกี่ยวข้องกับภัยคุกคามหนึ่ง ซึ่งในที่นี้ก็คือไวรัส และโดยทั่วไปหากความเสี่ยงนั้นจะเกิดขึ้นได้ จะต้องมีการใช้ประโยชน์จากจุดอ่อนหนึ่ง เช่น ไวรัสจะใช้ประโยชน์จากการที่ผู้ใช้งานไม่ได้ติดตั้งซอฟต์แวร์ป้องกันไวรัสไว้ในเครื่อง เป็นต้น

โดยสรุป ความเสี่ยงหนึ่งที่มีการระบุขึ้นจะต้องบ่งชี้ได้ว่ามีความเกี่ยวข้องกับภัยคุกคามอะไรและภัยคุกคามนั้นจะใช้จุดอ่อนใดมาทำให้เกิดความเสียหายขึ้น

วิธีการในการระบุความเสี่ยงมีหลายวิธี ได้แก่

(๑) การระดมสมองของผู้ปฏิบัติงานที่เกี่ยวข้อง

(๒) การใช้ Checklist เพื่อใช้ตรวจสอบหาจุดอ่อน เช่น Checklist ของมาตรฐาน ISO/IEC 27001 หรือของ COBIT5 เป็นต้น

(๓) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

(๔) การวิเคราะห์กระบวนการทำงานด้านเทคโนโลยีสารสนเทศเมื่อเทียบกับกระบวนการของมาตรฐานสากลเช่น COBIT5, ITIL, CMMI เป็นต้น

ตัวอย่าง การระบุความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ช่องโหว่	ภัยคุกคาม
ความเสี่ยงการขาดการสำรองข้อมูล	ความเสี่ยงด้านข้อมูล	ขาดการสำรองข้อมูลอย่างสม่ำเสมอ	ค่าคอนฟิกกูเรชันของระบบ/อุปกรณ์สำคัญสูญหาย
ความเสี่ยงที่เอกสารแสดงลิขสิทธิ์ของซอฟต์แวร์สูญหาย	ความเสี่ยงด้านข้อมูล	เอกสารแสดงลิขสิทธิ์ของซอฟต์แวร์สูญหาย	การไม่มีเอกสารแสดงสิทธิ์การใช้งานซอฟต์แวร์
ความเสี่ยงที่ผู้ดูแลระบบทำงานผิดพลาด	ความเสี่ยงด้านบุคลากร	ผู้ดูแลระบบทำงานผิดพลาด	ค่าคอนฟิกกูเรชันของระบบ/อุปกรณ์สำคัญสูญหายหรือเสียหาย
ความเสี่ยงไฟฟ้าดับ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	ไฟฟ้าดับ	อุปกรณ์คอมพิวเตอร์/อุปกรณ์เครือข่าย/ระบบสำคุญหยุดชะงัก
ความเสี่ยงการขาดการติดตั้งโปรแกรมป้องกันไวรัส	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	ขาดการติดตั้งโปรแกรมป้องกันไวรัส	การแพร่ระบาดของไวรัส
ความเสี่ยงที่อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุการใช้งาน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	ขาดการเปลี่ยนอุปกรณ์เทคโนโลยีสารสนเทศตามรอบระยะเวลาการใช้งาน	อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุการใช้งาน

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

ในการประเมินความเสี่ยงโดยทั่วไปเกณฑ์การประเมินความเสี่ยงจะประกอบด้วยองค์ประกอบ ๒ ส่วนคือ

- โอกาสการเกิดขึ้นของความเสี่ยง (Likelihood) ซึ่งหมายถึง ความเป็นไปได้ที่ความเสี่ยงที่ผู้ประเมินสนใจจะเกิดขึ้น
- ระดับความรุนแรงของผลกระทบ (Impact) ซึ่งหมายถึง ความเสี่ยงนั้นหากเกิดขึ้นจะมีความรุนแรงในระดับใด

ตัวอย่าง การกำหนดเกณฑ์การประเมินทั้ง ๒ ส่วน

โอกาสการเกิดขึ้นของความเสี่ยง (Likelihood)

ระดับ	โอกาสที่จะเกิด
๑	แทบจะไม่เกิดหรืออย่างมากปีละ ๑ ครั้ง
๒	โอกาสเกิดน้อยหรืออย่างมากไม่เกินปีละ ๒ ครั้ง
๓	ปานกลาง ปีละ ๓-๕ ครั้ง
๔	ค่อนข้างบ่อย ปีละ ๖-๑๐ ครั้ง
๕	เกิดเป็นประจำ อย่างน้อยเดือนละ ๑ ครั้ง

ระดับความรุนแรงของผลกระทบ (Impact)

เกณฑ์	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	๑=น้อยมาก	๒=น้อย	๓=ปานกลาง	๔=สูง	๕=สูงมาก
ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร	กระทบชื่อเสียงขององค์กรน้อยมากหรือไม่กระทบ	กระทบชื่อเสียงขององค์กรน้อยภายในกลุ่มงาน	กระทบชื่อเสียงขององค์กร โดยมีการรายงานต่อผู้บริหารระดับสูง	กระทบชื่อเสียงขององค์กร ทำให้เกิดความไม่พอใจจากสาธารณะ เช่น การเขียนวิจารณ์	กระทบชื่อเสียงขององค์กรมาก ทำให้เกิดความไม่พอใจจากสาธารณะ เช่น การแสดงความเห็นคัดค้านผ่านสื่อต่างๆ
ผลกระทบต่อองค์กรด้านการเงิน	ไม่เกิน ๑๐๐,๐๐๐ บาท หรือ เกิดเหตุร้ายที่ไม่มี	> ๑ แสนบาท – ๒.๕ แสนบาท หรือเกิดเหตุร้ายเล็กน้อยที่แก้ไขได้	> ๒.๕ แสนบาท – ๕ แสนบาท หรือระบบมีปัญหาและมี	> ๕ แสนบาท – ๑๐ ล้านบาท หรือเกิดปัญหากับระบบ IT ที่สำคัญ	> ๑๐ ล้านบาท หรือเกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความ

เกณฑ์	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	๑=น้อยมาก	๒=น้อย	๓=ปานกลาง	๔=สูง	๕=สูงมาก
	ความสำคัญ		ความสูญเสียไม่มาก	และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน	เสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
การดำเนินการทางธุรกิจ	ไม่มีปัญหา	มีปัญหาเล็กน้อย แก้ไขได้ ในระดับกลุ่มงาน	ระบบสนับสนุนสำคัญหยุดชะงัก มีผลต่อการดำเนินการภายในกลุ่มงาน และต้องใช้หน่วยงานภายนอกในการแก้ไข	ระบบสำคัญ ระบบความปลอดภัย / ระบบที่สำคัญหยุดชะงัก บางระบบหรือบางฟังก์ชัน อาจส่งผลต่อประชาชน	Total disruption จนทำงานไม่ได้และก่อผลกระทบต่อการทำงานของระบบสำคัญทั้งหมด ส่งผลต่อประชาชน
ด้านกฎหมายระเบียบข้อบังคับอื่นๆ ที่องค์กรต้องปฏิบัติตาม	ไม่มีผลต่อการปฏิบัติตามกฎหมายระเบียบ และข้อบังคับที่เกี่ยวข้อง	ขัดต่อกระบวนการปฏิบัติงานทีม	ขัดต่อนโยบายและแนวปฏิบัติเฉพาะกลุ่มงาน	ขัดต่อนโยบายและแนวปฏิบัติทั่วไปในระดับองค์กร	ขัดต่อกฎหมายพระราชบัญญัติที่เกี่ยวข้อง เช่น พรบ. เป็นต้น

จากตารางที่เสนอในข้างต้น สรอ. ได้กำหนดค่าระดับความเสี่ยงไว้ ดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ความรุนแรงของเหตุการณ์

ในการพิจารณาความรุนแรงของเหตุการณ์จะต้องพิจารณาจากผลกระทบทั้ง ๔ ด้านร่วมกัน เช่น หากความเสี่ยงเรื่องการแพร่ระบาดของไวรัสเกิดขึ้น จะมีผลกระทบแต่ละด้าน ได้แก่

๑. ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร มีผลกระทบในระดับใด

๒. ผลกระทบต่อองค์กรด้านการเงิน มีผลกระทบในระดับใด

๓. การดำเนินการทางธุรกิจ มีผลกระทบในระดับใด

๔. ด้านกฎหมาย ระเบียบ ข้อบังคับอื่นๆ ที่องค์กรต้องปฏิบัติตาม มีผลกระทบในระดับใด

และใช้ค่าผลกระทบที่มากที่สุดของผลกระทบทั้ง ๔ ด้าน เป็นค่าระดับความรุนแรงของเหตุการณ์

ตัวอย่างเช่น ความเสี่ยงเรื่องการแพร่ระบาดของไวรัส เมื่อพิจารณาจากโอกาสการเกิดขึ้นของความเสี่ยงในตารางจะมีค่าเท่ากับ **๓** และระดับความรุนแรงของผลกระทบแต่ละด้านคือ

๑. ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร มีผลกระทบในระดับ **๓**

๒. ผลกระทบต่อองค์กรด้านการเงิน มีผลกระทบในระดับ **๕**

๓. การดำเนินการทางธุรกิจ มีผลกระทบในระดับ **๕**

๔. ด้านกฎหมาย ระเบียบ ข้อบังคับอื่นๆ ที่องค์กรต้องปฏิบัติตาม มีผลกระทบในระดับ **๓**

ดังนั้นระดับความรุนแรงของผลกระทบจึงมีค่าเท่ากับ **๕** ระดับความเสี่ยงของการแพร่กระจายของไวรัสจึงเท่ากับ **๑๕** ตาราง ๒ มิติ แสดงระดับความเสี่ยงสำหรับทุกค่าที่เป็นไปได้คือ

ระดับความเสี่ยงของการแพร่กระจายของไวรัส

ระดับความรุนแรงของผลกระทบ (Impact)						
	สูงมาก	๒๕	๕๐	๗๕	๑๐๐	๑๒๕
	สูง	๔	๘	๑๒	๑๖	๒๐
	ปานกลาง	๓	๖	๙	๑๒	๑๕
	ต่ำ	๒	๔	๖	๘	๑๐
	น้อยมาก	๑	๒	๓	๔	๕
		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
	โอกาสการเกิดขึ้นของความเสี่ยง (Likelihood)					

ค่าระดับความเสี่ยงในตารางข้างต้นจึงมีค่าอยู่ระหว่าง ๑-๒๕

จากการพิจารณาค่าระดับความเสี่ยงในตารางข้างต้น สรอ. ได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น ๔ โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
๑-๓	ต่ำ	ระดับความเสี่ยงที่องค์กรยอมรับ (Acceptable) ซึ่งอาจมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
๔-๘	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ แต่ต้องมีมาตรการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงมีค่าสูงขึ้นไปยังระดับที่ไม่สามารถยอมรับได้
๙-๒๔	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับหรือยอมรับได้ต่อไป
๒๕ ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจำเป็นต้องเร่งจัดการความเสี่ยงจนกระทั่งให้อยู่ในระดับที่สามารถยอมรับได้ทันที

โดยแสดงเป็นตาราง ๒ มิติ แสดงการแบ่งระดับความเสี่ยงทั้ง ๔ โซน ดังนี้

ระดับความเสี่ยงของการแพร่กระจายของไวรัส

ระดับความรุนแรงของผลกระทบ (Impact)						
	สูงมาก	๒๕	๕๐	๗๕	๑๐๐	๑๒๕
	สูง	๔	๘	๑๒	๑๖	๒๐
	ปานกลาง	๓	๖	๙	๑๒	๑๕
	ต่ำ	๒	๔	๖	๘	๑๐
	น้อยมาก	๑	๒	๓	๔	๕
		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
	โอกาสการเกิดขึ้นของความเสี่ยง (Likelihood)					

ตัวอย่าง การประเมินระดับความเสี่ยง แสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ช่องโหว่	ภัยคุกคาม	โอกาสในการเกิดเหตุการณ์	ความรุนแรงของเหตุการณ์	ระดับความเสี่ยง
ความเสี่ยงการขาดการสำรองข้อมูล	ความเสี่ยงด้านข้อมูล	ขาดการสำรองข้อมูลอย่างสม่ำเสมอ	ค่าคอนฟิกกูเรชันของระบบ/อุปกรณ์สำคัญสูญหาย	๒	๒๕	๕๐
ความเสี่ยงที่เอกสารแสดงลิขสิทธิ์ของซอฟต์แวร์สูญหาย	ความเสี่ยงด้านข้อมูล	เอกสารแสดงลิขสิทธิ์ของซอฟต์แวร์สูญหาย	การไม่มีเอกสารแสดงสิทธิ์การใช้งานซอฟต์แวร์	๒	๔	๘
ความเสี่ยงที่ผู้ดูแลระบบทำงานผิดพลาด	ความเสี่ยงด้านบุคลากร	ผู้ดูแลระบบทำงานผิดพลาด	ค่าคอนฟิกกูเรชันของระบบ/อุปกรณ์สำคัญสูญหายหรือเสียหาย	๒	๒๕	๕๐
ความเสี่ยงไฟฟ้าดับ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	ไฟฟ้าดับ	อุปกรณ์คอมพิวเตอร์/อุปกรณ์เครือข่าย/ระบบสำคุญหยุดชะงัก	๒	๒๕	๕๐
ความเสี่ยงการขาดการติดตั้งโปรแกรมป้องกันไวรัส	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	ขาดการติดตั้งโปรแกรมป้องกันไวรัส	การแพร่ระบาดของไวรัส	๑	๕	๒๕
ความเสี่ยงที่อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุการใช้งาน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	ขาดการเปลี่ยนอุปกรณ์เทคโนโลยีสารสนเทศตามรอบระยะเวลาการใช้งาน	อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุการใช้งาน	๒	๔	๘

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

ในการควบคุมและบรรเทาความเสี่ยง จะขึ้นอยู่กับค่าระดับความเสี่ยงที่ประเมินและได้ค่ามานั้น ทางเลือกในการควบคุมหรือบรรเทาความเสี่ยงจะมีด้วยกัน ๔ ทางเลือก ดังนี้

๕.๕.๑ การยอมรับความเสี่ยง (Acceptance) กรณีที่ค่าระดับความเสี่ยงอยู่ในบริเวณสีเขียว ผู้ประเมินความเสี่ยงสามารถยอมรับความเสี่ยงได้ กรณีการยอมรับความเสี่ยงยังหมายรวมถึง

- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเหลือง สีส้ม หรือ สีแดง ก็ตาม แต่หน่วยงานหรือสำนักยังไม่สามารถระบุมาตรการที่เหมาะสมได้ จึงอาจต้องยอมรับความเสี่ยงไว้ก่อน ในภายหลังเมื่อได้มาตรการที่เหมาะสมแล้ว จึงเสนอมาตรการเพื่อหาทางลดความเสี่ยงให้ลดลงมาอยู่ในระดับสีเขียว เป็นต้น
- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเหลือง สีส้ม หรือ สีแดง แต่หน่วยงานหรือสำนักพบว่าการจะจัดการกับความเสี่ยงนี้จะมีค่าใช้จ่ายที่ค่อนข้างสูงและไม่คุ้มค่าที่จะลงทุน จึงเห็นสมควรให้ยอมรับความเสี่ยงและไม่ดำเนินการใดๆ

ในทั้งสองกรณีนี้หน่วยงานหรือสำนักจำเป็นจะต้องรายงานให้คณะกรรมการบริหารได้รับทราบด้วย

๕.๕.๒ การเลี่ยงความเสี่ยง (Avoidance) คือ การหาหนทางที่เหมาะสมเพื่อหลีกเลี่ยงความเสี่ยงที่พบนั้น เช่น หากพบว่าการนำทรัพย์สินไปตั้งไว้ในบริเวณที่มีความเสี่ยงต่อการสูญหาย ก็ควรจะหลีกเลี่ยงโดยการนำไปจัดเก็บไว้ในสถานที่ที่ปลอดภัย

การตัดสินใจที่จะแลกเปลี่ยนข้อมูลสำคัญกับองค์กรหนึ่งผ่านทางระบบออนไลน์ เมื่อพบว่าองค์กรนั้นยังไม่มีมาตรการความมั่นคงปลอดภัยที่ดีเพียงพอ ก็อาจยับยั้งการตัดสินใจนั้น โดยหลีกเลี่ยงความเสี่ยงไปใช้วิธีการแลกเปลี่ยนแบบ Manual แทน

การหาหนทางที่เหมาะสมกว่า ควรพิจารณาว่าความเสี่ยงลดลงมาอยู่ในระดับที่ยอมรับได้หรือไม่ เช่น ตกอยู่ในบริเวณสีเขียวหรือไม่

๕.๕.๓ การโอนย้ายความเสี่ยง (Transfer) คือ การให้หน่วยงานอื่นเป็นผู้รับความเสี่ยงหรือดำเนินการแทน สรอ. เช่น การใช้ Outsource เรื่องการพัฒนาระบบ ให้หน่วยงานภายนอกโดยการทำสัญญาดูแลรักษาฮาร์ดแวร์ อุปกรณ์เครือข่าย การซื้อประกันภัยจากหน่วยงานภายนอก

การโอนย้ายความเสี่ยง ควรพิจารณาว่า ผู้ดำเนินการสามารถจัดการความเสี่ยงนั้นได้เป็นอย่างดีหรือไม่ ระดับความเสี่ยงที่เกิดจากผู้ดำเนินการแทน ควรจะอยู่ในระดับที่ สรอ. ยอมรับได้ หากผู้ดำเนินการแทนไม่สามารถทำได้ดี ความเสี่ยงจะตกกลับมาที่ สรอ. เอง

สำหรับกรณีการซื้อประกันภัย หน่วยงานหรือสำนักควรจัดการกับความเสี่ยงนั้นในระดับหนึ่ง แต่อาจจะยังไม่เพียงพอ จึงเสริมด้วยการซื้อประกัน หากเหตุการณ์ความเสี่ยงยังคงเกิดขึ้นได้ สรอ. จะไม่เสียหายมากเกินไป ทั้งนี้เนื่องจากมีการจัดการไว้ในระดับหนึ่ง

๕.๕.๔ การลดความเสี่ยง (Reduction) คือ การหาทางลดค่าความเสี่ยงที่อาจตกอยู่ในบริเวณสีเหลือง สีส้ม หรือ สีแดงก็ตาม ให้ลงมาอยู่ในระดับที่น้อยลง

กรณีที่หน่วยงานหรือสำนักสามารถลดความเสี่ยงลงมาอยู่ในบริเวณสีเขียวได้ หน่วยงานสามารถยอมรับความเสี่ยงได้ และไม่ต้องทำอะไรเพิ่มเติม แต่หากอยู่ในบริเวณสีเหลือง หน่วยงานยังต้องคอยคุมความเสี่ยงไว้ (เพื่อป้องกันการเลื่อนระดับไปสู่ระดับที่สูงขึ้น)

เมื่อมีการประเมินระดับความเสี่ยงในหัวข้อที่แล้ว หน่วยงานหรือสำนักต้องพิจารณาค่าระดับความเสี่ยงนั้นและตัดสินใจว่าจะใช้ทางเลือกใด (จาก ๑ ใน ๔ ทางเลือก) เพื่อจัดการกับความเสี่ยงที่ประเมินนั้น ซึ่งได้อธิบายวิธีการใช้ทางเลือกแต่ละทางเลือกไปแล้วในข้างต้น

๕.๖ กิจกรรมการควบคุม (Control Activities)

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง และหน่วยงานที่เกี่ยวข้องหรือเป็นเจ้าของความเสี่ยง มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ โดยจะควบคุมความเสี่ยง ให้สอดคล้องกับระดับความเสี่ยง ที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการบริหาร สรอ. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

๕.๗ การรายงานความเสี่ยง (Risk Reporting)

ทุกหน่วยงานของ สรอ. ต้องมีการจัดทำรายงานการประเมินการควบคุมความเสี่ยงด้วยตนเอง (Risk and Control Self Assessment หรือ RCSA) อย่างน้อยปีละ ๑ ครั้ง โดยจุดที่มีความเสี่ยงอยู่ในระดับที่มีนัยสำคัญและระดับสูง จะต้องมีการจัดทำ Action Plan เพื่อปิดความเสี่ยงที่เกิดขึ้นกับหน่วยงานต่อไป

ในกรณีที่มีความความเสียหายที่เกิดจากความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Operational Loss Data) หน่วยงานต้องรายงานเหตุการณ์ความเสียหายที่เกิดจากความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่เกิดขึ้นกับหน่วยงานทันทีหรือภายในวันทำการถัดไป และในกรณีที่ไม่มีเหตุการณ์ความเสียหายฯ หน่วยงานก็ต้องรายงานให้ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงทราบด้วย เพื่อให้มั่นใจว่าส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยงได้รับข้อมูลที่ถูกต้องและครบถ้วน โดยข้อมูลทั้งหมดนั้นส่วนพัฒนาคุณภาพองค์กรและ

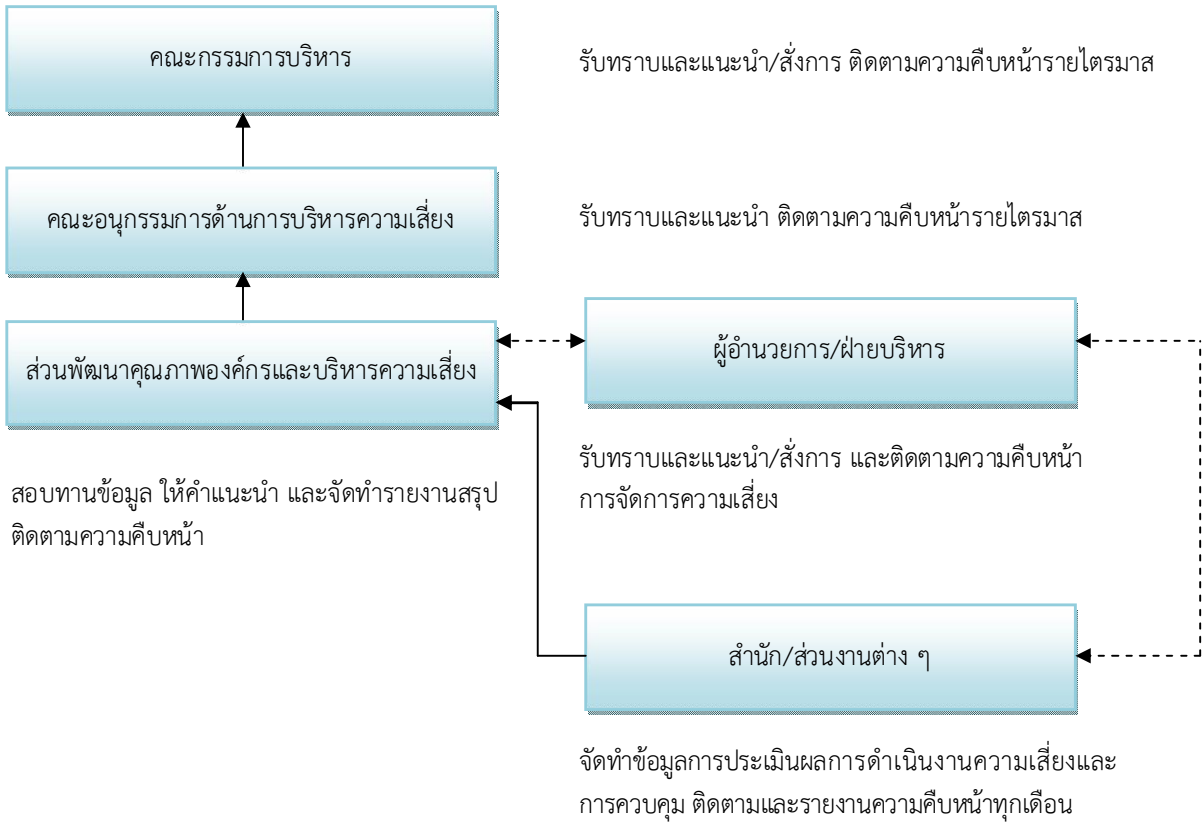
บริหารความเสี่ยงจะรวบรวมสรุปผล และนำเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง หรือคณะอนุกรรมการที่เกี่ยวข้องต่อไป

ทั้งนี้ หากมีความเสียหายที่มีนัยสำคัญเกิดขึ้นกับหน่วยงาน หน่วยงานจะต้องมีการจัดทำ Treatment Plan เพื่อลดหรือป้องกันไม่ให้เกิดความเสียหายดังกล่าวขึ้นกับ สรอ. ได้อีกในอนาคต และหากมีเหตุฉุกเฉินเกิดขึ้น เจ้าหน้าที่ของ สรอ. ที่พบจะต้องรายงานเหตุการณ์ความเสี่ยงตามคู่มือ Business Continuity Plan ที่กำหนดไว้ และหน่วยงานที่มีความเสี่ยงอยู่ในระดับสูงหรือมีนัยสำคัญ ต้องมีการนำดัชนีชี้วัดความเสี่ยง (Key Risk Indicators: KRIs) ที่สะท้อนถึงสาเหตุและโอกาสที่จะเกิดความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ซึ่งดัชนีชี้วัดความเสี่ยงนี้ถือเป็นเครื่องมือในการวัด ติดตาม และบริหารความเสี่ยงที่สำคัญของหน่วยงาน ทั้งนี้ หน่วยงานต้องมีการรายงานดัชนีชี้วัดความเสี่ยงมายังส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ตามรูปแบบและระยะเวลาที่กำหนด เพื่อใช้ในการติดตามดูแลความเสี่ยงที่มีอยู่หรือที่อาจจะเกิดขึ้น

๕.๘ การติดตามและประเมินผล (Monitoring)

ทุกหน่วยงานต้องจัดให้มีกระบวนการในการติดตามความเสี่ยงที่มีอยู่ ตามแต่ช่วงเวลาที่เหมาะสมหรือตามการเปลี่ยนแปลงของความเสี่ยง โดยหน่วยงานควรกำหนดความถี่ในการติดตามให้มากขึ้น เช่น รายสัปดาห์ หากความเสี่ยงมีการเปลี่ยนแปลงที่มากขึ้น เป็นต้น แต่หากข้อมูลปัจจัยเสี่ยงมีการเปลี่ยนแปลงน้อยและเปลี่ยนแปลงค่อนข้างช้า หน่วยงานอาจติดตามเพียงเดือนละครั้ง ไตรมาสละครั้ง หรือปีละสองครั้ง ทั้งนี้ เพื่อให้ผู้บริหาร ผู้อำนวยการ สรอ. สามารถติดตามสถานะของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่มีอยู่ในแต่ละช่วงเวลา และสามารถวางแผนในการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่เกิดขึ้นได้อย่างเหมาะสมและมีประสิทธิภาพ อีกทั้งยังช่วยให้หน่วยงานสามารถป้องกันและควบคุมเหตุการณ์ความเสียหายที่อาจเกิดขึ้นได้อย่างทันท่วงที

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติ ส่วนนโยบายและกลยุทธ์องค์กรต้องรายงานให้ผู้บริหาร สรอ. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สรอ. / ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการบริหาร
ปานกลาง หรือเตือน (Warning)	รับทราบ/แนะนำ และสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำ และสั่งการ
ค่อนข้างสูง หรือรุนแรง (Severe)	รับทราบ/แนะนำ และสั่งการรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ
สูง หรือรุนแรงมาก (High Severe)	รับทราบ/แนะนำ/ สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ

แหล่งข้อมูลอ้างอิง

หน่วยงานที่เกี่ยวข้อง

๑. สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.)
๒. สำนักงานการตรวจเงินแผ่นดิน
๓. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๔. บริษัท ทริส คอร์ปอเรชั่น จำกัด

กฎหมายที่เกี่ยวข้อง

๑. พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๔๖
๒. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐
๓. พระราชบัญญัติองค์การมหาชน

เว็บไซต์ที่เกี่ยวข้อง

๑. www.opdc.go.th
๒. www.oag.go.th
๓. www.coso.org
๔. www.iso.org
๕. www.isaca.org
๖. www.bot.or.th
๗. www.itgthailand.com
๘. www.sec.or.th
๙. www.set.or.th
๑๐. www.mict.go.th
๑๑. www.ega.or.th

คำขอบคุณจากคณะผู้จัดทำ
นโยบายและคู่มือบริหารความเสี่ยง
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

ในนามของคณะผู้จัดทำนโยบายและคู่มือบริหารความเสี่ยงของสำนักงานรัฐบาลอิเล็กทรอนิกส์ ฉบับนี้ ขอขอบพระคุณคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ คณะอนุกรรมการด้านการบริหารความเสี่ยงสำนักงานรัฐบาลอิเล็กทรอนิกส์ คณะผู้บริหารและคณะทำงาน และผู้ที่มีส่วนเกี่ยวข้องทุกท่านในการให้การช่วยเหลือ และให้ความร่วมมือจนทำให้นโยบายและคู่มือบริหารความเสี่ยงของสำนักงานสามารถจัดทำขึ้นได้อย่างสมบูรณ์และสำเร็จ เพื่อให้เจ้าหน้าที่ทุกคนในสำนักงาน ใช้เป็นแนวทางในการดูแลและบริหารความเสี่ยงภายใต้ความรับผิดชอบของแต่ละคน และหวังเป็นอย่างยิ่งว่านโยบายและคู่มือบริหารความเสี่ยงฉบับนี้จะมีประโยชน์แก่ทุกคนและส่วนรวม

<u>รายนามคณะกรรมการบริหาร</u>

๑. รศ. ดร. วรากรณ์ สามโกเศศ	ประธานกรรมการ
๒. ศ. เข็มชัย ชุติวงศ์	กรรมการ
๓. นายจเรรัฐ ปิงคลาศัย	กรรมการ
๔. รศ. จารุพร ไวยนันท์	กรรมการ
๕. พ.อ. เจียรนัย วงศ์สอาด	กรรมการ
๖. นายไชยเจริญ อติแพทย์	กรรมการ
๗. นายวรวิทย์ จำปีรัตน์	กรรมการ
๘. นายไชยยันต์ พึ่งเกียรติไพโรจน์	กรรมการ
๙. ศ. พิเศษ ดร. ทศพร ศิริสัมพันธ์	กรรมการ
๑๐. ดร. ทวีศักดิ์ กออนันตกูล	กรรมการ
๑๑. ดร. ศักดิ์ เสกขุนทด	เลขานุการ

<u>รายนามคณะอนุกรรมการบริหารความเสี่ยง</u>

๑. ดร. ทวีศักดิ์ กออนันตกูล	ที่ปรึกษา
๒. ดร. รอม หิรัญพฤกษ์	ที่ปรึกษา
๓. พ.อ. เจียรนัย วงศ์สอาด	ประธานอนุกรรมการ
๔. นางสาววลัยรัตน์ ศรีอรุณ	อนุกรรมการ
๕. นายจเรรัฐ ปิงคลาศัย	อนุกรรมการ
๖. ดร. รุ่งโรจน์ โชคงามวงศ์	อนุกรรมการ
๗. ผศ. ดร. สรายุทธ์ นาทะพันธ์	อนุกรรมการ
๘. นายสุจินดา สุขุม	อนุกรรมการ
๘. ดร. ศักดิ์ เสกขุนทด	อนุกรรมการ
๙. นางกนกพร สาณะวัฒนา	เลขานุการ
๑๐. นายประสงค์ พันธ์ลิมา	ผู้ช่วยเลขานุการ

<u>รายนามที่ปรึกษา</u>

นางสาววลัยรัตน์ ศรีอรุณ	ที่ปรึกษาสำนักงานรัฐบาลอิเล็กทรอนิกส์

<u>รายนามคณะผู้บริหาร</u>

๑. ดร. ศักดิ์ เสกขุนทด	ผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์
๒. นางไอรดา เหลืองวิไล	รองผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์
๓. นางสาวอภิณห์พร อังคกมลเศรษฐ์	ผู้ช่วยผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์
๔. นางกนกพร สาณะวัฒนา	ผู้อำนวยการสำนักบริหารและจัดการองค์กร
๕. นางสาวนันทนา พจนานันทกุล	ผู้อำนวยการสำนักสถาปัตยกรรมรัฐบาลอิเล็กทรอนิกส์
๖. ดร. อาศิส อัญญะโพธิ์	ผู้อำนวยการสำนักพัฒนาระบบสารสนเทศ
๗. นายวิบูลย์ ภัทรพิบูล	ผู้อำนวยการสำนักที่ปรึกษาระบบรัฐบาลอิเล็กทรอนิกส์
๘. นางสาวนันทวัน วงศ์ขจรกิตติ	ผู้อำนวยการสำนักวิศวกรรมและปฏิบัติการโครงสร้างพื้นฐานสารสนเทศ
๙. นายชรินทร์ ธีรฐิตยางกูร	ผู้อำนวยการสำนักส่งเสริมและถ่ายทอดเทคโนโลยี

<u>รายนามคณะผู้จัดทำ</u>

๑. นางกนกพร สาณะวัฒนา	ผู้อำนวยการสำนักบริหารและจัดการองค์กร
๒. นายประสงค์ พันธ์ลิมา	ผู้จัดการส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง
๓. นายโชติพันธ์ ไชยสุวกุล	เจ้าหน้าที่พัฒนาคุณภาพองค์กรและบริหารความเสี่ยงอาวุโส
๔. ว่าที่ร้อยตรี ทวีชัย พรมขันธ์	เจ้าหน้าที่พัฒนาคุณภาพองค์กรและบริหารความเสี่ยงอาวุโส
๕ นายชติพจน์ ศรีเมือง	เจ้าหน้าที่พัฒนาคุณภาพองค์กรและบริหารความเสี่ยง ๒

<u>ออกแบบโดย</u> นายโชติพันธ์ ไชยสุวกุล เจ้าหน้าที่พัฒนาคุณภาพองค์กรและบริหารความเสี่ยงอาวุโส

<u>ปีที่พิมพ์</u> ๒๕๕๖

<u>จำนวนที่พิมพ์</u> ๑๐๐ เล่ม

สำนักบริหารและจัดการองค์กร

(Corporate Management and Administration Department

ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง

(Corporate Quality Development and Risk Management Division)