นโยบายและคู่มือบริหารความเสี่ยง ปี ๒๕๕๘

RISK MANAGEMENT POLICY AND MANUAL 2015

นโยบายและคู่มือบริหารความเสี่ยง ปี ๒๕๕๘

RISK MANAGEMENT POLICY AND MANUAL 2015

นโยบายและคู่มือบริหารความเสี่ยง ปี ๒๕๕๘
RISK MANAGEMENT POLICY AND MANUAL 2015

ISBN : 978-974-9765-72-2
พิมพ์ครั้งที่ 1 (มกราคม 2559) จำนวนพิมพ์ 400 เล่ม

จัดทำโดย

ส่วนบริหารความเสี่ยง
ฝ่ายนโยบายและยุทธศาสตร์
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.)
ชั้น 17 อาคารบางกอกไทยทาวน์เวอร์
108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ
โทรศัพท์ 0 2612 6000 โทรสาร 0 2612 6010-12
http://www.ega.or.th e-mail: contact@ega.or.th

จัดพิมพ์โดย

บริษัท พี.เอ็ม. มีเดีย พริ้นท์ จำกัด
1575/1 อาคารชัยสงวน ถนนเพชรบุรีตัดใหม่
แขวงมักกะสัน เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2253 6350-1, 08 1467 8559
โทรสาร 0 2253 6352
e-mail: pmmediaprint@yahoo.com

คำนิยม

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

ภายใต้การบริหารความเปลี่ยนแปลงต่าง ๆ ที่เกิดจากปัจจัยทั้งภายในและภายนอกที่มากระทบกับองค์กร แน่นอนที่สุดที่ทุกคนต้องยอมรับและต้องตระหนักควบคู่กันไปด้วยคือ “การบริหารความเสี่ยง” ซึ่งองค์กรที่มีความพร้อมรับมือการเปลี่ยนแปลงและให้ความสำคัญกับการบริหารจัดการและควบคุมความเสี่ยงให้อยู่ในระดับการยอมรับได้เท่านั้นที่จะทำให้ธุรกิจสามารถรับมือกับการเปลี่ยนแปลงและดำเนินภารกิจได้ประสบความสำเร็จ การบริหารความเสี่ยงเป็นองค์ประกอบของการกำกับดูแลกิจการที่ดี ซึ่งนอกจากจะสนับสนุนให้องค์กรสามารถดำเนินงานได้บรรลุตามเป้าหมายที่กำหนดแล้ว ยังสามารถสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้ ส่วนเสียขององค์กร (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 ปฏิบัติได้ในการจัดการกับความเสี่ยงที่มิใช่การขจัดความเสี่ยงให้หมดสิ้นไปซึ่งเป็นสิ่งที่เป็นไปไม่ได้ ดังนั้น การลดความเสี่ยงในด้านต่าง ๆ ให้อยู่ในระดับที่ยอมรับได้จึงเป็นเป้าหมายของคู่มือฉบับนี้ของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ซึ่งนับว่าเป็นคู่มือที่มีความครบถ้วน สมบูรณ์ อันจะนำไปสู่การบริหารจัดการความเสี่ยงในการปฏิบัติภารกิจของสรอ.ได้อย่างมีประสิทธิผล

อย่างไรก็ตาม การมีคู่มือบริหารความเสี่ยงเพียงอย่างเดียวไม่ได้ทำให้สรอ.มีการบริหารจัดการความเสี่ยงที่ดีได้การปฏิบัติตามคู่มือฉบับนี้อย่างเคร่งครัด เป็นเงื่อนไขสำคัญยิ่งที่จะนำไปสู่ความสำเร็จในการควบคุมความเสี่ยงทุกด้านของ สรอ. ฉะนั้น การสร้างความตระหนักและการทำความเข้าใจกับผู้บริหารและพนักงานทุกคนจึงเป็นสิ่งแรกที่ควรกระทำเพื่อให้คู่มือฉบับนี้ได้ถูกนำไปใช้กับทุกปัจจัยเสี่ยงซึ่งจะทำให้ สรอ. สามารถปฏิบัติภารกิจ และบรรลุเป้าหมายขององค์กรได้อย่างมีความเสี่ยงน้อยที่สุด

นางสาววลัยรัตน์ ศรีอรุณ
ที่ปรึกษา สำนักงานรัฐบาลอิเล็กทรอนิกส์

คำนิยม

ความเสี่ยง เป็นเรื่องปกติของวิวัฒนาการความเจริญก้าวหน้าสำหรับการบริหารองค์กร จุดที่สำคัญคือ ต้อง Identify ให้ได้ว่าความเสี่ยงอยู่ระดับไหน มีโอกาสเพียงใดจะลดระดับความเสี่ยง และตัดสินใจเดินหน้าอย่างมีเหตุมีผลได้อย่างไร

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) เป็นหน่วยงานที่ให้ความสำคัญเป็นอย่างยิ่งในการบริหารจัดการความเสี่ยง ครอบคลุมทั้ง PROCESS, PEOPLE และ TECHNOLOGY เพื่อให้การดำเนินงานการขับเคลื่อนเศรษฐกิจดิจิตอล (Digital Economy) และรัฐบาลอิเล็กทรอนิกส์ (e-Government) ตามภารกิจที่ให้เป็นไปตามเป้าหมาย และสามารถขับเคลื่อนประเทศได้อย่างมั่นคง และ ยั่งยืน

นายไชยเจริญ อติแพทย์
ประธานคณะอนุกรรมการด้านการบริหารความเสี่ยง
สำนักงานรัฐบาลอิเล็กทรอนิกส์

คำนิยม

การเปลี่ยนแปลงของสภาวะแวดล้อมในปัจจุบัน เป็นความจริงที่ไม่สามารถหลีกเลี่ยงได้ ไม่เว้นแม้แต่วิวัฒนาการด้านเทคโนโลยีสารสนเทศ การจับกระแสทิศทางการเปลี่ยนแปลงของโลกยุคใหม่เพื่อปรับเปลี่ยนให้ทันหรือสอดรับต่อเหตุการณ์ที่เปลี่ยนผันตลอดเวลานั้น อาจส่งผลให้การดำเนินงานของหลาย ๆ องค์กรไม่เป็นไปตามเป้าหมายที่ได้กำหนดไว้ตามแผนการดำเนินงาน เนื่องจากต้องเผชิญหน้ากับการเปลี่ยนแปลงตลอดเวลา อีกทั้งความเสี่ยงที่อาจเกิดขึ้นได้จากสภาพแวดล้อมทั้งภายในและภายนอกองค์กร อาจส่งผลกระทบสร้างความเสียหายหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ที่กำหนดไว้ หากองค์กรละเลยในการดูแลและจัดการกับ “การบริหารความเสี่ยง”

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ตระหนักถึงความสำคัญของการบริหารความเสี่ยงซึ่งถือได้ว่าเป็นองค์ประกอบของการกำกับดูแลกิจการที่ดี (Good Governance) จึงได้จัดทำนโยบายบริหารความเสี่ยงขึ้น เพื่อให้เป็นกรอบแนวทางในการดำเนินการและการพัฒนาระบบการบริหารความเสี่ยงที่มีคุณภาพและมีมาตรฐานตามแนวทางการกำกับดูแลของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และสำนักงานคณะกรรมการพัฒนาระบบราชการ โดยเล็งเห็นว่าหากสำนักงานมีการบริหารความเสี่ยงที่มีประสิทธิภาพ จะเป็นส่วนสำคัญอย่างยิ่งในการเพิ่มศักยภาพขององค์กร จึงได้กำหนดนโยบายการบริหาร ความเสี่ยง (Enterprise Risk Management Policy) ของสำนักงานให้ครอบคลุม ๕ ด้าน ได้แก่ ด้านนโยบายและกลยุทธ์ ด้านการปฏิบัติงาน ด้านการเงิน ด้านกฎหมาย กฎระเบียบ และด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

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

ดร.ศักดิ์ เสกขุนทด
ผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์

โครงสร้างเนื้อหา

ประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์(องค์การมหาชน)

ที่ ๑ / ๒๕๕๘

เรื่อง นโยบายบริหารความเสี่ยงสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

.....

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ตระหนักถึงความสำคัญของการบริหารความเสี่ยง ซึ่งครอบคลุมคู่มือบริหารความเสี่ยงองค์กรและคู่มือบริหารความเสี่ยง ๕ ด้าน ประกอบด้วย ด้านนโยบายและกลยุทธ์ ด้านการปฏิบัติงาน ด้านการเงิน ด้านกฎหมาย กฎระเบียบ และด้านระบบเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินงานภายในองค์กรมีประสิทธิภาพสามารถบรรลุตามภารกิจขององค์กรตามหลักการกำกับดูแลกิจการที่ดี (Good Corporate Government)

อาศัยอำนาจตามมาตรา ๒๖ และ ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ๒๕๕๔ ประกอบกับมติคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ ครั้งที่ ๑๑/๒๕๕๗ เมื่อวันที่ ๑๗ พฤศจิกายน ๒๕๕๗ คณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์จึงออกประกาศดังต่อไปนี้

๑. ให้ยกเลิกประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ ๕/๒๕๕๕ เรื่องนโยบายบริหารความเสี่ยงสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ลงวันที่ ๒๒ สิงหาคม ๒๕๕๕

๒. ให้ยกเลิกประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ ๖/๒๕๕๕ เรื่องนโยบายบริหารความเสี่ยงด้านการปฏิบัติงาน สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ลงวันที่ ๒๒ สิงหาคม ๒๕๕๕

๓. ให้ยกเลิกประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ ๗/๒๕๕๕ เรื่องนโยบายบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ลงวันที่ ๑๑ กันยายน ๒๕๕๕

๔. ให้ยกเลิกประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ ๘/๒๕๕๕ เรื่องนโยบายบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ลงวันที่ ๑๑ กันยายน ๒๕๕๕

๕. ให้ยกเลิกประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ ๙/๒๕๕๕ เรื่องนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ลงวันที่ ๒๒ ตุลาคม ๒๕๕๕

๖. ให้ยกเลิกประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ ๑๐/๒๕๕๕ เรื่องนโยบายบริหารความเสี่ยงด้านการเงิน สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ลงวันที่ ๒๒ ตุลาคม ๒๕๕๕

๗. กำหนดให้มีการดำเนินงานบริหารความเสี่ยงดังต่อไปนี้

(๑) ให้ทุกส่วนงานมีการดำเนินงานระบบบริหารจัดการความเสี่ยงและควบคุมคุมภายในผ่านระบบอิเล็กทรอนิกส์ (โปรแกรมบริหารความเสี่ยงและควบคุมภายใน) ตามกระบวนการและขั้นตอนการบริหารความเสี่ยง

(๒) ให้ทุกส่วนงานที่มีการระบุความเสี่ยง ประเมินความเสี่ยง หรือแผนลดความเสี่ยงในช่วงที่ผ่านมาให้ดำเนินการลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ หรือดำเนินงานตามแผนงานที่ได้กำหนดไว้แล้ว

(๓) มีการทบทวนและทดสอบแผนรองรับความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ในทุกส่วนงานที่เกี่ยวข้อง เพื่อเป็นการเตรียมความพร้อมต่อเหตุการณ์ภัยพิบัติได้ทันท่วงที

(๔) มีการพัฒนาองค์ความรู้ของบุคลากรในองค์กรเกี่ยวกับการบริหารจัดการความเสี่ยงและแผนรองรับความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อเพิ่มประสิทธิภาพในการบริหารความเสี่ยงอย่างเหมาะสม

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีการเปลี่ยนแปลง

ประกาศ ณ วันที่ ๑๔ มกราคม พ.ศ. ๒๕๕๘

(นายศักดิ์ เสกขุนทด)
ผู้อำนวยการ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

คู่มือบริหารความเสี่ยงสำนักงานรัฐบาลอิเล็กทรอนิกส์
(Enterprise Risk Management Manual)

สารบัญ

๑. บทสรุปผู้บริหาร

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ตระหนักถึงความสำคัญของการบริหารความเสี่ยง จึงได้จัดทำนโยบายบริหารความเสี่ยง (Enterprise Risk Management Policy) ขึ้น เพื่อให้เป็นกรอบแนวทางการพัฒนาระบบการบริหารความเสี่ยงให้มีคุณภาพและมาตรฐานตามแนวทางการกำกับดูแลของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และสำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) รวมถึงแนวทางปฏิบัติที่ดี โดยคำนึงถึงความสอดคล้องกับวัตถุประสงค์และเป้าหมายการดำเนินงานของสำนักงาน ทั้งนี้ เพื่อให้นโยบายบริหารความเสี่ยงสำนักงานรัฐบาลอิเล็กทรอนิกส์ (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 เป้าหมายและวัตถุประสงค์อันจะเป็นการสร้างความรับผิดชอบอย่างทั่วถึงและเป็นไปในทิศทางเดียวกันทั่วทั้งสำนักงานได้อย่างมีประสิทธิภาพ

นโยบายการบริหารความเสี่ยง (Enterprise Risk Management Policy) จัดทำขึ้นเพื่อวัตถุประสงค์ ดังนี้

๑) เพื่อใช้เป็นแนวทางให้กับผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กร ในการเป็นส่วนหนึ่งของการพัฒนากระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์

๒) เพื่อให้สำนักงานมีกรอบการดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่อาจส่งผลให้เกิดความเสี่ยงทุกด้านได้อย่างเป็นระบบและมีมาตรฐาน รวมทั้งมีการดำเนินการเพื่อสร้างพื้นฐานในการป้องกันความเสี่ยงระยะยาวให้กับสำนักงานที่สำคัญ

๓) เพื่อเป็นกลไกในการพัฒนาองค์ความรู้ด้านการบริหารความเสี่ยงให้เกิดขึ้นกับผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งสำนักงาน และสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน

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

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

๑) ด้านนโยบายและกลยุทธ์

๒) ด้านการปฏิบัติงาน

๓) ด้านการเงิน

๔) ด้านกฎหมาย กฎระเบียบ

๕) ด้านระบบเทคโนโลยีสารสนเทศ

ซึ่งสามารถจัดทำเป็นนโยบายที่เกี่ยวข้องด้านการบริหารความเสี่ยง ๕ นโยบาย ประกอบด้วย

๑) นโยบายด้านนโยบายและกลยุทธ์ หมายถึงความเสี่ยงที่เกิดจากการกำหนดนโยบายต่าง ๆ เช่น นโยบายระดับรัฐจนถึงนโยบายในระดับผู้บริหารแผนกลยุทธ์ แผนดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับสภาพแวดล้อมภายใน และปัจจัยภายนอก เป็นต้น ทำให้มีโอกาสที่จะไม่ประสบความสำเร็จตามทิศทางที่กำหนดไว้ ซึ่งจะส่งผลกระทบต่อตัวชี้วัดผลการปฏิบัติงานของสำนักงาน

๒) นโยบายด้านการปฏิบัติงาน หมายถึง ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากบุคลากร ระบบงาน และระบบสารสนเทศ รวมถึงการขาดระบบการควบคุมที่เกี่ยวข้องกับกระบวนการปฏิบัติงานทั้งหมด โดยเฉพาะการไม่ได้ประเมินความเสี่ยงของโครงการของสำนักงาน

๓) นโยบายด้านการเงิน หมายถึง ความเสี่ยงทางการเงินในภาพรวม ทั้งในด้านการบริหารจัดการด้านการเงิน การวางแผนทางการเงินซึ่งต้องเป็นไปในทิศทางเดียวกับกลยุทธ์ของสำนักงาน และกฎหมาย กฎระเบียบต่าง ๆ ที่เกี่ยวข้อง

๔) นโยบายด้านกฎหมาย กฎระเบียบ หมายถึง ความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับกฎหมาย 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

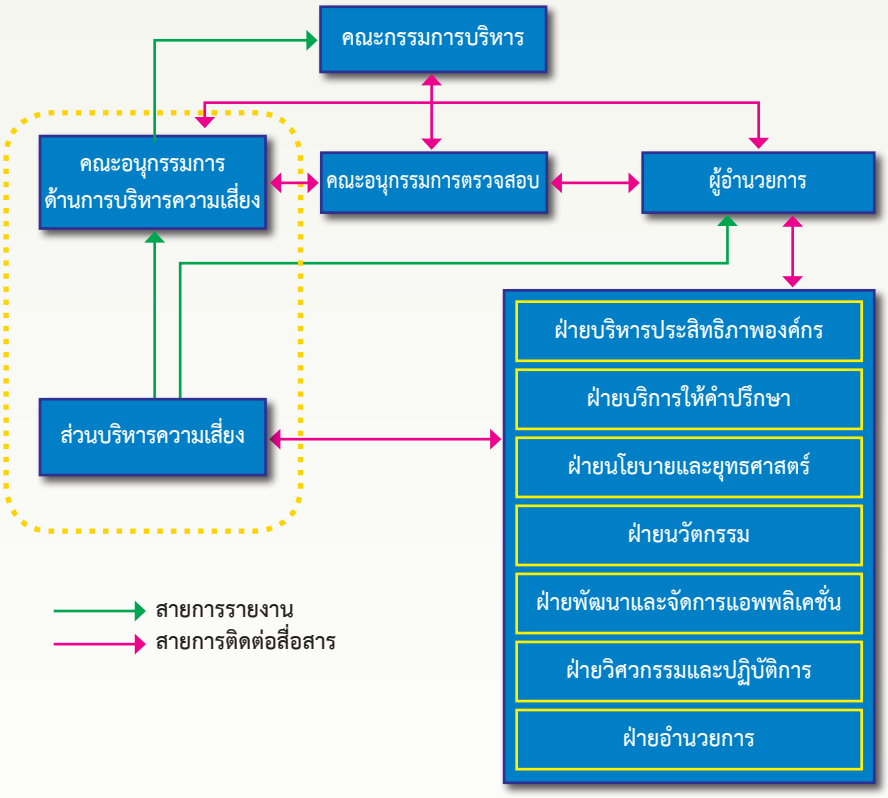
๒) ความสอดคล้องกับแนวทางมาตรฐานของหน่วยงานกำกับดูแล ข้อกำหนดของกฎหมาย ระเบียบ ประกาศ หลักเกณฑ์ และแนวทางปฏิบัติที่ดี

๓) สำนักงานจะต้องทบทวนกลยุทธ์การบริหารความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง ตามแผนประจำปี หรือทบทวนทันทีที่มีเหตุการณ์เปลี่ยนแปลงที่มีนัยสำคัญเพื่อให้ทราบถึงปัญหา อุปสรรค ที่ส่งผลต่อการบรรลุเป้าหมายการบริหารความเสี่ยง และเพื่อสร้างความมั่นใจถึงการบรรลุเป้าหมายโดยรวมของสำนักงาน

๔. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงและบทบาทหน้าที่รับผิดชอบการบริหารความเสี่ยง

สำนักงานต้องจัดให้มีโครงสร้างหน้าที่ของคณะอนุกรรมการและหน่วยงานเพื่อกำกับดูแลและรับผิดชอบด้านการบริหารความเสี่ยง โดยโครงสร้างหน้าที่ต้องมีความชัดเจน สอดคล้องกับการบริหารความเสี่ยงของสำนักงาน และเหมาะสมกับการดำเนินงานขององค์กรรวมถึงมีความเป็นอิสระและมีการถ่วงดุลอำนาจอย่างเหมาะสม ดังนี้



๕. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการที่เกี่ยวข้องกับการบริหารความเสี่ยง

คณะกรรมการ	บทบาทหน้าที่และความรับผิดชอบ
คณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์	๑) อนุมัตินโยบาย และกลยุทธ์การบริหารความเสี่ยงเพื่อประกาศใช้ ๒) กำกับดูแลให้มีการดำเนินงานที่เป็นไปตามหลักเกณฑ์ของทางการ และเป็นไปตามหลักการกำกับดูแลกิจการที่ดี มีความโปร่งใส เป็นธรรมต่อทุกหน่วยงานที่เกี่ยวข้อง
คณะอนุกรรมการด้านบริหารความเสี่ยง	๑) เสนอแนะนโยบายการบริหารความเสี่ยงและกรอบของการบริหารความเสี่ยงต่อคณะกรรมการ ๒) ให้คำปรึกษาและเสนอแนะการจัดทำแผนบริหารความเสี่ยงเพื่อให้บรรลุเป้าหมายตามแผนปฏิบัติงานของสำนักงานเพื่อเสนอต่อคณะกรรมการ ๓) เสนอแนะแนวทาง ในการบริหารจัดการหรือการดำเนินงาน เพื่อลดผลกระทบและความเสี่ยงที่อาจจะเกิดขึ้นกับสำนักงาน ๔) พิจารณาผลการประเมินและติดตามความมีประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงเพื่อรายงานต่อคณะกรรมการ ๕) ในกรณีการพิจารณากลั่นกรอง ให้คำปรึกษา ประเมินหรือวิเคราะห์ในเรื่องใดที่จำเป็นต้องมีผู้เชี่ยวชาญเฉพาะด้านในสาขาที่เกี่ยวข้องเข้าร่วมพิจารณาในรายละเอียด ให้คณะอนุกรรมการเชิญบุคคลดังกล่าวเข้าร่วมพิจารณากับคณะอนุกรรมการเป็นคราว ๆ ไป โดยให้บุคคลดังกล่าวได้รับค่าตอบแทนตามระเบียบสำนักงาน ๖) ปฏิบัติงานอื่นใดตามที่ประธานกรรมการ หรือคณะกรรมการมอบหมาย

คณะกรรมการ	บทบาทหน้าที่และความรับผิดชอบ
คณะอนุกรรมการตรวจสอบ	๑) สอบทานให้สำนักงานมีระบบการควบคุมภายในระบบการตรวจสอบภายในและระบบการบริหารความเสี่ยงที่เหมาะสมและมีประสิทธิผล ๒) ให้คำปรึกษาและเสนอแนะแนวทางการพัฒนาปรับปรุงระบบการควบคุมภายในระบบการตรวจสอบภายในและระบบการบริหารความเสี่ยงที่สำคัญและจำเป็นเพื่อให้มีความทันสมัยอยู่เสมอ ๓) กำกับดูแลการปฏิบัติให้สอดคล้องตามนโยบายข้อบังคับกฎระเบียบประกาศคำสั่งมติคณะรัฐมนตรีและกฎหมายอื่น ๆ ที่เกี่ยวข้อง

บทบาท หน้าที่และความรับผิดชอบของผู้บริหาร หน่วยงาน และเจ้าหน้าที่ที่เกี่ยวข้องกับการบริหารความเสี่ยง

หน่วยงาน/ผู้บริหาร/คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
ผู้อำนวยการ เจ้าหน้าที่และลูกจ้างทุกคนในสำนักงาน	๑) มีหน้าที่รับผิดชอบการวิเคราะห์ระบุและประเมินความเสี่ยงกำหนดระดับความเสี่ยงที่ยอมรับได้และกำหนดมาตรการหรือแผนบริหารความเสี่ยงของหน่วยงาน/โครงการหรืองานที่อยู่ในความรับผิดชอบ ๒) ติดตามและรายงานความเสี่ยงให้ผู้บังคับบัญชาทราบตามลำดับชั้นตลอดจนคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอเพื่อให้การบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ
ผู้บริหาร	ผู้บริหารตั้งแต่ระดับผู้จัดการขึ้นไปมีหน้าที่กำกับดูแลหน่วยงาน/โครงการให้มีการบริหารและจัดการความเสี่ยงและเป็นเจ้าของความเสี่ยง (Risk Owner)

หน่วยงาน/ผู้บริหาร/คณะทำงาน	บทบาทหน้าที่และความรับผิดชอบ
คณะทำงานการบริหารความเสี่ยงด้าน/เรื่องต่าง ๆ	มีหน้าที่ตามที่ได้รับมอบหมายจากคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์หรือคณะอนุกรรมการด้านการบริหารความเสี่ยง
ส่วนบริหารความเสี่ยง	๑) จัดและทบทวนนโยบายและกลยุทธ์ในการดำเนินงานด้านการบริหารความเสี่ยงเพื่อนำเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยง ๒) จัดทำและทบทวนเครื่องมือในการวัดติดตามและควบคุมความเสี่ยงเพื่อเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง ๓) ติดตามและรายงานสถานะความเสี่ยงต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง
ส่วนตรวจสอบภายใน	๑) สอบทานและประเมินความเพียงพอความมีประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงระบบการควบคุมภายในและระบบที่ส่งเสริมการกำกับดูแลกิจการที่ดี ๒) ตรวจสอบการดำเนินงานตามแผนงานหรือโครงการเพื่อสอดคล้องกับวัตถุประสงค์และเป้าหมายที่กำหนดไว้อย่างมีประสิทธิภาพและประสิทธิผล
ฝ่าย/ส่วน	๑) ควบคุมดูแลการปฏิบัติงานในฝ่าย/ส่วนให้เป็นไปตามนโยบายและกลยุทธ์การบริหารความเสี่ยงรวมทั้งจัดให้มีระบบบริหารความเสี่ยงที่มีประสิทธิภาพ ๒) สร้างความมั่นใจว่าการปฏิบัติงานรายวันมีการประเมินจัดการและรายงานความเสี่ยงอย่างเพียงพอ ๓) ส่งเสริมเจ้าหน้าที่ในฝ่ายและส่วนงานให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง ๔) สร้างความมั่นใจว่าแผนการบริหารความเสี่ยงได้รับการปฏิบัติอย่างครบถ้วน

หน่วยงาน/ผู้บริหาร/คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
Risk-Internal Control Officer (RICO)	๑) รับผิดชอบในการประสานงานการประเมินความเสี่ยงการควบคุมภายในและการปฏิบัติตามกฎเกณฑ์รวมทั้งเผยแพร่ความรู้ที่เกี่ยวข้องแก่เจ้าหน้าที่ในหน่วยงานของตนเอง ๒) ให้คำปรึกษาพร้อมทั้งประสานงานให้หน่วยงานตนเองดำเนินการตามกระบวนการบริหารความเสี่ยงโดยมีการระบุประเมินและจัดการความเสี่ยงด้านต่าง ๆ ที่อาจเกิดขึ้นเพื่อป้องกันหรือลดระดับความเสี่ยง ๓) ช่วยเหลือและสนับสนุนการจัดประชุมเชิงปฏิบัติการเพื่อจัดทำแผนจัดการความเสี่ยงทุกระดับ ๔) บันทึกติดตามและรายงานความก้าวหน้าของแผนจัดการความเสี่ยงระดับฝ่ายและส่วนงาน ๕) ประสานงานกับส่วนบริหารความเสี่ยง

๖. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

ความหมายของความเสี่ยง

การดำเนินงานในองค์กรโดยทั่วไปมีเป้าหมายเพื่อเพิ่มมูลค่าให้แก่ผู้มีส่วนได้ส่วนเสีย ทำให้ทุกองค์กรต้องเผชิญกับความไม่แน่นอน ที่อาจเกิดขึ้นจากปัจจัยภายในและภายนอกหลายประการ เช่น การเปลี่ยนแปลงของกฎ ระเบียบ และนโยบายของรัฐบาล การบริหารงานด้านความปลอดภัยในชีวิตและทรัพย์สินอันเนื่องมาจากการเปลี่ยนแปลงปัจจัยต่าง ๆ ภัยจากการก่อการร้าย ภัยธรรมชาติ และความเสี่ยงอื่น ๆ เป็นต้น ผู้บริหารจึงต้องพิจารณาว่าควรจัดการกับความไม่แน่นอนที่เกิดขึ้นอย่างไร เพื่อให้องค์การสามารถรักษาหรือเพิ่มมูลค่าของผู้มีส่วนได้ส่วนเสียได้

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

นิยามการบริหารความเสี่ยง

การบริหารความเสี่ยง คือ การกำหนดนโยบาย โครงสร้าง และกระบวนการ เพื่อให้คณะกรรมการ ผู้บริหารและบุคลากรขององค์กรนำไปปฏิบัติในการกำหนดกลยุทธ์และปฏิบัติงานทั่วทั้งองค์กร กระบวนการบริหารความเสี่ยงได้รับการออกแบบให้สามารถบ่งชี้เหตุการณ์ที่เกิดขึ้น ประเมินผลกระทบต่อองค์กร และกำหนดวิธีการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อให้เกิดความเชื่อมั่นในระดับหนึ่งว่า การดำเนินการในองค์กรจะบรรลุตามวัตถุประสงค์ที่กำหนดไว้

การบริหารความเสี่ยงที่มีประสิทธิผลมีข้อดี ดังต่อไปนี้

- เพิ่มมูลค่าขององค์กรที่มีต่อผู้มีส่วนได้ส่วนเสีย
- ทำให้เกิดความมั่นใจต่อการปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ
- เพิ่มประสิทธิภาพการทำงานของเจ้าหน้าที่
- ป้องกันและดูแลทรัพย์สินต่าง ๆ
- 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
Risk Criteria	ระดับ/เกณฑ์ความเสี่ยง
DegreeOf Acceptance	ระดับของการยอมรับความเสี่ยง
Risk Map	แผนภาพแสดงความสัมพันธ์ของปัจจัยเสี่ยงและผลกระทบทั้งในเชิงปริมาณและเชิงคุณภาพที่ส่งผลเชื่อมโยงกันต่อเป้าหมายของหน่วยงานต่าง ๆ ภายในองค์กร Risk Map สามารถช่วยในการจัดทำแผนการบริหารความเสี่ยงให้มีประสิทธิภาพมากขึ้นและครอบคลุมถึงปัจจัยเสี่ยงต่าง ๆ ครบถ้วน

ศัพท์เฉพาะ	คำนิยาม
Risk Profile	กลุ่ม (set) ของความเสี่ยง ที่แสดงให้เห็นถึงความเสี่ยงต่าง ๆ ที่อาจส่งผลกระทบต่อเป้าหมายของหน่วยงานต่าง ๆ โดยจะมีข้อมูลที่บ่งบอกลักษณะของความเสี่ยง ประเภทของความเสี่ยง ผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงนั้น ตลอดจนข้อมูลต่าง ๆ ที่เกี่ยวข้องกับความเสี่ยงนั้นสามารถแสดงด้วยแผนภูมิ (Risk Map) ๒ มิติ ขนาด ๕x๕ ประกอบด้วยแกนด้านผลกระทบ และแกนด้านโอกาสเกิดแต่ละแกนแบ่งระดับความรุนแรงเป็น ๕ ระดับมีวัตถุประสงค์เพื่อเป็นการวัดระดับความเสี่ยง
Risk Appetite	ระดับความเสี่ยงโดยรวมที่องค์กรยอมรับได้เพื่อมุ่งไปสู่พันธกิจหรือวิสัยทัศน์ขององค์กร
Risk Tolerance	ระดับความเบี่ยงเบนที่องค์กรยอมรับได้จากเกณฑ์หรือดัชนีวัดผลการดำเนินงานที่เกี่ยวข้องกับการบรรลุวัตถุประสงค์
KRI (Key Risk Indicator)	ตัวชี้วัดเชิงปริมาณ กิจกรรม หรือเหตุการณ์ ที่บ่งบอกถึงการเปลี่ยนแปลงของความเสี่ยงสำคัญที่ส่งผลกระทบต่อเป้าหมาย ได้โดยสามารถใช้ประโยชน์ในการบริหารความเสี่ยง เพื่อติดตามผลการบริหารความเสี่ยงว่าเป็นไปตามเป้าหมายหรือไม่ เพื่อจะได้ปรับปรุง/เปลี่ยนแปลงแผนการบริหารความเสี่ยงให้มีประสิทธิภาพมากยิ่งขึ้น และในกรณีตัวชี้วัดมีลักษณะเป็นดัชนีชี้นำ (Leading Indicator) สามารถนำไปใช้ประโยชน์ในการวางแผนการบริหารความเสี่ยงให้มีระบบเตือนล่วงหน้า (Early Warning System) ได้
Value Driver Diagram	แผนภาพแสดงปัจจัยที่ส่งผลกระทบต่อเป้าหมายทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ใช้หลักการเดียวกับ Cause-and–Effect Analysis โดย Value Driver Diagram เป็นเครื่องมือที่สำคัญในขั้นตอนการระบุปัจจัยเสี่ยง

ศัพท์เฉพาะ	คำนิยาม
Risk Factor	ปัจจัยเสี่ยงหมายถึง สิ่งที่เกิดขึ้นจากเหตุการณ์หรือรายละเอียดของเหตุการณ์ที่ทำให้ทราบว่าความเสี่ยงเกิดจากอะไร
Risk Driver	เหตุแห่งความเสี่ยง ซึ่งอาจเป็นเหตุเกิดจากปัจจัยภายในองค์กร เช่น วัฒนธรรมองค์กร โครงสร้างองค์กร บุคลากร หรือเหตุที่เกิดจากปัจจัยภายนอก เช่น การเมือง คู่แข่ง สภาวะเศรษฐกิจ เป็นต้น
Cost & Benefit Analysis	การวิเคราะห์ถึงผลประโยชน์เปรียบเทียบกับต้นทุนทั้งที่เป็นตัวเงินและไม่สามารถวัดเป็นตัวเงิน เพื่อใช้ในการตัดสินใจเลือกใช้วิธีการที่เหมาะสม โดยการตัดสินใจเลือกใช้การจัดการความเสี่ยงวิธีใดนั้นควรคำนึงถึงประโยชน์ทั้งในด้านของการลดผลกระทบหรือโอกาสเกิด โดยเปรียบเทียบกับต้นทุนหรือค่าใช้จ่ายที่เกิดจากการจัดการความเสี่ยงนั้น ๆ แล้วพิจารณาเลือกวิธีการจัดการความเสี่ยงที่ได้รับประโยชน์มากกว่าต้นทุนหรือค่าใช้จ่ายที่ต้องใช้
ความมั่นคงปลอดภัย (Security)	การจัดการป้องกันการเข้าถึง การเข้าไปแก้ไขเปลี่ยนแปลง การทำลาย การเปิดเผยข้อมูล การรักษาความลับ (Confidential) ทั้งระหว่างที่กำลังพัฒนาระบบงาน หรือในการจัดส่งข้อมูล การประมวลผล หรือการจัดเก็บรักษาข้อมูลในระบบงาน การจัดเก็บระบบงาน โดยจัดการป้องกันให้มีความเหมาะสมและความสำคัญของข้อมูลรวมถึงระบบงานด้วย
ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)	ข้อมูลที่จะส่งมอบให้กับผู้ใช้ข้อมูล (End User) เป็นข้อมูลที่มีความสมบูรณ์ ถูกต้อง ครบถ้วน ซึ่งจะทำให้การดำเนินงานและการบริหารงานขององค์กรมีประสิทธิภาพ
ความพร้อมใช้งานของระบบงานและข้อมูล (Availability)	เรื่องของการจัดส่งข้อมูลไปให้ผู้ที่ต้องการใช้ข้อมูลได้รวดเร็วทันเวลา และสามารถให้ข้อมูลได้อย่างต่อเนื่องในเวลาที่

ศัพท์เฉพาะ	คำนิยาม
	เหมาะสม เพื่อสนับสนุนการดำเนินงานขององค์กร ทั้งนี้ องค์กรต้องมีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (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 จากทุกคนในองค์กรตั้งแต่ระดับกรรมการผู้บริหารทุกระดับ และเจ้าหน้าที่ทุกคน

๗. องค์ประกอบการบริหารความเสี่ยง

การบริหารความเสี่ยง เป็นกระบวนการที่ดำเนินการอย่างต่อเนื่องภายในองค์กร และควรถูกรวมกับกิจกรรมปกติทางธุรกิจ เพื่อให้องค์กรสามารถดำเนินการตามกลยุทธ์ ที่กำหนดเพื่อให้บรรลุพันธกิจและวัตถุประสงค์ที่ต้องการ

กระบวนการ ๘ ขั้นตอนหลักประกอบด้วย

๑. สภาพแวดล้อมภายในองค์กร แนวนโยบายโดยทั่วไปของสำนักงาน ซึ่งเป็นพื้นฐานที่สำคัญของกรอบการบริหารความเสี่ยง และการจัดการกับความเสี่ยง

๒. การกำหนดวัตถุประสงค์และเป้าหมาย ที่สอดคล้องกับกลยุทธ์ สรอ.

๓. การระบุเหตุการณ์ การบ่งชี้และเข้าใจความเสี่ยงทั้งหมดที่มีผลกระทบต่อวัตถุประสงค์ที่กำหนดไว้

๔. การประเมินความเสี่ยง โดยพิจารณาถึงผลกระทบและโอกาสเกิดความเสี่ยง

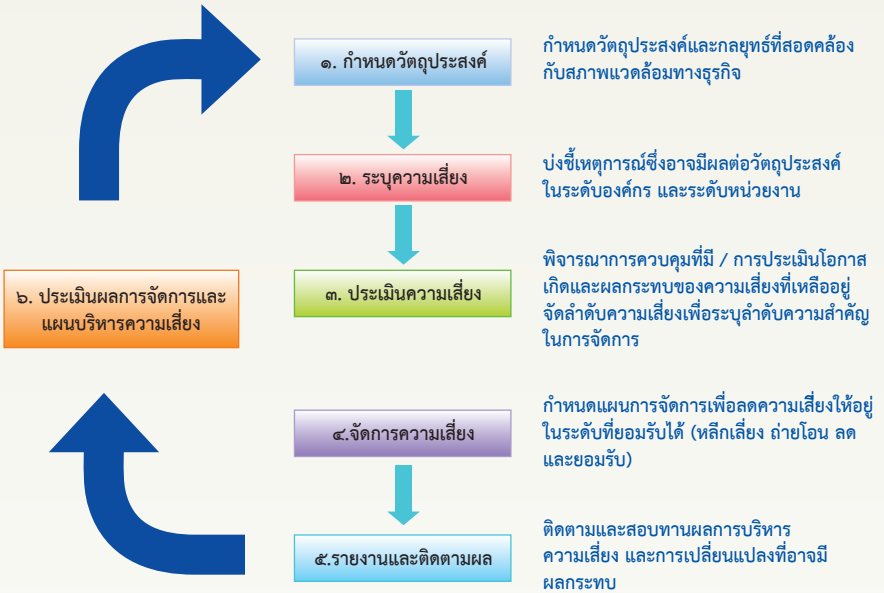
๕. การตอบสนองความเสี่ยง กำหนดการจัดการความเสี่ยงที่ปฏิบัติอยู่ในปัจจุบัน

๖. กิจกรรมการควบคุม โดยพิจารณาถึงการควบคุมเพิ่มเติมรวมทั้งความสัมพันธ์ของต้นทุนและผลประโยชน์ที่เกิดขึ้น ผู้บริหารควรนำวิธีการจัดการความเสี่ยงไปปฏิบัติและติดตามเพื่อให้มั่นใจได้ว่า มีการดำเนินการตามวิธีการที่กำหนดไว้ กิจกรรมการควบคุม คือนโยบายและขั้นตอนปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง

๗. สารสนเทศและการสื่อสาร เพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง

๘. การติดตามผลและรายงานความมีประสิทธิผลของกระบวนการและระบบการบริหารความเสี่ยง

ทั้งนี้ กระบวนการของการบริหารความเสี่ยง ๘ ขั้นตอน เพื่อการนำเอาขั้นตอนทั้ง ๘ ไปปฏิบัติ มีรายละเอียดดังนี้



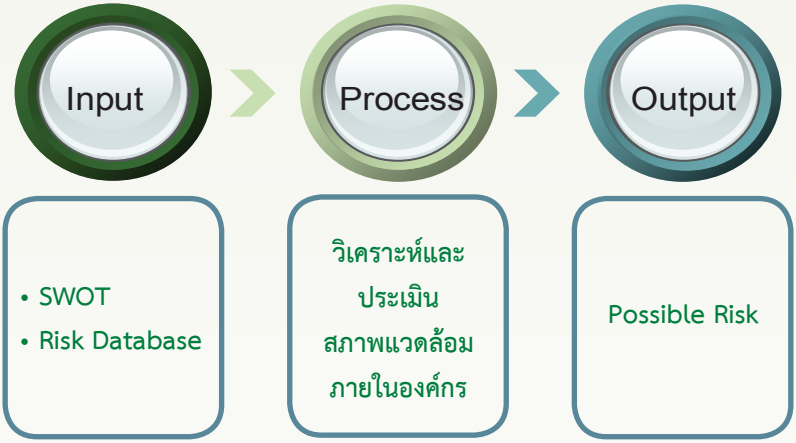
๗.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

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 ควรกำหนดให้ครอบคลุมแต่ละประเภทของวัตถุประสงค์ดังต่อไปนี้

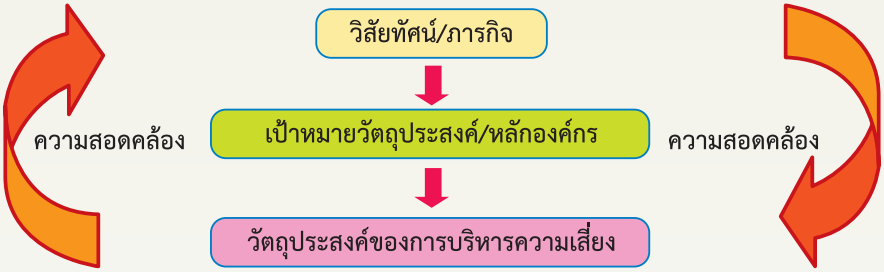
- วัตถุประสงค์ด้านกลยุทธ์ คือ วัตถุประสงค์ระดับนโยบายขององค์กร โดยสอดคล้องกับวิสัยทัศน์และพันธกิจขององค์กรโดยรวม ซึ่งมุ่งสู่การบรรลุเป้าหมายขององค์กรในภาพรวม
- วัตถุประสงค์ด้านการปฏิบัติงาน คือ วัตถุประสงค์ที่เกี่ยวข้องกับประสิทธิภาพและประสิทธิผลของการปฏิบัติงาน
- วัตถุประสงค์ด้านการเงิน คือ วัตถุประสงค์ที่เกี่ยวข้องกับการบริหารการเงินขององค์กรในทุกด้าน ได้แก่ ประสิทธิภาพในการเบิกจ่ายงบลงทุน ประสิทธิภาพในการบริหารค่าใช้จ่ายความน่าเชื่อถือและความทันเวลาของการรายงานข้อมูลทางการเงินและข้อมูลที่ไม่ใช่ทางการเงิน ทั้งจากภายในและภายนอกองค์กร
- วัตถุประสงค์ด้านกฎหมาย กฎระเบียบ คือ วัตถุประสงค์ที่เกี่ยวข้องกับการปฏิบัติตามกฎหมาย และกฎระเบียบต่าง ๆ การปฏิบัติตามกฎระเบียบเกี่ยวข้อง

ความสอดคล้องของวัตถุประสงค์

วัตถุประสงค์ต้องมีความสอดคล้องทั่วทั้งองค์กร เพื่อให้เกิดความมั่นใจว่า หน่วยงาน ผู้บริหาร และเจ้าหน้าที่ ดำเนินการเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

วิสัยทัศน์เป็นจุดเริ่มต้นในการกำหนดทิศทางขององค์กร ผู้บริหารระดับสูงจะทำการกำหนดวัตถุประสงค์ระดับองค์กรขึ้นในการจัดทำแผนประจำปี แต่ละหน่วยงานดำเนินการกำหนดวัตถุประสงค์ของหน่วยงานให้สอดคล้องกับวัตถุประสงค์ที่องค์กรได้กำหนดไว้ และการกำหนดวัตถุประสงค์ของกระบวนการและโครงการต่าง ๆ ต้องคำนึงถึงความสอดคล้องกับวัตถุประสงค์ของหน่วยงานและระดับองค์กร

วัตถุประสงค์อาจเกี่ยวข้องกับองค์การในหลาย ๆ ด้าน รวมไปถึง ทรัพยากร เทคโนโลยี สารสนเทศ 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 ขั้นตอนโดยเกี่ยวข้องกับกระบวนการในการปฏิบัติงาน อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากร ซึ่งส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินธุรกิจขององค์กร เช่น โครงการล่าช้า ขาดอุปกรณ์หรือเครื่องมือที่มีประสิทธิภาพ ขาดการติดตามการบริหารสัญญา บุคลากรขาดแรงจูงใจในการปฏิบัติงาน เป็นต้น

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

๔. ความเสี่ยงด้านกฎหมาย กฎระเบียบ (Compliance Risk) เป็นความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงาน ได้ กฎระเบียบหรือกฎหมายที่มีอยู่ไม่เหมาะสมเป็นอุปสรรคต่อการปฏิบัติงาน นโยบายและวิธีการปฏิบัติงานที่องค์กรกำหนดขึ้นไม่สามารถปฏิบัติได้ เช่น ความสับสนในการเลือก กฎระเบียบหรือกฎหมายที่จะบังคับใช้ เนื่องจากกฎระเบียบหรือกฎหมายหลายฉบับที่สามารถอ้างถึงและบังคับใช้ในกรณีหนึ่ง ๆ เป็นต้น

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

โดยได้กำหนดแนวทางการวิเคราะห์ความเสี่ยงของแผนงาน/โครงการตามหลักธรรมาภิบาลมี ๑๐ ประเภท ได้แก่

๑. ความเสี่ยงต่อหลักประสิทธิผล (Effectiveness) ต้องมีวิสัยทัศน์เชิงยุทธศาสตร์เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกฝ่ายปฏิบัติตามหน้าที่ตามพันธกิจให้บรรลุวัตถุประสงค์ขององค์กร มีการวางเป้าหมายการปฏิบัติงานที่ชัดเจน และอยู่ในระดับที่ตอบสนองต่อความคาดหวังของประชาชน สร้างกระบวนการปฏิบัติงานอย่างเป็นระบบและมีมาตรฐาน มีการจัดการความเสี่ยงและมุ่งเน้นผลการปฏิบัติงานที่เป็นเลิศ รวมถึงมีการติดตามประเมินผล และพัฒนาปรับปรุงการปฏิบัติงานให้ดีขึ้นอย่างต่อเนื่อง

๒. ความเสี่ยงต่อหลักประสิทธิภาพ (Efficiency) ในการปฏิบัติงานต้องมีการใช้ทรัพยากรอย่างประหยัด เกิดผลิตภาพ คุ้มค่าการลงทุนและบังเกิดประโยชน์สูงสุดต่อส่วนรวม รวมทั้งต้องมีการลดขั้นตอนและระยะเวลาในการปฏิบัติงานเพื่ออำนวยความสะดวกและลดภาระค่าใช้จ่าย ตลอดจนยกเลิกภารกิจที่ล้าสมัย และไม่มีความจำเป็น

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

๔. ความเสี่ยงต่อหลักความโปร่งใส (Transparency) ต้องปฏิบัติงานด้วยความซื่อสัตย์สุจริต ตรงไปตรงมา ร่วมทั้งต้องมีการเปิดเผยข้อมูลข่าวสารที่จำเป็นและเชื่อถือได้ให้ประชาชนได้รับทราบอย่างสม่ำเสมอ ตลอดจนวางระบบให้การเข้าถึงข้อมูลข่าวสารเป็นไปโดยง่าย

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

๖. ความเสี่ยงต่อหลักภาระรับผิดชอบ (Acountability) ในการปฏิบัติงานต้องสามารถตอบคำถาม และชี้แจงได้เมื่อมีข้อสงสัย รวมทั้งต้องมีการจัดวางระบบการรายงานความก้าวหน้าและผลสัมฤทธิ์ตามเป้าหมายที่กำหนดไว้ต่อสาธารณะ เพื่อประโยชน์ในการตรวจสอบและการให้คุณให้โทษ ตลอดจนมีการจัดเตรียมระบบการแก้ไขหรือบรรเทาปัญหา และผลกระทบใด ๆ ที่อาจจะเกิดขึ้น

๗. ความเสี่ยงต่อหลักนิติธรรม (Rule of Law) ต้องใช้อำนาจของกฎหมาย กฎระเบียบข้อบังคับในการปฏิบัติงานอย่างเคร่งครัด ด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของประชาชน และผู้มีส่วนได้ส่วนเสียฝ่ายต่าง ๆ

๘. ความเสี่ยงต่อหลักการกระจายอำนาจ (Decentralization) ในการปฏิบัติงานควรมีการมอบอำนาจและกระจายความรับผิดชอบในการตัดสินใจและการดำเนินการให้แก่ผู้ปฏิบัติงานในระดับต่าง ๆ ได้อย่างเหมาะสม รวมทั้งมีการโอนถ่ายบทบาท และภารกิจให้แก่องค์กรปกครองส่วนท้องถิ่น หรือภาคส่วนอื่น ๆ ในสังคม

๙. ความเสี่ยงต่อหลักความเสมอภาค (Equity) ต้องให้บริการอย่างเท่าเทียมกัน ไม่มีการแบ่งแยกด้าน ชาย/หญิง ถิ่นกำเนิด เชื้อชาติ ภาษา เพศ อายุ สภาพทางกายหรือสุขภาพ สถานะของบุคคล ฐานะทางเศรษฐกิจและสังคม ความเชื่อทางศาสนา การศึกษาอบรม และอื่น ๆ นอกจากนี้ยังต้องคำนึงถึงโอกาสความทัดเทียมกันของการเข้าถึงบริการสาธารณะของกลุ่มบุคคลผู้ด้อยโอกาสในสังคม

๑๐. ความเสี่ยงต่อหลักการมุ่งเน้นฉันทามติ (Consensus Oriented) ในการปฏิบัติงานต้องมีกระบวนการในการแสวงหาฉันทามติ หรือข้อตกลงร่วมกัน ระหว่างกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องโดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง จะต้องไม่มีข้อคัดค้านที่หาข้อยุติไม่ได้ ในประเด็นที่สำคัญ

จากแนวคิดธรรมภิบาลที่เกี่ยวข้อง สามารถแสดงความเชื่อมโยง ต่อปัจจัยในการวิเคราะห์ความเสี่ยงเช่น

- ด้านนโยบายและกลยุทธ์ โครงการที่คัดเลือกมานั้น อาจมีความเสี่ยงต่อเรื่องประสิทธิผลและการมีส่วนร่วม
- ด้านการปฏิบัติงาน 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

การประเมินความเสี่ยงควรพิจารณาถึงความไม่แน่นอนของเหตุการณ์หรือเงื่อนไขต่าง ๆ ใน ๒ ปัจจัย ดังต่อไปนี้

- ผลกระทบของความเสี่ยง
- โอกาสเกิดที่จะเกิดความเสี่ยง

ผลกระทบ (Impact)

การประเมินความเสี่ยงควรพิจารณาถึงผลกระทบทั้งทางด้านการเงิน และที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ผลกระทบสามารถวัดได้ในเชิงของการสูญเสียทางการเงินทั้งทางตรงและทางอ้อม การวัดผลการดำเนินงานที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ความพึงพอใจของผู้มีส่วนได้ส่วนเสีย สภาพแวดล้อมและสังคม เป็นต้น

การประเมินผลกระทบของปัจจัยเสี่ยง ควรครอบคลุมทั้งการกำหนดผลกระทบในเชิงการเงินและผลกระทบที่มิใช่ทางการเงิน อย่างไรก็ตาม บางปัจจัยเสี่ยงอาจไม่สามารถกำหนดผลกระทบในเชิงการเงินที่ชัดเจนได้ ดังนั้นในการประเมินความเสี่ยงเบื้องต้นจึงพิจารณาผลกระทบที่เกิดจากความเสี่ยงในเชิงคุณภาพเป็นส่วนใหญ่ โดยเมื่อพิจารณาระดับความรุนแรงของผลกระทบแล้วนั้น ความเสี่ยงที่มีผลกระทบมากหรือมีโอกาสเกิดสูง จำเป็นต้องได้รับการพิจารณาจากผู้บริหารระดับสูงมาก และทันท่วงที โดยกำหนดแผนการบริหารความเสี่ยงที่ท้าทาย และติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ

ตารางด้านล่างแสดงถึงตัวอย่างของผลกระทบที่เกิดจากความเสี่ยงในแบบต่าง ๆ

ประเภทของผลกระทบ	ตัวอย่าง
การเงิน	การลดลงหรือความล่าช้าในการบรรลุเป้าหมายทางรายได้ กำไรสุทธิ กระแสเงินสด หรือสินทรัพย์รวม
กลยุทธ์	การไม่บรรลุวัตถุประสงค์ขององค์การหรือสายงาน
ทรัพยากรบุคคล	การลาออกของเจ้าหน้าที่ การสูญเสียเจ้าหน้าที่หลักหรือปัญหาด้านจริยธรรม
ชื่อเสียง	การเผยแพร่ข่าวที่เสียหายขององค์การในสื่อต่าง ๆ เช่น หนังสือพิมพ์ โทรทัศน์ เป็นต้น
ระบบเทคโนโลยีและสารสนเทศ	ระบบเทคโนโลยีและสารสนเทศล้มเหลว หรือการละเมิดความปลอดภัยของข้อมูล องค์การ
กฎระเบียบ ข้อบังคับ	การละเมิดกฎระเบียบ
การต่อเนื่องของการดำเนินธุรกิจ	การหยุดชะงักของกระบวนการและการดำเนินการทางธุรกิจ

โอกาสเกิด (Likelihood)

การประเมินโอกาสเกิดของความเสี่ยง โดยทั่วไปการหาข้อมูลมาทำการสนับสนุนการประมาณการที่ถูกต้องเป็นไปได้ยาก ในกรณีที่สามารถหาข้อมูลที่เกี่ยวกับเหตุการณ์ความล้มเหลวหรือความถี่ที่เกิดขึ้นในอดีต ต้องมีความมั่นใจในฐานข้อมูลดังกล่าวว่าสามารถบ่งชี้ถึงความเป็นไปได้ของเหตุการณ์ในอนาคตได้

การประเมินโอกาสเกิดขึ้นอยู่กับระยะเวลาที่นำมาพิจารณา ดังนั้นแล้ว เมื่อทำการประเมินโอกาสเกิด ผู้บริหารต้องมีความชัดเจนในการกำหนดระยะเวลาที่จะใช้ในการพิจารณาโดยไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นได้ในระยะยาว

ประโยชน์ของผู้บริหารที่ได้จากการประเมินความเสี่ยงมีดังต่อไปนี้

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

จากประเด็นดังกล่าว แสดงให้เห็นถึงความสำคัญของการกำหนดระดับความเสี่ยงที่ยอมรับได้ และระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ขององค์กร ซึ่ง

ความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้ โดยธุรกิจยังคงดำเนินการได้บรรลุตามเป้าหมาย

ความเสี่ยงที่ยอมรับได้กำหนดขึ้นเพื่อใช้เป็นแนวทางกำหนดกลยุทธ์ขององค์กร ทั้งนี้ ความเสี่ยงที่ยอมรับได้ควรได้รับการกำหนดโดยผู้บริหารและอนุมัติโดยคณะกรรมการ การกำหนดความเสี่ยงที่ยอมรับได้ควรพิจารณาถึงความสมดุลระหว่างการเติบโต ความเสี่ยง และผลตอบแทนขององค์กร ในขณะเดียวกันองค์กรควรบริหารความเสี่ยงที่เกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้

ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) คือ ระดับความเบี่ยงเบนจากวัตถุประสงค์ที่ยอมรับได้

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

การจัดลำดับความเสี่ยง

ผู้บริหารระดับสูงควรกำหนดเงื่อนไขที่ใช้ในการจัดลำดับความเสี่ยง และควรมีการสอบทานการจัดลำดับความเสี่ยงเป็นประจำ เพื่อให้สอดคล้องกับเงื่อนไขทางธุรกิจที่เปลี่ยนไป ขั้นตอนในการจัดลำดับความเสี่ยงมีดังต่อไปนี้

การกำหนดระดับของผลกระทบ

- กำหนดเงื่อนไขที่จะใช้ในการพิจารณา
  - พิจารณาทั้งเงื่อนไขทางการเงินและเงื่อนไขอื่น ๆ ที่ไม่เกี่ยวข้องกับการเงิน เช่น ยอดขาย ผลตอบแทนทางการเงิน ผลกำไร ชื่อเสียง ความสามารถในการบรรลุวัตถุประสงค์ อัตราการลาออกของเจ้าหน้าที่ ความปลอดภัยในชีวิตและทรัพย์สิน และระบบเทคโนโลยีสารสนเทศ
  - ทำให้มั่นใจได้ว่าเงื่อนไขนั้นสอดคล้องกับวัตถุประสงค์ขององค์กร
- กำหนดมูลค่าของผลกระทบให้กับระดับคะแนน ๑, ๒, ๓, ๕ และ ๒๕ ในการจัดลำดับ โดยระดับคะแนนนี้อาจมีการเปลี่ยนแปลงได้ ขึ้นอยู่กับความเหมาะสมกับสถานการณ์ในขณะนั้น
- ทำให้มั่นใจว่ามูลค่าต่าง ๆ ที่กำหนดเพื่อใช้ในการจัดลำดับสำหรับเงื่อนไขที่ต่างกันมีความสอดคล้องกัน ดังตัวอย่าง ระดับผลกระทบ ๓ ของผลกระทบทางการเงินสามารถเทียบเท่ากับระดับคะแนน ๓ ของเงื่อนไขด้านสิ่งแวดล้อม เป็นต้น

การกำหนดระดับของโอกาสเกิด

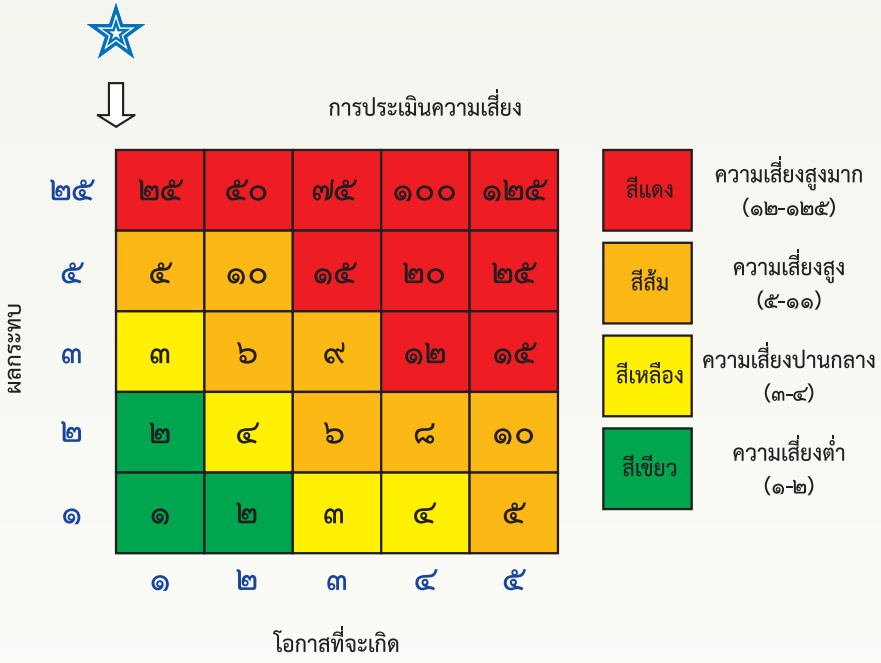
- กำหนดช่วงเวลาที่ชัดเจนสำหรับการพิจารณาโอกาสเกิด อย่างไรก็ตาม ไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นในระยะยาว

- ประยุกต์คำอธิบายในแต่ละคะแนน โดยระดับคะแนนนี้สามารถเปลี่ยนแปลงได้เช่นเดียวกับระดับคะแนนของผลกระทบ ขึ้นอยู่กับความเหมาะสมกับสถานการณ์ในขณะนั้น

แนวทางการพิจารณาความมีนัยสำคัญของความเสี่ยง

การประเมินความเสี่ยง สามารถทำได้โดยการอ้างอิงกับตารางแสดงการจัดลำดับความเสี่ยง การพิจารณาว่าความเสี่ยงใดมีนัยสำคัญ ที่ต้องนำมาดำเนินการก่อนหลัง โดยทั่วไปอาจใช้การกำหนดค่าลำดับความเสี่ยงทั้งในด้านของผลกระทบและโอกาสเกิด ทั้งนี้ การกำหนด

นัยสำคัญของความเสี่ยงขององค์กร ควรได้รับการพิจารณาจากผู้บริหารระดับสูงและผ่านความเห็นชอบจากคณะกรรมการบริหารความเสี่ยงองค์กร หลังจากการประเมินความมีนัยสำคัญของความเสี่ยงเพื่อนำมาใช้ในการกำหนดกลยุทธ์การจัดการความเสี่ยงต่าง ๆ ควรคำนึงถึงประสิทธิผลของต้นทุนที่ต้องใช้ในการจัดการความเสี่ยงนั้น ๆ กับระดับความสำคัญของความเสี่ยงที่ลดลงว่าเหมาะสมเพียงใด ทั้งนี้ความมีประสิทธิผลของการจัดการความเสี่ยงอาจประเมินได้ในเชิงของการลดลงของโอกาสเกิดและผลกระทบ



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

๗.๕ การตอบสนองความเสี่ยง (Risk Response)

เป็นการระบุว่ามีทางเลือกใดบ้างที่สามารถใช้ในการจัดการความเสี่ยง มีความเหมาะสมและนำไปปฏิบัติเป็นส่วนหนึ่งของการบริหารความเสี่ยงของสำนักงาน ซึ่งจะต้องประเมินผลกระทบที่มีต่อโอกาสที่จะเกิดรวมทั้งต้นทุนและประโยชน์ที่ได้รับ เพื่อให้ความเสี่ยงที่เหลืออยู่ภายในช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ ทั้งนี้การตอบสนองต่อความเสี่ยงแบ่งเป็น ๔ ประการ คือ การยอมรับ (Accept) การลด (Reduce) การหลีกเลี่ยง/ยกเลิก (Avoid/Terminate) และการโอนความเสี่ยง (Transfer)

สำนักงานต้องจัดให้มีการควบคุมความเสี่ยงและเพดานความเสี่ยงที่เพียงพอและเหมาะสมตามแต่ละประเภทความเสี่ยงและต้องอยู่ภายใต้ระดับความเสี่ยงที่สำนักงานยอมรับได้ รวมทั้งสอดคล้องกับมาตรฐานและหลักเกณฑ์ของหน่วยงานกำกับดูแล แนวทางปฏิบัติที่ดี ตลอดจนนโยบายบริหารความเสี่ยงกับทิศทางและกลยุทธ์การดำเนินงานของสำนักงานพร้อมทั้งกำหนดกระบวนการปฏิบัติตามการควบคุมความเสี่ยงและเพดานความเสี่ยงที่กำหนดไว้ แนวทางการอนุมัติข้อยกเว้นกรณีจำเป็นหรือเหตุการณ์ไม่ปกติต่าง ๆ รวมถึงการทบทวนการควบคุมความเสี่ยงและเพดานความเสี่ยงดังกล่าวเป็นระยะ เพื่อให้มีประสิทธิภาพในการควบคุมและป้องกันความเสี่ยงให้กับสำนักงาน

ผู้บริหารต้องประเมินว่าปัจจุบันการจัดการความเสี่ยงเพียงพอหรือไม่ ทั้งประสิทธิภาพในการลดโอกาสเกิดความเสี่ยง และผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงต่าง ๆ หากไม่มีการจัดการความเสี่ยง หรือการจัดการในปัจจุบันไม่เพียงพอ ควรมีการพิจารณากิจกรรมอื่น ๆ เพิ่มเติมให้เหมาะสมและนำไปปฏิบัติ

วัตถุประสงค์ของการจัดการความเสี่ยง

- ลดโอกาสในการเกิดและผลกระทบของความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้ โดยการจัดการสาเหตุของความเสี่ยงอย่างมีประสิทธิภาพ หรือโดยการจัดการผลกระทบที่อาจจะเกิดขึ้นของความเสี่ยง เช่น การมีเจ้าหน้าที่ปฏิบัติการที่พร้อมซ่อมแซมความเสียหายที่เกิดขึ้น เป็นต้น
- การลดผลกระทบของความเสี่ยง ซึ่งโดยมากมักใช้ระบบการเตือนภัย หรือระบบการบริหาร พร้อมด้วยการจัดทำแผนฉุกเฉิน หรือแผนฟื้นฟู
- การเพิ่มโอกาสในการเกิด หรือผลกระทบจากความเสี่ยงที่เป็นโอกาสให้มากที่สุด โดยการปฏิบัติเพื่อสร้างหรือหาโอกาส หรือการจัดการเพื่อให้ได้ผลลัพธ์ที่ดีขึ้น

กลยุทธ์ในการบริหารความเสี่ยง

การยอมรับความเสี่ยง (Accept) ความเสี่ยงหลังการควบคุมอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใด ๆ 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 (Transfer) การโอนย้าย หรือการแบ่งความเสี่ยงบางส่วนกับบุคคลหรือองค์การอื่น

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

แนวทางในการกำหนดกลยุทธ์การจัดการความเสี่ยง

กลยุทธ์การจัดการความเสี่ยงถูกกำหนดขึ้นเพื่อลดระดับของความเสี่ยง ทั้งผลกระทบและโอกาสเกิดให้เป็นไปตามระดับความเสี่ยงที่ยอมรับได้ ในบางกรณีการรวมกลยุทธ์การจัดการความเสี่ยง อาจทำให้เกิดผลที่มีประสิทธิภาพมากขึ้นทั้งทางด้านต้นทุนและการปฏิบัติงาน ดังนั้น ควรต้องมีการพิจารณาการจัดการความเสี่ยงต่าง ๆ ที่อาจมีความเกี่ยวข้องกัน และอาจดำเนินการโดยหลายหน่วยงาน รวมทั้งคำนึงถึงต้นทุนที่อาจเกิดขึ้น ในการจัดให้มีการจัดการความเสี่ยงสำหรับกำหนดเป็นกลยุทธ์ในการจัดการความเสี่ยงโดยรวมเพื่อให้เกิดการจัดการความเสี่ยงอย่างเป็นบูรณาการ

ผู้บริหารอาจทำการพิจารณาปัจจัยในการกำหนดกลยุทธ์การจัดการความเสี่ยง ต่อไปนี้

- การประเมินผลกระทบและโอกาสเกิดจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง

ในการประเมินทางเลือกของแต่ละกลยุทธ์การจัดการความเสี่ยง ผู้บริหารต้องมีความเข้าใจว่ากิจกรรมการจัดการความเสี่ยงอาจส่งผลต่อผลกระทบและโอกาสเกิดของความเสี่ยงต่างกัน ดังนั้นแล้ว การประเมินผลกระทบและโอกาสเกิดของความเสี่ยงที่อาจเปลี่ยนแปลงจากการดำเนินการตามกิจกรรมการจัดการความเสี่ยง จึงควรพิจารณาก่อนการตัดสินใจเลือกกลยุทธ์ เพื่อให้ระดับความเสี่ยงสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ขององค์กร

ทั้งนี้ การประเมินผลกระทบและโอกาสเกิดหลังจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง สามารถอ้างอิงข้อมูลได้จากเหตุการณ์ในอดีต แนวโน้มของเหตุการณ์ที่อาจเกิดขึ้น และวิเคราะห์การเปลี่ยนแปลงที่อาจเกิดขึ้นในอนาคต ความเสี่ยงสามารถถูกระบุได้ทั้งอันตรายหรือโอกาสที่อาจเกิดขึ้น การกำหนดกลยุทธ์การจัดการความเสี่ยงจึงสามารถทำได้จากการประเมินปัจจัยหลัก ๒ ประการ ดังนี้

๑. ประเมินต้นทุนและผลตอบแทนของการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง

เนื่องจากทรัพยากรองค์กรมีจำกัด จึงมีความจำเป็นต้องประเมินต้นทุนและผลตอบแทนที่เกิดขึ้น หากมีการดำเนินการตามกิจกรรมการจัดการความเสี่ยง ในกรณีที่พบว่าผลตอบแทนที่ได้จากการดำเนินการที่ได้ไม่คุ้มกับต้นทุนส่วนเพิ่ม ผู้บริหารอาจพิจารณาถึงแนวทางในการโอนย้ายความเสี่ยง (Transfer) เพื่อทำการแบ่งต้นทุนให้หน่วยงานภายนอกรับผิดชอบ เช่น การทำประกันภัย หรือการร่วมทุน เป็นต้น

๒. การประเมินความเป็นไปได้ที่จะประสบผลสำเร็จในการจัดการความเสี่ยง

เนื่องจากกิจกรรมการจัดการความเสี่ยงที่องค์กรจะกำหนดขึ้นนั้น ต้องประกอบด้วยปัจจัยหลายประเภทที่สนับสนุนให้การดำเนินการประสบความสำเร็จ ดังนั้น การประเมินความเป็นไปได้ที่กิจกรรมการจัดการความเสี่ยงจะประสบความสำเร็จจึงมีความจำเป็น โดยควรพิจารณาถึงปัจจัยต่าง ๆ เช่น ความรู้ความเข้าใจของบุคลากร งบประมาณที่ใช้ในการจัดการ ระยะเวลาแล้วเสร็จ เป็นต้น หากพิจารณาแล้วพบว่ากิจกรรมดังกล่าวมีแนวโน้มที่จะไม่ประสบความสำเร็จ ควรพิจารณาถึงกลยุทธ์การจัดการความเสี่ยงด้วยวิธีการอื่นเพื่อใช้เป็นทางเลือกหรือปรับปรุงแผนการจัดการความเสี่ยงที่มีอยู่ให้เหมาะสมยิ่งขึ้น

หลังจากได้ทำการประเมินเพื่อกำหนดกลยุทธ์การจัดการความเสี่ยงที่มีประสิทธิผลจากแนวทางที่ได้กล่าวมาแล้วข้างต้น ผู้บริหารต้องทำการกำหนดแผนการปฏิบัติงาน (Implementation Plan) หรือขั้นตอนในการปฏิบัติ (Procedure) โดยต้องระบุระยะเวลาแล้วเสร็จเพื่อให้มั่นใจได้ว่าจะมีการดำเนินงานตามกลยุทธ์เพื่อให้เกิดโอกาสตามที่คาดหวังไว้จริง และได้รับการดำเนินการโดยเจ้าของความเสี่ยง

- ความรับผิดชอบในการบริหารความเสี่ยง หรือ “การเป็นเจ้าของความเสี่ยง” (Risk Owner) คือ หน่วยงาน หรือบุคคลที่รับผิดชอบให้การดำเนินการจัดการความเสี่ยงบรรลุวัตถุประสงค์หรือประสบความสำเร็จ โดยทั่วไปเจ้าของความเสี่ยง

จะต้องรับผิดชอบในการตัดสินใจ เกี่ยวกับแผนการบริหารความเสี่ยง และแผนการปรับปรุงที่เหมาะสมสำหรับความเสี่ยงที่ไม่สามารถยอมรับได้ เมื่อแผนได้ถูกอนุมัติและเห็นชอบแล้วเจ้าของความเสี่ยงจะต้องรับผิดชอบต่อการนำแผนไปปฏิบัติและติดตามผลการดำเนินงานของแผนนั้น และต้องแสดงให้ผู้บริหารเห็นความสำเร็จในการทำหน้าที่ของตนเกี่ยวกับการบริหารความเสี่ยง

- การพัฒนาการจัดการความเสี่ยงสำหรับความเสี่ยงที่ซับซ้อนอาจเกี่ยวข้องกับผู้บริหารระดับสูงและเจ้าหน้าที่ของหลายหน่วยงาน ดังนั้น การสื่อสารที่ดีจึงเป็นสิ่งจำเป็นเพื่อให้แน่ใจว่าบุคคลที่เกี่ยวข้องภายในองค์กรได้ตระหนักถึงสิ่งที่กำลังดำเนินการและบทบาทที่ต้องเกี่ยวข้องหรือปฏิบัติ

๗.๖ กิจกรรมการควบคุม (Control Activities)

เมื่อมีการเลือกวิธีในการตอบสนองความเสี่ยงที่เหมาะสมแล้วกิจกรรมการควบคุมความเสี่ยงจะถูกกำหนดขึ้นเพื่อให้มั่นใจได้ว่ามีการจัดการความเสี่ยงอย่างเหมาะสมซึ่งกิจกรรมการควบคุมเป็นกิจกรรมที่มีอยู่ในทุกหน้าที่ และทุกระดับของการปฏิบัติงานของ สรอ. ซึ่งในการปฏิบัติงานทุกด้านนั้นต้องจัดให้มีกิจกรรมการควบคุมที่เหมาะสมเพียงพอกับระดับความเสี่ยงต่อความผิดพลาดหรือความเสียหายที่อาจเกิดขึ้น ทั้งนี้ ประเภทของการควบคุมสามารถจัดกลุ่มได้ดังนี้

การควบคุมแบบป้องกัน (Preventive control) เป็นการควบคุมแบบป้องกันหรือลดความเสี่ยงจากความผิดพลาดความเสียหาย เช่น การแบ่งแยกหน้าที่การติดอุปกรณ์เพื่อป้องกันเหตุ

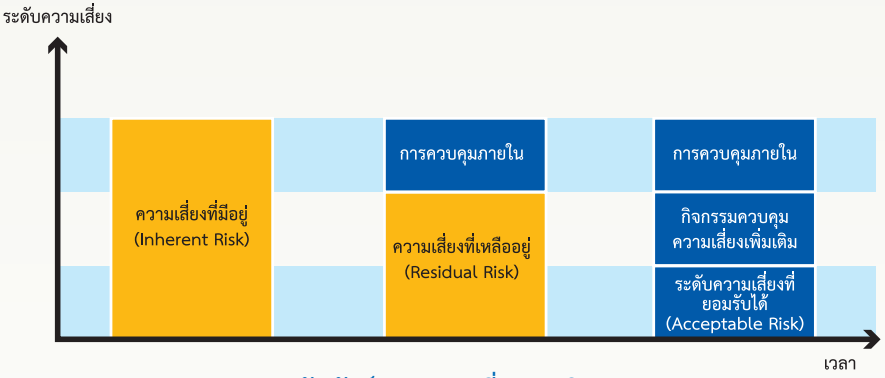
การควบคุมแบบค้นหา (Detective control) เป็นการควบคุมเพื่อค้นหาความผิดพลาดหรือความเสียหายที่เกิดขึ้นแล้ว เช่น การตรวจนับการสอบทานงาน

การควบคุมแบบแก้ไข (Corrective control) เป็นวิธีควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เคยเกิดขึ้นแล้วให้ถูกต้องหรือไม่ให้เกิดซ้ำในอนาคต เช่น แผนจูงใจลูกค้าไม่ให้ยกเลิกบริการแผนรองรับกรณีเกิดเหตุสุดวิสัย/ภัยพิบัติหรือการจัดหาระบบคอมพิวเตอร์สำรอง

การควบคุมแบบส่งเสริม (Directive control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การประกวดหรือให้รางวัลแก่ผู้ที่มีผลงานดี

ดังนั้น กิจกรรมการควบคุมจึงเป็นวิธีการต่าง ๆ ที่นำมาใช้ในการปฏิบัติงานเพื่อให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผลโดยอาจกำหนดเป็นมาตรการหรือขั้นตอนต่าง ๆ เป็นแผนปฏิบัติการ จัดการความเสี่ยงโดยแผนดังกล่าวต้องได้รับความเห็นชอบจากผู้บริหารในระดับที่เกี่ยวข้องเพื่อให้การสนับสนุนทรัพยากรที่จำเป็นตามที่กำหนดไว้ในแผน เช่น บุคลากรงบประมาณ เป็นต้น ซึ่งจะประกอบด้วย

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



ตารางแสดงความสัมพันธ์ของความเสี่ยงและกิจกรรมการควบคุม

การเลือกกิจกรรมการควบคุมควรมีการพิจารณาความเกี่ยวข้องเหมาะสมของกิจกรรมควบคุมที่มีต่อการตอบสนองความเสี่ยงและการนำมาใช้เพื่อให้บรรลุวัตถุประสงค์เป็นสำคัญ ไม่ใช่เพื่อให้เห็นว่าต้องมีกิจกรรมการควบคุมเท่านั้นกิจกรรมการควบคุมบางอย่างที่กำหนดอาจช่วยให้องค์กรบรรลุวัตถุประสงค์มากกว่าหนึ่งวัตถุประสงค์

๗.๗ สารสนเทศและการสื่อสาร (Information and Communication)

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

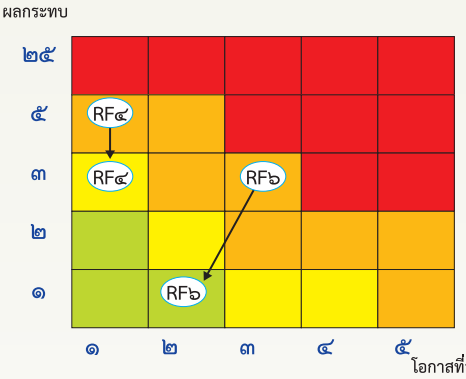
สารสนเทศที่ใช้ในการปฏิบัติงาน ได้มาจากแหล่งภายในและภายนอก ทั้งในรูปแบบเชิงปริมาณ และคุณภาพ ทั้งที่เป็นสารสนเทศทางการเงิน และที่มิใช่การเงิน ที่มีความเกี่ยวข้องกับวัตถุประสงค์ขององค์กรหลาย ๆ ประเภท

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 ทั้งก่อนและหลังบริหารปัจจัยเสี่ยงนั้น ๆ โดยใช้แผนภูมิความเสี่ยง (Risk Profile) ในการอธิบาย



การจัดทำผลการบริหารความเสี่ยง ควรรายงานระดับความรุนแรงในแต่ละปัจจัยเสี่ยง โดยครอบคลุมทั้ง ๔ ปัจจัย ดังนี้

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

ทุกระดับที่ลดลงไม่ว่าจะเป็นโอกาสหรือผลกระทบก็ตาม องค์กรควรแสดงผลการวิเคราะห์อย่างชัดเจนเปรียบเทียบกับเกณฑ์ที่กำหนด

ผลการบริหารความเสี่ยง : ปัจจัยเสี่ยง A

ความรุนแรงก่อนการบริหารความเสี่ยง	
โอกาส	ผลกระทบ

เป้าหมายที่คาดหวัง	
โอกาส	ผลกระทบ

ความรุนแรงหลังการบริหารความเสี่ยง	
โอกาส	ผลกระทบ

ความรุนแรงที่องค์กรยอมรับได้	
โอกาส	ผลกระทบ

ทั้งนี้ องค์กรจะต้องมีการสื่อสารเพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง นอกจากนี้ควรมีการประเมินประสิทธิภาพ และประสิทธิผลของการสื่อสารเป็นระยะ ๆ เพื่อให้การสื่อสารเป็นส่วนหนึ่งของการควบคุมภายใน ที่เป็นประโยชน์สูงสุดต่อองค์กร

๗.๘ การติดตามและประเมินผล (Monitoring)

การติดตามและการรายงานผลเป็นกิจกรรมที่ใช้เพื่อติดตามและสอบทานแผนการจัดการความเสี่ยงเพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงมีประสิทธิภาพและเหมาะสมหรือควรปรับเปลี่ยนหากแผนนั้นไม่มีประสิทธิภาพเพียงพอโดยกำหนดข้อมูลที่ต้องติดตามและความถี่ในการสอบทานและควรกำหนดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ ๒ ครั้ง เพื่อประเมินว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้วหรือมีความเสี่ยงใหม่เพิ่มขึ้น

การติดตามผลโดยทั่วไปมักจะดำเนินการโดยผู้บริหารและบุคลากรภายในองค์กรเอง อย่างไรก็ตามอาจให้บุคคลภายนอก เช่น ที่ปรึกษาหรือผู้เชี่ยวชาญอิสระช่วยในการติดตามการจัดการความเสี่ยงเป็นครั้งคราวได้ความเสี่ยงและการจัดการต่อความเสี่ยงอาจมีการเปลี่ยนแปลงตลอดเวลาการจัดการต่อความเสี่ยงที่เคยมีประสิทธิผลอาจเปลี่ยนเป็นกิจกรรมที่ไม่เหมาะสมกิจกรรมการควบคุมอาจมีประสิทธิผลน้อยลงหรือไม่ควรดำเนินการต่อไปหรืออาจมีการเปลี่ยนแปลงในวัตถุประสงค์หรือกระบวนการต่าง ๆ ดังนั้นแล้วผู้บริหารควรประเมินกระบวนการบริหารความเสี่ยงเป็นประจำเพื่อให้มั่นใจว่าการบริหารความเสี่ยงมีประสิทธิผลเสมอ

ลักษณะหลักของการติดตามความเสี่ยง คือ

- การประเมินควรมีประสิทธิผลและความต่อเนื่องของกิจกรรมการควบคุมและกิจกรรมอื่นที่ใช้จัดการความเสี่ยง
- การกำหนดระดับความเสี่ยงที่ยอมรับได้ที่เหมาะสมและสอดคล้องกับกลยุทธ์ทางธุรกิจ
- การรวบรวมและบันทึกข้อมูลอย่างครบถ้วนถูกต้องทันเวลา
- การติดต่อสื่อสารเกี่ยวกับความเสี่ยงและกระบวนการต่าง ๆ อย่างสม่ำเสมอและเปิดเผยทั้งแบบเป็นทางการและไม่เป็นทางการ

แนวทางการรายงานผลการดำเนินงาน มีดังนี้

๘.๑ คณะอนุกรรมการด้านการบริหารความเสี่ยง

๘.๑.๑ รายงานต่อคณะกรรมการบริหาร สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

- รายงานแผนการบริหารความเสี่ยงประจำปีรวมทั้งแผนปฏิบัติการเพื่อการจัดการความเสี่ยงปีละ ๑ ครั้ง
- รายงานผลการดำเนินการและความคืบหน้าการจัดการความเสี่ยงที่สำคัญระดับองค์กร ต่อคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) อย่างน้อยไตรมาสละ ๑ ครั้ง

๘.๑.๒ รายงานต่อคณะกรรมการตรวจสอบ

- รายงานผลการดำเนินงานอย่างน้อยปีละ ๑ ครั้ง

๘.๒ ผู้จัดการความเสี่ยงและการควบคุมภายใน (ของแต่ละฝ่าย)

- รายงานต่อ คณะอนุกรรมด้านการบริหารความเสี่ยง / ผู้อำนวยการ สรอ. / รองผู้อำนวยการ สรอ. / ฝ่ายที่เกี่ยวข้อง
- รายงานความเสี่ยงระดับองค์กรในส่วนที่รับผิดชอบและแผนปฏิบัติการการจัดการความเสี่ยงตลอดจนความคืบหน้าในการจัดการความเสี่ยงตามแผนพร้อมทั้งปัญหาและอุปสรรค เดือนละ ๑ ครั้ง

๘.๓ ส่วนบริหารความเสี่ยง

๘.๓.๑ รายงานต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

- รายงานความเสี่ยงที่สำคัญระดับองค์กรรวมทั้งรายละเอียดการจัดการความเสี่ยงตลอดจนความคืบหน้าของแผนปฏิบัติการและประเด็นสำคัญเพื่อการพิจารณาของคณะอนุกรรมการด้านการความเสี่ยง ทุกครั้งที่มีการประชุมคณะอนุกรรมการด้านการความเสี่ยง

- รายงานเหตุการณ์ที่เกิดขึ้นใหม่ทั้งที่เป็นโอกาสและความเสี่ยงที่มีผลต่อสำนักงานจากสภาพแวดล้อมที่เปลี่ยนแปลงไปเป็นการเฉพาะกิจ
- รายงานกรณีฉุกเฉินภายใน ๓ วันทำการในการประชุมเป็นกรณีพิเศษเมื่อดัชนีชี้วัดความเสี่ยงมีการเปลี่ยนแปลงและอาจมีผลกระทบอย่างรุนแรงต่อการบรรลุวัตถุประสงค์และเป้าหมายขององค์กร

สรอ. ต้องสนับสนุนให้เกิดการสื่อสารในเชิงรุกและให้มีการสื่อสารอย่างสม่ำเสมอ ช่องทางในการสื่อสารอย่างเป็นทางการที่ใช้ในการพิจารณาความเสี่ยง การควบคุม และแผนการดำเนินการ ได้แก่ การประชุมทั่วไปผู้บริหาร การประชุมคณะทำงาน รายงานประจำเดือนสำหรับผู้บริหาร การประชุมคณะกรรมการบริหารความเสี่ยง เป็นต้น การสื่อสารอย่างต่อเนื่องจะช่วยให้มีข้อมูลความเสี่ยงที่เพียงพอและได้รับการนำเสนอเพื่อใช้ในการตัดสินใจอย่างทันท่วงที ในบางกรณีการจัดการกับความเสี่ยงด้วยวิธีการที่เร่งด่วน จากการพูดคุยทางโทรศัพท์เกิดขึ้น อาจมีความเหมาะสมกว่ารอการจัดทำรายงานอย่างเป็นทางการผู้ที่เกี่ยวข้องต้องรายงานความเสี่ยงที่มีระดับความเสี่ยงสูง ให้แก่ผู้บังคับบัญชาทราบอย่างสม่ำเสมอและทันท่วงที พร้อมทั้งอธิบายวิธีการจัดการความเสี่ยงเหล่านั้น นอกจากนี้ ผู้บริหารในแต่ละหน่วยงานควรพิจารณาและนำเสนอความเสี่ยงที่มีระดับความเสี่ยงสูงของหน่วยงาน หรือความเสี่ยงที่ควรจะต้องได้รับการจัดการในระดับที่สูงกว่าขึ้นไปยังผู้บริหารในสายบังคับบัญชาเพื่อทำการพิจารณาความเสี่ยง และหาแนวทางการจัดการความเสี่ยงในระดับงานที่สูงขึ้นต่อไป

๘. Governance Risk management & Compliance (GRC)

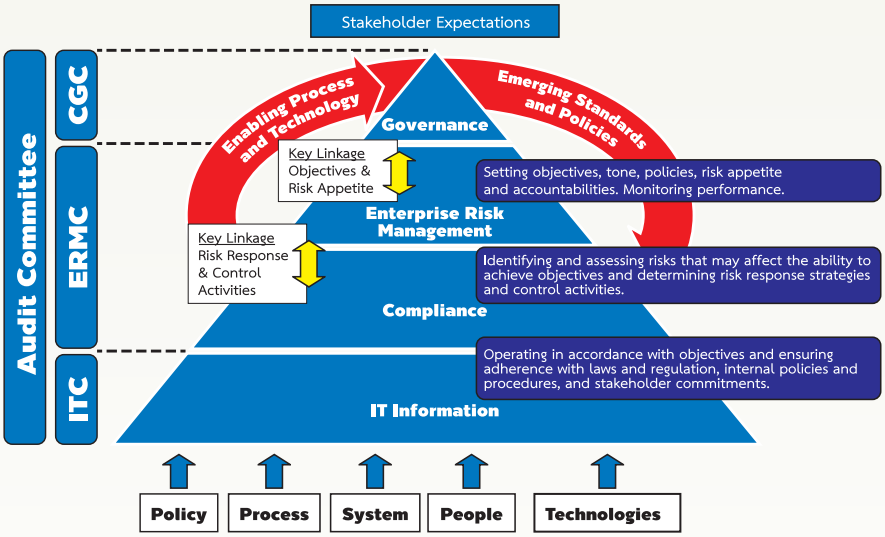
GRC คือ แนวคิดในการเชื่อมโยงและบูรณาการนิยามของสามองค์ประกอบ ได้แก่

Governance หมายถึง นโยบาย วัฒนธรรมองค์กร กระบวนการขั้นตอนการปฏิบัติงานที่ถูกกำหนดออกมาอย่างชัดเจนในการบริหารจัดการและกำกับดูแลองค์กรโดยผู้บริหารระดับสูงเพื่อการบริหารองค์กรที่โปร่งใส ซึ่งรวมถึงความสัมพันธ์และบทบาทของทุกคนในองค์กร ตลอดจนกำหนดเป้าหมายหลักที่เน้นเรื่องความโปร่งใสในการบริหารจัดการของผู้บริหารระดับสูงในองค์กร

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

Compliance หมายถึง การดำเนินงานกำกับให้มั่นใจว่า การปฏิบัติการทุกอย่างอยู่ภายใต้กฎเกณฑ์อย่างเหมาะสม ไม่เกิดการฝ่าฝืนใด ๆ เกิดขึ้น โดยกฎเกณฑ์ที่ว่านี้รวมทั้งระเบียบ ข้อบังคับ กฎหมาย คำสั่งภายในองค์กร พันธะที่ผูกพันไว้กับผู้มีส่วนได้เสีย คู่สัญญาทุกภาคส่วน ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความปลอดภัยขององค์กรอย่างถูกต้องตามมาตรฐาน การปฏิบัติตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์ เป็นต้น การดำเนินงานในส่วนของการปรับปรุงประสิทธิภาพและประสิทธิผลในการกำกับการปฏิบัติตามกฎเกณฑ์ ในลักษณะที่ติดตามเฝ้าระวังการเปลี่ยนแปลงในด้านกฎเกณฑ์และระเบียบเพื่อทำความเข้าใจ การศึกษาผลกระทบของกฎเกณฑ์ภายนอกต่อการดำเนินงานภายในและความจำเป็นในการปรับนโยบาย ระเบียบ ประกาศ กระบวนการปฏิบัติงานและสื่อสารเพื่อมิให้เกิดการฝ่าฝืน ซึ่งถือเป็นส่วนหนึ่งของการกำกับดูแลที่ดี

การพัฒนาแนวคิดจากการบริหารแบบ Silo มาเป็นกรอบแนวคิดที่บูรณาการ GRC เข้าด้วยกัน โดยแนวคิด GRC นั้นไม่ได้เป็นการพยายามที่จะรวบเอางาน ๓ ด้าน มาไว้ที่ศูนย์กลางเพียงจุดเดียว หากแต่ต้องการที่จะนำองค์ประกอบทั้ง ๓ มาปฏิบัติร่วมกันในรูปแบบของการทำงานเป็นทีม เป็นการแสวงหาแนวทาง การเชื่อมโยงบูรณาการงาน ๓ ด้านเข้าด้วยกัน ในเชิงนโยบาย กระบวนการดำเนินงาน ขั้นตอนการปฏิบัติและระบบการควบคุม แบ่งปันข้อมูลซึ่งกันและกัน มีการเปิดกว้างทางความคิดที่จะปรับปรุงองค์กรจากข้อมูลและแนวทางจากผู้บริหารของหลาย ๆ ฝ่าย โดยต้องได้รับการสนับสนุนจากองค์ประกอบพื้นฐานหลัก ๕ ประการขององค์กร ได้แก่ กลยุทธ์ กระบวนการ ระบบ บุคลากร เทคโนโลยี ดังรูปความสัมพันธ์และความเชื่อมโยงตามภาพ ตัวอย่าง เช่น



- การรณรงค์ปลูกฝัง ปรับเปลี่ยนวัฒนธรรมขององค์กร เพื่อนำบุคคลภายในองค์กรไปสู่วัตถุประสงค์และเป้าหมายด้านวัฒนธรรมองค์กรที่คาดหวังเพื่อเพิ่มประสิทธิภาพ สนับสนุนหรือผลักดันให้การดำเนินงานขององค์กรบรรลุตามวัตถุประสงค์ได้ดีขึ้น ทั้งยังทำให้เกิดผลลัพธ์เชิงวัฒนธรรมองค์กรที่พึงประสงค์ด้วย

- กลยุทธ์/กระบวนการ/ระบบ การส่งเสริมให้คณะกรรมการสามารถกำกับดูแลองค์กรและให้คำแนะนำแก่ผู้บริหารเพื่อดำเนินงานให้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องได้อย่างมั่นใจ โดยผู้บริหารต้องจัดให้มีการบริหารความเสี่ยงที่เป็นระบบมุ่งเน้นความเสี่ยงที่ตรงประเด็น และสามารถจัดกระบวนการทำงานเพื่อให้มีการปฏิบัติตามระเบียบหรือการควบคุมภายในได้อย่างเหมาะสม ภายใต้ต้นทุนการดำเนินงานที่สมเหตุสมผล รวมถึงการนำเทคโนโลยีมาสนับสนุนการทำงานให้มีประสิทธิภาพ และการสื่อสารข้อมูลอย่างถูกต้องเหมาะสมทันเวลาต่อผู้เกี่ยวข้องทุกระดับ
- การที่บุคลากรมีความมุ่งมั่น ยึดถือและส่งเสริมวัฒนธรรมของการดำเนินธุรกิจอย่างมีศักดิ์ศรีและคุณค่าทางจริยธรรม รับผิดชอบในผลงานของตน มีมุมมองที่เป็นหนึ่งเดียวกับองค์กรและต่อต้านการทำกิจกรรมที่ต่างคนต่างทำตามอำนาจหน้าที่เฉพาะตัว เน้นการทำงานเป็นทีมโดยคำนึงถึงประโยชน์ขององค์กรเป็นหลัก
- การควบคุมภายในที่เพียงพอในการลดความเสี่ยงของบุคคล ช่วยกำกับคนมากขึ้น เช่น การกำกับติดตาม (Monitoring) การใช้ระบบควบคุมการตรวจสอบคุณภาพงานและการทดสอบผลงานว่าใช้งานได้จริงอย่างสม่ำเสมอและมีประสิทธิผล หรือกระบวนการฝึกอบรมบุคลากร เพื่อให้เหมาะสมกับความรับผิดชอบในภารกิจการกำหนดให้มีมาตรฐานการทำงานที่ชัดเจน
- การใช้เทคโนโลยี หรือ ไอทีภิบาล (IT Governance) มาช่วยในการกำกับดูแลที่ดีด้วยการนำ IT มาทำหน้าที่เป็นระบบเฝ้าระวัง เป็นเครื่องเตือนภัยล่วงหน้า เป็นระบบอัตโนมัติที่กำกับการปฏิบัติในลักษณะที่ฝ่าฝืนกฎเกณฑ์ หรือเป็นระบบรายงานความผิดปกติ
- การประสานงานและเชื่อมโยงเครื่องมือ ระบบงาน และคนโดย GRC จะช่วยทำให้องค์กรเกิดความสามารถในการแข่งขันในระยะยาว เพิ่มความโปร่งใสในการเปิดเผยข้อมูล เสริมภาพลักษณ์ที่ดีให้กับองค์กร ตลอดจนคณะผู้บริหารระดับสูง รวมทั้งการสร้างจิตสำนึกในการปฏิบัติงานที่ดีให้กับเจ้าหน้าที่ทุกคน ส่งผลให้ลูกค้าเกิดความเชื่อถือและความมั่นใจในการใช้บริการต่าง ๆ ขององค์กร

๙. ปัจจัยสำเร็จในการบริหารความเสี่ยงขององค์กร

การบริหารความเสี่ยงที่ประสบความสำเร็จต้องมีปัจจัยสำคัญ ซึ่งประกอบทั้งด้านทรัพยากรและโครงสร้างพื้นฐานที่จำเป็นเพื่อให้เกิดการบริหารความเสี่ยงที่ประสบผลสำเร็จและยั่งยืน ดังนี้

๑. ความมุ่งมั่นของผู้บริหารในการจัดให้มีระบบการบริหารความเสี่ยง

การปฏิบัติตามกรอบการบริหารความเสี่ยงขององค์กร จะประสบความสำเร็จเพียงใดขึ้นอยู่กับเจตนารมย์ การสนับสนุน การมีส่วนร่วม และความเป็นผู้นำของผู้บริหารระดับสูงในองค์กร คณะกรรมการและผู้บริหารระดับสูงต้องให้ความสำคัญและสนับสนุนให้ทุกคนในองค์กรเข้าใจความสำคัญในคุณค่าของการบริหารความเสี่ยงต่อองค์กร มิฉะนั้นแล้วการบริหารความเสี่ยงไม่สามารถเกิดขึ้นได้ การบริหารความเสี่ยงต้องเริ่มต้นจากผู้นำสูงสุดขององค์กรต้องการให้เกิดระบบขึ้น โดยกำหนดนโยบายให้มีการปฏิบัติ รวมถึงการกำหนดให้ผู้บริหารต้องใช้ข้อมูลเกี่ยวกับความเสี่ยงในการตัดสินใจและบริหารงาน

๒. ความเข้าใจเกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงในทางเดียวกัน

การใช้คำนิยามเกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงแบบเดียวกัน จะทำให้เกิดความมีประสิทธิภาพในการกำหนดวัตถุประสงค์ นโยบาย กระบวนการ เพื่อใช้ในการบ่งชี้และประเมินความเสี่ยง และกำหนดวิธีการจัดการความเสี่ยงที่เหมาะสม

องค์กรที่ได้มีการจัดทำกรอบ และนโยบายการบริหารความเสี่ยงที่มีคำอธิบายองค์ประกอบในกรอบการบริหารความเสี่ยงอย่างชัดเจน จะทำให้ผู้บริหารและเจ้าหน้าที่ทุกคนมีความเข้าใจความเสี่ยงในแนวทางเดียวกันและมีจุดหมายร่วมกันในการบริหารความเสี่ยง

๓. กระบวนการบริหารการเปลี่ยนแปลง

ในการนำเอากระบวนการและระบบบริหารแบบใหม่มาใช้ องค์กรจำเป็นต้องมีการบริหารการเปลี่ยนแปลงเหล่านี้ การพัฒนาการบริหารความเสี่ยงก็เช่นเดียวกัน ต้องมีการชี้แจงให้ผู้บริหารและเจ้าหน้าที่ทุกคนรับทราบถึงการเปลี่ยนแปลงผลที่องค์กรและแต่ละบุคคลจะได้รับการจากการเปลี่ยนแปลงเหล่านั้น

๔. การกำหนดกระบวนการบริหารความเสี่ยงที่ต่อเนื่อง

องค์กรที่ประสบความสำเร็จในการปฏิบัติตามกระบวนการบริหารความเสี่ยง คือ องค์กรที่สามารถนำกระบวนการบริหารความเสี่ยงมาปฏิบัติอย่างทั่วถึงทั้งองค์กร และกระทำอย่างต่อเนื่องอย่างสม่ำเสมอ

๕. การสื่อสาร การเรียนรู้ และการอบรมที่มีประสิทธิภาพ

วัตถุประสงค์ของการสื่อสารอย่างมีประสิทธิผลนั้น เพื่อให้มั่นใจได้ว่า

- ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา
- ผู้บริหารสามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่
- มีการติดตามแผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กร และจัดการความเสี่ยงต่าง ๆ เพื่อให้องค์กรมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด การสื่อสารเกี่ยวกับกลยุทธ์ การบริหารความเสี่ยงและวิธีปฏิบัติมีความสำคัญอย่างมาก เพราะการสื่อสารจะเน้นให้เห็นถึงความเชื่อมโยงระหว่างการบริหารความเสี่ยงกับกลยุทธ์องค์กร การชี้แจงทำความเข้าใจต่อเจ้าหน้าที่ทุกคนถึงความรับผิดชอบแต่ละบุคคลต่อกระบวนการบริหารความเสี่ยง จะช่วยให้เกิดการยอมรับในกระบวนการและนำมาซึ่งความสำเร็จในการพัฒนาการบริหารความเสี่ยง โดยควรได้รับการสนับสนุนในทางปฏิบัติจากผู้บริหารระดับสูง และคณะกรรมการขององค์กร

๖. การวัดความเสี่ยง

การวัดผลการบริหารความเสี่ยงประกอบด้วย ๒ รูปแบบ ดังนี้

๖.๑ การวัดความเสี่ยง ในรูปแบบของผลกระทบและโอกาสที่อาจเกิดขึ้น การบริหารความเสี่ยงที่ประสบความสำเร็จจะช่วยให้ความเสี่ยงที่เหลืออยู่ในระดับที่องค์กรยอมรับได้

๖.๒ การวัดความสำเร็จของการบริหารความเสี่ยง โดยอาศัยดัชนีวัดผลการดำเนินงาน ซึ่งอาจกำหนดเป็นระดับองค์กร สายงาน ฝ่ายหรือของแต่ละบุคคล การใช้ดัชนีวัดผลการดำเนินงานนี้อาจปฏิบัติร่วมกับกระบวนการด้านทรัพยากรบุคคล

๗. การสนับสนุนการบริหารความเสี่ยงโดยกลไกด้านทรัพยากรบุคคล

คณะกรรมการและผู้บริหารและเจ้าหน้าที่ทุกคนในองค์กรควรต้องได้รับการฝึกอบรม เพื่อให้เข้าใจกรอบการบริหารความเสี่ยง และความรับผิดชอบของแต่ละบุคคลในการจัดการความเสี่ยงและสื่อสารข้อมูลเกี่ยวกับความเสี่ยง การฝึกอบรมในองค์กรควรคำนึงถึงประเด็นดังต่อไปนี้

- ความแตกต่างกันของระดับความรับผิดชอบในการบริหารความเสี่ยง
- ความรู้ที่เกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงที่มีอยู่แล้วในองค์กร

ระบบการประเมินผลการดำเนินงาน ถือเป็นเครื่องมือสำคัญที่ใช้ในการส่งเสริมความรับผิดชอบของแต่ละบุคคล โดยความรับผิดชอบเกี่ยวกับการบริหารความเสี่ยงควรกำหนดรวมอยู่ในงานที่แต่ละบุคคลรับผิดชอบ และในคำอธิบายลักษณะงาน (Job Description) การประเมินผลการดำเนินงานส่วนที่เกี่ยวกับการบริหารความเสี่ยงมีประเด็นที่ควรประเมินดังต่อไปนี้

- ความรับผิดชอบและการสนับสนุนกระบวนการบริหารความเสี่ยงและกรอบการบริหารความเสี่ยงที่แต่ละบุคคลมีต่อองค์กร
- การวัดระดับของความเสี่ยงที่บุคคลนั้น เป็นผู้รับผิดชอบว่าความเสี่ยงได้รับการจัดการอย่างมีประสิทธิผลเพียงใด

๘. กระบวนการติดตามการบริหารความเสี่ยง

ขั้นตอนสุดท้ายของปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง คือ การกำหนดวิธีที่เหมาะสมในการติดตามการบริหารความเสี่ยง

การติดตามกระบวนการบริหารความเสี่ยง

- การนำแผนตอบสนองความเสี่ยงไปปฏิบัติ และระดับความเสี่ยงที่เหลืออยู่หลังการปฏิบัติตามแผน
- การรายงานและการสอบทานตามขั้นตอนตามกระบวนการบริหารความเสี่ยง
- ความชัดเจนและสม่ำเสมอของการมีส่วนร่วมและความมุ่งมั่นของผู้บริหารระดับสูง
- บทบาทของผู้นำในการสนับสนุนและติดตามการบริหารความเสี่ยง
- การประยุกต์ใช้เกณฑ์การประเมินผลการดำเนินงานที่เกี่ยวข้องกับการบริหารความเสี่ยง

คู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์
(Strategic Risk Management Manual)

สารบัญ

๑. บทนำ

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ให้ความสำคัญต่อการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ (Strategic Risk Management) เป็นอย่างมากโดยมีคณะกรรมการบริหาร สรอ. แนะนำและติดตามการรายงานผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอเพื่อหาแนวทางแก้ไขปัญหาที่เกิดจากปัจจัยเสี่ยงต่าง ๆ นอกจากนี้ยังกำหนดให้มีการดูแลและทบทวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์อย่างต่อเนื่องเพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ สรอ. ยอมรับได้

การบริหารความเสี่ยงด้านนโยบายและกลยุทธ์จึงเป็นกระบวนการสำคัญที่จะลดโอกาสของความเสี่ยงที่อาจเกิดขึ้นและบรรเทาผลกระทบที่องค์กรจะได้รับในทุกหน่วยงานของ สรอ. ดังนั้น กระบวนการบริหารความเสี่ยงจะช่วยลดความสูญเสียที่อาจจะเกิดขึ้นให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้รวมทั้งเป็นองค์ประกอบสำคัญในการกำกับดูแล สรอ. ให้บรรลุผลสำเร็จตามเป้าหมายที่กำหนด

สรอ. ได้กำหนดกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์เพื่อให้หน่วยงานต่าง ๆ ของ สรอ. ได้ใช้เป็นแนวทางในการพิจารณา และจัดทำแผนกลยุทธ์และแผนธุรกิจที่สอดคล้องกับกลยุทธ์หลักของ สรอ. โดยการระบุความเสี่ยงที่อาจเกิดขึ้นแล้วทำการประเมินความเสี่ยงถึงโอกาสที่จะเกิดขึ้นรวมทั้งผลกระทบที่จะได้รับพร้อมทั้งจัดหาแนวทางหรือมาตรการควบคุมที่เหมาะสมมาดำเนินการหรือจัดการกับความเสี่ยงนั้นโดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่ สรอ. กำหนด

คู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ของ สรอ. นี้ จึงมุ่งเน้นถึงการสร้างความตระหนักให้เกิดแก่ทุกคนที่เกี่ยวข้องในสำนักงาน ในการที่จะช่วยสอดส่องดูแล ระมัดระวังเพื่อลดความเสี่ยง หรือ บรรเทาผลกระทบจากความเสี่ยงด้านนโยบายและกลยุทธ์ อันเกิดจากความเสี่ยงที่ไม่สามารถบรรลุเป้าหมายตามนโยบายและกลยุทธ์ ของ สรอ. เช่น การไม่สามารถดำเนินโครงการ GIN หรือ Mail Go Thai ได้ตามแผนงาน เป็นต้น ความเสี่ยงที่เกิดขึ้นดังกล่าวข้างต้นเป็นความเสี่ยงด้านนโยบายและกลยุทธ์ ที่ส่งผลต่อนโยบายที่ได้รับมอบหมายจากกระทรวงเทคโลยีสารสนเทศและการสื่อสาร หรือนโยบายภาครัฐได้ตามกำหนด รวมทั้งอาจส่งผลต่อภาพลักษณ์ขององค์กรและทำให้องค์กรไม่สามารถดำเนินการได้ครบถ้วนสมบูรณ์ตามวัตถุประสงค์และภารกิจที่กำหนดไว้ ดังนั้นการส่งเสริมให้ทุกคนตระหนักถึงความสำคัญและมีส่วนร่วมในการการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ (Strategic Risk

Management) โดยคณะกรรมการบริหาร สรอ. จะให้คำแนะนำและติดตามการรายงานการบริหารความเสี่ยงฯ ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อวางแนวทางแก้ไขปัญหาที่เกิดจากปัจจัยเสี่ยงต่าง ๆ นอกจากนี้ยังกำหนดให้มีการดูแลและทบทวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ อย่างต่อเนื่อง เพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ สรอ. ยอมรับได้

ดังนั้น คู่มือการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ฉบับนี้ถือเป็นส่วนหนึ่งของนโยบายการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ โดยจะกล่าวถึงวัตถุประสงค์ ขอบเขต โครงสร้างและบทบาทหน้าที่ของผู้รับผิดชอบกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ และรายละเอียดของกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ เพื่อเป็นแนวทางในการปฏิบัติงานของ สรอ. และเพื่อให้หน่วยงานต่าง ๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ตนเองตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

แนวทางการบริหารความเสี่ยงที่นำมาใช้

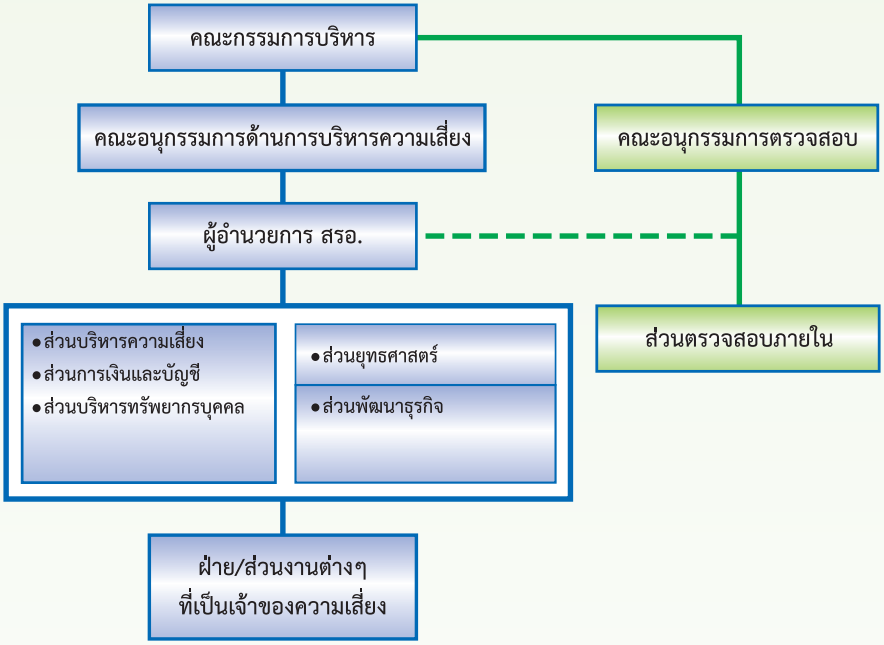
สรอ. กำหนดกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ตามแนวทางการปฏิบัติงานของ สรอ. และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Tread way Commission (COSO) โดยครอบคลุมความเสี่ยงธุรกิจ (Business Risk) ที่เกี่ยวกับการจัดทำและการกำหนดแผนงานของแผนกลยุทธ์ (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 เป็นต้นโดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์เพื่อให้หน่วยงานต่าง ๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ของตนเองเพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาทหน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายนโยบายและยุทธศาสตร์ มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ และนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๓. จัดทำคู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์และเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๔. ประสานงานกับส่วนยุทธศาสตร์ ส่วนการเงินและบัญชี และส่วนพัฒนาธุรกิจเพื่อจัดให้หน่วยงานต่าง ๆ ดำเนินการพิจารณา Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของหน่วยงานต่าง ๆ รวมถึงแนวทางการจัดการความเสี่ยงที่เหมาะสม

๕. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทางความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๖. ดูแลให้มีการปฏิบัติตามกระบวนการในการออก/ปรับปรุงผลิตภัณฑ์ตามแนวทางที่ สรอ. กำหนดและมีส่วนร่วมพิจารณาให้ความเห็นในการออกผลิตภัณฑ์ในประเด็นที่เกี่ยวข้องกับความเสี่ยงรวมทั้งปรับปรุงหรือแก้ไขข้อบกพร่องที่เกี่ยวกับความเสี่ยงด้านต่าง ๆ ที่เกิดขึ้นภายหลังการออก/ปรับปรุงผลิตภัณฑ์โดยดำเนินการร่วมกับหน่วยงานเจ้าของผลิตภัณฑ์นั้น ๆ

๗. ร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) สำหรับสถานการณ์ที่ไม่ปกติเพื่อรองรับการเปลี่ยนแปลงสภาพแวดล้อมที่ไม่เป็นไปตามที่คาดไว้

๘. ร่วมกับส่วนการเงินและบัญชีส่วนพัฒนาธุรกิจ และส่วนยุทธศาสตร์ เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์แผนธุรกิจแผนนโยบายและกลยุทธ์ และงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

(๑) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับ สรอ. พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ที่ได้ระบุไว้เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือก พร้อมทั้งระบุการควบคุมอย่างชัดเจน

(๒) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนดเพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหารควบคุมและจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนการเงินและบัญชี ฝ่ายบริหารประสิทธิภาพองค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดทำแผนการเงิน ให้สอดคล้องกับแผนกลยุทธ์แผนธุรกิจในภาพรวมของ สรอ. รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๓. ติดตามและวิเคราะห์ผลการดำเนินงานของ สรอ. เปรียบเทียบกับแผนการเงินและอื่น ๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมายและแนวทางการจัดการความเสี่ยง (Mitigation)

๔. ร่วมกับส่วนบริหารความเสี่ยง ส่วนพัฒนาธุรกิจ และส่วนยุทธศาสตร์ เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจแผนการเงินและงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

(๑) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับ สรอ. พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ที่ได้ระบุไว้เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือก พร้อมทั้งระบุการควบคุมอย่างชัดเจน

(๒) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนดเพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหารควบคุมและจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนยุทธศาสตร์ ฝ่ายนโยบายและยุทธศาสตร์ มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดทำแผนนโยบายและกลยุทธ์ ให้สอดคล้องกับแผนกลยุทธ์แผนธุรกิจในภาพรวมของ สรอ. รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๓. ติดตามและวิเคราะห์ผลการดำเนินงานของ สรอ. เปรียบเทียบกับแผนนโยบายและกลยุทธ์ และอื่น ๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมายและแนวทางการจัดการความเสี่ยง (Mitigation) เพื่อให้การปฏิบัติงานเป็นไปอย่างประสิทธิภาพและเกิดประสิทธิผลกรณีที่มีการเบี่ยงเบนไปจากแผนให้เสนอแนวทางแก้ไขให้ทันท่วงที

๔. ร่วมกับส่วนบริหารความเสี่ยง ส่วนพัฒนาธุรกิจ และส่วนการเงินและบัญชี เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจแผนนโยบายและกลยุทธ์ และงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

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

(๒) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนดเพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหารควบคุมและจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนพัฒนาธุรกิจ ฝ่ายบริการให้คำปรึกษา มีหน้าที่รับผิดชอบ ดังนี้

๑. ศึกษาความเป็นไปได้ตามแผนกลยุทธ์ แผนธุรกิจในภาพรวมของ สรอ. รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

๓. ติดตามและวิเคราะห์ผลการดำเนินงานของ สรอ. เปรียบเทียบกับแผนพัฒนาธุรกิจและอื่น ๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมายและแนวทางการจัดการความเสี่ยง (Mitigation)

๔. ร่วมกับส่วนยุทธศาสตร์ ส่วนการเงินและบัญชีและส่วนบริหารความเสี่ยง เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์แผนธุรกิจแผนนโยบายและกลยุทธ์ และงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

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

(๒) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนดเพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหารควบคุมและจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนบริหารทรัพยากรบุคคล ฝ่ายบริหารประสิทธิภาพองค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดองค์กรและกำหนดวิธีการปฏิบัติงานที่เอื้อต่อการปฏิบัติตามแผนกลยุทธ์โดยจัดให้มีการสอบยันและถ่วงดุลอำนาจ (Check and Balance) อย่างเหมาะสมรวมถึงกำหนดสายการบังคับบัญชาที่ชัดเจนและเปิดเผยเพื่อการสั่งการที่รวดเร็วและมีประสิทธิภาพ

๒. จัดอัตรากำลังให้เหมาะสมกับคุณสมบัติและหน้าที่ตำแหน่งงานที่รับผิดชอบรวมทั้งกำหนดระบบการสรรหาการฝึกอบรมและการกำหนดผลตอบแทนที่เหมาะสมเพื่อสนับสนุนเจ้าหน้าที่ให้ปฏิบัติตามแผนกลยุทธ์เพื่อบรรลุเป้าหมายของ สรอ.

๓. สร้างเสริมให้เกิดการกำกับดูแลกิจการที่ดีภายใน สรอ. เพื่อให้การดำเนินธุรกิจของ สรอ. มีความเจริญเติบโตอย่างต่อเนื่องและมั่นคงบริหารงานอย่างมีประสิทธิภาพโปร่งใสและเป็นธรรมซึ่งจะสร้างความเชื่อมั่นให้กับทุกหน่วยงาน

ส่วนตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

ตรวจสอบและสอบทานการควบคุมภายในด้านต่าง ๆ ของ สรอ. ก่อนนำเสนอคณะอนุกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

ฝ่ายและส่วนงานต่าง ๆ ของ สรอ. มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกลยุทธ์และแผนปฏิบัติการของฝ่าย และส่วนงานต่าง ๆ ให้สอดคล้องกับแผนกลยุทธ์หลักของ สรอ.

๒. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับฝ่ายและส่วนงานต่าง ๆ

๓. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนกลยุทธ์ฝ่าย และส่วนงานต่าง ๆ ให้กับส่วนบริหารความเสี่ยง เพื่อนำไปจัดทำแผนภาพความเสี่ยงด้านนโยบายและกลยุทธ์และภาพความเสี่ยงแบบบูรณาการตามลำดับต่อไป

๔. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของฝ่ายให้กับส่วนบริหารความเสี่ยงเป็นรายไตรมาส

๕. บริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงานในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๖. ดูแลติดตามการจัดการความเสี่ยงและประเมินผลการจัดการความเสี่ยงเป็นประจำเพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับรวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติมเพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๗. แต่งตั้งผู้ประสานงานด้านความเสี่ยง (Risk Officer) เพื่อประสานงานกับส่วนบริหารความเสี่ยงในการจัดทำ Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของส่วนงานและฝ่ายสื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๔.๑ ความเสี่ยงด้านนโยบายและกลยุทธ์ (Policy and Strategic Risk)

ความเสี่ยงด้านนโยบายและกลยุทธ์ (Policy and Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดนโยบายต่าง ๆ เช่น นโยบายระดับรัฐจนถึงนโยบายในระดับผู้บริหารแผนกลยุทธ์ แผนดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับสภาพแวดล้อมภายใน และปัจจัยภายนอก ทำให้มีโอกาสที่จะไม่ประสบความสำเร็จตามทิศทางที่กำหนดไว้ ซึ่งจะส่งผลกระทบต่อตัวชี้วัดผลการปฏิบัติงานของสำนักงาน

แผนกลยุทธ์ (Strategic Plan) หรือ **แผนยุทธศาสตร์** หมายถึง แผนที่แสดงทิศทางการดำเนินงานและสะท้อนวิสัยทัศน์หรือเป้าหมายหรือนโยบายของ สรอ. โดยทั่วไปจะมีระยะเวลา ๓ ถึง ๕ ปี ซึ่งแผนกลยุทธ์ที่ดีจะต้องมีความชัดเจนสอดคล้องกับเป้าหมายยืดหยุ่นและสามารถปรับเปลี่ยนให้สอดคล้อง กับสภาวการณ์ที่เปลี่ยนแปลงได้

แผนธุรกิจ (Business Plan) หมายถึง แผนที่กำหนดกรอบการดำเนินงานโดยรวมของ สรอ. เพื่อสนับสนุนการปฏิบัติงานให้สำเร็จตามแผนกลยุทธ์และเป็นแนวทางให้แก่หน่วยงานต่าง ๆ ในการกำหนดแผนปฏิบัติการ (Action Plan) โดยทั่วไปจะเป็นแผนระยะสั้นไม่เกิน ๑ ปี ประกอบด้วยเป้าหมายผลดำเนินการหน่วยงานที่รับผิดชอบปริมาณทรัพยากรที่ใช้กรอบเวลาการดำเนินงานและเกณฑ์ในการติดตามผลการปฏิบัติงานซึ่งควรสอดคล้องกับงบประมาณของ 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 อาจทำให้สภาวะการทำงานหยุดชะงักหรือต้องวางกลยุทธ์และแผนการดำเนินงานใหม่

(๓) การเปลี่ยนแปลงพฤติกรรมของกลุ่มลูกค้าเป้าหมายการเปลี่ยนแปลงของโครงสร้างประชากรและความต้องการของลูกค้าจะมีผลต่อฐานลูกค้าของ สรอ. ซึ่ง สรอ. ต้องมีการกำหนดกลุ่มลูกค้าเป้าหมายที่มีศักยภาพและวิธีการเสนอบริการที่ดีให้แก่ลูกค้าเหล่านั้นเพื่อป้องกันความเสี่ยงที่จะสูญเสียส่วนแบ่งตลาด

(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 และคำสั่งตลอดจนระเบียบของหน่วยงานที่กำกับดูแล อาจเป็นอุปสรรคในการดำเนินงานอันส่งผลกระทบต่อการปฏิบัติตามแผนกลยุทธ์และแผนดำเนินงานให้บรรลุเป้าหมายและจำเป็นต้องปรับเปลี่ยนแผนกลยุทธ์และแผนดำเนินงานให้สอดคล้องกับกฎหมาย ฯลฯ

๔.๒.๒ ปัจจัยความเสี่ยงภายใน หมายถึง ปัจจัยที่ สรอ. สามารถควบคุมได้แต่สามารถส่งผลกระทบหรือเป็นอุปสรรคต่อการดำเนินงานตามแผนกลยุทธ์เพื่อให้บรรลุเป้าหมาย ได้แก่

(๑) สรอ. ต้องจัดให้มีกระบวนการสื่อสารองค์กรในเรื่องแผนกลยุทธ์ และแผนดำเนินงานขององค์กรสู่เจ้าหน้าที่อย่างทั่วถึงทุกระดับและต่อเนื่อง

(๒) โครงสร้างองค์กรการจัดโครงสร้างองค์กรมีความสำคัญต่อการปฏิบัติตามแผนกลยุทธ์และแผนดำเนินงานให้บรรลุเป้าหมายและมีประสิทธิภาพหาก สรอ. ไม่มีการทบทวนการแบ่งแยกหน้าที่ความรับผิดชอบตามนโยบายหรือภารกิจที่ได้รับจากรัฐบาลเป็นรายปี หรือรายเฉพาะกิจจะทำให้เกิดปัญหาในการจัดการเพื่อบรรลุต่อเป้าหมายที่ต้องการ

(๓) กระบวนการและวิธีปฏิบัติงานหาก สรอ. มิได้กำหนดกระบวนการและวิธีปฏิบัติงานที่ชัดเจนหรือกำหนดความรับผิดชอบที่ซับซ้อนกันอาจส่งผลให้การปฏิบัติตามแผนการดำเนินงานและแผนปฏิบัติการล่าช้าและผิดพลาดได้ง่ายยากแก่การติดตามและรายงานผลการปฏิบัติงานได้ถูกต้องและทันกาล

(๔) ความเพียงพอและคุณภาพของบุคลากรการดำเนินงานตามแผนกลยุทธ์และแผนดำเนินงานในทุกระดับของ สรอ. จะบรรลุเป้าหมายได้หรือไม่นั้นขึ้นอยู่กับปริมาณ

และคุณภาพของบุคลากรจำนวนบุคลากรที่เพียงพอจะช่วยรองรับปริมาณงานและธุรกรรมได้ครบถ้วนบุคลากรควรมีความเชี่ยวชาญและได้รับการฝึกอบรมที่จำเป็นเพื่อให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผล

(๕) ความเพียงพอของข้อมูลผู้บริหารของ สรอ. จะต้องได้รับข้อมูลที่เหมาะสมเพื่อใช้ในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์การได้รับข้อมูลไม่เพียงพอไม่เหมาะสมไม่ถูกต้องและไม่ทันกาลจะเป็นอุปสรรคต่อการเข้าใจสภาวการณ์และส่งผลต่อการวางแผนกลยุทธ์และแผนดำเนินงานการกำหนดเป้าหมายและการบริหารงานของ สรอ.

(๖) เทคโนโลยี สรอ. จะต้องมีเทคโนโลยีที่สามารถแข่งขันและตอบสนองความต้องการของลูกค้าได้โดยเฉพาะธุรกรรมที่ซับซ้อนพร้อมทั้งต้องปรับปรุงระบบเทคโนโลยีสารสนเทศให้สามารถแข่งขันและรองรับปริมาณธุรกรรมใหม่ได้

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การดำเนินงานตามแผนกลยุทธ์ในบางกลยุทธ์ที่สำคัญไม่เป็นไปตามเป้าหมาย เนื่องจากนโยบายภาครัฐที่เปลี่ยนแปลงระหว่างปี	๑. ไม่มีคณะทำงานในการพิจารณาการปรับโครงสร้างองค์กร ๒. ช่องทางในการรับฟัง และสื่อสารกับบุคลากร เพื่อให้เกิดการยอมรับโครงสร้างของบุคลากรไม่เพียงพอ ๓. ขาดการติดตามการเปลี่ยนแปลงนโยบายภาครัฐระหว่างปีอย่างใกล้ชิด	✓	✓
ขาดการบูรณาการกลยุทธ์ในระดับองค์กรและฝ่ายงาน	๑. ไม่มีคณะทำงานที่มีหน้าที่รับผิดชอบในการเชื่อมโยงเป้าหมายแต่ละโครงการกับเป้าประสงค์ระดับองค์กร ๒. ไม่มีการกำหนดเป้าประสงค์ที่เป็นรูปธรรมสำหรับยุทธศาสตร์ในระดับองค์กรและเป็นที่ยอมรับทั่วทั้งองค์กร		

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
	๓. ขาดการติดตามการดำเนินงานผลความสำเร็จของเป้าประสงค์ในยุทธศาสตร์หลัก และเชื่อมโยงกับผลความสำเร็จของโครงการ	✓	
ขาดการถ่ายทอดกลยุทธ์ให้พนักงานและผู้เกี่ยวข้องรับทราบและเข้าใจ	๑. ไม่มีการกำหนดกระบวนการในการถ่ายทอดแผนยุทธศาสตร์ กลยุทธ์และแผนปฏิบัติการสู่พนักงานที่เกี่ยวข้อง ๒. ไม่มีการกำหนดช่องทางการถ่ายทอดแผนยุทธศาสตร์กลยุทธ์และแผนปฏิบัติการที่เพียงพอและเหมาะสม และประเมินประสิทธิผลของแต่ละช่องทาง ๓. ไม่มีการกำหนดรูปแบบการถ่ายทอดแผนยุทธศาสตร์จากระดับผู้บริหารลงสู่ระดับล่าง	✓	

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

การวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงทางนโยบายและกลยุทธ์ นั้น จากการที่สำนักงานเป็นหน่วยงานกลางของประเทศในการผลักดันและขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ โดยมีพันธกิจคือ การพัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์โดยมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงทางนโยบายและกลยุทธ์ เพื่อให้การดำเนินงานในขั้นตอนต่าง ๆ ของการจัดทำแผนธุรกิจและแผนกลยุทธ์มีประสิทธิภาพ รวมทั้งมีประโยชน์สำหรับตัดสินใจในการดำเนินธุรกิจของ สรอ. ผู้บริหารและหน่วยงานที่เกี่ยวข้องกับความเสี่ยงด้านนโยบายและกลยุทธ์จะต้องร่วมกันกำหนดและทบทวนกลยุทธ์อย่างสม่ำเสมอเพื่อใช้กำหนดแผนปฏิบัติการ (Action Plan) ในการพัฒนางานเพื่อป้องกันและลดความเสียหายที่อาจจะเกิดขึ้นรวมถึงช่วยให้สามารถบรรลุเป้าหมายและวัตถุประสงค์ของแผนดำเนินงานโดยแผนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่จัดทำขึ้นจะต้องมีรายละเอียดของวัตถุประสงค์ขอบเขตงานผู้มีหน้าที่รับผิดชอบงบประมาณรองรับหรือทรัพยากรที่ต้องการผลที่จะได้รับรวมถึงระยะเวลาการดำเนินงานของแผนที่ชัดเจนเพื่อประโยชน์ในการบริหารและติดตามการดำเนินงานตามแผนการบริหารความเสี่ยงที่กำหนดไว้

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

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านนโยบายและกลยุทธ์ อันมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามแผนกลยุทธ์ แผนปฏิบัติการประจำปี และการปฏิบัติตามกฎหมาย กฎระเบียบต่าง ๆ ที่จะส่งผลต่อการดำเนินงานด้านนโยบายและกลยุทธ์ต่าง ๆ ของหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร คณะกรรมการกิจการการจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เป็นต้น

๕.๓ การระบุเหตุการณ์ (Event Identification)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร สามารถระบุเหตุการณ์ความเสี่ยงได้เบื้องต้น ตามกระบวนการกำหนดยุทธศาสตร์ของ สรอ. ดังนี้

๑. ความเสี่ยงด้านการกำหนดแผนยุทธศาตร์ หรือแผนการดำเนินงานไม่เหมาะสมสอดคล้องกันของนโยบาย กลยุทธ์ โครงสร้างองค์กร

๒. ความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงานไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณา ไม่สามารถติดตามเป้าหมายได้

๓. ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์หรือแผนปฏิบัติการประจำปี

ความเสี่ยงด้านการกำหนดแผนยุทธศาตร์ หรือแผนการดำเนินงานไม่เหมาะสมสอดคล้องกัน ของนโยบาย กลยุทธ์ โครงสร้างองค์กร

การระบุความเสี่ยง แนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อความสอดคล้องกันของแผนงานต่าง ๆ ที่จะสนับสนุนยุทธศาสตร์หลักของ สรอ. รวมทั้งความสอดคล้องหรือข้อจำกัดของทรัพยากรที่เกี่ยวข้องกับ

การดำเนินยุทธศาสตร์ ทั้งทรัพยาการด้านงบประมาณ ด้านบุคลากร หรือระบบสนับสนุนอื่น ๆ เช่น ระบบสารสนเทศ โครงสร้างองค์กร เป็นต้น เพื่อให้เกิดการใช้ทรัพยากรอย่างคุ้มค่าและลดความซ้ำซ้อน สามารถพิจารณาได้จากความถี่ในการเปลี่ยนแปลง การปรับปรุงแผนปฏิบัติการที่ได้รับอนุมัติจากคณะกรรมการบริหารแล้วในระหว่างปี รวมทั้งปัจจัยภายนอกต่าง ๆ เช่นนโยบายหน่วยงานกำกับ นโยบายรัฐบาล ที่มีผลต่อการดำเนินกำหนดแผนยุทธศาสตร์ รวมทั้งกำหนดกิจกรรมในการดำเนินโครงการหลักของ สรอ.

ความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงานไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณา ไม่สามารถติดตามเป้าหมายได้

การระบุความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงานไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณา ไม่สามารถติดตามเป้าหมายได้ เป็นการระบุปัจจัยเสี่ยงแนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อการปฏิบัติงาน ที่ดำเนินการแล้วไม่สามารถทำให้ภาพรวม สรอ. บรรลุเป้าหมายที่แท้จริงได้ตามนโยบายและกลยุทธ์ และแผนงานประจำปี รวมทั้งปัจจัยเสี่ยงของกระบวนการกำหนดหรือการจัดทำเป้าหมายของตัวชี้วัดที่ได้กำหนดไว้ของยุทธศาสตร์ไม่ชัดเจนได้ ซึ่งจะส่งผลต่อการดำเนินกิจกรรมหลักของ สรอ.

ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์หรือแผนปฏิบัติการประจำปี

การระบุความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์ หรือแผนปฏิบัติการประจำปี ให้ระบุจากเป้าหมายของ สรอ. ในการกำหนดเป้าหมาย รวมทั้งกิจกรรมตามแผนยุทธศาสตร์ ที่อาจไม่บรรลุได้ตามกำหนด หรือความเสี่ยงที่อาจเกิดจากความล่าช้าในการดำเนินกิจกรรมตามแผนยุทธศาตร์ และแผนปฏิบัติการประจำปีรวมทั้งปัจจัยที่จะส่งผลกระทบการการดำเนินกิจกรรมตามแผนงาน เช่น กิจกรรมพัฒนาเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) กิจกรรมพัฒนาระบบเว็บไซต์กลางบริการอิเล็กทรอนิกส์ภาครัฐ (e-Portal) กิจกรรมพัฒนาความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนเพื่อส่งเสริมการพัฒนารัฐบาลอิเล็กทรอนิกส์ (Public-Private Partnership) กิจกรรมยกระดับขีดความสามารถและพัฒนาฐานข้อมูลบุคลากร ICT ภาครัฐ (ICT Training) เป็นต้น

ส่วนบริหารความเสี่ยง ส่วนยุทธศาสตร์ ส่วนการเงินและบัญชี ส่วนพัฒนาธุรกิจและส่วนบริหารทรัพยากรบุคคล ฝ่ายและส่วนงานต่าง ๆ ของ สรอ. ที่เกี่ยวข้องกับกลยุทธ์ของ สรอ. จะร่วมกันพิจารณา วิเคราะห์ และกำหนดปัจจัยต่าง ๆ ที่มีผลกระทบต่อความเสี่ยงด้านนโยบายและกลยุทธ์ ในแต่ละช่วงเวลา ทำให้ประเมินได้ว่าในอนาคต สรอ. จะมีการดำเนินงานตามแผนกลยุทธ์ หรือแผนงานโครงการหลักในช่วงใด อีกทั้งยังมีการร่วมพิจารณาถึงความเสี่ยงที่เกิดจากการดำเนินโครงการหลักของ สรอ. ที่ไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการและของ สรอ.

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงจะพิจารณาปัจจัยการประเมินความเสี่ยง ๒ ด้าน คือ การประเมินโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) จากการเกิดเหตุการณ์ความเสี่ยงเพื่อทราบระดับความรุนแรงของความเสี่ยง ทั้งนี้ ความเสี่ยงด้านนโยบายและกลยุทธ์ สามารถประเมินด้วยเครื่องมือเป้าหมายการดำเนินงานที่กำหนดไว้ รวมทั้งการประเมินจากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือ โอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านนโยบายและกลยุทธ์ เหล่านั้นขึ้น เป็นแต่ละเหตุการณ์ เช่น ผลกระทบจากนโยบายรัฐบาล สาเหตุเกิดจากความไม่ชัดเจนของภารกิจที่ทางรัฐบาลจะมอบหมายลงมาและ ไม่มีการเตรียมความพร้อมใด ๆ ในการรองรับ เป็นต้น

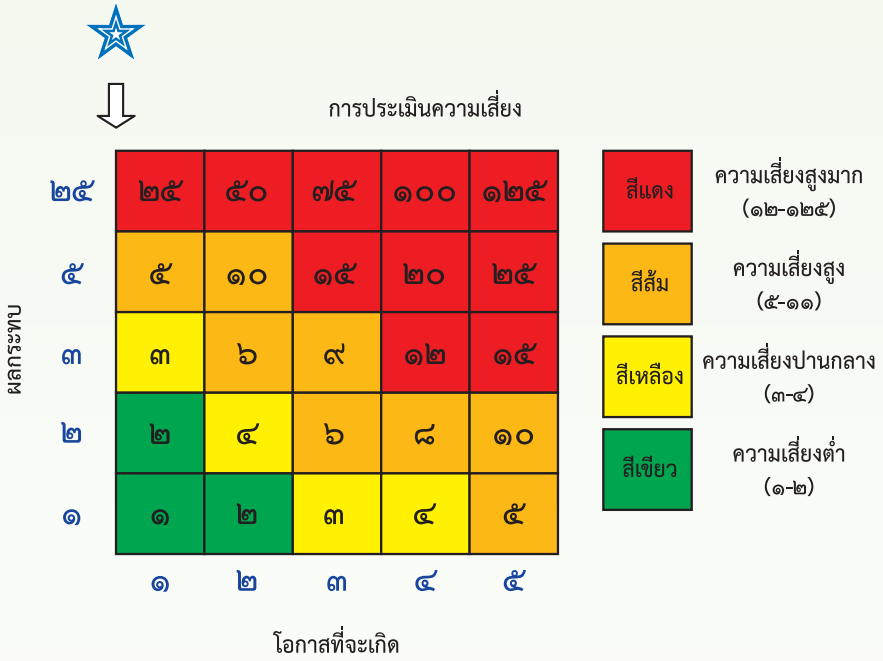
ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์หรือแผนปฏิบัติการประจำปีประสิทธิภาพในการบริหารงบประมาณ

ชื่อปัจจัยเสี่ยง การดำเนินงานตามแผนกลยุทธ์ในบางกลยุทธ์ที่สำคัญไม่เป็นไปตามเป้าหมาย เนื่องจากนโยบายภาครัฐที่เปลี่ยนแปลงระหว่างปี

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	ดำเนินการได้ครบถ้วนในระดับ ๒ รวมถึงมีการประเมินผลติดตามแผนงานทั้งแผนงานเดิม และแผนงานที่กระทบจากนโยบายภาครัฐ และมีการเสนอแนวทางการแก้ไขต่อฝ่ายบริหารเป็นประจำ เพื่อมุ่งสู่การบรรลุเป้าหมายองค์กร	ดำเนินการได้ครบถ้วนในระดับ ๓ และมีการจัดสรรทรัพยากรสำหรับการดำเนินงานนโยบายที่เปลี่ยนแปลงไปอย่างเหมาะสม โดยคำนึงถึงข้อจำกัดของทรัพยากรเดิม	มีหน่วยงานรับผิดชอบในเรื่องผลกระทบของนโยบายภาครัฐที่ชัดเจน รวมถึงถ่ายทอดสู่แผนปฏิบัติการ และถ่ายทอดให้บุคลากรในองค์กรได้รับทราบ	มีหน่วยงานรับผิดชอบในเรื่องผลกระทบของนโยบายภาครัฐที่ชัดเจน รวมถึงถ่ายทอดสู่แผนปฏิบัติการ แต่ยังไม่มีกระบวนการถ่ายทอดให้บุคลากรในองค์กรได้รับทราบ	มีหน่วยงานรับผิดชอบในเรื่องนโยบายภาครัฐที่ชัดเจน แต่ยังไม่มีการถ่ายทอดสู่แผนปฏิบัติการ
	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๕	ระดับ ๒๕
ผลกระทบ	ความสำเร็จตามแผนกลยุทธ์ ร้อยละ ๑๐๐	ความสำเร็จตามแผนกลยุทธ์ ร้อยละ ๙๕	ความสำเร็จตามแผนกลยุทธ์ ร้อยละ ๙๐	ความสำเร็จตามแผนกลยุทธ์ ร้อยละ ๘๕	ความสำเร็จตามแผนกลยุทธ์ ร้อยละ ๘๐

เมื่อประเมินระดับความเสี่ยงได้แล้วขั้นต่อไปคือการจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญและจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของ สรอ. หรือหน่วยงานและสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสมโดย สรอ. ได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น ๔ ระดับตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้น ๆ ได้แก่ระดับสูงมากระดับสูงระดับปานกลางระดับต่ำตามลำดับโดยใช้ตารางแสดงระดับวัดความเสี่ยงเป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมินซึ่งตารางจะแสดงข้อมูลเป็น ๒ แกนได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact) ตามตารางแสดงระดับวัดความเสี่ยง



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

ระดับความเสี่ยงด้านนโยบายและกลยุทธ์

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

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้วทำให้ทราบว่าความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใดหน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการควบคุมและลดความเสี่ยงดังกล่าวที่เหมาะสมเพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้วซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดจากความเสี่ยงนั้น ๆ จะทำให้ทราบว่าความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใดหน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการควบคุมและลดความเสี่ยงดังกล่าวเพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
การดำเนินงานตามแผนกลยุทธ์ในบางกลยุทธ์ที่สำคัญไม่เป็นไปตามเป้าหมายเนื่องจากนโยบายภาครัฐที่เปลี่ยนแปลงระหว่างปี	๑. มีแผนการจัดประชุมเพื่อกำหนด/ทบทวน ยุทธศาสตร์และเป้าหมายร่วมกับผู้บริหารและผู้รับผิดชอบโครงการเป็นประจำทุกปี ๒. มีการประชุมหารือกับผู้บริหารในการดำเนินงานเพื่อรายงานความก้าวหน้า และปัญหาอุปสรรคต่าง ๆ ๓. มีการเตรียมความพร้อมด้านบุคลากร ระบบงาน และเครื่องมือต่าง ๆ เพื่อรองรับการให้บริการที่มากขึ้นในแต่ละปี	การลดความเสี่ยง (Treat)

๕.๖ กิจกรรมการควบคุม (Control Activities)

ส่วนบริหารความเสี่ยง ส่วนการเงินและบัญชี ส่วนยุทธศาสตร์ มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านนโยบายและกลยุทธ์ โดยจะควบคุมความเสี่ยงทางด้านสภาพคล่องด้านการบริหารเงินลงทุน และอื่น ๆ ให้สอดคล้องกับเพดานความเสี่ยง (Risk Limit) หรือตัวบ่งชี้ความเสี่ยงด้านนโยบายและกลยุทธ์ ที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านนโยบายและกลยุทธ์ของสำนักงานให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการบริหาร สรอ. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

๕.๗ สารสนเทศและการสื่อสาร (Information and Communication)

แหล่งที่มาของข้อมูล

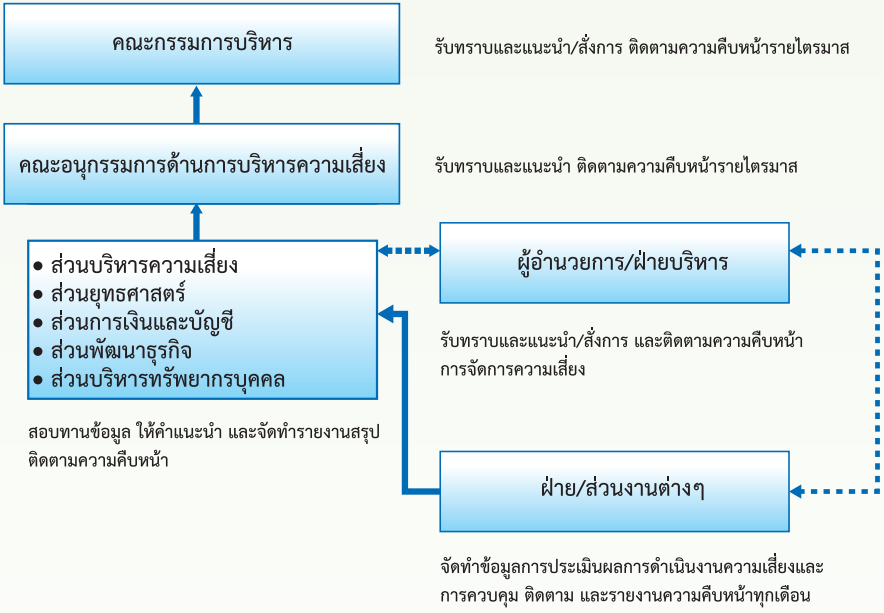
ส่วนบริหารความเสี่ยง ส่วนยุทธศาสตร์ และส่วนการเงินและบัญชี จัดเก็บข้อมูลซึ่งมีรายละเอียด ดังนี้

ข้อมูล	แหล่งที่มา	หมายเหตุ
○ แผนนโยบายและกลยุทธ์ระยะยาว ○ แผนนโยบายและกลยุทธ์ประจำปี ○ การปรับปรุงแผนการดำเนินงาน	○ ส่วนยุทธศาสตร์ ○ ส่วนการเงินและบัญชี	○ พิจารณาจากการจัดทำงบประมาณตามแผนงานทั้งระยะสั้น และระยะยาว ○ รายละเอียดกิจกรรมตามแผนงานที่กำหนด
○ สถานะการดำเนินงานตามแผนงาน ทั้งระยะสั้นและระยะยาว ○ สถานะการดำเนินงานตามตัวชี้วัด ตามยุทธศาสตร์ สรอ.	○ ส่วนยุทธศาสตร์	○ พิจารณาจากการรายงานความคืบหน้าการติดตามโครงการตามแผนยุทธศาสตร์ ○ พิจารณาจากการรายงานความคืบหน้าของตัวชี้วัดตามยุทธศาสตร์ ○ รายงานปัญหาอุปสรรคและแนวทางแก้ไขของการดำเนินโครงการที่สำคัญรวมทั้งตามแผนงาน

๕.๘ การติดตามและประเมินผล (Monitoring)

ส่วนยุทธศาสตร์ ส่วนการเงินและบัญชี มีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการ สรอ. และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านนโยบายและกลยุทธ์ ที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านนโยบายและกลยุทธ์ ในภาพรวมต่อคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อคณะกรรมการบริหาร สรอ. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่อง ต่อไป

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติส่วนยุทธศาสตร์ต้องรายงานให้ผู้บริหาร สรอ. ทราบตามลำดับความรุนแรงดังนี้

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

คู่มือบริหารความเสี่ยงด้านการปฏิบัติงาน
(Operational Risk Management Manual)

สารบัญ

๑. บทนำ

เพื่อให้การบริหารความเสี่ยงด้านการปฏิบัติงานของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) เป็นไปในแนวทางเดียวกัน สรอ. จึงได้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านการปฏิบัติงาน (Operational Risk Management Policy) เพื่อบังคับใช้กับทุกหน่วยงานของ สรอ. โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจและตระหนักถึงหน้าที่ความรับผิดชอบต่อการบริหารความเสี่ยงด้านการปฏิบัติงานอยู่เสมอ นับเป็นการสนับสนุนให้ทุกหน่วยงานของ สรอ. มีการบริหารความเสี่ยงด้านการปฏิบัติงานอย่างเป็นระบบและยังเป็นการส่งเสริมให้มีกระบวนการควบคุมภายในที่ดีอีกทางหนึ่งด้วยและเพื่อให้เจ้าหน้าที่ทุกระดับสามารถเข้าใจต่อการบริหารความเสี่ยงด้านการปฏิบัติงาน สรอ. จึงได้จัดทำคู่มือการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงด้านการปฏิบัติงาน โดยจะใช้ประกอบในการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งคู่มือฯ จะกล่าวลงไปในรายละเอียดเพื่อให้หน่วยงานสามารถวางระบบการบริหารความเสี่ยงด้านการปฏิบัติงานภายในหน่วยงานของตนเองได้อย่างมีประสิทธิภาพมีกระบวนการการป้องกันการควบคุมความเสี่ยงด้านการปฏิบัติงานให้ความเสี่ยงอยู่ในระดับที่ 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) โดยการบริหารความเสี่ยงด้านการปฏิบัติงานจะอยู่บนพื้นฐานของการควบคุมภายในซึ่งเป็นกระบวนการที่เป็นขั้นตอนที่ต่อเนื่องและแทรกอยู่ในการปฏิบัติงานตามปกติของทุกหน่วยงาน ทั้งนี้เจ้าหน้าที่ในทุกหน่วยงานของ สรอ. มีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านการปฏิบัติงานซึ่งมีผู้บริหารเป็นผู้รับผิดชอบให้มีระบบการบริหารความเสี่ยงด้านการปฏิบัติงานตามที่ สรอ. กำหนดคือมีการระบุประเมินติดตามควบคุมและรายงานความเสี่ยง

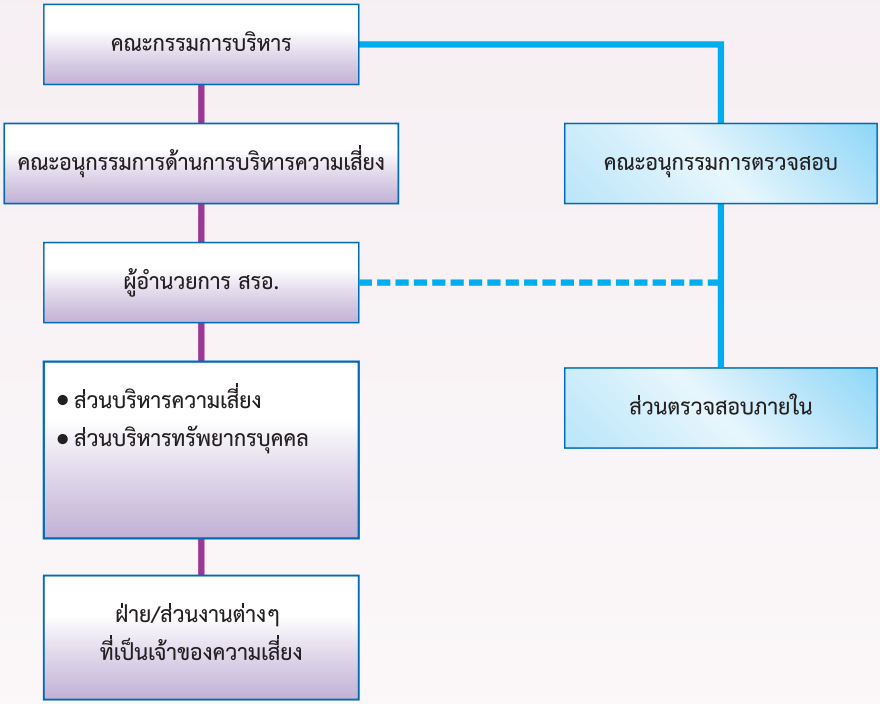
การบริหารความเสี่ยงด้านการปฏิบัติงานควรให้ความมั่นใจอย่างสมเหตุสมผลว่าหน่วยงานจะบรรลุตามเป้าหมายที่ได้กำหนดไว้กล่าวคือแม้ว่าจะมีการวางระบบการบริหารความเสี่ยงด้านการปฏิบัติงานไว้ดีเพียงใดก็ไม่สามารถรับรองได้ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้อย่างสมบูรณ์เพราะมีข้อจำกัดจากปัจจัยอื่นนอกเหนือการควบคุมของหน่วยงาน เช่น ผลกระทบจากปัจจัยภายนอก เป็นต้น

ขอบเขตของคู่มือบริหารความเสี่ยงด้านการปฏิบัติงาน

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งครอบคลุมถึงความเสี่ยงอันเกิดจากการดำเนินงานที่ไม่เป็นไปตามแผนกลยุทธ์ สรอ. รวมทั้งนโยบายที่ได้รับจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งนโยบายภาครัฐ ตั้งแต่การกำหนดแผนงานที่รองรับนโยบายไม่ครบถ้วนการดำเนินงานไม่ได้ตามเป้าหมายแผนกลยุทธ์ของโครงการหลัก รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นปัจจัยภายนอก เช่น การเปลี่ยนแปลงนโยบายภาครัฐ เป็นต้น โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานเพื่อให้หน่วยงานต่าง ๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านการปฏิบัติงานของตนเองเพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านการปฏิบัติงาน



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยงฝ่ายนโยบายและยุทธศาสตร์ มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานและนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านการปฏิบัติงานให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานที่กำหนดในกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงาน

๓. จัดทำคู่มือบริหารความเสี่ยงด้านการปฏิบัติงานและเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๔. ประสานงานกับส่วนปฏิบัติงานต่าง ๆ ส่วนพัฒนาธุรกิจ และส่วนยุทธศาสตร์องค์กรเพื่อจัดให้หน่วยงานต่าง ๆ ดำเนินการพิจารณา Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของหน่วยงานต่าง ๆ รวมถึงแนวทางการจัดการความเสี่ยงที่เหมาะสม

๕. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทางความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านการปฏิบัติงาน

๖. ดูแลให้มีการปฏิบัติตามกระบวนการในการออก/ปรับปรุงผลิตภัณฑ์ตามแนวทางที่ สรอ. กำหนดและมีส่วนร่วมพิจารณาให้ความเห็นในการออกผลิตภัณฑ์ในประเด็นที่เกี่ยวข้องกับความเสี่ยงรวมทั้งปรับปรุงหรือแก้ไขข้อบกพร่องที่เกี่ยวกับความเสี่ยงด้านต่าง ๆ ที่เกิดขึ้นภายหลังการออก/ปรับปรุงผลิตภัณฑ์โดยดำเนินการร่วมกับหน่วยงานเจ้าของผลิตภัณฑ์นั้น ๆ

๗. ร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) สำหรับสถานการณ์ที่ไม่ปกติเพื่อรองรับการเปลี่ยนแปลงสภาพแวดล้อมที่ไม่เป็นไปตามที่คาดไว้

ผู้ประสานงานความเสี่ยง (Risk Internal Control Officer: RICO)

ทุกหน่วยงานต้องกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็น RICO ประจำหน่วยงานซึ่งจะดูแลรับผิดชอบในการประสานงานกับส่วนบริหารความเสี่ยงที่จะนำเครื่องมือต่าง ๆ ที่ใช้ในการบริหารความเสี่ยงด้านการปฏิบัติงานไปใช้บริหารความเสี่ยงด้านการปฏิบัติงานภายในหน่วยงานตนเองและรายงานข้อมูลที่เกี่ยวข้องให้ส่วนบริหารความเสี่ยงตามกำหนดเวลารวมไปถึงให้ความรู้ที่เกี่ยวกับการบริหารความเสี่ยงด้านการปฏิบัติงานแก่เจ้าหน้าที่ในหน่วยงานของตนเองทั้งนี้เพื่อให้เจ้าหน้าที่ทุกระดับในหน่วยงานตนเองรับทราบถึงความเสี่ยงด้านการปฏิบัติงานโดยรวมและแนวทางแก้ไขที่ได้กำหนดไว้ ดังนั้น RICO จึงควรเป็นบุคคลที่มีความเข้าใจในกระบวนการในการปฏิบัติงานต่าง ๆ ของหน่วยงานตนเองเป็นอย่างดีเพื่อจะได้สามารถระบุและประเมินความเสี่ยงด้านการปฏิบัติงานของหน่วยงานตนเองได้อย่างถูกต้องพร้อมทั้งรายงานข้อมูลที่เกี่ยวกับความเสี่ยงด้านการปฏิบัติงานได้อย่างครบถ้วนถูกต้อง

ผู้จัดการความเสี่ยง (Risk Manager)

ผู้จัดการความเสี่ยง (Risk Manager) หมายถึง หัวหน้าหน่วยงานนั้น ๆ โดยเป็นบุคคลที่ทำหน้าที่รับผิดชอบในการบริหารจัดการความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานที่อยู่ภายใต้ความรับผิดชอบของตนเองในฐานะเจ้าของความเสี่ยง (Risk owner) รวมถึงมีหน้าที่ดูแลให้การปฏิบัติงานเป็นไปตามนโยบายและกรอบการบริหารความเสี่ยงด้านการปฏิบัติงานตามที่ สรอ. กำหนดพร้อมทั้งให้ความเห็นชอบต่อข้อมูลที่เกี่ยวกับการบริหารความเสี่ยงด้านการปฏิบัติงานที่ RICO รายงานให้แก่ส่วนบริหารความเสี่ยง

เจ้าหน้าที่ทุกคน (Employees)

มีหน้าที่ในการปฏิบัติตามนโยบายและกรอบการบริหารความเสี่ยงด้านการปฏิบัติงานตามที่ สรอ. กำหนดรวมไปถึงรับผิดชอบในการบริหารความเสี่ยงด้านการปฏิบัติงานภายใต้ขอบเขตความรับผิดชอบของตนโดยมีหน้าที่ทำความเข้าใจหลักการของความเสี่ยงภายใต้กรอบการบริหารความเสี่ยงของ สรอ. เพื่อให้แน่ใจว่าการบริหารความเสี่ยงด้านการปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพส่งผลให้เกิดมูลค่าเพิ่มแก่หน่วยงานและ สรอ. สอดคล้องกับแผนงานวัตถุประสงค์และกลยุทธ์ที่กำหนดไว้

ส่วนบริหารทรัพยากรบุคคล ฝ่ายบริหารประสิทธิภาพองค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดองค์กรและกำหนดวิธีการปฏิบัติงานที่เอื้อต่อการปฏิบัติตามแผนกลยุทธ์ โดยจัดให้มีการสอบยันและถ่วงดุลอำนาจ (Check and Balance) อย่างเหมาะสมรวมถึงกำหนดสายการบังคับบัญชาที่ชัดเจนและเปิดเผยเพื่อการสั่งการที่รวดเร็วและมีประสิทธิภาพ

๒. จัดอัตรากำลังให้เหมาะสมกับคุณสมบัติและหน้าที่ตำแหน่งงานที่รับผิดชอบ รวมทั้งกำหนดระบบการสรรหาการฝึกอบรมและการกำหนดผลตอบแทนที่เหมาะสม เพื่อสนับสนุนเจ้าหน้าที่ให้ปฏิบัติตามแผนกลยุทธ์เพื่อบรรลุเป้าหมายของ สรอ.

๓. สร้างเสริมให้เกิดการกำกับดูแลกิจการที่ดีภายใน สรอ. เพื่อให้การดำเนินธุรกิจของ สรอ. มีความเจริญเติบโตอย่างต่อเนื่องและมั่นคงบริหารงานอย่างมีประสิทธิภาพ โปร่งใสและเป็นธรรมซึ่งจะสร้างความเชื่อมั่นให้กับทุกหน่วยงาน

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๔.๑ ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)

ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk) คือ ความเสี่ยงที่ทำให้เกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดีหรือขาดธรรมาภิบาลในองค์กร และขาดการควบคุมดูแลที่เหมาะสมโดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายในคน (เจ้าหน้าที่บุคคลภายนอกหรือลูกค้า) ระบบงานหรือเหตุการณ์ภายนอกซึ่งส่งผลกระทบต่อการดำเนินงานของ สรอ.

ความเสี่ยงด้านการปฏิบัติงานยังครอบคลุมถึงเหตุการณ์ความเสียหาย (Loss Incidents) ที่อาจเกิดขึ้นเนื่องจากการดำเนินงานผิดพลาดของหน่วยงาน (Business Unit) ใด ๆ ใน สรอ. และสามารถเกิดขึ้นได้กับการปฏิบัติงานในทุกระดับชั้นนอกจากนี้ความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานหนึ่งอาจส่งผลกระทบและก่อให้เกิดความเสียหายแก่หน่วยงานอื่น ๆ ต่อเนื่องกันไปได้ ดังนั้น จึงมีความจำเป็นที่ในแต่ละหน่วยงานของ สรอ. ต้องมีระบบการบริหารความเสี่ยงด้านการปฏิบัติงานที่มีประสิทธิภาพและเหมาะสมกับสภาวะแวดล้อมในการดำเนินธุรกิจเพื่อให้มั่นใจว่า สรอ. สามารถจัดการความเสี่ยงด้านการปฏิบัติงานได้และลดความสูญเสียให้อยู่ในระดับต่ำที่สุด

๔.๒ ที่มาของความเสี่ยงด้านการปฏิบัติงาน สามารถจำแนกได้ ๗ ประเภทดังนี้

๔.๒.๑. ความเสี่ยงจากการทุจริตจากภายใน (Internal fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายใน สรอ. เพื่อให้ผลประโยชน์ที่เกิดขึ้นจากการทุจริตดังกล่าวตกแก่พวกพ้องของตนเอง

๔.๒.๒. ความเสี่ยงจากการทุจริตจากภายนอก (External fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายนอกแต่ก่อให้เกิดความเสียหายโดยตรงต่อ สรอ.

๔.๒.๓. ความเสี่ยงจากการจ้างงานและความปลอดภัยในสถานที่ปฏิบัติงาน (Employment practices and workplace safety) ความเสี่ยงจากการจ้างงานสามารถเกิดขึ้นจากกระบวนการต่าง ๆ ที่เกี่ยวกับการจ้างงาน เช่น การจ่ายค่าตอบแทนการปฏิบัติต่อเจ้าหน้าที่อย่างไม่เป็นธรรม เป็นต้นซึ่งอาจก่อให้เกิดการลาออกการฟ้องร้องหรือการหยุดงานประท้วงได้ และสำหรับความปลอดภัยในสถานที่ปฏิบัติงาน หากไม่มีการกำหนดมาตรการ

การรักษาความปลอดภัยในการปฏิบัติงาน หรือการควบคุมสภาพแวดล้อมในการปฏิบัติงานที่ไม่เพียงพออาจส่งผลกระทบต่อสุขภาพของเจ้าหน้าที่อันเนื่องมาจากโรคภัยหรือได้รับบาดเจ็บจากอุบัติเหตุอันเนื่องมาจากการปฏิบัติงานได้

๔.๒.๔. ความเสี่ยงจากลูกค้า ผลิตภัณฑ์และวิธีปฏิบัติในการดำเนินธุรกิจ (Clients, Products and Business practices) เป็นความเสี่ยงที่เกิดขึ้นจากวิธีปฏิบัติในการดำเนินธุรกิจกระบวนการออกแบบพัฒนาผลิตภัณฑ์และการเข้าถึงข้อมูลลูกค้าที่ไม่เหมาะสมไม่เป็นไปตามกฎหมายระเบียบและข้อบังคับที่ทางการกำหนด เช่น การทำธุรกรรมที่ละเมิดกฎหมายและการที่ สรอ. นำข้อมูลความลับของลูกค้าไปหาผลประโยชน์ เป็นต้น

๔.๒.๕. ความเสี่ยงด้านความปลอดภัยของทรัพย์สิน (Damage to physical assets) เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ทรัพย์สินของ สรอ. อันเนื่องมาจากภัยต่าง ๆ ที่เกิดขึ้นเช่นอุทกภัย วาตภัย อัคคีภัยการก่อการร้ายความไม่สงบทางการเมืองการก่อวินาศภัย เป็นต้น

๔.๒.๖. ความเสี่ยงจากการขัดข้องหรือการหยุดชะงักของระบบงานและระบบคอมพิวเตอร์ (Business disruption and system failures) เป็นความเสี่ยงที่เกิดขึ้นจากระบบงานที่ผิดปกติหรือการหยุดทำงานของระบบงานด้านต่าง ๆ เช่นความไม่สอดคล้องกันหรือความแตกต่างของระบบงานความบกพร่องของระบบงานคอมพิวเตอร์หรือระบบเครือข่ายรวมถึงการใช้เครื่องมือและเทคโนโลยีที่ไม่เหมาะสมล้าสมัยและไม่มีประสิทธิภาพ เป็นต้น

๔.๒.๗. ความเสี่ยงจากกระบวนการทำงาน (Execution, Delivery and Process management) เป็นความเสี่ยงที่เกิดขึ้นจากความผิดพลาดในวิธีปฏิบัติงาน (Methodology) ความผิดพลาดของระบบการปฏิบัติงานหรือความผิดพลาดจากการปฏิบัติงานของเจ้าหน้าที่ภายใน สรอ. และเจ้าหน้าที่หรือผู้รับจ้างจากการจ้างงานภายนอกเช่นการบันทึกข้อมูลเข้าระบบผิดพลาดผู้รับจ้างจากภายนอกไม่ปฏิบัติตามสัญญาการจ้างงานการขาดความรู้ความเข้าใจในการปฏิบัติงานและการใช้งานระบบคอมพิวเตอร์ของเจ้าหน้าที่การปรับปรุงกระบวนการทำงานที่ไม่เหมาะสมรวมถึงการจัดทำนิติกรรมสัญญาและเอกสารทางกฎหมายที่ไม่สมบูรณ์ทำให้ไม่สามารถใช้บังคับได้ตามกฎหมาย 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
ระบบประเมินผลการปฏิบัติงานยังไม่มีประสิทธิภาพ	๑. ไม่มีการจัดทำระบบการประเมินผลการปฏิบัติงานที่มีประสิทธิภาพ ๒. ไม่มีการกำหนดแผนงานการพัฒนาระบบประเมินผลการปฏิบัติงานของ สรอ. ๓. ไม่มีสื่อสารระบบประเมินผลการปฏิบัติงานให้พนักงานรับทราบ	✓	
การแก้ไขปัญหาของผู้ให้บริการภายนอก (Provider) ล่าช้าและไม่มีความเสถียร	๑. ไม่มีการสรุปประเด็นปัญหา และกำหนดระยะเวลาในการแก้ไขที่ชัดเจน ๒. ไม่มีการกำหนดมาตรการเร่งรัดการติดตามในการแก้ไขปัญหา ๓. ไม่มีการติดตามและรายงานผลการแก้ไขปัญหาให้ สรอ. ทราบ		✓
ระบบงานภายในยังไม่เชื่อมโยง และไม่มีระบบสารสนเทศที่สามารถเชื่อมข้อมูลระหว่างส่วนงานที่จำเป็นต้องใช้ข้อมูลร่วมกัน	๑. ไม่มีหน่วยงานในการวิเคราะห์ระบบงานที่จำเป็นต้องเชื่อมโยงข้อมูล ๒. ไม่มีการประเมินระบบงานที่สำคัญที่จำเป็นต้องเชื่อมโยง ๓. ไม่มีการกำหนดความต้องของข้อมูลหรือระบบงานที่ต้องการใช้งานร่วมกัน	✓	

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

การวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงทางปฏิบัติงานนั้น จากการที่สำนักงานเป็นหน่วยงานกลางของประเทศในการผลักดันและขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ โดยมีพันธกิจคือ การพัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์ โดยมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงทางปฏิบัติงานเพื่อให้มีกระบวนการในการบริหารความเสี่ยงด้านการปฏิบัติงานให้เป็นไปตามหลักมาตรฐานสากลและเป็นมาตรฐานเดียวกันทั่วทั้ง สรอ. เช่นเดียวกับกระบวนการบริหารความเสี่ยงด้านอื่น ๆ โดยจะครอบคลุมการปฏิบัติงานในทุกระดับชั้นของแต่ละหน่วยงานใน สรอ. เพื่อช่วยให้การดำเนินงานเกิดผลดีและปฏิบัติงานได้ตามกฎระเบียบที่เกี่ยวข้อง โดยแผนการบริหารความเสี่ยงด้านการปฏิบัติงานที่จัดทำขึ้นจะต้องมีรายละเอียดของวัตถุประสงค์ขอบเขตงานผู้มีหน้าที่รับผิดชอบงบประมาณรองรับหรือทรัพยากรที่ต้องการผลที่จะได้รับรวมถึงระยะเวลาการดำเนินงานของแผนที่ชัดเจนเพื่อประโยชน์ในการบริหารและติดตามการดำเนินงานตามแผนการบริหารความเสี่ยงที่กำหนดไว้

ทั้งนี้ การวิเคราะห์สภาพแวดล้อมต้องคำนึงถึงระบบงานที่รองรับการปฏิบัติงานในทุกขั้นตอนของ สรอ. ได้แก่ กระบวนการเทคโนโลยี สารสนเทศ อุปกรณ์ บุคลากรความเพียงพอของข้อมูล ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินงานที่มีผลกระทบต่อ สรอ.

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านการปฏิบัติงานอันมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามกระบวนการหรือขั้นตอนการปฏิบัติงาน รวมทั้งการปฏิบัติตามกฎหมาย กฎระเบียบต่าง ๆ ที่จะส่งผลต่อการดำเนินงานด้านการปฏิบัติงานต่าง ๆ ของหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ก.พ.ร. เป็นต้น

๕.๓ การระบุเหตุการณ์ (Event Identification)

การระบุเหตุการณ์ความเสี่ยงจะเริ่มด้วยการแจกแจงกระบวนการปฏิบัติงาน (Work flow) เพื่อให้ได้ทราบขั้นตอนงานที่มีอยู่และจะทำให้บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยหน่วยงานต้องมีการระบุจุด/พื้นที่ ที่มีความเสี่ยง (Risk Area) และสาเหตุหรือปัจจัยของความเสี่ยง (Risk Factor) ในแต่ละผลิตภัณฑ์/บริการหรือในแต่ละระบบงานก่อนที่จะมีกิจกรรมการควบคุม (Control Activities) เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่ (Inherent Risk) ผ่านระบบการควบคุมภายในและการประเมินการควบคุมความเสี่ยงด้วยตนเอง (Risk and Control Self-Assessment หรือ RCSA) โดยการระบุความเสี่ยงของหน่วยงานนั้นควรดำเนินการในทุกระดับตั้งแต่ระดับปฏิบัติงานขึ้นไปจนถึงระดับบริหารและครอบคลุมในทุกกิจกรรมของหน่วยงานทั้งนี้หน่วยงานควรมีการทบทวนการระบุความเสี่ยงด้านการปฏิบัติงานที่มีอยู่อย่างน้อยปีละ ๑ ครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงของปัจจัยความเสี่ยงต่าง ๆ ที่ส่งผลกระทบต่อกระบวนการในการปฏิบัติงาน เช่น ระบบหรือขั้นตอนที่ในการปฏิบัติงานเปลี่ยนไป มีการเปลี่ยนแปลงโครงสร้างองค์กรการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศการออกผลิตภัณฑ์ใหม่ ๆ การเปลี่ยนแปลงทางกฎหมายและกฎระเบียบข้อบังคับต่าง ๆ เป็นต้น ทั้งนี้ ในการระบุความเสี่ยงเบื้องต้น หน่วยงานสามารถระบุความเสี่ยงได้จากแผนผังกระบวนการทำงานหรือขั้นตอนการปฏิบัติงาน (Working Process/Work Flow) หรือข้อมูลเหตุการณ์ความเสียหายที่เคยเกิดขึ้นกับหน่วยงาน (Loss Incidents)

ความเสี่ยงด้านกระบวนการทำงานหรือขั้นตอนในการปฏิบัติงาน

ในการระบุความเสี่ยงนั้นหน่วยงานเจ้าของความเสี่ยง (Risk Owner) จะต้องทำความเข้าใจเกี่ยวกับกระบวนการทำงานหรือขั้นตอนการปฏิบัติงานของตนเองเพื่อสามารถระบุจุดที่อาจเกิดความเสี่ยง (Risk Area) ซึ่งวิธีที่นิยมในการระบุจุดความเสี่ยงนั้น จะสร้างแผนผังกระบวนการทำงานหรือขั้นตอนการปฏิบัติงานซึ่งมีการระบุถึงปัจจัยความเสี่ยงเอกสารระบบงานและผู้รับผิดชอบที่เกี่ยวข้องในแต่ละกระบวนการทำงานอย่างชัดเจน และการจัดทำแผนผังกระบวนการทำงานและสัญลักษณ์ที่ใช้ของแต่ละหน่วยงาน ควรกำหนดใช้สัญลักษณ์แทนในแต่ละกระบวนการทำงานที่เป็นมาตรฐานเดียวกันทั้ง สรอ.

ความเสี่ยงด้านข้อมูลเหตุการณ์ความเสียหาย (Loss Incidents)

ในการระบุความเสี่ยงนั้น สามารถนำข้อมูลจากเหตุการณ์ความเสียหายของหน่วยงานที่เคยเกิดขึ้นในอดีตซึ่งจะช่วยให้หน่วยงานทราบถึงความรุนแรง (Severity) และโอกาส (Likelihood)

ที่จะเกิดความเสี่ยงเหล่านั้นอีกนอกจากนี้ยังช่วยให้หน่วยงานสามารถคาดคะเนหรือระบุความเสี่ยงที่อาจจะเกิดขึ้นในอนาคตได้หากปัจจัยแวดล้อมต่าง ๆ ของหน่วยงานไม่ได้เปลี่ยนแปลงไปอย่างมีนัยสำคัญ

ส่วนบริหารความเสี่ยง และหน่วยงานต่าง ๆ ของ สรอ. ที่เกี่ยวข้องกับกระบวนการดำเนินงานที่สำคัญจะร่วมกันพิจารณา วิเคราะห์ และกำหนดปัจจัยต่าง ๆ ที่มีผลกระทบต่อความสี่ยงด้านการปฏิบัติงานในแต่ละกระบวนการ หรือกระบวนการ/โครงสร้างองค์กร/เทคโนโลยี ที่มีการเปลี่ยนแปลงอย่างเป็นนัยสำคัญ

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

เมื่อหน่วยงานได้มีการระบุจุดที่อาจก่อให้เกิดความเสี่ยง (Key Risk Area) และสาเหตุ/ปัจจัยที่ก่อให้เกิดความเสี่ยง (Risk Factor) ในแต่ละกระบวนการทำงานแล้วหน่วยงานต้องมีการประเมินความเสี่ยงด้านการปฏิบัติงานในแต่ละจุดที่มีความเสี่ยงในแต่ละขั้นตอนการปฏิบัติงานซึ่งต้องอาศัยดุลยพินิจและประสบการณ์ของผู้ปฏิบัติงานในหน่วยงาน รวมถึงข้อมูลความเสี่ยงที่เคยเกิดขึ้นในอดีตเป็นสำคัญโดยจะพิจารณาจาก ๒ ปัจจัยคือ

- โอกาสที่จะเกิดความเสี่ยง (Likelihood) โดยพิจารณาจากความถี่ของเหตุการณ์ที่เกิดขึ้นในอดีตและประมาณโอกาสที่จะเกิดขึ้นในอนาคต
- ระดับของผลกระทบ (Impact) ที่เกิดจากความเสี่ยงนั้น ๆ พิจารณาจากความรุนแรงของเหตุการณ์ในอดีตและประมาณความรุนแรงของเหตุการณ์ที่อาจเกิดขึ้นในอนาคต เพื่อหน่วยงานจะได้ทราบถึงระดับความเสี่ยงที่มีอยู่ (Inherent Risk) และยังเป็นข้อมูลสำหรับการจัดลำดับความสำคัญในการดำเนินการปรับปรุงควบคุมและลดความเสี่ยงต่อไป

ทั้งนี้ในขั้นตอนของการระบุและการประเมินความเสี่ยงของหน่วยงานนั้นจะต้องพิจารณาถึงปัจจัยเสี่ยงทั้งภายในและภายนอกหน่วยงานประกอบด้วย เช่น คุณภาพของบุคลากรอัตราการหมุนเวียนของเจ้าหน้าที่ กระบวนการในการปฏิบัติงานสภาพการแข่งขันความก้าวหน้าของเทคโนโลยีกฎหมายหรือกฎระเบียบข้อบังคับต่าง ๆ และสภาวะเศรษฐกิจ เป็นต้น นอกจากนี้การระบุและประเมินความเสี่ยงของหน่วยงานควรดำเนินการอย่างต่อเนื่องและทบทวนความเหมาะสมเป็นระยะ

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ชื่อปัจจัยเสี่ยง ระบบประเมินผลการปฏิบัติงานยังไม่มีประสิทธิภาพ

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	มีการพัฒนาระบบประเมินผลการปฏิบัติงาน และสามารถใช้ประเมินผลบุคลากรได้ครบทุกระดับ	มีการพัฒนาระบบประเมินผลการปฏิบัติงาน และสามารถใช้ประเมินผลบุคลากร ได้ระดับบริหารชั้นต้นขึ้นไป	มีการพัฒนาระบบประเมินผลการปฏิบัติงาน และสามารถใช้ประเมินผลบุคลากรได้เฉพาะผู้บริหารระดับสูง (ระดับฝ่ายขึ้นไป)	มีการพัฒนาระบบประเมินผลการปฏิบัติงาน และมีการสื่อสารให้กับพนักงานเข้าใจในหลักเกณฑ์แนวทางของระบบการประเมินผลที่จะนำมาใช้อย่างทั่วทั้งองค์กร	อยู่ระหว่างการพัฒนาระบบประเมินผลการปฏิบัติงาน เพื่อให้สามารถใช้ประเมินผลได้อย่างมีประสิทธิภาพ
	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๕	ระดับ ๒๕
ผลกระทบ	ความสำเร็จตามเป้าประสงค์ปี ๒๕๕๗ ในแต่ละยุทธศาสตร์ดีกว่าเป้าหมายทุกยุทธศาสตร์	ความสำเร็จตามเป้าประสงค์ปี ๒๕๕๗ ในแต่ละยุทธศาสตร์ดีกว่าเป้าหมายบางยุทธศาสตร์	ความสำเร็จตามเป้าประสงค์ปี ๒๕๕๗ ในแต่ละยุทธศาสตร์เป็นไปตามเป้าหมายทุกยุทธศาสตร์	ความสำเร็จตามเป้าประสงค์ปี ๒๕๕๗ ในแต่ละยุทธศาสตร์เป็นไปตามเป้าหมายบางยุทธศาสตร์	ความสำเร็จตามเป้าประสงค์ปี ๒๕๕๗ ในแต่ละยุทธศาสตร์ต่ำกว่าเป้าหมายทุกยุทธศาสตร์

ชื่อปัจจัยเสี่ยง การแก้ไขปัญหาของผู้ให้บริการภายนอก (Provider) ล่าช้าและไม่มีความเสถียร

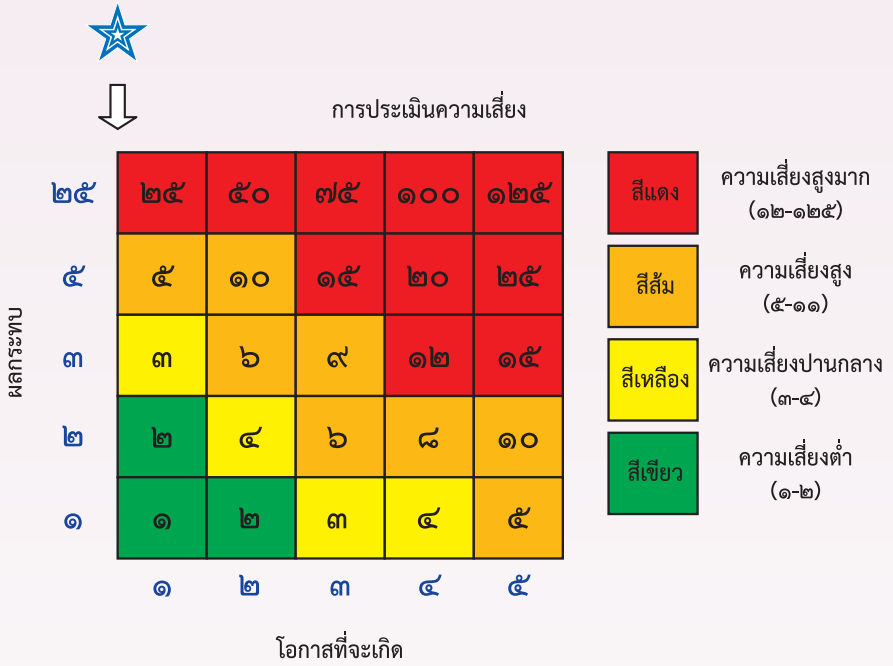
	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	มีการติดตามการแก้ไขปัญหาเป็นรายสัปดาห์ และผู้ให้บริการภายนอก (Provider) สามารถแก้ไขปัญหาจนไม่เกิดความล่าช้าและมีความเสถียร	มีการติดตามการแก้ไขปัญหาเป็นรายเดือน และผู้ให้บริการภายนอก (Provider) สามารถแก้ไขปัญหาจนไม่เกิดความล่าช้าและมีความเสถียร	มีการติดตามการแก้ไขปัญหาเป็นรายเดือน โดยผู้ให้บริการภายนอก (Provider) สามารถแก้ไขปัญหาความล่าช้าและไม่มีความเสถียรได้เพียงบางครั้ง	มีการติดตามการแก้ไขปัญหาเป็นรายเดือน โดยผู้ให้บริการภายนอก (Provider) ไม่สามารถแก้ไขปัญหาความล่าช้าและไม่มีความเสถียร	ไม่สามารถติดตามการแก้ไขปัญหากับผู้ให้บริการภายนอก (Provider) ที่ความล่าช้าและไม่มีความเสถียร
	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๕	ระดับ ๒๕
ผลกระทบ	ความพึงพอใจของผู้ใช้บริการสูงกว่าปีที่ผ่านมาร้อยละ ๑๐	ความพึงพอใจของผู้ใช้บริการสูงกว่าปีที่ผ่านมาร้อยละ ๕	ความพึงพอใจของผู้ใช้บริการเท่ากับปีที่ผ่านมา	ความพึงพอใจของผู้ใช้บริการต่ำกว่าปีที่ผ่านมาร้อยละ ๕	ความพึงพอใจของผู้ใช้บริการต่ำกว่าปีที่ผ่านมาร้อยละ ๑๐

เมื่อประเมินระดับความเสี่ยงได้แล้วขั้นต่อไปคือการจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญและจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของ สรอ. หรือหน่วยงานและสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสมโดย สรอ. ได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น ๔ ระดับตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้น ๆ ได้แก่ระดับสูงมากระดับสูงระดับปานกลางระดับต่ำตามลำดับโดยใช้ตารางแสดงระดับวัดความเสี่ยงเป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมินซึ่งตารางจะแสดงข้อมูลเป็น ๒ แกน ได้แก่แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact) ตามตารางแสดงระดับวัดความเสี่ยง

สรอ. ได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น ๔ โซน ดังแสดงในตารางดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
๑-๒	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ ซึ่งอาจมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
๓-๔	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ แต่ต้องมีมาตรการควบคุม เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำ และป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น โดยต้องจัดให้มีแผนการลดความเสี่ยงด้วย
๕-๑๑	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
๑๒ ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

โดยแสดงเป็นตาราง ๒ มิติ แสดงการแบ่งระดับความเสี่ยงทั้ง ๔ โซน ดังนี้



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้วทำให้ทราบว่าความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใดหน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการควบคุมและลดความเสี่ยงดังกล่าวที่เหมาะสมเพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้วซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดจากความเสี่ยงนั้น ๆ จะทำให้ทราบว่าความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใดหน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการควบคุมและลดความเสี่ยงดังกล่าวเพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ระดับความเสี่ยง
ระบบประเมินผลการปฏิบัติงานยังไม่มีประสิทธิภาพ	๑. กำหนดแผนงานการพัฒนาระบบประเมินผลการปฏิบัติงานของ สรอ. ๒. จัดทำระบบการประเมินผลการปฏิบัติงาน (แนวทางการประเมินผล หลักเกณฑ์การประเมินผล การเชื่อมโยงผลประเมินกับผลตอบแทน) ๓. สื่อสารระบบประเมินผลการปฏิบัติงานให้พนักงานรับทราบ ๔. นำแนวทางการประเมินผลการปฏิบัติงานไปใช้ประเมินผลกับบุคลากรในทุกระดับ ๕. ประเมินผลการปฏิบัติงานตามระบบการประเมินผลการปฏิบัติงานจริงรอบ ๑๒ เดือน	การลดความเสี่ยง (Treat)

๕.๖ กิจกรรมการควบคุม (Control Activities)

ระบบการควบคุมภายในที่มีประสิทธิภาพนับเป็นกลไกพื้นฐานสำคัญในการควบคุมและป้องกันความเสียหายที่อาจเกิดขึ้นแก่หน่วยงาน ดังนั้น เมื่อหน่วยงานได้ทำการระบุและประเมินความเสี่ยงด้านการปฏิบัติงานแล้วควรดำเนินการจัดอันดับของความเสี่ยงตามลำดับความสำคัญหรือตามความรุนแรงของผลกระทบของความเสี่ยงนั้น ๆ เพื่อหน่วยงานสามารถวางระบบการควบคุมความเสี่ยงในแต่ละประเภทซึ่งวัตถุประสงค์หลักของระบบควบคุมคือการควบคุมความเสี่ยงด้านการปฏิบัติงานให้อยู่ในระดับที่หน่วยงานและ สรอ. สามารถยอมรับได้และเพื่อให้มั่นใจว่าการดำเนินงานเป็นไปตามวัตถุประสงค์ที่หน่วยงานหรือ สรอ. ได้วางไว้รวมถึงต้องมีการติดตามและรายงานต่อคณะกรรมการบริหาร สรอ. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

อย่างไรก็ตามการพัฒนาระบบการควบคุมความเสี่ยงด้านการปฏิบัติงานที่เหมาะสมของหน่วยงานนั้นหน่วยงานควรพิจารณาถึงปัจจัยต่าง ๆ เหล่านี้ด้วย

- ความมีประสิทธิภาพของระบบการควบคุมความเสี่ยงจะต้องสามารถลดความเสี่ยงด้านการปฏิบัติงานได้อย่างชัดเจนและมีความเกี่ยวข้องโดยตรงกับสาเหตุหลักของความเสี่ยง
- ผลกระทบต่อประสิทธิภาพของการดำเนินงานโดยระบบการควบคุมความเสี่ยงที่เหมาะสมนั้น ควรสร้างผลกระทบที่น้อยที่สุดต่อระยะเวลาที่ใช้ในการปฏิบัติงาน ต้นทุน/ค่าใช้จ่ายบุคลากร และคุณภาพของงาน
- ความยากง่ายในการนำไปปฏิบัติโดยควรมีต้นทุนของการนำไปปฏิบัติต่ำและสามารถนำไปปฏิบัติได้ในเวลาที่รวดเร็ว

๕.๗ สารสนเทศและการสื่อสาร (Information and Communication)

แหล่งที่มาของข้อมูล

ส่วนบริหารความเสี่ยง เป็นหน่วยงานกลางในตามติดตามเพื่อจัดเก็บข้อมูลตามปัจจัยเสี่ยงด้านการปฏิบัติงาน ซึ่งมีรายละเอียด เช่น ตัวอย่างดังนี้

ข้อมูล	แหล่งที่มา	หมายเหตุ
○ โครงสร้างองค์กรที่มีการเปลี่ยนแปลง ○ ระบบหรือขั้นตอนที่ใช้ในการปฏิบัติงาน	○ ส่วนบริหารทรัพยากรบุคคล	○ พิจารณาจากการจัดทำโครงสร้างองค์กรฉบับปรับปรุง ○ รายละเอียดระบบหรือขั้นตอนการปฏิบัติงานที่สำคัญโดยเฉพาะโครงการหลัก
○ การเปลี่ยนแปลงทางกฎหมายและกฎระเบียบข้อบังคับต่าง ๆ	○ ส่วนกฎหมาย	○ พิจารณาจากการรายงานการเปลี่ยนแปลงทางกฎหมาย และกฎระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับ สรอ.

๕.๘ การติดตามและประเมินผล (Monitoring)

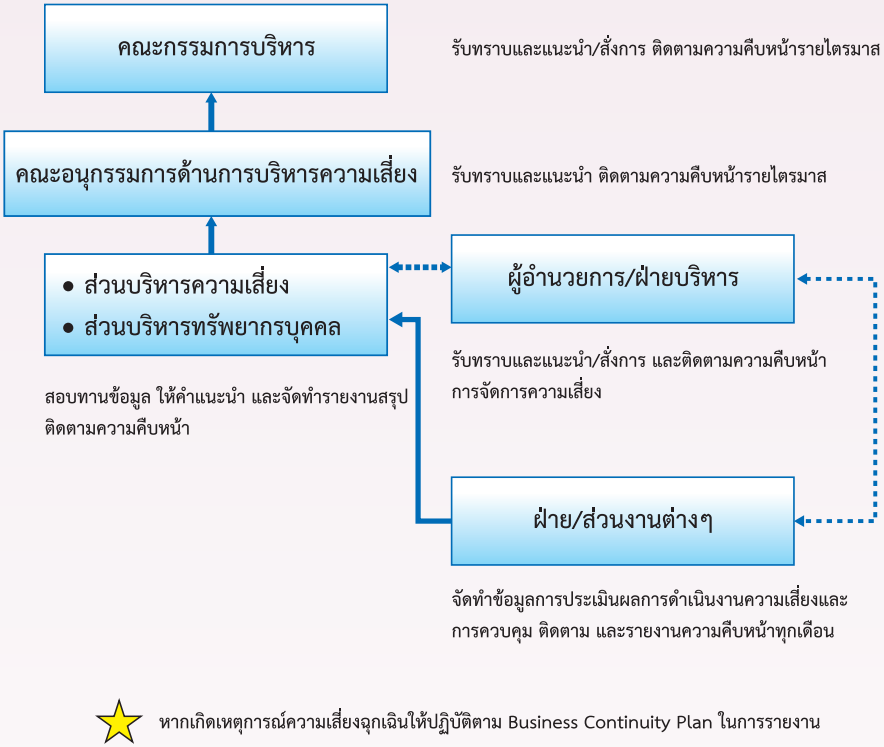
ส่วนงานที่เกี่ยวข้องและเป็นหน่วยงานเจ้าของความเสี่ยงมีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการ สรอ. และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านการปฏิบัติงานที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านการปฏิบัติงานในภาพรวมต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อคณะกรรมการบริหาร สรอ. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่องต่อไป

ทั้งนี้ หน่วยงานต้องรายงานเหตุการณ์ความเสียหายที่เกิดจากความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานทันทีหรือภายในวันทำการถัดไปและในกรณีที่ไม่มีเหตุการณ์ความเสียหายฯหน่วยงานก็ต้องรายงานให้ส่วนบริหารความเสี่ยงทราบด้วยเพื่อให้มั่นใจว่าส่วนบริหารความเสี่ยงได้รับข้อมูลที่ถูกต้องและครบถ้วนโดยข้อมูลทั้งหมดนั้นส่วนความเสี่ยงจะรวบรวมสรุปผลพร้อมวิเคราะห์จุดที่เกิดความเสี่ยง (Risk Area) เพื่อหาแนวทางในการป้องกันแก้ไขและนำเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยงหรือคณะอนุกรรมการที่เกี่ยวข้องต่อไปทั้งนี้หากมีความเสียหายฯที่มีนัยสำคัญเกิดขึ้นกับหน่วยงานหน่วยงานจะต้องมีการจัดทำ Action Plan 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 โดยต้องรายงานทั้งในกรณีที่มีความเสียหายและไม่มีความเสียหาย
Key Risk Indicator: KRI	○ การรายงาน ○ การติดตาม	ความถี่ในการติดตามและรายงาน KRI มีทั้งรายสัปดาห์ รายเดือน รายไตรมาส รายครึ่งปี และรายปี ขึ้นอยู่กับ KRI แต่ละตัว

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติส่วนยุทธศาสตร์ต้องรายงานให้ผู้บริหาร สรอ. ทราบตามลำดับความรุนแรงดังนี้

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

คู่มือบริหารความเสี่ยงด้านการเงิน
(Financial Risk Management Manual)

สารบัญ

๑. บทนำ

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) มีภารกิจดำเนินงานภายใต้ พ.ร.ฎ. จัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งต้องดำเนินงานและบริหารความเสี่ยงภายใต้ความเปลี่ยนแปลงและปรับตัวต่อผลกระทบจากสิ่งแวดล้อมภายนอก ทั้งที่มาจากปัจจัยภายในประเทศและภายนอกประเทศ ทำให้ สรอ. ต้องตระหนักและระมัดระวังในการบริหารจัดการความเสี่ยง โดยเฉพาะความเสี่ยงด้านการเงินที่มีความผันผวนและมีความอ่อนไหวต่อการเปลี่ยนแปลงจากสภาพแวดล้อมทั้งภายในและภายนอก

สรอ. เป็นหน่วยงานของรัฐที่ได้รับการจัดสรรงบประมาณเพื่อใช้ดำเนินการตามภารกิจ อีกทั้งยังสามารถจัดหารายได้เองบางส่วนจากการให้บริการด้านระบบเทคโนโลยีสารสนเทศต่าง ๆ ที่สอดคล้องตามวัตถุประสงค์ใน พ.ร.ฎ. จัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

ดังนั้น คู่มือบริหารความเสี่ยงด้านการเงินของ สรอ. นี้ จึงมุ่งเน้นถึงการสร้างความตระหนักให้เกิดแก่ทุกคนที่เกี่ยวข้องในสำนักงาน ในการที่จะช่วยสอดส่องดูแลระมัดระวังเพื่อลดความเสี่ยง หรือ บรรเทาผลกระทบจากความเสี่ยงด้านการเงิน อันเกิดจากความเสี่ยงด้านงบประมาณที่ส่งผลให้เกิดความไม่สอดคล้องกับแผนที่กำหนด เช่น การไม่ได้รับการจัดสรรงบประมาณตามแผนงานประจำปี และการบริหารการใช้จ่ายงบประมาณที่ไม่มีประสิทธิภาพ อีกทั้งความเสี่ยงด้านการเงินยังครอบคลุมถึงการดำเนินการที่ไม่เป็นไปตามแผนรายได้ประจำปี เช่น รายได้ที่ไม่เป็นไปตามแผน การบริหารลูกหนี้การค้าที่ไม่มีประสิทธิภาพ การจัดเก็บค่าบริการที่ไม่เป็นตามแผนการจัดหารายได้ ความเสี่ยงที่เกิดขึ้นดังกล่าวข้างต้นเป็นความเสี่ยงด้านการเงินที่ส่งผลต่อกระแสเงินสดรับเข้าเพื่อใช้จ่ายในการดำเนินการตามภารกิจ และอาจจะส่งผลต่อเนื่องทำให้เกิดความเสี่ยงทางด้านสภาพคล่องในการดำเนินการของ สรอ. ทำให้ สรอ. ไม่สามารถชำระหนี้สิน และภาระผูกพันต่าง ๆ ได้ ท้ายที่สุดอาจจะส่งผลต่อภาพลักษณ์ขององค์กรและทำให้องค์กรไม่สามารถดำเนินการได้ครบถ้วนสมบูรณ์ตามวัตถุประสงค์และภารกิจที่กำหนดไว้ สรอ. ส่งเสริมให้ทุกคนตระหนักถึงความสำคัญและมีส่วนร่วมในการบริหารความเสี่ยงด้านการเงิน (Financial Risk Management) โดยคณะกรรมการบริหาร สรอ. จะให้คำแนะนำและติดตาม

การรายงานการบริหารความเสี่ยง ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อวางแนวทางแก้ไขปัญหาที่เกิดจากปัจจัยเสี่ยงต่าง ๆ นอกจากนี้ยังกำหนดให้มีการดูแลและทบทวนการบริหารความเสี่ยงด้านการเงินอย่างต่อเนื่อง เพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ สรอ. ยอมรับได้

สรอ. ได้กำหนดกระบวนการบริหารความเสี่ยงด้านการเงินเพื่อให้หน่วยงานต่าง ๆ ของ สรอ. ใช้เป็นแนวทางในการจัดทำแผนกลยุทธ์และแผนธุรกิจที่สอดคล้องกับกลยุทธ์หลักของ สรอ. โดยการระบุความเสี่ยงที่อาจเกิดขึ้น แล้วทำการประเมินถึงโอกาสที่จะเกิดความเสี่ยงขึ้น รวมทั้งผลกระทบที่จะได้รับพร้อมทั้งจัดทำแนวทางหรือมาตรการควบคุมที่เหมาะสมเพื่อจัดการกับความเสี่ยงนั้นโดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่ สรอ. กำหนด

คู่มือการบริหารความเสี่ยงด้านการเงินฉบับนี้ถือเป็นส่วนหนึ่งของนโยบายการบริหารความเสี่ยงด้านการเงิน โดยจะกล่าวถึงวัตถุประสงค์ ขอบเขต โครงสร้างและบทบาทหน้าที่ของผู้รับผิดชอบกระบวนการบริหารความเสี่ยงด้านการเงิน และรายละเอียดของกระบวนการบริหารความเสี่ยงด้านการเงินเพื่อเป็นแนวทางในการปฏิบัติงานของ สรอ. และเพื่อให้หน่วยงานต่าง ๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านการเงินตนเองตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

แนวทางการบริหารความเสี่ยงที่นำมาใช้

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

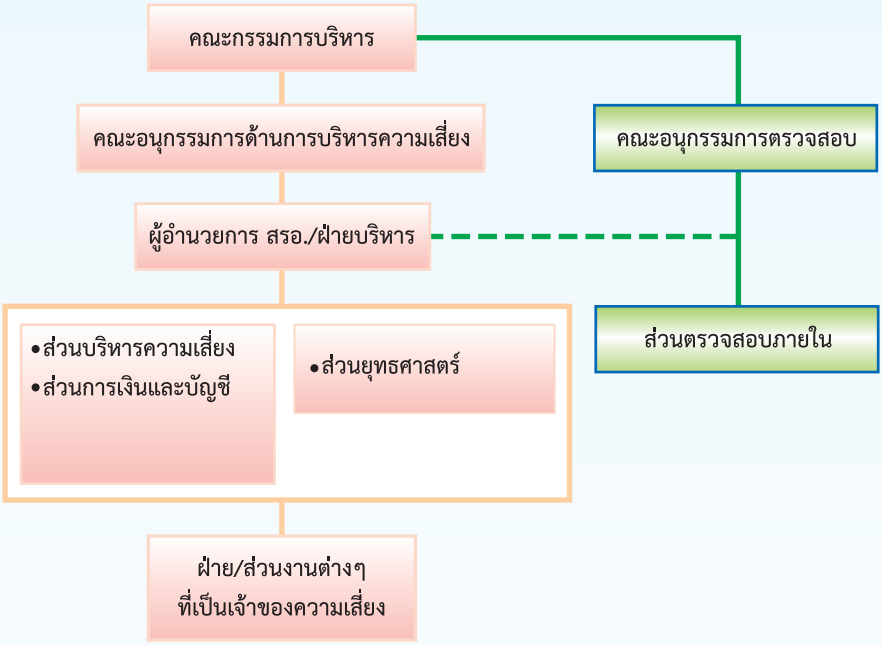
ขอบเขตของคู่มือบริหารความเสี่ยงด้านการเงิน

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านการเงิน ซึ่งครอบคลุมถึงความเสี่ยงอันเกิดจากการปฏิบัติที่ไม่เป็นไปตามแผนงบประมาณประจำปี ตั้งแต่การวางแผนงบประมาณ การของบประมาณ การได้รับอนุมัติงบประมาณจากรัฐบาล การเบิกจ่ายงบประมาณ รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้จ่ายงบประมาณที่ไม่มีประสิทธิภาพการปฏิบัติที่ไม่สอดคล้องกับกฎหมาย หรือกฎระเบียบที่เกี่ยวข้องทั้งภายในและภายนอกที่กำหนดไว้

อีกทั้งยังครอบคลุมถึงความเสี่ยงที่เกิดจากความผันผวนของอัตราแลกเปลี่ยน ความเสี่ยงที่ทำให้ สรอ. ไม่สามารถชำระหนี้และภาระผูกพันต่าง ๆ เมื่อถึงกำหนดชำระ การไม่สามารถจัดหาเงินทุนได้เพียงพอเพื่อใช้จ่ายตามภารกิจในการดำเนินการประจำปีหรือเมื่อเกิดภาวะวิกฤติ ฉุกเฉิน ความเสี่ยงที่ทำให้ สรอ. ไม่สามารถรับชำระหนี้จากการให้บริการลูกค้าอันส่งผลต่อสภาพคล่องเนื่องจากกระแสเงินสดรับเข้าไม่เป็นไปตามแผน รวมทั้งความเสี่ยงอันเกิดจากการบริหารจัดการเงินทุนที่ไม่มีประสิทธิภาพ ส่งผลให้ สรอ. เสียผลประโยชน์ต่าง ๆ ที่ควรจะได้รับ ทั้งที่เป็นไปหรือไม่เป็นไปตามแผน

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านการเงิน



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาทหน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายนโยบายและยุทธศาสตร์ มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการเงินและนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อพิจารณาอนุมัติตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านการเงินให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. จัดทำและทบทวนเพดาน หรือตัวบ่งชี้ (Trigger) ความเสี่ยงด้านการเงิน ที่เกี่ยวกับเพดานของสภาพคล่อง และหลักเกณฑ์การขออนุมัติกรณีมีการเกินเพดานหรือตัวบ่งชี้ของสภาพคล่องที่กำหนดไว้ เพื่อนำเสนอขออนุมัติต่อคณะกรรมการบริหาร สรอ.

๓. รายงานความเสี่ยงด้านการเงิน ที่แสดงถึงการปฏิบัติหรือไม่ปฏิบัติตามแนวทาง สตง. หรือ ก.พ.ร. ที่กำหนดไว้ หรือความเสี่ยงที่เกิดจากการดำเนินทางการเงินไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการและของ สรอ. และแสดงถึงความเสี่ยงด้านการเงินเปรียบเทียบกับเพดาน หรือตัวบ่งชี้ที่ได้รับอนุมัติต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

๔. จัดทำตัวแบบ Risk Model และ Stress Testing และรายงานสรุปผลเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

๕. ประเมิน ติดตาม และควบคุมความเสี่ยงด้านการเงิน ที่เกี่ยวกับสภาพคล่อง เพื่อให้มีการปฏิบัติตามนโยบายที่กำหนด

๖. จัดทำคู่มือบริหารความเสี่ยงด้านการเงินและเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๗. ประสานงานกับส่วนการเงินและบัญชี และส่วนยุทธศาสตร์เพื่อจัดให้หน่วยงานต่าง ๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการเงินที่กำหนด

๘. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทางความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านการเงิน

๙. ร่วมกับส่วนการเงินและบัญชีและส่วนยุทธศาสตร์ เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์แผนธุรกิจแผนการเงินและงบประมาณรวมของ สรอ. โดยดำเนินการต่อไปนี้

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

(๒) ติดตามผลการบริหารความเสี่ยงด้านการเงินโดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator : KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนดเพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(๓) บริหารควบคุมและจัดการความเสี่ยงด้านการเงินในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

(๔) จัดทำแผนฉุกเฉินด้านการเงิน รวมถึงทบทวนแผนปีละ ๑ ครั้ง หรือตามความเหมาะสม

ส่วนการเงินและบัญชี ฝ่ายบริหารประสิทธิภาพองค์กร มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดทำแผนการเงิน ให้สอดคล้องกับแผนกลยุทธ์แผนธุรกิจในภาพรวมของ สรอ. รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์ รวมถึงทบทวนแผนปีละ ๑ ครั้ง หรือตามความเหมาะสม

๒. รับผิดชอบในการบริหารสภาพคล่อง การบริหารโครงสร้างเงินทุน การบริหารอัตราแลกเปลี่ยนต่าง ๆ ที่เกี่ยวข้อง และรายงานสถานะการเงินด้านต่าง ๆ ของ สรอ. ต่อคณะกรรมการบริหาร

๓. รับผิดชอบในการดูแลและจัดทำแผนการลงทุนด้านการเงิน ปฏิบัติตามนโยบายการบริหารเงินลงทุนเพื่อให้เกิดผลตอบแทนและประโยชน์สูงสุดแก่องค์กร และรายงานการลงทุนด้านการเงินต่อคณะอนุกรรมการบริหารการลงทุน เพื่อรายงานคณะกรรมการบริหารต่อไป

๔. จัดทำรายงานและจัดหาข้อมูลที่เพียงพอให้แก่ส่วนบริหารความเสี่ยง เพื่อประโยชน์ในการประเมินและควบคุมความเสี่ยงด้านการเงินของ สรอ.

๕. ร่วมกับส่วนบริหารความเสี่ยง เสนอแนะวิธีการลดหรือปิดความเสี่ยงด้านการเงินให้อยู่ในระดับที่เหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ และสอดคล้องกับการปฏิบัติงานด้านการเงินและการงบประมาณที่มีอยู่ หรือที่จะได้รับต่อไป

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

๗. ร่วมกับส่วนบริหารความเสี่ยงจัดทำแผนฉุกเฉินด้านการเงินรวมถึงทบทวนแผนปีละ ๑ ครั้ง หรือตามเหมาะสม

ส่วนยุทธศาสตร์ ฝ่ายนโยบายและยุทธศาสตร์ มีหน้าที่รับผิดชอบ ดังนี้

๑. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับการงบประมาณที่กำหนดไว้ในกระบวนการบริหารความเสี่ยงด้านการเงิน

๒. ร่วมกับส่วนการเงินและบัญชีและส่วนบริหารความเสี่ยงเชื่อมโยงการบริหารความเสี่ยงด้านการเงินที่เกี่ยวข้องกับการงบประมาณเข้ากับแผนกลยุทธ์แผนธุรกิจแผนการเงินและแผนงบประมาณรวมของ สรอ.

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

๔. ติดตามผลการบริหารความเสี่ยงด้านการเงินที่เกี่ยวข้องกับการงบประมาณโดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนดเพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

๕. บริหารควบคุมและจัดการความเสี่ยงด้านการเงินที่เกี่ยวกับการงบประมาณในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

สอบทานการควบคุมภายในด้านต่าง ๆ ของ สรอ. ก่อนนำเสนอคณะอนุกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

ฝ่าย และส่วนงานต่าง ๆ ของ สรอ. มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกลยุทธ์และแผนปฏิบัติการของฝ่าย และส่วนงานต่าง ๆ ให้สอดคล้องกับแผนการเงินและการงบประมาณของ สรอ.

๒. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับฝ่ายและส่วนงานต่าง ๆ

๓. พิจารณาและประเมิน Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนการเงินและแผนงบประมาณของฝ่าย และส่วนงานต่าง ๆ ให้กับส่วนบริหารความเสี่ยง เพื่อนำไปจัดทำความเสี่ยงด้านการเงินและภาพความเสี่ยงแบบบูรณาการตามลำดับต่อไป

๔. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของฝ่ายให้กับส่วนบริหารความเสี่ยงเป็นรายเดือนหรือรายไตรมาสตามความเหมาะสม

๕. บริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงานในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๖. ดูแลติดตามการจัดการความเสี่ยงและประเมินผลการจัดการความเสี่ยงเป็นประจำเพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับรวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติมเพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๗. แต่งตั้งผู้ประสานงานด้านความเสี่ยง (Risk Officer) เพื่อประสานงานกับส่วนบริหารความเสี่ยงในการจัดทำ Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของส่วนงานและฝ่าย

๘. สื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๔.๑ ความเสี่ยงด้านการเงิน (Financial Risk)

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

หากพิจารณาความเสี่ยงด้านการเงินที่เกี่ยวข้องกับสำนักงานแล้ว อาจแยกเป็นประเภทหลัก ๆ ของความเสี่ยงด้านการเงิน ได้ดังนี้

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

โดยรายงานทางการเงินที่มีส่วนสนับสนุนในการวิเคราะห์ความเสี่ยงทางด้านการเงิน ได้แก่

งบดุล (Balance Sheet) หมายถึง งบแสดงฐานะของสำนักงาน ณ วันสิ้นรอบระยะเวลาบัญชี (วันสิ้นงวดบัญชี) โดยจัดทำขึ้นทุก ๆ รอบระยะเวลาที่กำหนดไว้ เช่น ๑ เดือน ๓ เดือน ๖ เดือนหรือ ๑ ปี โดยในส่วนของงบดุลนั้นจะแสดงความสัมพันธ์ของทรัพย์สิน หนี้สิน และส่วนของทุน

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

งบกระแสเงินสด (Cash Flow Statement) หมายถึง งบที่แสดงการเปลี่ยนแปลงเงินสดของกิจการในช่วงเวลาใดเวลาหนึ่ง เช่น รอบปีบัญชี โดยจะแสดงการได้มาและใช้ไปของเงินสดและรายการเทียบเท่าเงินสดของ ๓ กิจกรรมหลักคือ กิจกรรมดำเนินงาน กิจกรรมลงทุน และ กิจกรรมจัดหาเงิน ช่วยให้ผู้ใช้สามารถประเมินสภาพคล่องของกิจการ โดยเฉพาะความสามารถในการชำระหนี้

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

๔.๒ ที่มาของความเสี่ยงด้านการเงิน สามารถจำแนกเป็นปัจจัยเสี่ยงได้ ๒ ประเภท ดังนี้

๔.๒.๑ ปัจจัยความเสี่ยงภายนอก ได้แก่

(๑) ความเสี่ยงจากการที่ความไม่ตระหนักถึงความสำคัญของภารกิจของ สรอ. หรือการที่งบประมาณของประเทศมีจำกัด ทำให้ สรอ. ได้รับจัดสรรงบประมาณไม่สอดคล้องกับความจำเป็น และแผนงานที่กำหนดไว้

(๒) ความเสี่ยงจากการเปลี่ยนแปลงกฎระเบียบ กฎหมาย หรือกฎเกณฑ์ด้านการเงินต่าง ๆ ของรัฐบาล ที่มีผลกระทบต่อการปฏิบัติงานด้านการเงินและงบประมาณของ สรอ.

(๓) ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของสิ่งแวดล้อมภายนอกต่าง ๆ ทั้งภายในประเทศและภายนอกประเทศ ที่ทำให้เกิดความผันผวนของค่าเงิน อัตราแลกเปลี่ยน อัตราดอกเบี้ย ฯลฯ ที่มีผลกระทบต่อการบริหารด้านการเงินของ สรอ.

๔.๒.๒ ปัจจัยความเสี่ยงภายใน ได้แก่

(๑) การเปลี่ยนแปลงและความไม่ชัดเจนของนโยบายและกลยุทธ์ระดับองค์กร ซึ่งส่งผลต่อกลยุทธ์ในระดับปฏิบัติการและมีผลกระทบทั้งทางตรงและทางอ้อมต่อแผนการปฏิบัติงานด้านการเงิน และงบประมาณ

(๒) การเปลี่ยนแปลงโครงสร้างองค์กรอาจทำให้มีผลกระทบต่อค่าใช้จ่ายทางการเงินและการใช้จ่ายเงินงบประมาณของ สรอ.

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

ตัวอย่างปัจจัยเสี่ยงทางด้านการเงิน

ตัวอย่างปัจจัยเสี่ยงทางด้านการเงิน	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การเบิกจ่ายงบประมาณไม่เป็นไปตามเป้าหมาย	๑. ไม่มีการเร่งรัดให้มีการดำเนินโครงการให้เป็นไปตามแผนงานที่กำหนด ๒. ไม่มีการเร่งรัดให้มีการดำเนินการตามแผนจัดซื้อ จัดจ้าง ๓. ไม่มีการติดตาม และรายงานผลการเบิกจ่ายเงินงบประมาณต่อคณะกรรมการบริหารเป็นประจำ	✓	

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงทางการเงินนั้น จากการที่สำนักงานเป็นหน่วยงานกลางของประเทศในการผลักดันและขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ โดยมีพันธกิจคือ การพัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์ โดยมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงทางการเงิน จึงมุ่งเน้นไปที่การบริหารงบประมาณให้มีประสิทธิภาพ รวมถึงการวางแผนทางการเงินให้เหมาะสมกับการกำหนดกลยุทธ์ในแต่ละปี

อย่างไรก็ตามมีบางส่วนงานของสำนักงานที่มีหน้าที่สร้างรายได้นอกเหนือจากรายได้ตามงบประมาณ ดังนั้นความเสี่ยงทางการเงินในอีกมุมมองหนึ่งคือ รายได้นอกงบประมาณดังกล่าวไม่เป็นไปตามเป้าหมายที่กำหนด

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านการเงินอันมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามแผนบริหารงบประมาณและเงินรายได้นอกงบประมาณ การบริหารสภาพคล่อง การบริหารเงินลงทุน การกำหนดและบริหารโครงสร้างของเงินทุน การป้องกันความเสี่ยงด้านอัตราแลกเปลี่ยน และการปฏิบัติตามกฎหมายกฎระเบียบทางด้านการเงิน การงบประมาณต่าง ๆ ของทางการ

๕.๓ การระบุเหตุการณ์ (Event Identification)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร สามารถระบุเหตุการณ์ความเสี่ยงได้เป็น ๓ ประเภทหลัก ดังนี้

๑. ความเสี่ยงด้านประสิทธิภาพในการบริหารงบประมาณ

๒. ความเสี่ยงด้านการเงินและการวางแผนทางการเงิน

๓. ความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย

ความเสี่ยงด้านประสิทธิภาพในการบริหารงบประมาณ

การระบุความเสี่ยง แนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อการปฏิบัติที่ไม่เป็นไปตามแผนดำเนินงานด้านการเงินและงบประมาณประจำปี สามารถพิจารณาได้จากความถี่ในการเปลี่ยนแปลง การปรับปรุงแผนงบประมาณที่ได้รับอนุมัติจากคณะกรรมการบริหารแล้วในระหว่างปี สัดส่วนประสิทธิภาพการเบิกจ่าย การผูกพันงบประมาณต่อแผนงบประมาณรวมทั้งปี และปัจจัยต่าง ๆ ที่มีผลต่อการไม่ได้รับการจัดสรรงบประมาณจากภาครัฐตามแผนที่วางไว้

ความเสี่ยงด้านการเงินและการวางแผนทางการเงิน

การระบุความเสี่ยงด้านการบริหารสภาพคล่อง ให้ระบุประเมินจากความสามารถในการจ่ายชำระหนี้ และภาระผูกพันต่าง ๆ ความสามารถในการบริหารงบประมาณ และการบริหารลูกหนี้การค้า และโอกาสเสี่ยงที่จะเกิดหนี้สูญจากการเรียกเก็บเงินจากลูกหนี้การค้าไม่ได้ วิเคราะห์ถึงความเพียงพอของการดำรงเงินสดขั้นต่ำเพื่อใช้ในการหมุนเวียนในสำนักงานทั้งในภาวะปกติและภาวะเกิดเหตุการณ์ไม่ปกติ รวมถึงปัจจัยความเสี่ยงที่อาจส่งผลกระทบต่อกระแสเงินสดในช่วงระยะเวลาต่าง ๆ เพื่อให้ สรอ. มีการบริหารความเสี่ยงด้านการเงินที่เหมาะสม มีสภาพคล่องเพียงพอสามารถจ่ายหนี้สินและภาระผูกพันเมื่อถึงกำหนดชำระได้

การระบุความเสี่ยงที่เกิดจากการบริหารโครงสร้างของเงินทุนและการบริหารเงินลงทุน ควรวิเคราะห์และระบุปัจจัยเสี่ยงที่ส่งผลกระทบต่อแหล่งที่มาและใช้ไปของเงินทุน การระบุและประเมินสัดส่วนโครงสร้างเงินทุนที่เหมาะสม การจัดทำประมาณการงบการเงิน และงบกระแสเงินสด เพื่อวิเคราะห์ประเมินสถานะการเงิน สถานะเงินสดส่วนเกินจากการใช้หมุนเวียนในสำนักงานตามรอบระยะเวลาบัญชีนั้น ๆ และการวิเคราะห์เพื่อระบุปัจจัยต่าง ๆ ที่ส่งผลให้การบริหารการลงทุนไม่เป็นไปตามนโยบายและแผนการบริหารการลงทุนทางทั้งในระยะสั้นและระยะยาว

ความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย

การระบุความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย ให้ระบุประเมินจากเป้าหมายของสำนักงานในการสร้างรายได้นอกงบประมาณ รวมถึงแผนการตลาดที่จะรองรับในการกำหนดกลยุทธ์ในการหาหน่วยงานภาครัฐที่เป็นกลุ่มเป้าหมาย รวมถึงวิเคราะห์ถึงความต้องการของลูกค้าที่เหมาะสม พร้อมกับกำหนดทรัพยากรของสำนักงานที่ต้องการในการสนับสนุนถึงการบรรลุเป้าหมายดังกล่าว

ส่วนบริหารความเสี่ยง ส่วนการเงินและบัญชี และส่วนยุทธศาสตร์ จะร่วมกันพิจารณาวิเคราะห์ และกำหนดปัจจัยต่าง ๆ ที่มีผลกระทบต่อความเสี่ยงด้านการเงินในแต่ละช่วงเวลา ทำให้ประเมินได้ว่าในอนาคต สรอ. จะมีสภาพคล่องส่วนเกินหรือขาดในช่วงใด ซึ่งสะท้อนถึงความเสี่ยงด้านการเงินของ สรอ.

อย่างไรก็ตามส่วนบริหารความเสี่ยง ส่วนการเงินและบัญชี และส่วนยุทธศาสตร์ ยังมีการร่วมพิจารณาถึงความเสี่ยงที่เกิดจากการใช้งบประมาณที่ไม่เป็นไปตามแนวทางของ สตง. กรมบัญชีกลาง หรือ ก.พ.ร. ที่กำหนดไว้ หรือความเสี่ยงที่เกิดจากการดำเนินงานทางการเงินและงบประมาณไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการและของ สรอ.

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยงด้านการเงิน สามารถวัดได้จากประมาณการกระแสเงินสดรับและจ่ายเพื่อดูฐานะ

สภาพคล่องในแต่ละช่วงเวลาต่าง ๆ หรือการวิเคราะห์อัตราส่วนทางการเงิน เช่น อัตราส่วนเงินทุนหมุนเวียนหรืออัตราส่วนสภาพคล่อง (Current Ratio) อัตราส่วนเงินทุนหมุนเร็ว (Quick Ratio) อัตราส่วนเงินสด (Cash Ratio) เป็นต้น เพื่อทราบถึงแนวโน้มสภาพคล่องทางการเงินหรือความเป็นไปได้ที่ สรอ. จะขาดสภาพคล่องในอนาคต

ความเสี่ยงด้านการบริหารโครงสร้างเงินทุน สามารถวัดประเมินได้ด้วยการวิเคราะห์สัดส่วนระหว่างหนี้สินและทุน (Debt/Equity Ratio) เพื่อให้ทราบถึงนโยบายการจัดหาแหล่งที่มาของเงินทุนมาเพื่อใช้ในสำนักงานซึ่งต้องดูให้สอดคล้องกับนโยบายด้านการเงินเพื่อให้เกิดประสิทธิภาพในการบริหารงานสูงสุด

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

ทั้งนี้ ความเสี่ยงด้านการเงินอื่น ๆ ที่ไม่สามารถประเมินด้วยเครื่องมือทางการเงิน สามารถประเมินได้จากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือ โอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านการเงินเหล่านั้นขึ้น เป็นแต่ละเหตุการณ์ เช่น ความเสี่ยงที่เกิดจากการวิเคราะห์ข้อมูลหรือการนำข้อมูลด้านประมาณการงบการเงินไปใช้

ไม่ถูกต้อง เกิดจากสาเหตุความผิดพลาดในการประมาณการตัวเลขจากเรื่องอะไร ให้วิเคราะห์และกำหนดเป็นตัวประเมินความเสี่ยงทีละเหตุการณ์ไป เป็นต้นและควรมีการจัดทำ Sensitivity and Simulation Analysis ด้วย

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ชื่อปัจจัยเสี่ยง การเบิกจ่ายงบประมาณไม่เป็นไปตามเป้าหมาย

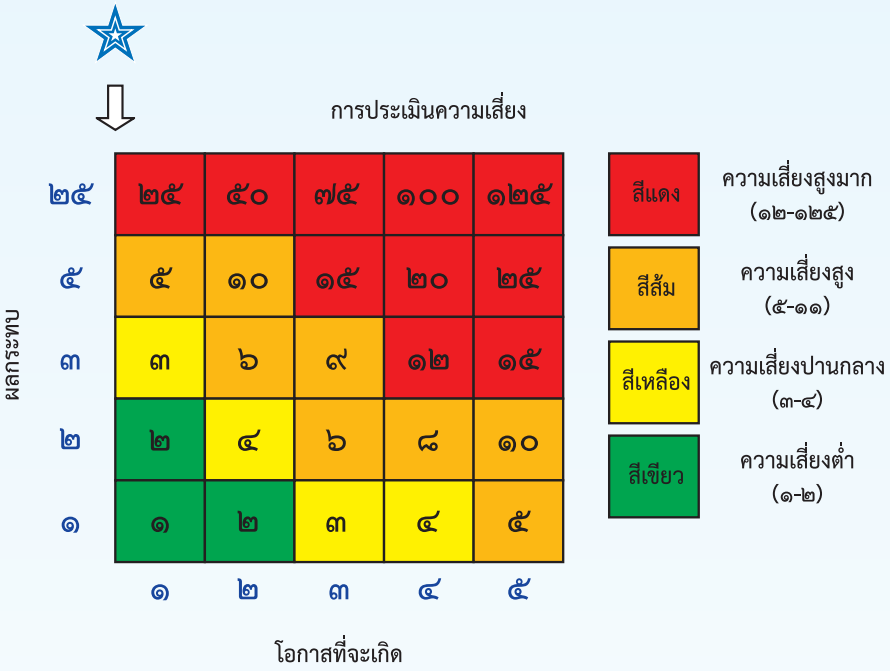
	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	เบิกจ่ายงบประมาณได้ตามเป้าหมายที่กำหนด	เบิกจ่ายงบประมาณล่าช้ากว่าแผน ๑ เดือน	เบิกจ่ายงบประมาณล่าช้ากว่าแผน ๒ เดือน	เบิกจ่ายงบประมาณล่าช้ากว่าแผน ๓ เดือน	เบิกจ่ายงบประมาณล่าช้ากว่าแผน ๔ เดือน
	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๕	ระดับ ๒๕
ผลกระทบ	การเบิกจ่ายงบประมาณร้อยละ ๙๖ - ๑๐๐	การเบิกจ่ายงบประมาณร้อยละ ๙๑ – ๙๕	การเบิกจ่ายงบประมาณร้อยละ ๘๖ – ๙๐	การเบิกจ่ายงบประมาณร้อยละ ๘๑ – ๘๕	การเบิกจ่ายงบประมาณน้อยกว่า หรือเท่ากับร้อยละ ๘๐

การประเมินตัวบ่งชี้ (Trigger) ความเสี่ยงด้านการเงิน

ตัวบ่งชี้ความเสี่ยงด้านการเงินของ สรอ. ได้มีการกำหนดและประเมินไว้ให้สอดคล้องตามนโยบายด้านการเงิน การลงทุน และการงบประมาณต่าง ๆ โดยความเห็นชอบจากคณะกรรมการบริหาร สรอ. เช่น

การกำหนดตัวบ่งชี้ความเสี่ยงด้านการเงิน โดยการดำรงเงินสดหมุนเวียนขั้นต่ำไว้เพื่อใช้จ่ายสำหรับค่าใช้จ่ายดำเนินงานประจำเดือนอย่างน้อย ๑ เดือน เป็นต้น

เมื่อประเมินระดับความเสี่ยงได้แล้วขั้นต่อไปคือการจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญและจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของ สรอ. หรือหน่วยงานและสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสมโดย สรอ. ได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น ๔ ระดับตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้น ๆ ได้แก่ ระดับสูงมาก ระดับสูงระดับปานกลางระดับต่ำตามลำดับโดยใช้ตารางแสดงระดับวัดความเสี่ยงเป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมินซึ่งตารางจะแสดงข้อมูลเป็น ๒ แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact) ตามตารางแสดงระดับวัดความเสี่ยง



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจาก สรอ. เป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

ระดับความเสี่ยงด้านการเงิน

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

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้วซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดจากความเสี่ยงนั้น ๆ จะทำให้ทราบว่าความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใดหน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการควบคุมและลดความเสี่ยงดังกล่าวเพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
การเบิกจ่ายงบประมาณไม่เป็นไปตามเป้าหมาย	๑. เร่งรัดให้มีการดำเนินโครงการให้เป็นไปตามแผนงานที่กำหนด ๒. เร่งรัดให้มีการดำเนินการตามแผนจัดซื้อจัดจ้าง ๓. ให้มีการรายงานผลการเบิกจ่ายเงินงบประมาณต่อคณะกรรมการบริหารเป็นประจำทุกเดือน ๔. กำหนดมาตรการในการเร่งรัดเพิ่มเติมในช่วงไตรมาสที่ ๒ และไตรมาสที่ ๓ เนื่องจากผลการเบิกจ่ายต่ำกว่าเป้าหมายที่กำหนด ๕. รายงานต่อคณะกรรมการ สรอ. เป็นประจำทุกเดือน	การลดความเสี่ยง (Treat)

๕.๖ กิจกรรมการควบคุม (Control Activities)

ส่วนบริหารความเสี่ยง ส่วนการเงินและบัญชี และส่วนยุทธศาสตร์ มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านการเงินโดยจะควบคุมความเสี่ยงทางด้านการเงิน ด้านการบริหารเงินลงทุน และอื่น ๆ ให้สอดคล้องกับเพดานความเสี่ยง (Risk Limit) หรือตัวบ่งชี้ความเสี่ยงด้านการเงินที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านการเงินของสำนักงานให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการบริหาร สรอ. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

๕.๗ สารสนเทศและการสื่อสาร (Information and Communication)

แหล่งที่มาของข้อมูล

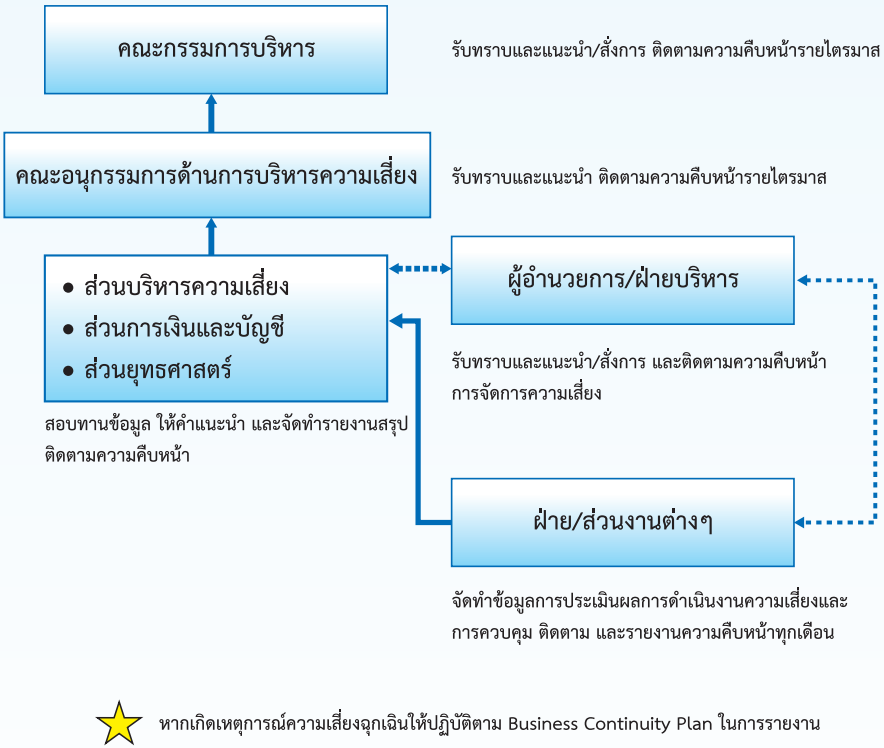
ส่วนบริหารความเสี่ยง จัดเก็บข้อมูลซึ่งมีรายละเอียด ดังนี้

ข้อมูล	แหล่งที่มา	หมายเหตุ
สถานะสภาพคล่องสุทธิ ○ ประมาณการกระแสเงินสด ○ Current Ratio ○ อัตราส่วนทางการเงิน	○ ส่วนการเงินและบัญชี	○ พิจารณาจากการจัดทำงบประมาณกระแสเงินสดด้วยวิธีทางอ้อม ○ อัตราส่วนต่าง ๆ พิจารณาจากงบแสดงสถานะการเงิน (งบดุล) และงบรายได้ค่าใช้จ่าย (งบกำไรขาดทุน)
สถานะการเบิกจ่ายงบประมาณ	○ ส่วนการเงินและบัญชี	○ พิจารณาจากการรายงานการเบิกจ่ายงบประมาณรายเดือน ○ พิจารณาจากการรายงานความคืบหน้าการติดตามโครงการที่ต้องมีการเบิกจ่ายเงินงบประมาณ
ผลการดำเนินงานของรายได้นอกงบประมาณ	○ ส่วนการเงินและบัญชี	○ ความคืบหน้าการให้บริการหน่วยงานภาครัฐ ○ การรายงานผลการดำเนินงานของรายได้นอกงบประมาณเทียบกับเป้าหมายแต่ละเดือน พร้อมรายงานถึงปัญหาอุปสรรคและแนวทางแก้ไข

๕.๘ การติดตามและประเมินผล (Monitoring)

ส่วนการเงินและบัญชี ส่วนยุทธศาสตร์ มีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการสรอ.และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านการเงินที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านการเงินในภาพรวมต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อคณะกรรมการบริหาร สรอ. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่อง ต่อไป

สรุปขั้นตอนการรายงานความเสี่ยง



ในกรณีที่เกิดเหตุการณ์ผิดปกติส่วนการเงินและบัญชีต้องแจ้งข้อมูลให้ส่วนบริหารความเสี่ยง พร้อมทั้งรายงานให้ผู้บริหาร สรอ. ทราบตามลำดับความรุนแรงดังนี้

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

คู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ
(Compliance Risk Management Manual)

สารบัญ

๑. บทนำ

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

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

คู่มือการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบฉบับนี้ถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ โดยจะกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบเพื่อใช้เป็นแนวทางในการปฏิบัติงานของ สรอ.

แนวทางการบริหารความเสี่ยงที่นำมาใช้

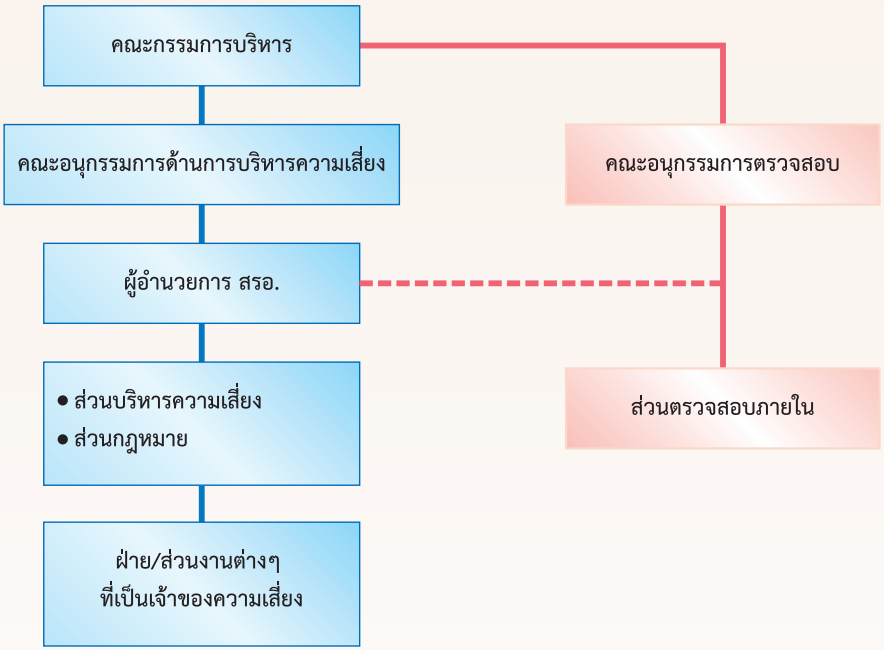
สรอ. กำหนดกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบตามแนวทางการปฏิบัติงานของ สรอ. และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Tread way Commission (COSO)

ขอบเขตของคู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบเท่านั้นโดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ เพื่อให้หน่วยงานต่าง ๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบของตนเองเพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านกฎหมาย และกฎระเบียบ



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาทหน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายนโยบายและยุทธศาสตร์ มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบและนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. ประสานงานกับหน่วยงานต่าง ๆ เพื่อให้หน่วยงานต่าง ๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบที่กำหนดในกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

๓. จัดทำคู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบและเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๔. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทางความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

๕. รวบรวมข้อมูลความเสี่ยงด้านกฎหมาย กฎระเบียบ และรายงานคณะอนุกรรมการด้านการบริหารความเสี่ยง

ส่วนกฎหมาย ฝ่ายอำนวยการ มีหน้าที่รับผิดชอบ ดังนี้

๑. พิจารณากฎระเบียบภายในต่าง ๆ ให้สอดคล้องและอยู่ภายใต้กฎหมายที่เกี่ยวข้อง

๒. ให้คำปรึกษาหน่วยงานต่าง ๆ ของ สรอ. ในการดำเนินการเพื่อให้เป็นไปตามกฎหมายกฎระเบียบ

ส่วนตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

ตรวจสอบและสอบทานการควบคุมภายในด้านต่าง ๆ ของ สรอ. ก่อนนำเสนอคณะอนุกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

ฝ่ายและส่วนงานต่าง ๆ ของ สรอ. มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดแผนปฏิบัติการของฝ่าย และส่วนงานต่าง ๆ โดยดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงที่กำหนดในกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

๒. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับฝ่ายและส่วนงานต่าง ๆ

๓. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนปฏิบัติงานฝ่าย และส่วนงานต่าง ๆ ให้กับส่วนบริหารความเสี่ยง เพื่อนำไปจัดทำแผนภาพบริหารความเสี่ยง (Risk Map) ต่อไป

๔. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของฝ่ายให้กับส่วนบริหารความเสี่ยงเป็นรายไตรมาส

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

ความเสี่ยงด้านกฎหมาย กฎระเบียบ (Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการหรือการปฏิบัติงานที่เป็นไปตามและไม่เป็นไปตามกฎหมาย และกฎระเบียบที่เกี่ยวข้อง ทำให้มีผลกระทบต่อธรรมาภิบาลและหรือต่อ สรอ. และเจ้าหน้าที่ ทั้งนี้ ความเสี่ยงด้านกฎหมาย กฎระเบียบ ยังรวมถึงความเสี่ยงจากการตีความกฎหมาย การไม่ทราบการไม่เข้าใจกฎระเบียบ ที่ไม่สอดคล้องตรงกันของหน่วยงานต่าง ๆ

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

(๒) โอกาสที่จะเกิดความเสี่ยง (Likelihood) หมายถึง ความเป็นไปได้ที่จะเกิดความเสี่ยงด้านกฎหมาย กฎระเบียบ

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

(๔) ดัชนีชี้วัดความเสี่ยง (Key Risk Indicators) หมายถึง เครื่องมือที่จะช่วยให้ผู้บริหาร สรอ. ทราบถึงระดับความเสี่ยงที่มีอยู่ในช่วงเวลาใดเวลาหนึ่งโดยอาศัยการชี้วัดจากปัจจัยเสี่ยงต่าง ๆ ที่กำหนดขึ้น

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

(๖) ระดับความเสี่ยงที่ทนได้หรือความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึงความเสี่ยงที่เกินจากความเสี่ยงที่ยอมรับได้ แต่อยู่ในช่วงกำหนดที่ทน ซึ่งจะต้องมีการจัดการทันที

(๗) ปัจจัยเสี่ยง (Risk Factor) หมายถึง เหตุการณ์หรือปัจจัยที่เป็นสาเหตุของความเสี่ยงควรเป็นสาเหตุที่แท้จริง (Root Cause) เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในอนาคตได้อย่างถูกต้อง

(๘) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ระดับของความเสี่ยงที่ สรอ. จะยอมรับได้ซึ่งในความเป็นจริงนั้น ความเสี่ยงด้านกฎหมายเกิดได้สองด้าน ได้แก่ การที่ทำตามกฎหมายแต่ไม่บรรลุวัตถุประสงค์ของแผนงานที่กำหนดไว้ กับการไม่ทำตามกฎหมายซึ่งไม่ควรมี สำหรับด้านกฎระเบียบต้องพิจารณาว่าเป็นกฎระเบียบภายใน หรือกฎระเบียบภายนอก และระดับของผลกระทบต่อ สรอ. และเจ้าหน้าที่ผู้ปฏิบัติงาน โดยจักต้องจัดทำแผนจัดการความเสี่ยงที่มีอยู่ในปัจจุบันให้ครอบคลุมความเสี่ยงทั้งหมด รวมถึงความเสี่ยงด้านธรรมาภิบาลด้วย

(๙) ความเสี่ยงคงเหลือ (Residual Risk) เป็นความเสี่ยงที่เหลืออยู่หลังจากที่ได้มีการจัดการหรือควบคุมความเสี่ยงนั้นแล้วความเสี่ยงคงเหลือจะเป็นจุดเริ่มต้นของการกำหนดระดับความเสี่ยงที่ยอมรับได้

สำหรับ สรอ. เพื่อช่วยให้องค์กรสามารถเผชิญกับความเสี่ยงจากการดำเนินกิจกรรมหรือธุรกิจได้อย่างมีประสิทธิภาพยิ่งขึ้น

การดำเนินการของ สรอ. เกี่ยวกับการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ต้องเริ่มตั้งแต่การจัดทำแผนธุรกิจแผนกลยุทธ์ของ 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. หรือหน่วยงานนั้น ๆ ในการวิเคราะห์ดังกล่าวจะทำให้สามารถระบุได้ว่า แผนงาน/โครงการ นั้น ๆ จะสามารถดำเนินงานต่อไปได้หรือไม่ หรือจักต้องปรับปรุงแผนงาน/โครงการ อย่างไร เพื่อไปสู่เป้าหมายที่กำหนดไว้

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

ส่วนกฎหมายเป็นผู้รับผิดชอบหลักในการกำหนดระดับความเสี่ยงด้านกฎหมาย กฎระเบียบ รวมถึง ธรรมาภิบาลของ สรอ. องค์กรและส่วนความเสี่ยงเป็นผู้รับผิดชอบหลักในการกำหนดวัตถุประสงค์ของการบริหารความเสี่ยงในภาพรวมของ สรอ.

ฝ่ายส่วนงานหรือโครงการต่าง ๆ เป็นผู้รับผิดชอบในการจัดการความเสี่ยงด้านกฎหมาย กฎระเบียบ เพื่อให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ที่ได้ร่วมกับส่วนกฎหมาย และส่วนบริหาร

ความเสี่ยง กำหนดไว้สำหรับงานหรือโครงการที่รับผิดชอบ พร้อมทั้งมีการรายงานความเสี่ยงตามระยะเวลาตามแต่ระดับความเสี่ยงที่ได้กำหนดไว้

๕.๓ การระบุเหตุการณ์ (Event Identification)

การระบุเหตุการณ์ความเสี่ยง จะเริ่มด้วยการแจกแจงกระบวนการปฏิบัติงาน (Work flow) เพื่อให้ได้ทราบขั้นตอนงานที่มีอยู่และจะทำให้บรรลุวัตถุประสงค์ที่กำหนดไว้แล้วจึงระบุปัจจัยเสี่ยงด้านกฎหมายกฎระเบียบที่มีผลกระทบในแต่ละขั้นตอนการปฏิบัติงานนั้น ๆ ที่อาจส่งผลต่อวัตถุประสงค์/เป้าหมายของงาน/โครงการทั้งทางตรงและทางอ้อมต่อ สรอ.

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย กฎระเบียบ

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย กฎระเบียบ	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การปฏิบัติงานไม่เป็นไปตามกฎหมาย กฎระเบียบ ข้อบังคับ และสัญญา ที่ทำไว้กับหน่วยงานภายนอก	๑. ไม่มีการเผยแพร่ระเบียบ คำสั่ง ประกาศ ของ สรอ. และหน่วยงานที่เกี่ยวข้องทั้งในอดีตและปัจจุบันที่ยังมีผลบังคับใช้ผ่านทางระบบ intranet ๒. ไม่มีการทบทวนการจัดทำระบบควบคุมภายในเพื่อให้มีความรัดกุมและมีประสิทธิภาพยิ่งขึ้น		✓
การปฏิบัติงานไม่เป็นไปตามนโยบาย ข้อบังคับ ระเบียบ คำสั่ง คู่มือการปฏิบัติงานขององค์กร	๑. พนักงานยังไม่เข้าใจกฎระเบียบขององค์กร ๒. กฎระเบียบเปลี่ยนแปลงตลอดเวลาแต่พนักงานไม่ได้ติดตามการเปลี่ยนแปลง ๓. พนักงานไม่ปฏิบัติตามอย่างเคร่งครัด	✓	

๕.๔ การประเมินความเสี่ยง (Risk Assessment)

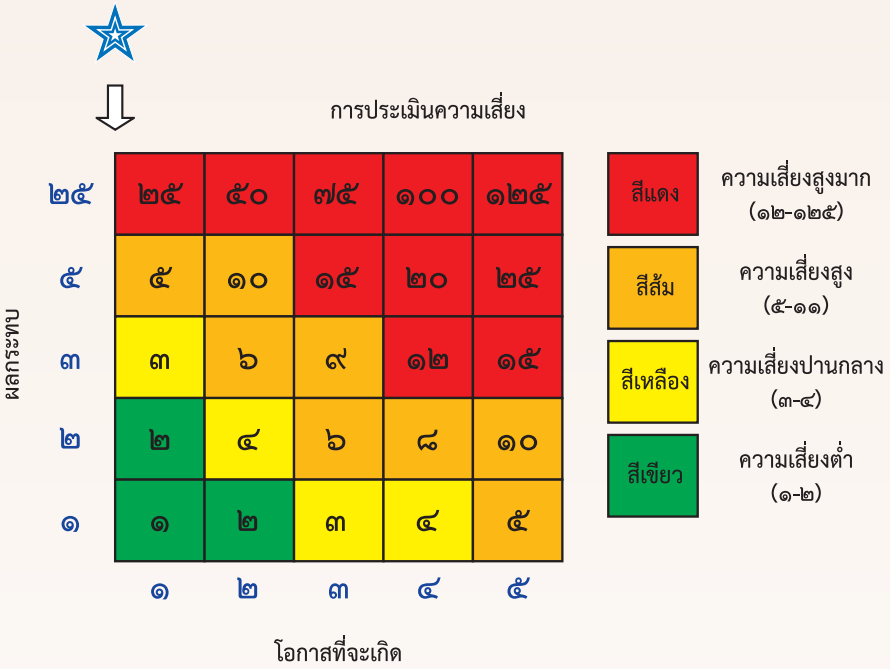
ทั้งนี้ ความเสี่ยงด้านกฎหมาย กฎระเบียบ สามารถประเมินได้จากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือ โอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านกฎหมายและกฎระเบียบเหล่านั้นขึ้น เป็นแต่ละเหตุการณ์ โดยทั่วไปความเสี่ยงด้านกฎหมายและกฎระเบียบ จะมีลักษณะการกำหนดผลกระทบที่ท้าทายมาก นั่นคือ มีเพียงระดับ ๕ ซึ่งหมายถึงการมีเหตุการณ์ที่ไม่ปฏิบัติตามกฎหมายกฎระเบียบเกิดขึ้น แม้เพียง ๑ ครั้ง และระดับ ๑ คือ ทุกธุรกรรมขององค์กรเป็นไปตามกฎหมาย และกฎระเบียบที่เกี่ยวข้อง

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ชื่อปัจจัยเสี่ยง การปฏิบัติงานไม่เป็นไปตามกฎหมาย กฎระเบียบ ข้อบังคับ และสัญญาที่ทำไว้กับหน่วยงานภายนอก

	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
โอกาส	เกิดขึ้นน้อยกว่า ๕ ครั้งต่อปี	เกิดขึ้น ๕ ครั้งต่อปี	เกิดขึ้น ๑๐ ครั้งต่อปี	เกิดขึ้น ๑๕ ครั้งต่อปี	เกิดขึ้น ๒๐ ครั้งต่อปี
	ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๕	ระดับ ๒๕
ผลกระทบ	มีการปฏิบัติตามกฎระเบียบข้อบังคับ และไม่มีการละเมิดข้อกฎหมาย	มีการไม่ปฏิบัติตามกฎระเบียบข้อบังคับและการละเมิดข้อกฎหมายที่ไม่มีนัยสำคัญ	มีการไม่ปฏิบัติตามกฎระเบียบข้อบังคับและการละเมิดข้อกฎหมายที่มีนัยสำคัญ	มีการฝ่าฝืน/ละเมิดกฎหมายสัญญาที่มีนัยสำคัญและถูกเรียกร้องค่าเสียหาย	มีการฟ้องร้องดำเนินคดีและเรียกร้องค่าเสียหายที่สำคัญ

เมื่อประเมินระดับความเสี่ยงได้แล้วขั้นต่อไปคือการจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญและจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของ สรอ. หรือหน่วยงานและสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสมโดย สรอ. ได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น ๔ ระดับตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้น ๆ ได้แก่ ระดับสูงมาก ระดับสูงระดับปานกลางระดับต่ำตามลำดับโดยใช้ตารางแสดงระดับวัดความเสี่ยงเป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมินซึ่งตารางจะแสดงข้อมูลเป็น ๒ แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact) ตามตารางแสดงระดับวัดความเสี่ยง



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)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้วซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดจากความเสี่ยงนั้น ๆ จะทำให้ทราบว่าความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใดหน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการควบคุมและลดความเสี่ยงดังกล่าวเพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่ สรอ. ยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
การปฏิบัติงานไม่เป็นไปตามกฎหมาย กฎระเบียบ ข้อบังคับ และสัญญา ที่ทำไว้กับหน่วยงานภายนอก	๑. เผยแพร่ระเบียบ คำสั่ง ประกาศของ สรอ. และหน่วยงานที่เกี่ยวข้องทั้งในอดีตและปัจจุบันที่ยังมีผลบังคับใช้ผ่านทางระบบ intranet ๒. ให้มีการทบทวนการจัดทำระบบควบคุมภายในเพื่อให้มีความรัดกุมและมีประสิทธิภาพยิ่งขึ้น ๓. เพิ่มความเข้มงวดในการตรวจสอบการปฏิบัติงานภายในองค์กรของฝ่ายตรวจสอบภายในโดยการกำกับดูแลผ่าน Audit Committee	การลดความเสี่ยง (Treat)

๕.๖ กิจกรรมการควบคุม (Control Activities)

การควบคุมเป็นเครื่องมือที่ใช้ในการจัดการกับความเสี่ยงที่มีอยู่ ดังนั้น หน่วยงานควรดำเนินการระบุการควบคุมที่มีอยู่และประเมินประสิทธิผลและความเพียงพอของการควบคุม หากไม่เพียงพอให้หน่วยงานดังกล่าวจัดทำแผนจัดการความเสี่ยงเพิ่มเติม โดยการประเมินการควบคุมสามารถจัดทำตามตาราง

๕.๗ สารสนเทศและการสื่อสาร (Information and Communication)

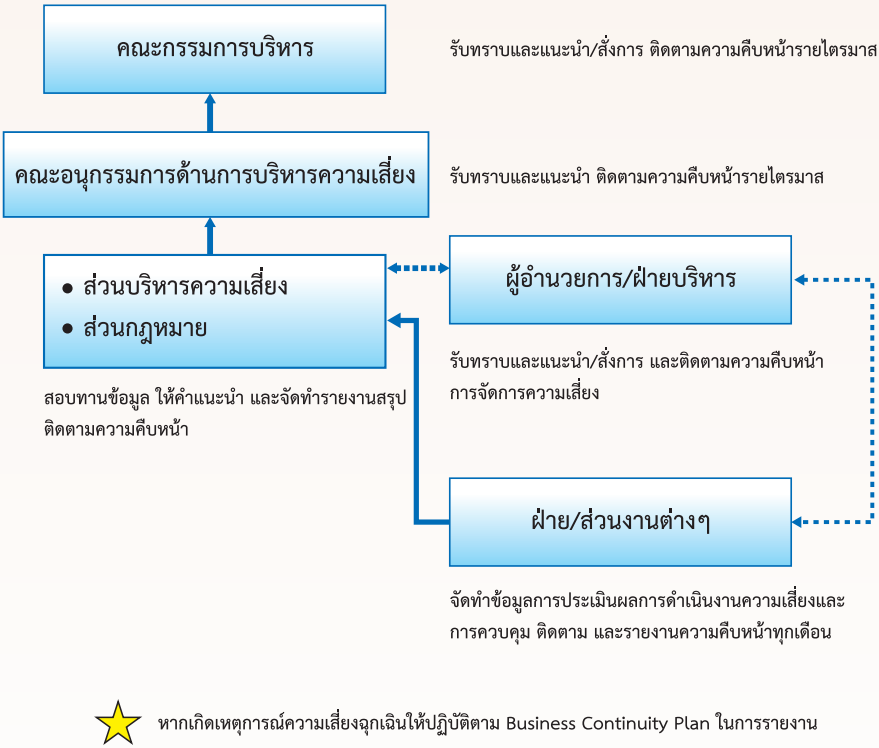
ระดับความเสี่ยงของความเสี่ยงด้านกฎหมาย กฎระเบียบ

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

๕.๘ การติดตามและประเมินผล (Monitoring)

ส่วนบริหารความเสี่ยง ส่วนกฎหมาย ต้องรายงานความเสี่ยงด้านกฎหมาย กฎระเบียบ ต่อคณะอนุกรรมการด้านการบริหารความเสี่ยงและคณะกรรมการบริหาร สรอ. เพื่อให้ทราบผลการดำเนินงานปัญหาที่เกิดขึ้นและตรวจสอบสาเหตุของปัญหาตลอดจนหาแนวทางแก้ไข เพื่อป้องกันควบคุมและลดความเสี่ยงด้านกฎหมาย กฎระเบียบตามที่กำหนดซึ่งในรายงานความเสี่ยงต้องแสดงถึงความเสี่ยงด้านกฎหมาย กฎระเบียบที่มีอยู่ และแนวทางแก้ไขระยะเวลาแล้วเสร็จอย่างชัดเจน

สรุปขั้นตอนการรายงานความเสี่ยง



คู่มือการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
(Information Technology Risk Management Manual)

สารบัญ

๑. บทนำ

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

คู่มือการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศฉบับนี้ถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศซึ่งจะใช้ประกอบกับคู่มือเฉพาะของแต่ละเครื่องมือที่ใช้ในการบริหารความเสี่ยงซึ่งจะกล่าวลงไปในรายละเอียดเพื่อให้หน่วยงานสามารถวางระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศภายในหน่วยงานของตนเองได้อย่างมีประสิทธิภาพและเป็นการป้องกันควบคุมและลดผลกระทบจากเหตุการณ์ความเสียหายที่อาจเกิดขึ้นต่อ สรอ. โดยกระบวนการดังกล่าวจะอยู่ภายใต้การดูแลของหัวหน้าหน่วยงานฝ่ายบริหารและมีการกำกับ ดูแลและสั่งการโดยคณะกรรมการบริหาร สรอ. ผ่านทางคณะอนุกรรมการด้านการบริหารความเสี่ยง

แนวคิดเกี่ยวกับการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๑. การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศจะอยู่บนพื้นฐานของการควบคุมภายในซึ่งเป็นกระบวนการที่เป็นขั้นตอนที่ต่อเนื่องและแทรกอยู่ในการปฏิบัติงานตามปกติของทุกหน่วยงาน

๒. เจ้าหน้าที่ในทุกหน่วยงานของ สรอ. มีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศซึ่งมีผู้บริหารเป็นผู้รับผิดชอบให้มีระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศตามที่ สรอ. กำหนดคือมีการระบุประเมินติดตามควบคุมและรายงานความเสี่ยง

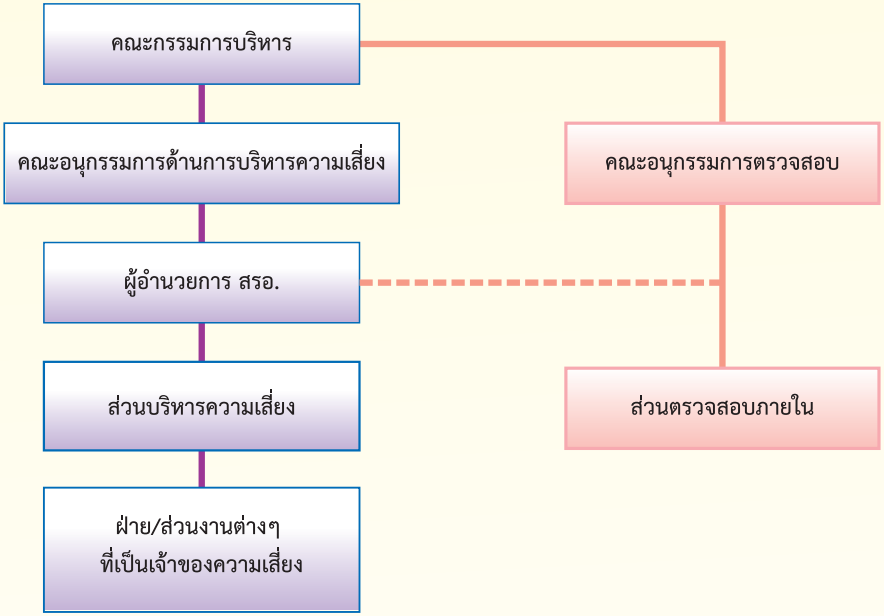
๓. การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศควรให้ความมั่นใจอย่างสมเหตุสมผลว่าหน่วยงานจะบรรลุตามเป้าหมายที่ได้กำหนดไว้กล่าวคือแม้ว่าจะมีการวางระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศไว้ดีเพียงใดก็ไม่สามารถรับรองได้ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้อย่างสมบูรณ์เพราะมีข้อจำกัดจากปัจจัยอื่นนอกเหนือการควบคุมของหน่วยงาน เช่น ผลกระทบจากปัจจัยภายนอกเป็นต้น

ขอบเขตของคู่มือบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศซึ่งเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยง สรอ. โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศเพื่อให้หน่วยงานต่าง ๆ ของ สรอ. ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของตนเองเพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



๓. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาทหน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายนโยบายและยุทธศาสตร์ มีหน้าที่รับผิดชอบ ดังนี้

๑. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และนำเสนอต่อคณะกรรมการบริหาร สรอ. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๒. รายงานความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ที่แสดงถึงการปฏิบัติหรือไม่ปฏิบัติตามนโยบายที่กำหนดไว้

๓. ประเมิน ติดตาม และควบคุมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ที่เกี่ยวกับสภาพคล่อง เพื่อให้มีการปฏิบัติตามนโยบายที่กำหนด

๔. ประสานงานกับหน่วยงานต่าง ๆ ที่เป็นเจ้าของความเสี่ยงเพื่อให้หน่วยงานต่าง ๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่กำหนด

๕. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทางความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๖. บริหารควบคุมและจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

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

ฝ่ายและส่วนงานต่าง ๆ ของ สรอ. มีหน้าที่รับผิดชอบ ดังนี้

๑. กำหนดกลยุทธ์และแผนปฏิบัติงานของฝ่าย และส่วนงานต่าง ๆ ให้สอดคล้องกับนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๒. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับฝ่ายและส่วนงานต่าง ๆ

๓. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance ให้กับส่วนบริหารความเสี่ยง เพื่อนำไปจัดทำความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและภาพความเสี่ยงแบบบูรณาการตามลำดับต่อไป

๔. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของฝ่ายให้กับส่วนบริหารความเสี่ยงเป็นรายเดือนหรือรายไตรมาสตามความเหมาะสม

๕. จัดทำแผนจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Treatment Plan) ของฝ่ายและส่วนงานต่าง ๆ และบริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงานในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

๖. ดูแลติดตามการจัดการความเสี่ยงและประเมินผลการจัดการความเสี่ยงเป็นประจำเพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับรวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติมเพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้

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

๘. สื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

ส่วนตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

สอบทานการควบคุมภายในด้านต่าง ๆ ของ สรอ. ก่อนนำเสนอคณะอนุกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำการสอบทานความเสี่ยงควรพิจารณาแผนจัดการความเสี่ยงของฝ่ายและส่วนงานต่าง ๆ ว่ามีความเหมาะสมหรือไม่ และให้ข้อคิดไว้ในการปรับปรุงหรือแก้ไขตามสมควร

การสอบทานควรรวมถึงการติดตามว่ามีการดำเนินตามแผนการจัดการความเสี่ยงหรือไม่ และสถานการณ์ดำเนินการว่าอยู่ในระดับใด

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้มีการนำมาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็นมาตรฐานที่กำลังได้รับความนิยมอย่างแพร่หลายในปัจจุบัน และกล่าวถึงข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS (Information Security Management System) ให้กับองค์กรซึ่งวัตถุประสงค์ของมาตรฐานนี้เพื่อให้องค์กรสามารถบริหารจัดการทางด้านความปลอดภัยได้อย่างมีระบบและเพียงพอเหมาะสมต่อการดำเนินธุรกิจขององค์กรมาร่วมกำหนดเป็นประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วย โดยสามารถกำหนดกรอบการบริหาร ดังนี้

๔.๑ ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk)

ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk) คือ ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำระบบเทคโนโลยีสารสนเทศมาใช้ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน ทั้งนี้ ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ จะมีองค์ประกอบที่สำคัญ ๓ ประการ ได้แก่ แผนงานการใช้ระบบเทคโนโลยีสารสนเทศ การตัดสินใจในการนำเทคโนโลยีสารสนเทศมาใช้ และการวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายในระบบงานเหตุการณ์ภายนอกหรือคน (เจ้าหน้าที่บุคคลภายนอกหรือลูกค้า) ซึ่งส่งผลกระทบต่อการดำเนินงานของ สรอ.

๔.๒ ประเภทของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Type of Risk)

สามารถจำแนกออกได้เป็น ๘ ประเภท ดังนี้

๔.๒.๑ ความเสี่ยงด้านข้อมูล (Information Risk) หมายถึง ความเสี่ยงที่เกิดจากข้อมูลต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาดโดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้เกิดการฟ้องร้องได้หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้โดยความเสี่ยงนี้อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์

และป้องกันความเสียหายอย่างเพียงพอ 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 ที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการและเหมาะสมกับงบประมาณ หรือความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงจากการที่เทคโนโลยีสารสนเทศหมดอายุไปเอง ความเสี่ยงจากการไม่ได้กำหนดหรือกำหนดกระบวนการอนุมัติใช้อุปกรณ์เทคโนโลยีสารสนเทศไม่ชัดเจน

๔.๒.๓ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากการเลือกใช้หรือความเสี่ยงจากการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ไม่หวังดีทำลายระบบ (Hacker) การควบคุมการ Reversionsoftware ไม่เพียงพอการที่ 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 ในเรื่องของการกำหนดโครงสร้างการมอบหมายงานในหน้าที่ให้แก่บุคลากรด้านระบบเทคโนโลยีสารสนเทศ ที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดระบบเทคโนโลยีสารสนเทศและสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ 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 บริษัท ทีโอที จำกัด (มหาชน) และ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) ความเสี่ยงที่ผู้ดูแลระบบไม่มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่าง ๆ ที่ส่งผ่านทางเครือข่าย เป็นต้น

๔.๒.๗ ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) เพื่อจัดทำโครงการด้านระบบเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้ เป็นต้น

๔.๒.๘ ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) หมายถึง ความเสี่ยงที่เกิดจากกระบวนการทำงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ซึ่งส่งผลให้ขาดการนำ Best Practice ที่ดีต่าง ๆ มาใช้งาน COBIT 5 ได้กำหนดกระบวนการที่เป็นมาตรฐานที่ดีต่าง ๆ ไว้จำนวน ๓๗ กระบวนการ และ กำหนด Best Practice ของกระบวนการต่าง ๆ ไว้ให้ เช่นกันการขาดการนำ Best Practice เหล่านั้นมาใช้งานจะทำให้องค์กรไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่มาตรฐานดังกล่าวได้กำหนดไว้ COBIT 5 ได้กำหนดเป้าหมายทางธุรกิจสำหรับการนำเทคโนโลยีสารสนเทศมาใช้งานไว้จำนวน ๑๗ เป้าหมาย

๕. องค์ประกอบการบริหารความเสี่ยง

๕.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment)

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

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

ทั้งนี้ การวิเคราะห์สภาพแวดล้อมต้องคำนึงถึงปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อ สรอ. หรือหน่วยงานที่เกี่ยวข้องกับนโยบายหลัก เนื่องจากการวิเคราะห์ถึงสภาพแวดล้อมทั้งภายในและภายนอก (SWOT Analysis) จะทำให้ สรอ. ทราบถึงปัจจัยเสี่ยงที่จะส่งผลกระทบต่อความสำเร็จของ สรอ. ช่วยให้ สรอ. ทราบว่าต้องบริหารจัดการอย่างไรเพื่อสร้างเสถียรภาพ ความมั่นคง และความน่าเชื่อถือของระบบเทคโนโลยีสารสนเทศเมื่อต้องเผชิญกับสภาพการเปลี่ยนแปลงที่รวดเร็ว

๕.๒ การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านระบบเทคโนโลยีสารสนเทศมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามแผนงานโครงการของระบบสารสนเทศ

หรือการปฏิบัติตามกฎหมาย กฎระเบียบต่าง ๆ ที่จะส่งผลต่อการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร คณะกรรมการกิจการกระจายเสียง 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/IEC27001 หรือ ของ COBIT5 เป็นต้น

(๓) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

(๔) การวิเคราะห์กระบวนการทำงานด้านเทคโนโลยีสารสนเทศเมื่อเทียบกับกระบวนการของมาตรฐานสากลเช่น COBIT5, ITIL, CMMI เป็นต้น

ตัวอย่าง การระบุความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ภัยคุกคาม	ช่องโหว่
ความเสี่ยงด้านข้อมูล	เมื่อเกิดเหตุภัยพิบัติต่าง ๆ กับผู้ให้บริการ อาจไม่สามารถนำข้อมูลสำรองของระบบที่ผู้ให้บริการจัดเก็บมาใช้งานได้	ไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่ (Backup Site)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	เหตุการณ์หรือสถานการณ์ภายนอกส่งผลให้เกิดไฟไหม้อาคารสำนักงาน	อาคารสำนักงานตั้งอยู่ในพื้นที่ใกล้ชุมชนหรือแหล่งเชื้อเพลิงซึ่งเสี่ยงต่อการเกิดไฟไหม้
ความเสี่ยงด้านบุคลากร	ข้อมูล Log อาจถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต ก่อนที่ข้อมูล Log จะผ่านการ Hash	พนักงานซึ่งทำหน้าที่เป็นผู้ดูแล Centralized Log มีหน้าที่ในการดูแลอุปกรณ์อื่น ๆ ด้วย โดยได้รับสิทธิเป็นผู้ดูแลระบบ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	อุปกรณ์ของระบบ Cloud ของผู้ให้บริการไม่สามารถใช้งานได้ ทำให้เกิดผลกระทบกับสัญญาที่ทำไว้กับลูกค้า	ขาดการจัดทำหรือทบทวนสัญญา Maintenance Agreement (MA) กับทาง Supplier
ความเสี่ยงด้านผู้ให้บริการภายนอก	ระบบที่มีการเชื่อมโยงกับผู้ให้บริการหลายรายไม่สามารถเชื่อมโยงกันได้ทำให้เกิดการหยุดชะงัก	ขาดการกำหนดไว้ในสัญญาการให้บริการว่าผู้ให้บริการต้องสามารถ Interoperate กันได้

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)

ประเภทความเสี่ยง	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	๑ = น้อยมาก	๒ = น้อย	๓ = ปานกลาง	๕ = สูง	๒๕ = สูงมาก
ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร (Reputation)	กระทบชื่อเสียงขององค์กรน้อยมากหรือไม่กระทบ	กระทบชื่อเสียงขององค์กรน้อยภายในกลุ่มงาน	กระทบชื่อเสียงขององค์กร ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	กระทบชื่อเสียงขององค์กร ทำให้เกิดความไม่พอใจจากผู้มีส่วนได้ส่วนเสีย (Stakeholder)	กระทบชื่อเสียงขององค์กรมาก ทำให้เกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ
ผลกระทบต่อองค์กรด้านการเงิน (Finance)	เกิดเหตุร้ายที่ไม่มีความสำคัญ อาจประเมินมูลค่าความเสียหายไม่เกิน ๑๐๐,๐๐๐ บาท	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้ อาจประเมินมูลค่าความเสียหายมากกว่า ๑ แสนบาท แต่ไม่เกิน ๑ ล้านบาท	ระบบมีปัญหาและมีความสูญเสียไม่มากอาจประเมินมูลค่าความเสียหายมากกว่า ๑ ล้านบาท แต่ไม่เกิน ๑๐ ล้านบาท	เกิดปัญหากับระบบที่สำคัญและระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูล บางส่วนอาจประเมินมูลค่าความเสียหายมากกว่า ๑๐ ล้านบาท แต่ไม่เกิน ๑๐๐ ล้านบาท	เกิดความสูญเสียต่อระบบที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ อาจประเมินมูลค่าความเสียหายมากกว่า ๑๐๐ ล้านบาท
การดำเนินงาน (Operation)	การดำเนินงานมีปัญหาที่แต่ไม่เป็นนัยสำคัญและสามารถแก้ไขได้ ทันที	การดำเนินงานมีปัญหาเล็กน้อยแก้ไขได้ในระดับกลุ่มงาน	การดำเนินงานมีปัญหาและส่งผลให้เกิดการหยุดชะงักของดำเนินงานภายใน	การดำเนินงานมีปัญหาและส่งผลกระทบต่อระบบที่สำคัญ หยุดชะงักบางระบบอาจส่งผลต่อผู้รับบริการในวงกว้าง	การดำเนินงานมีปัญหาจนทำงานไม่ได้และก่อผลกระทบต่อการทำงานของระบบสำคัญทั้งหมด ส่งผลต่อผู้รับบริการในวงกว้าง

ประเภทความเสี่ยง	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	๑ = น้อยมาก	๒ = น้อย	๓ = ปานกลาง	๕ = สูง	๒๕ = สูงมาก
ด้านกฎหมายหรือระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม (Compliance)	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร โดยไม่เกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญและไม่เกิดความเสียหายต่อองค์กรหรือบุคคลอื่น	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร และเกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญ แต่ไม่เกิดความเสียหายต่อองค์กรหรือบุคคลอื่น	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร ซึ่งเกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญและเกิดความเสียหายเพียงเล็กน้อยต่อองค์กรหรือบุคคลอื่น	ปฏิบัติหรือละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญและเกิดความเสียหายอย่างร้ายแรงต่อองค์กรหรือบุคคลอื่น	ปฏิบัติหรือละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญและเกิดความเสียหายอย่างร้ายแรงต่อองค์กรหรือบุคคลอื่นโดยปรากฏเป็นข่าวในสื่อสาธารณะที่ก่อให้เกิดความเสียหายต่อชื่อเสียงหรือภาพลักษณ์ขององค์กร

จากตารางที่เสนอในข้างต้น สรอ. ได้กำหนดค่าระดับความเสี่ยงไว้ ดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ความรุนแรงของเหตุการณ์

ในการพิจารณาความรุนแรงของเหตุการณ์จะต้องพิจารณาจากผลกระทบทั้ง ๔ ด้านร่วมกัน เช่น หากความเสี่ยงเรื่องไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่จะมีผลกระทบแต่ละด้าน ได้แก่

๑. ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กรมีผลกระทบในระดับใด

๒. ผลกระทบต่อองค์กรด้านการเงินมีผลกระทบในระดับใด

๓. การดำเนินการทางธุรกิจมีผลกระทบในระดับใด

๔. ด้านกฎหมาย ระเบียบ ข้อบังคับอื่น ๆ ที่องค์กรต้องปฏิบัติตามมีผลกระทบในระดับใด

และใช้ค่าผลกระทบที่มากที่สุดของผลกระทบทั้ง ๔ ด้าน เป็นค่าระดับความรุนแรงของเหตุการณ์

ตัวอย่างเช่น ความเสี่ยงเรื่องไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่เมื่อพิจารณาจากโอกาสการเกิดขึ้นของความเสี่ยงในตารางจะมีค่าเท่ากับ ๒ และระดับความรุนแรงของผลกระทบแต่ละด้านคือ

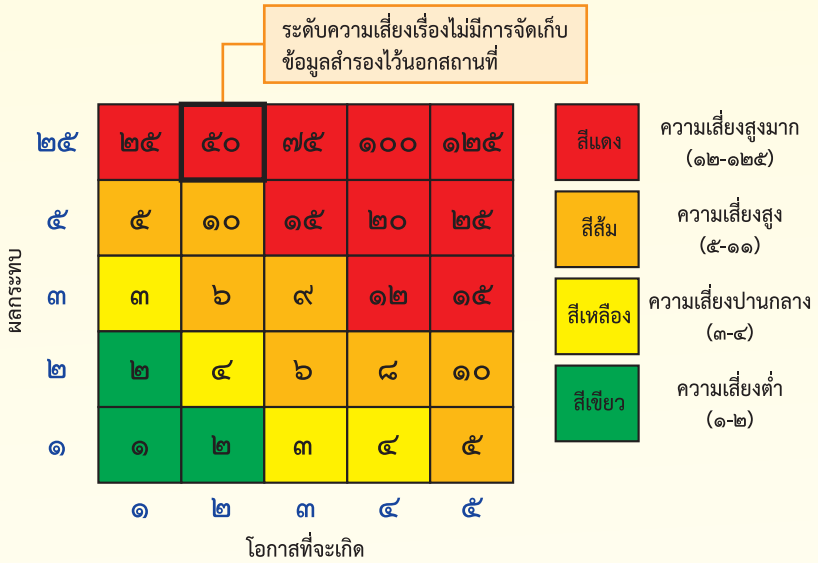
๑. ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กรมีผลกระทบในระดับ ๒๕

๒. ผลกระทบต่อองค์กรด้านการเงินมีผลกระทบในระดับ ๒๕

๓. การดำเนินการทางธุรกิจมีผลกระทบในระดับ ๒๕

๔. ด้านกฎหมาย ระเบียบ ข้อบังคับอื่น ๆ ที่องค์กรต้องปฏิบัติตามมีผลกระทบในระดับ ๓

ดังนั้น ระดับความรุนแรงของผลกระทบมากที่สุดจะมีค่าเท่ากับ ๒๕ ทำให้ระดับความเสี่ยงเรื่องไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่จึงเท่ากับ ๕๐ ตามตาราง ๒ มิติ แสดงระดับความเสี่ยงสำหรับทุกค่าที่เป็นไปได้คือ



จากการพิจารณาค่าระดับความเสี่ยงในตารางข้างต้น สรอ. ได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น ๔ โซน ดังแสดงในตารางดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
๑-๒	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ ซึ่งอาจมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
๓-๔	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ แต่ต้องมีมาตรการควบคุมเพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำ และป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น โดยต้องจัดให้มีแผนการลดความเสี่ยงด้วย
๕-๑๑	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
๑๒ ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

ตัวอย่าง การประเมินระดับความเสี่ยงแสดงดังตารางต่อไปนี้

ประเภทความเสี่ยง	ภัยคุกคาม	ช่องโหว่	โอกาสในการเกิดเหตุการณ์	ความรุนแรงของเหตุการณ์	ระดับความเสี่ยง
ความเสี่ยงด้านข้อมูล	เมื่อเกิดเหตุภัยพิบัติต่าง ๆ กับผู้ให้บริการอาจไม่สามารถนำข้อมูลสำรองของระบบ Cloud ที่ผู้ให้บริการจัดเก็บมาใช้งานได้	ไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่ (Backup Site)	๒	๒๕	๕๐
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	เหตุการณ์หรือสถานการณ์ภายนอกส่งผลให้เกิดไฟไหม้อาคารสำนักงาน	อาคารสำนักงานตั้งอยู่ในพื้นที่ใกล้ชุมชนหรือแหล่งเชื้อเพลิงซึ่งเสี่ยงต่อการเกิดไฟไหม้	๒	๒๕	๕๐
ความเสี่ยงด้านบุคลากร	ข้อมูล Log อาจถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต ก่อนที่ข้อมูล Log จะผ่านการ Hash	พนักงานซึ่งทำหน้าที่เป็นผู้ดูแล Centralized Log มีหน้าที่ในการดูแลอุปกรณ์อื่น ๆ ด้วย โดยได้รับสิทธิเป็นผู้ดูแลระบบ	๑	๓	๓
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	อุปกรณ์ของระบบ Cloud ของผู้ให้บริการไม่สามารถใช้งานได้ ทำให้ เกิดผลกระทบกับสัญญาที่ทำไว้กับลูกค้า	ขาดการจัดทำหรือทบทวนสัญญา Maintenance Agreement (MA) กับทาง Supplier	๑	๓	๓
ความเสี่ยงด้านผู้ให้บริการภายนอก	ระบบที่มีการเชื่อมโยงกับผู้ให้บริการหลายรายไม่สามารถเชื่อมโยงกันได้ทำให้เกิดการหยุดชะงัก	ขาดการกำหนดไว้ในสัญญาการให้บริการว่าผู้ให้บริการต้องสามารถ Interoperate กันได้	๑	๒๕	๒๕

๕.๕ การตอบสนองความเสี่ยง (Risk Response)

ในการควบคุมและบรรเทาความเสี่ยง จะขึ้นอยู่กับค่าระดับความเสี่ยงที่ประเมินและได้ค่ามานั้น ทางเลือกในการควบคุมหรือบรรเทาความเสี่ยงจะมีด้วยกัน ๔ ทางเลือก ดังนี้

๕.๕.๑ การยอมรับความเสี่ยง (Acceptance) กรณีที่ค่าระดับความเสี่ยงอยู่ในบริเวณสีเขียว ผู้ประเมินความเสี่ยงสามารถยอมรับความเสี่ยงได้ กรณีการยอมรับความเสี่ยงยังหมายรวมถึง

- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเหลือง สีส้ม หรือ สีแดง ก็ตาม แต่หน่วยงานหรือสำนักงานยังไม่สามารถระบุมาตรการที่เหมาะสมได้ จึงอาจต้องยอมรับความเสี่ยงไว้ก่อน ในภายหลังเมื่อได้มาตรการที่เหมาะสมแล้ว จึงเสนอมาตรการเพื่อหาทางลดความเสี่ยงให้ลดลงมาอยู่ในระดับสีเขียว เป็นต้น
- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเหลือง สีส้ม หรือ สีแดงแต่หน่วยงานหรือสำนักงานพบว่าการจะจัดการกับความเสี่ยงนี้จะมีค่าใช้จ่ายที่ค่อนข้างสูงและไม่คุ้มค่าที่จะลงทุน จึงเห็นสมควรให้ยอมรับความเสี่ยงและไม่ดำเนินการใด ๆ

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. เช่นการใช้ Outsource เรื่องการพัฒนาระบบให้หน่วยงานภายนอกโดยการทำสัญญาดูแลรักษาฮาร์ดแวร์ อุปกรณ์เครือข่าย การซื้อประกันภัยจากหน่วยงานภายนอก

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

สำหรับกรณีการซื้อประกันภัย หน่วยงานหรือฝ่ายควรจัดการกับความเสี่ยงนั้นในระดับหนึ่ง แต่อาจจะยังไม่เพียงพอ จึงเสริมด้วยการซื้อประกัน หากเหตุการณ์ความเสี่ยงยังคงเกิดขึ้นได้ สรอ. จะไม่เสียหายมากเกินไป ทั้งนี้เนื่องจากมีการจัดการไว้ในระดับหนึ่ง

๕.๕.๔ การลดความเสี่ยง (Reduction) คือ การหาทางลดค่าความเสี่ยงที่อาจตกอยู่ในบริเวณสีเหลือง สีส้ม หรือ สีแดงก็ตาม ให้ลงมาอยู่ในระดับที่น้อยลง

กรณีที่หน่วยงานหรือฝ่ายสามารถลดความเสี่ยงลงมาอยู่ในบริเวณสีเขียวได้ หน่วยงานสามารถยอมรับความเสี่ยงได้ และไม่ต้องทำอะไรเพิ่มเติม แต่หากอยู่ในบริเวณสีเหลือง หน่วยงานยังต้องคอยคุมความเสี่ยงไว้ (เพื่อป้องกันการเลื่อนระดับไปสู่ระดับที่สูงขึ้น)

เมื่อมีการประเมินระดับความเสี่ยงในหัวข้อที่แล้ว หน่วยงานหรือฝ่ายต้องพิจารณาค่าระดับความเสี่ยงนั้นและตัดสินใจว่าจะใช้ทางเลือกใด (จาก ๑ ใน ๔ ทางเลือก) เพื่อจัดการกับความเสี่ยงที่ประเมินนั้น ซึ่งได้อธิบายวิธีการใช้ทางเลือกแต่ละทางเลือกไปแล้วในข้างต้น

๕.๖ กิจกรรมการควบคุม (Control Activities)

ส่วนบริหารความเสี่ยง และหน่วยงานที่เกี่ยวข้องหรือเป็นเจ้าของความเสี่ยง มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ โดยจะควบคุมความเสี่ยงให้สอดคล้องกับระดับความเสี่ยง ที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการบริหาร สรอ. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

๕.๗ การรายงานความเสี่ยง (Risk Reporting)

ทุกหน่วยงานของ สรอ. ต้องมีการจัดทำรายงานการประเมินการควบคุมความเสี่ยงด้วยตนเอง (Risk and Control Self-Assessment หรือ RCSA) อย่างน้อยปีละ ๑ ครั้งโดยจุดที่มีความเสี่ยงอยู่ในระดับที่มีนัยสำคัญและระดับสูงจะต้องมีการจัดทำ Action Plan เพื่อปิดความเสี่ยงที่เกิดขึ้นกับหน่วยงานต่อไป

ในกรณีที่มีความความเสียหายที่เกิดจากความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Operational Loss Data) หน่วยงานต้องรายงานเหตุการณ์ความเสียหายที่เกิดจาก

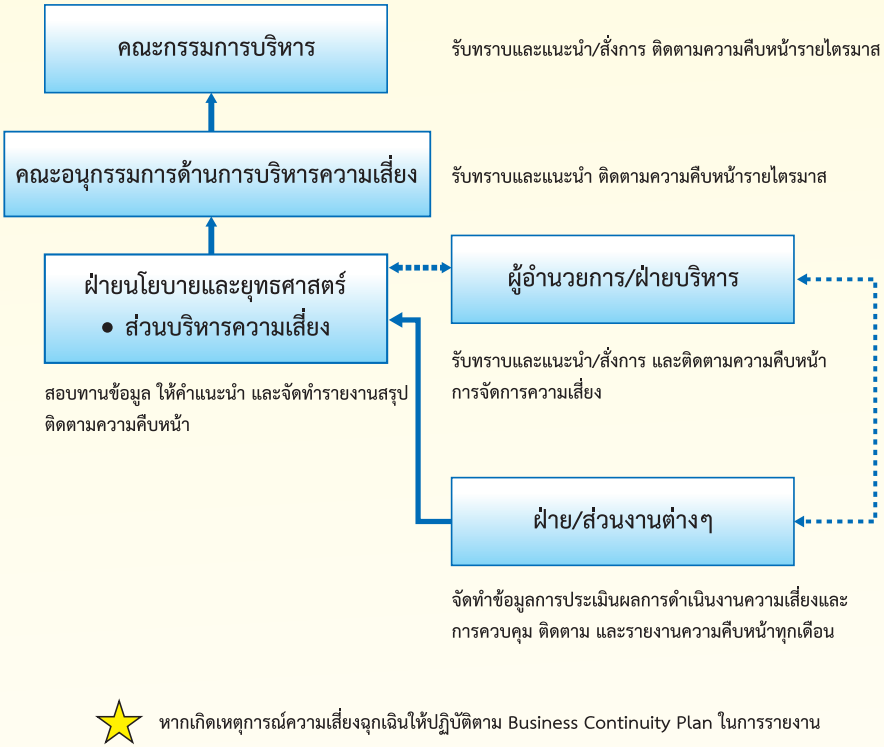
ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่เกิดขึ้นกับหน่วยงานทันทีหรือภายในวันทำการถัดไปและในกรณีที่ไม่มีเหตุการณ์ความเสียหายฯ หน่วยงานก็ต้องรายงานให้ส่วนบริหารความเสี่ยงทราบด้วยเพื่อให้มั่นใจว่าส่วนบริหารความเสี่ยงได้รับข้อมูลที่ถูกต้องและครบถ้วน โดยข้อมูลทั้งหมดนั้นส่วนบริหารความเสี่ยงจะรวบรวมสรุปผลและนำเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยงหรือคณะอนุกรรมการที่เกี่ยวข้องต่อไป

ทั้งนี้ หากมีความเสียหายที่มีนัยสำคัญเกิดขึ้นกับหน่วยงานหน่วยงานจะต้องมีการจัดทำ Treatment Plan เพื่อลดหรือป้องกันไม่ให้เกิดความเสียหายดังกล่าวขึ้นกับ สรอ. ได้อีกในอนาคต และหากมีเหตุฉุกเฉินเกิดขึ้น เจ้าหน้าที่ของ สรอ. ที่พบจะต้องรายงานเหตุการณ์ความเสี่ยงตามคู่มือ Business Continuity Plan ที่กำหนดไว้ และหน่วยงานที่มีความเสี่ยงอยู่ในระดับสูงหรือมีนัยสำคัญต้องมีการนำดัชนีชี้วัดความเสี่ยง (Key Risk Indicators : KRI) ที่สะท้อนถึงสาเหตุและโอกาสที่จะเกิดความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศซึ่งดัชนีชี้วัดความเสี่ยงนี้ถือเป็นเครื่องมือในการวัดติดตามและบริหารความเสี่ยงที่สำคัญของหน่วยงาน ทั้งนี้หน่วยงานต้องมีการรายงานดัชนีชี้วัดความเสี่ยงมายังส่วนบริหารความเสี่ยงตามรูปแบบและระยะเวลาที่กำหนดเพื่อใช้ในการติดตามดูแลความเสี่ยงที่มีอยู่หรือที่อาจจะเกิดขึ้น

๕.๘ การติดตามและประเมินผล (Monitoring)

ทุกหน่วยงานต้องจัดให้มีกระบวนการในการติดตามความเสี่ยงที่มีอยู่ตามแต่ช่วงเวลาที่เหมาะสมหรือตามการเปลี่ยนแปลงของความเสี่ยง โดยหน่วยงานควรกำหนดความถี่ในการติดตามให้มากขึ้นเช่นรายสัปดาห์หากความเสี่ยงมีการเปลี่ยนแปลงที่มากขึ้นเป็นต้นแต่หากข้อมูลปัจจัยเสี่ยงมีการเปลี่ยนแปลงน้อยและเปลี่ยนแปลงค่อนข้างช้าหน่วยงานอาจติดตามเพียงเดือนละครั้ง ไตรมาสละครั้งหรือปีละสองครั้งทั้งนี้เพื่อให้ผู้บริหาร ผู้อำนวยการ สรอ. สามารถติดตามสถานะของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่มีอยู่ในแต่ละช่วงเวลาและสามารถวางแผนในการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่เกิดขึ้นได้อย่างเหมาะสมและมีประสิทธิภาพอีกทั้งยังช่วยให้หน่วยงานสามารถป้องกันและควบคุมเหตุการณ์ความเสียหายที่อาจเกิดขึ้นได้อย่างทันท่วงที

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติส่วนยุทธศาสตร์ต้องรายงานให้ผู้บริหาร สรอ. ทราบตามลำดับความรุนแรงดังนี้

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

แบบฟอร์ม

แบบฟอร์มการรายงานและการติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยง

EGA e-Government Agency	รายงานการบริหารความเสี่ยง (Risk Management Report)		
ความเสี่ยงของ	โครงการ		
ยุทธศาสตร์/กลยุทธ์			
สำนัก		ส่วนงาน	
รหัสความเสี่ยง		ชื่อความเสี่ยง	
ตัวชี้วัด		ด้านความเสี่ยง	
ประเภทความเสี่ยง		กลุ่มความเสี่ยง	
ปัจจัยเสี่ยง			
การควบคุมที่มีอยู่			
การประเมินความเสี่ยงก่อนและหลังการควบคุม			
	ก่อนการควบคุม	หลังการควบคุม	
โอกาส			
ผลกระทบ			
ระดับความเสี่ยง			
การจัดการความเสี่ยง			
แผนการปรับปรุงการควบคุม			
ปัญหาอุปสรรค			
สถานะการดำเนินงาน			
ผู้รายงาน		กำหนดเสร็จ	
ผู้อนุมัติ		วันที่อนุมัติ	

ตัวอย่างแบบฟอร์มการติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยงด้าน SOFC

การบริหารความเสี่ยงห้อง..... (SOFC) ประจำปีงบประมาณ พ.ศ. .....

ลำดับ	ประเด็นความเสี่ยง	การระบุประเด็นความเสี่ยง	สาเหตุ	การควบคุมที่มีอยู่	การประเมินความเสี่ยง		ระดับความเสี่ยง	การดำเนินการ/แผนการลดความเสี่ยง	กำหนดแล้วเสร็จ	การประเมินความเสี่ยงที่คาดหวังภายในปีงบประมาณ.....		ระดับความเสี่ยง	ผู้รับผิดชอบ
					โอกาส	ผลกระทบ				โอกาส	ผลกระทบ		

ตัวอย่างแบบฟอร์มการติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยงด้าน IT

การบริหารความเสี่ยง..... (IT) ประจำปีงบประมาณ พ.ศ. .....

ลำดับ	ประเด็นความเสี่ยง		การควบคุมที่มีอยู่	การประเมินความเสี่ยง						ระดับความเสี่ยง	ข้อกำหนด	การดำเนินการ/แผนการลดความเสี่ยง	กำหนดแล้วเสร็จ	ความเสี่ยงที่คาดหวังภายในปีงบประมาณ.....						ระดับความเสี่ยง	ผู้รับผิดชอบ
	ภัยคุกคาม	ช่องโหว่		ผลกระทบ					โอกาส					ผลกระทบ					โอกาส		
				R	F	O	C	ค่าสูงสุด						R	F	O	C	ค่าสูงสุด			

R ภาพลักษณ์/ชื่อเสียงขององค์กร
F การเงิน
O การดำเนินงาน
C กฎหมาย ระเบียบ ข้อบังคับ

รายงานผลการวิเคราะห์เปรียบเทียบการบริหารความเสี่ยง ระหว่าง ISO 31000:2009 กับกรอบแนวคิดของ COSO ERM

สารบัญ

๑. ที่มาของการบริหารความเสี่ยงตามแนวทางของ ISO 31000:2009

จากการประชุมหารือถึง ๖ ครั้งในรอบหลายปีของคณะทำงานที่ประกอบด้วยผู้ทรงคุณวุฒิมากกว่า ๒๐ ประเทศ ท้ายที่สุดในเดือนพฤศจิกายน ปี ๒๐๐๙ ที่ผ่านมา คณะทำงานก็เห็นสมควรให้มีการปรับปรุงมาตรฐานเดิมที่ใช้กันอยู่ที่เรียกกันว่า The Australia/New Zealand risk management standard (AS/NZS 4360:2004) เพื่อที่จะสามารถนำไปใช้กับองค์กรต่าง ๆ ให้หลากหลายมากยิ่งขึ้น โดยหลังจากการปรับในเนื้อหาบางส่วนของมาตรฐานเดิมแล้ว มาตรฐานการบริหารความเสี่ยงใหม่ที่ว่าถูกใช้ชื่อว่า การบริหารความเสี่ยง หลักการและแนวทางในการปฏิบัติ (Risk Management- Principles and Guidelines) หรือที่หลาย ๆ คนรู้จักกันในนาม ISO 31000:2009

มาตรฐานการบริหารความเสี่ยงฉบับใหม่นี้อ้างอิงคำจำกัดความต่าง ๆ ตามเอกสารของ ISO Guide 73 ซึ่งถูกตีพิมพ์ในเดือนพฤศจิกายน ปี ๒๐๐๙ เช่นกัน โดยเอกสาร ISO Guide 73 นั้นเป็นการรวบรวมคำจำกัดความต่าง ๆ ในการบริหารความเสี่ยง

๒. หลักการ กรอบแนวคิด และกระบวนการของการบริหารความเสี่ยง ตามแนวทางของ ISO 31000:2009

๑.๑ หลักการ

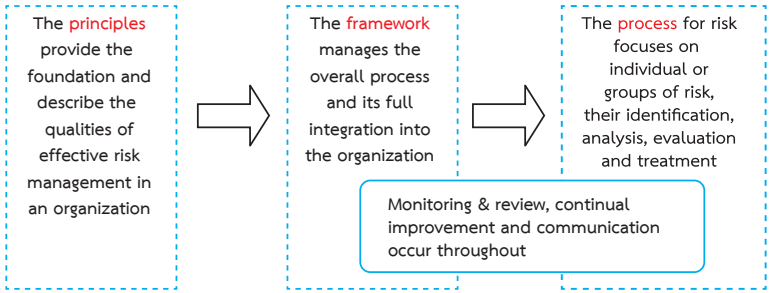
หลักการเบื้องต้นของการบริหารความเสี่ยงตามกระบวนการบริหารความเสี่ยงของ ISO 31000:2009 นั้น จะเน้นถึงการกำหนดเป้าหมายที่สำคัญของกระบวนการต่าง ๆ โดยที่หลักการจะสนับสนุนมุมมองของการบริหารความเสี่ยงที่ครอบคลุมและประสานกัน โดยที่สามารถประยุกต์ใช้ได้ทั้งองค์กร หลักการบริหารความเสี่ยงเป็นการเชื่อมโยงระหว่างกรอบแนวคิด (Framework) และการปฏิบัติจริงที่เกิดขึ้น (Practices) เข้าด้วยกันเพื่อโยงไปยังเป้าหมายกลยุทธ์ขององค์กรผ่านกิจกรรมการบริหารต่าง ๆ ขององค์กร

๑.๒ กรอบแนวคิด

ISO 31000:2009 เน้นการพัฒนากรอบแนวคิดที่จะผนวกการบริหารความเสี่ยงเข้ากับองค์กรอย่างเป็นอันหนึ่งอันเดียว กรอบแนวคิดใหม่นี้สามารถทำให้มั่นใจได้ว่ากระบวนการทำงานต่าง ๆ ทั่วทั้งองค์กรได้รับการสนับสนุนจากการบริหารความเสี่ยงอย่างต่อเนื่องและมีประสิทธิภาพ กล่าวคือ การบริหารความเสี่ยงจะเป็นองค์ประกอบที่สำคัญต่อการบริหารกลยุทธ์และการวางแผน การจัดการ กระบวนการรายงานผล นโยบายต่าง ๆ คุณค่าและวัฒนธรรมองค์กร

ส่วนประกอบต่าง ๆ ของกรอบแนวคิดการบริหารความเสี่ยงของ ISO 31000:2009 นั้น ประกอบไปด้วยการทำความเข้าใจและการกำหนดบริบททั้งภายใน และภายนอกต่าง ๆ ที่กระทบต่อองค์กร การกำหนดนโยบายการบริหารความเสี่ยง การบูรณาการการบริหารความเสี่ยงเข้ากับกระบวนการต่าง ๆ ขององค์กร การรายงานและการสื่อสารต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก การนำกระบวนการบริหารความเสี่ยงไปปฏิบัติ การติดตามและทบทวนกระบวนการบริหารความเสี่ยง และการพัฒนากรอบแนวคิดโดยที่สามารถแสดงถึงแผนผังขั้นตอนของการบริหารความเสี่ยงตามรูปที่ ๑

รูปที่ ๑ : แผนผังขั้นตอนของการบริหารความเสี่ยง

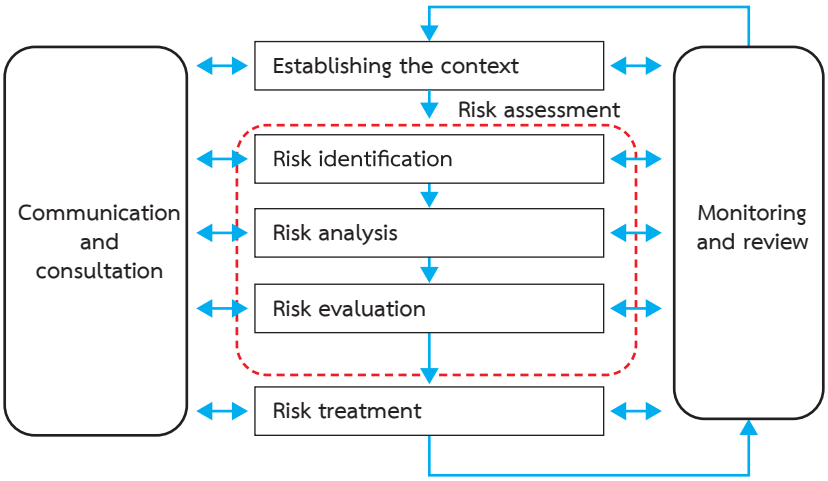


รูปที่ ๑ แสดงให้เห็นถึงขั้นตอนการทำงานของการบริหารความเสี่ยงทั้งหมด กล่าวคือ หลักการของการบริหารความเสี่ยง (principles) ทำให้เราทราบว่าพื้นฐานของการบริหารความเสี่ยงที่ดีนั้นเป็นอย่างไร เมื่อเราทราบหลักการที่ดีแล้วก็จะทำให้เราทราบถึงกรอบแนวคิด (framework) ในการบริหารความเสี่ยงขององค์กร โดยที่กรอบแนวคิดดังกล่าวเป็นเครื่องมือในการจัดการกระบวนการบริหารความเสี่ยงทั้งหมดให้ถูกบูรณาการเข้ากับการทำงานต่าง ๆ ขององค์กร และขั้นตอนสุดท้ายคือกระบวนการบริหารความเสี่ยงจะเป็นตัวที่ให้ความสำคัญกับที่มาของการระบุปัจจัยเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินความรุนแรงของความเสี่ยง และการจัดการความเสี่ยง

๑.๓ กระบวนการบริหารความเสี่ยงตามแนวทางของ ISO 31000:2009

กระบวนการบริหารความเสี่ยงตามแนวทางของ ISO 31000:2009 สามารถแบ่งออกได้เป็น ๕ กระบวนการหลักด้วยกันที่สอดคล้องกับกระบวนการบริหารความเสี่ยงทั่วไปที่รู้จักกัน ได้แก่ การระบุปัจจัยเสี่ยง/ความเสี่ยง การวิเคราะห์ทางเลือกในการจัดการความเสี่ยง การเลือกการตอบสนองกับความเสี่ยงที่ดีที่สุด การนำแผนบริหารความเสี่ยงไปปฏิบัติ การควบคุมและติดตามผลลัพธ์รวมทั้งการทบทวนปรับปรุงเมื่อจำเป็น ในแบบจำลองของ ISO 31000:2009 กระบวนการบริหารความเสี่ยงที่สำคัญสามารถแสดงได้ตามรูปที่ ๒

รูปที่ ๒ : กระบวนการบริหารความเสี่ยง



รูปที่ ๒ แสดงกระบวนการ ๕ กระบวนการ ได้แก่ การกำหนดบริบทที่มีผลต่อเป้าหมายขององค์กร (Establishing the context) การระบุความเสี่ยง/ปัจจัยเสี่ยงขององค์กร (Risk identification) การวิเคราะห์ความเสี่ยง (Risk analysis) การประเมินความมีนัยสำคัญของความเสี่ยง (Risk evaluation) และการจัดการความเสี่ยง (Risk treatment) อย่างไรก็ตามเราสามารถรวมกระบวนการระบุความเสี่ยง/ปัจจัยเสี่ยงขององค์กร (Risk identification) การวิเคราะห์ความเสี่ยง (Risk analysis) และการประเมินความมีนัยสำคัญความเสี่ยง (Risk evaluation) ว่าเป็นการประเมินภาพรวมของความเสี่ยง (Risk assessment) และตลอดการดำเนินการตามกระบวนการบริหารความเสี่ยงทั้งหมด ต้องมีการสื่อสารและให้คำปรึกษากับผู้เกี่ยวข้อง และผู้มีส่วนได้ส่วนเสียอย่างสม่ำเสมอ (Communication and consultant) รวมถึงการติดตามและการทบทวนและปรับปรุงแก้ไขเมื่อจำเป็น (Monitoring and review) หากจะกล่าวถึงความแตกต่างที่สำคัญ (Significant difference) ระหว่างการบริหารความเสี่ยงแบบเดิมหรือ COSO กับ ISO นั้นก็คือกระบวนการกำหนดบริบทที่มีผลต่อเป้าหมายขององค์กร (Establishing the context) และการสื่อสารและให้คำปรึกษากับผู้เกี่ยวข้อง และผู้มีส่วนได้ส่วนเสียอย่างสม่ำเสมอ (Communication and consultant) โดยที่รายละเอียดของแต่ละกระบวนการของการบริหารความเสี่ยงสามารถแสดงรายละเอียดได้ ดังนี้

๑. การกำหนดบริบทที่มีผลต่อเป้าหมายขององค์กร (Establishing the context) : ถือว่าเป็นกระบวนการที่สำคัญและเป็นกระบวนที่มีรายละเอียดที่แตกต่างจากกระบวนการบริหารความเสี่ยงแบบเดิม เช่น COSO กล่าวคือ ก่อนที่เราจะดำเนินการประเมินความเสี่ยงในภาพรวมนั้น จำเป็นต้องมีการกำหนดวัตถุประสงค์ขององค์กรและรายละเอียดต่าง ๆ ให้ชัดเจน รวมถึงกำหนดขอบเขต และเกณฑ์ความเสี่ยง (Risk criteria) เพื่อใช้ในการประเมินต่อไปว่าความเสี่ยงดังกล่าว องค์กรนั้นสามารถยอมรับกับผลที่เกิดขึ้นตามมาได้มากน้อยเพียงใด โดยที่ขอบเขตและเกณฑ์ความเสี่ยงที่กำหนดต้องสอดคล้องกับวัตถุประสงค์ขององค์กรที่กำหนดไว้

การกำหนดบริบทต่าง ๆ ที่มีผลต่อเป้าหมายขององค์กรตามแนวทางของ ISO สามารถแบ่งได้เป็น ๓ ประเภทย่อย ได้แก่ **(๑)** การกำหนดบริบทภายนอก (Establishing the external context) เช่น กฎระเบียบข้อบังคับ วัฒนธรรม สังคม การเมือง ปัจจัยขับเคลื่อนและกระแสของสังคม และมุมมองจากคนภายนอกต่อองค์กรของเรา **(๒)** การกำหนดบริบทภายใน (Establishing the internal context) เช่น โครงสร้างการบริหาร วัฒนธรรมองค์กร และกลยุทธ์องค์กร เป็นต้น เพื่อที่จะให้การบริหารความเสี่ยงที่เกิดขึ้นเป็นไปตามเป้าหมายขององค์กร **(๓)** การกำหนดบริบทของกระบวนการบริหารความเสี่ยง (Establishing the context of the risk management process) เช่น การกำหนดเป้าหมายของกิจกรรมต่าง ๆ การกำหนดหน้าที่ความรับผิดชอบ การกำหนดขอบเขตของการดำเนินกิจกรรมการบริหารความเสี่ยง เป็นต้น

จากแนวทางของ ISO ที่กล่าวข้างต้นของการกำหนดบริบท สิ่งที่มาให้แบบจำลองใหม่นี้ต่างจากแนวทางของ COSO คือ การที่ ISO ให้ความสำคัญกับการบริหารความเสี่ยงที่ส่งผลไปยังเป้าหมายองค์กรอย่างชัดเจน ผ่านกระบวนการกำหนดบริบทต่าง ๆ อย่างกว้างขวางและครอบคลุมทุกด้าน เช่น ด้านบริบทภายนอกในเรื่องของ ปัจจัยขับเคลื่อนและกระแสของสังคม และมุมมองจากคนภายนอกต่อองค์กร เป็นต้น อย่างไรก็ตามกระบวนการดังกล่าวก็มีทั้งข้อดีและข้อเสีย โดยที่ข้อดีคือการกำหนดบริบทที่ครอบคลุมทำให้การบรรลุเป้าหมายผ่านกระบวนการบริหารความเสี่ยงมีความเป็นไปได้สูง ส่วนข้อเสียคือ ในทางปฏิบัติข้อมูลหรือการได้มาซึ่งบริบทที่ครบถ้วนถือว่าเป็นเรื่องยาก และมีต้นทุนในการได้ข้อมูลดังกล่าวมาค่อนข้างสูง อีกทั้งการกำหนดเป้าหมายที่ลงรายละเอียดตั้งแต่องค์กร สายงาน จนถึงผลิตภัณฑ์อาจทำให้เกิดความซับซ้อนและสูญเสียทรัพยากรอย่างมาก

เมื่อการกำหนดบริบททุกด้านครบถ้วนแล้ว องค์กรสามารถนำข้อมูลที่มีอยู่มากำหนดเกณฑ์ในการประเมินความมีนัยสำคัญของความเสี่ยงนั้น (Risk criteria)

๒. การระบุความเสี่ยง/ปัจจัยเสี่ยง (Risk identification) : เป็นกระบวนการระบุถึงแหล่งที่มาของความเสี่ยงนั้น ๆ ผลกระทบที่จะเกิดขึ้น จุดมุ่งหมายของกระบวนการนี้ต้องให้องค์กรสามารถสร้างชุดของรายการความเสี่ยงทั้งหมดซึ่งอยู่บนหลักการที่ว่าความเสี่ยงนั้นสามารถที่จะกระทบต่อการบรรลุเป้าหมายขององค์กรทั้งทางบวกและทางลบ การระบุปัจจัยเสี่ยงควรครอบคลุมทั้งปัจจัยเสี่ยงที่สาเหตุดังกล่าวสามารถจัดการได้ และไม่สามารถจัดการได้ โดยที่การระบุปัจจัยเสี่ยงอาจมาจากข้อมูลในอดีต การวิเคราะห์ทางทฤษฎี การใช้ความเห็นจากผู้เชี่ยวชาญ และความต้องการของผู้มีส่วนได้ส่วนเสีย เป็นต้น อย่างไรก็ตาม องค์กรควรประยุกต์ใช้เครื่องมือหรือเทคนิคของการระบุปัจจัยเสี่ยงที่เหมาะสมกับเป้าหมายขององค์กรนั้น ๆ รวมถึงความสามารถของบุคลากรในองค์กร โดยที่การได้มาซึ่งข้อมูลที่มีความถูกต้องและทันต่อเหตุการณ์มีความสำคัญอย่างมากต่อการระบุปัจจัยเสี่ยงที่สมบูรณ์

๓. การวิเคราะห์ความเสี่ยง (Risk analysis) : เป็นกระบวนการที่เกี่ยวข้องกับการทำความเข้าใจถึงปัจจัยเสี่ยงต่าง ๆ ที่องค์กรได้มีการระบุไว้ กล่าวคือ เป็นการพิจารณาถึงสาเหตุปัจจัยเสี่ยง บ่อเกิดของปัจจัยเสี่ยง ผลที่เกิดสืบเนื่อง (Consequence) ทั้งด้านบวกและด้านลบของปัจจัยเสี่ยงดังกล่าว รวมถึงโอกาส (Likelihood) ของปัจจัยเสี่ยงที่อาจเกิดขึ้น โดยที่เมื่อเราพิจารณาผลกระทบ และโอกาสเข้าด้วยกันทำให้เราสามารถกำหนดระดับความเสี่ยง (Risk level) ของปัจจัยเสี่ยงนั้น ๆ ซึ่งสิ่งเรากำหนดนี้ต้องมีความสอดคล้องกับเกณฑ์ความเสี่ยงที่ได้กำหนดมาจากบริบท การวิเคราะห์ความเสี่ยงสามารถจัดทำได้ในหลายระดับขึ้นอยู่กับลักษณะของความเสี่ยง จุดมุ่งหมายของการวิเคราะห์ รวมถึงข้อมูลต่าง ๆ ที่องค์กรมีอยู่การวิเคราะห์ในส่วนนี้อาจจะเป็นเชิงปริมาณ เชิงคุณภาพ หรือเชิงกึ่งปริมาณก็ได้ ผลที่เกิดสืบเนื่องจากปัจจัยเสี่ยงใด ๆ สามารถแสดงในลักษณะของผลกระทบ (Impact) ที่จับต้องได้ เช่น ตัวเงิน ผลผลิตที่เสียหาย หรือลักษณะของผลกระทบที่จับต้องไม่ได้ เช่น ภาพลักษณ์ที่เสียหายจากมุมมองของผู้มีส่วนได้ส่วนเสีย เป็นต้น

๔. การประเมินความเสี่ยง (Risk evaluation) : เป็นกระบวนการเพื่อช่วยในการตัดสินใจโดยอาศัยข้อมูลจากผลการวิเคราะห์ความเสี่ยงจากกระบวนการก่อนหน้า เพื่อที่จะใช้ในการพิจารณาว่าปัจจัยเสี่ยงใดที่องค์กรจำเป็นต้องมีการจัดการปัจจัยเสี่ยง (Risk treatment) นั้น รวมถึงการจัดลำดับความสำคัญก่อนหลังในการดำเนินการจัดการลดความเสี่ยงเหล่านั้น กระบวนการประเมินความเสี่ยงเป็นการเปรียบเทียบระดับความเสี่ยง (Risk level) ที่ได้จากการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยง (Risk criteria) ที่ได้มาจากกระบวนการกำหนดบริบทต่าง ๆ ที่มีผลต่อเป้าหมายขององค์กร เพื่อที่จะทำให้ทราบว่าปัจจัยเสี่ยงใดที่องค์กรยอมรับได้ ปัจจัยเสี่ยงใดองค์กรยอมรับไม่ได้ซึ่งต้องมีการกำหนดการจัดการความเสี่ยงต่อไป

๕. การจัดการความเสี่ยง (Risk treatment) : เป็นกระบวนการที่เกี่ยวข้องกับการเลือกทางเลือกใดทางเลือกหนึ่ง หรือหลายทางเลือกสำหรับการลดระดับความเสี่ยง และนำแนวทางหรือทางเลือกนั้นไปปฏิบัติโดยที่เราสามารถเรียกทางเลือกหรือแนวทางนั้นว่า การควบคุมความเสี่ยง กระบวนการจัดการความเสี่ยงเป็นกระบวนการที่เป็นวงจรหรือวัฏจักร (Cyclical) ของการประเมินการจัดการความเสี่ยง การพิจารณาว่าระดับความเสี่ยงที่เหลืออยู่ (Residual risk level) จากการจัดการความเสี่ยงนั้นยอมรับได้หรือไม่ หากรับไม่ได้การจัดการความเสี่ยงใหม่ที่จะต้องเป็นอย่างไร และการประเมินความมีประสิทธิผลของการจัดการความเสี่ยงที่มีอยู่

แนวทางต่าง ๆ ในการจัดการความเสี่ยงไม่จำเป็นต้องเป็นอิสระซึ่งกันและกัน (Mutually exclusive) หรือไม่จำเป็นที่แนวทางหนึ่งจะต้องลดระดับความเสี่ยงได้ทุกปัจจัยเสี่ยงซึ่งครอบคลุมลักษณะต่าง ๆ เช่น การหลีกเลี่ยงความเสี่ยง การเปลี่ยนแปลงโอกาสที่จะเกิดการเปลี่ยนแปลงผลกระทบที่ตามมาของปัจจัยเสี่ยง การกระจายความเสี่ยง เป็นต้น

หลักการในการเลือกแนวทางที่เหมาะสมในการจัดการความเสี่ยงนั้น เราต้องคำนึงถึงการสร้างความสมดุลระหว่างต้นทุนต่าง ๆ ที่เกิดขึ้นจากการนำแนวทางหรือมาตรการจัดการความเสี่ยงไปปฏิบัติกับผลประโยชน์ที่ได้รับเมื่อระดับความเสี่ยงของปัจจัยเสี่ยงนั้นลดลงภายในเงื่อนไขกฎระเบียบข้อบังคับ และความต้องการของผู้มีส่วนได้ส่วนเสีย อย่างไรก็ตามสิ่งที่องค์กรพึงระวังก็คือการดำเนินมาตรการจัดการความเสี่ยงที่ผิดพลาดนั้น นอกจากไม่สามารถลดระดับความเสี่ยงของปัจจัยเสี่ยงนั้นแล้ว ยังอาจก่อให้เกิดปัจจัยเสี่ยงใหม่ตามมาได้ ดังนั้นการติดตามและประเมินประสิทธิผลของการจัดการความเสี่ยงจึงจำเป็นต้องถูกผนวกเข้าเป็นเนื้อเดียวกับแผนการดำเนินงานการจัดการความเสี่ยงเพื่อสร้างความมั่นใจในประสิทธิผลที่เกิดขึ้น

๖. การติดตามและการทบทวน (monitoring and review) : ถึงแม้ว่ากระบวนการนี้ไม่ได้เป็นกระบวนการหลักในการบริหารความเสี่ยง อย่างไรก็ตามการติดตามและการทบทวนเป็นขั้นตอนที่มีความสำคัญอย่างมากที่ควรถูกรวมเข้ากับกระบวนการอื่น เพื่อที่จะทำให้องค์กรมั่นใจว่ามาตรการจัดการเสี่ยงมีประสิทธิภาพและประสิทธิผลมากน้อยเพียงใด เพื่อที่จะได้รับข้อมูลเพิ่มเติมตลอดเวลาในการปรับปรุงกระบวนการต่าง ๆ ให้ดีขึ้น เป็นต้น นอกจากนี้ผลที่ได้จากการติดตามและทบทวนความเสี่ยงที่ได้จัดทำขึ้นนี้จะเป็นปัจจัยที่สำคัญในการทบทวนกรอบแนวคิดในการบริหารความเสี่ยงต่อไป

๓. กระบวนการของการบริหารความเสี่ยงตามแนวทางของ COSO ERM

กระบวนการ ๘ ขั้นตอนหลักประกอบด้วย

๑. สภาพแวดล้อมภายในองค์กรแนวนโยบายโดยทั่วไปของสำนักงาน ซึ่งเป็นพื้นฐานที่สำคัญของกรอบการบริหารความเสี่ยง และการจัดการกับความเสี่ยง

๒. การกำหนดวัตถุประสงค์และเป้าหมายที่สอดคล้องกับกลยุทธ์สรอ.

๓. การระบุเหตุการณ์ การบ่งชี้และเข้าใจความเสี่ยงทั้งหมดที่มีผลกระทบต่อวัตถุประสงค์ที่กำหนดไว้

๔. การประเมินความเสี่ยง โดยพิจารณาถึงผลกระทบและโอกาสเกิดความเสี่ยง

๕. การตอบสนองความเสี่ยง กำหนดการจัดการความเสี่ยงที่มีอยู่ในปัจจุบัน

๖. กิจกรรมการควบคุม โดยพิจารณาถึงการควบคุมเพิ่มเติมรวมทั้งความสัมพันธ์ของต้นทุนและผลประโยชน์ที่เกิดขึ้น ผู้บริหารควรนำวิธีการจัดการความเสี่ยงไปปฏิบัติและติดตาม เพื่อให้มั่นใจได้ว่า มีการดำเนินการตามวิธีการที่กำหนดไว้ กิจกรรมการควบคุม คือนโยบายและขั้นตอนปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง

๗. สารสนเทศและการสื่อการ การสื่อสารเพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง

๘. การติดตามผลและรายงานความมีประสิทธิผลของกระบวนการและระบบการบริหารความเสี่ยง

๔. การเปรียบเทียบแนวทางการบริหารความเสี่ยงระหว่าง ISO กับ COSO

การเปรียบเทียบระหว่างแนวทางการบริหารความเสี่ยงแบบ ISO 31000:2009 กับ COSO ERM นั้น สามารถแสดงได้ด้วยความแตกต่างที่สำคัญ ดังนี้

๑.๑ กรอบแนวคิดในการบริหารความเสี่ยง

กรอบแนวคิดของ COSOERM นั้นหากเทียบกับกรอบแนวคิดของ ISO นั้นมีความซับซ้อนกว่าและอาศัยขั้นตอนต่าง ๆ ทำให้องค์กรหลายแห่งประสบกับปัญหาการนำกรอบการบริหารความเสี่ยงนี้ไปใช้ในทางปฏิบัติ ในขณะที่ ISO กำหนดกรอบแนวคิดที่ง่ายต่อความเข้าใจมากกว่าตามมุมมองของคณะทำงาน กล่าวคือ กรอบแนวคิดของ ISO อยู่บนพื้นฐานของกระบวนการจัดการ (Management process) และสามารถประยุกต์ใช้กับลักษณะขององค์กรต่าง ๆ ได้ โดยถูกผนวกเข้ากับการจัดการที่มีอยู่ขององค์กรมากกว่ากรอบแนวคิดของ COSO ซึ่งเป็นกรอบแนวคิดที่อยู่บนพื้นฐานของการควบคุมและการปฏิบัติตามกฎระเบียบ (Control and compliance) ทำให้อาจจะยากต่อการที่ฝ่ายบริหารจะเข้าใจ ในทางกลับกันหากให้ฝ่ายงานที่ทำหน้าที่ตรวจสอบภายในหรือควบคุมภายในดำเนินการบริหารความเสี่ยงเองก็อาจเกิดปัญหาที่คนดำเนินการกับคนตรวจสอบเป็นบุคคลกลุ่มเดียวกัน หรืออาจเกิดความขัดแย้งทางผลประโยชน์ได้ (Conflict of interest)

จากมุมมองข้างต้นที่ได้กล่าวมานั้น สามารถสรุปได้ว่ากรอบแนวคิดของ ISO จะกำหนดไว้ค่อนข้างยืดหยุ่นและอิงกับหลักการบริหารองค์กรที่หน่วยงานต่าง ๆ ส่วนใหญ่มีอยู่แล้วเพื่อให้สามารถเข้าใจและนำไปใช้ได้ง่าย ในขณะที่กรอบแนวคิดของ COSO นั้นจะอิงเข้ากับหลักการของการตรวจสอบภายในที่อาศัยหลักการเฉพาะด้านมากกว่าข้อดีก็คือการบริหารความเสี่ยงนี้จะมีขั้นตอนที่ค่อนข้างตายตัวอาจจะเหมาะกับองค์กรที่เริ่มในการบริหารความเสี่ยง อย่างไรก็ตามไม่ว่าจะเป็นกรอบแนวคิดแบบใดล้วนมีจุดมุ่งหมายในการบริหารความเสี่ยงเพื่อบรรลุเป้าหมายขององค์กรทั้งสิ้น แต่ข้อดีข้อเสียของแต่ละแนวคิดก็เป็นสิ่งที่องค์กรที่จะต้องเลือกใช้อย่างเหมาะสม

ซึ่งเมื่อทำการทบทวนคู่มือการบริหารความเสี่ยงของสำนักงานทั้งในภาพรวมและแยกเป็นคู่มือแต่ละด้านได้ทำการวิเคราะห์ถึงเป้าหมายขององค์กรอย่างครบถ้วนทุกมุมมอง ดังนั้น หลักการที่ใช้ในการกำหนดแนวทางของการทบทวนคู่มือให้เป็นไปตามหลักการของ COSO ERM นั้น จะมีความครอบคลุมแนวทางของ ISO อย่างครบถ้วนแล้ว เนื่องจากคู่มือดังกล่าวสามารถนำไปปฏิบัติได้จริง ดังนั้น กรอบแนวคิดของ ISO ที่กำหนดอยู่บนพื้นฐานของกระบวนการจัดการ (Management process) จึงสามารถอธิบายด้วยแนวทางของ COSO ERM ได้สมบูรณ์

๑.๒ นิยามของคำจำกัดความ

นอกจากกรอบแนวคิดที่แตกต่างกันแล้ว เราสามารถสรุปคำจัดความสำคัญ หรือคำอธิบายที่แตกต่างกันระหว่าง ISO และ COSO ได้ตามรูปที่ ๓ เช่น

- นิยามความเสี่ยง (Risk definition) ISO ให้ความหมายไว้ว่าเป็นผลของความไม่แน่นอนที่ส่งผลต่อองค์กร ในขณะที่ COSO คือ เหตุการณ์ที่เกิดขึ้นและก่อให้เกิดผลเชิงลบต่อเป้าหมายขององค์กร

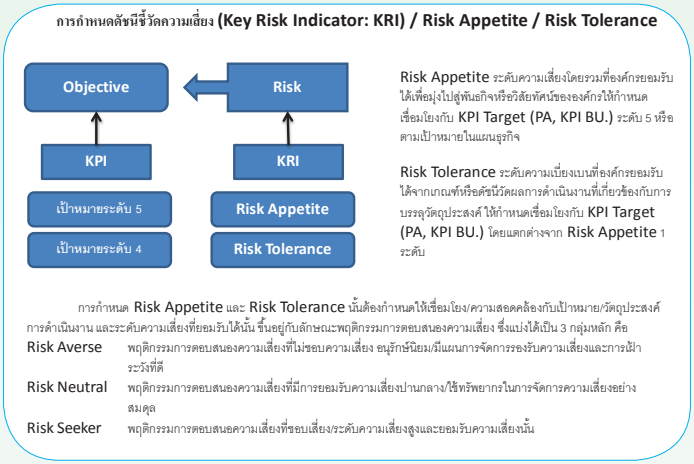
ในคู่มือการบริหารความเสี่ยงของ สรอ. ทั้งในภาพรวมและแยกเป็นคู่มือแต่ละด้าน การระบุปัจจัยเสี่ยงที่ยกตัวอย่างในคู่มือแต่ละด้านจะมองครอบคลุมถึงมุมมองทั้งความไม่แน่นอนที่ส่งผลต่อองค์กร ทั้งนี้ ความไม่แน่นอนดังกล่าวอาจเป็นแนวคิดในเชิงการระบุความเสี่ยงเพื่อเข้าหาโอกาสที่มีอยู่ขององค์กร เช่น ความเสี่ยงด้านการเงิน ในมุมมองของรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย ซึ่งรายได้นอกงบประมาณนั้น ไม่ถือว่าเป็นภารกิจหลักขององค์กร แต่เป็นโอกาสทางธุรกิจที่เกิดขึ้นจากการให้บริการหน่วยงานภาครัฐ ดังนั้น ความไม่แน่นอนในเชิงการเข้าหาโอกาส จึงถือเป็นการระบุปัจจัยเสี่ยงอย่างหนึ่ง รวมถึงการระบุปัจจัยเสี่ยงในการทบทวนคู่มือการบริหารความเสี่ยงของสำนักงานทั้งในภาพรวมและแยกเป็นคู่มือแต่ละด้าน พิจารณาถึงเหตุการณ์ที่เกิดขึ้นและก่อให้เกิดผลเชิงลบต่อเป้าหมายขององค์กร เช่น จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการไม่เป็นไปตามเป้าหมาย การพัฒนา Data Center Consolidation ล่าช้ากว่าแผนงานที่กำหนด เป็นต้น ดังนั้น การระบุความเสี่ยงของสรอ. ส่วนบริหารความเสี่ยงใช้นิยามความเสี่ยงที่ครอบคลุมทั้งหลักการของ ISO และ COSO ERM

- การประเมินความเสี่ยง (Risk assessment) สำหรับแนวทางของ ISO ให้ความหมายถึงกระบวนการภาพรวมตั้งแต่ การระบุความเสี่ยง (Risk identification) การวิเคราะห์ความเสี่ยง (Risk analysis) การประเมินความมีนัยสำคัญของความเสี่ยง (Risk evaluation) ในขณะที่ COSO ให้ความหมายของ Risk assessment ไว้ว่าเป็นการประเมินโอกาสและผลกระทบของปัจจัยเสี่ยง (Inherent risk) เพื่อกำหนดมาตรการจัดการความเสี่ยง

จากการทบทวนทบทวนคู่มือการบริหารความเสี่ยงของสำนักงานทั้งในภาพรวมและแยกเป็นคู่มือแต่ละด้านในส่วนของการประเมินความเสี่ยงนั้น ส่วนบริหารความเสี่ยงใช้นิยามที่ครอบคลุมทั้ง ISO และ COSO ERM โดยประเด็นที่ ISO เพิ่มขึ้นมาคือมุมมองในด้านการประเมินความมีนัยสำคัญของความเสี่ยง (Risk evaluation) ซึ่งเมื่อประเมินระดับความรุนแรงของปัจจัยเสี่ยงที่เกิดขึ้นแล้ว จะต้องมาพิจารณาถึงความมีนัยสำคัญประกอบ

โดยพิจารณาเพิ่มเติมเทียบกับระดับความเสี่ยงขององค์กรที่ยอมรับได้ หากระดับความรุนแรงของปัจจัยเสี่ยงนั้นสูงกว่าระดับความเสี่ยงขององค์กรที่ยอมรับได้ จะมีการประเมินนัยสำคัญในการกำหนดแผนหรือมาตรการในการจัดการความเสี่ยง

แผนภาพด้านล่าง แสดงถึงหลักการในการกำหนดระดับความเสี่ยงที่ยอมรับได้ เพื่อเป็นบรรทัดฐานในการพิจารณาความมีนัยสำคัญของปัจจัยเสี่ยงนั้น ๆ



รูปที่ ๓ ตารางเปรียบเทียบความแตกต่างระหว่าง ISO และ COSO

Key Term or Description	ISO 31000	COSO
Scope	This International Standard providesprinciples and generic guidelineson risk management. It can be usedby any public, private or communityenterprise, association, group orindividual. Therefore, this International Standard is not specific to any industryor sector.	This definition (of ERM) is purposefullybroad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries and sectors. It focuses directly onachievement of objectives established

Key Term or Description	ISO 31000	COSO
		by a particular entity and provides a basisfor defining enterprise risk management effectiveness.
Risk management, defined.	Coordinated activities to direct andcontrol an organization with regard to risk.	Enterprise risk management is a process,effected by an entity's board of directors,management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
Risk, defined	The effect of uncertainty uponobjectives.	The possibility that an event will occurand adversely affect the achievement of objectives.
Risk appetite, defined.	The amount and type of risk that an organization is willing to pursue or retain.	A broad amount of risk an entity is willing to accept in pursuit of its mission or vision.

Key Term or Description	ISO 31000	COSO
Risk assessment, defined.	The overall process of riskidentification, risk analysis and riskevaluation.	Risks are analyzed, considering likelihoodand impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
Risk management process	Continually and iteratively : Communicate and consult o Establish the context o Risk assessment: • Identification • Analysis • Evaluation o Risk treatment Continually & iteratively: Monitor and review	o Internal environment o Objective setting o Event identification o Risk assessment o Risk response o Control activities o Info & communication o Monitoring

ที่มา : Gjerdrum and Peter (2011). The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000 : 2009 and the COSO ERM Framework. Risk Management Newsletter. Society of Actuaries.

จากคำนิยามต่าง ๆ ตามรูปที่ ๓ สะท้อนในเห็นถึงทัศนคติต่อความเสี่ยง (Risk attitude) ที่ต่างกันของ ISO กับ COSO อย่างไรก็ตามการเลือกใช้ขึ้นอยู่กับวิธีการที่เหมาะสมกับองค์กรและความตั้งใจขององค์กรนั้นสำหรับการบริหารความเสี่ยง

๑.๓ กระบวนการบริหารความเสี่ยง

ตามรูปที่ ๓ แสดงให้เห็นว่าจุดต่างที่สำคัญซึ่งทำให้กระบวนการบริหารความเสี่ยงตามแนวคิดของ ISO แตกต่างจาก COSO คือ การกำหนดบริบทต่าง ๆ ที่มีผลต่อเป้าหมายขององค์กร (Establishing the context) และกระบวนการวิเคราะห์ความเสี่ยง (Risk assessment) โดยมีรายละเอียด ดังนี้

การกำหนดเป้าหมาย

	ISO	COSO
Establishing Thecontext	ISO ให้ความสำคัญกับการกำหนดบริบทต่าง ๆ ก่อนที่องค์กรนั้นจะกำหนดเป้าหมายที่ต้องการบรรลุ โดยเป้าหมายที่ถูกกำหนดควรพิจารณาตั้งแต่เป้าหมายขององค์กร สายงาน ผลิตภัณฑ์ หรือบุคคล ดังนั้นการกำหนดบริบทที่ชัดเจน และครอบคลุมทุกด้านจึงมีความสำคัญมากต่อการกำหนดเป้าหมายที่ถูกต้องและทำให้การบริหารความเสี่ยงเป็นส่วนในการสนับสนุนให้เป้าหมายต่าง ๆ เป็นไปตามที่ต้องการ บริบทที่องค์กรควรพิจารณาประกอบด้วย บริบทภายนอก (external context) เช่น กฎระเบียบข้อบังคับ วัฒนธรรม สังคม การเมือง ปัจจัยขับเคลื่อนและกระแสของสังคม (key drivers and trends) และมุมมองจากผู้มีส่วนได้ส่วนเสียต่อองค์กร (external stakeholder) และบริบทภายใน (internal	COSO ไม่ได้กล่าวถึงรายละเอียดที่มาของวิธีการในการกำหนดเป้าหมายขององค์กร เพียงแต่มีการอธิบายกระบวนการคร่าวๆ เท่านั้นว่ากระบวนการบริหารความเสี่ยงที่ดีควรมีการกำหนดเป้าหมายที่ชัดเจนโดยให้การบริหารความเสี่ยงเป็นส่วนช่วยในการบรรลุเป้าหมายนั้น

	ISO	COSO
	context) เช่น โครงสร้างการบริหาร วัฒนธรรมองค์กร กลยุทธ์องค์กร และความต้องการของผู้มีส่วนได้ส่วนเสียภายใน (internal stakeholder)	
การดำเนินงานของส่วนบริหารความเสี่ยงสำหรับประเด็นดังกล่าวเพื่อให้คู่มือการบริหารความเสี่ยงของสำนักงานครอบคลุมทั้ง ISO และ COSO ERM : การกำหนดบริบทขององค์กรในคู่มือการบริหารความเสี่ยงทั้งในภาพรวมและคู่มือการบริหารความเสี่ยงในแต่ละด้าน มีการพิจารณาครอบคลุมทุกด้านทั้งบริบทภายนอก และบริบทภายในโดยการระบุความเสี่ยงจากบริบทนั้น จะมีการพิจารณาถึงมุมมองของผู้มีส่วนได้เสียขององค์กรประกอบด้วย		

การวิเคราะห์ความเสี่ยง

	ISO	COSO
Risk assessment	ISO ให้ความหมายและอธิบายกระบวนการนี้ครอบคลุมรายละเอียดถึง ๓ กระบวนการย่อยที่ต่อเนื่องกัน ได้แก่ การระบุความเสี่ยง/ปัจจัยเสี่ยง (Risk identification) เป็นกระบวนการระบุถึงแหล่งที่มาของความเสี่ยงนั้น ๆ ผลกระทบที่จะเกิดขึ้นต่อการบรรลุเป้าหมายขององค์กรทั้งทางบวกและทางลบ การวิเคราะห์ความเสี่ยง (Risk analysis) เป็นการ	การวิเคราะห์ความเสี่ยงจะพิจารณาในเรื่องของการกำหนดระดับความรุนแรงผ่านตัวโอกาสและผลกระทบ เพื่อกำหนดมาตรการบริหารความเสี่ยงสำหรับปัจจัยเสี่ยงที่องค์กรยอมรับไม่ได้

	ISO	COSO
	พิจารณาผลกระทบที่สืบเนื่อง (consequence) ทั้งด้านบวกและด้านลบของปัจจัยเสี่ยงดังกล่าว รวมถึงโอกาส (likelihood) ของปัจจัยเสี่ยงที่อาจเกิดขึ้น โดยที่เมื่อเราพิจารณาผลกระทบ และโอกาสเข้าด้วยกันทำให้เราสามารถกำหนดระดับความเสี่ยง (Risk level) ของปัจจัยเสี่ยงนั้น ๆ การประเมินความมีนัยสำคัญของความเสี่ยง (Risk evaluation) เป็นกระบวนการเพื่อช่วยในการตัดสินใจโดยอาศัยข้อมูลจากผลการวิเคราะห์ความเสี่ยงจากกระบวนการก่อนหน้าเพื่อที่จะใช้ในการพิจารณาว่าปัจจัยเสี่ยงใดที่องค์กรจำเป็นต้องมีการจัดการปัจจัยเสี่ยง (Risk treatment)	

การดำเนินงานของส่วนบริหารความเสี่ยงสำหรับประเด็นดังกล่าวเพื่อให้คู่มือการบริหารความเสี่ยงของสำนักงานครอบคลุมทั้ง ISO และ COSO ERM :

จากการทบทวนคู่มือการบริหารความเสี่ยงของสำนักงานทั้งในภาพรวมและแยกเป็นคู่มือแต่ละด้านในส่วนของการประเมินความเสี่ยงนั้น ส่วนบริหารความเสี่ยงใช้นิยามที่ครอบคลุมทั้ง ISO และ COSO ERM โดยประเด็นที่ ISO เพิ่มขึ้นมาคือมุมมองในด้านการประเมินความมีนัยสำคัญของความเสี่ยง (Risk evaluation) ซึ่งเมื่อประเมินระดับความรุนแรงของปัจจัยเสี่ยงที่เกิดขึ้นแล้ว จะต้องมาพิจารณาถึงความมีนัยสำคัญประกอบ โดยพิจารณาเพิ่มเติมเปรียบเทียบกับระดับความเสี่ยงขององค์กรที่ยอมรับได้ หากระดับความรุนแรงของปัจจัยเสี่ยงนั้นสูงกว่าระดับความเสี่ยงขององค์กรที่ยอมรับได้ จะมีการประเมินนัยสำคัญในการกำหนดแผนหรือมาตรการในการจัดการความเสี่ยง

จากที่กล่าวไว้ข้างต้นถึงรายละเอียดกระบวนการบริหารความเสี่ยงของ ISO นั้น องค์ประกอบหลัก ๆ กระบวนการที่ถือว่าทำให้ ISO แตกต่างจาก COSO คือ การกำหนดบริบทที่มีผลต่อเป้าหมายขององค์กร (Establishing the context) ตามกรอบแนวคิดของ ISO ให้ความสำคัญค่อนข้างมากกับองค์ประกอบนี้เนื่องจาก ISO เน้นการบริหารความเสี่ยงที่สามารถนำไปใช้กับองค์กรต่าง ๆ ได้อย่างหลากหลายระดับ ตั้งแต่ระดับภาพรวม ระดับสายงาน ระดับฝ่ายงาน ถึงระดับผลิตภัณฑ์จนกระทั่งถึงตัวปัจเจกบุคคล ทำให้การริหารความเสี่ยง โดยที่ข้อดีคือการกำหนดบริบทที่ครอบคลุมทำให้การบรรลุเป้าหมายผ่านกระบวนการบริหารความเสี่ยงมีความเป็นไปได้สูง ส่วนข้อเสียคือ ในทางปฏิบัติข้อมูลหรือการได้มาซึ่งบริบทที่ครบถ้วนถือว่าเป็นเรื่องยาก และมีต้นทุนในการได้ข้อมูลดังกล่าวมาค่อนข้างสูง อีกทั้งการกำหนดเป้าหมายที่ลงรายละเอียดตั้งแต่องค์กร สายงาน จนถึงผลิตภัณฑ์อาจทำให้เกิดความซับซ้อนและสูญเสียทรัพยากรอย่างมาก ในขณะที่ COSO ให้ความสำคัญกับการบริหารความเสี่ยงในภาพรวมขององค์กรมากกว่าหน่วยย่อยขององค์กร ข้อดีคือง่ายต่อการบริหารจัดการ แต่ข้อเสียคืออาจทำให้การกำหนดปัจจัยเสี่ยงไม่ครบถ้วน รวมถึง COSO ยังไม่ได้อธิบายที่มาของการกำหนดเป้าหมายในรายละเอียดเท่ากับ ISO

๕. สรุป

ตามที่แนวทาง ISO ได้ถูกเสนอขึ้นมาเพื่อเป็นทางเลือกให้กับหน่วยงานต่าง ๆ สามารถนำการบริหารความเสี่ยงไปใช้กับองค์กรของตนเองได้ง่ายขึ้น อย่างไรก็ตามหากพิจารณาอย่างละเอียดแล้ว จากการวิเคราะห์เปรียบเทียบจะเห็นได้ว่า**แนวทางของ ISO กับ COSO มีส่วนที่ร่วมและสอดคล้องกันมากกว่าส่วนที่แตกต่างกัน** สำหรับองค์กรที่นำแนวทางการบริหารความเสี่ยงของ COSO มาใช้อย่างเต็มรูปแบบอาจไม่จำเป็นต้องเปลี่ยนรูปแบบมาเป็น COSO ตราบเท่าที่เมื่อองค์กรเห็นจุดอ่อนของ COSO และลดจุดบอดต่าง ๆ โดยใช้วิธีการที่ ISO เสนอแนะในบางเรื่องไม่ว่าจะเป็นการระบุปัจจัยเสี่ยงองค์กรที่อยู่บนฐานข้อมูลที่ครอบคลุมทุกด้านจากการกำหนดบริบท หรือ การสื่อสารแบบสองทางและถูกผนวกเข้ากับกระบวนการต่าง ๆ ก็ถือว่าเพียงพอในการบริหารความเสี่ยงที่มีประสิทธิผลและประสิทธิภาพ

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 ที่ปรึกษาสำนักงานรัฐบาลอิเล็กทรอนิกส์ คณะผู้บริหาร คณะทำงาน และผู้ที่มีส่วนเกี่ยวข้องทุกท่านในการให้การช่วยเหลือ และให้ความร่วมมือจนทำให้นโยบายและคู่มือบริหารความเสี่ยงของสำนักงานสามารถจัดทำขึ้นได้อย่างสมบูรณ์และสำเร็จ เพื่อให้เจ้าหน้าที่ทุกคนในสำนักงาน ใช้เป็นแนวทางในการดูแลและบริหารความเสี่ยงภายใต้ความรับผิดชอบของแต่ละคน และหวังเป็นอย่างยิ่งว่านโยบายและคู่มือบริหารความเสี่ยงฉบับนี้จะมีประโยชน์แก่ทุกคนและส่วนรวม

รายนามคณะกรรมการบริหาร

๑. **นายวรากรณ์ สามโกเศศ** ประธานกรรมการ

๒. **นายเข็มชัย ชุติวงศ์** กรรมการ
(ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : กฎหมายเทคโนโลยีสารสนเทศและการสื่อสาร)

๓. **นายไชยเจริญ อติแพทย์** กรรมการ
(ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : เทคโนโลยีสารสนเทศและการสื่อสาร)

๔. **นายณรงค์ศักดิ์ อังคะสุวพลา** กรรมการ
(ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : บริหารจัดการสาธารณสุข)

๕. **นายปรีชา วัชราภัย** กรรมการ
(ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : บริหารจัดการและทรัพยากรบุคคล)

๖. **นายวิเชียร ชิดชนกนารถ** กรรมการ
(ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : เทคโนโลยีสารสนเทศและการสื่อสาร)

๗. **นางทรงพร โกมลสุรเดช** กรรมการ
(ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร)

๘. **นายชูเกียรติ รัตนชัยชาญ** กรรมการ
(เลขาธิการสำนักงานคณะกรรมการพัฒนาระบบราชการ)

๙. **นายสมศักดิ์ โชติรัตนะศิริ** กรรมการ
(ผู้อำนวยการสำนักงบประมาณ)

๑๐. **นายทวีศักดิ์ กออนันตกูล** กรรมการ
(ผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ)

๑๑. **นายศักดิ์ เสกขุนทด** กรรมการและเลขานุการ
(ผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์)

รายนามคณะอนุกรรมการด้านการบริหารความเสี่ยง

๑.	นายทวีศักดิ์ กออนันตกุล	ที่ปรึกษา
๒.	นายรอม หิรัญพฤกษ์	ที่ปรึกษา
๓.	นายไชยเจริญ อติแพทย์	ประธานอนุกรรมการ
๔.	นางสาววลัยรัตน์ ศรีอรุณ	อนุกรรมการ
๕.	พันเอกเจียรนัย วงศ์สอาด	อนุกรรมการ
๖.	นายสรายุทธ์ นาทะพันธ์	อนุกรรมการ
๗.	นายสุจินดา สุขุม	อนุกรรมการ
๘.	นายศักดิ์ เสกขุนทด	อนุกรรมการ
๙.	นายชรินทร์ ธีรฐิตยางกูร	เลขานุการ
๑๐.	นายโชติพันธ์ ไชยสุวกุล	ผู้ช่วยเลขานุการ

รายนามที่ปรึกษา

๑.	นางสาววลัยรัตน์ ศรีอรุณ	ที่ปรึกษาสำนักงานรัฐบาลอิเล็กทรอนิกส์
๒.	นางจารุพร ไวยนันท์	ที่ปรึกษาสำนักงานรัฐบาลอิเล็กทรอนิกส์

รายนามคณะผู้บริหาร

๑.	**นายศักดิ์ เสกขุนทด**	ผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์
๒.	**นางไอรดา เหลืองวิไล**	รองผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์ (ด้านบริหาร)
๓.	**นางสาวอภิณห์พร อังคกมลเศรษฐ์**	รองผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์ (ด้านเทคนิค)
๔.	**นายนิเวช มิ่งมิตรโอฬาร**	ผู้อำนวยการฝ่ายวิศวกรรมและปฏิบัติการ
๕.	**นางสาวเรขา ศรีสมบูรณ์**	ผู้อำนวยการฝ่ายบริหารประสิทธิภาพองค์กร
๖.	**นางศุภวรรณ ธาราโภคากุล**	ผู้อำนวยการฝ่ายอำนวยการ
๗.	**นายอาศิส อัญญะโพธิ์**	ผู้อำนวยการฝ่ายพัฒนาและจัดการแอปพลิเคชัน
๘.	**นายวิบูลย์ ภัทรพิบูล**	ผู้อำนวยการฝ่ายบริการให้คำปรึกษา
๙.	**นายชรินทร์ ธีรฐิตยางกูร**	ผู้อำนวยการฝ่ายนโยบายและยุทธศาสตร์
๑๐.	**นางสาวนันทวัน วงศ์ขจรกิตติ**	ผู้อำนวยการฝ่ายนวัตกรรม

รายนามคณะผู้จัดทำ

๑.	นายชรินทร์ ธีรฐิตยางกูร	ผู้อำนวยการฝ่ายนโยบายและยุทธศาสตร์
๒.	นายโชติพันธ์ ไชยสุวกุล	ผู้จัดการส่วนบริหารความเสี่ยง
๓.	ว่าที่ร้อยตรี ทวีชัย พรมขันธ์	เจ้าหน้าที่บริหารความเสี่ยงอาวุโส
๔.	นายชติพจน์ ศรีเมือง	เจ้าหน้าที่บริหารความเสี่ยงอาวุโส
๕.	นายวิทวัส พานิช	เจ้าหน้าที่บริหารความเสี่ยง ๑
๖.	นางสาวรัชตา ด่านซ้าย	เจ้าหน้าที่บริหารความเสี่ยง ๑

ออกแบบโดย

๑.	นายโชติพันธ์ ไชยสุวกุล	ผู้จัดการส่วนบริหารความเสี่ยง
๒.	นายชติพจน์ ศรีเมือง	เจ้าหน้าที่บริหารความเสี่ยงอาวุโส
๓.	นายวิทวัส พานิช	เจ้าหน้าที่บริหารความเสี่ยง ๑

ปรับปรุง ครั้งที่ ๑ เดือนพฤศจิกายน ๒๕๕๗

ครั้งที่ ๒ เดือนธันวาคม ๒๕๕๘

Risk Management Policy and Manual 2015
นโยบายและคู่มือบริหารความเสี่ยง ปี ๒๕๕๘

โดย สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ EGA
Electronic Government Agency (Public Organization) or EGA
www.ega.or.th I 02-612-6060 I contact@ega.or.th

ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
Ministry of Information and Communication Technology