ประกาศสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
ที่ ๔ /๒๕๕๕
เรื่อง นโยบายการบริหารความเสี่ยง สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

.....

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

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

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

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

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๒ สิงหาคม พ.ศ. ๒๕๕๕

(นายศักดิ์ เสกขุนทด)
ผู้อำนวยการ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

รายละเอียดประกอบ
นโยบายบริหารความเสี่ยง
(Enterprise Risk Management Policy)

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 เป้าหมายและวัตถุประสงค์ อันจะเป็นการสร้างความรับผิดชอบอย่างทั่วถึงและเป็นไปในทิศทางเดียวกันทั่วทั้งสำนักงานได้อย่างมีประสิทธิภาพ

นโยบายการบริหารความเสี่ยง (Enterprise Risk Management Policy) จัดทำขึ้นเพื่อวัตถุประสงค์ ดังนี้

๑) เพื่อใช้เป็นแนวทางให้กับผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งองค์กร ในการเป็นส่วนหนึ่งของการพัฒนากระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์

๒) เพื่อให้สำนักงานมีกรอบการดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่อาจส่งผลให้เกิดความเสี่ยงทุกด้านได้อย่างเป็นระบบและมีมาตรฐาน รวมทั้งมีการดำเนินการเพื่อสร้างพื้นฐานในการป้องกันความเสี่ยงระยะยาวให้กับสำนักงานที่สำคัญ

๓) เพื่อเป็นกลไกในการพัฒนาองค์ความรู้ด้านการบริหารความเสี่ยงให้เกิดขึ้นกับผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งสำนักงาน และสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน

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

๓. องค์ประกอบการบริหารความเสี่ยง

๓.๑ แนวทางการกำหนดกลยุทธ์การบริหารความเสี่ยง

สำนักงานต้องกำหนดกลยุทธ์ในการบริหารความเสี่ยงโดยคำนึงถึงสาระสำคัญ ดังนี้

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

๒) ความสอดคล้องกับแนวทางมาตรฐานของหน่วยงานกำกับดูแล ข้อกำหนดของกฎหมาย ระเบียบประกาศ หลักเกณฑ์ และแนวทางปฏิบัติที่ดี

๓) สำนักงานจะต้องทบทวนกลยุทธ์การบริหารความเสี่ยงอย่างน้อยปีละ ๑ ครั้งตามแผนประจำปี หรือทบทวนทันทีที่มีเหตุการณ์เปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้ทราบถึงปัญหา อุปสรรค ที่ส่งผลต่อการบรรลุเป้าหมายการบริหารความเสี่ยง และเพื่อสร้างความมั่นใจถึงการบรรลุเป้าหมายโดยรวมของสำนักงาน

๓.๒ โครงสร้างการบริหารความเสี่ยงและบทบาทหน้าที่รับผิดชอบการบริหารความเสี่ยง

สำนักงานต้องจัดให้มีโครงสร้างหน้าที่ของคณะอนุกรรมการและหน่วยงาน เพื่อกำกับดูแลและรับผิดชอบด้านการบริหารความเสี่ยง โดยโครงสร้างหน้าที่ต้องมีความชัดเจน สอดคล้องกับการบริหารความเสี่ยงของสำนักงาน และเหมาะสมกับการดำเนินงานขององค์กร รวมถึงมีความเป็นอิสระและมีการถ่วงดุลอำนาจอย่างเหมาะสม ดังนี้

๑) บทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการที่เกี่ยวข้องกับการบริหารความเสี่ยง

คณะกรรมการ	บทบาท หน้าที่ และความรับผิดชอบ
คณะกรรมการบริหาร สำนักงานรัฐบาลอิเล็กทรอนิกส์	๑. อนุมัตินโยบายและกลยุทธ์การบริหารความเสี่ยงเพื่อประกาศใช้ ๒. กำกับดูแลให้มีการดำเนินงานที่เป็นไปตามหลักเกณฑ์ของทางการ และเป็นไปตามหลักการกำกับดูแล กิจการที่ดีมีความโปร่งใส เป็นธรรมต่อทุกหน่วยงานที่เกี่ยวข้อง
คณะอนุกรรมการด้าน บริหารความเสี่ยง	๑. เสนอแนะนโยบายการบริหารความเสี่ยงและกรอบของการบริหารความเสี่ยงต่อคณะกรรมการ ๒. ให้คำปรึกษาและเสนอแนะการจัดทำแผนบริหารความเสี่ยงเพื่อให้บรรลุเป้าหมายตามแผนปฏิบัติงานของสำนักงาน เพื่อเสนอต่อคณะกรรมการ ๓. เสนอแนะแนวทาง ในการบริหารจัดการหรือการดำเนินงาน เพื่อลดผลกระทบและความเสี่ยงที่อาจจะเกิดขึ้นกับสำนักงาน ๔. พิจารณาผลการประเมินและติดตามความมีประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงเพื่อรายงานต่อคณะกรรมการ ๕. ในกรณีการพิจารณากลั่นกรอง ให้คำปรึกษาประเมินหรือวิเคราะห์ในเรื่องใดที่จำเป็นต้องมีผู้เชี่ยวชาญเฉพาะด้านในสาขาที่เกี่ยวข้องเข้าร่วมพิจารณาในรายละเอียด ให้คณะอนุกรรมการเชิญบุคคลดังกล่าวเข้าร่วมพิจารณากับคณะอนุกรรมการเป็นคราวๆไป โดยให้บุคคลดังกล่าวได้รับค่าตอบแทนตามระเบียบสำนักงาน ๖. ปฏิบัติงานอื่นใดตามที่ประธานกรรมการ หรือคณะกรรมการมอบหมาย
คณะอนุกรรมการตรวจสอบ	๑. สอบทานให้สำนักงานมีระบบการควบคุมภายในระบบการตรวจสอบภายในและระบบการบริหารความเสี่ยงที่เหมาะสมและมีประสิทธิผล

	๒. ให้คำปรึกษาและเสนอแนะแนวทางการพัฒนาปรับปรุงระบบการควบคุมภายใน ระบบการตรวจสอบภายในและระบบการบริหารความเสี่ยงที่สำคัญและจำเป็น เพื่อให้มีความทันสมัยอยู่เสมอ ๓. กำกับดูแลการปฏิบัติให้สอดคล้องตามนโยบาย ข้อบังคับ กฎระเบียบ ประกาศ คำสั่ง มติคณะรัฐมนตรี และกฎหมายอื่นๆที่เกี่ยวข้อง

๒) บทบาท หน้าที่ และความรับผิดชอบของผู้บริหาร หน่วยงาน และเจ้าหน้าที่ที่เกี่ยวข้องกับการบริหารความเสี่ยง

หน่วยงาน	**บทบาท/หน้าที่/ความรับผิดชอบ**
ผู้อำนวยการ เจ้าหน้าที่และลูกจ้างทุกคนในสำนักงาน	๑. เป็นเจ้าของความเสี่ยง (Risk Owner) มีหน้าที่รับผิดชอบการวิเคราะห์ ระบุ และประเมินความเสี่ยง กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือแผนบริหารความเสี่ยงของหน่วยงาน/โครงการ หรืองานที่อยู่ในความรับผิดชอบ ๒. ติดตามและรายงานความเสี่ยงให้ผู้บังคับบัญชาทราบตามลำดับชั้น ตลอดจนคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอเพื่อให้การบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ
ผู้บริหาร	๑. ผู้บริหารตั้งแต่ระดับผู้จัดการขึ้นไปมีหน้าที่กำกับ ดูแลหน่วยงาน/โครงการให้มีการบริหารและจัดการความเสี่ยง และเป็นเจ้าของความเสี่ยง (Risk Owner)
คณะทำงานการบริหารความเสี่ยงด้าน/เรื่อง ต่าง ๆ	๑. มีหน้าที่ตามที่ได้รับมอบหมายจากคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ หรือคณะอนุกรรมการด้านการบริหารความเสี่ยง
ส่วนพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง	๑. จัดและทบทวนนโยบายและกลยุทธ์ในการดำเนินงานด้านการบริหารความเสี่ยงเพื่อนำเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยง

	๒. จัดทำและทบทวนเครื่องมือในการวัด ติดตาม และควบคุมความเสี่ยง เพื่อเสนอต่อ คณะอนุกรรมการด้านการบริหารความเสี่ยง ๓. ติดตามและรายงานสถานะความเสี่ยงต่อ คณะอนุกรรมการด้านการบริหารความเสี่ยง
ส่วนตรวจสอบภายใน	๑. สอบทานและประเมินความเพียงพอ ความมีประสิทธิภาพและประสิทธิผลของกระบวนการบริหารความเสี่ยง ระบบการควบคุมภายใน และระบบที่ส่งเสริมการกำกับดูแลกิจการที่ดี ๒. ตรวจสอบการดำเนินงานตามแผนงานหรือโครงการเพื่อสอดคล้องกับวัตถุประสงค์ และเป้าหมายที่กำหนดไว้อย่างมีประสิทธิภาพและประสิทธิผล
สำนัก/ส่วน	๑. ควบคุมดูแลการปฏิบัติงานในสำนัก/ส่วน ให้เป็นไปตามนโยบายและกลยุทธ์การบริหารความเสี่ยง รวมทั้งจัดให้มีระบบบริหารความเสี่ยงที่มีประสิทธิภาพ
Risk – Internal Control Officer (RICO)	๑. รับผิดชอบในการประสานงาน การประเมินความเสี่ยงการควบคุมภายใน และการปฏิบัติตามกฎเกณฑ์ รวมทั้งเผยแพร่ความรู้ที่เกี่ยวข้องแก่พนักงานในหน่วยงานของตนเอง

๓.๓) การจัดแบ่งประเภทความเสี่ยง

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

๑) ด้านนโยบายและกลยุทธ์

๒) ด้านการเงินและงบประมาณ

๓) ด้านการปฏิบัติงาน

๔) ด้านกฎหมาย กฎระเบียบ

๕) ด้านระบบเทคโนโลยีสารสนเทศ

ซึ่งสามารถจัดทำเป็นนโยบายที่เกี่ยวข้องด้านการบริหารความเสี่ยง ๕ นโยบาย ประกอบด้วย

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

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

๓) นโยบายด้านการปฏิบัติงาน หมายถึง ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดความชัดเจนของนโยบายการปฏิบัติงานที่ดี นโยบายการกำกับดูแลกิจการอย่างมีธรรมาภิบาล และขาดระบบการควบคุมที่เกี่ยวข้องกับกระบวนการปฏิบัติงานทั้งหมด โดยเฉพาะการไม่ได้ประเมินความเสี่ยงของโครงการของสำนักงาน

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

๕) นโยบายด้านระบบเทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่ครอบคลุมการบริหารจัดการและประสิทธิภาพการดำเนินงานด้านเทคโนโลยีสารสนเทศ ซึ่งเกี่ยวข้องกับความมั่งคงปลอดภัย (Security) ความถูกต้องเชื่อถือได้ของข้อมูล (Integrity) และความพร้อมใช้งานของระบบงานและข้อมูล (Availability)

๔. ขอบเขต

เพื่อใช้เป็นแนวทางให้กับผู้บริหาร เจ้าหน้าที่ และลูกจ้างของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ในการพัฒนากระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานของสำนักงานให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์

๕. นิยาม

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือความเป็นไปที่อาจเกิดขึ้นและส่งผลกระทบทั้งในด้านลบและด้านบวกต่อการบรรลุวัตถุประสงค์หรือเป้าหมายของสำนักงาน

ความเสี่ยงที่มีอยู่ (Inherent Risk) หมายถึง ความเสี่ยงที่มีอยู่แล้วในสำนักงานโดยที่หน่วยงานยังไม่ได้มีการจัดการใด ๆ เพื่อที่จะเปลี่ยนแปลงโอกาสที่จะเกิดหรือผลกระทบของความเสี่ยงนั้น

การควบคุมภายใน (Internal Control) หมายถึง กระบวนการที่กำหนดขึ้นและนำมาใช้โดยคณะกรรมการบริหาร ผู้บริหารเจ้าหน้าที่ และลูกจ้างของสำนักงาน เพื่อความมีประสิทธิผลและประสิทธิภาพของการดำเนินงาน และการปฏิบัติตามกฎหมาย ระเบียบ ประกาศ คำสั่ง หรือมาตรฐานที่ดี

โอกาสที่จะเกิดความเสี่ยง (Risk Likelihood) หมายถึง ความน่าจะเป็นที่ความเสี่ยงหรือเหตุการณ์จะเกิดขึ้นและส่งผลกระทบต่อสำนักงาน

ผลกระทบของความเสี่ยงที่เกิดขึ้น (Risk Impact) หมายถึง ผลกระทบทั้งในด้านลบและด้านบวกต่อการบรรลุวัตถุประสงค์หรือเป้าหมายของหน่วยงาน และสำนักงาน

ความเสี่ยงที่เหลืออยู่ (Residual Risk) หมายถึง ความเสี่ยงที่เหลืออยู่หลังจากหน่วยงานได้ดำเนินการที่จะเปลี่ยนแปลงระดับของโอกาสที่จะเกิด หรือผลกระทบของความเสี่ยงแล้ว

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ระดับความเสี่ยงที่สำนักงานยอมรับได้ ซึ่งได้กำหนดไว้

ความมั่นคงปลอดภัย (Security) หมายถึง การจัดการป้องกันการเข้าถึง การเข้าไปแก้ไขเปลี่ยนแปลง การทำลาย การเปิดเผยข้อมูล การรักษาความลับ (Confidential) ทั้งระหว่างที่กำลังพัฒนาระบบงาน หรือในการจัดส่งข้อมูลการประมวลผล หรือการจัดเก็บรักษาข้อมูลในระบบงาน การจัดเก็บระบบงาน โดยจัดการป้องกันให้มีความเหมาะสมและความสำคัญของข้อมูลรวมถึงระบบงานด้วย

ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity) หมายถึง ข้อมูลที่จะส่งมอบให้กับผู้ใช้ข้อมูล (End User) เป็นข้อมูลที่มีความสมบูรณ์ ถูกต้อง ครบถ้วน ซึ่งจะทำให้การดำเนินงานและการบริหารงานขององค์กรมีประสิทธิภาพ

ความพร้อมใช้งานของระบบงานและข้อมูล (Availability) หมายถึง เรื่องของการจัดส่งข้อมูลไปให้ผู้ที่ต้องการใช้ข้อมูลได้รวดเร็วทันเวลา และสามารถให้ข้อมูลได้อย่างต่อเนื่องในเวลาที่เหมาะสม เพื่อสนับสนุนการดำเนินงานขององค์กร ทั้งนี้องค์กรต้องมีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ซึ่งเป็นแผนการดำเนินงานหลักขององค์กร และมีแผนงานรองประกอบแผนงานหลักได้แก่ แผนการกู้ระบบกลับคืน (Disaster Recovery Plan) แผนสำรองฉุกเฉิน (Contingency Plan) และแผนรองรับเหตุการณ์ไม่คาดว่าจะเกิดขึ้น (Incident Response Plan)

๖. กระบวนการบริหารความเสี่ยง

๑) สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมภายในองค์กรครอบคลุมถึงแนวนโยบายโดยทั่วไปของสำนักงาน ซึ่งเป็นพื้นฐานที่สำคัญของกรอบการบริหารความเสี่ยง และการจัดการกับความเสี่ยงโดยผู้บริหาร เจ้าหน้าที่และลูกจ้างทั้งหมดในสำนักงาน ซึ่งมีอิทธิพลต่อความตระหนักถึงความเสี่ยงของบุคลากรของสำนักงาน และช่วยก่อให้เกิดแนวทางการบริหารความเสี่ยงของสำนักงาน

๒) การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

สำนักงานต้องกำหนดให้หน่วยงานทุกระดับมีการกำหนดวัตถุประสงค์และเป้าหมายการดำเนินงานที่สอดคล้องกับวิสัยทัศน์ พันธกิจ กลยุทธ์ และเป้าหมายโดยรวมของสำนักงาน โดยต้องมีความชัดเจน สามารถวัดหรือประเมินผลได้

๓) การระบุเหตุการณ์ (Event Identification)

คือ การระบุเหตุการณ์ความเสี่ยงหรือความไม่แน่นอนที่อาจเกิดขึ้น โดยพิจารณาจากปัจจัยทั้งภายในและภายนอกสำนักงาน ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของสำนักงาน

๔) การประเมินความเสี่ยง(Risk Assessment)

สำนักงานต้องกำหนดให้หน่วยงานทุกระดับประเมินความเสี่ยงของทุกปัจจัยเสี่ยงที่ได้ระบุไว้ โดยอ้างอิงจากเกณฑ์วัดระดับความเสี่ยง โอกาสและผลกระทบ ที่สำนักงานกำหนดไว้ โดยอาจใช้ฐานข้อมูลในอดีตหรือการคาดการณ์ในอนาคตเพื่อประกอบการประเมินระดับความเสี่ยง

๕) การตอบสนองความเสี่ยง(Risk Response)

เป็นการระบุว่ามีทางเลือกใดบ้างที่สามารถใช้ในการจัดการความเสี่ยง มีความเหมาะสม และนำไปปฏิบัติเป็นส่วนหนึ่งของการบริหารความเสี่ยงของสำนักงาน ซึ่งจะต้องประเมินผลกระทบที่มีต่อโอกาสที่จะเกิด รวมทั้งต้นทุนและประโยชน์ที่ได้รับ เพื่อให้ความเสี่ยงที่เหลืออยู่ภายในช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ ทั้งนี้การตอบสนองต่อความเสี่ยงแบ่งเป็น ๔ ประการ คือ การยอมรับ (Accept) การลด (Reduce) การหลีกเลี่ยง/ยกเลิก (Avoid/Terminate) และการโอนความเสี่ยง (Transfer)

๖) กิจกรรมการควบคุม (Control Activities)

สำนักงานต้องจัดให้มีการควบคุมความเสี่ยงและเพดานความเสี่ยงที่เพียงพอและเหมาะสมตามแต่ละประเภทความเสี่ยงและต้องอยู่ภายใต้ระดับความเสี่ยงที่สำนักงานยอมรับได้ รวมทั้งสอดคล้องกับมาตรฐานและหลักเกณฑ์ของหน่วยงานกำกับดูแล แนวทางปฏิบัติที่ดี ตลอดจนนโยบายบริหารความเสี่ยงกับทิศทางและกลยุทธ์การดำเนินงานของสำนักงาน พร้อมทั้งกำหนดกระบวนการปฏิบัติตามการควบคุมความเสี่ยงและเพดานความเสี่ยงที่กำหนดไว้ แนวทางการอนุมัติข้อยกเว้นกรณีจำเป็นหรือเหตุการณ์ไม่ปกติต่าง ๆ รวมถึงการทบทวนการควบคุมความเสี่ยงและเพดานความเสี่ยงดังกล่าวเป็นระยะ เพื่อให้มีประสิทธิภาพในการควบคุมและป้องกันความเสี่ยงให้กับสำนักงาน

๗) สารสนเทศและการสื่อการ (Information and Communication)

สำนักงานต้องจัดให้มีระบบสารสนเทศและการสื่อสารเกี่ยวกับการบริหารความเสี่ยงด้านต่าง ๆ ได้อย่างครบถ้วน เพียงพอ และเหมาะสมกับกลยุทธ์การบริหารความเสี่ยง การดำเนินงานของสำนักงานผ่านช่องทางการสื่อสารที่มีประสิทธิภาพ โดยมีการสื่อสารภายในสำนักงานอย่างสม่ำเสมอในเรื่องความสำคัญของการบริหารความเสี่ยงจากผู้บริหารถึงเจ้าหน้าที่ (Top-Down) และจากเจ้าหน้าที่ถึงผู้บริหาร (Bottom-Up) รวมถึงการสื่อสารภายนอกสำนักงานถึงลูกค้า ผู้มีส่วนได้ส่วนเสีย และสาธารณชนทั่วไป ที่ครอบคลุมถึงนโยบาย กระบวนการ โครงสร้าง และปัจจัยสนับสนุน รวมทั้งแสดงถึงการที่คณะกรรมการบริหารและผู้บริหารได้ให้ความสำคัญกับการบริหารความเสี่ยงเพื่อให้เข้าใจแนวทางการบริหารความเสี่ยง และสามารถประเมินความมีประสิทธิภาพของระบบบริหารความเสี่ยงของสำนักงานได้ อันจะเป็นประโยชน์ต่อการตัดสินใจดำเนินงาน ใช้บริการ หรือร่วมดำเนินงานกับสำนักงาน พร้อมทั้งจัดให้มีการทบทวนและปรับปรุงระบบสารสนเทศและการสื่อสารอยู่เสมอ

๘) การติดตามและประเมินผล (Monitoring)

สำนักงานต้องกำหนดให้หน่วยงานทุกระดับมีการติดตามและเมินผลความเสี่ยง พร้อมทั้งรายงานผลให้ผู้บริหารและคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ โดยติดตามจากแผนหรือมาตรการจัดการความเสี่ยง ดัชนีชี้วัดความเสี่ยง (Key Risk Indicators: KRIs) และผลการบริหารความเสี่ยง รวมถึง

ติดตามดูแลกิจกรรมการดำเนินงานและเหตุการณ์ที่เกิดขึ้นภายในและภายนอกสำนักงาน ซึ่งอาจส่งผลกระทบวัตถุประสงค์และเป้าหมายการดำเนินงานหรือก่อให้เกิดความเสียหายต่อสำนักงาน เพื่อประโยชน์การบริหารจัดการความเสี่ยงในภาพรวมของสำนักงาน

๗. ระบบสนับสนุนการบริหารความเสี่ยง

สำนักงานต้องจัดให้มีระบบสนับสนุนการบริหารความเสี่ยง เพื่อให้การบริหารความเสี่ยงสัมฤทธิ์ผลและเกิดประโยชน์สูงสุดแก่สำนักงาน ดังนี้

๑) การพัฒนาเครื่องมือบริหารความเสี่ยง

สำนักงานต้องจัดให้มีการพัฒนาเครื่องมือในการบริหารความเสี่ยงตามแต่ละประเภทความเสี่ยง ให้มีคุณภาพและมาตรฐานตามหลักเกณฑ์ของหน่วยงานกำกับดูแล แนวทางปฏิบัติที่ดี และต้องเหมาะสมสอดคล้องกับเป้าหมายในการบริหารความเสี่ยงของสำนักงาน รวมทั้งต้องมีประสิทธิภาพในการควบคุมและป้องกันความเสี่ยงที่อาจเกิดขึ้นกับสำนักงาน

๒) การควบคุมความเสี่ยงและเพดานความเสี่ยง

สำนักงานต้องจัดให้มีการควบคุมความเสี่ยงและเพดานความเสี่ยงที่เพียงพอและเหมาะสมตามแต่ละประเภทความเสี่ยง และต้องอยู่ภายใต้ระดับความเสี่ยงที่สำนักงานยอมรับได้ รวมทั้งสอดคล้องกับมาตรฐานและหลักเกณฑ์ของหน่วยงานกำกับดูแล แนวทางปฏิบัติที่ดี ตลอดจนนโยบายบริหารความเสี่ยงกับทิศทางและกลยุทธ์การดำเนินงานของสำนักงาน พร้อมทั้งกำหนดกระบวนการปฏิบัติตามการควบคุมความเสี่ยงและเพดานความเสี่ยงที่กำหนดไว้ แนวทางการอนุมัติข้อยกเว้นกรณีจำเป็นหรือเหตุการณ์ไม่ปกติต่าง ๆ รวมถึงกำหนดการทบทวนการควบคุมความเสี่ยงและเพดานความเสี่ยงดังกล่าวเป็นระยะ เพื่อให้มีประสิทธิภาพในการควบคุมและป้องกันความเสี่ยงให้กับสำนักงาน

๓) การวิเคราะห์ภาพรวมของความเสี่ยง

สำนักงานต้องจัดให้มีกระบวนการวิเคราะห์และจัดทำแบบจำลองที่เหมาะสม เพื่อวิเคราะห์ภาพรวมของความเสี่ยงที่มีต่อเป้าหมายสำนักงาน กรณีที่มีปัจจัยเสี่ยงมากกว่า ๑ ปัจจัยเกิดขึ้นพร้อมกัน เพื่อสะท้อนถึงผลกระทบโดยรวมสูงสุดที่สำนักงานยอมรับได้ อันจะเป็นการสร้างความมั่นใจว่าระดับความเสี่ยงในภาพรวมของสำนักงานอยู่ในวิสัยที่สามารถจัดการได้ ทั้งนี้สำนักงานจะต้องมีการทดสอบความแม่นยำของแบบจำลองเพื่อให้มีความเหมาะสมอยู่เสมอ

๔) การส่งเสริมและสนับสนุนให้เกิดความตระหนักด้านการบริหารความเสี่ยง

สำนักงานต้องจัดให้มีกระบวนการเพื่อส่งเสริมและสนับสนุนให้เกิดความตระหนักด้านการบริหารความเสี่ยงอย่างต่อเนื่องและสม่ำเสมอ เพื่อให้ผลักดันให้คณะกรรมการบริหาร ผู้บริหาร เจ้าหน้าที่และลูกจ้างทุกคนในสำนักงานสามารถดำเนินการตามกรอบนโยบายบริหารความเสี่ยงได้อย่างถูกต้อง เหมาะสม และมีประสิทธิภาพ มีการนำกระบวนการบริหารความเสี่ยงไปปฏิบัติจนเป็นส่วนหนึ่งของกิจกรรมการดำเนินงานปกติประจำวัน และเป็นส่วนหนึ่งที่สำคัญของการพิจารณาผลตอบแทน ความดีความชอบ เพื่อให้การบริหารความเสี่ยงเกิดเป็นวัฒนธรรมองค์กรที่นำสำนักงานรัฐบาลอิเล็กทรอนิกส์ไปสู่การเติบโตอย่างยั่งยืน

๕) การบูรณาการระหว่าง Corporate Governance + Risk Management + Compliance (GRC)

สำนักงานต้องจัดให้มีการบูรณาการกระบวนการทำงานเกี่ยวกับการกำกับดูแลกิจการ (Corporate Governance) การบริหารความเสี่ยง (Risk Management) และการปฏิบัติตามกฎหมาย ระเบียบ ประกาศ คำสั่ง หรือมาตรฐานที่ดี (Compliance) เพื่อให้บรรลุถึงผลการดำเนินงานที่เกิดจากการมีส่วนร่วมของหน่วยงานต่าง ๆ คณะกรรมการบริหาร ผู้บริหาร เจ้าหน้าที่และลูกจ้างในสำนักงาน อย่างมีประสิทธิภาพและประสิทธิผลให้กับสำนักงาน

๘. การปฏิบัติที่ไม่เป็นไปตามนโยบายบริหารความเสี่ยง

กรณีมีการปฏิบัติที่ไม่เป็นไปตามนโยบายให้ดำเนินการ ดังนี้

๑) หน่วยงานผู้รับผิดชอบ (Risk Owner) ต้องกำหนดให้การปฏิบัติตามนโยบายบริหารความเสี่ยงเป็นส่วนหนึ่งในแผนปฏิบัติงานประจำปี และเป็น KPI ด้วย

๒) ส่วนงานพัฒนาคุณภาพองค์กรและบริหารความเสี่ยง สรุปรายงานผลการปฏิบัติที่ไม่เป็นไปตามนโยบายต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง และคณะอนุกรรมการด้านการบริหารความเสี่ยงรายงานต่อคณะกรรมการบริหาร

๓) คณะกรรมบริหาร คณะอนุกรรมการด้านต่าง ๆ ผู้บริหาร สำนัก/ส่วน เจ้าหน้าที่หรือลูกจ้างในสำนักงาน เมื่อพบเหตุการณ์ความเสี่ยงเกิดขึ้นภายใน หรือภายนอกโดยอาจมีผลกระทบต่อกิจการการดำเนินงานของสำนักงาน ให้ปฏิบัติตามคู่มือการแจ้งข่าวสาร (Call Tree Manual) ซึ่งเป็นส่วนหนึ่งของแผนการรองรับธุรกิจอย่างต่อเนื่อง (Business Continuity Plan)

หน่วยงานผู้รับผิดชอบ (Risk Owner) และ/หรือหน่วยงานที่เกี่ยวข้อง ต้องรายงานต่อผู้บังคับบัญชาตามลำดับชั้นและผู้บริหารทันที

หากหน่วยงานผู้รับผิดชอบ(Risk Owner) และ/หรือหน่วยงานที่เกี่ยวข้องใด พบการปฏิบัติที่ไม่เป็นไปตามนโยบายความเสี่ยงแล้วเพิกเฉย ไม่รายงานและก่อให้เกิดความเสียหายแก่องค์กร ถือว่ามีความผิดตามข้อบังคับคณะกรรมการบริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ ว่าด้วยการบริหารงานบุคคล พ.ศ. ๒๕๕๕ หมวด ๙ วินัย ส่วนที่ ๑ การรักษาวินัยและความผิดทางวินัย

๙. การทบทวนและปรับปรุงนโยบายบริหารความเสี่ยง

นโยบายบริหารความเสี่ยงต้องได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือทบทวนเมื่อเกิดเหตุการณ์ที่มีผลกระทบที่สำคัญ เช่น การเกิดภัยธรรมชาติ การจลาจล เป็นต้น เพื่อปรับปรุงนโยบายบริหารความเสี่ยงให้มีความเหมาะสมสอดคล้องกับสถานการณ์ความเสี่ยงในการดำเนินงานของสำนักงาน โดยส่วนพัฒนาคุณภาพองค์กร

และบริหารความเสี่ยงเป็นหน่วยงานกลางทำหน้าที่ทบทวนและปรับปรุงนโยบายการบริหารความเสี่ยงเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยงเห็นชอบ เพื่อเสนอต่อคณะกรรมการบริหารเพื่ออนุมัติต่อไป

ภาคผนวก

หน่วยงานที่เกี่ยวข้อง

๑. สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.)
๒. สำนักงานการตรวจเงินแผ่นดิน
๓. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

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.mict.go.th
๕. www.ega.or.th