เอกสารประกอบ (Supporting Document)

นโยบายและคู่มือบริหารความเสี่ยง

(SP-S14-001)

แก้ไขครั้งที่ 0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

Digital Government Development Agency (Public Organization

การควบคุมเอกสาร

ผู้เรียบเรียง/ผู้จัดทำ	ผู้ตรวจสอบ/ผู้ทบทวน	ผู้อนุมัติ
นางสาวสิรีพิชญ์ สุขผล	นายภัทรพงศ์ วงศ์สุวัฒน์	นางสาวทิสวรรณ ชูปัญญา
นักวิเคราะห์อาวุโส 1	ผจก. ส่วนบริหารความเสี่ยง	ผอ. ฝ่ายกลยุทธ์องค์กร

ครั้งที่	วันที่	รายละเอียดการแก้ไข
0	1/5/2566	ประกาศครั้งแรก - เปลี่ยนแปลง DGA Logo ให้สอดคล้องตามที่ สนง. ประกาศ - เปลี่ยนแปลงหมายเลขเอกสารจาก SP-S17-001 เป็น SP-S14-001 เพื่อให้สอดคล้องตามที่มีการเปลี่ยนแปลงกระบวนการหลักและกระบวนการสนับสนุนของ สพร. - ปรับปรุงเนื้อหาและขั้นตอนปฏิบัติให้เป็นปัจจุบัน - ปรับปรุงแบบฟอร์มแผนและรายงานผลการบริหารความเสี่ยงและควบคุมภายใน รวมทั้งเกณฑ์การประเมินความเสี่ยง (โอกาสเกิดและผลกระทบ) ตามที่ได้รับความเห็นชอบจากคณะกรรมการ สพร. ในคราวประชุม ครั้งที่ 4/2566 เมื่อวันที่ 19 เมษายน 2566

RISK MANAGEMENT
POLICY & MANUAL

นโยบายและคู่มือ บริหารความเสี่ยง

สำนักงานพัฒนารัฐบาลดิจิทัล
(องค์การมหาชน)

DIGITAL GOVERNMENT DEVELOPMENT
AGENCY (PUBLIC ORGANIZATION)

โครงสร้างเนื้อหา

ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ที่ ๑๖ / ๒๕๖๔
เรื่อง นโยบายการบริหารความเสี่ยง
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ตระหนักถึงความสำคัญของการบริหารความเสี่ยง จึงได้จัดให้มีการบริหารความเสี่ยงขึ้น ซึ่งครอบคลุมการดำเนินงานภายในสำนักงาน โดยมีการกำหนดคู่มือบริหารความเสี่ยงองค์กร และคู่มือบริหารความเสี่ยง ๕ ด้าน ซึ่งประกอบด้วย ด้านนโยบายและกลยุทธ์ ด้านการปฏิบัติงาน ด้านการเงิน ด้านกฎหมาย กฎระเบียบ และด้านเทคโนโลยีสารสนเทศ เป็นแนวทางในการบริหารความเสี่ยง เพื่อให้การดำเนินงานของสำนักงานให้มีประสิทธิภาพ ลดความสูญเสีย และสร้างมูลค่าเพิ่มให้กับองค์กร สามารถบรรลุตามภารกิจขององค์กรตามหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance) ทั้งนี้ กระทรวงการคลังได้ประกาศหลักเกณฑ์กระทรวงการคลังว่าด้วยด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒ และแนวทางบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร พ.ศ. ๒๕๖๔ กำหนดให้หน่วยงานของรัฐมีหน้าที่ในการจัดให้มีการบริหารจัดการความเสี่ยงตามมาตรฐานและหลักเกณฑ์ที่สอดคล้องกับพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ หมวด ๔ การบัญชี การรายงานและการตรวจสอบ เพื่อให้การบริหารจัดการความเสี่ยงของหน่วยงานของรัฐมีประสิทธิภาพ รวมถึงยกระดับการบริหารจัดการความเสี่ยงให้สามารถเป็นเครื่องมือสำคัญในการตัดสินใจเชิงกลยุทธ์ (Informed Strategic Decision Making)

อาศัยอำนาจตามความในมาตรา ๒๙ และ ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ๒๕๖๑ ประกอบกับมติที่ประชุมคณะอนุกรรมการด้านการบริหารความเสี่ยงในการประชุม ครั้งที่ ๓/๒๕๖๔ และการประชุมคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล ครั้งที่ ๓/๒๕๖๔ จึงออกประกาศ ดังต่อไปนี้

๑. ให้ยกเลิกประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ๒๙/๒๕๖๓ เรื่องนโยบายบริหารความเสี่ยง สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ลงวันที่ ๖ พฤศจิกายน พ.ศ. ๒๕๖๓

๒. กำหนดให้มีการดำเนินงานบริหารความเสี่ยงของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ดังนี้

๒.๑ สำนักงานจะดำเนินการจัดวางระบบและกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กรให้สอดรับกับกลยุทธ์และวัตถุประสงค์ของสำนักงาน และนโยบายการยอมรับความเสี่ยงระดับองค์กรที่แนบท้ายฉบับนี้ โดยการประเมินความเสี่ยงครอบคลุมความเสี่ยง ๕ ด้าน ได้แก่ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านการเงิน ความเสี่ยงด้านกฎหมาย กฎระเบียบ และความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๒ ให้ทุกส่วนงานมีการบริหารจัดการความเสี่ยงและควบคุมภายในตามกระบวนการและขั้นตอนการบริหารความเสี่ยง

๒.๓ ให้ทุกส่วนงานที่มีการระบุความเสี่ยง ประเมินความเสี่ยง หรือแผนลดความเสี่ยงในช่วงที่ผ่านมาให้ดำเนินการลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ หรือดำเนินงานตามแผนงานที่ได้กำหนดไว้แล้ว

๒.๔ ให้เจ้าหน้าที่ทุกระดับในสำนักงาน มีหน้าที่ปฏิบัติตามกระบวนการบริหารความเสี่ยงทั้งในระดับองค์กร ระดับฝ่ายงาน ระดับส่วนงาน และระดับปฏิบัติการ ตามที่สำนักงาน คณะอนุกรรมการด้านการบริหารความเสี่ยง ฝ่ายบริหาร และส่วนบริหารความเสี่ยงกำหนด

๒.๕ ให้มีการทบทวนและปรับปรุงแผนบริหารความเสี่ยงให้สอดคล้องกับการเปลี่ยนแปลงที่สำคัญที่กระทบต่อเป้าหมาย และบรรจุไว้ในวาระการประชุมคณะอนุกรรมการด้านการบริหารความเสี่ยงทุกครั้ง

๒.๖ ให้มีการใช้ระบบสารสนเทศในการบริหารจัดการความเสี่ยงเพื่อใช้ในการบริหาร ติดตาม และสื่อสารให้กับเจ้าหน้าที่และผู้มีส่วนได้ส่วนเสีย

จึงประกาศให้ทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๑๕ ตุลาคม พ.ศ. ๒๕๖๔

(นายสุพจน์ เธียรวุฒิ)
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

นโยบายการยอมรับความเสี่ยงระดับองค์กร
ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ความเสี่ยงด้าน กฎหมาย กฎระเบียบ (Compliance Risk)	ความเสี่ยงด้าน การปฏิบัติงาน (Operational Risk)	ความเสี่ยงด้านการเงิน (Financial Risk)	ความเสี่ยงด้าน เทคโนโลยีสารสนเทศ (Information Technology Risk)	ความเสี่ยงด้าน นโยบายและกลยุทธ์ (Strategic Risk)
สำนักงานปฏิเสธที่จะยอมรับความเสี่ยงจากการละเมิดกฎหมายหรือกฎระเบียบทุกประเภทที่มีผลบังคับใช้	• สำนักงานปฏิเสธที่จะยอมรับความเสี่ยง - เรื่องการปฏิบัติงานที่เกี่ยวข้องกับการทุจริตทุกกรณี - เรื่องความปลอดภัยที่เกี่ยวข้องกับข้อมูลด้านการเงิน ข้อมูลส่วนบุคคล และความมั่นคงของประเทศ • สำนักงานยอมรับความเสี่ยงได้ระดับต่ำเรื่องการปฏิบัติงานหรือการให้บริการของเจ้าหน้าที่ที่สร้างความเสียหายหรือผลกระทบระดับสูงขึ้นไปต่อสำนักงาน	• สำนักงานยอมรับความเสี่ยงได้ระดับต่ำเรื่องการขาดสภาพคล่องทางเงิน • สำนักงานยอมรับความเสี่ยงได้ระดับปานกลางเรื่องการใช้จ่ายงบประมาณที่ได้รับการจัดสรรน้อยกว่า 80%	• สำนักงานยอมรับความเสี่ยงได้ระดับต่ำเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) • สำนักงานยอมรับความเสี่ยงได้ระดับปานกลางจากการพัฒนาระบบงานเพื่อเพิ่มประสิทธิภาพการปฏิบัติงานให้กับสำนักงาน	• สำนักงานยอมรับความเสี่ยงได้ระดับสูงเรื่องการลงทุนพัฒนางานด้านนวัตกรรมเพื่อเป็นการยกระดับคุณภาพการให้บริการภาครัฐด้วยเทคโนโลยีดิจิทัล และการเพิ่มขีดความสามารถในการแข่งขัน โดยประชาชนมีส่วนร่วมและสามารถเข้าถึงบริการได้อย่างทั่วถึง สะดวก รวดเร็ว ทุกที่ ทุกเวลา และสามารถนำนวัตกรรมนั้นไปใช้ประโยชน์ได้อย่างน้อย 1 ชิ้นงาน/ปี • สำนักงานยอมรับความเสี่ยงได้ระดับต่ำ เรื่องการบรรลุเป้าหมายผลการดำเนินงานของโครงการสำคัญ Flagship Projects ตามแผนกลยุทธ์/แผนยุทธศาสตร์

คู่มือบริหารความเสี่ยงองค์กร

(Enterprise Risk Management Manual)

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สารบัญ

1. บทสรุปผู้บริหาร

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ตระหนักถึงความสำคัญของการบริหารความเสี่ยง จึงได้จัดทำนโยบายบริหารความเสี่ยง (Enterprise Risk Management Policy) ขึ้น เพื่อให้เป็นกรอบแนวทางการพัฒนาระบบการบริหารความเสี่ยงให้มีคุณภาพและมาตรฐานตามแนวทางการกำกับดูแลของนายกรัฐมนตรี สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) รวมถึงแนวทางปฏิบัติที่ดี โดยคำนึงถึงความสอดคล้องกับวัตถุประสงค์และเป้าหมายการดำเนินงานของสำนักงาน ทั้งนี้ เพื่อให้นโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) มีประสิทธิภาพและประสิทธิผลในการบริหารจัดการความเสี่ยงของสำนักงาน ตลอดจนสร้างความมั่นใจว่า สำนักงานมีการบูรณาการกระบวนการทำงานเกี่ยวกับการกำกับดูแลกิจการ (Corporate Governance) การบริหารความเสี่ยง (Risk Management) และการปฏิบัติตามกฎหมาย ระเบียบ ประกาศ คำสั่ง และมาตรฐานที่ดี (Compliance) เพื่อให้บรรลุถึงผลการดำเนินงานที่เกิดจากการมีส่วนร่วมของหน่วยงานและบุคลากรทุกระดับในสำนักงาน

2. หลักการและวัตถุประสงค์

การเปลี่ยนแปลงสภาพแวดล้อมในการดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ทั้งปัจจัยภายใน อาทิ การปรับเปลี่ยนภารกิจ กลยุทธ์ โครงสร้างองค์กร การเปลี่ยนแปลงทรัพยากรภายในสำนักงาน รวมถึงปัจจัยภายนอก อาทิ นโยบายรัฐบาล เหตุการณ์ความไม่สงบทางการเมือง ภัยธรรมชาติ เป็นต้น อาจส่งผลกระทบให้การดำเนินงานของสำนักงาน ไม่เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์ ซึ่งจะก่อให้เกิดความเสี่ยงต่อสำนักงาน โดยรวม

การบริหารความเสี่ยงเป็นองค์ประกอบของการกำกับดูแลกิจการที่ดี ซึ่งนอกจากจะสนับสนุนให้องค์กรสามารถดำเนินงานได้บรรลุตามเป้าหมายที่กำหนดแล้ว ยังสามารถสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้ส่วนเสียขององค์กร (Stakeholders) ได้อีกทางหนึ่ง สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จึงได้นำกรอบการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ (Enterprise Risk Management – Integrated Framework) ตามแนวทาง COSO ERM มาประยุกต์ใช้เป็นกรอบและแนวทางในการพัฒนาระบบการบริหารความเสี่ยงของสำนักงาน ซึ่งมีวัตถุประสงค์ให้ผู้บริหาร เจ้าหน้าที่และลูกจ้างในองค์กรได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง และมีความเข้าใจตรงกันในคำนิยาม เป้าหมายและวัตถุประสงค์ อันจะเป็นการสร้างความรับผิดชอบอย่างทั่วถึงและเป็นไปในทิศทางเดียวกันทั่วทั้งสำนักงาน ได้อย่างมีประสิทธิภาพ

นโยบายบริหารความเสี่ยง (Risk Management Policy) จัดทำขึ้นเพื่อวัตถุประสงค์ ดังต่อไปนี้

1) เพื่อใช้เป็นแนวทางให้ผู้บริหาร เจ้าหน้าที่ และลูกจ้างทั่วทั้งองค์กร เป็นส่วนหนึ่งของการพัฒนากระบวนการบริหารความเสี่ยง เพื่อสนับสนุนการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงานและแผนกลยุทธ์

2) เพื่อให้สำนักงานมีกรอบการดำเนินงาน ซึ่งตอบสนองต่อเหตุการณ์ที่อาจส่งผลให้เกิดความเสี่ยงทุกด้านได้อย่างเป็นระบบและมีมาตรฐาน รวมทั้งมีการดำเนินการเพื่อสร้างพื้นฐานในการป้องกันความเสี่ยงระยะยาวที่สำคัญให้สำนักงาน

3) เพื่อเป็นกลไกในการพัฒนาองค์ความรู้ด้านการบริหารความเสี่ยงสำหรับผู้บริหาร เจ้าหน้าที่และลูกจ้างทั่วทั้งสำนักงาน และสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน

4) เพื่อให้ผู้บริหาร เจ้าหน้าที่ และลูกจ้าง ตระหนักและมีความเข้าใจตรงกันถึงเป้าหมายวัตถุประสงค์ รวมทั้งแนวทางการบริหารความเสี่ยงของสำนักงาน เพื่อร่วมกันสร้างความพึงพอใจให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholders) และสร้างมูลค่าเพิ่มให้องค์กร โดยพิจารณาถึงผลกระทบต่อเป้าหมายการ

ดำเนินงานให้เป็นไปตามหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance) และข้อกำหนดของหน่วยงานที่กำกับดูแลสำนักงาน

ตามคู่มือการบริหารและกำกับดูแลของคณะกรรมการองค์การมหาชน กำหนดให้องค์การมหาชนควรดำเนินการวิเคราะห์และประเมินความเสี่ยงขององค์กรให้ครอบคลุมอย่างน้อย 4 ด้าน ได้แก่ ด้านนโยบายและกลยุทธ์ ด้านการเงินและงบประมาณ ด้านการปฏิบัติงาน และด้านกฎหมาย กฎระเบียบ และสามารถเพิ่มนโยบายการบริหารความเสี่ยงด้านอื่น ๆ ได้ เพื่อให้ครอบคลุมการดำเนินงานของสำนักงาน

ดังนั้น สำนักงานจึงแบ่งประเภทความเสี่ยงออกเป็น 5 ด้าน ดังนี้

1) ด้านนโยบายและกลยุทธ์ หมายถึง ความเสี่ยงที่เกิดจากการกำหนดนโยบายต่าง ๆ เช่น นโยบายระดับรัฐ จนถึงนโยบายในระดับผู้บริหาร แผนกลยุทธ์ แผนดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสมหรือไม่สอดคล้องกับสภาพแวดล้อมภายใน และปัจจัยภายนอก เป็นต้น ทำให้มีโอกาสที่จะไม่ประสบความสำเร็จตามทิศทางที่กำหนดไว้ ซึ่งจะส่งผลกระทบต่อตัวชี้วัดผลการปฏิบัติงานของสำนักงาน

2) ด้านการปฏิบัติงาน หมายถึง ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากบุคลากร ระบบงาน และระบบสารสนเทศ รวมถึงการขาดระบบการควบคุมที่เกี่ยวข้องกับกระบวนการปฏิบัติงานทั้งหมด

3) ด้านการเงิน หมายถึง ความเสี่ยงทางการเงินในภาพรวม ทั้งในด้านการบริหารจัดการ ด้านการเงิน การวางแผนทางการเงิน ซึ่งต้องเป็นไปในทิศทางเดียวกับกลยุทธ์ของสำนักงาน และกฎหมาย กฎระเบียบต่าง ๆ ที่เกี่ยวข้อง

4) ด้านกฎหมาย กฎระเบียบ หมายถึง ความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับกฎหมาย ระเบียบ ประกาศ คำสั่ง มติคณะรัฐมนตรี หรือมาตรฐานที่ดี ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงกฎระเบียบ เป็นต้น

5) ด้านเทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่ครอบคลุมการบริหารจัดการ และประสิทธิภาพการดำเนินงานด้านเทคโนโลยีสารสนเทศ ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัย (Security) เช่น การเข้าถึงระบบงานและข้อมูลเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูล (Integrity) และความพร้อมใช้งานของระบบงานและข้อมูล (Availability)

3. แนวทางการกำหนดกลยุทธ์การบริหารความเสี่ยง

สำนักงานต้องกำหนดกลยุทธ์ในการบริหารความเสี่ยงโดยคำนึงถึงสาระสำคัญ ดังนี้

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

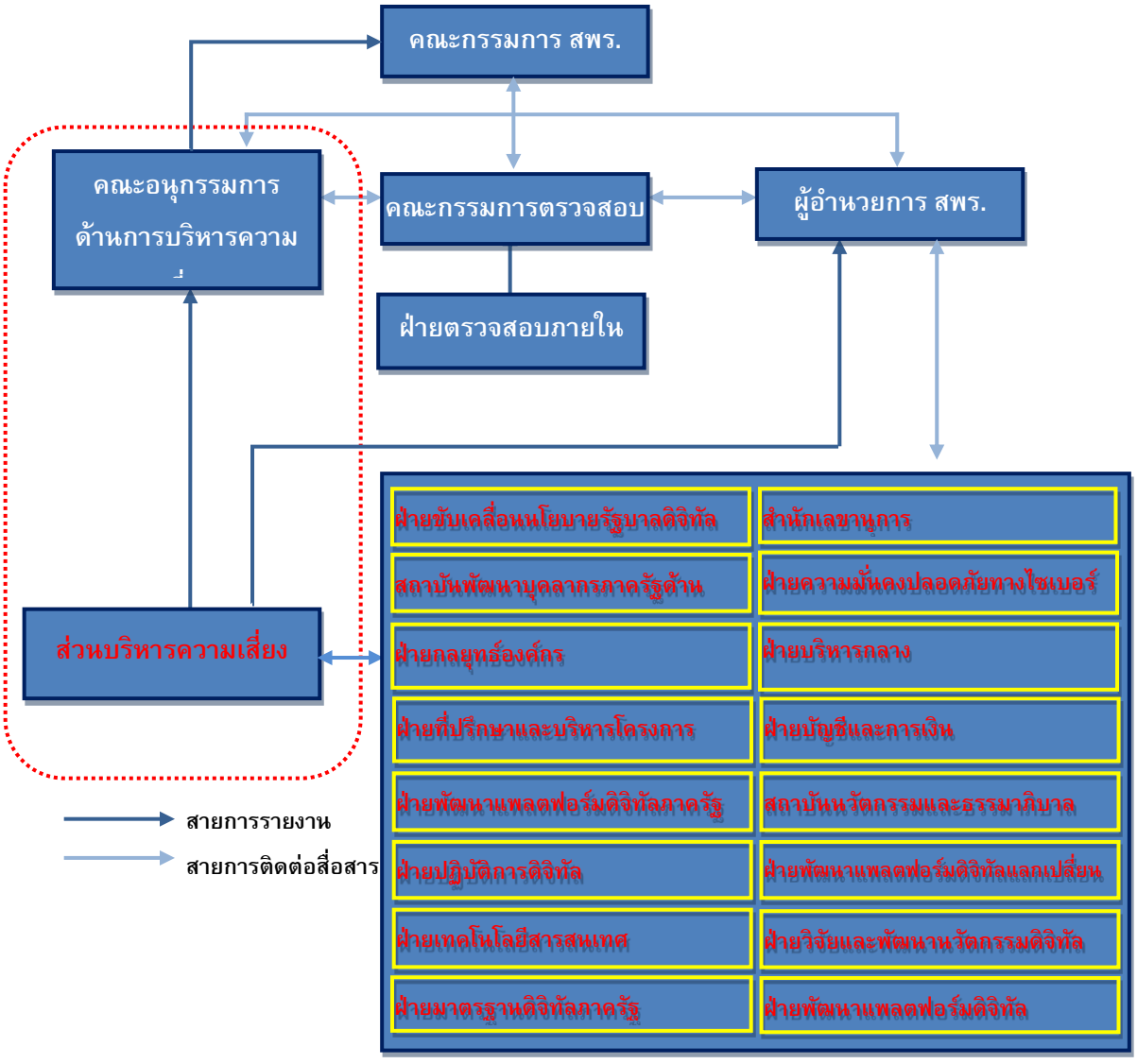
2) ความสอดคล้องกับแนวทางมาตรฐานของหน่วยงานกำกับดูแล ข้อกำหนดของกฎหมาย ระเบียบ ประกาศ หลักเกณฑ์ และแนวทางปฏิบัติที่ดี

3) สำนักงานจะต้องทบทวนกลยุทธ์การบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้งตามแผนปฏิบัติงานประจำปี หรือทบทวนทันทีที่มีเหตุการณ์เปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้ทราบถึงปัญหา อุปสรรค ที่ส่งผลต่อการบรรลุเป้าหมายการบริหารความเสี่ยง และเพื่อสร้างความมั่นใจในการบรรลุเป้าหมายโดยรวมของสำนักงาน

4. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงและบทบาทหน้าที่รับผิดชอบการบริหารความเสี่ยง

สำนักงานต้องจัดให้มีโครงสร้างหน้าที่ของคณะอนุกรรมการและหน่วยงาน เพื่อกำกับดูแลและรับผิดชอบด้านการบริหารความเสี่ยง โดยโครงสร้างหน้าที่ต้องมีความชัดเจน สอดคล้องกับการบริหารความเสี่ยงของสำนักงาน และเหมาะสมกับการดำเนินงานของสำนักงาน รวมถึงมีความเป็นอิสระและมีการถ่วงดุลอำนาจอย่างเหมาะสม ดังนี้



5. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการที่เกี่ยวข้องกับการบริหารความเสี่ยง

คณะกรรมการ	บทบาท หน้าที่ และความรับผิดชอบ
คณะกรรมการ สำนักงานพัฒนารัฐบาลดิจิทัล	1) อนุมัตินโยบาย แผนงานการบริหารความเสี่ยงและกลยุทธ์การบริหารความเสี่ยงเพื่อประกาศใช้ 2) กำกับดูแลให้มีการดำเนินงานที่เป็นไปตามหลักเกณฑ์ของทางการ และเป็นไปตามหลักการกำกับดูแลกิจการที่ดี มีความโปร่งใส เป็นธรรมต่อทุกหน่วยงานที่เกี่ยวข้อง
คณะอนุกรรมการ ด้านการบริหารความเสี่ยง	1) เสนอแนะนโยบายการบริหารความเสี่ยงและกรอบของการบริหารความเสี่ยงต่อคณะกรรมการ 2) ให้คำปรึกษาและเสนอแนะการจัดทำแผนบริหารความเสี่ยงเพื่อให้บรรลุเป้าหมายตามแผนปฏิบัติงานของสำนักงาน เพื่อเสนอต่อคณะกรรมการ 3) เสนอแนะแนวทางในการบริหารจัดการ การดำเนินงาน และการขับเคลื่อนงานบริหารความเสี่ยงของสำนักงาน เพื่อลดผลกระทบและความเสี่ยงที่อาจจะเกิดขึ้นกับสำนักงาน 4) พิจารณาผลการประเมินและติดตามความมีประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงเพื่อรายงานผลต่อคณะกรรมการ 5) พิจารณารายงานผลการประเมินการควบคุมภายในของสำนักงานก่อนเสนอคณะกรรมการ 6) ในกรณีการพิจารณากลั่นกรอง ให้คำปรึกษา ประเมิน หรือวิเคราะห์ในเรื่องใดที่จำเป็นต้องมีผู้เชี่ยวชาญเฉพาะด้านในสาขาที่เกี่ยวข้องเข้าร่วมพิจารณาในรายละเอียด ให้คณะอนุกรรมการเชิญบุคคลดังกล่าวเข้าร่วมพิจารณากับคณะอนุกรรมการเป็นคราวๆ ไป โดยให้บุคคลดังกล่าวได้รับค่าตอบแทนตามระเบียบสำนักงาน 7) ปฏิบัติงานอื่นใดตามที่คณะกรรมการมอบหมาย

คณะกรรมการ	บทบาท หน้าที่ และความรับผิดชอบ
คณะกรรมการตรวจสอบ	1) สอบทาน ให้คำปรึกษา และติดตาม ระบบควบคุมภายใน ระบบการตรวจสอบภายในรายงานผลการตรจสอบภายใน และรายงานผลการดำเนินงานทางด้านการเงิน และด้านการบริหารงาน 2) สอบทานการบริหารความเสี่ยงจากรายงานผลการตรวจสอบที่เกี่ยวข้องกับระบบการบริหารความเสี่ยงซึ่งอยู่ในแผนการตรวจสอบประจำปี

บทบาท หน้าที่และความรับผิดชอบของผู้บริหาร หน่วยงาน และเจ้าหน้าที่ที่เกี่ยวข้องกับการบริหารความเสี่ยง

หน่วยงาน/ผู้บริหาร/ คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
ผู้อำนวยการ เจ้าหน้าที่ และลูกจ้างทุกคนในสำนักงาน	1) มีหน้าที่รับผิดชอบการวิเคราะห์ระบุและประเมินความเสี่ยง กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือแผนบริหารความเสี่ยงของหน่วยงาน/โครงการ หรืองานที่อยู่ในความรับผิดชอบ 2) ติดตามและรายงานความเสี่ยงให้ผู้บังคับบัญชาทราบตามลำดับชั้น ตลอดจนคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอเพื่อให้การบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ
ผู้บริหาร	ผู้บริหารตั้งแต่ระดับผู้จัดการขึ้นไป มีหน้าที่กำกับ ดูแล หน่วยงาน/โครงการ ให้มีการบริหารและจัดการความเสี่ยง และเป็นเจ้าของความเสี่ยง (Risk Owner)
คณะทำงานการบริหารความเสี่ยงด้าน/เรื่อง ต่าง ๆ	มีหน้าที่ตามที่ได้รับมอบหมายจากคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล หรือคณะอนุกรรมการด้านการบริหารความเสี่ยง
ส่วนบริหารความเสี่ยง	1) จัดทำแผนการบริหารจัดการความเสี่ยง 2) จัดทำแนวทางการบริหารความเสี่ยง และกำหนดนโยบาย หลักเกณฑ์ กรอบ กระบวนการ วิธีการ มาตรการ ตัวชี้วัด ด้านการบริหารความเสี่ยงที่เหมาะสมเป็นระบบและต่อเนื่อง 3) พัฒนา ประยุกต์ใช้เครื่องมือ เพื่อใช้ในการบริหารความเสี่ยงสำหรับสำนักงาน

หน่วยงาน/ผู้บริหาร/ คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
	4) สื่อสาร สนับสนุน ให้คำปรึกษาการบริหารความเสี่ยงในสำนักงาน พร้อมประเมินความเสี่ยงและกำหนดแนวทางในการปรับลดความเสี่ยงของสำนักงาน 5) วัดผล ติดตาม ควบคุม รายงานและให้ข้อเสนอแนะเพิ่มเติมถึงแนวทางในการบริหารและจัดการความเสี่ยงในสำนักงาน 6) สนับสนุนการดำเนินงานของคณะอนุกรรมการด้านการบริหารความเสี่ยง
ฝ่ายตรวจสอบภายใน	1) สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายในและกระบวนการบริหารความเสี่ยงเพื่อให้มั่นใจว่ามีระบบการควบคุมภายในที่เหมาะสมและเพียงพอสำหรับการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ควบคุมได้และเป็นไปตามกระบวนการกำกับดูแลกิจการที่ดี 2) ให้ความเห็นเกี่ยวกับประสิทธิผลของการบริหารจัดการความเสี่ยงด้านการทุจริตและระบบการร้องเรียนของสำนักงาน 3) ติดตามผลการตรวจสอบและการปฏิบัติตามข้อเสนอแนะที่หน่วยรับตรวจต้องดำเนินการเพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพ ประสิทธิผลและประหยัดยิ่งขึ้น
ฝ่าย/ส่วนงาน	1) ควบคุมดูแลการปฏิบัติงานในฝ่าย/ส่วน ให้เป็นไปตามนโยบายและ กลยุทธ์การบริหารความเสี่ยง รวมทั้งจัดให้มีระบบบริหารความเสี่ยงที่มีประสิทธิภาพ 2) สร้างความมั่นใจว่าการปฏิบัติงานรายวันมีการประเมินจัดการและรายงานความเสี่ยงอย่างเพียงพอ 3) ส่งเสริมเจ้าหน้าที่ในฝ่ายและส่วนงานให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง 4) สร้างความมั่นใจว่าแผนการบริหารความเสี่ยงได้รับการปฏิบัติอย่างครบถ้วน

หน่วยงาน/ผู้บริหาร/ คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
Risk – Internal Control Officer (RICO)	1) รับผิดชอบในการประสานงาน การประเมินความเสี่ยง การควบคุมภายใน และการปฏิบัติตามกฎเกณฑ์ รวมทั้งเผยแพร่ความรู้ที่เกี่ยวข้องแก่เจ้าหน้าที่ในหน่วยงานของตนเอง 2) ให้คำปรึกษา พร้อมทั้งประสานงานให้หน่วยงานตนเอง ดำเนินการตามกระบวนการบริหารความเสี่ยงโดยมีการระบุ ประเมิน และจัดการความเสี่ยงด้านต่าง ๆ ที่อาจเกิดขึ้น เพื่อป้องกันหรือลดระดับความเสี่ยง 3) ช่วยเหลือและสนับสนุนการจัดประชุมเชิงปฏิบัติการเพื่อจัดทำแผนจัดการความเสี่ยงทุกระดับ 4) บันทึก ติดตาม และรายงานความก้าวหน้าของแผนจัดการความเสี่ยงระดับฝ่ายและส่วนงาน 5) ประสานงานกับส่วนบริหารความเสี่ยง

6. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

ความหมายของความเสี่ยง

การดำเนินงานในองค์กรโดยทั่วไป มีเป้าหมายเพื่อเพิ่มมูลค่าให้แก่ผู้มีส่วนได้ส่วนเสีย ทำให้ทุกองค์กรต้องเผชิญกับความไม่แน่นอน ที่อาจเกิดขึ้นจากปัจจัยภายในและภายนอกหลายประการ เช่น การเปลี่ยนแปลงของ กฎระเบียบ และนโยบายของรัฐบาล การบริหารงานด้านความปลอดภัยในชีวิตและทรัพย์สินอันเนื่องมาจากการเปลี่ยนแปลงปัจจัยต่าง ๆ ภัยจากการก่อการร้าย ภัยธรรมชาติ และความเสี่ยงอื่น ๆ เป็นต้น ผู้บริหารจึงต้องพิจารณาว่าควรจัดการกับความไม่แน่นอนที่เกิดขึ้นอย่างไร เพื่อให้องค์กรสามารถรักษาหรือเพิ่มมูลค่าของผู้มีส่วนได้ส่วนเสียได้

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

นิยามการบริหารความเสี่ยง

การบริหารความเสี่ยง คือ การกำหนดนโยบาย โครงสร้าง และกระบวนการ เพื่อให้คณะกรรมการ ผู้บริหาร และบุคลากรขององค์กรนำไปปฏิบัติในการกำหนดกลยุทธ์และปฏิบัติงานทั่วทั้งองค์กร กระบวนการบริหารความเสี่ยงได้รับการออกแบบให้สามารถบ่งชี้เหตุการณ์ที่เกิดขึ้น ประเมินผลกระทบต่อองค์กร และกำหนดวิธีการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อให้เกิดความเชื่อมั่นในระดับหนึ่งว่าการดำเนินการในองค์กรจะบรรลุตามวัตถุประสงค์ที่กำหนดไว้

การบริหารความเสี่ยงที่มีประสิทธิผล มีข้อดีดังต่อไปนี้

- เพิ่มมูลค่าขององค์กรที่มีต่อผู้มีส่วนได้ส่วนเสีย
- ทำให้เกิดความมั่นใจต่อการปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ
- เพิ่มประสิทธิภาพการทำงานของเจ้าหน้าที่
- ป้องกันและดูแลทรัพย์สินต่าง ๆ
- ทำให้การดำเนินงานเป็นไปอย่างยั่งยืน
- เพิ่มความน่าเชื่อถือของการเปิดเผยข้อมูลต่อบุคคลภายนอก

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
Degree Of Acceptance	ระดับของการยอมรับความเสี่ยง
Risk Matrix	แผนภูมิ 2 มิติ ขนาด 5*5 ประกอบด้วยแกนด้านผลกระทบ และแกนด้านโอกาสที่จะเกิด แต่ละแกนแบ่งระดับความรุนแรงเป็น 5 ระดับ มีวัตถุประสงค์เพื่อเป็นการแสดงระดับความเสี่ยง
Risk Profile	กลุ่ม (Set) ของความเสี่ยง ที่แสดงให้เห็นถึงความเสี่ยงต่าง ๆ ที่อาจส่งผลกระทบต่อเป้าหมายของหน่วยงานต่าง ๆ โดยจะมีข้อมูลที่บ่งบอกลักษณะของความเสี่ยง ประเภทของความเสี่ยง ผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงนั้น ตลอดจนข้อมูลต่าง ๆ ที่เกี่ยวข้องกับความเสี่ยงนั้น สามารถแสดงด้วย Risk Map

ศัพท์เฉพาะ	คำนิยาม
Risk Appetite	ระดับความเสี่ยงโดยรวมที่องค์กรยอมรับได้เพื่อมุ่งไปสู่พันธกิจหรือวิสัยทัศน์ขององค์กร
Risk Tolerance	ระดับความเบี่ยงเบนที่องค์กรยอมรับได้จากเกณฑ์หรือดัชนีวัดผลการดำเนินงานที่เกี่ยวข้องกับการบรรลุวัตถุประสงค์
KRIs (Key Risk Indicators)	ตัวชี้วัดความเสี่ยงเชิงปริมาณ กิจกรรม หรือเหตุการณ์ ที่บ่งบอกถึงการเปลี่ยนแปลงของความเสี่ยงสำคัญที่ส่งผลกระทบต่อเป้าหมายได้ โดยสามารถใช้ประโยชน์ในการบริหารความเสี่ยง เพื่อติดตามผลการบริหารความเสี่ยงว่าเป็นไปตามเป้าหมายหรือไม่ เพื่อจะได้ปรับปรุง/เปลี่ยนแปลงแผนการบริหารความเสี่ยงให้มีประสิทธิภาพมากยิ่งขึ้น และในกรณีตัวชี้วัดมีลักษณะเป็นดัชนีชี้นำ (Leading Indicator) สามารถนำไปใช้ประโยชน์ในการวางแผนการบริหารความเสี่ยงให้มีระบบเตือนล่วงหน้า (Early Warning System) ได้
Value Driver Diagram	แผนภาพแสดงปัจจัยที่ส่งผลกระทบต่อเป้าหมายทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ซึ่งเป็นเครื่องมือที่สำคัญในขั้นตอนการระบุปัจจัยเสี่ยง ใช้หลักการเดียวกับ Cause-and–Effect Analysis
Risk Factor	ปัจจัยเสี่ยง หมายถึง สิ่งที่เกิดขึ้นจากเหตุการณ์ หรือรายละเอียดของเหตุการณ์ที่ทำให้ทราบว่าความเสี่ยงเกิดจากอะไร
Risk Driver	เหตุแห่งความเสี่ยง ซึ่งอาจเป็นเหตุที่เกิดจากปัจจัยภายในองค์กร เช่น วัฒนธรรมองค์กร โครงสร้างองค์กร บุคลากร หรือเหตุที่เกิดจากปัจจัยภายนอก เช่น การเมือง คู่แข่ง สภาวะเศรษฐกิจ เป็นต้น
Cost & Benefit Analysis	การวิเคราะห์ถึงผลประโยชน์เปรียบเทียบกับต้นทุนทั้งที่เป็นตัวเงินและไม่สามารถวัดเป็นตัวเงิน เพื่อใช้ในการตัดสินใจ เลือกใช้วิธีการที่เหมาะสม โดยการตัดสินใจเลือกใช้การจัดการความเสี่ยงวิธีใดนั้นควรคำนึงถึงประโยชน์ทั้งในด้านของการลดผลกระทบหรือโอกาสเกิด โดยเปรียบเทียบกับต้นทุนหรือค่าใช้จ่ายที่เกิดจากการจัดการความเสี่ยงนั้น ๆ แล้วพิจารณาเลือกวิธีการจัดการความเสี่ยงที่ได้รับประโยชน์มากกว่าต้นทุนหรือค่าใช้จ่ายที่ต้องใช้
ความมั่นคงปลอดภัย (Security)	การจัดการป้องกันการเข้าถึง การเข้าไปแก้ไขเปลี่ยนแปลง การทำลาย การเปิดเผยข้อมูล การรักษาความลับ (Confidential) ทั้งในระหว่างที่กำลังพัฒนาระบบงาน หรือในการจัดส่งข้อมูลการประมวลผล หรือการจัดเก็บรักษาข้อมูลในระบบงาน

ศัพท์เฉพาะ	คำนิยาม
	การจัดเก็บระบบงาน โดยจัดการป้องกันให้มีความเหมาะสมและความสำคัญของข้อมูลรวมถึงระบบงานด้วย
ความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)	ข้อมูลที่จะส่งมอบให้กับผู้ใช้ข้อมูล (End User) เป็นข้อมูลที่มีความสมบูรณ์ถูกต้อง ครบถ้วน ซึ่งจะทำให้การดำเนินงานและการบริหารงานขององค์กรมีประสิทธิภาพ
ความพร้อมใช้งานของระบบงานและข้อมูล (Availability)	การจัดส่งข้อมูลไปให้ผู้ที่ต้องการใช้ข้อมูลได้รวดเร็วทันเวลา และสามารถให้ข้อมูลได้อย่างต่อเนื่องในเวลาที่เหมาะสม เพื่อสนับสนุนการดำเนินงานขององค์กร ทั้งนี้องค์กรต้องมีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ซึ่งเป็นแผนการดำเนินงานหลักขององค์กร และมีแผนงานรองประกอบแผนงานหลักได้แก่ แผนการกู้ระบบกลับคืน (Disaster Recovery Plan) แผนสำรองฉุกเฉิน (Contingency Plan) และแผนรองรับเหตุการณ์ไม่คาดว่าจะเกิดขึ้น (Incident Response Plan)

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

- ผสมผสานและเป็นส่วนหนึ่งของธุรกิจ โดยการบริหารความเสี่ยงควรสอดคล้องกับแผนธุรกิจ วัตถุประสงค์ การตัดสินใจ และสามารถนำไปใช้กับองค์ประกอบอื่น ๆ ในการบริหารองค์กร
- พิจารณาความเสี่ยงทั้งหมด โดยครอบคลุมความเสี่ยงระดับองค์กร (Corporate Risk) และระดับกิจกรรม (Functional Risk) ได้แก่ ความเสี่ยงด้านนโยบายและกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านการเงิน ความเสี่ยงด้านกฎหมาย กฎระเบียบ และความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งความเสี่ยงเหล่านี้อาจทำให้เกิดความเสียหาย ความไม่แน่นอน และโอกาส รวมถึงการมีผลกระทบต่อวัตถุประสงค์ และความต้องการของผู้มีส่วนได้ส่วนเสีย
- ระบุความเสี่ยงโดยการคาดการณ์ในอนาคต โดยองค์กรต้องสามารถระบุว่าความเสี่ยงอะไรที่อาจเกิดขึ้นบ้าง และเมื่อเกิดขึ้นจริงจะมีผลกระทบต่อวัตถุประสงค์อย่างไร เพื่อให้องค์กรได้จัดเตรียมการบริหารความเสี่ยง

- การจัดทำตัวชี้วัดความเสี่ยง (Key Risk Indicators : KRIs) และระบบติดตามและรายงานความเสี่ยง (Risk Dashboard) ที่มีความสัมพันธ์กับการเกิดขึ้นของปัจจัยเสี่ยงอย่างมีนัยสำคัญ โดยสามารถวัดค่าและบ่งชี้ความเสี่ยงที่อาจเกิดความเสียหายขึ้น ซึ่งจะเป็นสัญญาณเตือนภัยช่วยให้ทุกคนในองค์กรตระหนักถึงความสำคัญและเห็นชอบที่จะบริหารจัดการความเสี่ยงร่วมกันจนเกิดเป็นวัฒนธรรม
- การกำหนดความรับผิดชอบที่เหมาะสมกับการบริหารความเสี่ยงภาพรวมขององค์กรตามแนวปฏิบัติ Three Lines of Defense ประกอบด้วย 3 ระดับ คือ ระดับ 1 หน่วยงานที่เป็นผู้เผชิญกับความเสี่ยงโดยตรง ระดับ 2 หน่วยงานบริหารความเสี่ยงและกำกับการปฏิบัติงาน มีบทบาทในการช่วยเหลือหน่วยงานระดับ 1 ในการบริหารจัดการความเสี่ยงที่เผชิญ และระดับ 3 คือ หน่วยงานตรวจสอบภายใน ทำหน้าที่ในการประเมินความเพียงพอของมาตรการต่าง ๆ โดยอยู่ภายใต้การดูแลของผู้ตรวจสอบภายนอกและทางการ
- ได้รับการสนับสนุนและมีส่วนร่วม จากทุกคนในองค์กรตั้งแต่ระดับคณะกรรมการ ผู้บริหารทุกระดับและเจ้าหน้าที่ทุกคน

7. องค์ประกอบการบริหารความเสี่ยง

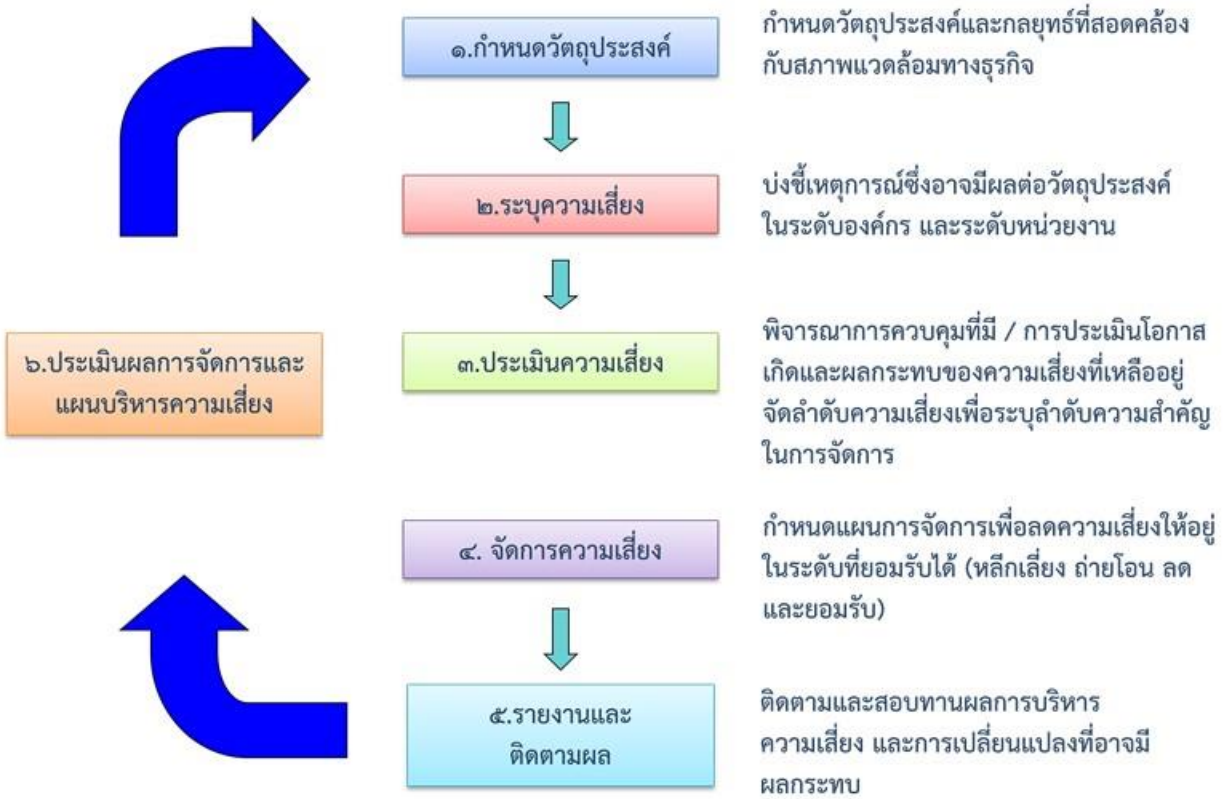
การบริหารความเสี่ยง เป็นกระบวนการที่ต้องดำเนินการอย่างต่อเนื่องภายในองค์กร และควรผนวกกับกิจกรรมปกติทางธุรกิจ เพื่อให้องค์กรสามารถดำเนินการตามกลยุทธ์ที่กำหนด ส่งผลให้องค์กรบรรลุตามพันธกิจและวัตถุประสงค์ที่ต้องการ

กระบวนการ 8 ขั้นตอนหลักประกอบด้วย

1. สภาพแวดล้อมภายในองค์กร แนวนโยบายโดยทั่วไปของสำนักงาน ซึ่งเป็นพื้นฐานที่สำคัญของกรอบการบริหารความเสี่ยง และการจัดการกับความเสี่ยง
2. การกำหนดวัตถุประสงค์และเป้าหมาย ที่สอดคล้องกับกลยุทธ์สำนักงาน
3. การระบุเหตุการณ์ การบ่งชี้และเข้าใจความเสี่ยงทั้งหมดที่มีผลกระทบต่อวัตถุประสงค์ที่กำหนดไว้

4. การประเมินความเสี่ยง โดยพิจารณาถึงผลกระทบและโอกาสเกิดความเสี่ยง
5. การตอบสนองความเสี่ยง กำหนดการจัดการความเสี่ยงที่ปฏิบัติอยู่ในปัจจุบัน
6. กิจกรรมการควบคุม โดยพิจารณาถึงการควบคุมเพิ่มเติมรวมทั้งความสัมพันธ์ของต้นทุนและผลประโยชน์ที่เกิดขึ้น ผู้บริหารควรนำวิธีการจัดการความเสี่ยงไปปฏิบัติและติดตาม เพื่อให้มั่นใจได้ว่า มีการดำเนินการตามวิธีการที่กำหนดไว้ กิจกรรมการควบคุม คือนโยบายและขั้นตอนปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง
7. สารสนเทศและการสื่อการ การสื่อสารเพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่ มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง
8. การติดตามผลและรายงานความมีประสิทธิผลของกระบวนการและระบบการบริหารความเสี่ยง

ทั้งนี้ การนำกระบวนการของการบริหารความเสี่ยง 8 ขั้นตอน ไปปฏิบัติ มีรายละเอียดดังนี้



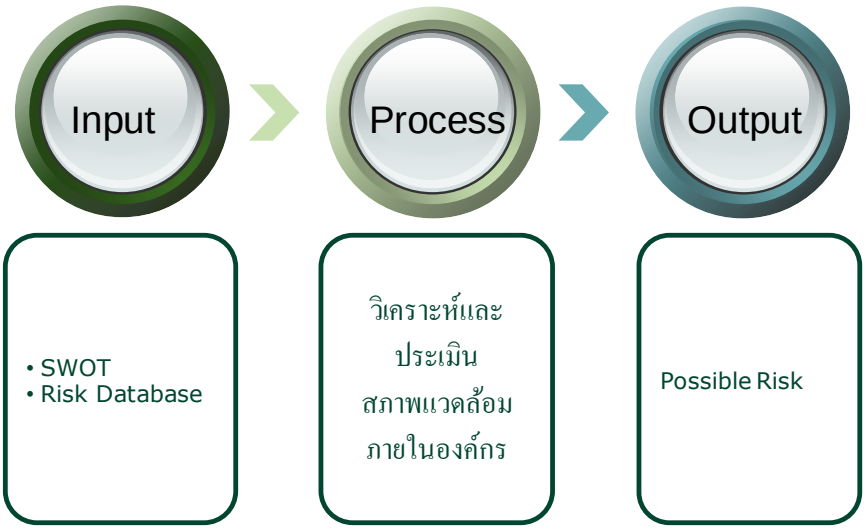
7.1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมภายในองค์กรครอบคลุมถึงแนวนโยบายโดยทั่วไปของสำนักงาน ซึ่งเป็นพื้นฐานที่สำคัญของกรอบการบริหารความเสี่ยง และการจัดการความเสี่ยงโดยผู้บริหาร เจ้าหน้าที่และลูกจ้างทั้งหมดในสำนักงาน ซึ่งมีอิทธิพลต่อความตระหนักถึงความเสี่ยงของบุคลากร และช่วยก่อให้เกิดแนวทางการบริหารความเสี่ยงของสำนักงาน

สภาพแวดล้อมภายในองค์กร เป็นพื้นฐานสำคัญขององค์ประกอบการบริหารความเสี่ยง และช่วยก่อให้เกิดแนวทางปฏิบัติและโครงสร้างของการบริหารความเสี่ยงขององค์กร โดยการวิเคราะห์สภาพแวดล้อมภายในองค์กร จะมีผลต่อการประเมินและการดำเนินการในการกำหนดกลยุทธ์และวัตถุประสงค์ขององค์กร การกำหนดกิจกรรมทางธุรกิจ และการระบุความเสี่ยง

การวิเคราะห์และประเมินสภาพแวดล้อมภายในองค์กร ควรครอบคลุมถึงแนวนโยบายทั่วไปขององค์กร ซึ่งเป็นพื้นฐานของการพิจารณาความเสี่ยงและการจัดการความเสี่ยงโดยบุคลากรทั้งหมดในองค์กร องค์ประกอบสำคัญที่มีผลต่อสภาพแวดล้อมในองค์กร ได้แก่ ค่านิยมและความเชื่อ ศักยภาพและการพัฒนาของบุคลากร รูปแบบการบริหารจัดการของฝ่ายบริหาร วิธีการมอบอำนาจหน้าที่ความรับผิดชอบ ลักษณะโครงสร้างขององค์กร ตลอดจนพฤติกรรมที่คนในองค์กรยึดถือเพื่อเป็นแนวทางในการปฏิบัติงาน

สามารถแสดงองค์ประกอบที่เกี่ยวข้องในการวิเคราะห์และประเมินสภาพแวดล้อมภายในองค์กร ได้ดังนี้



จากแผนภาพดังกล่าว เพื่อให้การวิเคราะห์สภาพแวดล้อมภายในองค์กร สะท้อนการดำเนินธุรกิจได้ชัดเจนขึ้น ควรพิจารณาให้ครอบคลุมถึงปัจจัยภายในและภายนอกที่อาจมีผลกระทบต่อองค์กร ตลอดจนวิเคราะห์จากฐานข้อมูลความเสี่ยงองค์กร (Risk Database) ดังนี้

- ปัจจัยภายใน เช่น โครงสร้างองค์กร กระบวนการและวิธีปฏิบัติงาน วัฒนธรรมองค์กร ความสามารถในการแข่งขัน ปรัชญาการบริหารความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้ของผู้บริหาร

- ปัจจัยภายนอก เช่น ภาวะเศรษฐกิจ การเมืองทั้งในประเทศและต่างประเทศ การแข่งขันทางธุรกิจ ลักษณะของตลาดและความสามารถของคู่เปรียบเทียบ ความก้าวหน้าทางเทคโนโลยี กฎเกณฑ์การกำกับดูแลของหน่วยงานที่เกี่ยวข้อง

7.2 การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

สำนักงานต้องกำหนดให้หน่วยงานทุกระดับมีการกำหนดวัตถุประสงค์และเป้าหมายการดำเนินงานที่สอดคล้องกับวิสัยทัศน์ พันธกิจ กลยุทธ์ และเป้าหมายโดยรวมของสำนักงาน โดยต้องมีความชัดเจน สามารถวัดหรือประเมินผลได้

ในการกำหนดวัตถุประสงค์ ควรกำหนดให้ครอบคลุมแต่ละประเภทของวัตถุประสงค์ ดังต่อไปนี้

- วัตถุประสงค์ด้านนโยบายและกลยุทธ์ คือ วัตถุประสงค์ระดับนโยบายขององค์กร โดยสอดคล้องกับวิสัยทัศน์และพันธกิจขององค์กรโดยรวม ซึ่งมุ่งสู่การบรรลุเป้าหมายขององค์กรในภาพรวม

- วัตถุประสงค์ด้านการปฏิบัติงาน คือ วัตถุประสงค์ที่เกี่ยวข้องกับประสิทธิภาพและประสิทธิผลของการปฏิบัติการ

- วัตถุประสงค์ด้านการเงิน คือ วัตถุประสงค์ที่เกี่ยวข้องกับการบริหารการเงินขององค์กรในทุกด้าน ได้แก่ ประสิทธิภาพในการเบิกจ่ายงบลงทุน ประสิทธิภาพในการบริหารค่าใช้จ่าย ความน่าเชื่อถือและความทันเวลาของการรายงานข้อมูลทางการเงินและข้อมูลที่ไม่ใช่ทางการเงิน ทั้งจากภายในและภายนอกองค์กร

- วัตถุประสงค์ด้านกฎหมาย กฎระเบียบ คือ วัตถุประสงค์ที่เกี่ยวข้องกับการปฏิบัติตามกฎหมายและกฎระเบียบต่าง ๆ การปฏิบัติตามกฎระเบียบที่เกี่ยวข้อง

- วัตถุประสงค์ด้านเทคโนโลยีสารสนเทศ คือ วัตถุประสงค์ที่เกี่ยวข้องกับการดำเนินการในด้านเทคโนโลยีสารสนเทศใด ๆ เพื่อให้มี ความมั่นคงปลอดภัยของข้อมูล (Security) ความถูกต้องเชื่อถือได้ของข้อมูล (Integrity) และความพร้อมใช้งานของระบบงานและข้อมูล (Availability)

<u>ความสอดคล้องของวัตถุประสงค์</u>

วัตถุประสงค์ต้องมีความสอดคล้องทั่วทั้งองค์กร เพื่อให้เกิดความมั่นใจว่า หน่วยงาน ผู้บริหาร และเจ้าหน้าที่ ดำเนินการเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

วิสัยทัศน์เป็นจุดเริ่มต้นในการกำหนดทิศทางขององค์กร ผู้บริหารระดับสูงจะทำการกำหนดวัตถุประสงค์ระดับองค์กรขึ้นในการจัดทำแผนประจำปี แต่ละหน่วยงานดำเนินการกำหนดวัตถุประสงค์ของหน่วยงานให้สอดคล้องกับวัตถุประสงค์ที่องค์กรได้กำหนดไว้ และการกำหนดวัตถุประสงค์ของกระบวนการและโครงการต่าง ๆ ต้องคำนึงถึงความสอดคล้องกับวัตถุประสงค์ของหน่วยงานและระดับองค์กร

วัตถุประสงค์อาจเกี่ยวข้องกับองค์กรในหลาย ๆ ด้าน รวมไปถึง ทรัพยากร เทคโนโลยีสารสนเทศ ผลการดำเนินการด้านปฏิบัติการ เป็นต้น

7.3 การระบุเหตุการณ์ (Event Identification)

คือ การระบุเหตุการณ์ความเสี่ยงหรือความไม่แน่นอนที่อาจเกิดขึ้น โดยพิจารณาจากปัจจัยทั้งภายในและภายนอกองค์กร ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร

ประเภทความเสี่ยง ความเสี่ยงแบ่งออกเป็น 5 ด้าน ดังนี้

1. **ความเสี่ยงด้านนโยบายและกลยุทธ์ (Strategic Risk)** เป็นความเสี่ยงที่เกิดจากการกำหนดกลยุทธ์ หรือนโยบายการบริหารงาน ทำให้องค์กรไม่สามารถบรรลุกลยุทธ์และเพิ่มมูลค่าให้องค์กรได้ เช่น การเปลี่ยนแปลงโครงสร้างองค์กร ขาดการกำหนด Job Description การวิเคราะห์อัตรากำลังและขาดอัตรากำลัง ผลงานนวัตกรรมไม่สามารถนำมาใช้ประโยชน์ได้ ขาดการนำระบบงานมาใช้บริหารจัดการติดตามและรายงานผล การเปลี่ยนแปลงปัจจัยภายนอกด้านเศรษฐกิจ สภาพการแข่งขัน การเปลี่ยนแปลงของหน่วยงานราชการ เทคโนโลยี และกฎหมายต่าง ๆ เป็นต้น

2. **ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)** เป็นความเสี่ยงที่เกิดจากการปฏิบัติงานปกติในทุก ๆ ขั้นตอน โดยเกี่ยวข้องกับกระบวนการในการปฏิบัติงาน อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากร ซึ่งส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินธุรกิจขององค์กร เช่น การทำธุรกรรมโดย

ไม่ได้รับอนุญาต การทุจริตและฉ้อโกง การคัดเลือกหรือให้การสนับสนุนคู่ค้าที่ไม่เหมาะสมในธุรกิจหลักขององค์กร การบริหารจัดการบุคคลไม่มีประสิทธิภาพ ไม่มีการสร้างความผูกพันต่อองค์กร ความไม่ปลอดภัยในสภาพแวดล้อมการทำงาน ความผิดพลาดจากการปฏิบัติงาน ภัยพิบัติหรือเหตุการณ์อื่น ๆ ความเสียหายของทรัพย์สินสำนักงาน ขาดการติดตามและรายงานผล การบริหารจัดการด้านเอกสารไม่มีประสิทธิภาพและไม่มีการควบคุมธุรกรรมกับคู่ค้า/คู่สัญญา เป็นต้น

3. **ความเสี่ยงด้านการเงิน (Financial Risk)** เป็นความเสี่ยงจากการขาดข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงานเพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้อง เหมาะสม ส่งผลต่อสถานะทางการเงินขององค์กร เช่น การขาดสภาพคล่องทางการเงิน การบริหารจัดการและการใช้งบประมาณให้เป็นไปตามวัตถุประสงค์ เป็นต้น

4. **ความเสี่ยงด้านกฎหมาย กฎระเบียบ (Compliance Risk)** เป็นความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงานได้ กฎระเบียบหรือกฎหมายที่มีอยู่ไม่เหมาะสมเป็นอุปสรรคต่อการปฏิบัติงาน นโยบายและวิธีการปฏิบัติงานที่องค์กรกำหนดขึ้นไม่สามารถปฏิบัติได้ เช่น การไม่ปฏิบัติตามกฎหมายภายนอกที่เกี่ยวข้อง และการไม่ปฏิบัติตามวิธีปฏิบัติ นโยบายหรือหลักเกณฑ์ภายในสำนักงานที่เกี่ยวข้อง รวมถึงผลิตภัณฑ์หรือวิธีปฏิบัติไม่ได้มาตรฐาน เป็นต้น

5. **ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)** เป็นความเสี่ยงที่เกิดจากความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะมีองค์ประกอบที่สำคัญ 3 ประการ ได้แก่ แผนงานการใช้เทคโนโลยีสารสนเทศ การตัดสินใจในการนำเทคโนโลยีสารสนเทศมาใช้ และการวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน ระบบงาน เหตุการณ์ภายนอก หรือคน (เจ้าหน้าที่ บุคคลภายนอก หรือลูกค้า) ซึ่งส่งผลกระทบต่อการดำเนินงาน

ความเสี่ยงของแผนงาน/โครงการ ตามมติคณะรัฐมนตรีวันที่ 22 เมษายน 2551 ได้เห็นชอบในหลักเกณฑ์และแนวทางคัดเลือกแผนงาน/โครงการที่สำคัญตามนโยบายรัฐบาล เพื่อให้มีการวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล เพื่อให้ส่วนงานรัฐวิสาหกิจ และหน่วยงานอื่นของรัฐใช้เป็นมาตรฐานเดียวกันทุกหน่วยงาน

โดยได้กำหนดแนวทางการวิเคราะห์ความเสี่ยงของแผนงาน/โครงการตามหลักธรรมาภิบาล มี 10 ประเภท ได้แก่

1. **ความเสี่ยงต่อหลักประสิทธิผล (Effectiveness)** ต้องมีวิสัยทัศน์เชิงยุทธศาสตร์ เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกฝ่าย ปฏิบัติตามหน้าที่ตามพันธกิจให้บรรลุวัตถุประสงค์ขององค์กร มีการวางเป้าหมายการปฏิบัติงานที่ชัดเจน และอยู่ในระดับที่ตอบสนองต่อความคาดหวังของประชาชน สร้างกระบวนการปฏิบัติงานอย่างเป็นระบบและมีมาตรฐาน มีการจัดการความเสี่ยงและมุ่งเน้นผลการปฏิบัติงานที่เป็นเลิศ รวมถึงมีการติดตามประเมินผล และพัฒนาปรับปรุงการปฏิบัติงานให้ดีขึ้นอย่างต่อเนื่อง
2. **ความเสี่ยงต่อหลักประสิทธิภาพ (Efficiency)** ในการปฏิบัติงานต้องมีการใช้ทรัพยากรอย่างประหยัด เกิดผลิตภาพ คุ้มค่าการลงทุนและบังเกิดประโยชน์สูงสุดต่อส่วนรวม รวมทั้งต้องมีการลดขั้นตอนและระยะเวลาในการปฏิบัติงาน เพื่ออำนวยความสะดวกและลดภาระค่าใช้จ่าย ตลอดจนยกเลิกภารกิจที่ล้าสมัย และไม่มีความจำเป็น
3. **ความเสี่ยงต่อหลักการมีส่วนร่วม (Participation)** ต้องรับฟังความคิดเห็นของประชาชน รวมทั้งเปิดให้ประชาชนมีส่วนร่วมในการรับรู้ เรียนรู้ ทำความเข้าใจ รวมทั้งแสดงทัศนะ ร่วม

เสนอปัญหา/ประเด็นสำคัญที่เกี่ยวข้อง ร่วมคิดแก้ไขปัญหา ร่วมในกระบวนการตัดสินใจและการดำเนินงาน และร่วมตรวจสอบผลการปฏิบัติงาน

4. **ความเสี่ยงต่อหลักความโปร่งใส (Transparency)** ต้องปฏิบัติงานด้วยความซื่อสัตย์สุจริต ตรงไปตรงมา รวมทั้งต้องมีการเปิดเผยข้อมูลข่าวสารที่จำเป็นและเชื่อถือได้ ให้ประชาชนได้รับทราบอย่างสม่ำเสมอ ตลอดจนวางระบบให้การเข้าถึงข้อมูลข่าวสารเป็นไปโดยง่าย
5. **ความเสี่ยงต่อหลักการตอบสนอง (Responsiveness)** ต้องสามารถให้บริการได้อย่างมีคุณภาพ สามารถดำเนินการแล้วเสร็จภายในระยะเวลาที่กำหนด สร้างความเชื่อมั่นไว้วางใจ รวมถึงตอบสนองตามความคาดหวัง/ความต้องการของประชาชนผู้รับบริการ และผู้มีส่วนได้ส่วนเสียที่มีความหลากหลายและมีความแตกต่างกันได้อย่างเหมาะสม
6. **ความเสี่ยงต่อหลักภาระรับผิดชอบ (Acountability)** ในการปฏิบัติงานต้องสามารถตอบคำถาม และชี้แจงได้เมื่อมีข้อสงสัย รวมทั้งต้องมีการจัดวางระบบการรายงานความก้าวหน้าและผลสัมฤทธิ์ตามเป้าหมายที่กำหนดไว้ต่อสาธารณะ เพื่อประโยชน์ในการตรวจสอบและการให้คุณให้โทษ ตลอดจนมีการจัดเตรียมระบบการแก้ไขหรือบรรเทาปัญหา และผลกระทบใด ๆ ที่อาจจะเกิดขึ้น
7. **ความเสี่ยงต่อหลักนิติธรรม (Rule of Law)** ต้องใช้อำนาจของกฎหมาย กฎระเบียบข้อบังคับในการปฏิบัติงานอย่างเคร่งครัด ด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของประชาชน และผู้มีส่วนได้ส่วนเสียฝ่ายต่าง ๆ
8. **ความเสี่ยงต่อหลักการกระจายอำนาจ (Decentralization)** ในการปฏิบัติงานควรมีการมอบอำนาจและกระจายความรับผิดชอบในการตัดสินใจและการดำเนินการให้แก่ผู้ปฏิบัติงานในระดับต่าง ๆ ได้อย่างเหมาะสม รวมทั้งมีการโอนถ่ายบทบาท และภารกิจให้แก่องค์กรปกครองส่วนท้องถิ่น หรือภาคส่วนอื่น ๆ ในสังคม
9. **ความเสี่ยงต่อหลักความเสมอภาค (Equity)** ต้องให้บริการอย่างเท่าเทียมกัน ไม่มีการแบ่งแยกด้าน ชาย/หญิง ถิ่นกำเนิด เชื้อชาติ ภาษา เพศ อายุ สภาพทางกายหรือสุขภาพ สถานะของบุคคล ฐานะทางเศรษฐกิจและสังคม ความเชื่อทางศาสนา การศึกษาอบรม และอื่น ๆ นอกจากนี้ยังต้องคำนึงถึงโอกาสความทัดเทียมกันของการเข้าถึงบริการสาธารณะ ของกลุ่มบุคคลผู้ด้อยโอกาสในสังคม
10. **ความเสี่ยงต่อหลักการมุ่งเน้นฉันทามติ (Consensus Oriented)** ในการปฏิบัติงานต้องมีกระบวนการในการแสวงหาฉันทามติ หรือข้อตกลงร่วมกัน ระหว่างกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องโดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง จะต้องไม่มีข้อคัดค้าน ที่หาข้อยุติไม่ได้ ในประเด็นที่สำคัญ

จากแนวคิดธรรมาภิบาลที่เกี่ยวข้อง สามารถแสดงความเชื่อมโยงต่อปัจจัยในการวิเคราะห์ความเสี่ยง เช่น

- ด้านนโยบายและกลยุทธ์ โครงการที่คัดเลือกมานั้น อาจมีความเสี่ยงต่อเรื่องประสิทธิผลและการมีส่วนร่วม
- ด้านการปฏิบัติงาน อาจมีความเสี่ยงต่อเรื่องประสิทธิภาพและความโปร่งใส
- ด้านการเงิน อาจมีความเสี่ยงต่อเรื่องนิติธรรมและภาระรับผิดชอบ
- ด้านกฎหมาย กฎระเบียบ อาจมีความเสี่ยงต่อเรื่องนิติธรรมและความเสมอภาค
- ด้านเทคโนโลยีสารสนเทศ อาจมีความเสี่ยงต่อเรื่องประสิทธิภาพและหลักการตอบสนอง

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	✓	✓			✓		✓		✓	
Information Technology Risk	✓	✓		✓	✓				✓	

7.4 การประเมินความเสี่ยง (Risk Assessment)

องค์กรต้องกำหนดให้หน่วยงานทุกระดับประเมินความเสี่ยงของทุกปัจจัยเสี่ยงที่ได้ระบุไว้ โดยอ้างอิงจากเกณฑ์วัดระดับความเสี่ยง โอกาสและผลกระทบ ที่องค์กรกำหนด โดยอาจใช้ฐานข้อมูลในอดีตหรือการคาดการณ์ในอนาคตเพื่อประกอบการประเมินระดับความเสี่ยง

การประเมินความเสี่ยงควรพิจารณาถึงความไม่แน่นอนของเหตุการณ์หรือเงื่อนไขต่าง ๆ ใน 2 ปัจจัยดังต่อไปนี้

- ผลกระทบของความเสี่ยง
- โอกาสที่จะเกิดความเสี่ยง

ผลกระทบ (Impact)

การประเมินความเสี่ยงควรพิจารณาถึงผลกระทบทั้งทางด้านการเงิน และที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ผลกระทบสามารถวัดได้ในเชิงของการสูญเสียทางการเงินทั้งทางตรงและทางอ้อม ส่วนการวัดผลการดำเนินงานที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ความพึงพอใจของผู้มีส่วนได้ส่วนเสีย สภาพแวดล้อมและสังคม เป็นต้น

การประเมินผลกระทบของปัจจัยเสี่ยง ควรครอบคลุมทั้งการกำหนดผลกระทบในเชิงการเงินและผลกระทบที่มิใช่ทางการเงิน อย่างไรก็ตาม บางปัจจัยเสี่ยงอาจไม่สามารถกำหนดผลกระทบในเชิงการเงินที่ชัดเจนได้ ดังนั้นในการประเมินความเสี่ยงเบื้องต้นจึงพิจารณาผลกระทบที่เกิดจากความเสี่ยงในเชิงคุณภาพเป็นส่วนใหญ่ โดยเมื่อพิจารณาระดับความรุนแรงของผลกระทบแล้วนั้น ความเสี่ยงที่มีผลกระทบมากหรือมีโอกาสเกิดสูง จำเป็นต้องได้รับการพิจารณาอย่างละเอียดจากผู้บริหารระดับสูงให้ทันท่วงที โดยกำหนดแผนการบริหารความเสี่ยงที่ท้าทาย และติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ

ตารางด้านล่างแสดงถึงตัวอย่างของผลกระทบที่เกิดจากความเสี่ยงในแบบต่าง ๆ

ประเภทของผลกระทบ	ตัวอย่าง
การเงิน	การลดลงหรือความล่าช้าในการบรรลุเป้าหมายทางรายได้ กำไร สุทธิ กระแสเงินสด หรือสินทรัพย์รวม
กลยุทธ์	การไม่บรรลุวัตถุประสงค์ขององค์กรหรือสายงาน
ทรัพยากรบุคคล	การลาออกของเจ้าหน้าที่ การสูญเสียเจ้าหน้าที่หลัก หรือปัญหาด้านจริยธรรม

ประเภทของผลกระทบ	ตัวอย่าง
ชื่อเสียง	การเผยแพร่ข่าวที่เสียหายขององค์กรในสื่อต่าง ๆ เช่น หนังสือพิมพ์ โทรทัศน์ อินเทอร์เน็ต เป็นต้น
เทคโนโลยีสารสนเทศ	เทคโนโลยีสารสนเทศล้มเหลว หรือการละเมิดความปลอดภัยของข้อมูล องค์กร
กฎระเบียบ ข้อบังคับ	การละเมิดกฎระเบียบ ข้อบังคับ
การต่อเนื่องของการดำเนินธุรกิจ	การหยุดชะงักของกระบวนการและการดำเนินการทางธุรกิจ

<u>โอกาสเกิด</u> (Likelihood)

การประเมินโอกาสเกิดของความเสี่ยง โดยทั่วไปการหาข้อมูลมาทำการสนับสนุนการประมาณการที่ถูกต้องเป็นไปได้ยาก ในกรณีที่สามารถหาข้อมูลที่เกี่ยวกับเหตุการณ์ความล้มเหลวหรือความถี่ที่เกิดขึ้นในอดีต ต้องมีความมั่นใจในฐานข้อมูลดังกล่าวว่าสามารถบ่งชี้ถึงความเป็นไปได้ของเหตุการณ์ในอนาคตได้

การประเมินโอกาสเกิดขึ้นอยู่กับระยะเวลาที่นำมาพิจารณา ดังนั้นแล้ว เมื่อทำการประเมินโอกาสเกิด ผู้บริหารต้องมีความชัดเจนในการกำหนดระยะเวลาที่จะใช้ในการพิจารณา โดยไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นได้ในระยะยาว

ประโยชน์ของผู้บริหารที่ได้จากการประเมินความเสี่ยงมีดังต่อไปนี้

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

จากประเด็นดังกล่าว แสดงให้เห็นถึงความสำคัญของการกำหนดระดับความเสี่ยงที่ยอมรับได้ และระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ขององค์กร

ความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้ โดยธุรกิจยังคงดำเนินการได้บรรลุตามเป้าหมาย

ความเสี่ยงที่ยอมรับได้กำหนดขึ้นเพื่อใช้เป็นแนวทางกำหนดกลยุทธ์ขององค์กร ทั้งนี้ความเสี่ยงที่ยอมรับได้ควรได้รับการกำหนดโดยผู้บริหารและอนุมัติโดยคณะกรรมการ การกำหนดความเสี่ยงที่ยอมรับได้ควรพิจารณาถึงความสมดุลระหว่างการเติบโต ความเสี่ยงและผลตอบแทนขององค์กร ในขณะเดียวกันองค์กรควรบริหารความเสี่ยงที่เกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้

ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) คือ ระดับความเบี่ยงเบนจากความเสี่ยงที่ยอมรับได้

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

<u>การจัดลำดับความเสี่ยง</u>

ผู้บริหารระดับสูงควรกำหนดเงื่อนไขที่ใช้ในการจัดลำดับความเสี่ยง และควรมีการสอบทานการจัดลำดับความเสี่ยงเป็นประจำ เพื่อให้สอดคล้องกับเงื่อนไขทางธุรกิจที่เปลี่ยนไป โดยมีขั้นตอนการจัดลำดับความเสี่ยงดังต่อไปนี้

<u>การกำหนดระดับของผลกระทบ</u>

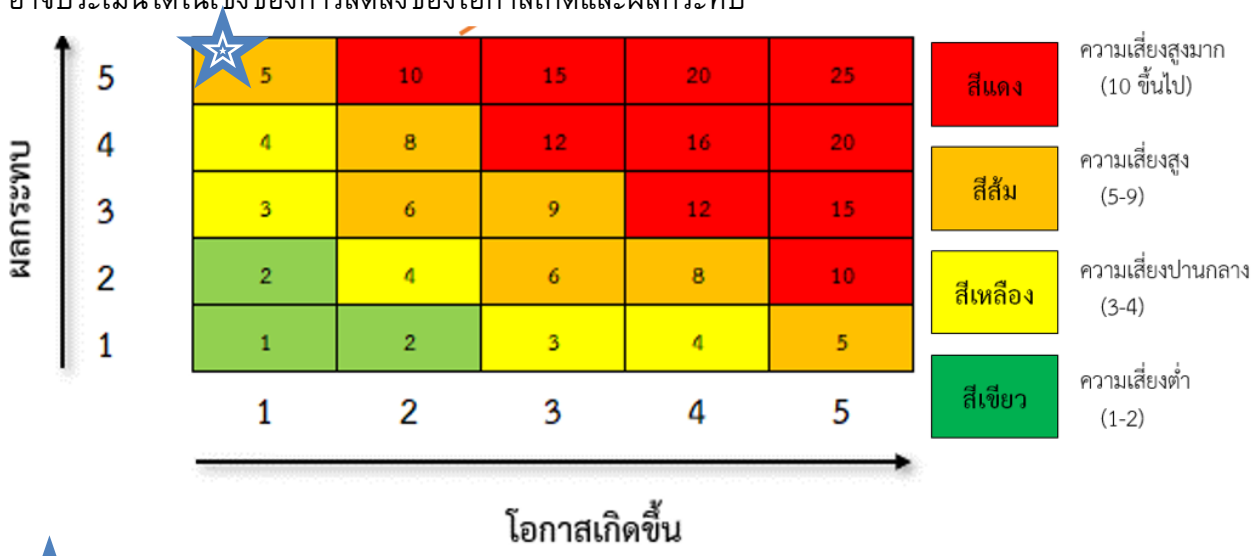
- กำหนดเงื่อนไขที่จะใช้ในการพิจารณา
  - พิจารณาทั้งเงื่อนไขทางการเงินและเงื่อนไขอื่น ๆ ที่ไม่เกี่ยวข้องกับการเงิน เช่น ยอดขาย ผลตอบแทนทางการเงิน ผลกำไร ชื่อเสียง ความสามารถในการบรรลุวัตถุประสงค์ อัตราการลาออกของเจ้าหน้าที่ ความปลอดภัยในชีวิตและทรัพย์สิน และเทคโนโลยีสารสนเทศ
  - ทำให้มั่นใจได้ว่าเงื่อนไขนั้นสอดคล้องกับวัตถุประสงค์ขององค์กร
- กำหนดมูลค่าของผลกระทบ ตามระดับคะแนน 1, 2, 3, 5 และ 25 ในการจัดลำดับ โดยระดับคะแนนนี้อาจมีการเปลี่ยนแปลงได้ ขึ้นอยู่กับความเหมาะสมกับสถานการณ์ในขณะนั้น
- ทำให้มั่นใจว่ามูลค่าต่าง ๆ ที่กำหนดเพื่อใช้ในการจัดลำดับสำหรับเงื่อนไขที่ต่างกันมีความสอดคล้องกัน ดังตัวอย่าง ระดับผลกระทบ 3 ของผลกระทบทางการเงิน สามารถเทียบเท่ากับระดับผลกระทบ 3 ของ-ผลกระทบด้านชื่อเสียง เป็นต้น

การกำหนดระดับของโอกาสเกิด

- กำหนดช่วงเวลาที่ชัดเจนสำหรับการพิจารณาโอกาสเกิด อย่างไรก็ตาม ไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นในระยะยาว
- ประยุกต์คำอธิบายในแต่ละคะแนน โดยระดับคะแนนนี้สามารถเปลี่ยนแปลงได้เช่นเดียวกับระดับคะแนนของผลกระทบ ขึ้นอยู่กับความเหมาะสมกับสถานการณ์ในขณะนั้น

แนวทางการพิจารณาความมีนัยสำคัญของความเสี่ยง

การประเมินความเสี่ยง สามารถทำได้โดยการอ้างอิงกับตารางแสดงการจัดลำดับความเสี่ยง การพิจารณาว่าความเสี่ยงใดมีนัยสำคัญ ที่ต้องนำมาดำเนินการก่อนหลัง โดยทั่วไปอาจใช้การกำหนดค่าลำดับความเสี่ยงทั้งในด้านของผลกระทบและโอกาสเกิด ทั้งนี้ การกำหนดนัยสำคัญของความเสี่ยงขององค์กรควรได้รับการพิจารณาจากผู้บริหารระดับสูงและผ่านความเห็นชอบจากคณะอนุกรรมการด้านการบริหารความเสี่ยง หลังจากการประเมินความมีนัยสำคัญของความเสี่ยงเพื่อนำมาใช้ในการกำหนดกลยุทธ์การจัดการความเสี่ยงต่าง ๆ ควรคำนึงถึงประสิทธิผลของต้นทุนที่ต้องใช้ในการจัดการความเสี่ยงนั้น ๆ กับระดับความสำคัญของความเสี่ยงที่ลดลงว่าเหมาะสมเพียงใด ทั้งนี้ความมีประสิทธิผลของการจัดการความเสี่ยงอาจประเมินได้ในเชิงของการลดลงของโอกาสเกิดและผลกระทบ



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจากเป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
3-4	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

7.5 การตอบสนองความเสี่ยง (Risk Response)

เป็นการระบุว่ามีทางเลือกใดบ้างที่สามารถใช้ในการจัดการความเสี่ยง มีความเหมาะสม และนำไปปฏิบัติเป็นส่วนหนึ่งของการบริหารความเสี่ยงของสำนักงาน ซึ่งจะต้องประเมินผลกระทบที่มีต่อโอกาสที่จะเกิดรวมทั้งต้นทุนและประโยชน์ที่ได้รับ เพื่อให้ความเสี่ยงที่เหลืออยู่ภายในช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ ทั้งนี้การตอบสนองต่อความเสี่ยงแบ่งเป็น 4 ประการ คือ การยอมรับ (Accept) การลด (Reduce) การหลีกเลี่ยง/ยกเลิก (Avoid/Terminate) และการโอนความเสี่ยง (Transfer)

สำนักงานต้องจัดให้มีการควบคุมความเสี่ยงและเพดานความเสี่ยงที่เพียงพอและเหมาะสมตามแต่ละประเภทความเสี่ยงและต้องอยู่ภายใต้ระดับความเสี่ยงที่สำนักงานยอมรับได้ รวมทั้งสอดคล้องกับมาตรฐานและหลักเกณฑ์ของหน่วยงานกำกับดูแล แนวทางปฏิบัติที่ดี ตลอดจนนโยบายบริหารความเสี่ยงกับทิศทางและกลยุทธ์การดำเนินงานของสำนักงาน พร้อมทั้งกำหนดกระบวนการปฏิบัติตามการควบคุมความเสี่ยงและเพดานความเสี่ยงที่กำหนดไว้ แนวทางการอนุมัติข้อยกเว้นกรณีจำเป็นหรือเหตุการณ์ไม่ปกติต่าง ๆ รวมถึงการทบทวนการควบคุมความเสี่ยงและเพดานความเสี่ยงดังกล่าวเป็นระยะ เพื่อให้มีประสิทธิภาพในการควบคุมและป้องกันความเสี่ยงให้กับสำนักงาน

ผู้บริหารต้องประเมินว่าปัจจุบันการจัดการความเสี่ยงเพียงพอหรือไม่ ทั้งประสิทธิภาพในการลดโอกาสเกิดความเสี่ยง และผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงต่าง ๆ หากไม่มีการจัดการความเสี่ยง หรือการจัดการในปัจจุบันไม่เพียงพอ ควรมีการพิจารณากิจกรรมอื่น ๆ เพิ่มเติมให้เหมาะสมและนำไปปฏิบัติ

<u>วัตถุประสงค์ของการจัดการความเสี่ยง</u>

- ลดโอกาสในการเกิดและผลกระทบของความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้โดยการจัดการสาเหตุของความเสี่ยงอย่างมีประสิทธิภาพ หรือโดยการจัดการผลกระทบที่อาจจะเกิดขึ้นของความเสี่ยง เช่น การมีเจ้าหน้าที่ปฏิบัติการที่พร้อมซ่อมแซมความเสียหายที่เกิดขึ้น เป็นต้น
- การลดผลกระทบของความเสี่ยง ซึ่งโดยมากมักใช้ระบบการเตือนภัย หรือระบบการบริหารพร้อมด้วยการจัดทำแผนฉุกเฉิน หรือแผนฟื้นฟู
- การเพิ่มโอกาสในการเกิด หรือผลกระทบจากความเสี่ยงที่เป็นโอกาสให้มากที่สุด โดยการปฏิบัติเพื่อสร้างหรือหาโอกาส หรือการจัดการเพื่อให้ได้ผลลัพธ์ที่ดีขึ้น

<u>กลยุทธ์ในการบริหารความเสี่ยง</u>

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 หรือลดส่วนแบ่งตลาด
- การลดขนาดการลงทุน
- เปลี่ยน หรือปรับเป้าหมาย
- การออกแบบใหม่ เช่น กระบวนการทางธุรกิจ ระบบ เครื่องมือ

การโอนย้ายความเสี่ยง (Transfer) การโอนย้าย หรือการแบ่งความเสี่ยงบางส่วนกับบุคคลหรือองค์กรอื่น

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

<u>แนวทางในการกำหนดกลยุทธ์การจัดการความเสี่ยง</u>

กลยุทธ์การจัดการความเสี่ยงถูกกำหนดขึ้นเพื่อลดระดับของความเสี่ยง ทั้งผลกระทบและโอกาสเกิดให้เป็นไปตามระดับความเสี่ยงที่ยอมรับได้ ในบางกรณีการรวมกลยุทธ์การจัดการความเสี่ยง อาจทำให้เกิดผลที่มีประสิทธิภาพมากขึ้นทั้งทางด้านต้นทุนและการปฏิบัติงาน ดังนั้น ควรต้องมีการพิจารณาการจัดการความเสี่ยงต่าง ๆ ที่อาจมีความเกี่ยวข้องกัน และอาจดำเนินการโดยหลายหน่วยงาน รวมทั้งคำนึงถึงต้นทุนที่อาจเกิดขึ้น ในการจัดให้มีการจัดการความเสี่ยงสำหรับกำหนดเป็นกลยุทธ์ในการจัดการความเสี่ยงโดยรวมเพื่อให้เกิดการจัดการความเสี่ยงบูรณาการ

ผู้บริหารอาจพิจารณาปัจจัยในการกำหนดกลยุทธ์การจัดการความเสี่ยง ต่อไปนี้

- การประเมินผลกระทบและโอกาสเกิดจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง

ในการประเมินทางเลือกของแต่ละกลยุทธ์การจัดการความเสี่ยง ผู้บริหารต้องมีความเข้าใจว่ากิจกรรมการจัดการความเสี่ยงอาจส่งผลต่อผลกระทบและโอกาสเกิดของความเสี่ยงต่างกัน ดังนั้นแล้ว การประเมินผลกระทบและโอกาสเกิดของความเสี่ยงที่อาจเปลี่ยนแปลงจากการดำเนินการตามกิจกรรมการจัดการความเสี่ยง จึงควรพิจารณาก่อนการตัดสินใจเลือกกลยุทธ์ เพื่อให้ระดับความเสี่ยงสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ขององค์กร ทั้งนี้ การประเมินผลกระทบและโอกาสเกิดหลังจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง สามารถอ้างอิงข้อมูลได้จากเหตุการณ์ในอดีต แนวโน้มของเหตุการณ์ที่อาจเกิดขึ้น และวิเคราะห์การเปลี่ยนแปลงที่อาจเกิดขึ้นในอนาคต ความเสี่ยงสามารถถูกระบุได้ทั้งอันตรายหรือโอกาสที่อาจเกิดขึ้น การกำหนดกลยุทธ์การจัดการความเสี่ยงจึงสามารถทำได้จากการประเมินปัจจัยหลัก 2 ประการ ดังนี้

1. ประเมินต้นทุนและผลตอบแทนของการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง

เนื่องจากทรัพยากรองค์กรมีจำกัด จึงมีความจำเป็นต้องประเมินต้นทุนและผลตอบแทนที่เกิดขึ้น หากมีการดำเนินการตามกิจกรรมการจัดการความเสี่ยง ในกรณีที่พบว่าผลตอบแทนที่ได้จากการดำเนินการไม่คุ้มกับต้นทุนส่วนเพิ่ม ผู้บริหารอาจพิจารณาถึงแนวทางในการโอนย้ายความเสี่ยง (Sharing) เพื่อทำการแบ่งต้นทุนให้หน่วยงานภายนอกรับผิดชอบ เช่น การทำประกันภัย หรือการร่วมทุน เป็นต้น

2. 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 โดยทั่วไปเจ้าของความเสี่ยงจะต้องรับผิดชอบในการตัดสินใจ เกี่ยวกับแผนการบริหารความเสี่ยง และแผนการปรับปรุงที่เหมาะสมสำหรับความเสี่ยงที่ไม่สามารถยอมรับได้ เมื่อแผนได้ถูกอนุมัติและได้รับการเห็นชอบ เจ้าของความเสี่ยงจะต้องรับผิดชอบต่อการนำแผนไปปฏิบัติและติดตามผลการ

ดำเนินงานของแผนนั้น และต้องแสดงให้ผู้บริหารเห็นความสำเร็จในการทำหน้าที่ของตนเกี่ยวกับการบริหารความเสี่ยง

- การพัฒนาการจัดการความเสี่ยงสำหรับความเสี่ยงที่ซับซ้อนอาจเกี่ยวข้องกับผู้บริหารระดับสูงและเจ้าหน้าที่หลายส่วนงาน ดังนั้น การสื่อสารที่ดีจึงเป็นสิ่งจำเป็นเพื่อให้แน่ใจว่าบุคคลที่เกี่ยวข้องภายในองค์กรได้ตระหนักถึงสิ่งที่กำลังดำเนินการ และบทบาทที่ต้องเกี่ยวข้องหรือปฏิบัติ

7.6 กิจกรรมการควบคุม (Control Activities)

เมื่อมีการเลือกวิธีในการตอบสนองความเสี่ยงที่เหมาะสมแล้ว กิจกรรมการควบคุมความเสี่ยง จะถูกกำหนดขึ้น เพื่อให้มั่นใจได้ว่ามีการจัดการความเสี่ยงอย่างเหมาะสม ซึ่งกิจกรรมการควบคุมเป็นกิจกรรมที่มีอยู่ในทุกหน้าที่ และทุกระดับของการปฏิบัติงานของสำนักงาน ซึ่งในการปฏิบัติงานทุกด้านนั้นต้องจัดให้มีกิจกรรมการควบคุมที่เหมาะสมเพียงพอกับระดับความเสี่ยงต่อความผิดพลาดหรือความเสียหายที่อาจเกิดขึ้น ทั้งนี้ประเภทของการควบคุม สามารถจัดกลุ่มได้ดังนี้

การควบคุมแบบป้องกัน (Preventive control) เป็นการควบคุมแบบป้องกันหรือลดความเสี่ยงจากความผิดพลาด ความเสียหาย เช่น การแบ่งแยกหน้าที่ การติดอุปกรณ์เพื่อป้องกันเหตุ เป็นต้น

การควบคุมแบบค้นหา (Detective control) เป็นการควบคุมเพื่อค้นหาความผิดพลาดหรือความเสียหายที่เกิดขึ้นแล้ว เช่น การตรวจนับ การสอบทานงาน เป็นต้น

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

การควบคุมแบบส่งเสริม (Directive control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การประกวดหรือให้รางวัลแก่ผู้ที่มีผลงานดี เป็นต้น

ดังนั้น กิจกรรมการควบคุมจึงเป็นวิธีที่นำมาใช้ในการปฏิบัติงาน เพื่อให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล โดยอาจกำหนดเป็นมาตรการ หรือขั้นตอนต่าง ๆ เป็นแผนปฏิบัติการ จัดการความเสี่ยง โดยแผนดังกล่าวต้องได้รับความเห็นชอบจากผู้บริหารในระดับที่เกี่ยวข้อง เพื่อให้การสนับสนุนทรัพยากรที่จำเป็นตามที่กำหนดไว้ในแผน เช่น บุคลากร งบประมาณ เป็นต้น ซึ่งจะประกอบด้วย

- กิจกรรมแสดงขั้นตอนและวิธีการดำเนินงาน
- ระยะเวลา / วันที่ดำเนินการแล้วเสร็จ
- เป้าหมาย

- ผู้รับผิดชอบ
- ตัวชี้วัดความเสี่ยง (KRI) เพื่อใช้ในการติดตามผลหรือเป็นสัญญาณเตือนภัยล่วงหน้า

ภาพแสดงความสัมพันธ์ของความเสี่ยงและกิจกรรมการควบคุม

การเลือกกิจกรรมการควบคุม ควรมีการพิจารณาความเกี่ยวข้อง เหมาะสมของกิจกรรมควบคุมที่มีต่อการตอบสนองความเสี่ยง และ การนำมาใช้เพื่อให้บรรลุวัตถุประสงค์เป็นสำคัญ ไม่ใช่เพื่อให้เห็นว่าต้องมีกิจกรรมการควบคุมเท่านั้น กิจกรรมการควบคุมบางอย่างที่กำหนดอาจช่วยให้องค์กรบรรลุวัตถุประสงค์มากกว่าหนึ่งวัตถุประสงค์

7.7 สารสนเทศและการสื่อสาร (Information and Communication)

สารสนเทศ หมายถึง ข้อมูลที่ได้ผ่านการประมวลผลและถูกจัดให้อยู่ในรูปแบบที่เหมาะสม มีความหมายและเป็นประโยชน์ต่อการใช้งาน ซึ่งข้อมูลสารสนเทศหมายรวมถึงข้อมูลทางการเงิน (Financial Information) และการดำเนินงานในด้านอื่น ๆ (Non-Financial Information) โดยเป็นข้อมูลทั้งจากแหล่งภายในของสำนักงาน และภายนอกสำนักงาน

สารสนเทศที่ใช้ในการปฏิบัติงาน ได้มาจากแหล่งภายในและภายนอก ทั้งในรูปแบบเชิงปริมาณ และคุณภาพ ทั้งที่เป็นสารสนเทศทางการเงิน และที่มิใช่การเงิน ที่มีความเกี่ยวข้องกับวัตถุประสงค์ขององค์กรหลาย ๆ ประเภท

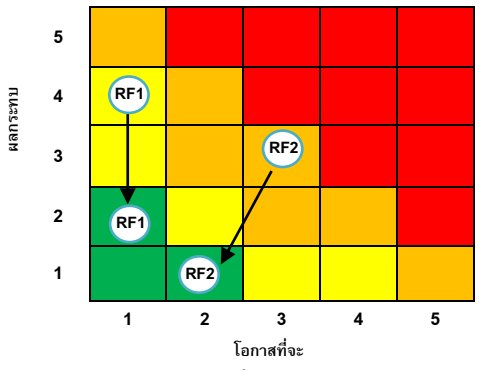
การมีสารสนเทศที่ถูกต้อง ตรงเวลา และถูกสถานที่ เป็นสิ่งจำเป็นที่จะมีผลต่อการบริหารความเสี่ยงขององค์กร ทุกระดับขององค์กรต้องการสารสนเทศ เพื่อใช้ในการกำหนดกลยุทธ์ ระบุ ประเมิน ตอบสนองควบคุม และติดตามรายงานผล ความเสี่ยง เพื่อให้การดำเนินงานบรรลุวัตถุประสงค์ขององค์กร

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 การเชิญพบปะหารือ การเชิญประชุม เป็นต้น

- **แสดงผลการบริหารความเสี่ยงของแต่ละปัจจัยเสี่ยง เทียบกับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite)**
- **แสดงระดับความเสียหายของแต่ละปัจจัยเสี่ยง ทั้งก่อนและหลังบริหารปัจจัยเสี่ยงนั้น ๆ โดยใช้แผนภูมิความเสี่ยง (Risk Map) ในการอธิบาย**



การจัดทำผลการบริหารความเสี่ยง ควรรายงานระดับความรุนแรงในแต่ละปัจจัยเสี่ยง โดยครอบคลุมทั้ง 4 ปัจจัย ดังนี้

1. **ระดับความรุนแรงก่อนการบริหารความเสี่ยง**
2. **ระดับความรุนแรงตามเป้าหมายที่องค์กรคาดหวัง**
3. **ระดับความรุนแรงหลังการบริหารความเสี่ยง**
4. **ระดับความรุนแรงที่องค์กรยอมรับได้**

ทุกระดับที่ลดลงไม่ว่าจะเป็นโอกาสหรือผลกระทบก็ตาม องค์กรควรแสดงผลการวิเคราะห์อย่างชัดเจนเปรียบเทียบกับเกณฑ์ที่กำหนด

ผลการบริหารความเสี่ยง : ปัจจัยเสี่ยง

ความรุนแรงก่อนการบริหารความเสี่ยง	
โอกาส	ผลกระทบ

เป้าหมายที่คาดหวัง	
โอกาส	ผลกระทบ

ความรุนแรงหลังการบริหารความเสี่ยง	
โอกาส	ผลกระทบ

ความรุนแรงที่องค์กรยอมรับได้	
โอกาส	ผลกระทบ

ทั้งนี้ องค์กรจะต้องมีการสื่อสารเพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่ มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง นอกจากนี้ควรมีการประเมินประสิทธิภาพและประสิทธิผลของการสื่อสาร เป็นระยะ ๆ เพื่อให้การสื่อสารเป็นส่วนหนึ่งของการควบคุมภายใน ที่เป็นประโยชน์สูงสุดต่อองค์กร

7.8 การติดตามและประเมินผล (Monitoring)

การติดตามและการรายงานผลเป็นกิจกรรมที่ใช้เพื่อติดตามและสอบทานแผนการจัดการความเสี่ยง เพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงมีประสิทธิภาพและเหมาะสม หรือควรปรับเปลี่ยน หากแผนนั้นไม่มีประสิทธิภาพเพียงพอ โดยกำหนดข้อมูลที่ต้องติดตาม และความถี่ในการสอบทาน และควรกำหนดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อประเมินว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้วหรือมีความเสี่ยงใหม่เพิ่มขึ้น

การติดตามผลโดยทั่วไปมักจะดำเนินการโดยผู้บริหารและบุคลากรภายในองค์กรเอง อย่างไรก็ตาม อาจให้บุคคลภายนอก เช่น ที่ปรึกษา หรือผู้เชี่ยวชาญอิสระ ช่วยในการติดตามการจัดการความเสี่ยงเป็นครั้งคราวได้ ความเสี่ยงและการจัดการต่อความเสี่ยงอาจมีการเปลี่ยนแปลงตลอดเวลา การจัดการต่อความเสี่ยงที่เคยมีประสิทธิผล อาจเปลี่ยนเป็นกิจกรรมที่ไม่เหมาะสม กิจกรรมการควบคุมอาจมีประสิทธิผลน้อยลงหรือไม่ควรดำเนินการต่อไป หรืออาจมีการเปลี่ยนแปลงในวัตถุประสงค์หรือกระบวนการต่าง ๆ ดังนั้นแล้ว ผู้บริหารควรประเมินกระบวนการบริหารความเสี่ยง เป็นประจำเพื่อให้มั่นใจว่าการบริหารความเสี่ยงมีประสิทธิผลเสมอ

ลักษณะหลักของการติดตามความเสี่ยง คือ

- การประเมินควรมีประสิทธิผลและความต่อเนื่องของกิจกรรมการควบคุม และกิจกรรมอื่นที่ใช้จัดการความเสี่ยง
- การกำหนดระดับความเสี่ยงที่ยอมรับได้ที่เหมาะสมและสอดคล้องกับกลยุทธ์ทางธุรกิจ
- การรวบรวมและบันทึกข้อมูลอย่างครบถ้วน ถูกต้อง ทันเวลา
- การติดต่อสื่อสารเกี่ยวกับความเสี่ยงและกระบวนการต่าง ๆ อย่างสม่ำเสมอและเปิดเผยทั้งแบบเป็นทางการและไม่เป็นทางการ
- การกำหนดตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators : KRIs) ที่สะท้อนถึงสาเหตุความเสี่ยง (Root Cause) เพื่อการติดตามระบบการควบคุมภายในของหน่วยงาน และสถานะของความเสี่ยงในแต่ละประเภท (Risk Type) ทำให้หน่วยงานสามารถวางแผนในการบริหารจัดการความเสี่ยงได้อย่างเหมาะสม และมีประสิทธิภาพ และสามารถป้องกัน ควบคุมเหตุการณ์ความเสียหายได้อย่างทันท่วงที โดยตัวชี้วัดความเสี่ยงที่ดีนั้น นอกจากจะสะท้อนให้หน่วยงานเห็นถึงความเสี่ยงที่เคยเกิดขึ้นในอดีตที่ผ่านมา (Lagging Indicators) แล้ว ยังควรสามารถบ่งชี้ หรือพยากรณ์ให้ผู้บริหารหน่วยงาน และผู้บริหารสายงานสามารถคาดคะเนถึงความเสี่ยงที่อาจจะเกิดขึ้นในอนาคต (Forward Looking/Leading Indicators) ได้อีกด้วย

ตารางแสดง ตย.ดัชนีชี้วัดความเสี่ยง (KRIs)

Lagging Indicators	Forward Looking/Leading Indicators
เป็นตัวชี้วัดความเสี่ยงที่ได้มาจากเหตุการณ์ความเสียหายในอดีต ตัวอย่างเช่น	เป็นตัวชี้วัดความเสี่ยงที่สามารถชี้นำให้เห็นถึง**แนวโน้มที่จะเกิด**เหตุการณ์ความเสียหายในอนาคตได้ ตัวอย่างเช่น
● พนักงานที่เป็น High Performer ลาออก	● อัตราการลาออกของพนักงาน
● ระบบงานหลักขององค์กรหยุดชะงัก/ขัดข้อง	● ระบบงานหยุดชะงัก/ขัดข้อง

แนวทางการรายงานผลการดำเนินงาน มีดังนี้

8.1 คณะอนุกรรมการด้านการบริหารความเสี่ยง

8.1.1 รายงานต่อคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

- รายงานแผนการบริหารความเสี่ยงประจำปี รวมทั้งแผนปฏิบัติการเพื่อการจัดการความเสี่ยง ปีละ 1 ครั้ง

- รายงานผลการดำเนินการและความคืบหน้าการจัดการความเสี่ยงที่สำคัญระดับองค์กร ต่อคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) อย่างน้อยไตรมาสละ 1 ครั้ง

8.1.2 รายงานต่อคณะกรรมการตรวจสอบ

- รายงานผลการดำเนินงานอย่างน้อยปีละ 1 ครั้ง

8.2 ผู้จัดการความเสี่ยงและการควบคุมภายใน (ของแต่ละฝ่าย)

- รายงานต่อฝ่ายที่เกี่ยวข้อง /รองผู้อำนวยการ สพร. /ผู้อำนวยการ สพร. /คณะอนุกรรมด้านการบริหารความเสี่ยง

- รายงานความเสี่ยงระดับองค์กรในส่วนที่รับผิดชอบและแผนปฏิบัติการการจัดการความเสี่ยง ตลอดจนความคืบหน้าในการจัดการความเสี่ยงตามแผน พร้อมทั้งปัญหาและอุปสรรค เดือนละ 1 ครั้ง

8.3 ส่วนบริหารความเสี่ยง

8.3.1 รายงานต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

- รายงานความเสี่ยงที่สำคัญระดับองค์กร รวมทั้งรายละเอียดการจัดการความเสี่ยงตลอดจนความคืบหน้าของแผนปฏิบัติการและประเด็นสำคัญเพื่อการพิจารณาของคณะอนุกรรมการด้านการบริหารความเสี่ยงทุกครั้ง ที่มีการประชุมคณะอนุกรรมการด้านการบริหารความเสี่ยง

- รายงานเหตุการณ์ที่เกิดขึ้นใหม่ทั้งที่เป็นโอกาสและความเสี่ยงที่มีผลต่อสำนักงาน จาก สภาพแวดล้อมที่เปลี่ยนแปลงไปเป็นการเฉพาะกิจ

- รายงานกรณีฉุกเฉินภายใน 3 วันทำการ ในการประชุมเป็นกรณีพิเศษ เมื่อดัชนีชี้วัด ความเสี่ยง (KRI) มีการเปลี่ยนแปลงและอาจมีผลกระทบอย่างรุนแรงต่อการบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร

สำนักงานต้องสนับสนุนให้เกิดการสื่อสารในเชิงรุกและให้มีการสื่อสารอย่างสม่ำเสมอ ช่องทางในการสื่อสารอย่างเป็นทางการที่ใช้ในการพิจารณาความเสี่ยง การควบคุม และแผนการดำเนินการ ได้แก่ การประชุมทั่วไปของผู้บริหาร การประชุมคณะทำงาน รายงานประจำเดือนสำหรับผู้บริหาร การประชุมคณะอนุกรรมการ ด้านการบริหารความเสี่ยง เป็นต้น การสื่อสารอย่างต่อเนื่องจะช่วยให้มีข้อมูลความเสี่ยงที่เพียงพอและได้รับการนำเสนอเพื่อใช้ในการตัดสินใจอย่างทันท่วงที ในบางกรณีการจัดการกับความเสี่ยงด้วยวิธีการที่เร่งด่วน เช่น การประสานงานทางโทรศัพท์ อาจมีความเหมาะสมกว่ารอการจัดทำรายงานอย่างเป็นทางการ ผู้ที่เกี่ยวข้องต้องรายงานความเสี่ยงที่มีระดับความเสี่ยงสูงให้แก่ผู้บังคับบัญชาทราบอย่างสม่ำเสมอและทันท่วงที พร้อมทั้งอธิบายวิธีการจัดการความเสี่ยงเหล่านั้น นอกจากนี้ ผู้บริหารในแต่ละหน่วยงานควรพิจารณาและนำเสนอความเสี่ยงที่มีระดับความเสี่ยงสูงของหน่วยงาน หรือความเสี่ยงที่ควร

จะต้องได้รับการจัดการในระดับที่สูงกว่าขึ้นไปยังผู้บริหารในสายบังคับบัญชาเพื่อทำการพิจารณาความเสี่ยงและหาแนวทางการจัดการความเสี่ยงในระดับงานที่สูงขึ้นต่อไป

8. Governance Risk management & Compliance (GRC)

GRC คือ แนวคิดในการเชื่อมโยงและบูรณาการนิยามของสามองค์ประกอบ ได้แก่

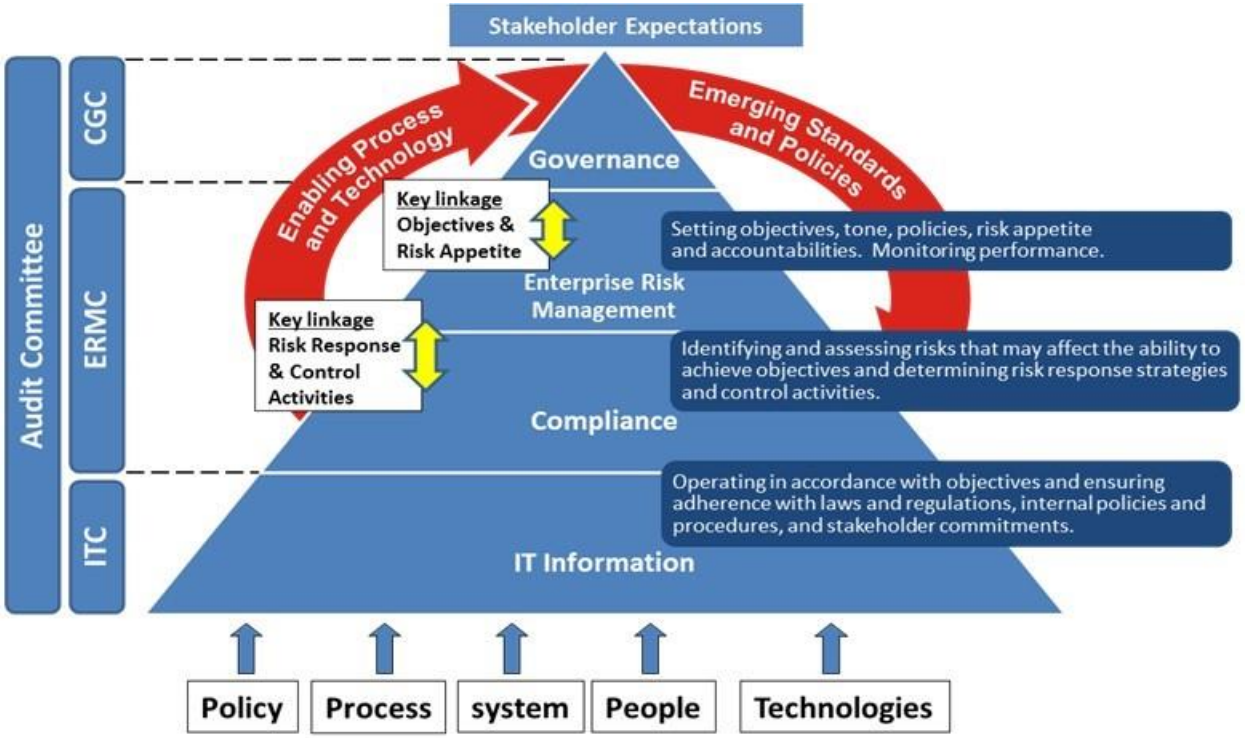
Governance หมายถึง นโยบาย วัฒนธรรมองค์กร กระบวนการขั้นตอนการปฏิบัติงานที่ถูกกำหนดออกมาอย่างชัดเจนในการบริหารจัดการและกำกับดูแลองค์กรโดยผู้บริหารระดับสูงเพื่อการบริหารองค์กรที่โปร่งใส ซึ่งรวมถึงความสัมพันธ์และบทบาทของทุกคนในองค์กร ตลอดจนกำหนดเป้าหมายหลักที่เน้นเรื่องความโปร่งใสในการบริหารจัดการของผู้บริหารระดับสูงในองค์กร

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

Compliance หมายถึง การดำเนินงานกำกับเพื่อให้มั่นใจว่า การปฏิบัติการทุกอย่างอยู่ภายใต้กฎเกณฑ์อย่างเหมาะสม ไม่มีการฝ่าฝืนใด ๆ เกิดขึ้น โดยกฎเกณฑ์ที่ว่านี้รวมทั้งระเบียบ ข้อบังคับ กฎหมาย คำสั่งภายในองค์กร พันธะที่ผูกพันไว้กับผู้มีส่วนได้เสีย คู่สัญญาทุกภาคส่วน ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความปลอดภัยขององค์กรอย่างถูกต้องตามมาตรฐาน การปฏิบัติตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์ เป็นต้น การดำเนินงานในส่วนของการปรับปรุงประสิทธิภาพและประสิทธิผลในการกำกับการปฏิบัติตามกฎเกณฑ์ ในลักษณะที่ติดตาม เฝ้าระวังการเปลี่ยนแปลงในด้านกฎเกณฑ์และระเบียบเพื่อทำความเข้าใจ การศึกษาผลกระทบของกฎเกณฑ์ภายนอกต่อการดำเนินงานภายในและความจำเป็นในการปรับนโยบาย ระเบียบประกาศ กระบวนการปฏิบัติงานและสื่อสารเพื่อมิให้เกิดการฝ่าฝืน ซึ่งถือเป็นส่วนหนึ่งของการกำกับดูแลที่ดี

การพัฒนาแนวคิดจากการบริหารแบบ Silo มาเป็นกรอบแนวคิดที่บูรณาการ GRC เข้าด้วยกัน โดยแนวคิด GRC นั้นไม่ได้เป็นการพยายามที่จะรวบเอางาน 3 ด้าน มาไว้ที่ศูนย์กลางเพียงจุดเดียว หากแต่ต้องการที่จะนำองค์ประกอบทั้ง 3 มาปฏิบัติร่วมกันในรูปแบบของการทำงานเป็นทีม เป็นการแสวงหาแนวทาง การเชื่อมโยงบูรณาการงาน 3 ด้านเข้าด้วยกันในเชิงนโยบาย กระบวนการดำเนินงาน ขั้นตอนการปฏิบัติและระบบการควบคุม แบ่งปันข้อมูลซึ่งกันและกัน มีการเปิดกว้างทางความคิดที่จะปรับปรุงองค์กรจากข้อมูลและแนวทางจากผู้บริหารของหลาย ๆ ฝ่าย โดยต้องได้รับการสนับสนุนจากองค์ประกอบพื้นฐาน

หลัก 5 ประการขององค์กร ได้แก่ กลยุทธ์ กระบวนการ ระบบ บุคลากร เทคโนโลยี ดังรูปความสัมพันธ์และความเชื่อมโยงตามภาพ ตัวอย่าง เช่น



- การรณรงค์ปลูกฝัง ปรับเปลี่ยนวัฒนธรรมขององค์กร เพื่อนำบุคคลภายในองค์กรไปสู่วัตถุประสงค์และเป้าหมายด้านวัฒนธรรมองค์กรที่คาดหวังเพื่อเพิ่มประสิทธิภาพ สนับสนุนหรือผลักดันให้การดำเนินงานขององค์กรบรรลุตามวัตถุประสงค์ได้ดีขึ้น ทั้งยังทำให้เกิดผลลัพธ์เชิงวัฒนธรรมองค์กรที่พึงประสงค์ด้วย

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

- การที่บุคลากรมีความมุ่งมั่น ยึดถือและส่งเสริมวัฒนธรรมของการดำเนินธุรกิจอย่างมีศักดิ์ศรีและคุณค่าทางจริยธรรม รับผิดชอบในผลงานของตน มีมุมมองที่เป็นหนึ่งเดียวกับองค์กรและต่อต้านการทำกิจกรรมที่ต่างคนต่างทำตามอำนาจหน้าที่เฉพาะตัว เน้นการทำงานเป็นทีมโดยคำนึงถึงประโยชน์ขององค์กรเป็นหลัก

- การควบคุมภายในที่เพียงพอในการลดความเสี่ยงของบุคคล ช่วยกำกับคนมากขึ้น เช่น การกำกับติดตาม (Monitoring) การใช้ระบบควบคุมการตรวจสอบคุณภาพงานและการทดสอบผลงานว่าใช้งานได้จริงอย่างสม่ำเสมอและมีประสิทธิผล หรือกระบวนการฝึกอบรมบุคลากร เพื่อให้เหมาะสมกับความรับผิดชอบในภารกิจ การกำหนดให้มีมาตรฐานการทำงานที่ชัดเจน

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

- การประสานงานและเชื่อมโยงเครื่องมือ ระบบงาน และคน

โดย GRC จะช่วยทำให้องค์กรเกิดความสามารถในการแข่งขันในระยะยาว เพิ่มความโปร่งใสในการเปิดเผยข้อมูล เสริมภาพลักษณ์ที่ดีให้กับองค์กร ตลอดจนคณะผู้บริหารระดับสูง รวมทั้งการสร้างจิตสำนึกในการปฏิบัติงานที่ดีให้กับเจ้าหน้าที่ทุกคน ส่งผลให้ลูกค้าเกิดความเชื่อถือและความมั่นใจในการใช้บริการต่าง ๆ ขององค์กร

9. ปัจจัยสำเร็จในการบริหารความเสี่ยงขององค์กร

การบริหารความเสี่ยงที่ประสบความสำเร็จต้องมีปัจจัยสำคัญ ซึ่งประกอบทั้งด้านทรัพยากรและโครงสร้างพื้นฐานที่จำเป็นเพื่อให้เกิดการบริหารความเสี่ยงที่ประสบผลสำเร็จและยั่งยืน ดังนี้

1. ความมุ่งมั่นของผู้บริหารในการจัดให้มีระบบการบริหารความเสี่ยง

การปฏิบัติตามกรอบการบริหารความเสี่ยงขององค์กร จะประสบความสำเร็จเพียงใดขึ้นอยู่กับเจตนารมย์ การสนับสนุน การมีส่วนร่วม และความเป็นผู้นำของผู้บริหารระดับสูงในองค์กร คณะกรรมการและผู้บริหารระดับสูงต้องให้ความสำคัญและสนับสนุนให้ทุกคนในองค์กรเข้าใจความสำคัญในคุณค่าของการบริหารความเสี่ยงต่อองค์กร มิฉะนั้นแล้วการบริหารความเสี่ยงไม่สามารถเกิดขึ้นได้ การบริหารความเสี่ยงต้องเริ่มต้นจากผู้นำสูงสุดขององค์กรต้องการให้เกิดระบบขึ้น โดยกำหนดนโยบายให้มีการปฏิบัติ รวมถึงการกำหนดให้ผู้บริหารต้องใช้ข้อมูลเกี่ยวกับความเสี่ยงในการตัดสินใจและบริหารงาน

2. ความเข้าใจเกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงในทางเดียวกัน

การใช้คำนิยามเกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงแบบเดียวกัน จะทำให้มีประสิทธิภาพในการกำหนดวัตถุประสงค์ นโยบาย กระบวนการ เพื่อใช้ในการบ่งชี้และประเมินความเสี่ยงและกำหนดวิธีการจัดการความเสี่ยงที่เหมาะสม

องค์กรที่จัดทำนโยบาย และกรอบ การบริหารความเสี่ยง ที่มีคำอธิบายองค์ประกอบในกรอบการบริหารความเสี่ยงอย่างชัดเจน จะทำให้ผู้บริหารและเจ้าหน้าที่ทุกคนเข้าใจความเสี่ยงในแนวทางเดียวกันและมีจุดหมายร่วมกันในการบริหารความเสี่ยง

3. กระบวนการบริหารการเปลี่ยนแปลง

ในการนำเอากระบวนการและระบบบริหารแบบใหม่มาใช้ องค์กรจำเป็นต้องมีการบริหารการเปลี่ยนแปลงเหล่านี้ การพัฒนาการบริหารความเสี่ยงก็เช่นเดียวกัน ต้องมีการชี้แจงให้ผู้บริหารและเจ้าหน้าที่ทุกคนรับทราบถึงการเปลี่ยนแปลง และผลที่องค์กรและแต่ละบุคคลจะได้รับจากการเปลี่ยนแปลงเหล่านั้น

4. การกำหนดกระบวนการบริหารความเสี่ยงที่ต่อเนื่อง

องค์กรที่ประสบความสำเร็จในการปฏิบัติตามกระบวนการบริหารความเสี่ยง คือ องค์กรที่สามารถนำกระบวนการบริหารความเสี่ยงมาปฏิบัติอย่างทั่วถึงทั้งองค์กร และกระทำอย่างต่อเนื่องสม่ำเสมอ

5. การสื่อสาร การเรียนรู้ และการอบรมที่มีประสิทธิภาพ

วัตถุประสงค์ของการสื่อสารอย่างมีประสิทธิผลนั้น เพื่อให้มั่นใจได้ว่า

- ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา
- ผู้บริหารสามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่

- มีการติดตามแผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กร และจัดการความเสี่ยงต่าง ๆ เพื่อให้องค์กรมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด โดยที่การสื่อสารเกี่ยวกับกลยุทธ์ การบริหารความเสี่ยงและวิธีปฏิบัติมีความสำคัญอย่างมาก เพราะการสื่อสารจะเน้นให้เห็นถึงความเชื่อมโยงระหว่างการบริหารความเสี่ยงกับกลยุทธ์องค์กร การชี้แจงทำความเข้าใจต่อเจ้าหน้าที่ทุกคนถึงความรับผิดชอบแต่ละบุคคลต่อกระบวนการบริหารความเสี่ยง จะช่วยให้เกิดการยอมรับในกระบวนการและนำมาซึ่งความสำเร็จในการพัฒนาการบริหารความเสี่ยง โดยควรได้รับการสนับสนุนในทางปฏิบัติจากผู้บริหารระดับสูง และคณะกรรมการขององค์กร

6. การวัดความเสี่ยง

การวัดผลการบริหารความเสี่ยงประกอบด้วย 2 รูปแบบ ดังนี้

6.1 การวัดความเสี่ยงในรูปแบบของผลกระทบและโอกาสที่อาจเกิดขึ้น การบริหารความเสี่ยงที่ประสบความสำเร็จจะช่วยให้ความเสี่ยงเหลืออยู่ในระดับที่องค์กรยอมรับได้

6.2 การวัดความสำเร็จของการบริหารความเสี่ยง โดยอาศัยดัชนีวัดผลการดำเนินงาน (KRI) ซึ่งอาจกำหนดเป็นระดับองค์กร สายงาน ฝ่าย หรือรายบุคคล การใช้ดัชนีวัดผลการดำเนินงานนี้อาจปฏิบัติร่วมกับกระบวนการด้านทรัพยากรบุคคล

7. การสนับสนุนการบริหารความเสี่ยงโดยกลไกด้านทรัพยากรบุคคล

คณะกรรมการ ผู้บริหารและเจ้าหน้าที่ทุกคนในองค์กรควรได้รับการฝึกอบรมเพื่อให้เข้าใจกรอบการบริหารความเสี่ยง และความรับผิดชอบของแต่ละบุคคลในการจัดการความเสี่ยงและสื่อสารข้อมูลเกี่ยวกับความเสี่ยง การฝึกอบรมในองค์กรควรคำนึงถึงประเด็นดังต่อไปนี้

- ความแตกต่างกันของระดับความรับผิดชอบในการบริหารความเสี่ยง
- ความรู้ที่เกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงที่มีอยู่แล้วในองค์กร

ระบบการประเมินผลการดำเนินงาน ถือเป็นเครื่องมือสำคัญที่ใช้ในการส่งเสริมความรับผิดชอบของแต่ละบุคคล โดยความรับผิดชอบเกี่ยวกับการบริหารความเสี่ยงควรกำหนดรวมอยู่ในงานที่แต่ละบุคคลรับผิดชอบ และในคำอธิบายลักษณะงาน (Job Description) การประเมินผลการดำเนินงานส่วนที่เกี่ยวกับการบริหารความเสี่ยงมีประเด็นที่ควรประเมินดังต่อไปนี้

- ความรับผิดชอบและการสนับสนุนกระบวนการบริหารความเสี่ยงและกรอบการบริหารความเสี่ยงที่แต่ละบุคคลมีต่อองค์กร
- การวัดระดับของความเสี่ยงที่บุคคลนั้นเป็นผู้รับผิดชอบว่าความเสี่ยงได้รับการจัดการอย่างมีประสิทธิผลเพียงใด

8. กระบวนการติดตามการบริหารความเสี่ยง

ขั้นตอนสุดท้ายของปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง คือ การกำหนดวิธีที่เหมาะสมในการติดตามการบริหารความเสี่ยง

การติดตามกระบวนการบริหารความเสี่ยง

- การนำแผนตอบสนองความเสี่ยงไปปฏิบัติ และระดับความเสี่ยงที่เหลืออยู่หลังการปฏิบัติตามแผน
- การรายงานและการสอบทานตามขั้นตอนตามกระบวนการบริหารความเสี่ยง
- ความชัดเจนและสม่ำเสมอของการมีส่วนร่วมและความมุ่งมั่นของผู้บริหารระดับสูง
- บทบาทของผู้นำในการสนับสนุนและติดตามการบริหารความเสี่ยง
- การประยุกต์ใช้เกณฑ์การประเมินผลการดำเนินงานที่เกี่ยวข้องกับการบริหารความเสี่ยง

คู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

(Strategic Risk Management Manual)

สารบัญ

หน้า

1. บทนำ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ให้ความสำคัญต่อการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ (Strategic Risk Management) เป็นอย่างมาก โดยมีคณะกรรมการ สพร. แนะนำและติดตามการรายงานผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อหาแนวทางแก้ไขปัญหาที่เกิดจากปัจจัยเสี่ยงต่าง ๆ นอกจากนี้ยังกำหนดให้มีการดูแลและทบทวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์อย่างต่อเนื่อง เพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่สำนักงานยอมรับได้

การบริหารความเสี่ยงด้านนโยบายและกลยุทธ์จึงเป็นกระบวนการสำคัญที่จะลดโอกาสของความเสี่ยงที่อาจเกิดขึ้นและบรรเทาผลกระทบที่องค์กรจะได้รับในทุกหน่วยงานของสำนักงาน ดังนั้น กระบวนการบริหารความเสี่ยงจะช่วยลดความสูญเสียที่อาจจะเกิดขึ้นให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ รวมทั้งเป็นองค์ประกอบสำคัญในการกำกับดูแลสำนักงาน ให้บรรลุผลสำเร็จตามเป้าหมายที่กำหนด

สำนักงานได้กำหนดกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ เพื่อให้หน่วยงานต่าง ๆ ของ สำนักงานใช้เป็นแนวทางในการพิจารณา และจัดทำแผนกลยุทธ์และแผนธุรกิจที่สอดคล้องกับกลยุทธ์หลักของสำนักงาน โดยการระบุความเสี่ยงที่อาจเกิดขึ้นแล้วทำการประเมินความเสี่ยงถึงโอกาสที่จะเกิดขึ้นรวมทั้งผลกระทบที่จะได้รับ พร้อมทั้งจัดหาแนวทางหรือมาตรการควบคุมที่เหมาะสมมาดำเนินการหรือจัดการกับความเสี่ยงนั้น โดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่สำนักงานกำหนด

คู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ของสำนักงานนี้ จึงมุ่งเน้นถึงการสร้างความตระหนักให้เกิดแก่ทุกคนที่เกี่ยวข้องในสำนักงาน ในการที่จะช่วยสอดส่องดูแล ระมัดระวัง เพื่อลดความเสี่ยง หรือบรรเทาผลกระทบจากความเสี่ยงด้านนโยบายและกลยุทธ์ อันเกิดจากความเสี่ยงที่ไม่สามารถบรรลุเป้าหมายตามนโยบายและกลยุทธ์ ของสำนักงาน เช่น การไม่สามารถดำเนินโครงการ G-Cloud หรือ MailGoThai ได้ตามแผนงาน เป็นต้น ความเสี่ยงที่เกิดขึ้นดังกล่าวข้างต้นเป็นความเสี่ยงด้านนโยบายและกลยุทธ์ ที่ส่งผลต่อความสำเร็จตามนโยบายที่ได้รับมอบหมายจากสำนักนายกรัฐมนตรี หรือนโยบายภาครัฐได้ตามกำหนด รวมทั้งอาจส่งผลต่อภาพลักษณ์ขององค์กรและทำให้องค์กรไม่สามารถดำเนินการได้ครบถ้วนสมบูรณ์ตามวัตถุประสงค์และภารกิจที่กำหนดไว้

คู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) โดยจะกล่าวถึงวัตถุประสงค์ ขอบเขต โครงสร้างและบทบาทหน้าที่ของผู้รับผิดชอบกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ และรายละเอียดของกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ เพื่อเป็นแนวทางในการปฏิบัติงาน และเพื่อให้

หน่วยงานต่าง ๆ ของสำนักงานใช้เป็นแนวทางในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

แนวทางการบริหารความเสี่ยงที่นำมาใช้

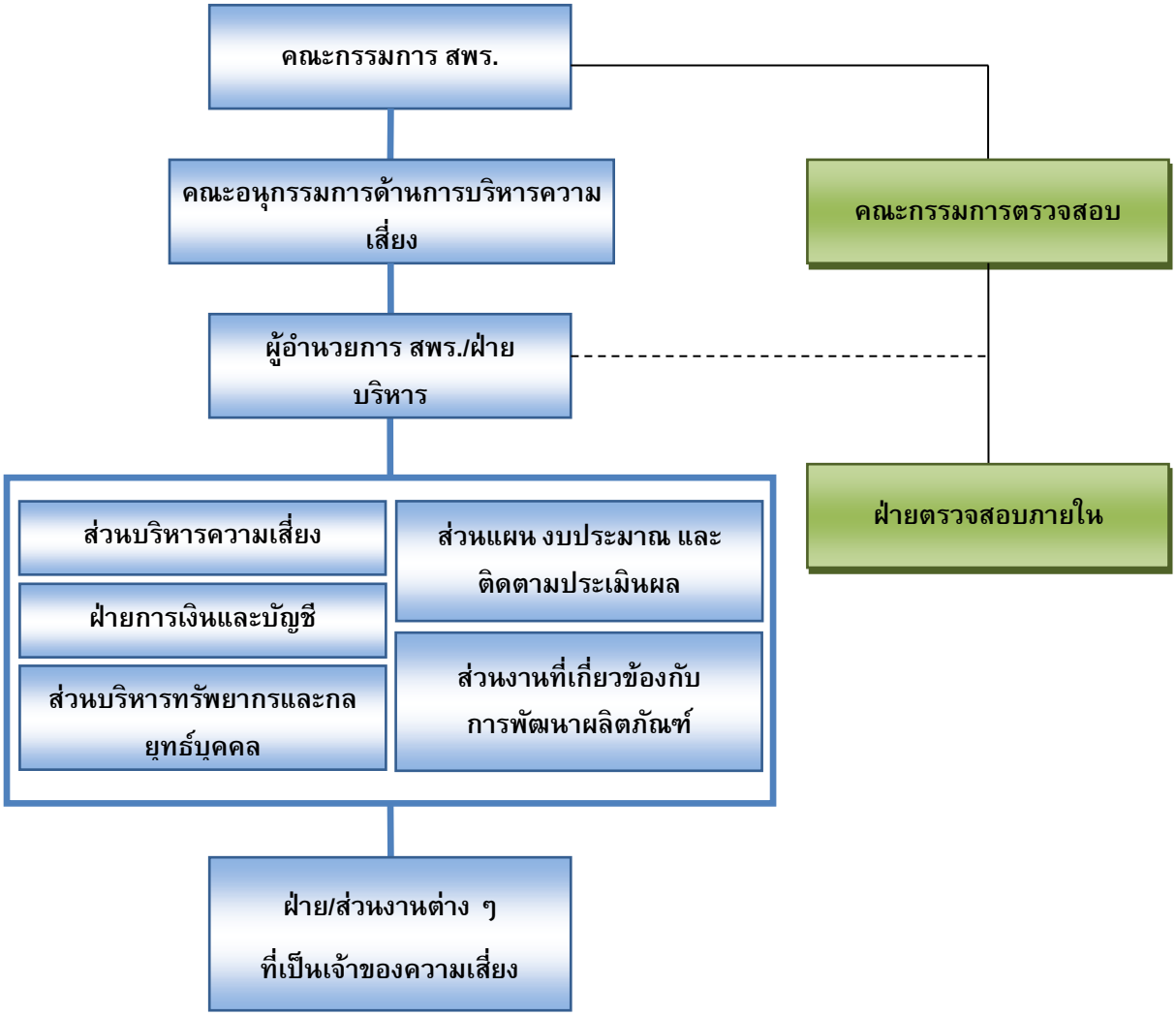
สำนักงานกำหนดกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ตามแนวทางการปฏิบัติงานของ สำนักงาน และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Treadway Commission (COSO) โดยครอบคลุมความเสี่ยงธุรกิจ (Business Risk) ที่เกี่ยวกับการจัดทำและการกำหนดแผนงานของแผนกลยุทธ์ (Strategic Risk) และการจัดการ (Management Risk) ให้อยู่ในระดับที่เหมาะสมกับความซับซ้อนของธุรกิจ

ขอบเขตของคู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ ซึ่งครอบคลุมถึงความเสี่ยงอันเกิดจากการดำเนินงานที่ไม่เป็นไปตามแผนกลยุทธ์ของสำนักงาน รวมทั้งนโยบายที่ได้รับจากสำนักนายกรัฐมนตรี รวมทั้งนโยบายภาครัฐ ตั้งแต่การกำหนดแผนงานที่รองรับนโยบายไม่ครบถ้วน การดำเนินงานไม่ได้ตามเป้าหมายแผนกลยุทธ์ของโครงการหลัก เช่น โครงการ G-Cloud, GINหรือ MailGoThai เป็นต้น รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นจากปัจจัยภายนอก เช่น การเปลี่ยนแปลงนโยบายภาครัฐ เป็นต้น โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ เพื่อให้หน่วยงานต่าง ๆ ของสำนักงานใช้เป็นแนวทางในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ของตนเอง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

2. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์



3. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายกลยุทธ์องค์กร มีหน้าที่รับผิดชอบดังนี้

1. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ และนำเสนอต่อคณะกรรมการ สพร. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
2. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์
3. จัดทำคู่มือบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ และเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
4. ประสานงานกับส่วนแผน งบประมาณ และติดตามประเมินผล ฝ่ายบัญชีและการเงิน ส่วนงานที่เกี่ยวข้องกับการพัฒนาผลิตภัณฑ์ เพื่อจัดให้หน่วยงานต่าง ๆ ดำเนินการพิจารณา Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของหน่วยงาน รวมถึงแนวทางการจัดการความเสี่ยงที่เหมาะสม
5. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทาง ความสำคัญ และความรับผิดชอบในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์
6. ดูแลให้มีการปฏิบัติตามกระบวนการในการออก/ปรับปรุงผลิตภัณฑ์ตามแนวทางที่สำนักงานกำหนดและมีส่วนร่วมพิจารณาให้ความเห็นในการออกผลิตภัณฑ์ในประเด็นที่เกี่ยวข้องกับความเสี่ยง รวมทั้งปรับปรุงหรือแก้ไขข้อบกพร่องที่เกี่ยวกับความเสี่ยงด้านต่าง ๆ ที่เกิดขึ้นภายหลังการออก/ปรับปรุงผลิตภัณฑ์ โดยดำเนินการร่วมกับหน่วยงานเจ้าของผลิตภัณฑ์นั้น ๆ
7. ร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) สำหรับสถานการณ์ที่ไม่ปกติ เพื่อรองรับการเปลี่ยนแปลงสภาพแวดล้อมที่ไม่เป็นไปตามที่คาดไว้
8. ร่วมกับฝ่ายบัญชีและการเงิน ส่วนแผน งบประมาณ และติดตามประเมินผล ส่วนงานที่เกี่ยวข้องกับการพัฒนาผลิตภัณฑ์ เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนนโยบายและกลยุทธ์ และงบประมาณรวมของสำนักงาน โดยดำเนินการต่อไปนี้
   (1) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับสำนักงาน พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง

(Likelihood) และผลกระทบ (Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยง และกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือก พร้อมทั้งระบุการควบคุมอย่างชัดเจน

(2) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(3) บริหาร ควบคุม และจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ฝ่ายบัญชีและการเงิน มีหน้าที่รับผิดชอบ ดังนี้

1. จัดทำแผนการเงิน ให้สอดคล้องกับแผนกลยุทธ์ แผนธุรกิจในภาพรวมของสำนักงาน รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์
2. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์
3. ติดตามและวิเคราะห์ผลการดำเนินงานของสำนักงาน เปรียบเทียบกับแผนการเงิน และอื่น ๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมายและแนวทางการจัดการความเสี่ยง (Mitigation)
4. ร่วมกับส่วนบริหารความเสี่ยง ส่วนแผน งบประมาณ และติดตามประเมินผล ส่วนงานที่เกี่ยวข้องกับการพัฒนาผลิตภัณฑ์ เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนการเงินและงบประมาณรวมของสำนักงาน โดยดำเนินการต่อไปนี้

(1) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับสำนักงาน พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยง และกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือกพร้อมทั้งระบุการควบคุมอย่างชัดเจน

(2) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(3) บริหาร ควบคุม และจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนแผน งบประมาณ และติดตามประเมินผล ฝ่ายกลยุทธ์องค์กร มีหน้าที่รับผิดชอบ ดังนี้

1. จัดทำแผนนโยบายและกลยุทธ์ ให้สอดคล้องกับแผนกลยุทธ์ แผนธุรกิจในภาพรวมของสำนักงาน รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์
2. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์
3. ติดตามและวิเคราะห์ผลการดำเนินงานของสำนักงาน เปรียบเทียบกับแผนนโยบายและกลยุทธ์และอื่น ๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมายและแนวทางการจัดการความเสี่ยง (Mitigation) เพื่อให้การปฏิบัติงานเป็นไปอย่างประสิทธิภาพและเกิดประสิทธิผล กรณีที่มีการเบี่ยงเบนไปจากแผนให้เสนอแนวทางแก้ไขให้ทันท่วงที
4. ร่วมกับส่วนบริหารความเสี่ยง ฝ่ายบัญชีและการเงิน ส่วนงานที่เกี่ยวข้องกับการพัฒนาผลิตภัณฑ์ เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนนโยบายและกลยุทธ์ และงบประมาณรวมของสำนักงาน โดยดำเนินการต่อไปนี้
   (1) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับสำนักงาน พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยง และกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือกพร้อมทั้งระบุการควบคุมอย่างชัดเจน
   (2) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง
   (3) บริหาร ควบคุม และจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนงานที่เกี่ยวข้องกับการพัฒนาผลิตภัณฑ์ มีหน้าที่รับผิดชอบ ดังนี้

1. ศึกษาความเป็นไปได้ตามแผนกลยุทธ์ แผนธุรกิจในภาพรวมของสำนักงาน รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์

2. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงที่กำหนดในกระบวนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์
3. ติดตามและวิเคราะห์ผลการดำเนินงานของสำนักงาน เปรียบเทียบกับแผนพัฒนาธุรกิจและอื่น ๆ พร้อมทั้งอธิบายถึงสาเหตุความแตกต่างจากเป้าหมาย และแนวทางการจัดการความเสี่ยง (Mitigation)
4. ร่วมกับส่วนแผน งบประมาณ และติดตามประเมินผล ฝ่ายบัญชีและการเงิน และส่วนบริหารความเสี่ยงเชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนนโยบายและกลยุทธ์ และงบประมาณรวมของสำนักงาน โดยดำเนินการต่อไปนี้
   (1) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านนโยบายและกลยุทธ์ในระดับสำนักงาน พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยง และกำหนดแนวทางการจัดการที่เหมาะสมโดยพิจารณาต้นทุนและผลประโยชน์ที่จะได้รับของแต่ละทางเลือกพร้อมทั้งระบุการควบคุมอย่างชัดเจน
   (2) ติดตามผลการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์โดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator : KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง
   (3) บริหาร ควบคุม และจัดการความเสี่ยงด้านนโยบายและกลยุทธ์ในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ส่วนบริหารทรัพยากรและกลยุทธ์บุคคล ฝ่ายบริหารกลาง มีหน้าที่รับผิดชอบ ดังนี้

1. จัดองค์กร และกำหนดวิธีการปฏิบัติงานที่เอื้อต่อการปฏิบัติตามแผนกลยุทธ์ โดยจัดให้มีการสอบยันและถ่วงดุลอำนาจ (Check and Balance) อย่างเหมาะสม รวมถึงกำหนดสายการบังคับบัญชาที่ชัดเจนและเปิดเผย เพื่อการสั่งการที่รวดเร็วและมีประสิทธิภาพ
2. จัดอัตรากำลังให้เหมาะสมกับคุณสมบัติและหน้าที่ตำแหน่งงานที่รับผิดชอบ รวมทั้งกำหนดระบบการสรรหา การฝึกอบรม และการกำหนดผลตอบแทนที่เหมาะสม เพื่อสนับสนุนเจ้าหน้าที่ให้ปฏิบัติตามแผนกลยุทธ์เพื่อบรรลุเป้าหมายของสำนักงาน
3. สร้างเสริมให้เกิดการกำกับดูแลกิจการที่ดีภายในสำนักงาน เพื่อให้การปฏิบัติหน้าที่ตามภารกิจของสำนักงานมีความเจริญเติบโตอย่างต่อเนื่องและมั่นคง บริหารงานอย่างมีประสิทธิภาพ โปร่งใส และเป็นธรรมซึ่งจะสร้างความเชื่อมั่นให้กับทุกหน่วยงาน

ฝ่ายตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

ตรวจสอบและสอบทานการควบคุมภายในด้านต่าง ๆ ของสำนักงาน ก่อนนำเสนอคณะกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

ฝ่ายและส่วนงานต่าง ๆ ของสำนักงาน มีหน้าที่รับผิดชอบ ดังนี้

1. กำหนดกลยุทธ์และแผนปฏิบัติการของฝ่าย และส่วนงานต่าง ๆ ให้สอดคล้องกับแผนกลยุทธ์หลักของ สำนักงาน
2. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับฝ่ายและส่วนงานต่าง ๆ
3. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนกลยุทธ์ฝ่าย และส่วนงานต่าง ๆ ให้กับส่วนบริหารความเสี่ยง เพื่อนำไปจัดทำแผนภาพความเสี่ยงด้านนโยบายและกลยุทธ์และภาพความเสี่ยงแบบบูรณาการ ตามลำดับต่อไป
4. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของฝ่ายให้กับส่วนบริหารความเสี่ยงเป็นรายไตรมาส
5. บริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงาน ในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้
6. ดูแล ติดตามการจัดการความเสี่ยง และประเมินผลการจัดการความเสี่ยงเป็นประจำ เพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับ รวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติม เพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้
7. แต่งตั้งผู้ประสานงานด้านความเสี่ยง (Risk Officer) เพื่อประสานงานกับส่วนบริหารความเสี่ยงในการจัดทำ Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของส่วนงานและฝ่าย สื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

4. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

4.1 ความเสี่ยงด้านนโยบายและกลยุทธ์ (Policy and Strategic Risk)

ความเสี่ยงด้านนโยบายและกลยุทธ์ (Policy and Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดนโยบายต่าง ๆ เช่น นโยบายระดับรัฐจนถึงนโยบายในระดับผู้บริหาร แผนกลยุทธ์ แผนดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับสภาพแวดล้อมภายใน และปัจจัยภายนอกทำให้มีโอกาสที่จะไม่ประสบความสำเร็จตามทิศทางที่กำหนดไว้ ซึ่งจะส่งผลกระทบต่อตัวชี้วัดผลการปฏิบัติงานของสำนักงาน

แผนกลยุทธ์ (Strategic Plan) หรือแผนยุทธศาสตร์ หมายถึง แผนที่แสดงทิศทางการดำเนินงานและสะท้อนวิสัยทัศน์หรือเป้าหมายหรือนโยบายของสำนักงาน โดยทั่วไปจะมีระยะเวลา 3 ถึง 5 ปี ซึ่งแผนกลยุทธ์ที่ดี จะต้องมีความชัดเจนสอดคล้องกับเป้าหมาย ยืดหยุ่น และสามารถปรับเปลี่ยนให้สอดคล้องกับสภาวการณ์ที่เปลี่ยนแปลงได้

แผนธุรกิจ (Business Plan) หมายถึง แผนที่กำหนดกรอบการดำเนินงานโดยรวมของสำนักงาน เพื่อ สนับสนุนการปฏิบัติงานให้สำเร็จตามแผนกลยุทธ์ และเป็นแนวทางให้แก่ หน่วยงานต่าง ๆ ในการกำหนดแผนปฏิบัติการ (Action Plan) โดยทั่วไปจะเป็นแผนระยะสั้นไม่เกิน 1 ปี ประกอบด้วย เป้าหมาย ผลดำเนินการ หน่วยงานที่รับผิดชอบ ปริมาณทรัพยากรที่ใช้ กรอบเวลาการดำเนินงาน และเกณฑ์ในการติดตามผลการปฏิบัติงาน ซึ่งควรสอดคล้องกับงบประมาณของสำนักงาน ด้วย

4.2 ที่มาของความเสี่ยงด้านนโยบายและกลยุทธ์ สามารถจำแนกได้ 2 ประเภท ดังนี้

4.2.1 ปัจจัยความเสี่ยงภายนอก หมายถึง ปัจจัยที่สำนักงาน ไม่สามารถควบคุมได้ หรือควบคุมได้ยาก ซึ่งจะส่งผลกระทบหรือเป็นอุปสรรคต่อการจัดทำแผนกลยุทธ์ แผนดำเนินงานของสำนักงาน และการปฏิบัติ เพื่อให้บรรลุเป้าหมายที่วางไว้ของสำนักงาน

(1) การได้รับนโยบายต่าง ๆ จากหน่วยงานภายนอกที่กำกับดูแลสำนักงาน นั้น ทางสำนักงาน จะต้องสามารถสื่อสารสู่เจ้าหน้าที่ได้อย่างถูกต้องตามที่ได้รับนโยบายมา เพื่อที่หน่วยงานต่าง ๆ ของสำนักงาน จักได้นำไปกำหนดในแผนกลยุทธ์และแผนดำเนินงานได้อย่างสอดคล้องตามนโยบายที่ได้รับ

(2) การเปลี่ยนแปลงนโยบายระดับรัฐ อาจทำให้สภาวะการทำงานหยุดชะงัก หรือต้องวางกลยุทธ์และแผนการดำเนินงานใหม่

(3) การเปลี่ยนแปลงพฤติกรรมของกลุ่มลูกค้าเป้าหมาย การเปลี่ยนแปลงของโครงสร้างประชากรและความต้องการของลูกค้า จะมีผลต่อฐานลูกค้าของสำนักงาน ซึ่งสำนักงานต้องมีการกำหนดกลุ่มลูกค้าเป้าหมายที่มีศักยภาพ และวิธีการเสนอบริการที่ดีให้แก่ลูกค้าเหล่านั้น เพื่อป้องกันความเสี่ยงที่จะสูญเสียส่วนแบ่งตลาด

(4) การเลือกใช้เทคโนโลยีเป็นความเสี่ยงที่มีความสำคัญต่อการดำเนินงานของสำนักงานอย่างมาก ดังนั้น สำนักงานต้องมีการจัดการความเสี่ยงจากการเลือกใช้เทคโนโลยีเพื่อตอบสนองต่อนโยบายที่ได้รับ และสนับสนุนต่อแผนกลยุทธ์ แผนดำเนินงานของสำนักงาน

(5) การเกิดภัยพิบัติจากธรรมชาติ เช่น อุทกภัยปี พ.ศ. 2554 ภัยจากการประท้วงจนก่อให้เกิดการจลาจล แต่ระดับความรุนแรงของผลกระทบดังกล่าวขึ้นอยู่กับขอบเขตการ

ดำเนินงานที่เกี่ยวข้องกับเหตุการณ์หรือภัยพิบัติ และความสามารถในการปรับตัวของสำนักงาน

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

4.2.2 ปัจจัยความเสี่ยงภายใน หมายถึง ปัจจัยที่สำนักงาน สามารถควบคุมได้ แต่สามารถส่งผลกระทบหรือเป็นอุปสรรคต่อการดำเนินงานตามแผนกลยุทธ์เพื่อให้บรรลุเป้าหมาย ได้แก่

(1) <u>กระบวนการสื่อสารภายในองค์กร</u> สำนักงานต้องจัดให้มีกระบวนการสื่อสารองค์กรในเรื่องแผนกลยุทธ์ และแผนดำเนินงานขององค์กรสู่เจ้าหน้าที่อย่างทั่วถึงทุกระดับและต่อเนื่อง

(2) <u>โครงสร้างองค์กร</u> การจัดโครงสร้างองค์กร มีความสำคัญต่อการปฏิบัติตามแผนกลยุทธ์และแผนดำเนินงานให้บรรลุเป้าหมายและมีประสิทธิภาพ หากสำนักงานไม่มีการทบทวนการแบ่งแยกหน้าที่ความรับผิดชอบตามนโยบายหรือภารกิจที่ได้รับจากรัฐบาลเป็นรายปี หรือรายเฉพาะกิจจะทำให้เกิดปัญหาในการจัดการเพื่อบรรลุต่อเป้าหมายที่ต้องการ

(3) <u>กระบวนการและวิธีปฏิบัติงาน</u> หากสำนักงานมิได้กำหนดกระบวนการและวิธีปฏิบัติงานที่ชัดเจน หรือกำหนดความรับผิดชอบที่ซ้ำซ้อนกัน อาจส่งผลให้การปฏิบัติตามแผนการดำเนินงานและแผนปฏิบัติการล่าช้าและผิดพลาดได้ง่าย ยากแก่การติดตามและรายงานผลการปฏิบัติงานได้ถูกต้องและทันกาล

(4) <u>ความเพียงพอและคุณภาพของบุคลากร</u> การดำเนินงานตามแผนกลยุทธ์และแผนดำเนินงานในทุกระดับของสำนักงาน จะบรรลุเป้าหมายได้หรือไม่นั้นขึ้นอยู่กับปริมาณและคุณภาพของบุคลากร จำนวนบุคลากรที่เพียงพอจะช่วยรองรับปริมาณงานและธุรกรรมได้ครบถ้วน บุคลากรควรมีความเชี่ยวชาญและได้รับการฝึกอบรมที่จำเป็นเพื่อให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผล

(5) <u>ความเพียงพอของข้อมูล</u> ผู้บริหารของสำนักงาน จะต้องได้รับข้อมูลที่เหมาะสมเพื่อใช้ในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ การได้รับข้อมูลไม่เพียงพอ ไม่เหมาะสม ไม่ถูกต้องและไม่ทันกาลจะเป็นอุปสรรคต่อการเข้าใจสภาวการณ์ และส่งผลต่อการวางแผนกลยุทธ์และแผนดำเนินงานการกำหนดเป้าหมายและการบริหารงานของสำนักงาน

(6) <u>เทคโนโลยี</u> สำนักงานจะต้องมีเทคโนโลยีที่สามารถแข่งขันและตอบสนองความต้องการของลูกค้าได้ โดยเฉพาะธุรกรรมที่ซับซ้อน พร้อมทั้งต้องปรับปรุงระบบเทคโนโลยีสารสนเทศให้สามารถแข่งขันและรองรับปริมาณธุรกรรมใหม่ได้

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การดำเนินงานตามแผนกลยุทธ์ในบางกลยุทธ์ที่สำคัญไม่เป็นไปตามเป้าหมาย เนื่องจากนโยบายภาครัฐที่เปลี่ยนแปลงระหว่างปี	1. ไม่มีคณะทำงานในการพิจารณาการปรับโครงสร้างองค์กร 2. ช่องทางในการรับฟัง และสื่อสารกับบุคลากร เพื่อให้เกิดการยอมรับโครงสร้างของบุคลากรไม่เพียงพอ 3. ขาดการติดตามการเปลี่ยนแปลงนโยบายภาครัฐระหว่างปีอย่างใกล้ชิด	✓	✓
ขาดการบูรณาการกลยุทธ์ในระดับองค์กรและฝ่ายงาน	1. ไม่มีคณะทำงานที่มีหน้าที่รับผิดชอบในการเชื่อมโยงเป้าหมายแต่ละโครงการกับเป้าประสงค์ระดับองค์กร 2. ไม่มีการกำหนดเป้าประสงค์ที่เป็นรูปธรรมสำหรับยุทธศาสตร์ในระดับองค์กร และเป็นที่ยอมรับทั่วทั้งองค์กร 3. ขาดการติดตามการดำเนินงานผลความสำเร็จของเป้าประสงค์ในยุทธศาสตร์หลัก และเชื่อมโยงกับผลความสำเร็จของโครงการ	✓	
ขาดการถ่ายทอดกลยุทธ์ให้พนักงานและผู้เกี่ยวข้องรับทราบและเข้าใจ	1. ไม่มีการกำหนดกระบวนการในการถ่ายทอดแผนยุทธศาสตร์ กลยุทธ์ และแผนปฏิบัติการสู่พนักงานที่เกี่ยวข้อง 2. ไม่มีการกำหนดช่องทางการถ่ายทอดแผนยุทธศาสตร์ กลยุทธ์ และแผนปฏิบัติการที่เพียงพอและเหมาะสม และประเมินประสิทธิผลของแต่ละช่องทาง	✓	

ตัวอย่างปัจจัยเสี่ยงทางด้านนโยบายและกลยุทธ์	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
	3. ไม่มีการกำหนดรูปแบบการถ่ายทอดแผนยุทธศาสตร์จากระดับผู้บริหารลงสู่ระดับล่าง		

5. องค์ประกอบการบริหารความเสี่ยง

5.1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

การวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงทางนโยบายและกลยุทธ์นั้น จากการที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้รับมอบหมายให้ดำเนินการตามภารกิจทั้ง 9 ด้าน ภายใต้วิสัยทัศน์ “นำภาครัฐสู่การเป็นรัฐบาลดิจิทัล” ซึ่งสอดคล้องตามทิศทางและแนวทางการขับเคลื่อนประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand) รวมถึงแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 (พ.ศ. 2566 – 2570) โดยสำนักงานมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงทางนโยบายและกลยุทธ์ เพื่อให้การดำเนินงานในขั้นตอนต่าง ๆ ของการจัดทำแผนธุรกิจและแผนกลยุทธ์มีประสิทธิภาพ รวมทั้งมีประโยชน์สำหรับตัดสินใจในการดำเนินธุรกิจของ สำนักงาน ผู้บริหารและหน่วยงานที่เกี่ยวข้องกับความเสี่ยงด้านนโยบายและกลยุทธ์จะต้องร่วมกันกำหนดและทบทวนกลยุทธ์อย่างสม่ำเสมอ เพื่อใช้กำหนดแผนปฏิบัติการ (Action Plan) ในการพัฒนางานเพื่อป้องกันและลดความเสียหายที่อาจจะเกิดขึ้นรวมถึงช่วยให้สามารถบรรลุเป้าหมายและวัตถุประสงค์ของแผนดำเนินงาน โดยแผนการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ที่จัดทำขึ้นจะต้องมีรายละเอียดของวัตถุประสงค์ ขอบเขตงาน ผู้มีหน้าที่รับผิดชอบ งบประมาณรองรับหรือทรัพยากรที่ต้องการ ผลที่จะได้รับ รวมถึงระยะเวลาการดำเนินงานของแผนที่ชัดเจน เพื่อประโยชน์ในการบริหารและติดตามการดำเนินงานตามแผนการบริหารความเสี่ยงที่กำหนดไว้

ทั้งนี้ การวิเคราะห์สภาพแวดล้อมต้องคำนึงถึงปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อสำนักงาน หรือหน่วยงานที่เกี่ยวข้องกับนโยบายหลัก เนื่องจากการวิเคราะห์ถึงสภาพแวดล้อมทั้งภายในและภายนอก (SWOT Analysis) จะทำให้สำนักงาน ทราบถึงปัจจัยเสี่ยงที่จะส่งผลกระทบต่อความสำเร็จของสำนักงาน ช่วยให้สำนักงานทราบว่าต้องบริหารจัดการอย่างไร เพื่อสร้างข้อได้เปรียบทางการแข่งขันเมื่อต้องเผชิญกับสภาพการแข่งขันที่รุนแรง

5.2 การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านนโยบายและกลยุทธ์ อันมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามแผนกลยุทธ์ แผนปฏิบัติการประจำปี และการปฏิบัติตามกฎหมาย กฎระเบียบต่าง ๆ ที่จะส่งผลต่อการดำเนินงานด้านนโยบายและกลยุทธ์ต่าง ๆ ของหน่วยงานที่เกี่ยวข้อง เช่น สำนักนายกรัฐมนตรี กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เป็นต้น

5.3 การระบุเหตุการณ์ (Event Identification)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร สามารถระบุเหตุการณ์ความเสี่ยงได้เบื้องต้นตามกระบวนการกำหนดยุทธศาสตร์ของสำนักงาน ดังนี้

1. ความเสี่ยงด้านการกำหนดแผนยุทธศาสตร์ หรือแผนการดำเนินงานไม่เหมาะสม สอดคล้องกันของนโยบาย กลยุทธ์ โครงสร้างองค์กร
2. ความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงาน ไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณณา ไม่สามารถติดตามเป้าหมายได้
3. ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์หรือแผนปฏิบัติการประจำปี

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

การระบุความเสี่ยง แนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อความสอดคล้องกันของแผนงานต่าง ๆ ที่จะสนับสนุนยุทธศาสตร์หลักของสำนักงาน รวมทั้งความสอดคล้องหรือข้อจำกัดของทรัพยากรที่เกี่ยวข้องกับการดำเนินยุทธศาสตร์ ทั้งทรัพยากรด้านงบประมาณ ด้านบุคลากร หรือระบบสนับสนุนอื่น ๆ เช่น ระบบสารสนเทศ โครงสร้างองค์กร เป็นต้น เพื่อให้เกิดการใช้ทรัพยากรอย่างคุ้มค่าและลดความซ้ำซ้อน สามารถพิจารณาได้จากความถี่ในการเปลี่ยนแปลง การปรับปรุงแผนปฏิบัติการที่ได้รับอนุมัติจากคณะกรรมการแล้วในระหว่างปี รวมทั้งปัจจัยภายนอกต่าง ๆ เช่น นโยบายหน่วยงานกำกับ นโยบายรัฐบาล ที่มีผลต่อการดำเนินการกำหนดแผนยุทธศาสตร์ รวมทั้งกำหนดกิจกรรมในการดำเนินโครงการหลักของสำนักงาน

ความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงาน ไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณา ไม่สามารถติดตามเป้าหมายได้

การระบุความเสี่ยงด้านการกำหนดเป้าหมายของยุทธศาสตร์ หรือแผนการดำเนินงาน ไม่ชัดเจน หรือกำหนดเป็นเชิงพรรณา ไม่สามารถติดตามเป้าหมายได้ เป็นการระบุปัจจัยเสี่ยง แนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อการปฏิบัติงาน ที่ดำเนินการแล้วไม่สามารถทำให้ภาพรวมสำนักงาน บรรลุเป้าหมายที่แท้จริงได้ตามนโยบายและกลยุทธ์ และแผนงานประจำปี รวมทั้งปัจจัยเสี่ยงของกระบวนการกำหนดหรือการจัดทำเป้าหมายของตัวชี้วัดที่ได้กำหนดไว้ของยุทธศาสตร์ไม่ชัดเจนได้ ซึ่งจะส่งผลต่อการดำเนินกิจกรรมหลักของสำนักงาน

ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์ หรือแผนปฏิบัติการประจำปี

การระบุความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์ หรือแผนปฏิบัติการประจำปี ให้ระบุจากเป้าหมายของสำนักงาน ในการกำหนดเป้าหมาย รวมทั้งกิจกรรมตามแผนยุทธศาสตร์ ที่อาจไม่บรรลุได้ตามกำหนด หรือความเสี่ยงที่อาจเกิดจากความล่าช้าในการดำเนินกิจกรรมตามแผนยุทธศาตร์ และแผนปฏิบัติการประจำปี รวมทั้งปัจจัยที่จะส่งผลกระทบการดำเนินกิจกรรมตามแผนงาน เช่น โครงการพัฒนาระบบเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (Government Information Network : GIN) โครงการพัฒนาระบบคลาวด์ภาครัฐ (Government Cloud : G-Cloud) ระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารของหน่วยงานภาครัฐ (MailGoThai) เป็นต้น

ส่วนบริหารความเสี่ยง ส่วนแผน งบประมาณ และติดตามประเมินผล ฝ่ายบัญชีและการเงิน ส่วนกลยุทธ์ผลิตภัณฑ์ ส่วนบริหารทรัพยากรและกลยุทธ์บุคคล ฝ่ายพัฒนาแพลตฟอร์มดิจิทัลภาครัฐ ฝ่ายพัฒนาแพลตฟอร์มดิจิทัลประชาชนและฝ่ายพัฒนาแพลตฟอร์มดิจิทัลแลกเปลี่ยนข้อมูล ฝ่ายและส่วนงานต่าง ๆ ของสำนักงาน ที่เกี่ยวข้องกับกลยุทธ์ของสำนักงาน จะร่วมกันพิจารณา วิเคราะห์ และกำหนดปัจจัยต่าง ๆ ที่มีผลกระทบต่อความเสี่ยงด้านนโยบายและกลยุทธ์ ในแต่ละช่วงเวลา ทำให้ประเมินได้ว่าในอนาคตสำนักงานจะมีการดำเนินงานตามแผนกลยุทธ์ หรือแผนงานโครงการหลักในช่วงใด อีกทั้งยังมีการร่วมพิจารณาถึงความเสี่ยงที่เกิดจากการดำเนินโครงการหลักของสำนักงาน ที่ไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการ และของ สำนักงาน

5.4 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงจะพิจารณาปัจจัยการประเมินความเสี่ยง 2 ด้าน คือ การประเมินโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) จากการเกิดเหตุการณ์ความเสี่ยงเพื่อทราบระดับความรุนแรงของความเสี่ยง ทั้งนี้ความเสี่ยงด้านนโยบายและกลยุทธ์ สามารถประเมินด้วยเครื่องมือเป้าหมายการดำเนินงาน

ที่กำหนดไว้ รวมทั้งการประเมินจากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือ โอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านนโยบายและกลยุทธ์เหล่านั้นขึ้นเป็นแต่ละเหตุการณ์ เช่น ผลกระทบจากนโยบายรัฐบาล สาเหตุเกิดจากความไม่ชัดเจนของภารกิจที่ทางรัฐบาลมอบหมายลงมา และไม่มีการเตรียมความพร้อมใด ๆ ในการรองรับ เป็นต้น

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ความเสี่ยงด้านการไม่สามารถดำเนินการได้ครบถ้วนหรือไม่บรรลุตามแผนยุทธศาสตร์ หรือแผนปฏิบัติการประจำปี ประสิทธิภาพในการบริหารงบประมาณ

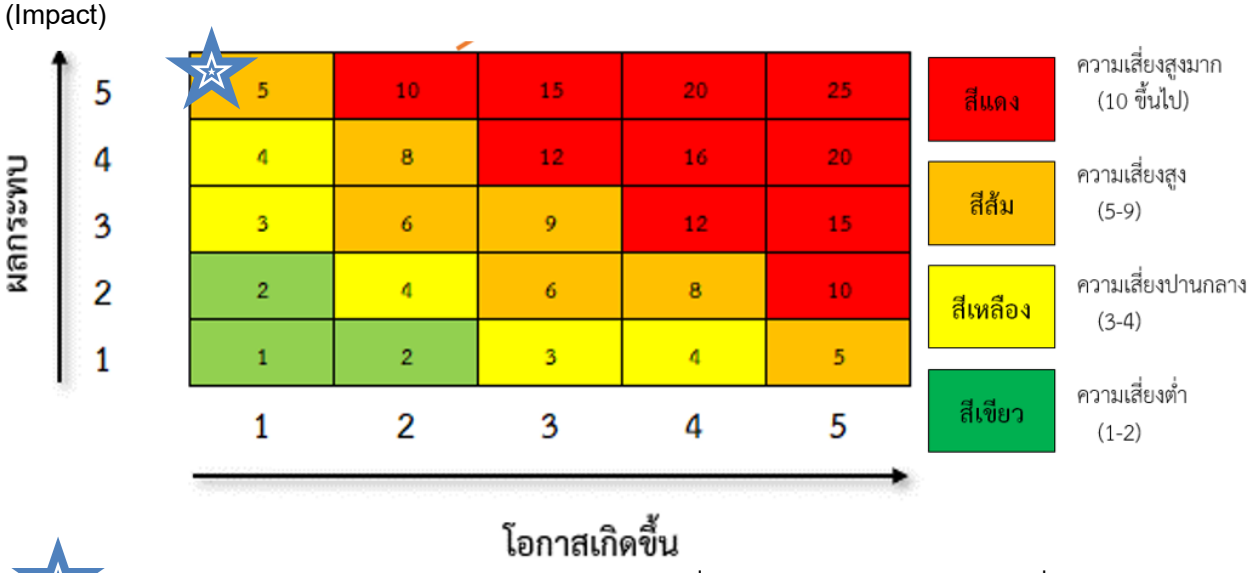
ชื่อปัจจัยเสี่ยง การดำเนินงานตามแผนกลยุทธ์ในบางกลยุทธ์ที่สำคัญไม่เป็นไปตามเป้าหมาย

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
โอกาส	ดำเนินการได้ครบถ้วนในระดับ 2 รวมถึงมีการประเมินผลติดตามแผนงานทั้งแผนงานเดิมและแผนงานที่กระทบจากนโยบายภาครัฐและมีการเสนอแนวทางการแก้ไขต่อฝ่ายบริหารเป็นประจำเพื่อมุ่งสู่การบรรลุเป้าหมายองค์กร	ดำเนินการได้ครบถ้วนในระดับ 3 และมีการจัดสรรทรัพยากรสำหรับการดำเนินงานนโยบายที่เปลี่ยนแปลงไปอย่างเหมาะสม โดยคำนึงถึงข้อจำกัดของทรัพยากรเดิม	มีหน่วยงานรับผิดชอบในเรื่องผลกระทบของนโยบายภาครัฐที่ชัดเจน รวมถึงถ่ายทอดสู่แผนปฏิบัติการและถ่ายทอดให้บุคลากรในองค์กรได้รับทราบ	มีหน่วยงานรับผิดชอบในเรื่องผลกระทบของนโยบายภาครัฐที่ชัดเจน รวมถึงถ่ายทอดสู่แผนปฏิบัติการแต่ยังไม่มีกระบวนการถ่ายทอดให้บุคลากรในองค์กรได้รับทราบ	มีหน่วยงานรับผิดชอบในเรื่องนโยบายภาครัฐที่ชัดเจนแต่ยังไม่มีการถ่ายทอดสู่แผนปฏิบัติการ

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 5	ระดับ 25
ผลกระทบ	ความสำเร็จตามแผนกลยุทธ์มากกว่าหรือ	ความสำเร็จตามแผนกลยุทธ์มากกว่าหรือ	ความสำเร็จตามแผนกลยุทธ์มากกว่าหรือ	ความสำเร็จตามแผนกลยุทธ์มากกว่าหรือ	ความสำเร็จตามแผนกลยุทธ์น้อยกว่าร้อยละ 80

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
	เท่ากับร้อยละ 95 ขึ้นไป	เท่ากับร้อยละ 90 ขึ้นไป	เท่ากับร้อยละ 85 ขึ้นไป	เท่ากับร้อยละ 80 ขึ้นไป	

เมื่อประเมินระดับความเสี่ยงได้แล้ว ขั้นต่อไปคือ การจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญ และจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของสำนักงาน หรือหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดยสำนักงานได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น 4 ระดับ ตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้น ๆ ได้แก่ ระดับสูงมาก ระดับสูง ระดับปานกลาง ระดับต่ำ ตามลำดับ โดยใช้ Risk Map เป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมิน ซึ่ง Risk Map จะแสดงข้อมูลเป็น 2 แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact)



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจากสำนักงานเป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
3-4	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าวที่เหมาะสม เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่สำนักงานยอมรับได้

5.5 การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบ ที่เกิดจากความเสี่ยงนั้น ๆ จะทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าว เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่สำนักงานยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
การดำเนินงานตามแผนกลยุทธ์ในบางกลยุทธ์ที่สำคัญไม่เป็นไปตามเป้าหมาย	1. มีแผนการจัดประชุมเพื่อกำหนด/ทบทวน ยุทธศาสตร์และเป้าหมายร่วมกับผู้บริหารและผู้รับผิดชอบโครงการเป็นประจำทุกปี 2. มีการประชุมหารือกับผู้บริหารในการดำเนินงาน เพื่อรายงานความก้าวหน้า และปัญหาอุปสรรคต่าง ๆ 3. มีการเตรียมความพร้อมด้านบุคลากร ระบบงาน และเครื่องมือต่าง ๆ เพื่อรองรับการให้บริการที่มากขึ้นในแต่ละปี 4. มีการติดตามนโยบายดิจิทัลเพื่อเศรษฐกิจและสังคม (Digital Economy) ว่าส่งผลกระทบกับสำนักงาน อย่างไร โดยทางส่วนกฎหมายจะทำการสอบทานและติดตามนโยบายดังกล่าว เพื่อรายงานให้ผู้บริหารทราบ	การลดความเสี่ยง (Treat)

5.6 กิจกรรมการควบคุม (Control Activities)

ส่วนบริหารความเสี่ยง ส่วนแผน งบประมาณ และติดตามประเมินผล และฝ่ายบัญชีและการเงิน มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านนโยบายและกลยุทธ์ โดยจะควบคุมความเสี่ยงทางด้านสภาพคล่อง ด้านการบริหารเงินลงทุน และอื่น ๆ ให้สอดคล้องกับเพดานความเสี่ยง (Risk Limit) หรือตัวบ่งชี้ความเสี่ยงด้านนโยบายและกลยุทธ์ ที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านนโยบายและกลยุทธ์ของสำนักงานให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการ สพร. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

5.7 สารสนเทศและการสื่อสาร (Information and Communication)

<u>แหล่งที่มาของข้อมูล</u>

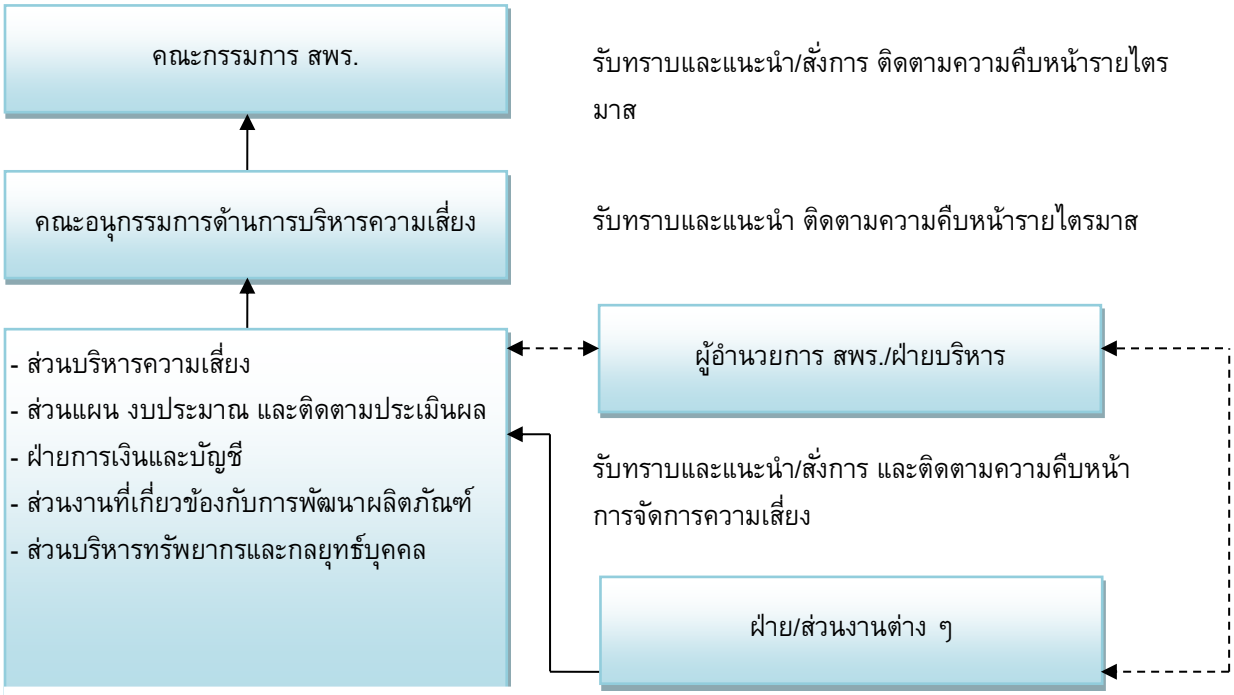
ส่วนบริหารความเสี่ยง ส่วนแผน งบประมาณ และติดตามประเมินผล และฝ่ายบัญชีและการเงิน จัดเก็บข้อมูลซึ่งมีรายละเอียดดังนี้

ข้อมูล	แหล่งที่มา	หมายเหตุ
• **แผนนโยบายและกลยุทธ์ ระยะยาว** (แผนยุทธศาสตร์ 4 ปี) • **แผนนโยบายและกลยุทธ์ประจำปี** • **การปรับปรุงแผนการดำเนินงาน**	• ส่วนแผน งบประมาณ และติดตามประเมินผล • ฝ่ายบัญชีและการเงิน	• พิจารณาจากการจัดทำงบประมาณตามแผนงานทั้งระยะสั้น และระยะยาว • รายละเอียดกิจกรรมตามแผนงานที่กำหนด
• **สถานะการดำเนินงานตามแผนงาน ทั้งระยะสั้นและระยะยาว** • **สถานะการดำเนินงานตามตัวชี้วัด ตามยุทธศาสตร์ของสำนักงาน**	• ส่วนแผน งบประมาณ และติดตามประเมินผล	• พิจารณาจากการรายงานความคืบหน้าการติดตามโครงการตามแผนยุทธศาตร์ • พิจารณาจากการรายงานความคืบหน้าของตัวชี้วัดตามยุทธศาสตร์ • รายงานปัญหาอุปสรรคและแนวทางแก้ไขของการดำเนินโครงการที่สำคัญรวมทั้งตามแผนงาน

5.8 การติดตามและประเมินผล (Monitoring)

ส่วนแผน งบประมาณ และติดตามประเมินผล และฝ่ายบัญชีและการเงิน มีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการ สพร. และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านนโยบายและกลยุทธ์ ที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านนโยบายและกลยุทธ์ ในภาพรวมต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อคณะกรรมการ สพร. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่อง ต่อไป

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติ ส่วนแผน งบประมาณ และติดตามประเมินผล ต้องรายงานให้ผู้บริหาร สพร. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สพร. / ฝ่ายบริหาร	คณะอนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการ สพร.
ปานกลาง หรือเตือน (Warning)	รับทราบ/แนะนำและสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำและสั่งการ

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สพร. / ฝ่ายบริหาร	คณะอนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการ สพร.
สูง หรือรุนแรง (Severe)	รับทราบ/แนะนำ/สั่งการ และ รายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง 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

หน้า

1. บทนำ

เพื่อให้การบริหารความเสี่ยงด้านการปฏิบัติงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) เป็นไปในแนวทางเดียวกันสำนักงาน จึงได้มีการกำหนดนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อบังคับใช้กับทุกหน่วยงานของสำนักงาน โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจและตระหนักถึงหน้าที่ความรับผิดชอบต่อการบริหารความเสี่ยงด้านการปฏิบัติงานอยู่เสมอ นับเป็นการสนับสนุนให้ทุกหน่วยงานของสำนักงาน มีการบริหารความเสี่ยงด้านการปฏิบัติงานอย่างเป็นระบบ และยังเป็นการส่งเสริมให้มีกระบวนการควบคุมภายในที่ดีอีกทางหนึ่งด้วย และเพื่อให้เจ้าหน้าที่ทุกระดับสามารถเข้าใจต่อการบริหารความเสี่ยงด้านการปฏิบัติงานของสำนักงาน จึงได้จัดทำคู่มือบริหารความเสี่ยงด้านการปฏิบัติงาน (คู่มือฯ) ซึ่งถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) โดยจะใช้ประกอบในการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งคู่มือฯ จะกล่าวลงไปในรายละเอียดเพื่อให้หน่วยงานสามารถวางระบบการบริหารความเสี่ยงด้านการปฏิบัติงานภายในหน่วยงานของตนเองได้อย่างมีประสิทธิภาพ มีกระบวนการการป้องกัน การควบคุมความเสี่ยงด้านการปฏิบัติงานให้ความเสี่ยงอยู่ในระดับที่สำนักงานสามารถยอมรับได้ (Risk Appetite) และระดับความเสี่ยงที่ทนได้ (Risk Tolerance) สามารถลดผลกระทบจากเหตุการณ์ความเสียหายที่อาจเกิดขึ้นต่อสำนักงาน และสอดคล้องกับการบริหารความเสี่ยงองค์กร (Enterprise Risk Management)

แนวทางการบริหารความเสี่ยงที่นำมาใช้

สำนักงานกำหนดกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานตามแนวทางการปฏิบัติงานของสำนักงาน และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Treadway Commission (COSO) โดยการบริหารความเสี่ยงด้านการปฏิบัติงานจะอยู่บนพื้นฐานของการควบคุมภายใน ซึ่งเป็นกระบวนการที่เป็นขั้นตอนที่ต่อเนื่องและแทรกอยู่ในการปฏิบัติงานตามปกติของทุกหน่วยงาน ทั้งนี้ เจ้าหน้าที่ในทุกหน่วยงานของสำนักงาน มีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งมีผู้บริหารเป็นผู้รับผิดชอบให้มีระบบการบริหารความเสี่ยงด้านการปฏิบัติงาน ตามที่สำนักงานกำหนด คือ มีการระบุ ประเมิน ติดตาม ควบคุม และรายงานความเสี่ยง

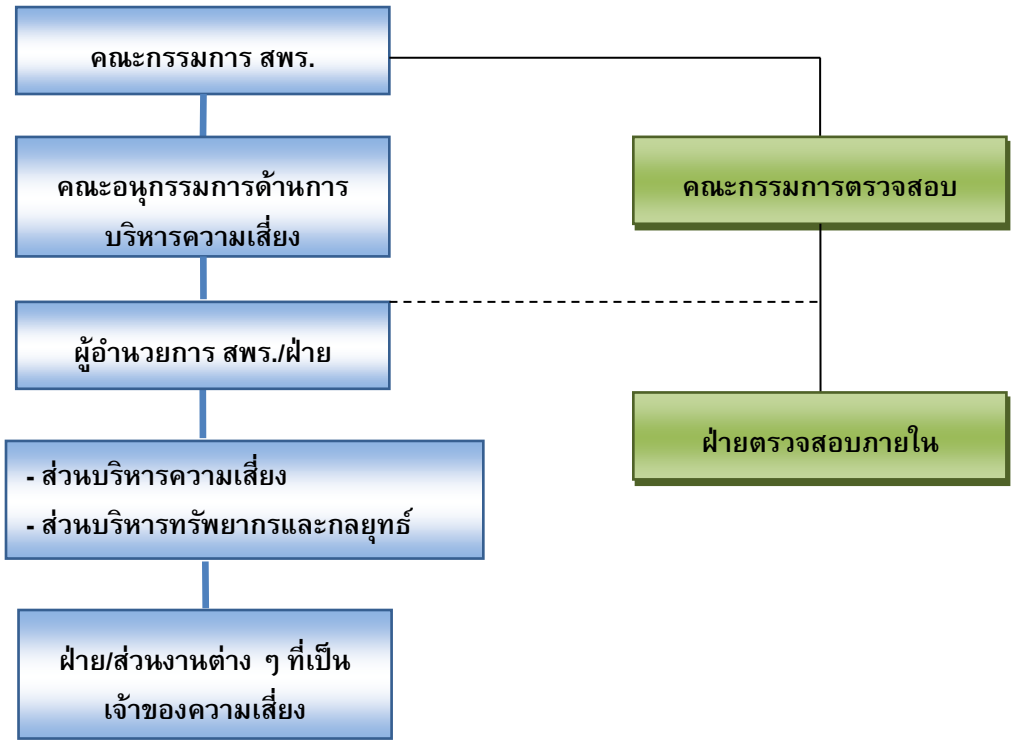
การบริหารความเสี่ยงด้านการปฏิบัติงานควรให้ความมั่นใจอย่างสมเหตุสมผลว่าหน่วยงานจะบรรลุตามเป้าหมายที่ได้กำหนดไว้ กล่าวคือ แม้ว่าจะมีการวางระบบการบริหารความเสี่ยงด้านการปฏิบัติงานไว้ดีเพียงใด ก็ไม่สามารถรับรองได้ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้อย่างสมบูรณ์ เพราะมีข้อจำกัดจากปัจจัยอื่นนอกเหนือการควบคุมของหน่วยงาน เช่น ผลกระทบจากปัจจัยภายนอก เป็นต้น

ขอบเขตของคู่มือบริหารความเสี่ยงด้านการปฏิบัติงาน

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านการปฏิบัติงาน ซึ่งครอบคลุมถึงความเสี่ยงอันเกิดจากการดำเนินงานที่ไม่เป็นไปตามแผนกลยุทธ์ของสำนักงาน รวมทั้งนโยบายที่ได้รับจากสำนักนายกรัฐมนตรี รวมทั้งนโยบายภาครัฐ ตั้งแต่การกำหนดแผนงานที่รองรับนโยบายไม่ครบถ้วน การดำเนินงานไม่ได้ตามเป้าหมายแผนกลยุทธ์ของโครงการหลัก รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นจากปัจจัยภายนอก เช่น การเปลี่ยนแปลงนโยบายภาครัฐ เป็นต้น โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานเพื่อให้หน่วยงานต่าง ๆ ของสำนักงานใช้เป็นแนวทางในการบริหารความเสี่ยงด้านการปฏิบัติงานของตนเอง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

2. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านการปฏิบัติงาน



3. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายกลยุทธ์องค์กร มีหน้าที่รับผิดชอบดังนี้

1. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงาน และนำเสนอต่อคณะกรรมการ สพร. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
2. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานที่กำหนดในกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงาน
3. จัดทำคู่มือบริหารความเสี่ยงด้านการปฏิบัติงานและเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
4. ประสานงานกับส่วนบริหารทรัพยากรและกลยุทธ์บุคคล ส่วนปฏิบัติงานต่าง ๆ เพื่อจัดให้หน่วยงานต่าง ๆ ดำเนินการพิจารณา Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของหน่วยงานต่าง ๆ รวมถึงแนวทางการจัดการความเสี่ยงที่เหมาะสม
5. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทาง ความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านการปฏิบัติงาน
6. ดูแลให้มีการปฏิบัติตามกระบวนการในการออก/ปรับปรุงผลิตภัณฑ์ตามแนวทางที่สำนักงานกำหนดและมีส่วนร่วมพิจารณาให้ความเห็นในการออกผลิตภัณฑ์ในประเด็นที่เกี่ยวข้องกับความเสี่ยง รวมทั้งปรับปรุงหรือแก้ไขข้อบกพร่องที่เกี่ยวกับความเสี่ยงด้านต่าง ๆ ที่เกิดขึ้นภายหลังการออก/ปรับปรุงผลิตภัณฑ์ โดยดำเนินการร่วมกับหน่วยงานเจ้าของผลิตภัณฑ์นั้น ๆ
7. ร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) สำหรับสถานการณ์ที่ไม่ปกติ เพื่อรองรับการเปลี่ยนแปลงสภาพแวดล้อมที่ไม่เป็นไปตามที่คาดไว้

ผู้ประสานงานความเสี่ยง (Risk Internal Control Officer: RICO)

ทุกหน่วยงานต้องกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็น RICO ประจำหน่วยงาน ซึ่งจะดูแลรับผิดชอบในการประสานงานกับส่วนบริหารความเสี่ยงที่จะนำเครื่องมือต่าง ๆ ที่ใช้ในการบริหารความเสี่ยงด้านการปฏิบัติงานไปใช้บริหารความเสี่ยงด้านการปฏิบัติงานภายในหน่วยงานตนเอง และรายงานข้อมูลที่เกี่ยวข้องให้ส่วนบริหารความเสี่ยงตามกำหนดเวลา รวมไปถึงให้ความรู้ที่เกี่ยวกับการบริหารความเสี่ยงด้านการปฏิบัติงานแก่เจ้าหน้าที่ในหน่วยงานของตนเอง ทั้งนี้ เพื่อให้เจ้าหน้าที่ทุกระดับในหน่วยงานตนเองรับทราบ

ถึงความเสี่ยงด้านการปฏิบัติงานโดยรวมและแนวทางแก้ไขที่ได้กำหนดไว้ ดังนั้น RICO จึงควรเป็นบุคคลที่มีความเข้าใจในกระบวนการในการปฏิบัติงานต่าง ๆ ของหน่วยงานตนเองเป็นอย่างดี เพื่อจะได้สามารถระบุและประเมินความเสี่ยงด้านการปฏิบัติงานของหน่วยงานตนเองได้อย่างถูกต้องพร้อมทั้งรายงานข้อมูลที่เกี่ยวกับความเสี่ยงด้านการปฏิบัติงานได้อย่างครบถ้วน ถูกต้อง

ผู้จัดการความเสี่ยง (Risk Manager)

ผู้จัดการความเสี่ยง (Risk Manager) หมายถึง หัวหน้าหน่วยงานนั้น ๆ โดยเป็นบุคคลที่ทำหน้าที่รับผิดชอบในการบริหารจัดการความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานที่อยู่ภายใต้ความรับผิดชอบของตนเองในฐานะเจ้าของความเสี่ยง (Risk Owner) รวมถึงมีหน้าที่ดูแลให้การปฏิบัติงานเป็นไปตามนโยบายและกรอบการบริหารความเสี่ยงด้านการปฏิบัติงานตามที่สำนักงานกำหนด พร้อมทั้งให้ความเห็นชอบต่อข้อมูลที่เกี่ยวกับการบริหารความเสี่ยงด้านการปฏิบัติงานที่ RICO รายงานให้แก่ส่วนบริหารความเสี่ยง

เจ้าหน้าที่ทุกคน (Employees)

มีหน้าที่ในการปฏิบัติตามนโยบายและกรอบการบริหารความเสี่ยงด้านการปฏิบัติงานตามที่สำนักงานกำหนด รวมไปถึงรับผิดชอบในการบริหารความเสี่ยงด้านการปฏิบัติงานภายใต้ขอบเขตความรับผิดชอบของตน โดยมีหน้าที่ทำความเข้าใจหลักการของความเสี่ยงภายใต้กรอบการบริหารความเสี่ยงของสำนักงาน เพื่อให้แน่ใจว่าการบริหารความเสี่ยงด้านการปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพ ส่งผลให้เกิดมูลค่าเพิ่มแก่หน่วยงานและ สอดคล้องกับแผนงาน วัตถุประสงค์ และกลยุทธ์ที่กำหนดไว้

ส่วนบริหารทรัพยากรและกลยุทธ์บุคคล ฝ่ายบริหารกลาง มีหน้าที่รับผิดชอบ ดังนี้

1. จัดองค์กร และกำหนดวิธีการปฏิบัติงานที่เอื้อต่อการปฏิบัติตามแผนกลยุทธ์ โดยจัดให้มีการสอบยันและถ่วงดุลอำนาจ (Check and Balance) อย่างเหมาะสม รวมถึงกำหนดสายการบังคับบัญชาที่ชัดเจนและเปิดเผย เพื่อการสั่งการที่รวดเร็วและมีประสิทธิภาพ
2. จัดอัตรากำลังให้เหมาะสมกับคุณสมบัติและหน้าที่ตำแหน่งงานที่รับผิดชอบ รวมทั้งกำหนดระบบการสรรหา การฝึกอบรม และการกำหนดผลตอบแทนที่เหมาะสม เพื่อสนับสนุนเจ้าหน้าที่ให้ปฏิบัติตามแผนกลยุทธ์เพื่อบรรลุเป้าหมายของสำนักงาน
3. เสริมสร้างให้เกิดการกำกับดูแลกิจการที่ดีภายในสำนักงาน เพื่อให้การปฏิบัติหน้าที่ตามภารกิจของสำนักงาน มีความเจริญเติบโตอย่างต่อเนื่องและมั่นคง บริหารงานอย่างมีประสิทธิภาพ โปร่งใส และเป็นธรรม ซึ่งจะสร้างความเชื่อมั่นให้กับทุกหน่วยงาน

4. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

4.1 ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)

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

ความเสี่ยงด้านการปฏิบัติงาน ยังครอบคลุมถึงเหตุการณ์ความเสียหาย (Loss Incidents) ที่อาจเกิดขึ้นเนื่องจากการดำเนินงานผิดพลาดของหน่วยงาน (Business Unit) ใด ๆ ในสำนักงานและสามารถเกิดขึ้นได้กับการปฏิบัติงานในทุกระดับชั้น นอกจากนี้ ความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานหนึ่ง อาจส่งผลกระทบและก่อให้เกิดความเสียหายแก่หน่วยงานอื่น ๆ ต่อเนื่องกันไปได้ ดังนั้น จึงมีความจำเป็นที่ในแต่ละหน่วยงานของ สำนักงานต้องมีระบบการบริหารความเสี่ยงด้านการปฏิบัติงานที่มีประสิทธิภาพและเหมาะสมกับสภาวะแวดล้อมในการดำเนินธุรกิจ เพื่อให้มั่นใจว่าสำนักงานสามารถจัดการความเสี่ยงด้านการปฏิบัติงานได้ และลดความสูญเสียให้อยู่ในระดับต่ำที่สุด

4.2 ที่มาของความเสี่ยงด้านการปฏิบัติงาน สามารถจำแนกได้ 7 ประเภท ดังนี้

4.2.1. ความเสี่ยงจากการทุจริตจากภายใน (Internal fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายในสำนักงาน เพื่อให้ผลประโยชน์ที่เกิดขึ้นจากการทุจริตดังกล่าวตกแก่พวกพ้องของตนเอง

4.2.2. ความเสี่ยงจากการทุจริตจากภายนอก (External fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายนอก แต่ก่อให้เกิดความเสียหายโดยตรงต่อสำนักงาน

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

4.2.4. ความเสี่ยงจากลูกค้า ผลิตภัณฑ์ และวิธีปฏิบัติในการดำเนินธุรกิจ (Clients, Products and Business practices) เป็นความเสี่ยงที่เกิดขึ้นจากวิธีปฏิบัติในการดำเนินธุรกิจ กระบวนการออกแบบพัฒนาผลิตภัณฑ์ และการเข้าถึงข้อมูลลูกค้าที่ไม่เหมาะสม ไม่เป็นไปตามกฎหมาย ระเบียบและข้อบังคับที่

ทางการกำหนด เช่น การทำธุรกรรมที่ละเมิดกฎหมาย และการที่สำนักงานนำข้อมูลความลับของลูกค้าไปหาผลประโยชน์ เป็นต้น

4.2.5. ความเสี่ยงด้านความปลอดภัยของทรัพย์สิน (Damage to physical assets) เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ทรัพย์สินของสำนักงาน อันเนื่องมาจากภัยต่าง ๆ ที่เกิดขึ้น เช่น อุทกภัย วาตภัย อัคคีภัย การก่อการร้าย ความไม่สงบทางการเมือง การก่อวินาศภัย เป็นต้น

4.2.6. ความเสี่ยงจากการขัดข้องหรือการหยุดชะงักของระบบงานและระบบคอมพิวเตอร์ (Business disruption and System failures) เป็นความเสี่ยงที่เกิดขึ้นจากระบบงานที่ผิดปกติ หรือการหยุดทำงานของระบบงานด้านต่าง ๆ เช่น ความไม่สอดคล้องกันหรือความแตกต่างของระบบงาน ความบกพร่องของระบบงานคอมพิวเตอร์หรือระบบเครือข่าย รวมถึงการใช้เครื่องมือและเทคโนโลยีที่ไม่เหมาะสม ล้าสมัย และไม่มีประสิทธิภาพ เป็นต้น

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

ประเภทความเสี่ยงด้านการปฏิบัติงาน (Risk Event Type)

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

ตัวอย่างปัจจัยเสี่ยงด้านการปฏิบัติงาน

ตัวอย่างปัจจัยเสี่ยงด้านการปฏิบัติงาน	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
กระบวนการประเมินผลการปฏิบัติงานยังล่าช้า	1. วิธีการประเมิน รวมทั้งแบบฟอร์มการประเมิน และวิธีการประมวลผลมีความซับซ้อน 2. ขาดการสื่อสารระบบประเมินผลการปฏิบัติงานให้พนักงานรับทราบ	✓	
การแก้ไขปัญหาของผู้ให้บริการภายนอก (Provider) ล่าช้าและไม่มีความเสถียร	1. ไม่มีการสรุปประเด็นปัญหา และกำหนดระยะเวลาในการแก้ไขที่ชัดเจน 2. ไม่มีการกำหนดมาตรการเร่งรัดการติดตามในการแก้ไขปัญหา 3. ไม่มีการติดตามและรายงานผลการแก้ไขปัญหาให้**สำนักงาน**ทราบ 4. มีการเปลี่ยนแปลงเจ้าหน้าที่ของผู้ให้บริการ ซึ่งส่งผลกระทบต่อการดำเนินการ		✓
ระบบสารสนเทศไม่สามารถเชื่อมข้อมูลระหว่างส่วนงานที่จำเป็นต้องใช้ข้อมูลร่วมกัน	1. ไม่มีหน่วยงานในการวิเคราะห์ระบบงานที่จำเป็นต้องเชื่อมโยงข้อมูล 2. ไม่มีการประเมินระบบงานที่สำคัญที่จำเป็นต้องเชื่อมโยง 3. ไม่มีการกำหนดความต้องของข้อมูล หรือระบบงานที่ต้องการใช้งานร่วมกัน	✓	

5. องค์ประกอบการบริหารความเสี่ยง

5.1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

การวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงด้านการปฏิบัติงานนั้น จากการที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้รับมอบหมายให้ดำเนินการตามภารกิจทั้ง 9 ด้าน ภายใต้วิสัยทัศน์ “นำภาครัฐสู่การเป็นรัฐบาลดิจิทัล” ซึ่งสอดคล้องตามทิศทางและแนวทางการขับเคลื่อนประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand) รวมถึงแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 (พ.ศ. 2566 – 2570) โดยสำนักงานมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงด้านการปฏิบัติงานเพื่อให้มีกระบวนการในการบริหารความเสี่ยงด้านการปฏิบัติงานให้เป็นไปตามหลักมาตรฐานสากลและเป็นมาตรฐานเดียวกันทั่วทั้งสำนักงาน เช่นเดียวกับกระบวนการบริหารความเสี่ยงด้านอื่น ๆ โดยจะครอบคลุมการปฏิบัติงานในทุกระดับชั้นของแต่ละหน่วยงานในสำนักงาน เพื่อช่วยให้การดำเนินงานเกิดผลดีและปฏิบัติงานได้ตามกฎระเบียบที่เกี่ยวข้อง โดยแผนการบริหารความเสี่ยงด้านการปฏิบัติงานที่จัดทำขึ้นจะต้องมีรายละเอียดของวัตถุประสงค์ ขอบเขตงาน ผู้มีหน้าที่รับผิดชอบ งบประมาณรองรับ หรือทรัพยากรที่ต้องการ ผลที่จะได้รับ รวมถึงระยะเวลา การดำเนินงานของแผนที่ชัดเจน เพื่อประโยชน์ในการบริหารและติดตามการดำเนินงานตามแผนการบริหารความเสี่ยงที่กำหนดไว้

ทั้งนี้ การวิเคราะห์สภาพแวดล้อมต้องคำนึงถึงระบบงานที่รองรับการปฏิบัติงานในทุกขั้นตอนของสำนักงาน ได้แก่ กระบวนการ เทคโนโลยี สารสนเทศ อุปกรณ์ บุคลากร ความเพียงพอของข้อมูล ซึ่งส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินงานที่มีผลกระทบต่อสำนักงาน

5.2 การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านการปฏิบัติงานอันมีผลมาจากความผิดพลาดหรือการปฏิบัติที่ไม่เป็นไปตามกระบวนการหรือขั้นตอนการปฏิบัติงาน รวมทั้งการปฏิบัติตามกฎหมาย กฎระเบียบต่าง ๆ ที่จะส่งผลต่อการดำเนินงานด้านการปฏิบัติงานต่าง ๆ ของหน่วยงานที่เกี่ยวข้อง เช่น สำนักนายกรัฐมนตรี กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กพร. เป็นต้น

5.3 การระบุเหตุการณ์ (Event Identification)

การระบุเหตุการณ์ความเสี่ยง จะเริ่มด้วยการแจกแจงกระบวนการปฏิบัติงาน (Work flow) เพื่อให้ทราบขั้นตอนงานที่มีอยู่และจะทำให้บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยหน่วยงานต้องมีการระบุจุด/พื้นที่ ที่มีความเสี่ยง (Risk Area) และสาเหตุหรือปัจจัยของความเสี่ยง (Risk Factor) ในแต่ละผลิตภัณฑ์/บริการ หรือในแต่ละระบบงานก่อนที่จะมีกิจกรรมการควบคุม (Control Activities) เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่ (Inherent Risk) ผ่านระบบการควบคุมภายในและการประเมินการควบคุมความเสี่ยงด้วยตนเอง (Risk and Control Self Assessment หรือ RCSA) โดยการระบุความเสี่ยงของหน่วยงานนั้น ควรดำเนินการในทุกระดับตั้งแต่ระดับปฏิบัติงานขึ้นไปจนถึงระดับบริหาร และครอบคลุมในทุกกิจกรรมของหน่วยงานทั้งนี้ หน่วยงานควรมีการทบทวนการระบุความเสี่ยงด้านการปฏิบัติงานที่มีอยู่อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงของปัจจัยความเสี่ยงต่าง ๆ ที่ส่งผลกระทบต่อกระบวนการในการปฏิบัติงาน เช่น ระบบหรือขั้นตอนที่ในการปฏิบัติงานเปลี่ยนไป มีการเปลี่ยนแปลงโครงสร้างองค์กร การเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ การออกผลิตภัณฑ์ใหม่ ๆ การเปลี่ยนแปลงทางกฎหมาย และกฎระเบียบข้อบังคับต่าง ๆ เป็นต้น ทั้งนี้ ในการระบุความเสี่ยงเบื้องต้น หน่วยงานสามารถระบุความเสี่ยงได้จากแผนผังกระบวนการทำงานหรือขั้นตอนการปฏิบัติงาน (Working Process/Work Flow) หรือข้อมูลเหตุการณ์ความเสียหายที่เคยเกิดขึ้นกับหน่วยงาน (Loss Incidents)

<u>ความเสี่ยงด้านกระบวนการทำงานหรือขั้นตอนในการปฏิบัติงาน</u>

ในการระบุความเสี่ยงนั้นหน่วยงานเจ้าของความเสี่ยง (Risk Owner) จะต้องทำความเข้าใจเกี่ยวกับกระบวนการทำงานหรือขั้นตอนการปฏิบัติงานของตนเอง เพื่อสามารถระบุจุดที่อาจเกิดความเสี่ยง (Risk Area) ซึ่งวิธีที่นิยมในการระบุจุดความเสี่ยงนั้น จะสร้างแผนผังกระบวนการทำงานหรือขั้นตอนการปฏิบัติงาน ซึ่งมีการระบุถึงปัจจัยความเสี่ยง เอกสาร ระบบงาน และผู้รับผิดชอบที่เกี่ยวข้องในแต่ละกระบวนการทำงานอย่างชัดเจน และการจัดทำแผนผังกระบวนการทำงานและสัญลักษณ์ที่ใช้ของแต่ละหน่วยงาน ควรกำหนดใช้สัญลักษณ์แทนในแต่ละกระบวนการทำงานที่เป็นมาตรฐานเดียวกันทั้งสำนักงาน

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

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

ส่วนบริหารความเสี่ยง และหน่วยงานต่าง ๆ ของสำนักงาน ที่เกี่ยวข้องกับกระบวนการดำเนินงานที่สำคัญจะร่วมกันพิจารณา วิเคราะห์ และกำหนดปัจจัยต่าง ๆ ที่มีผลกระทบต่อความเสี่ยงด้านการปฏิบัติงานในแต่ละกระบวนการ หรือกระบวนการ/โครงสร้างองค์กร/เทคโนโลยี ที่มีการเปลี่ยนแปลงอย่างเป็นนัยสำคัญ

5.4 การประเมินความเสี่ยง (Risk Assessment)

เมื่อหน่วยงานได้มีการระบุจุดที่อาจก่อให้เกิดความเสี่ยง (Risk Area) และสาเหตุ/ปัจจัยที่ก่อให้เกิดความเสี่ยง (Risk Factor) ในแต่ละกระบวนการทำงานแล้ว หน่วยงานต้องมีการประเมินความเสี่ยงด้านการปฏิบัติงานในแต่ละจุดที่มีความเสี่ยงในแต่ละขั้นตอนการปฏิบัติงาน ซึ่งต้องอาศัยดุลยพินิจและประสบการณ์ของผู้ปฏิบัติงานในหน่วยงาน รวมถึงข้อมูลความเสี่ยงที่เคยเกิดขึ้นในอดีตเป็นสำคัญ โดยจะพิจารณาจาก 2 ปัจจัย คือ

- โอกาสที่จะเกิดความเสี่ยง (Likelihood) โดยพิจารณาจากความถี่ของเหตุการณ์ที่เกิดขึ้นในอดีตและประมาณโอกาสที่จะเกิดขึ้นในอนาคต

- ระดับของผลกระทบ (Impact) ที่เกิดจากความเสี่ยงนั้น ๆ พิจารณาจากความรุนแรงของเหตุการณ์ในอดีตและประมาณความรุนแรงของเหตุการณ์ที่อาจเกิดขึ้นในอนาคตเพื่อหน่วยงานจะได้ทราบถึงระดับความเสี่ยงที่มีอยู่ (Inherent Risk) และยังเป็นข้อมูลสำหรับการจัดลำดับความสำคัญในการดำเนินการปรับปรุง ควบคุม และลดความเสี่ยงต่อไป

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

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ชื่อปัจจัยเสี่ยง กระบวนการประเมินผลการปฏิบัติงานยังล่าช้า

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
โอกาส	มีการพัฒนาระบบประเมินผลการปฏิบัติงาน และ	มีการพัฒนาระบบประเมินผลการปฏิบัติงาน และ	มีการพัฒนาระบบประเมินผลการปฏิบัติงาน และ	มีการพัฒนาระบบประเมินผลการปฏิบัติงานและมีการสื่อสาร	อยู่ระหว่างการพัฒนาระบบประเมินผลการปฏิบัติงาน

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
	สามารถใช้ประเมินผลบุคลากรได้ครบทุกระดับ	สามารถใช้ประเมินผลบุคลากรได้ระดับบริหารชั้นต้นขึ้นไป	สามารถใช้ประเมินผลบุคลากรได้เฉพาะผู้บริหารระดับสูง (ระดับฝ่ายขึ้นไป)	ให้กับพนักงานเข้าใจในหลักเกณฑ์แนวทางของระบบการประเมินผลที่จะนำมาใช้อย่างทั่วทั้งองค์กร	เพื่อให้สามารถใช้ประเมินผลได้อย่างมีประสิทธิภาพ
ผลกระทบ	ความสำเร็จตามเป้าประสงค์ปี 2565 ในแต่ละยุทธศาสตร์ดีกว่าเป้าหมายทุกยุทธศาสตร์	ความสำเร็จตามเป้าประสงค์ปี 2565 ในแต่ละยุทธศาสตร์ดีกว่าเป้าหมายบางยุทธศาสตร์	ความสำเร็จตามเป้าประสงค์ปี 2565 ในแต่ละยุทธศาสตร์เป็นไปตามเป้าหมายทุกยุทธศาสตร์	ความสำเร็จตามเป้าประสงค์ปี 2565 ในแต่ละยุทธศาสตร์เป็นไปตามเป้าหมายบางยุทธศาสตร์	ความสำเร็จตามเป้าประสงค์ปี 2565 ในแต่ละยุทธศาสตร์ต่ำกว่าเป้าหมายทุกยุทธศาสตร์

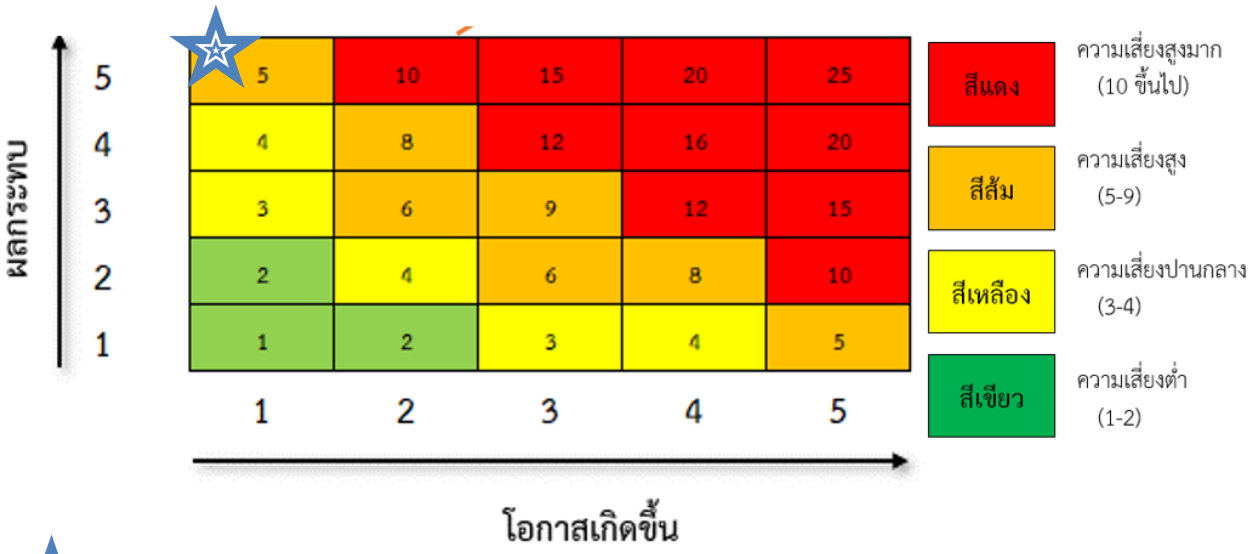
ชื่อปัจจัยเสี่ยง การแก้ไขปัญหาของผู้ให้บริการภายนอก (Provider) ล่าช้าและไม่มีความเสถียร

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
โอกาส	มีการติดตามการแก้ไขปัญหาเป็นรายสัปดาห์และผู้ให้บริการภายนอก (Provider) สามารถแก้ไขปัญหาจนไม่เกิดความล่าช้าและมีความเสถียรและมีการรายงานให้ผู้บริหารรับทราบ	มีการติดตามการแก้ไขปัญหาเป็นรายเดือนและผู้ให้บริการภายนอก (Provider) สามารถแก้ไขปัญหาจนไม่เกิดความล่าช้าและมีความเสถียรแต่ยังไม่มีการรายงานให้ผู้บริหารรับทราบ	มีการติดตามการแก้ไขปัญหาเป็นรายเดือน โดยผู้ให้บริการภายนอก (Provider) สามารถแก้ไขปัญหาความล่าช้าและไม่มีความเสถียร ได้เพียงบางครั้ง	มีการติดตามการแก้ไขปัญหาเป็นรายเดือน โดยผู้ให้บริการภายนอก (Provider) ไม่สามารถแก้ไขปัญหาความล่าช้าและไม่มีความเสถียร	ไม่สามารถติดตามการแก้ไขปัญหากับผู้ให้บริการภายนอก (Provider) ที่ความล่าช้าและไม่มีความเสถียร

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 5	ระดับ 5
ผลกระทบ	ความพึงพอใจของผู้ใช้บริการสูงกว่าปีที่ผ่านมาร้อยละ 5 ขึ้นไป	ความพึงพอใจของผู้ใช้บริการสูงกว่าปีที่ผ่านมาร้อยละ 1-5	ความพึงพอใจของผู้ใช้บริการสูงขึ้นหรือต่ำลงเทียบกับปีที่ผ่านมาไม่เกินร้อยละ 1	ความพึงพอใจของผู้ใช้บริการต่ำกว่าปีที่ผ่านมาร้อยละ 1-5	ความพึงพอใจของผู้ใช้บริการต่ำกว่าปีที่ผ่านมาร้อยละ 5 ขึ้นไป

เมื่อประเมินระดับความเสี่ยงได้แล้ว ขั้นต่อไปคือ การจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญ และจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของสำนักงาน หรือ

หน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดยสำนักงานได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น 4 ระดับ ตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้น ๆ ได้แก่ ระดับสูงมาก ระดับสูง ระดับปานกลาง ระดับต่ำ ตามลำดับ โดยใช้ Risk Map เป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมิน ซึ่ง Risk Map จะแสดงข้อมูลเป็น 2 แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact)



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจากสำนักงานเป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
3-4	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าวที่เหมาะสม เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลง โดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่สำนักงานยอมรับได้

5.5 การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบ ที่เกิดจากความเสี่ยงนั้น ๆ จะทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าว เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่สำนักงานยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
กระบวนการประเมินผลการปฏิบัติงานยังล่าช้า	1. มีการจัดทำแบบฟอร์มและนำมาประเมินผลการปฏิบัติงานของเจ้าหน้าที่ โดยมีการประเมินผลเจ้าหน้าที่ 2 ครั้ง/ปี 2. มีการสื่อสารทำความเข้าใจให้เจ้าหน้าที่ทราบเกี่ยวกับการกรอกรายละเอียดในแบบประเมินผลการปฏิบัติงาน	การลดความเสี่ยง (Treat)

5.6 กิจกรรมการควบคุม (Control Activities)

ระบบการควบคุมภายในที่มีประสิทธิภาพนับเป็นกลไกพื้นฐานสำคัญในการควบคุมและป้องกันความเสียหายที่อาจเกิดขึ้นแก่หน่วยงาน ดังนั้น เมื่อหน่วยงานได้ทำการระบุและประเมินความเสี่ยงด้านการปฏิบัติงานแล้วควรดำเนินการจัดอันดับของความเสี่ยงตามลำดับความสำคัญหรือตามความรุนแรงของผลกระทบของความเสี่ยงนั้น ๆ เพื่อหน่วยงานสามารถวางระบบการควบคุมความเสี่ยงในแต่ละประเภท ซึ่งวัตถุประสงค์หลักของระบบควบคุม คือ การควบคุมความเสี่ยงด้านการปฏิบัติงานให้อยู่ในระดับที่หน่วยงานและสำนักงาน สามารถยอมรับได้ และเพื่อให้มั่นใจว่าการดำเนินงานเป็นไปตามวัตถุประสงค์ที่หน่วยงานหรือสำนักงานได้วางไว้ รวมถึงต้องมีการติดตามและรายงานต่อคณะกรรมการ สพร. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

อย่างไรก็ตาม การพัฒนาระบบการควบคุมความเสี่ยงด้านการปฏิบัติงานที่เหมาะสมของหน่วยงานนั้นหน่วยงานควรพิจารณาถึงปัจจัยต่าง ๆ เหล่านี้ด้วย

• ความมีประสิทธิภาพของระบบการควบคุมความเสี่ยง จะต้องสามารถลดความเสี่ยงด้านการปฏิบัติงานได้อย่างชัดเจนและมีความเกี่ยวข้องโดยตรงกับสาเหตุหลักของความเสี่ยง

• ผลกระทบต่อประสิทธิภาพของการดำเนินงาน โดยระบบการควบคุมความเสี่ยงที่เหมาะสมนั้นควรสร้างผลกระทบที่น้อยที่สุดต่อระยะเวลาที่ใช้ในการปฏิบัติงาน ต้นทุน/ค่าใช้จ่าย บุคลากร และคุณภาพของงาน

• ความยากง่ายในการนำไปปฏิบัติ โดยควรมีต้นทุนของการนำไปปฏิบัติต่ำ และสามารถนำไปปฏิบัติได้ในเวลาที่รวดเร็ว

5.7 สารสนเทศและการสื่อสาร (Information and Communication)

แหล่งที่มาของข้อมูล

ส่วนบริหารความเสี่ยง เป็นหน่วยงานกลางในตามติดตามเพื่อจัดเก็บข้อมูลตามปัจจัยเสี่ยงด้านการปฏิบัติงาน ซึ่งมีรายละเอียดดังนี้

• **โครงสร้างองค์กรที่มีการเปลี่ยนแปลง** • **ระบบหรือขั้นตอนที่ใช้ในการปฏิบัติงาน**	• ส่วนบริหารทรัพยากรและกลยุทธ์บุคคล	• พิจารณาจากการจัดทำโครงสร้างองค์กรฉบับปรับปรุง • รายละเอียดระบบหรือขั้นตอนการปฏิบัติงานที่สำคัญโดยเฉพาะโครงการหลัก
• **การเปลี่ยนแปลงทางกฎหมาย และกฎระเบียบข้อบังคับ ต่าง ๆ**	• ส่วนกฎหมาย	• พิจารณาจากการรายงานการเปลี่ยนแปลงทางกฎหมายและกฎระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับสำนักงาน

5.8 การติดตามและประเมินผล (Monitoring)

ส่วนงานที่เกี่ยวข้องและเป็นหน่วยงานเจ้าของความเสี่ยงมีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการ สพร. และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านการปฏิบัติงานที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านการปฏิบัติงานในภาพรวมต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อคณะกรรมการ สพร. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่อง ต่อไป

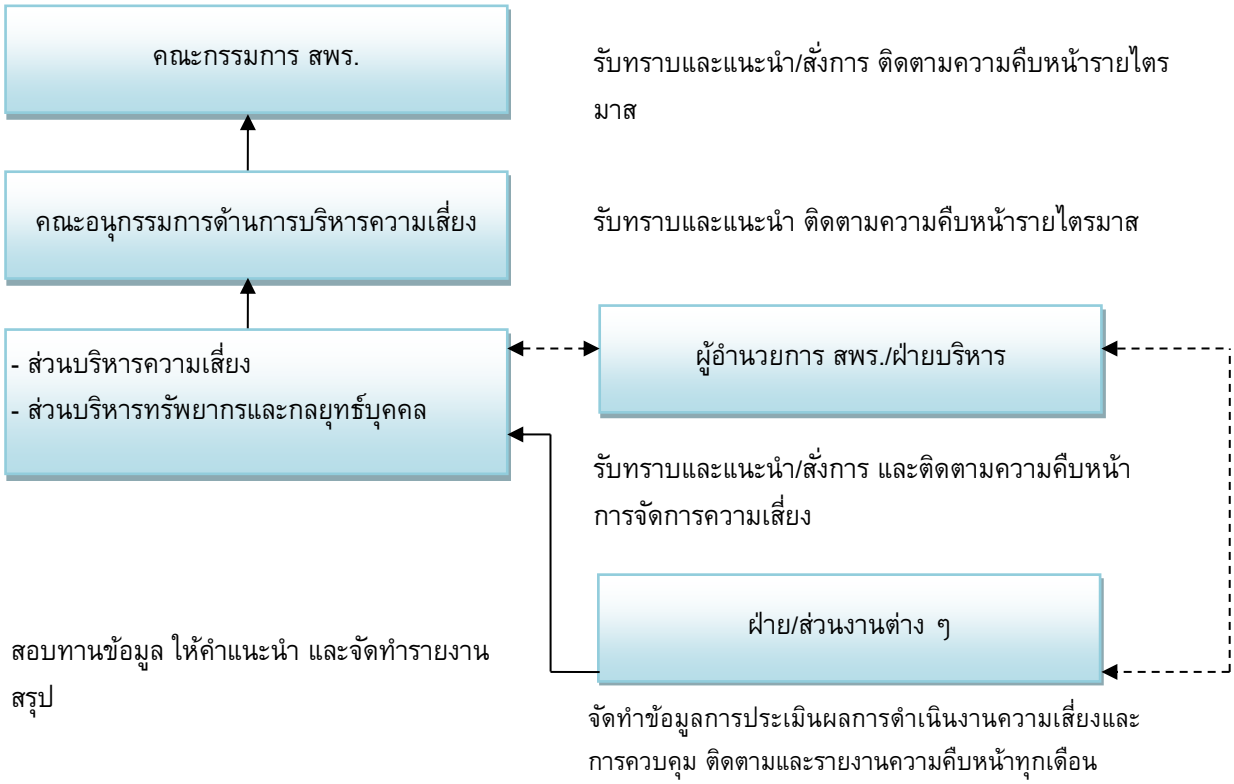
ทั้งนี้ หน่วยงานต้องรายงานเหตุการณ์ความเสียหายที่เกิดจากความเสี่ยงด้านการปฏิบัติงานที่เกิดขึ้นกับหน่วยงานทันทีหรือภายในวันทำการถัดไป และในกรณีที่ไม่มีเหตุการณ์ความเสียหาย หน่วยงานก็ต้องรายงานให้ส่วนบริหารความเสี่ยงทราบด้วย เพื่อให้มั่นใจว่าส่วนบริหารความเสี่ยงได้รับข้อมูลที่ถูกต้องและครบถ้วน โดยข้อมูลทั้งหมดนั้นส่วนบริหารความเสี่ยงจะรวบรวมสรุปผล พร้อมวิเคราะห์จุดที่เกิดความเสี่ยง (Risk Area) เพื่อหาแนวทางในการป้องกันแก้ไข และนำเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง หรือคณะอนุกรรมการที่เกี่ยวข้องต่อไป ทั้งนี้ หากมีความเสียหาย~~ง~~ ที่มีนัยสำคัญเกิดขึ้นกับ

หน่วยงาน หน่วยงานจะต้องมีการจัดทำ Action Plan เพื่อลดหรือป้องกันไม่ให้ความเสียหายดังกล่าวเกิดขึ้นกับสำนักงานได้อีกในอนาคต

สรุปความสัมพันธ์ของการบริหารความเสี่ยงด้านการปฏิบัติงาน
กับเครื่องมือบริหารความเสี่ยงด้านการปฏิบัติงาน

เครื่องมือบริหารความเสี่ยง	กระบวนการบริหารความเสี่ยงที่เกี่ยวข้อง	การนำเครื่องมือบริหารความเสี่ยงมาใช้ในหน่วยงาน
Risk Control Self Assessment: RCSA	- การระบุ - การประเมิน - การควบคุม - การรายงาน - การติดตาม	กำหนดให้หน่วยงานจัดทำปีละ 1 ครั้ง เป็นอย่างน้อย
Operational Loss Data	- การระบุ - การรายงาน - การติดตาม	กำหนดให้หน่วยงานรายงานเป็นรายเดือน โดยต้องรายงานทั้งในกรณีที่มีความเสียหาย และไม่มีความเสียหาย
Key Risk Indicator: KRIs	- การรายงาน - การติดตาม	ความถี่ในการติดตามและรายงาน KRIs มีทั้งรายสัปดาห์ รายเดือน รายไตรมาส รายครึ่งปี และรายปี ขึ้นอยู่กับ KRIs แต่ละตัว

สรุปขั้นตอนการรายงานความเสี่ยง



หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติ ส่วนงานที่เกี่ยวข้องต้องรายงานให้ผู้บริหาร สพร. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สพร. / ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการ สพร.
ปานกลาง หรือเตือน (Warning)	รับทราบ/แนะนำ และสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำ และสั่งการ
สูง หรือรุนแรง (Severe)	รับทราบ/แนะนำ/ สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยง โดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ
สูงมาก หรือรุนแรงมาก (High Severe)	รับทราบ/แนะนำ/ สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยง โดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ

คู่มือบริหารความเสี่ยงด้านการเงิน

(Financial Risk Management Manual)

สารบัญ

หน้า

1. บทนำ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) มีภารกิจดำเนินงานภายใต้ พ.ร.ฎ. จัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ซึ่งต้องดำเนินงานและบริหารความเสี่ยงภายใต้ความเปลี่ยนแปลงและปรับตัวต่อผลกระทบจากสิ่งแวดล้อมภายนอก ทั้งที่มาจากปัจจัยภายในประเทศและภายนอกประเทศ ทำให้ สำนักงานต้องตระหนักและระมัดระวังในการบริหารจัดการความเสี่ยง โดยเฉพาะความเสี่ยงด้านการเงินที่มีความผันผวนและมีความอ่อนไหวต่อการเปลี่ยนแปลงจากสภาพแวดล้อมทั้งภายในและภายนอก

สำนักงานเป็นหน่วยงานของรัฐที่ได้รับการจัดสรรงบประมาณเพื่อใช้ดำเนินการตามภารกิจ อีกทั้งยังสามารถจัดหารายได้เองบางส่วนจากการให้บริการด้านระบบเทคโนโลยีสารสนเทศต่าง ๆ ที่สอดคล้องตามวัตถุประสงค์ใน พ.ร.ฎ. จัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ดังนั้น คู่มือบริหารความเสี่ยงด้านการเงินของสำนักงาน นี้ จึงมุ่งเน้นถึงการสร้างความตระหนักให้เกิดแก่ทุกคนที่เกี่ยวข้องในสำนักงาน ในการที่จะช่วยสอดส่องดูแล ระมัดระวัง เพื่อลดความเสี่ยง หรือบรรเทาผลกระทบจากความเสี่ยงด้านการเงิน อันเกิดจากความเสี่ยงด้านงบประมาณที่ส่งผลให้เกิดความไม่สอดคล้องกับแผนที่กำหนด เช่น การไม่ได้รับการจัดสรรงบประมาณตามแผนงานประจำปี และการบริหารการใช้จ่ายงบประมาณที่ไม่มีประสิทธิภาพ เป็นต้น อีกทั้งความเสี่ยงด้านการเงินยังครอบคลุมถึงการดำเนินการที่ไม่เป็นไปตามแผนรายได้ประจำปี เช่น รายได้ที่ไม่เป็นไปตามแผน การบริหารลูกหนี้การค้าที่ไม่มีประสิทธิภาพ การจัดเก็บค่าบริการที่ไม่เป็นตามแผนการจัดหารายได้ เป็นต้น ความเสี่ยงที่เกิดขึ้นดังกล่าวข้างต้นเป็นความเสี่ยงด้านการเงินที่ส่งผลต่อกระแสเงินสดรับเข้าเพื่อใช้จ่ายในการดำเนินการตามภารกิจ และอาจจะส่งผลต่อเนื่องทำให้เกิดความเสี่ยงทางด้านสภาพคล่องในการดำเนินการของสำนักงานทำให้ไม่สามารถชำระหนี้สิน และภาระผูกพันต่าง ๆ ได้ ท้ายที่สุดอาจจะส่งผลต่อภาพลักษณ์ขององค์กรและทำให้องค์กรไม่สามารถดำเนินการได้ครบถ้วนสมบูรณ์ตามวัตถุประสงค์และภารกิจที่กำหนดไว้

สำนักงานต้องส่งเสริมให้ทุกคนตระหนักถึงความสำคัญและมีส่วนร่วมในการบริหารความเสี่ยงด้านการเงิน (Financial Risk Management) โดยคณะกรรมการ สพร. จะให้คำแนะนำและติดตามการรายงานการบริหารความเสี่ยง ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อวางแนวทางแก้ไขปัญหาที่เกิดจากปัจจัยเสี่ยงต่าง ๆ นอกจากนี้ยังกำหนดให้มีการดูแลและทบทวนการบริหารความเสี่ยงด้านการเงินอย่างต่อเนื่อง เพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่สำนักงานยอมรับได้

สำนักงานได้กำหนดกระบวนการบริหารความเสี่ยงด้านการเงินเพื่อให้หน่วยงานต่าง ๆ ของสำนักงานใช้เป็นแนวทางในการจัดทำแผนกลยุทธ์และแผนธุรกิจที่สอดคล้องกับกลยุทธ์หลักของสำนักงาน โดยการระบุความเสี่ยงที่อาจเกิดขึ้น แล้วทำการประเมินถึงโอกาสที่จะเกิดความเสี่ยงขึ้นรวมทั้งผลกระทบที่

จะได้รับ พร้อมทั้งจัดทำแนวทางหรือมาตรการควบคุมที่เหมาะสมเพื่อจัดการกับความเสี่ยงนั้น โดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่สำนักงานกำหนด

คู่มือบริหารความเสี่ยงด้านการเงินฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) โดยจะกล่าวถึงวัตถุประสงค์ ขอบเขต โครงสร้างและบทบาทหน้าที่ของผู้รับผิดชอบกระบวนการบริหารความเสี่ยงด้านการเงิน และรายละเอียดของกระบวนการบริหารความเสี่ยงด้านการเงินเพื่อเป็นแนวทางในการปฏิบัติงานของสำนักงานและเพื่อให้หน่วยงานต่าง ๆ ของสำนักงานใช้เป็นแนวทางในการบริหารความเสี่ยงด้านการเงินของตนเองตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

แนวทางการบริหารความเสี่ยงที่นำมาใช้

สำนักงานกำหนดกระบวนการบริหารความเสี่ยงด้านการเงินตามแนวทางการปฏิบัติงานของสำนักงาน และภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Treadway Commission (COSO)

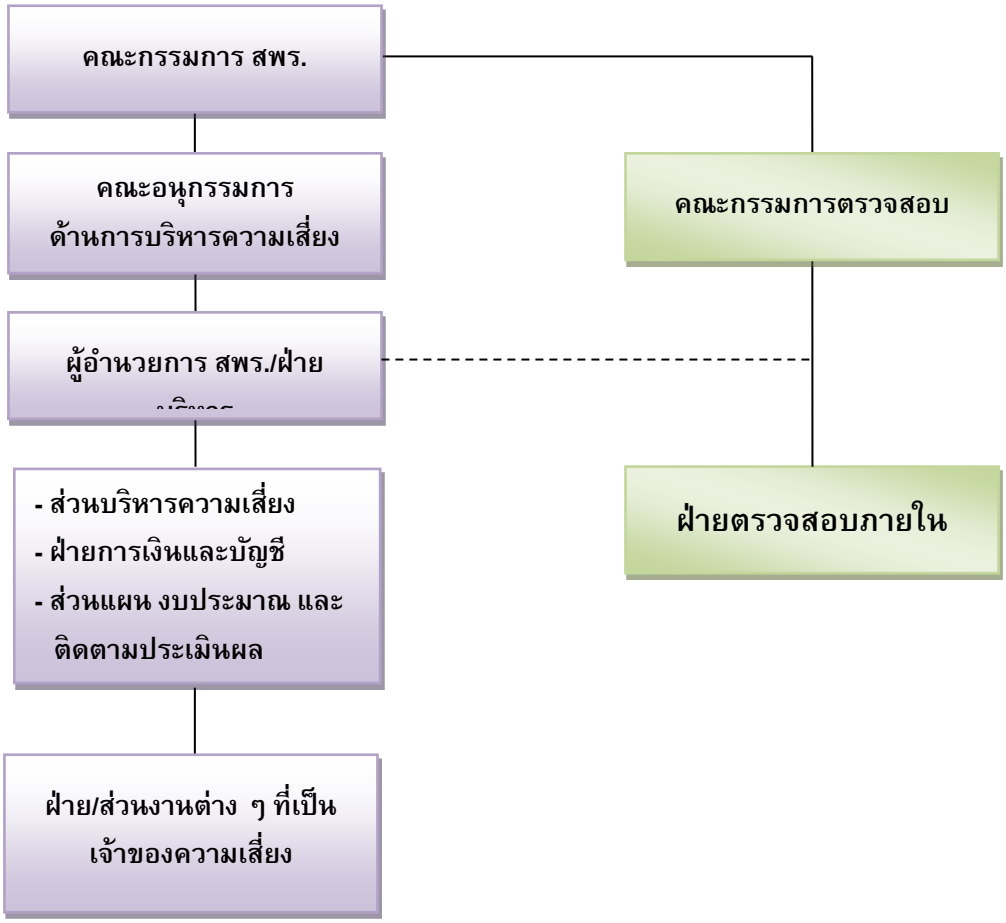
ขอบเขตของคู่มือบริหารความเสี่ยงด้านการเงิน

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านการเงิน ซึ่งครอบคลุมถึงความเสี่ยงอันเกิดจากการปฏิบัติที่ไม่เป็นไปตามแผนงบประมาณประจำปี ตั้งแต่การวางแผนงบประมาณ การของบประมาณ การได้รับอนุมัติงบประมาณจากรัฐบาล การเบิกจ่ายงบประมาณ รวมถึงความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้จ่ายงบประมาณที่ไม่มีประสิทธิภาพการปฏิบัติที่ไม่สอดคล้องกับกฎหมาย หรือกฎระเบียบที่เกี่ยวข้องทั้งภายในและภายนอกที่กำหนดไว้

อีกทั้งยังครอบคลุมถึง ความเสี่ยงที่เกิดจากความผันผวนของอัตราแลกเปลี่ยน ความเสี่ยงที่ทำให้สำนักงานไม่สามารถชำระหนี้และภาระผูกพันต่าง ๆ เมื่อถึงกำหนดชำระ การไม่สามารถจัดหาเงินทุนได้เพียงพอเพื่อใช้จ่ายตามภารกิจในการดำเนินการประจำปีหรือเมื่อเกิดภาวะวิกฤติ ฉุกเฉิน ความเสี่ยงที่ทำให้สำนักงานไม่สามารถรับชำระหนี้จากการให้บริการลูกค้าอันส่งผลต่อสภาพคล่องเนื่องจากกระแสเงินสดรับเข้าไม่เป็นไปตามแผน รวมทั้งความเสี่ยงอันเกิดจากการบริหารจัดการเงินทุนที่ไม่มีประสิทธิภาพ ส่งผลให้สำนักงาน เสียผลประโยชน์ต่าง ๆ ที่ควรจะได้รับ ทั้งที่เป็นไปหรือไม่เป็นไปตามแผน

2. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านการเงิน



3. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายกลยุทธ์องค์กร มีหน้าที่รับผิดชอบดังนี้

1. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการเงิน และนำเสนอต่อคณะกรรมการ สพร. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
2. จัดทำและทบทวนเพดาน หรือตัวบ่งชี้ (Trigger) ความเสี่ยงด้านการเงิน ที่เกี่ยวกับเพดานของสภาพคล่อง และหลักเกณฑ์การขออนุมัติกรณีมีการเกินเพดานหรือตัวบ่งชี้ของสภาพคล่องที่กำหนดไว้ เพื่อนำเสนอขออนุมัติต่อคณะกรรมการ สพร.
3. รายงานความเสี่ยงด้านการเงิน ที่แสดงถึงการปฏิบัติหรือไม่ปฏิบัติตามแนวทาง สตง. หรือ ก.พ.ร. ที่กำหนดไว้ หรือความเสี่ยงที่เกิดจากการดำเนินการทางการเงิน ไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการ และของสำนักงาน และความเสี่ยงด้านการเงินเปรียบเทียบกับเพดานหรือตัวบ่งชี้ที่ได้รับอนุมัติต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง
4. จัดทำตัวแบบ Risk Model และ Stress Testing และรายงานสรุปผลเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง
5. ประเมิน ติดตาม และควบคุมความเสี่ยงด้านการเงิน ที่เกี่ยวกับสภาพคล่อง เพื่อให้มีการปฏิบัติตามนโยบายที่กำหนด
6. จัดทำคู่มือบริหารความเสี่ยงด้านการเงิน และเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
7. ประสานงานกับฝ่ายบัญชีและการเงิน และส่วนแผน งบประมาณ และติดตามประเมินผล เพื่อจัดให้หน่วยงานต่าง ๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านการเงินที่กำหนด
8. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทางความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านการเงิน
9. ร่วมกับฝ่ายบัญชีและการเงิน และส่วนแผน งบประมาณ และติดตามประเมินผล เชื่อมโยงการบริหารความเสี่ยงเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนการเงินและงบประมาณรวมของสำนักงาน โดยดำเนินการต่อไปนี้

(1) ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านการเงินในระดับสำนักงาน พร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ที่ได้ระบุไว้ เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสม

(2) ติดตามผลการบริหารความเสี่ยงด้านการเงินโดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง

(3) บริหาร ควบคุม และจัดการความเสี่ยงด้านการเงินในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

(4) จัดทำแผนฉุกเฉินด้านการเงิน รวมถึงทบทวนแผนปีละ 1 ครั้ง หรือตามความเหมาะสม

ฝ่ายบัญชีและการเงิน มีหน้าที่รับผิดชอบ ดังนี้

1. จัดทำแผนการเงิน ให้สอดคล้องกับแผนกลยุทธ์ แผนธุรกิจในภาพรวมของสำนักงาน รวมทั้งปรับปรุงแผนการดำเนินงานให้สอดคล้องกับสถานการณ์ รวมถึงทบทวนแผนปีละ 1 ครั้ง หรือตามความเหมาะสม
2. รับผิดชอบในการบริหารสภาพคล่อง การบริหารโครงสร้างเงินทุน การบริหารอัตราแลกเปลี่ยนต่าง ๆ ที่เกี่ยวข้อง และรายงานสถานะการเงินด้านต่าง ๆ ของสำนักงาน ต่อคณะกรรมการ สพร.
3. รับผิดชอบในการดูแลและจัดทำแผนการลงทุนด้านการเงิน ปฏิบัติตามนโยบายการบริหารเงินลงทุนเพื่อให้เกิดผลตอบแทนและประโยชน์สูงสุดแก่องค์กร และรายงานการลงทุนด้านการเงินต่อคณะอนุกรรมการบริหารการลงทุน เพื่อรายงานคณะกรรมการ สพร. ต่อไป
4. จัดทำรายงานและจัดหาข้อมูลที่เพียงพอให้แก่ส่วนบริหารความเสี่ยง เพื่อประโยชน์ในการประเมินและควบคุมความเสี่ยงด้านการเงินของสำนักงาน
5. ร่วมกับส่วนบริหารความเสี่ยง เสนอแนะวิธีการลดหรือปิดความเสี่ยงด้านการเงิน ให้อยู่ในระดับที่เหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ และสอดคล้องกับการปฏิบัติงานด้านการเงินและการงบประมาณที่มีอยู่ หรือที่จะได้รับต่อไป
6. รวบรวมข้อมูล วิเคราะห์พฤติกรรมที่เกิดขึ้นจริงในอดีต (Behavioral Maturity) เพื่อจัดทำรายงานพร้อมวิเคราะห์สถานะสภาพคล่องของสำนักงาน จัดทำข้อเสนอแนะ และนำเสนอต่อคณะกรรมการ สพร.
7. ร่วมกับส่วนบริหารความเสี่ยง จัดทำแผนฉุกเฉินด้านการเงิน รวมถึงทบทวนแผนปีละ 1 ครั้ง หรือตามเหมาะสม

ส่วนแผน งบประมาณ และติดตามประเมินผล ฝ่ายกลยุทธ์องค์กร มีหน้าที่รับผิดชอบ ดังนี้

1. ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับการงบประมาณที่กำหนดไว้ในกระบวนการบริหารความเสี่ยงด้านการเงิน
2. ร่วมกับฝ่ายบัญชีและการเงิน และส่วนบริหารความเสี่ยง เชื่อมโยงการบริหารความเสี่ยงด้านการเงินที่เกี่ยวข้องกับการงบประมาณเข้ากับแผนกลยุทธ์ แผนธุรกิจ แผนการเงินและแผนงบประมาณรวมของ สำนักงาน
3. ระบุปัจจัยเสี่ยง (Risk Factors) ของความเสี่ยงด้านการเงินที่เกี่ยวกับการงบประมาณในระดับสำนักงานพร้อมทั้งประเมินระดับความรุนแรงของปัจจัยเสี่ยงโดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ที่ได้ระบุไว้เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงและกำหนดแนวทางการจัดการที่เหมาะสม
4. ติดตามผลการบริหารความเสี่ยงด้านการเงินที่เกี่ยวข้องกับการงบประมาณโดยกำหนดดัชนีชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) สำหรับใช้ในการติดตามความเสี่ยงและทบทวนระดับความเสี่ยงนั้น ๆ อย่างสม่ำเสมอตามระยะเวลาที่กำหนด เพื่อป้องกันและลดความเสียหายที่จะเกิดจากผลกระทบจากปัจจัยเสี่ยง
5. บริหาร ควบคุม และจัดการความเสี่ยงด้านการเงินที่เกี่ยวกับการงบประมาณในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้

ฝ่ายตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

ตรวจสอบและสอบทานการควบคุมภายในด้านต่าง ๆ ของสำนักงานก่อนนำเสนอคณะกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

ฝ่ายและส่วนงานต่าง ๆ ของสำนักงานมีหน้าที่รับผิดชอบ ดังนี้

1. กำหนดกลยุทธ์และแผนปฏิบัติการของฝ่ายและส่วนงานต่าง ๆ ให้สอดคล้องกับแผนการเงินและการงบประมาณของสำนักงาน
2. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับฝ่ายและส่วนงานต่าง ๆ
3. พิจารณาและประเมิน Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนการเงินและแผนงบประมาณของฝ่ายและส่วนงานต่าง ๆ ให้กับส่วนบริหารความเสี่ยงเพื่อนำไปจัดทำความเสี่ยงด้านการเงินและภาพความเสี่ยงแบบบูรณาการ ตามลำดับต่อไป
4. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของฝ่ายให้กับส่วนบริหารความเสี่ยงเป็นรายเดือนหรือรายไตรมาสตามความเหมาะสม

5. บริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงาน ในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้
6. ดูแล ติดตามการจัดการความเสี่ยง และประเมินผลการจัดการความเสี่ยงเป็นประจำ เพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับ รวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติม เพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้
7. แต่งตั้งผู้ประสานงานด้านความเสี่ยง (Risk Officer) เพื่อประสานงานกับส่วนบริหารความเสี่ยงในการจัดทำ Risk Factor, Risk Appetite และ Risk Tolerance จากแผนกลยุทธ์ของฝ่ายและส่วนงาน
8. สื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

4. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

4.1 ความเสี่ยงด้านการเงิน (Financial Risk)

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

หากพิจารณาความเสี่ยงด้านการเงินที่เกี่ยวข้องกับสำนักงานแล้ว อาจแยกเป็นประเภทหลัก ๆ ของความเสี่ยงด้านการเงิน ได้ดังนี้

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

โดยรายงานทางการเงินที่มีส่วนสนับสนุนในการวิเคราะห์ความเสี่ยงทางด้านการเงิน ได้แก่

งบดุล (Balance Sheet) หมายถึง งบแสดงฐานะของสำนักงาน ณ วันสิ้นรอบระยะเวลาบัญชี (วันสิ้นงวดบัญชี) โดยจัดทำขึ้นทุก ๆ รอบระยะเวลาที่กำหนดไว้ เช่น 1 เดือน 3 เดือน 6 เดือน หรือ 1 ปี โดยในส่วนของงบดุลนั้นจะแสดงความสัมพันธ์ของทรัพย์สิน หนี้สินและส่วนของทุน

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

งบกระแสเงินสด (Cash Flow Statement) หมายถึง งบที่แสดงการเปลี่ยนแปลงเงินสดของกิจการในช่วงเวลาใดเวลาหนึ่ง เช่น รอบปีบัญชี โดยจะแสดงการได้มาและใช้ไปของเงินสดและรายการเทียบเท่าเงินสดของ 3 กิจกรรมหลักคือ กิจกรรมดำเนินงาน กิจกรรมลงทุน และ กิจกรรมจัดหาเงิน ช่วยให้ผู้ใช้สามารถประเมินสภาพคล่องของกิจการ โดยเฉพาะความสามารถในการชำระหนี้

อัตราส่วนทางการเงิน (Financial Ratio) หมายถึง การนำตัวเลขที่อยู่ในงบการเงินมาหาอัตราส่วน เพื่อใช้ในการวิเคราะห์เปรียบเทียบ โดยผลลัพธ์ที่ได้อาจแสดงอยู่ในรูปร้อยละ สัดส่วน ระยะเวลา

จำนวนรอบ หรือ จำนวนครั้ง ซึ่งจะช่วยให้ผู้วิเคราะห์ประเมินผลการดำเนินงาน แนวโน้ม และความเสี่ยงของกิจการได้ดียิ่งขึ้น

4.2 ที่มาของความเสี่ยงด้านการเงิน สามารถจำแนกเป็นปัจจัยเสี่ยงได้ 2 ประเภท ดังนี้

4.2.1 ปัจจัยความเสี่ยงภายนอก ได้แก่

(1) ความเสี่ยงจากความไม่ตระหนักถึงความสำคัญของภารกิจของสำนักงาน หรือการที่งบประมาณของประเทศมีจำกัด ทำให้สำนักงาน ได้รับจัดสรรงบประมาณไม่สอดคล้องกับความจำเป็น และแผนงานที่กำหนดไว้

(2) ความเสี่ยงจากการเปลี่ยนแปลงกฎระเบียบ กฎหมาย หรือกฎเกณฑ์ด้านการเงินต่าง ๆ ของรัฐบาล ที่มีผลกระทบต่อการปฏิบัติงานด้านการเงินและงบประมาณของสำนักงาน

(3) ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของสิ่งแวดล้อมภายนอกต่าง ๆ ทั้งภายในประเทศและภายนอกประเทศ ที่ทำให้เกิดความผันผวนของค่าเงิน อัตราแลกเปลี่ยน อัตราดอกเบี้ย ฯลฯ ที่มีผลกระทบต่อการบริหารด้านการเงินของสำนักงาน

4.2.2 ปัจจัยความเสี่ยงภายใน ได้แก่

(1) การเปลี่ยนแปลง และความไม่ชัดเจนของนโยบายและกลยุทธ์ระดับองค์กร ซึ่งส่งผลต่อกลยุทธ์ในระดับปฏิบัติการและมีผลกระทบทั้งทางตรงและทางอ้อมต่อแผนการปฏิบัติงานด้านการเงิน และงบประมาณ

(2) การเปลี่ยนแปลงโครงสร้างองค์กร อาจทำให้มีผลกระทบต่อค่าใช้จ่ายทางการเงินและการใช้จ่ายเงินงบประมาณของสำนักงาน

(3) การปฏิบัติและไม่ปฏิบัติตามนโยบายด้านการเงิน การงบประมาณและการลงทุนต่าง ๆ ที่กำหนดไว้ และการที่ข้อมูลไม่เป็นปัจจุบัน (Up to date) ส่งผลให้การบริหารจัดการด้านการเงินของสำนักงาน ไม่มีประสิทธิภาพ เช่น การกำหนดโครงสร้างของเงินทุนที่ไม่สอดคล้องตามหลักการบริหารทางการเงินที่ทำให้ต้นทุนทางการเงินต่ำ หรือการสร้างผลตอบแทนทางการเงินเพื่อให้เกิดประโยชน์สูงสุด โดยไม่ส่งผลต่อสภาพคล่องทางการเงินของสำนักงาน

ตัวอย่างปัจจัยเสี่ยงทางด้านการเงิน

ตัวอย่างปัจจัยเสี่ยงทางด้านการเงิน	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การเบิกจ่ายงบประมาณไม่เป็นไปตามเป้าหมาย	1. ไม่มีการเร่งรัดให้มีการดำเนินโครงการให้เป็นไปตามแผนงานที่กำหนด 2. ไม่มีการเร่งรัดให้มีการดำเนินการตามแผนจัดซื้อ จัดจ้าง 3. ไม่มีการติดตาม และรายงานผลการเบิกจ่ายเงินงบประมาณต่อคณะกรรมการเป็นประจำ 4. การได้รับงบประมาณไม่เป็นไปตามระยะเวลาที่กำหนด	✓	

5. องค์ประกอบการบริหารความเสี่ยง

5.1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร เพื่อให้สะท้อนความเสี่ยงทางการเงินนั้น จากการที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้รับมอบหมายให้ดำเนินการตามภารกิจทั้ง 9 ด้าน ภายใต้วิสัยทัศน์ “นำภาครัฐสู่การเป็นรัฐบาลดิจิทัล” ซึ่งสอดคล้องตามทิศทางและแนวทางการขับเคลื่อนประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand) รวมถึงแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 (พ.ศ. 2566 – 2570) โดยสำนักงานมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงทางการเงิน จึงมุ่งเน้นไปที่การบริหารงบประมาณให้มีประสิทธิภาพ รวมถึงการวางแผนทางการเงินให้เหมาะสมกับการกำหนดกลยุทธ์ในแต่ละปี

อย่างไรก็ตาม มีบางส่วนงานของสำนักงานที่มีหน้าที่สร้างรายได้นอกเหนือจากรายได้ตามงบประมาณ ดังนั้นความเสี่ยงทางการเงินในอีกมุมมองหนึ่งคือ รายได้นอกงบประมาณดังกล่าวไม่เป็นไปตามเป้าหมายที่กำหนด

5.2 การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

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

5.3 การระบุเหตุการณ์ (Event Identification)

จากการวิเคราะห์สภาพแวดล้อมภายในองค์กร สามารถระบุเหตุการณ์ความเสี่ยงได้เป็น 3 ประเภทหลัก ดังนี้

1. ความเสี่ยงด้านประสิทธิภาพในการบริหารงบประมาณ
2. ความเสี่ยงด้านการเงินและการวางแผนทางการเงิน
3. ความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย

<u>ความเสี่ยงด้านประสิทธิภาพในการบริหารงบประมาณ</u>

การระบุความเสี่ยง แนวโน้มหรือปัจจัยที่อาจจะส่งผลต่อการปฏิบัติที่ไม่เป็นไปตามแผนดำเนินงานด้านการเงินและงบประมาณประจำปี สามารถพิจารณาได้จากความถี่ในการเปลี่ยนแปลง การปรับปรุงแผนงบประมาณที่ได้รับอนุมัติจากคณะกรรมการ สพร. แล้วในระหว่างปี สัดส่วนประสิทธิภาพการเบิกจ่าย การผูกพันงบประมาณต่อแผนงบประมาณรวมทั้งปี และปัจจัยต่าง ๆ ที่มีผลต่อการไม่ได้รับการจัดสรรงบประมาณจากภาครัฐตามแผนที่วางไว้

ความเสี่ยงด้านการเงินและการวางแผนทางการเงิน

การระบุความเสี่ยงด้านการบริหารสภาพคล่อง ให้ระบุประเมินจากความสามารถในการจ่ายชำระหนี้และภาระผูกพันต่าง ๆ ความสามารถในการบริหารงบประมาณ และการบริหารลูกหนี้การค้า และโอกาสเสี่ยงที่จะเกิดหนี้สูญจากการเรียกเก็บเงินจากลูกหนี้การค้าไม่ได้ วิเคราะห์ถึงความเพียงพอของการดำรงเงินสดขั้นต่ำเพื่อใช้ในการหมุนเวียนในสำนักงานทั้งในภาวะปกติและภาวะเกิดเหตุการณ์ไม่ปกติ รวมถึงปัจจัยความเสี่ยงที่อาจส่งผลกระทบต่อกระแสเงินสดในช่วงระยะเวลาต่าง ๆ เพื่อให้สำนักงานมีการบริหารความเสี่ยงด้านการเงินที่เหมาะสม
มีสภาพคล่องเพียงพอสามารถจ่ายหนี้สินและภาระผูกพันเมื่อถึงกำหนดชำระได้

การระบุความเสี่ยงที่เกิดจากการบริหารโครงสร้างของเงินทุนและการบริหารเงินลงทุน ควรวิเคราะห์และระบุปัจจัยเสี่ยงที่ส่งผลกระทบต่อแหล่งที่มาและใช้ไปของเงินทุน การระบุและประเมินสัดส่วนโครงสร้างเงินทุนที่เหมาะสม การจัดทำประมาณการงบการเงิน และงบกระแสเงินสด เพื่อวิเคราะห์ประเมินสถานะการเงิน สถานะเงินสดส่วนเกินจากการใช้หมุนเวียนในสำนักงานตามรอบระยะเวลาบัญชีนั้น ๆ และการวิเคราะห์เพื่อระบุปัจจัยต่าง ๆ ที่ส่งผลให้การบริหารการลงทุนไม่เป็นไปตามนโยบายและแผนการบริหารการลงทุนทั้งในระยะสั้นและระยะยาว

ความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย

การระบุความเสี่ยงด้านรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย ให้ระบุประเมินจากเป้าหมายของสำนักงานในการสร้างรายได้นอกงบประมาณ รวมถึงแผนการตลาดที่จะรองรับในการกำหนดกลยุทธ์ในการหาหน่วยงานภาครัฐที่เป็นกลุ่มเป้าหมาย รวมถึงวิเคราะห์ถึงความต้องการของลูกค้าที่เหมาะสม พร้อมกับกำหนดทรัพยากรของสำนักงานที่ต้องการในการสนับสนุนถึงการบรรลุเป้าหมายดังกล่าว

ส่วนบริหารความเสี่ยง ส่วนแผน งบประมาณ และติดตามประเมินผล และฝ่ายบัญชีและการเงิน จะร่วมกันพิจารณา วิเคราะห์ และกำหนดปัจจัยต่าง ๆ ที่มีผลกระทบต่อความเสี่ยงด้านการเงินในแต่ละช่วงเวลา ทำให้ประเมินได้ว่าในอนาคตสำนักงานจะมีสภาพคล่องส่วนเกินหรือขาดในช่วงใด ซึ่งสะท้อนถึงความเสี่ยงด้านการเงินของสำนักงาน

อย่างไรก็ตามส่วนบริหารความเสี่ยง ส่วนแผน งบประมาณ และติดตามประเมินผล และฝ่ายบัญชีและการเงิน ยังมีการร่วมพิจารณาถึงความเสี่ยงที่เกิดจากการใช้งบประมาณที่ไม่เป็นไปตามแนวทางของ

สตง. กรมบัญชีกลาง หรือ กพร. ที่กำหนดไว้ หรือความเสี่ยงที่เกิดจากการดำเนินงานทางการเงิน และงบประมาณไม่เป็นไปตามกฎหมาย กฎระเบียบ ของทางการ และของสำนักงาน

5.4 การประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยงด้านการเงิน สามารถวัดได้จากประมาณการกระแสเงินสดรับและจ่าย เพื่อดูฐานะสภาพคล่องในแต่ละช่วงเวลาต่าง ๆ หรือการวิเคราะห์อัตราส่วนทางการเงิน เช่น อัตราส่วนเงินทุนหมุนเวียนหรืออัตราส่วนสภาพคล่อง (Current Ratio) อัตราส่วนเงินทุนหมุนเร็ว (Quick Ratio) อัตราส่วนเงินสด (Cash Ratio) เป็นต้น เพื่อทราบถึงแนวโน้มสภาพคล่องทางการเงินหรือความเป็นไปได้ที่สำนักงานจะขาดสภาพคล่องในอนาคต

ความเสี่ยงด้านการบริหารโครงสร้างเงินทุน สามารถวัดประเมินได้ด้วยการวิเคราะห์สัดส่วนระหว่างหนี้สินและทุน (Debt/Equity Ratio) เพื่อให้ทราบถึงนโยบายการจัดหาแหล่งที่มาของเงินทุนมาเพื่อใช้ในสำนักงานซึ่งต้องดูให้สอดคล้องกับนโยบายด้านการเงินเพื่อให้เกิดประสิทธิภาพในการบริหารงานสูงสุด

ความเสี่ยงด้านการบริหารเงินทุน สามารถวัดประเมินจากการพิจารณาอัตราส่วนผลตอบแทนจากการลงทุน ด้วยเครื่องมือทางการเงินต่าง ๆ เพื่อวิเคราะห์ความสามารถในการทำกำไรของการลงทุนด้านการเงินแต่ละประเภท ทั้งนี้จะต้องสอดคล้องตามแผนและนโยบายการบริหารการลงทุนด้านการเงิน เช่น การใช้อัตราผลตอบแทนจากการลงทุน (Return on Investment; - ROI), การใช้อัตราผลตอบแทนต่อสินทรัพย์รวม (Return on Asset; - ROA) และ การใช้อัตราผลตอบแทนที่ปรับค่าความเสี่ยงต่อเงินทุน (Risk adjusted return on Control Capital – RAROC)

ทั้งนี้ ความเสี่ยงด้านการเงินอื่น ๆ ที่ไม่สามารถประเมินด้วยเครื่องมือทางการเงิน สามารถประเมินได้จากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือ โอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านการเงินเหล่านั้นขึ้น เป็นแต่ละเหตุการณ์ เช่น ความเสี่ยงที่เกิดจากการวิเคราะห์ข้อมูลหรือการนำข้อมูลด้านประมาณการงบการเงินไปใช้ไม่ถูกต้อง หากเกิดจากสาเหตุความผิดพลาดในการประมาณการตัวเลข ให้ทำการวิเคราะห์และกำหนดเป็นตัวประเมินความเสี่ยงทีละเหตุการณ์ เป็นต้น และควรมีการจัดทำ Sensitivity and Simulation Analysis ด้วย

ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ชื่อปัจจัยเสี่ยง การเบิกจ่ายงบประมาณไม่เป็นไปตามเป้าหมาย

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
โอกาส	มีการจัดทำแผนการเบิกจ่ายใช้งบประมาณแต่ละโครงการ และมีการรายงานผลการเบิกจ่ายงบประมาณต่อผู้บริหารระยะเวลาที่กำหนด และมีการเบิกจ่ายงบประมาณเป็นไปตามเป้าหมาย	มีการจัดทำแผนการเบิกจ่ายใช้งบประมาณแต่ละโครงการ และมีการรายงานผลการเบิกจ่ายงบประมาณต่อผู้บริหาร	มีการจัดทำแผนการเบิกจ่ายใช้งบประมาณแต่ละโครงการ แต่ยังไม่มีการรายงานผลการเบิกจ่ายงบประมาณต่อผู้บริหาร	มีการจัดทำแผนการเบิกจ่ายใช้งบประมาณแต่ละโครงการ	ไม่มีการจัดทำแผนการเบิกจ่ายใช้งบประมาณแต่ละโครงการ

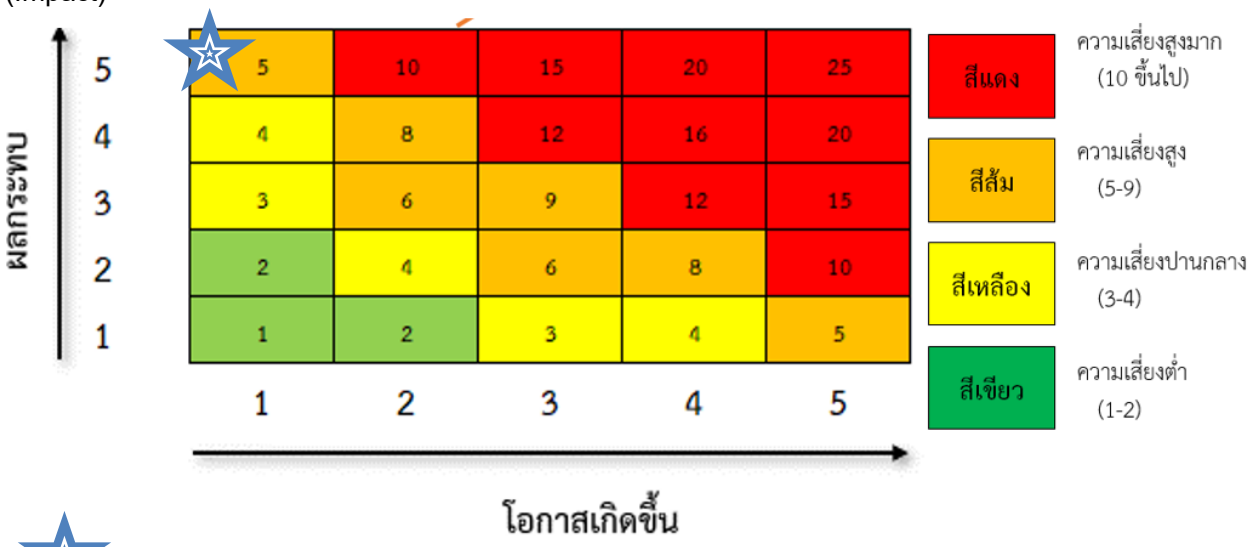
	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 5	ระดับ 25
ผลกระทบ	การเบิกจ่ายงบประมาณมากกว่าหรือเท่ากับร้อยละ 95 ขึ้นไป	การเบิกจ่ายงบประมาณมากกว่าหรือเท่ากับร้อยละ 90 ขึ้นไป	การเบิกจ่ายงบประมาณมากกว่าหรือเท่ากับร้อยละ 85 ขึ้นไป	การเบิกจ่ายงบประมาณมากกว่าหรือเท่ากับร้อยละ 80 ขึ้นไป	การเบิกจ่ายงบประมาณน้อยกว่าร้อยละ 80

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

ตัวบ่งชี้ความเสี่ยงด้านการเงินของสำนักงาน ได้มีการกำหนดและประเมินไว้ให้สอดคล้องตามนโยบายด้านการเงิน การลงทุน และการงบประมาณต่าง ๆ โดยความเห็นชอบจากคณะกรรมการ สพร. เช่น การกำหนดตัวบ่งชี้ความเสี่ยงด้านการเงิน โดยการดำรงเงินสดหมุนเวียนขั้นต่ำไว้เพื่อใช้จ่ายสำหรับค่าใช้จ่ายดำเนินงานประจำเดือนอย่างน้อย 1 เดือน เป็นต้น

เมื่อประเมินระดับความเสี่ยงได้แล้ว ขั้นต่อไปคือ การจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญ และจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของสำนักงาน หรือหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดย สำนักงานได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น 4 ระดับ ตามโอกาสที่จะเกิดความเสี่ยง

และผลกระทบของความเสี่ยงนั้น ๆ ได้แก่ ระดับสูงมาก ระดับสูง ระดับปานกลาง ระดับต่ำ ตามลำดับ โดยใช้ Risk Map เป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมิน ซึ่ง Risk Map จะแสดงข้อมูลเป็น 2 แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact)



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจากสำนักงานเป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
3-4	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

5.5 การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบ ที่เกิดจากความเสี่ยงนั้น ๆ จะทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าว เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่สำนักงานยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
การเบิกจ่ายงบประมาณไม่เป็นไปตามเป้าหมาย	มีการจัดทำแผนการใช้จ่ายงบประมาณของแต่ละโครงการ และมีการติดตามและเร่งรัดผลการเบิกจ่ายเป็นประจำทุกเดือน	การลดความเสี่ยง (Treat)

5.6 กิจกรรมการควบคุม (Control Activities)

ส่วนบริหารความเสี่ยง ส่วนแผน งบประมาณ และติดตามประเมินผล และฝ่ายบัญชีและการเงิน มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านการเงินโดยจะควบคุมความเสี่ยงทางด้านการเงิน ด้านการบริหารเงินลงทุนและอื่น ๆ ให้สอดคล้องกับเพดานความเสี่ยง (Risk Limit) หรือตัวบ่งชี้ความเสี่ยงด้านการเงินที่ได้รับอนุมัติและดำเนินการควบคุมป้องกันความเสี่ยงด้านการเงินของสำนักงานให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการ สพร. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

5.7 สารสนเทศและการสื่อสาร (Information and Communication)

แหล่งที่มาของข้อมูล

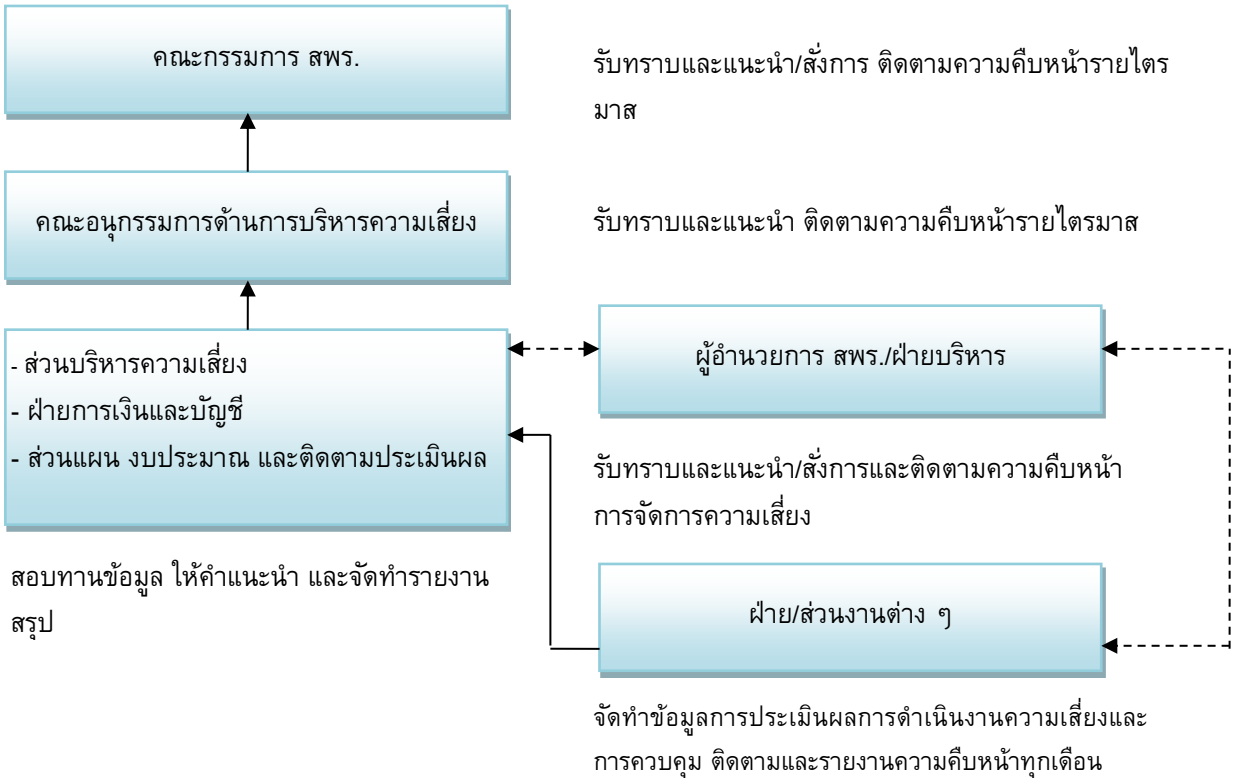
ส่วนบริหารความเสี่ยง จัดเก็บข้อมูลซึ่งมีรายละเอียดดังนี้

ข้อมูล	แหล่งที่มา	หมายเหตุ
สถานะสภาพคล่องสุทธิ ● **ประมาณการกระแสเงินสด** ● **Current Ratio** ● **อัตราส่วนทางการเงิน**	• ฝ่ายบัญชีและการเงิน	• พิจารณาจากการจัดทำงบประมาณกระแสเงินสดด้วยวิธีทางอ้อม • อัตราส่วนต่าง ๆ พิจารณาจากงบแสดงสถานะการเงิน (งบดุล) และงบรายได้ค่าใช้จ่าย (งบกำไร - ขาดทุน)
สถานะการเบิกจ่ายงบประมาณ	• ฝ่ายบัญชีและการเงิน	• พิจารณาจากการรายงานการเบิกจ่ายงบประมาณรายเดือน • พิจารณาจากการรายงานความคืบหน้าการติดตามโครงการที่ต้องมีการเบิกจ่ายเงินงบประมาณ
ผลการดำเนินงานของรายได้นอกงบประมาณ	• ฝ่ายบัญชีและการเงิน	• ความคืบหน้าการให้บริการหน่วยงานภาครัฐ • การรายงานผลการดำเนินงานของรายได้นอกงบประมาณเทียบกับเป้าหมายแต่ละเดือน พร้อมรายงานถึงปัญหาอุปสรรคและแนวทางแก้ไข

5.8 การติดตามและประเมินผล (Monitoring)

ฝ่ายบัญชีและการเงิน และส่วนแผน งบประมาณ และติดตามประเมินผล มีหน้าที่แจ้งรายงานความเสี่ยงต่อผู้บังคับบัญชาตามสายงานเพื่อรายงานต่อผู้อำนวยการ สพร. และฝ่ายบริหารทราบเพื่อหาแนวทางแก้ไขและป้องกันความเสี่ยงด้านการเงินที่พบเห็นและเกิดขึ้น โดยจะต้องมีการติดตามและรายงานความเสี่ยงให้แก่ส่วนบริหารความเสี่ยงเพื่อรวบรวมข้อมูล และจัดทำรายงานสถานะความเสี่ยงด้านการเงินในภาพรวมต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง เพื่อคณะกรรมการ สพร. ได้รับทราบอย่างสม่ำเสมอและต่อเนื่องต่อไป

สรุปขั้นตอนการรายงานความเสี่ยง



★ หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติ ฝ่ายบัญชีและการเงินต้องแจ้งข้อมูลให้ส่วนบริหารความเสี่ยง พร้อมทั้งรายงานให้ผู้บริหาร สพร. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สพร. / ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการ สพร.
ต่ำ	รับทราบ/แนะนำ	รับทราบ	รับทราบ

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สพร. / ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการ สพร.
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

หน้า

1. บทนำ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้ตระหนักถึงการดำเนินธุรกรรมต่าง ๆ เพื่อให้อยู่ภายใต้กฎหมาย มติคณะรัฐมนตรี ข้อบังคับ ระเบียบ ประกาศ และคำสั่ง ตลอดจนระเบียบของหน่วยงานที่กำกับดูแล เช่น คณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) สำนักงานการตรวจเงินแผ่นดิน (สตง.) เป็นอย่างมาก สำนักงานจึงให้ความสำคัญต่อการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ (Compliance Risk) โดยมีคณะกรรมการ สพร. แนะนำและติดตามการรายงานผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ

กระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ เป็นกระบวนการที่สำคัญมาก โดยเฉพาะความเสี่ยงด้านกฎหมาย ซึ่งถ้าสำนักงานมีการดำเนินธุรกรรมที่ขัดต่อกฎหมายนั้น อาจเป็นสาเหตุให้สำนักงานถูกระงับการดำเนินงานตามภารกิจลงได้ ดังนั้น กระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ จึงเป็นกระบวนการที่ช่วยให้การดำเนินการของสำนักงานมีการควบคุมการดำเนินการหรือจัดการความเสี่ยง โดยมีการติดตามและรายงานอย่างต่อเนื่องตามนโยบายที่สำนักงานกำหนด

คู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) โดยจะกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ เพื่อใช้เป็นแนวทางในการปฏิบัติงานของสำนักงาน

แนวทางการบริหารความเสี่ยงที่นำมาใช้

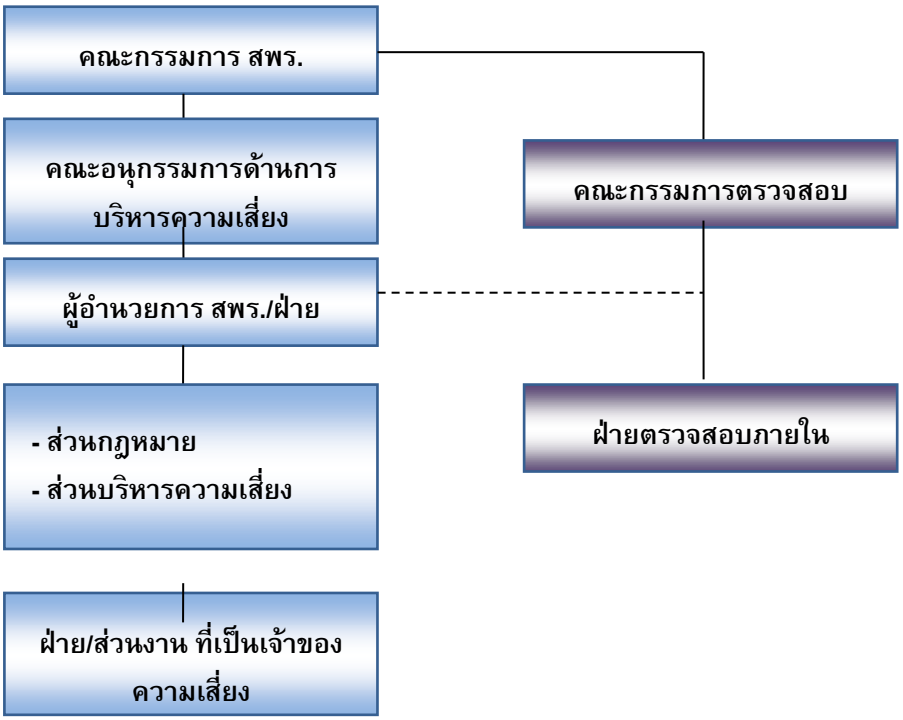
สำนักงานกำหนดกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบตามแนวทางการปฏิบัติงานของ สำนักงานและภายใต้กรอบการบริหารความเสี่ยง COSO ERM Framework ของ Committee of Sponsoring Organizations of The Treadway Commission (COSO)

ขอบเขตของคู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบเท่านั้น โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ เพื่อให้หน่วยงานต่าง ๆ ของสำนักงาน ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบของตนเอง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

2. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านกฎหมาย และกฎระเบียบ



3. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายกลยุทธ์องค์กร มีหน้าที่รับผิดชอบดังนี้

1. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ และนำเสนอต่อคณะกรรมการ สพร. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
2. ประสานงานกับหน่วยงานต่าง ๆ เพื่อให้หน่วยงานต่าง ๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ที่กำหนดในกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ
3. จัดทำคู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ และเสนอคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติพร้อมทั้งทบทวนเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
4. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทาง ความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ
5. รวบรวมข้อมูลความเสี่ยงด้านกฎหมาย กฎระเบียบ และรายงานคณะอนุกรรมการด้านการบริหารความเสี่ยง

ส่วนกฎหมาย สำนักเลขานุการผู้อำนวยการ มีหน้าที่รับผิดชอบดังนี้

1. พิจารณากฎระเบียบภายในต่าง ๆ ให้สอดคล้องและอยู่ภายใต้กฎหมายที่เกี่ยวข้อง
2. ให้คำปรึกษาหน่วยงานต่าง ๆ ของสำนักงานในการดำเนินการเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบ

ฝ่ายตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

ตรวจสอบและสอบทานการควบคุมภายในด้านต่าง ๆ ของสำนักงานก่อนนำเสนอคณะกรรมการตรวจสอบเพื่อพิจารณาให้คำแนะนำ

ฝ่ายและส่วนงานต่าง ๆ ของสำนักงาน มีหน้าที่รับผิดชอบ ดังนี้

1. กำหนดแผนปฏิบัติการของฝ่าย และส่วนงานต่าง ๆ โดยดำเนินการตามกรอบนโยบาย และกระบวนการบริหารความเสี่ยงที่กำหนดในคู่มือบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ
2. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับฝ่าย และส่วนงานต่าง ๆ
3. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance รวมถึงแผนปรับลดความเสี่ยงของแผนปฏิบัติงานฝ่าย และส่วนงานต่าง ๆ ให้กับส่วนบริหารความเสี่ยง เพื่อนำไปจัดทำแผนภาพบริหารความเสี่ยงต่อไป
4. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของฝ่ายให้กับส่วนบริหารความเสี่ยงเป็นรายไตรมาส

4. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

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

(1) แผนปฏิบัติงาน (Action Plan) หมายถึง กรอบการดำเนินงานประจำปี ที่หน่วยงานต่าง ๆ จัดทำขึ้นเพื่อใช้ในการปฏิบัติงานประจำปี โดยแผนปฏิบัติงานจะต้องสนับสนุนแผนธุรกิจ (Business Plan) ของสำนักงาน

(2) โอกาสที่จะเกิด (Likelihood) หมายถึง ความเป็นไปได้ที่จะเกิดความเสี่ยงด้านกฎหมาย กฎระเบียบ

(3) ผลกระทบของเหตุการณ์ (Impact) หมายถึง ผลกระทบหรือความเสียหายที่เกิดขึ้นกับสำนักงาน อันเนื่องมาจากการเกิดขึ้นของความเสี่ยงด้านกฎหมาย กฎระเบียบ

(4) ดัชนีชี้วัดความเสี่ยง (Key Risk Indicators) หมายถึง เครื่องมือที่จะช่วยให้ผู้บริหาร สพร. ทราบถึงระดับความเสี่ยงที่มีอยู่ในช่วงเวลาใดเวลาหนึ่ง โดยอาศัยการชี้วัดจากปัจจัยเสี่ยงต่าง ๆ ที่กำหนดขึ้น

(5) ความเสี่ยงตั้งต้น (Inherent Risk) เป็นความเสี่ยงด้านกฎหมาย กฎระเบียบที่มีอยู่ทันทีที่มีการกระทำกิจกรรมหรือการดำเนินงาน เช่น การดำเนินการด้านเทคโนโลยีสารสนเทศ ต้องสอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

(6) ระดับความเสี่ยงที่ทนได้หรือความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ความเสี่ยงที่เกินจากความเสี่ยงที่ยอมรับได้ แต่อยู่ในช่วงกำหนดที่ทนได้ ซึ่งจะต้องมีการจัดการทันที

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

(8) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ระดับของความเสี่ยงที่สำนักงานจะยอมรับได้ ซึ่งในความเป็นจริงนั้น ความเสี่ยงด้านกฎหมายเกิดได้สองประเด็น ได้แก่ การที่ทำตามกฎหมายแต่ไม่บรรลุวัตถุประสงค์ของแผนงานที่กำหนดไว้ และการไม่ปฏิบัติตามกฎหมาย ซึ่งไม่ควรเกิดขึ้น ทั้งนี้ ต้องพิจารณาว่าเป็นกฎระเบียบภายใน หรือกฎระเบียบภายนอก และ

ระดับของผลกระทบต่อ สำนักงานและเจ้าหน้าที่ผู้ปฏิบัติงาน โดยต้องจัดทำแผนจัดการความเสี่ยงที่มีอยู่ในปัจจุบันให้ครอบคลุมความเสี่ยงทั้งหมด รวมถึงความเสี่ยงด้านธรรมาภิบาลด้วย

(9) ความเสี่ยงคงเหลือ (Residual Risk) เป็นความเสี่ยงที่เหลืออยู่หลังจากได้จัดการ หรือควบคุมความเสี่ยงนั้นแล้ว ความเสี่ยงคงเหลือจะเป็นจุดเริ่มต้นของการกำหนดระดับความเสี่ยงที่ยอมรับได้

ดังนั้น การดำเนินการของสำนักงาน ในประเด็นที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ต้องเริ่มตั้งแต่การจัดทำแผนธุรกิจ แผนกลยุทธ์ของสำนักงาน และเมื่อหน่วยงานต่าง ๆ ได้รับทราบแผนธุรกิจสำนักงาน แล้วนำมาวิเคราะห์ จะทำให้ทราบว่าหน่วยงานของตนจะสนับสนุนแผนธุรกิจได้อย่างไร จึงจัดทำแผนปฏิบัติงาน (Action Plan) ของหน่วยงานตนเอง ซึ่งในการจัดทำแผนปฏิบัติงานของหน่วยงานนั้นต้องมีการดำเนินการตามกระบวนการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ไปพร้อมกัน

5. องค์ประกอบการบริหารความเสี่ยง

5.1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

การวิเคราะห์และประเมินสภาพแวดล้อมการบริหารความเสี่ยงด้านกฎหมาย กฎระเบียบ ต้องคำนึงถึงปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อสำนักงาน หรือหน่วยงานนั้น ๆ ในการวิเคราะห์ดังกล่าวจะทำให้สามารถระบุได้ว่า แผนงาน/โครงการ นั้น ๆ จะสามารถดำเนินงานต่อไปได้หรือไม่ หรือต้องปรับปรุงแผนงาน/โครงการ อย่างไร เพื่อไปสู่เป้าหมายที่กำหนดไว้

5.2 การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

ส่วนกฎหมายเป็นผู้รับผิดชอบหลักในการกำหนดระดับความเสี่ยงด้านกฎหมาย กฎระเบียบ รวมถึงธรรมาภิบาลของสำนักงาน และส่วนบริหารความเสี่ยงเป็นผู้รับผิดชอบหลักในการกำหนดวัตถุประสงค์ของการบริหารความเสี่ยงในภาพรวมของสำนักงาน

ฝ่าย ส่วนงาน หรือโครงการต่าง ๆ เป็นผู้รับผิดชอบในการจัดการความเสี่ยงด้านกฎหมาย กฎระเบียบ เพื่อให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยร่วมกับส่วนกฎหมาย และส่วนบริหารความเสี่ยงสำหรับงานหรือโครงการที่รับผิดชอบ พร้อมทั้งมีการรายงานความเสี่ยงตามระยะเวลาตามแต่ระดับความเสี่ยงที่ได้กำหนดไว้

5.3 การระบุเหตุการณ์ (Event Identification)

การระบุเหตุการณ์ความเสี่ยง จะเริ่มด้วยการแจกแจงกระบวนการปฏิบัติงาน (Work flow) เพื่อให้ทราบขั้นตอนงานที่มีอยู่และจะทำให้บรรลุวัตถุประสงค์ที่กำหนดไว้ แล้วจึงระบุปัจจัยเสี่ยงด้านกฎหมาย กฎระเบียบที่มีผลกระทบในแต่ละขั้นตอนการปฏิบัติงานนั้น ๆ ที่อาจส่งผลต่อวัตถุประสงค์/เป้าหมายของงาน/โครงการ ทั้งทางตรงและทางอ้อมต่อสำนักงาน

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย กฎระเบียบ

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย กฎระเบียบ	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การปฏิบัติงานไม่เป็นไปตามกฎหมาย กฎระเบียบ	ไม่มีการเผยแพร่กฎหมาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับองค์กร ทั้งในอดีตและ		✓

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย กฎระเบียบ	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
ข้อบังคับ และสัญญา ที่ทำไว้กับหน่วยงานภายนอก	ปัจจุบันที่ยังมีผลบังคับใช้ให้เจ้าหน้าที่รับทราบและปฏิบัติ		
การปฏิบัติงานไม่เป็นไปตามคำสั่ง ประกาศ ระเบียบ ข้อบังคับขององค์กร	1. ไม่มีการเผยแพร่คำสั่ง ประกาศ ระเบียบ ข้อบังคับขององค์กร 2. ไม่มีการทบทวน/ปรับปรุงให้เป็นปัจจุบันเป็นประจำทุกปี 3. ไม่มีการสื่อสารให้หน่วยงานที่เกี่ยวข้องทราบ หากมีการเปลี่ยนแปลงแก้ไขหลักเกณฑ์/วิธีปฏิบัติงาน 4. ไม่มีการปฏิบัติตามคำสั่ง ประกาศ ระเบียบ ข้อบังคับขององค์กร เช่น กระบวนการจัดซื้อจัดจ้าง เป็นต้น	✓	

5.4 การประเมินความเสี่ยง (Risk Assessment)

ทั้งนี้ ความเสี่ยงด้านกฎหมาย และกฎระเบียบ สามารถประเมินได้จากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในอดีต หรือโอกาสที่จะเกิดเหตุการณ์การปฏิบัติที่อาจจะเกิดความเสี่ยงด้านกฎหมายและกฎระเบียบเหล่านั้นขึ้น เป็นแต่ละเหตุการณ์ โดยทั่วไป ความเสี่ยงด้านกฎหมายและกฎระเบียบจะมีลักษณะการกำหนดผลกระทบที่ท้าทายมาก นั่นคือ มีเพียงระดับ 5 ซึ่งหมายถึงการมีเหตุการณ์ที่ไม่ปฏิบัติตามกฎหมายกฎระเบียบเกิดขึ้น แม้เพียง 1 ครั้ง และระดับ 1 คือ ทุกธุรกรรมขององค์กรเป็นไปตามกฎหมาย และกฎระเบียบที่เกี่ยวข้อง

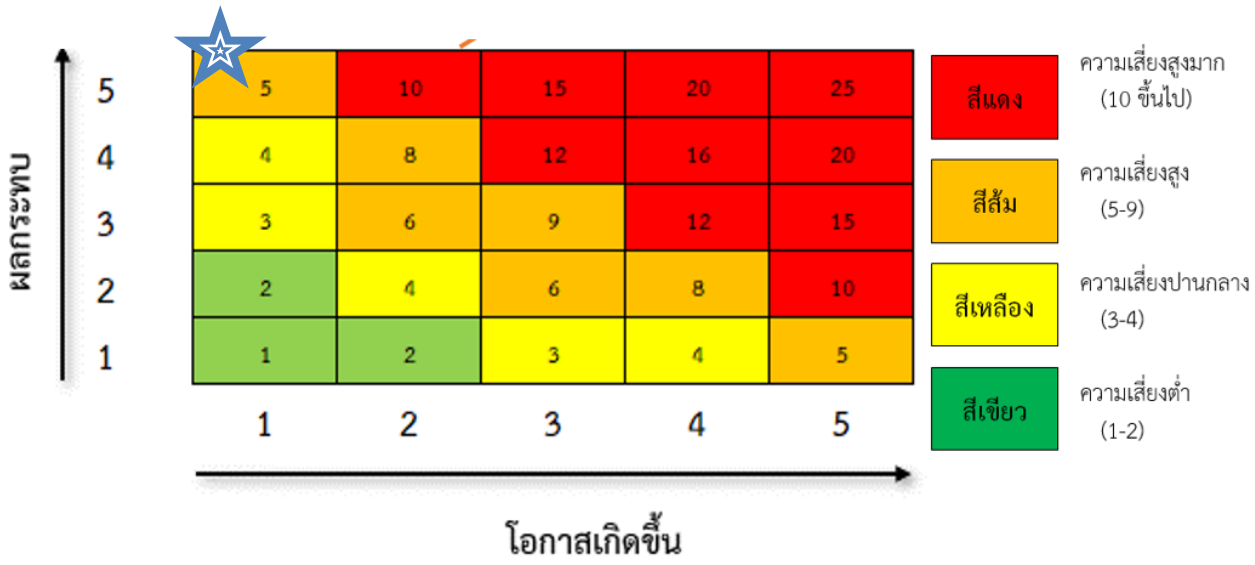
ตัวอย่างการกำหนดโอกาสและผลกระทบในแต่ละประเภทความเสี่ยง

ชื่อปัจจัยเสี่ยง การปฏิบัติงานไม่เป็นไปตามกฎหมาย กฎระเบียบ ข้อบังคับ และสัญญา ที่ทำไว้กับหน่วยงาน ภายนอก

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
โอกาส	เกิดขึ้น 1 ครั้งต่อปีหรือไม่เกิดเลย	เกิดขึ้น 2 ครั้งต่อปี	เกิดขึ้น 3 ครั้งต่อปี	เกิดขึ้น 4 ครั้งต่อปี	เกิดขึ้นมากกว่า 4 ครั้งต่อปี

	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
	ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 5	ระดับ 25
ผลกระทบ	มีการปฏิบัติตามกฎระเบียบข้อบังคับ และไม่มีการละเมิดข้อกฎหมาย	มีการไม่ปฏิบัติตามกฎระเบียบข้อบังคับ และการละเมิดข้อกฎหมายที่ไม่มีนัยสำคัญ	มีการไม่ปฏิบัติตามกฎระเบียบข้อบังคับ และการละเมิดข้อกฎหมายที่มีนัยสำคัญ	มีการฝ่าฝืน/ละเมิดกฎหมายสัญญาที่มีนัยสำคัญและถูกเรียกร้องค่าเสียหาย	มีการฟ้องร้องดำเนินคดีและเรียกร้องค่าเสียหายที่สำคัญ

เมื่อประเมินระดับความเสี่ยงได้แล้ว ขั้นต่อไปคือ การจัดลำดับความเสี่ยงเพื่อให้สามารถทราบความสำคัญ และจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของสำนักงาน หรือหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดยสำนักงานได้แยกระดับความสำคัญหรือความรุนแรงของความเสี่ยงออกเป็น 4 ระดับ ตามโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงนั้น ๆ ได้แก่ ระดับสูงมาก ระดับสูง ระดับปานกลาง ระดับต่ำ ตามลำดับ โดยใช้ Risk Map เป็นเครื่องมือสำหรับการรายงานระดับความเสี่ยงที่ได้จากการประเมิน ซึ่ง Risk Map จะแสดงข้อมูลเป็น 2 แกน ได้แก่ แกนโอกาสที่จะเกิดความเสี่ยง (Likelihood) และแกนผลกระทบของความเสี่ยง (Impact)



ถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจากสำนักงานเป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ

สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
3-4	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

5.5 การตอบสนองความเสี่ยง (Risk Response)

การวิเคราะห์และจัดลำดับความเสี่ยงของปัจจัยเสี่ยงที่ได้ระบุไว้แล้ว ซึ่งพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบ ที่เกิดจากความเสี่ยงนั้น ๆ จะทำให้ทราบว่า ความเสี่ยงดังกล่าวอยู่ภายในบริเวณพื้นที่ที่มีความเสี่ยงระดับใด หน่วยงานที่รับผิดชอบปัจจัยเสี่ยงนั้น ๆ ต้องหามาตรการจัดการ ควบคุม และลดความเสี่ยงดังกล่าว เพื่อให้ระดับความรุนแรงของผลกระทบลดลงหรือมีโอกาสที่จะเกิดน้อยลงโดยความเสี่ยงที่เหลืออยู่จะต้องอยู่ภายในระดับความเสี่ยงที่สำนักงานยอมรับได้

ตัวอย่างการกำหนดมาตรการจัดการความเสี่ยง

ความเสี่ยง	มาตรการในการจัดการความเสี่ยง	ประเภทของมาตรการในการจัดการความเสี่ยง
การปฏิบัติงานไม่เป็นไปตามกฎหมาย กฎระเบียบ ข้อบังคับ และสัญญา ที่ทำไว้กับหน่วยงานภายนอก	สำนักงานมีการสำรวจ และมีการศึกษา ให้ความรู้ และมีการตั้งคณะทำงาน รวมถึงมีการเผยแพร่กฎหมาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับสำนักงานทั้งในอดีตและปัจจุบันที่ยังมีผลบังคับใช้ผ่านทางมีการจัดประชุม , อีเมล์ , Intranet , Internet เพื่อให้เจ้าหน้าที่สามารถรับรู้และปฏิบัติตาม	การลดความเสี่ยง (Treat)

5.6 กิจกรรมการควบคุม (Control Activities)

การควบคุมเป็นเครื่องมือที่ใช้ในการจัดการกับความเสี่ยงที่มีอยู่ ดังนั้นหน่วยงานควรดำเนินการระบุการควบคุมที่มีอยู่ และประเมินประสิทธิผลและความเพียงพอของการควบคุม หากไม่เพียงพอให้หน่วยงานดังกล่าวจัดทำแผนจัดการความเสี่ยงเพิ่มเติม

5.7 สารสนเทศและการสื่อสาร (Information and Communication)

<u>แหล่งที่มาของข้อมูล</u>

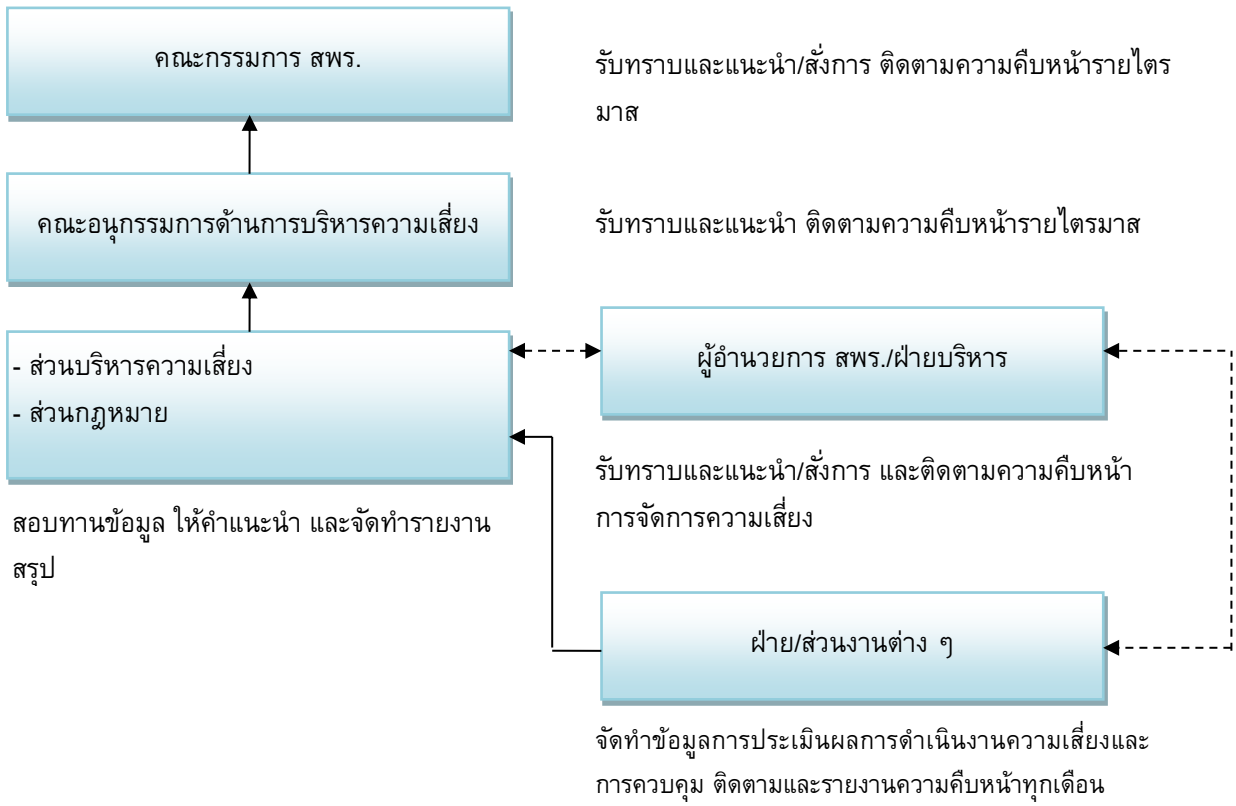
ส่วนบริหารความเสี่ยง จัดเก็บข้อมูลซึ่งมีรายละเอียดดังนี้

ข้อมูล	แหล่งที่มา	หมายเหตุ
ข้อมูลภายใน	ส่วนกฎหมาย	พิจารณาจากการรายงานการเปลี่ยนแปลงของระเบียบ ข้อบังคับ คำสั่ง ประกาศภายในสำนักงาน พิจารณาจากการรายงานเอกสารสัญญาที่สำนักงานเป็นคู่สัญญา
ข้อมูลภายนอก	ส่วนกฎหมาย	พิจารณาจากรายงานการเปลี่ยนแปลงของระเบียบของหน่วยงานกำกับดูแล รวมถึงกฎหมาย มติคณะรัฐมนตรี และกฎระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับสำนักงาน

5.8 การติดตามและประเมินผล (Monitoring)

ส่วนบริหารความเสี่ยง และส่วนกฎหมาย ต้องรายงานความเสี่ยงด้านกฎหมาย กฎระเบียบต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง และคณะกรรมการ สพร. เพื่อให้ทราบผลการดำเนินงาน ปัญหาที่เกิดขึ้น และตรวจสอบสาเหตุของปัญหา ตลอดจนหาแนวทางแก้ไขเพื่อป้องกัน ควบคุมและลดความเสี่ยงด้านกฎหมาย กฎระเบียบตามที่กำหนด ซึ่งในรายงานความเสี่ยงต้องแสดงถึงความเสี่ยงด้านกฎหมาย กฎระเบียบที่มีอยู่ และแนวทางแก้ไขระยะเวลาแล้วเสร็จอย่างชัดเจน

สรุปขั้นตอนการรายงานความเสี่ยง



★ หากเกิดเหตุการณ์ความเสี่ยงฉุกเฉินให้ปฏิบัติตาม Business Continuity Plan ในการรายงาน

ในกรณีที่เกิดเหตุการณ์ผิดปกติ ส่วนงานที่เกี่ยวข้องต้องรายงานให้ผู้บริหาร สพร. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	กฎหมาย กฎระเบียบที่เกี่ยวข้อง	ผู้อำนวยการ สพร. /ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการ สพร.
ปานกลาง	ข้อบังคับระเบียบ	รับทราบ/แนะนำและสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำและสั่งการ

ระดับความรุนแรงและการรายงาน	กฎหมาย กฎระเบียบที่เกี่ยวข้อง	ผู้อำนวยการ สพร. /ฝ่ายบริหาร	อนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการ สพร.
หรือเตือน (Warning)	ประกาศ และคำสั่งภายใน			
สูง หรือรุนแรง (Severe)	ระเบียบของหน่วยงานที่กำกับดูแล	รับทราบ/แนะนำ และสั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ
สูงมาก หรือ รุนแรงมาก (High Severe)	กฎหมาย มติคณะรัฐมนตรี	รับทราบ/แนะนำ/สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และ ติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ

คู่มือบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(Information Technology Risk Management Manual)

สารบัญ

หน้า

1. บทนำ

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) เป็นองค์ประกอบสำคัญของการดำเนินงานของ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) เป็นอย่างมาก จึงได้มีการกำหนดนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อบังคับใช้กับทุกหน่วยงานของสำนักงาน โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจและตระหนักถึงหน้าที่ความรับผิดชอบต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอยู่เสมอ และยังสนับสนุนให้เจ้าหน้าที่ทุกระดับชั้นเข้าใจ รวมถึงมีส่วนร่วมในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในทุกขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

คู่มือบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ซึ่งจะใช้ประกอบกับคู่มือเฉพาะของแต่ละเครื่องมือที่ใช้ในการบริหารความเสี่ยง ซึ่งจะกล่าวลงไปในรายละเอียดเพื่อให้หน่วยงานสามารถวางระบบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศภายในหน่วยงานของตนเองได้อย่างมีประสิทธิภาพ และเป็นการป้องกัน ควบคุม และลดผลกระทบจากเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้นกับสำนักงาน รวมถึงผลกระทบจากการเปลี่ยนแปลงเทคโนโลยีหรือนวัตกรรมต่าง ๆ อย่างเฉียบพลัน (Disruptive Technology / Disruptive Innovation) โดยกระบวนการดังกล่าวจะอยู่ภายใต้การดูแลของหัวหน้าส่วนงาน ผู้อำนวยการฝ่าย และมีการกำกับ ดูแลและสั่งการโดยคณะกรรมการ สพร. ผ่านทางคณะอนุกรรมการด้านการบริหารความเสี่ยง

แนวคิดเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศจะอยู่บนพื้นฐานของการควบคุมภายใน ซึ่งเป็นกระบวนการที่เป็นขั้นตอนที่ต่อเนื่องและแทรกอยู่ในการปฏิบัติงานตามปกติของทุกหน่วยงาน

2. เจ้าหน้าที่ในทุกหน่วยงานของสำนักงาน มีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งมีผู้บริหารเป็นผู้รับผิดชอบให้มีระบบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามที่สำนักงานกำหนด คือ มีการระบุ ประเมิน ติดตาม ควบคุม และรายงานความเสี่ยง

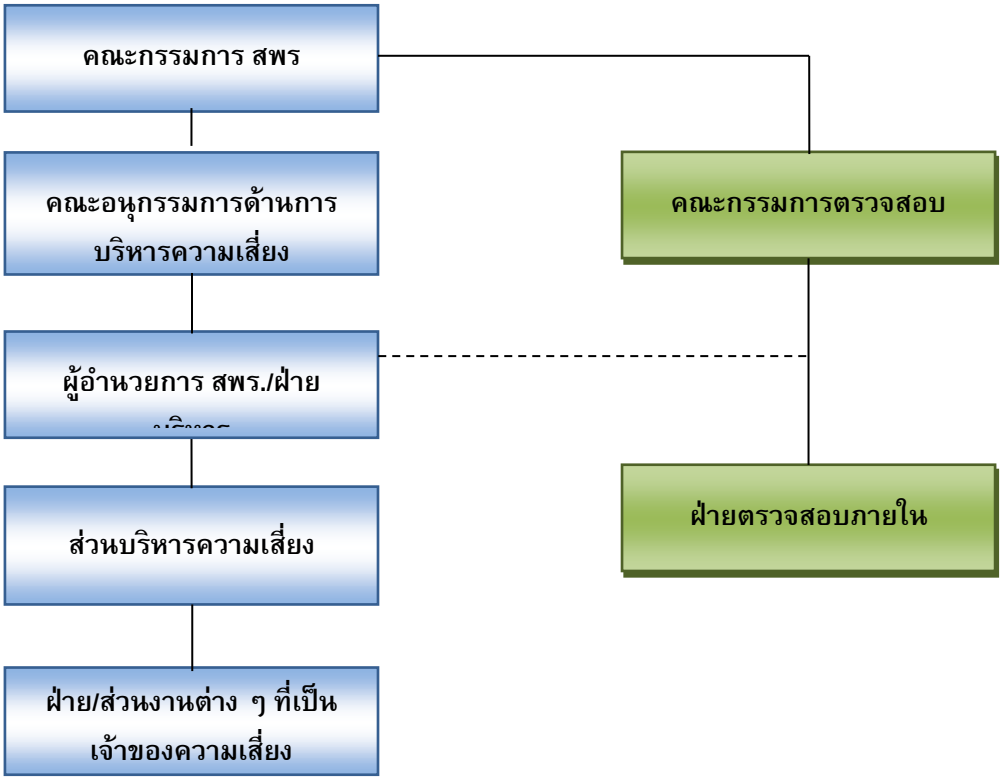
3. การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศควรให้ความมั่นใจอย่างสมเหตุสมผลว่าหน่วยงานจะบรรลุตามเป้าหมายที่ได้กำหนดไว้ กล่าวคือ แม้ว่าจะมีการวางระบบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศไว้ดีเพียงใด ก็ไม่สามารถรับรองได้ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้อย่างสมบูรณ์ เพราะมีข้อจำกัดจากปัจจัยอื่นนอกเหนือการควบคุมของหน่วยงาน เช่น ผลกระทบจากปัจจัยภายนอก เป็นต้น

ขอบเขตของคู่มือบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

คู่มือฉบับนี้จะกล่าวถึงการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นส่วนหนึ่งของนโยบายบริหารความเสี่ยงสำนักงาน โดยกล่าวถึงรายละเอียดของกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้หน่วยงานต่าง ๆ ของสำนักงาน ใช้เป็นแนวทางในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของตนเอง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้

2. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ



3. หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

บทบาท หน้าที่และความรับผิดชอบหลักของหน่วยงานหรือผู้ที่เกี่ยวข้อง

ส่วนบริหารความเสี่ยง ฝ่ายกลยุทธ์องค์กร มีหน้าที่รับผิดชอบดังนี้

1. จัดทำกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และนำเสนอต่อคณะกรรมการ สพร. หรือคณะกรรมการที่ได้รับมอบหมายผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงเพื่อพิจารณาอนุมัติ ตลอดจนทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้มีความเหมาะสมเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
2. รายงานความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่แสดงถึงการปฏิบัติหรือไม่ปฏิบัติตามนโยบาย ที่กำหนดไว้
3. ประเมิน ติดตาม และควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่เกี่ยวกับความต่อเนื่องในการดำเนินงาน เพื่อให้มีการปฏิบัติตามนโยบายที่กำหนด
4. ประสานงานกับหน่วยงานต่าง ๆ ที่เป็นเจ้าของความเสี่ยง เพื่อให้หน่วยงานต่าง ๆ ดำเนินการตามกรอบนโยบายและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนด
5. สื่อสารและสร้างความเข้าใจกับเจ้าหน้าที่และหน่วยงานต่าง ๆ ให้เข้าใจถึงแนวทาง ความสำคัญ และความรับผิดชอบในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
6. บริหาร ควบคุม และจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมให้อยู่ภายในระดับที่ยอมรับได้
7. ทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

ฝ่ายและส่วนงานต่าง ๆ ของสำนักงาน มีหน้าที่รับผิดชอบ ดังนี้

1. กำหนดกลยุทธ์และแผนปฏิบัติงานของฝ่าย และส่วนงานต่าง ๆ ให้สอดคล้องกับนโยบายบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
2. สนับสนุนและดูแลให้มีผู้ประสานงานความเสี่ยงระดับฝ่าย และส่วนงานต่าง ๆ
3. พิจารณา Risk Factor, Risk Appetite และ Risk Tolerance ให้กับส่วนบริหารความเสี่ยง เพื่อนำไปจัดทำความเสี่ยงด้านเทคโนโลยีสารสนเทศและภาพความเสี่ยงแบบบูรณาการ ตามลำดับต่อไป

4. ติดตามการจัดการความเสี่ยงของหน่วยงานในสังกัดเพื่อรายงานความเสี่ยงในภาพรวมของฝ่ายให้กับส่วนบริหารความเสี่ยงเป็นรายเดือนหรือรายไตรมาสตามความเหมาะสม
5. จัดทำแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Treatment Plan) ของฝ่าย และส่วนงานต่าง ๆ และบริหารจัดการความเสี่ยงที่มีผลต่อเป้าหมายตามกลยุทธ์ของหน่วยงาน ในฐานะผู้จัดการความเสี่ยง (Risk Manager) ให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้
6. ดูแล ติดตามการจัดการความเสี่ยง และประเมินผลการจัดการความเสี่ยงเป็นประจำ เพื่อรายงานผลการบริหารความเสี่ยงให้ผู้บังคับบัญชาตามลำดับ รวมถึงนำเสนอแผนการจัดการความเสี่ยงเพิ่มเติม เพื่อบริหารจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้
7. แต่งตั้งผู้ประสานงานด้านความเสี่ยง (Risk Internal Control Officer: RICO) เพื่อประสานงานกับส่วนบริหารความเสี่ยงในการจัดทำ Risk Factor, Risk Appetite และ Risk Tolerance จากแผนธุรกิจ แผนกลยุทธ์ หรือแผนปฏิบัติงานของฝ่ายและส่วนงาน
8. สื่อสารและนำกระบวนการบริหารความเสี่ยงไปยังเจ้าหน้าที่ทุกคนเพื่อสร้างความเข้าใจและนำกระบวนการบริหารความเสี่ยงไปใช้ในการปฏิบัติงานประจำวัน

ฝ่ายตรวจสอบภายใน มีหน้าที่รับผิดชอบ ดังนี้

ตรวจสอบและสอบทานการควบคุมภายในด้านต่าง ๆ ของสำนักงาน ก่อนนำเสนอคณะกรรมการตรวจสอบ เพื่อพิจารณาให้คำแนะนำ

4. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ได้มีการนำมาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็นมาตรฐานที่กำลังได้รับความนิยมอย่างแพร่หลายในปัจจุบัน และกล่าวถึงข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS (Information Security Management System) ให้กับองค์กร ซึ่งวัตถุประสงค์ของมาตรฐานนี้เพื่อให้องค์กรสามารถบริหารจัดการทางด้านความปลอดภัยได้อย่างมีระบบ และเพียงพอเหมาะสมต่อการดำเนินธุรกิจขององค์กร มาร่วมกำหนดเป็นประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วย โดยสามารถกำหนดกรอบการบริหาร ดังนี้

4.1 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) คือ ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้ หรือมีการเปลี่ยนแปลงเทคโนโลยีหรือนวัตกรรมต่าง ๆ อย่างเฉียบพลัน (Disruptive Technology / Disruptive Innovation) เช่น Internet of Things (IoT), Blockchain, Big Data เป็นต้น ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะมีองค์ประกอบที่สำคัญ 3 ประการ ได้แก่ แผนงานการใช้เทคโนโลยีสารสนเทศ การตัดสินใจในการนำเทคโนโลยีสารสนเทศมาใช้ และการวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน ระบบงาน เหตุการณ์ภายนอก หรือคน (เจ้าหน้าที่ บุคคลภายนอก หรือลูกค้า) ซึ่งส่งผลกระทบต่อการดำเนินงานของสำนักงาน

4.2 ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Type of Risk) สามารถจำแนกออกได้เป็น 8 ประเภทดังนี้

4.2.1 ความเสี่ยงด้านข้อมูล (Information Risk) หมายถึง ความเสี่ยงที่เกิดจากข้อมูลต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาดโดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้เกิดการฟ้องร้องได้ หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ยังรวมไปถึงความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back Up) ที่สำคัญคือ เพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูลสำรอง (Information Back-Up) การกู้คืนข้อมูล (Information

Recovery) ซึ่งเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่อง (Business Continuity Plan) และแผนกู้คืนข้อมูล (Disaster Recovery Plan)

4.2.2 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ความเสี่ยงในเรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงาน และขององค์กร ที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการและเหมาะสมกับงบประมาณ หรือความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงจากการที่อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุไปเอง ความเสี่ยงจากการไม่ได้กำหนดหรือกำหนดกระบวนการอนุมัติใช้อุปกรณ์เทคโนโลยีสารสนเทศไม่ชัดเจน

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

4.2.4 ความเสี่ยงด้านบุคลากร (People Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ในเรื่องของการกำหนดโครงสร้าง การมอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศ ที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ทั้งนี้ ยังรวมถึงการที่ขาดแผนการฝึกอบรมด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่ของสำนักงาน อย่างทั่วถึง ทั้งในส่วนของผู้ดูแลระบบ (Administration) ผู้พัฒนาระบบ (Developer/Programmer) และผู้ใช้งานทั่วไป (User) อย่างสม่ำเสมอ

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

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

4.2.7 ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้ เป็นต้น

4.2.8 ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) หมายถึง ความเสี่ยงที่เกิดจากกระบวนการทำงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ซึ่งส่งผลให้ขาดการนำ Best Practice ที่ดี มาใช้งาน โดย COBIT 5 กำหนดกระบวนการที่เป็นมาตรฐานที่ดีไว้จำนวน 37 กระบวนการ และ กำหนด Best Practice ของกระบวนการต่าง ๆ ไว้ให้ การขาดการนำ Best Practice เหล่านั้นมาใช้งานอาจทำให้องค์กรไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่มาตรฐานดังกล่าวได้กำหนดไว้ ซึ่ง COBIT 5 ได้กำหนดเป้าหมายทางธุรกิจสำหรับการนำเทคโนโลยีสารสนเทศมาใช้งานไว้จำนวน 17 เป้าหมาย

5. องค์ประกอบการบริหารความเสี่ยง

5.1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

สำนักงานได้จัดให้มีกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้เป็นไปตามหลักมาตรฐานสากลและเป็นมาตรฐานเดียวกันทั่วทั้งสำนักงาน เช่นเดียวกับกระบวนการบริหารความเสี่ยงด้านอื่น ๆ โดยจะครอบคลุมการปฏิบัติงานในทุกระดับชั้นของแต่ละหน่วยงานในสำนักงาน เพื่อช่วยให้การดำเนินงานเกิดผลดีและปฏิบัติงานได้ตามกฎระเบียบที่เกี่ยวข้อง ซึ่งการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการวิเคราะห์สภาพแวดล้อมภายในองค์กร และภายนอกที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงในเทคโนโลยีสารสนเทศ จากการที่ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ที่ได้รับมอบหมายให้ดำเนินการตามภารกิจทั้ง 9 ด้าน เป็นการขับเคลื่อนการพัฒนารัฐบาลดิจิทัลภายใต้วิสัยทัศน์ “นำภาครัฐสู่การเป็นรัฐบาลดิจิทัล”ที่สอดคล้องกับ ทิศทางและแนวทางการดำเนินงานที่สอดคล้องกับการขับเคลื่อนประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand) ซึ่งถือเป็นส่วนหนึ่งของนโยบายการพัฒนาเศรษฐกิจและสังคมดิจิทัล ที่กำลังดำเนินการปฏิรูปประเทศในทุกมิติ รวมถึงสอดคล้องตามทิศทางและกรอบยุทธศาสตร์ของแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 (พ.ศ. 2566 – 2570) โดยมีรายได้หลักมาจากงบประมาณนั้น

ดังนั้น การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินงานที่เกี่ยวกับเทคโนโลยีสารสนเทศที่ให้บริการกับลูกค้า และเทคโนโลยีสารสนเทศภายในของสำนักงาน มีเสถียรภาพและความมั่นคง รวมทั้งมีประโยชน์สำหรับตัดสินใจในการดำเนินธุรกิจอิเล็กทรอนิกส์ของสำนักงาน ผู้บริหารและหน่วยงานที่เกี่ยวข้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศจะต้องร่วมกันกำหนดและทบทวนกลยุทธ์อย่างสม่ำเสมอ เพื่อกำหนดแผนปฏิบัติการ (Action Plan) ในการพัฒนางานเพื่อป้องกันและลดความเสียหายที่อาจจะเกิดขึ้นรวมถึงช่วยให้สามารถบรรลุเป้าหมายและวัตถุประสงค์ของแผนดำเนินงาน

ทั้งนี้ การวิเคราะห์สภาพแวดล้อมต้องคำนึงถึงปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อสำนักงาน หรือหน่วยงานที่เกี่ยวข้องกับนโยบายหลัก เนื่องจากการวิเคราะห์ถึงสภาพแวดล้อมทั้งภายในและภายนอก (SWOT Analysis) จะทำให้สำนักงานทราบถึงปัจจัยเสี่ยงที่จะส่งผลกระทบต่อความสำเร็จของสำนักงาน ช่วยให้ทราบว่าต้องบริหารจัดการอย่างไร เพื่อสร้างเสถียรภาพ ความมั่นคง และความน่าเชื่อถือของเทคโนโลยีสารสนเทศเมื่อต้องเผชิญกับสภาพการเปลี่ยนแปลงที่รวดเร็ว

5.2 การกำหนดวัตถุประสงค์/เป้าหมาย (Objective Setting)

กรอบการบริหารความเสี่ยง COSO ERM Framework ที่กำหนดไว้ มีวัตถุประสงค์มุ่งเน้นในเรื่องของการจัดการและควบคุมความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ที่มีผลมาจากความผิดพลาดหรือการ

ปฏิบัติที่ไม่เป็นไปตามแผนงานโครงการด้านเทคโนโลยีสารสนเทศ หรือการปฏิบัติตามกฎหมาย กฎระเบียบต่าง ๆ ที่จะส่งผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานที่เกี่ยวข้อง เช่น สำนักนายกรัฐมนตรี กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ มาตรฐานความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ เป็นต้น

5.3 การระบุเหตุการณ์ (Event Identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องกับโครงการและกิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อสำนักงาน ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

การระบุความเสี่ยงประกอบด้วยคำศัพท์พื้นฐาน 2 คำ ได้แก่

1. ภัยคุกคาม (Threat) หมายถึง ภัยที่มีผลในทางลบต่อสินทรัพย์สารสนเทศ และการดำเนินธุรกิจขององค์กรในลักษณะใดลักษณะหนึ่ง เช่น ไวรัสซึ่งเป็นภัยชนิดหนึ่ง เมื่อภัยนี้เกิดขึ้นจริง จะทำให้ธุรกิจขององค์กรเกิดการหยุดชะงักได้
2. จุดอ่อนหรือช่องโหว่ (Vulnerability) หมายถึง สภาพหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ และหากถูกใช้ให้เป็นประโยชน์ โดยภัยคุกคามก็อาจทำให้สินทรัพย์สารสนเทศขององค์กรได้รับความเสียหายได้

โดยในบริบท เมื่อมีการระบุความเสี่ยงหนึ่ง เช่น ความเสี่ยงเรื่องของไวรัส จะมีความเกี่ยวข้องกับภัยคุกคามหนึ่ง ซึ่งในที่นี้ก็คือไวรัส และโดยทั่วไปหากความเสี่ยงนั้นจะเกิดขึ้นได้ จะต้องมีการใช้ประโยชน์จากจุดอ่อนหนึ่ง เช่น ไวรัสจะใช้ประโยชน์จากการที่ผู้ใช้งานไม่ได้ติดตั้งซอฟต์แวร์ป้องกันไวรัสไว้ในเครื่อง เป็นต้น

โดยสรุป ความเสี่ยงหนึ่งที่มีการระบุขึ้นจะต้องบ่งชี้ได้ว่ามีความเกี่ยวข้องกับภัยคุกคามอะไรและภัยคุกคามนั้นจะใช้จุดอ่อนใดมาทำให้เกิดความเสียหายขึ้น

วิธีการในการระบุความเสี่ยงมีหลายวิธี ได้แก่

(1) การระดมสมองของผู้ปฏิบัติงานที่เกี่ยวข้อง

(2) การใช้ Checklist เพื่อใช้ตรวจสอบหาจุดอ่อน เช่น Checklist ของมาตรฐาน ISO/IEC 27001, COBIT5 หรือ CCM ของ CSA-STAR เป็นต้น

(3) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

(4) การวิเคราะห์กระบวนการทำงานด้านเทคโนโลยีสารสนเทศเมื่อเทียบกับกระบวนการของมาตรฐานสากลเช่น COBIT5, ITIL, CMMI, CSA-STAR เป็นต้น

ตัวอย่าง การระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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 ด้วยโดยได้รับสิทธิเป็นผู้ดูแลระบบ
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	อุปกรณ์ของระบบ Cloud ของผู้ให้บริการ ไม่สามารถใช้งานได้ ทำให้เกิดผลกระทบกับสัญญาที่ทำไว้กับลูกค้า	ขาดการจัดทำหรือทบทวนสัญญา Maintenance Agreement (MA) กับทาง Supplier
ความเสี่ยงด้านผู้ให้บริการภายนอก	บริการของสำนักงาน ที่ได้รับการพัฒนาจากผู้ให้บริการภายนอกพัฒนาได้ไม่เต็มศักยภาพ และตามความต้องการของสำนักงาน	มีข้อจำกัดในการเลือกใช้ผู้ให้บริการเนื่องจากมีผู้ให้บริการมีน้อยราย

5.4 การประเมินความเสี่ยง (Risk Assessment)

ในการประเมินความเสี่ยงโดยทั่วไปเกณฑ์การประเมินความเสี่ยงจะประกอบด้วยองค์ประกอบ 2 ส่วนคือ

- โอกาสการเกิดขึ้นของความเสี่ยง (Likelihood) ซึ่งหมายถึง ความเป็นไปได้ที่ความเสี่ยงที่ผู้ประเมินสนใจจะเกิดขึ้น
- ระดับความรุนแรงของผลกระทบ (Impact) ซึ่งหมายถึง ความเสี่ยงนั้นหากเกิดขึ้นจะมีความรุนแรง ในระดับใด

เกณฑ์การประเมินความเสี่ยง (โอกาส และ ผลกระทบ)

โอกาสการเกิดขึ้นของความเสี่ยง Cyber Security (Likelihood)

ปัจจัย	ระดับโอกาส				
	1=เกิดยาก	2=ไม่น่าเป็นไปได้	3=เป็นไปได้	4=มีแนวโน้ม	5=มีแนวโน้มสูง
จุดอ่อนของทรัพย์สินสารสนเทศ (Discoverability (D)) : ผู้ไม่หวังดีสามารถค้นพบจุดอ่อนของทรัพย์สินสารสนเทศ	- สามารถค้นพบได้โดยการ**อ่าน Source Code** - สามารถค้นพบและโจมตีได้จากการ**เข้าถึงด้านกายภาพ (Physical)**	- สามารถค้นพบได้**โดยการเข้าใช้งาน** - สามารถค้นพบและโจมตีได้จากการ**เข้าถึงระบบแบบเครือข่ายเดียวกัน (Local Area Network)**	- สามารถค้นพบได้**โดยตรวจสอบการตอบสนอง พฤติกรรม และการสื่อสารของเป้าหมาย (network sniffing)** - สามารถค้นพบและโจมตีได้จาก**ภายในเครือข่ายย่อย (Subnet Addresses) หรือเครือข่ายเดียวกัน (Local Area Network)**	- สามารถค้นพบได้จากการ **scan port** - สามารถค้นพบและโจมตีได้จาก**เครือข่ายที่อยู่ใกล้เคียง หรือติดกัน (adjacent subnets or network segment)**	- สามารถค้นพบได้จากการ **scan Public Domain** - สามารถค้นพบและโจมตีจาก**เครือข่ายภายนอกได้ (Public Network)**
การโจมตี (Exploitability (E)) : ผู้ไม่หวังดีสามารถใช้ประโยชน์จากจุดอ่อนของระบบหรือ ทรัพย์สินสารสนเทศ	- สามารถทำได้ด้วยการเข้าถึงโดย**ใช้สิทธิ์พิเศษ (Privilege) ของเป้าหมายเช่น ระดับสิทธิadmin/SYSTEM/ root**	- สามารถทำได้ด้วยการเข้าถึงโดยใช้**สิทธิ์พิเศษ (Privilege) ของเป้าหมายเช่น ระดับสิทธิadmin/SYSTEM/ root**	- สามารถทำได้ด้วยการเข้าถึงโดย**ใช้สิทธิ์พิเศษ (Privilege) ของเป้าหมายเช่น ระดับสิทธิadmin/SYSTEM/ root**	- สามารถทำได้โดยการ**จำกัดสิทธิ์การเข้าถึงของเป้าหมาย** - สามารถทำได้ด้วยเครื่องมือที่เผยแพร่เป็นสาธารณะ โดย**มี**	- สามารถทำได้โดย **ไม่มีสิทธิ์การเข้าถึงของเป้าหมาย** - สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดย

ปัจจัย	ระดับโอกาส				
	1=เกิดยาก	2=ไม่น่าเป็นไปได้	3=เป็นไปได้	4=มีแนวโน้ม	5=มีแนวโน้มสูง
	รวมถึง multi factor authentication - สามารถทำได้ด้วยเครื่องมือเฉพาะที่**ต้องใช้ความรู้ด้านเทคนิคจากผู้เชี่ยวชาญ** - สามารถเชื่อมโยงไปยังช่องโหว่ของระบบที่อยู่ใกล้เคียง	- สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็น**สาธารณะ/เครื่องมือเฉพาะโดยมีความรู้เทคนิคระดับสูง** - สามารถเชื่อมโยงไปยังช่องโหว่ของระบบที่อยู่ใกล้เคียง	- สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็น**สาธารณะ โดยมีความรู้เทคนิคระดับปานกลาง**	**ความรู้ขั้นพื้นฐาน**	**ไม่ต้องมีความรู้ด้านเทคนิค**
การโจมตีหรือบุกรุกซ้ำ (Reproducibility (R)) : ผู้ไม่หวังดีสามารถโจมตีหรือบุกรุกซ้ำบนทรัพย์สินสารสนเทศและผ่านช่องโหว่ที่มีอยู่เดิม	- ไม่สามารถ**โจมตีหรือบุกรุกซ้ำ**ได้	- ไม่สามารถ**โจมตีหรือบุกรุกซ้ำ**ได้โดย**มีเงื่อนไขเหตุการณ์จากการสุ่มหรือการคาดเดาของผู้บุกรุก** - สามารถทำซ้ำได้จาก**ทฤษฎี หรือช่องโหว่ที่มีการพิสูจน์และเผยแพร่สู่สาธารณะ**	- สามารถ**โจมตีหรือบุกรุกซ้ำ**ได้โดย**มีเงื่อนไขเหตุการณ์ที่คาดการณ์ได้** - สามารถทำซ้ำได้ด้วย**การปรับแต่งช่องโหว่เฉพาะสำหรับเป้าหมาย**	- สามารถ**โจมตีหรือบุกรุกซ้ำ**โดย**ไม่มีการกำหนดค่าบางอย่างที่เป้าหมาย** - สามารถ**โจมตีหรือบุกรุกซ้ำ**ได้ด้วยการ**ปรับแต่งช่องโหว่ที่เผยแพร่เล็กน้อย เช่น การเปลี่ยนพารามิเตอร์**	- สามารถ**โจมตีหรือบุกรุกซ้ำ**โดย **ไม่มีการกำหนดค่าหรือเงื่อนไขเหตุการณ์ใด ๆ**

หมายเหตุ: **สำหรับกรณี Cyber Security Risk Assessment**

จากตาราง สามารถคำนวณคะแนนระดับโอกาสของสถานการณ์ความเสี่ยง ได้ตามขั้นตอน ดังนี้

1. ให้ค่าคะแนนของแต่ละปัจจัย (จุดอ่อนของทรัพย์สิน (D) การโจมตี (E) และการทำซ้ำ (R))

2. เฉลี่ยคะแนนโดยปัดเศษเป็นจำนวนเต็ม (D+E+R)/3

3. คะแนนที่ปัดเศษแล้วจะเป็นโอกาสของสถานการณ์ความเสี่ยง

เช่น D=3, E=2, R=2 ดังนั้นโอกาสเกิดสถานการณ์ความเสี่ยง = (3+2+2)/3 = 2.3 => ระดับ 2

ระดับความรุนแรงของผลกระทบ (Impact)

ด้านของผลกระทบ	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านภาพลักษณ์/ชื่อเสียง/สิทธิเสรีภาพ (Reputation)	มีผลกระทบน้อยต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล หรือไม่กระทบ	มีผลกระทบต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล สามารถดำเนินการแก้ไขได้	มีผลกระทบต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล ซึ่งคาดว่าไม่สามารถดำเนินการแก้ไขได้ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	มีผลกระทบมากต่อชื่อเสียงของสำนักงาน หรือ หรือสิทธิเสรีภาพของบุคคล และเกิดความไม่พอใจจากบุคคล หรือผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทำให้สำนักงานต้องติดต่อเพื่อขอชี้แจงต่อบุคคลหรือผู้มีส่วนได้ส่วนเสีย หรือประกาศชี้แจงผ่าน Social Media	มีผลกระทบมากต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล และเกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ ทำให้สำนักงานต้องดำเนินการแถลงข่าว
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านการเงิน (Finance)	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) น้อยกว่า 5 แสนบาท	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 5 แสนบาท แต่ไม่เกิน 1 ล้านบาท	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 1 ล้านบาท แต่ไม่เกิน 50 ล้านบาท	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 50 ล้านบาท แต่ไม่เกิน 100 ล้านบาท	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) มากกว่า 100 ล้านบาท

ด้านของผลกระทบ	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านผู้ใช้บริการและด้านการดำเนินงาน (User and Operation)	ระบบสามารถให้บริการได้อย่างสมบูรณ์ หรือทุกเหตุการณ์ที่เกิดเหตุขัดข้องสามารถให้บริการในส่วนของฟังก์ชันหลักได้ โดยระยะเวลาที่แก้ไขเฉลี่ยไม่เกิน 4 ชั่วโมงต่อเดือน	ทุกเหตุการณ์ที่เกิดเหตุขัดข้องสามารถให้บริการในส่วนของฟังก์ชันหลักได้ โดยระยะเวลาที่แก้ไขเฉลี่ยตั้งแต่ 4 ชั่วโมง - ไม่เกิน 1 วัน ต่อเดือน	มีบางเหตุการณ์ที่เกิดเหตุขัดข้องและไม่สามารถให้บริการได้ โดยระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าวเฉลี่ย ไม่เกิน 2 ชั่วโมง ต่อเดือน	มีบางเหตุการณ์ที่เกิดเหตุขัดข้อง และไม่สามารถให้บริการได้ โดยระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าวเฉลี่ย 2 - 4 ชั่วโมง ต่อเดือน	มีบางเหตุการณ์ที่เกิดเหตุขัดข้อง และไม่สามารถให้บริการได้ โดยเป็นระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าวเฉลี่ย มากกว่า 4ชั่วโมง ต่อเดือน
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านผู้ใช้บริการและด้านการดำเนินงาน (User and Operation)	มีผลกระทบต่อจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **น้อยกว่า 1,000 คน และไม่มีผลกระทบต่อภาพลักษณ์ สพร. โดยสามารถจัดการได้ตาม SLA** หรือ	มีผลกระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **ตั้งแต่ 1,000 - 1,999 คน และไม่มีผลกระทบต่อภาพลักษณ์ สพร. โดยสามารถจัดการได้ตาม SLA** หรือ	มีผลกระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **ตั้งแต่ 2,000 - 4,999 คน โดยอยู่ในช่วงระยะเวลาทำการในการให้บริการตาม SLA** หรือ	มีผลกระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **ตั้งแต่ 5,000 - 9,999 คน โดยอยู่ในช่วงระยะเวลาทำการในการให้บริการตาม SLA**หรือ	มีผลกระทบกับจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **มากกว่า 10,000 คนโดยอยู่ในช่วงระยะเวลาทำการในการให้บริการตาม SLA** หรือ

ด้านของผลกระทบ	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
	ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย หรือ	มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 100-200 คน หรือ	มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 200 - 500 คน หรือ	มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 500 - 1,000 คน หรือ	มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยมากกว่า 1,000 คน หรือต่อชีวิตตั้งแต่ 1 คนขึ้นไป หรือ
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านผู้ใช้บริการและด้านการดำเนินงาน (User and Operation)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบ **เล็กน้อย**ต่อสำนักงาน หรือบุคคล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบ **อย่างจำกัด**ต่อสำนักงาน หรือบุคคล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบ **ปานกลาง**ต่อสำนักงาน บุคคล หรือประเทศชาติ	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบ **ร้ายแรง**ต่อสำนักงาน บุคคล หรือประเทศชาติ	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบ **ร้ายแรงมาก**ต่อสำนักงาน บุคคล หรือประเทศชาติ

ด้านของผลกระทบ	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านกฎหมายหรือระเบียบข้อบังคับที่สำนักงานต้องปฏิบัติตาม (Compliance)	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบ ข้อบังคับที่สำนักงานต้องปฏิบัติตาม **แต่ไม่เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญ หรือต่อบุคคลอื่น**	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบ ข้อบังคับที่สำนักงานต้องปฏิบัติตาม **ทำให้เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญ หรือต่อบุคคลอื่น**	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบ ข้อบังคับที่สำนักงานต้องปฏิบัติตาม ทำให้ **เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญ และเกิดความเสียหายต่อสำนักงานหรือต่อบุคคลอื่น**	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบ ข้อบังคับที่สำนักงานต้องปฏิบัติตาม ทำให้ **เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญและไม่เป็นตามเป้าของ ก.พ.ร. และเกิดความเสียหายอย่างร้ายแรงต่อสำนักงานหรือต่อบุคคลอื่นจนเป็นเหตุให้สำนักงานถูกร้องเรียน**	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบ ข้อบังคับที่สำนักงานต้องปฏิบัติตาม ทำให้ **เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญและไม่เป็นตามเป้าของ ก.พ.ร. และเกิดความเสียหายอย่างร้ายแรงต่อสำนักงานหรือต่อบุคคลอื่นจนเป็นเหตุให้สำนักงานถูกฟ้องร้องดำเนินคดี**

จากตารางที่เสนอในข้างต้น สำนักงานได้กำหนดค่าระดับความเสี่ยงไว้ ดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ความรุนแรงของเหตุการณ์

ในการพิจารณาความรุนแรงของเหตุการณ์จะต้องพิจารณาจากผลกระทบทั้ง 4 ด้านร่วมกัน เช่น หากความเสี่ยงเรื่องไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่จะมีผลกระทบแต่ละด้าน ได้แก่

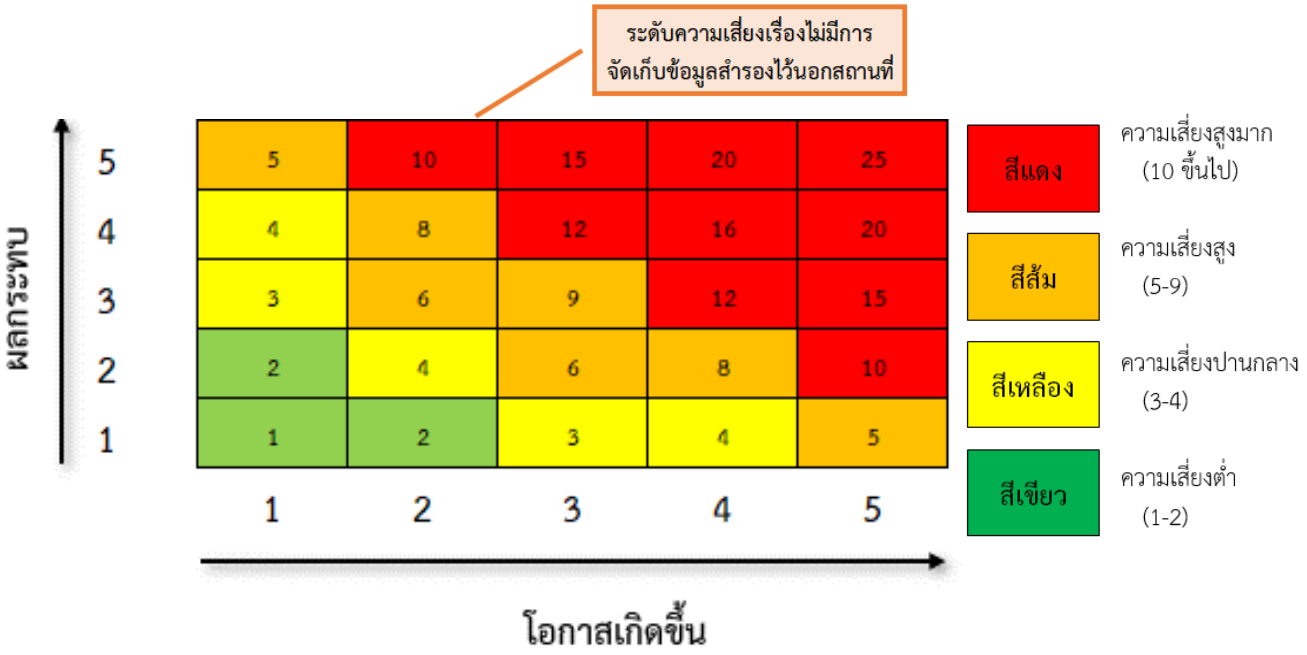
1. ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร มีผลกระทบในระดับใด
2. ผลกระทบต่อองค์กรด้านการเงิน มีผลกระทบในระดับใด
3. ผลกระทบต่อองค์กรด้านผู้ใช้บริการและด้านการดำเนินงาน มีผลกระทบในระดับใด
4. ด้านกฎหมายหรือระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม มีผลกระทบในระดับใด

และใช้ค่าผลกระทบที่มากที่สุดของผลกระทบทั้ง 4 ด้าน เป็นค่าระดับความรุนแรงของเหตุการณ์

ตัวอย่างเช่น ความเสี่ยงเรื่อง ไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่ เมื่อพิจารณาจากโอกาสการเกิดขึ้นของความเสี่ยงในตารางจะมีค่าเท่ากับ **2** และระดับความรุนแรงของผลกระทบแต่ละด้านคือ

1. ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร มีผลกระทบในระดับ **5**
2. ผลกระทบต่อองค์กรด้านการเงิน มีผลกระทบในระดับ **2**
3. ผลกระทบต่อองค์กรด้านผู้ใช้บริการและด้านการดำเนินงาน มีผลกระทบในระดับ **4**
4. ด้านกฎหมายหรือระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม มีผลกระทบในระดับ **2**

ดังนั้น ระดับความรุนแรงของผลกระทบมากที่สุดจะมีค่าเท่ากับ **5** ทำให้ระดับความเสี่ยงของสำนักงานยังไม่เป็นที่รู้จักในหน่วยงานราชการและประชาชนอย่างทั่วถึง จึงเท่ากับ **10** ตามตาราง 2 มิติ แสดงระดับความเสี่ยงสำหรับทุกค่าที่เป็นไปได้คือ



จากการพิจารณาค่าระดับความเสี่ยงในตารางข้างต้น สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
3-4	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

ตัวอย่าง การประเมินระดับความเสี่ยง แสดงดังตารางต่อไปนี้

ประเภทความเสี่ยง	ภัยคุกคาม	ช่องโหว่	โอกาสในการเกิดเหตุการณ์	ความรุนแรงของเหตุการณ์	ระดับความเสี่ยง
ความเสี่ยงด้านข้อมูล	เมื่อเกิดเหตุภัยพิบัติกับไซต์หลักของ ผู้ให้บริการ ระบบ Cloud ที่ให้บริการกับสำนักงานอาจไม่สามารถให้บริการได้	ผู้ให้บริการไม่มีไซต์สำรอง ในการสร้างความต่อเนื่องทางธุรกิจ	1	4	4
ความเสี่ยงด้าน	เหตุการณ์หรือสถานการณ์ภายนอก	อาคารสำนักงานตั้งอยู่ในพื้นที่ใกล้ชุมชนหรือ	1	3	3

ประเภทความเสี่ยง	ภัยคุกคาม	ช่องโหว่	โอกาสในการเกิดเหตุการณ์	ความรุนแรงของเหตุการณ์	ระดับความเสี่ยง
กายภาพและสิ่งแวด ล้อม	ส่งผลให้เกิดไฟไหม้อาคารสำนักงาน	แหล่งเชื้อเพลิงซึ่งเสี่ยงต่อการเกิดไฟไหม้			
ความเสี่ยงด้านบุคลากร	ข้อมูล Log อาจถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต ก่อนที่ข้อมูล Log จะผ่านการ Hash	พนักงานซึ่งทำหน้าที่เป็นผู้ดูแล Centralized Log มีหน้าที่ในการดูแลอุปกรณ์อื่น ๆ ด้วย โดยได้รับสิทธิเป็นผู้ดูแลระบบ	1	3	3
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	ข้อมูลสำคัญของระบบ Cloud ถูกเปิดเผยผ่านการใช้งานอุปกรณ์ BYOD/ mobile device	ขาดการจัดทำนโยบายและแนวทางในการบริหารจัดการอุปกรณ์ประเภท BYOD/ mobile device	1	3	3
ความเสี่ยงด้านผู้ให้บริการภายนอก	บริการของสำนักงานที่ได้รับการพัฒนาจากผู้ให้บริการภายนอกพัฒนาได้ไม่เต็มศักยภาพ และตามความต้องการของสำนักงาน	มีข้อจำกัดในการเลือกใช้ผู้ให้บริการเนื่องจากมีผู้ให้บริการมีน้อยราย	3	2	6

5.5 การตอบสนองความเสี่ยง (Risk Response)

ในการควบคุมและบรรเทาความเสี่ยง จะขึ้นอยู่กับค่าระดับความเสี่ยงที่ประเมินและได้ค่ามานั้น ทางเลือกในการควบคุมหรือบรรเทาความเสี่ยงจะมีด้วยกัน 4 ทางเลือก ดังนี้

5.5.1 การยอมรับความเสี่ยง (Acceptance) กรณีที่ค่าระดับความเสี่ยงอยู่ในบริเวณสีเขียว ผู้ประเมินความเสี่ยงสามารถยอมรับความเสี่ยงได้ กรณีการยอมรับความเสี่ยงยังหมายรวมถึง

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

ในทั้งสองกรณีนี้หน่วยงานหรือสำนักงานจำเป็นจะต้องรายงานให้คณะกรรมการ สพร. ได้รับทราบด้วย

5.5.2 การเลี่ยงความเสี่ยง (Avoidance) คือ การหาหนทางที่เหมาะสมเพื่อหลีกเลี่ยงความเสี่ยงที่พบนั้น เช่น หากพบว่าการนำทรัพย์สินไปตั้งไว้ในบริเวณที่มีความเสี่ยงต่อการสูญหาย ก็ควรจะหลีกเลี่ยงโดยการนำไปจัดเก็บไว้ในสถานที่ที่ปลอดภัย

การตัดสินใจที่จะแลกเปลี่ยนข้อมูลสำคัญกับองค์กรหนึ่งผ่านทางระบบออนไลน์ เมื่อพบว่าองค์กรนั้นยังไม่มีมาตรการความมั่นคงปลอดภัยที่ดีเพียงพอ ก็อาจยับยั้งการตัดสินใจนั้น โดยหลีกเลี่ยงความเสี่ยงไปใช้วิธีการแลกเปลี่ยนแบบ Manual แทน

การหาหนทางที่เหมาะสมกว่า ควรพิจารณาว่าความเสี่ยงลดลงมาอยู่ในระดับที่ยอมรับได้หรือไม่ เช่น ตกอยู่ในบริเวณสีเขียวหรือไม่

5.5.3 การโอนย้ายความเสี่ยง (Transfer) คือ การให้หน่วยงานอื่นเป็นผู้รับความเสี่ยงหรือดำเนินการแทนสำนักงาน เช่น การใช้ Outsource เรื่องการพัฒนาระบบให้หน่วยงานภายนอกโดยการทำสัญญาดูแลรักษาฮาร์ดแวร์ อุปกรณ์เครือข่าย การซื้อประกันภัยจากหน่วยงานภายนอก

การโอนย้ายความเสี่ยง ควรพิจารณาว่า ผู้ดำเนินการสามารถจัดการความเสี่ยงนั้นได้เป็นอย่างดีหรือไม่ ระดับความเสี่ยงที่เกิดจากผู้ดำเนินการแทน ควรจะอยู่ในระดับที่สำนักงานยอมรับได้ หากผู้ดำเนินการแทนไม่สามารถทำได้ดี ความเสี่ยงจะตกกลับมาที่สำนักงานเอง

สำหรับกรณีการซื้อประกันภัย หน่วยงานหรือฝ่ายควรจัดการกับความเสี่ยงนั้นในระดับหนึ่งแต่อาจจะยังไม่เพียงพอ จึงเสริมด้วยการซื้อประกัน หากเหตุการณ์ความเสี่ยงยังคงเกิดขึ้นได้สำนักงานจะไม่เสียหายมากเกินไป ทั้งนี้เนื่องจากมีการจัดการไว้ในระดับหนึ่ง

5.5.4 การลดความเสี่ยง (Reduction) คือ การหาทางลดค่าความเสี่ยงที่อาจตกอยู่ในบริเวณสีเหลือง สีส้ม หรือ สีแดงก็ตาม ให้ลงมาอยู่ในระดับที่น้อยลง

กรณีที่หน่วยงานหรือฝ่ายสามารถลดความเสี่ยงลงมาอยู่ในบริเวณสีเขียวได้ หน่วยงานสามารถยอมรับความเสี่ยงได้ และไม่ต้องทำอะไรเพิ่มเติม แต่หากอยู่ในบริเวณสีเหลือง หน่วยงานยังต้องคอยคุมความเสี่ยงไว้ (เพื่อป้องกันการเลื่อนระดับไปสู่ระดับที่สูงขึ้น)

เมื่อมีการประเมินระดับความเสี่ยงในหัวข้อที่แล้ว หน่วยงานหรือฝ่ายต้องพิจารณาค่าระดับความเสี่ยงนั้นและตัดสินใจว่าจะใช้ทางเลือกใด (จาก 1 ใน 4 ทางเลือก) เพื่อจัดการกับความเสี่ยงที่ประเมินนั้น ซึ่งได้อธิบายวิธีการใช้ทางเลือกแต่ละทางเลือกไปแล้วในข้างต้น

5.6 กิจกรรมการควบคุม (Control Activities)

ส่วนบริหารความเสี่ยง และหน่วยงานที่เกี่ยวข้องหรือเป็นเจ้าของความเสี่ยง มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจะควบคุมความเสี่ยง ให้สอดคล้องกับระดับความเสี่ยง ที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการ สพร. ผ่านคณะอนุกรรมการด้านการบริหารความเสี่ยงที่ได้รับมอบหมายอย่างสม่ำเสมอ

5.7 การรายงานความเสี่ยง (Risk Reporting)

ทุกหน่วยงานของสำนักงานต้องมีการจัดทำรายงานการประเมินการควบคุมความเสี่ยงด้วยตนเอง (Risk and Control Self Assessment หรือ RCSA) อย่างน้อยปีละ 1 ครั้ง โดยจุดที่มีความเสี่ยงอยู่ในระดับที่มีนัยสำคัญและระดับสูง จะต้องมีการจัดทำ Action Plan เพื่อปิดความเสี่ยงที่เกิดขึ้นกับหน่วยงานต่อไป

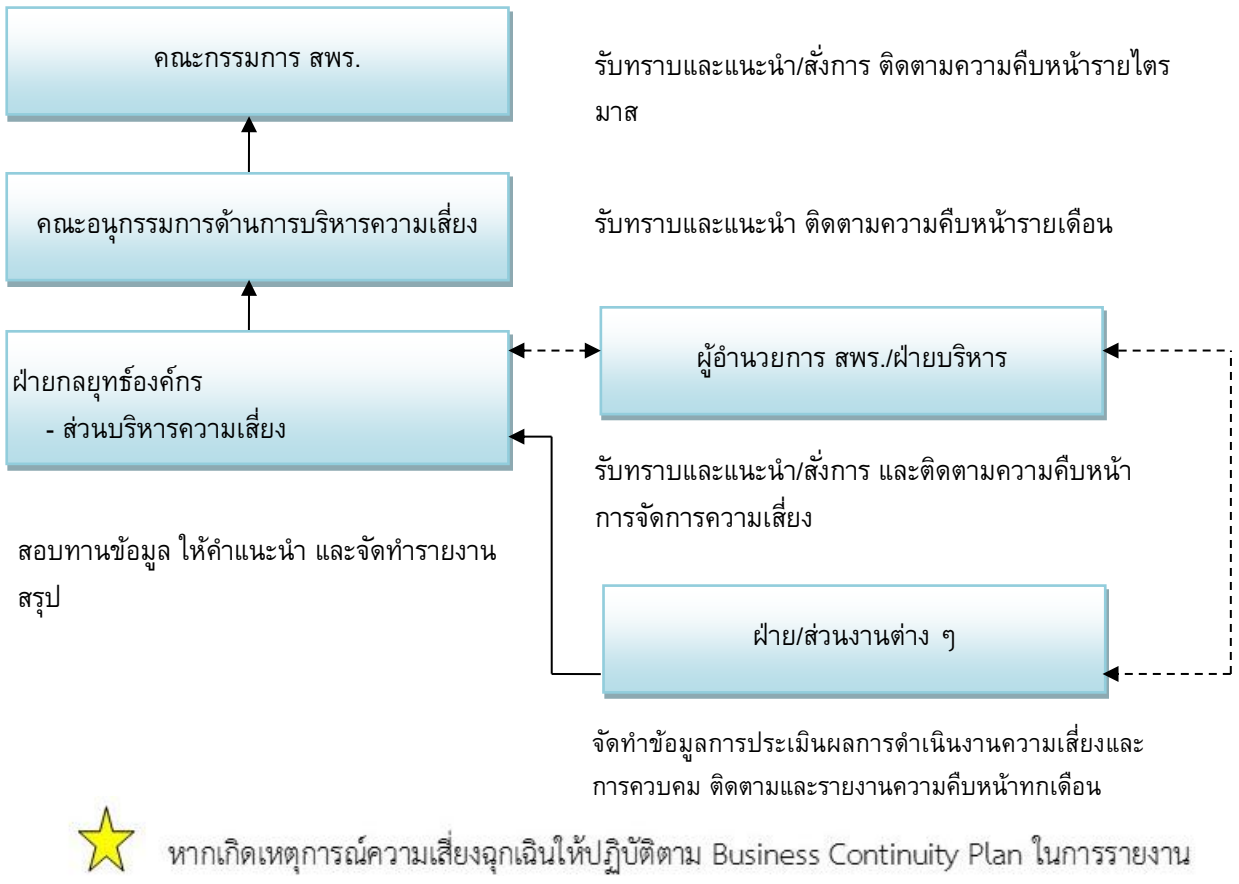
ในกรณีที่มีความความเสียหายที่เกิดจากความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Operational Loss Data) หน่วยงานต้องรายงานเหตุการณ์ความเสียหายที่เกิดจากความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นกับหน่วยงานทันทีหรือภายในวันทำการถัดไป และในกรณีที่ไม่มีเหตุการณ์ความเสียหาย หน่วยงานก็ต้องรายงานให้ส่วนบริหารความเสี่ยงทราบด้วย เพื่อให้มั่นใจว่าส่วนบริหารความเสี่ยงได้รับข้อมูลที่ถูกต้องและครบถ้วน โดยข้อมูลทั้งหมดนั้นส่วนบริหารความเสี่ยงจะรวบรวมสรุปผล และนำเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง หรือคณะอนุกรรมการ/คณะกรรมการ ที่เกี่ยวข้องต่อไป

ทั้งนี้ หากมีความเสียหายที่มีนัยสำคัญเกิดขึ้นกับหน่วยงาน หน่วยงานจะต้องมีการจัดทำ Treatment Plan เพื่อลดหรือป้องกันไม่ให้เกิดความเสียหายดังกล่าวขึ้นกับสำนักงาน ได้อีกในอนาคต และหากมีเหตุฉุกเฉินเกิดขึ้น เจ้าหน้าที่ของสำนักงานที่พบจะต้องรายงานเหตุการณ์ความเสี่ยงตามคู่มือ Business Continuity Plan ที่กำหนดไว้ และหน่วยงานที่มีความเสี่ยงอยู่ในระดับสูงหรือมีนัยสำคัญ ต้องมีการนำดัชนีชี้วัดความเสี่ยง (Key Risk Indicators: KRIs) ที่สะท้อนถึงสาเหตุและโอกาสที่จะเกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งดัชนีชี้วัดความเสี่ยงนี้ถือเป็นเครื่องมือในการวัด ติดตาม และบริหารความเสี่ยงที่สำคัญของหน่วยงาน ทั้งนี้ หน่วยงานต้องมีการรายงานดัชนีชี้วัดความเสี่ยงมายังส่วนบริหารความเสี่ยง ตามรูปแบบและระยะเวลาที่กำหนด เพื่อใช้ในการติดตามดูแลความเสี่ยงที่มีอยู่หรือที่อาจจะเกิดขึ้น

5.8 การติดตามและประเมินผล (Monitoring)

ทุกหน่วยงานต้องจัดให้มีกระบวนการในการติดตามความเสี่ยงที่มีอยู่ ตามแต่ช่วงเวลาที่เหมาะสม หรือตามการเปลี่ยนแปลงของความเสี่ยง โดยหน่วยงานควรกำหนดความถี่ในการติดตามให้มากขึ้น เช่น รายสัปดาห์ หากความเสี่ยงมีการเปลี่ยนแปลงที่มากขึ้น เป็นต้น แต่หากข้อมูลปัจจัยเสี่ยงมีการเปลี่ยนแปลงน้อยและเปลี่ยนแปลงค่อนข้างช้า หน่วยงานอาจติดตามเพียงเดือนละครั้ง ไตรมาสละครั้ง หรือปีละสองครั้ง ทั้งนี้ เพื่อให้ผู้บริหาร ผู้อำนวยการ สพร. สามารถติดตามสถานะของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีอยู่ในแต่ละช่วงเวลา และสามารถวางแผนในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นได้อย่างเหมาะสมและมีประสิทธิภาพ อีกทั้งยังช่วยให้หน่วยงานสามารถป้องกันและควบคุมเหตุการณ์ความเสียหายที่อาจเกิดขึ้นได้อย่างทันท่วงที

สรุปขั้นตอนการรายงานความเสี่ยง



ในกรณีที่เกิดเหตุการณ์ผิดปกติ ส่วนงานที่เกี่ยวข้องต้องรายงานให้ผู้บริหาร สพร. ทราบตามลำดับความรุนแรง ดังนี้

ระดับความรุนแรงและการรายงาน	ผู้อำนวยการ สพร. / ฝ่ายบริหาร	คณะอนุกรรมการด้านการบริหารความเสี่ยง	คณะกรรมการ สพร.
ปานกลาง หรือเตือน (Warning)	รับทราบ/แนะนำ และสั่งการ	รับทราบ/แนะนำ	รับทราบ/แนะนำ และสั่งการ
สูง หรือรุนแรง (Severe)	รับทราบ/แนะนำ และสั่งการรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ
สูงมาก หรือรุนแรงมาก (High Severe)	รับทราบ/แนะนำ/สั่งการ และรายงานอนุกรรมการด้านการบริหารความเสี่ยงโดยตรง พร้อมเสนอแนวทางแก้ไขทันทีที่เกิดเหตุการณ์	รับทราบ/แนะนำ และติดตามผลการดำเนินงาน	รับทราบ/แนะนำ และสั่งการ

แบบฟอร์มการรายงานและการติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยง

แบบฟอร์ม แผนและรายงานผลการบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ. 25xx

เหตุการณ์ความเสี่ยง (Event Identification)	ปัจจัยเสี่ยง (Risk Factor)	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง

ตัวชี้วัดความเสี่ยง (KRI)		
สูงกว่าเป้าหมาย	เป็นไปตามเป้าหมาย	ต่ำกว่าเป้าหมาย

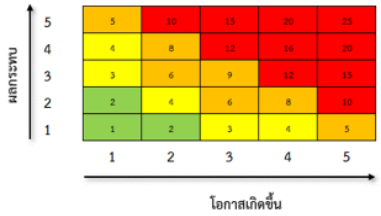
ความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ความเสี่ยงที่ยอมเบี่ยงเบนได้ (Risk Tolerance)

การควบคุมภายในที่มีอยู่	ผู้รับผิดชอบ
1.	
2.	
3.	

กิจกรรมการควบคุมเพื่อลดความเสี่ยง (เพิ่มเติม)	ระยะเวลา	ผู้รับผิดชอบ	ผลผลิต	ร้อยละความก้าวหน้าผลการดำเนินงาน	ผลการดำเนินงาน	ปัญหา/อุปสรรค	แนวทางการแก้ไข
ร้อยละความสำเร็จของการดำเนินงาน (สะสม)							

KRI	Q1		Q2		Q3		Q4	
	แผน	ผล	แผน	ผล	แผน	ผล	แผน	ผล

ชื่อปัจจัยเสี่ยง			
สถานะความเสี่ยง	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง
ระดับความเสี่ยงที่คาดหวัง			
ระดับความเสี่ยง Q1			
ระดับความเสี่ยง Q2			
ระดับความเสี่ยง Q3			
ระดับความเสี่ยง Q4			



แบบฟอร์มการติดตามผลารดำเนินงานการควบคุมภายใน

ภารกิจตามกฎหมายที่จัดตั้งหน่วยงานของรัฐหรือภารกิจตามแผนการดำเนินการหรือภารกิจอื่น ๆ ที่สำคัญของหน่วยงานของรัฐ/วัตถุประสงค์	จุดอ่อนของการควบคุมภายใน	มาตรการปรับปรุงการควบคุมภายใน	หน่วยงานที่รับผิดชอบ	ผลการดำเนินงาน

แบบฟอร์มประเมินความเพียงพอของการควบคุมภายใน และการวิเคราะห์ความเสี่ยง

1. กระบวนการ/กิจกรรม/โครงการ/บริการ (ตามขอบังคับคณะกรรมการ สพร. ว่าด้วยแบ่งส่วนงานและขอบเขตหน้าที่ของส่วนงานฯ)	ประเภทความเสี่ยงด้าน S-O-F-C			ประเภทความเสี่ยงด้าน IT Risk					10. เป็นความเสี่ยงที่มีผลกระทบต่อข้อมูลส่วนบุคคลและได้จัดทำ DPIA Identification	11. ชื่อปัจจัยเสี่ยง/ประเด็นความเสี่ยง (ภัยคุกคามและช่องโหว่)
	2. Risk Type	3. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 1	4. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 2	5. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 1 (NO. 13) *(เฉพาะ IT Risk)	6. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 2 (NO. 13) * (เฉพาะ IT Risk)	7. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 3 (NO. 13) * (เฉพาะ IT Risk)	8. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 4 (NO. 13) *(เฉพาะ IT Risk)	9. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 5 (NO. 13) *(เฉพาะ IT Risk)		

ประเภทความเสี่ยงด้าน IT Risk										14. การควบคุมภายในที่มีอยู่										15. จุดอ่อนของการควบคุมภายใน	16. การประเมินความเพียงพอของการควบคุมภายใน (เพียงพอ/ไม่เพียงพอ)	17. มาตรการปรับปรุงการควบคุมภายใน	18. กำหนดแล้วเสร็จ	19. ระบุชื่อผู้รับผิดชอบหลัก (Risk Owner)
12. ประเภทสินทรัพย์ที่ได้รับผลกระทบ *(เฉพาะ IT Risk)					13. ระดับชั้นความลับของข้อมูล *(เฉพาะ IT Risk)																			
Information	Software	Hardware	People	Service	Top Secret	Secret	Confidential	Internal Use	Public	Policy	WM / PC / WI	Action Plan	Format	Approve	Check&Balance	Monitoring	Report	Activity	Budget	Equipment	Man Power					

0						ประเภทความเสี่ยงด้าน S-O-F-C			29. สาเหตุความเสี่ยง	30. วิธีการจัดการความเสี่ยง (4T)				31. แผนจัดการความเสี่ยง/กิจกรรมที่จะดำเนินการ	32. กำหนดแล้วเสร็จ	33. ระบุชื่อผู้รับผิดชอบหลัก (Risk Owner)
20. D จุดอ่อนของทรัพย์สิน *(เฉพาะ IT Risk)	21. E การโจมตี *(เฉพาะ IT Risk)	22. R การบุกรุกซ้ำ *(เฉพาะ IT Risk)	23. โอกาสเกิด *(เฉลี่ย * (เฉพาะ IT Risk)	24. ผลกระทบ	25. ระดับความเสี่ยง	26. โอกาสเกิด S-O-F-C	27. ผลกระทบ	28. ระดับความเสี่ยง		Take	Treat	Transfer	Terminate			

เกณฑ์การประเมินความเสี่ยง (โอกาส และ ผลกระทบ)

โอกาสการเกิดขึ้นของความเสี่ยง (Likelihood)

ระดับโอกาส					
เกณฑ์	**1=เกิดยาก**	**2=ไม่น่าเป็นไปได้**	**3=เป็นไปได้**	**4=มีแนวโน้ม**	**5=มีแนวโน้มสูง**
ความถี่ในการเกิดความเสี่ยง	แทบจะไม่เกิด หรืออย่างมากปีละ 1 ครั้ง	โอกาสเกิดน้อย หรืออย่างมากไม่เกินปีละ 2 ครั้ง	ปานกลาง หรือปีละ 3-5 ครั้ง	ค่อนข้างบ่อย หรือปีละ 6-10 ครั้ง	เกิดเป็นประจำ หรืออย่างน้อยเดือนละ 1 ครั้ง
ความเป็นไปได้ในการเกิดความเสี่ยง	เป็นไปไม่ได้	ไม่มีข้อบ่งชี้หรือหลักฐานที่บ่งชี้ความเป็นไปได้ที่จะเกิดขึ้นในระยะอันใกล้	มีข้อบ่งชี้ถึงความเป็นไปได้ที่จะเกิดขึ้นในระยะอันใกล้	มีข้อบ่งชี้ที่คาดว่าจะเกิดขึ้นในระยะอันใกล้	มีข้อบ่งชี้ถึงความน่าจะเป็นสูงที่จะเกิดขึ้นในระยะใกล้
ระดับความสำเร็จของการดำเนินงาน	ร้อยละความก้าวหน้าของการดำเนินงานคิดเป็นร้อยละ 100	ร้อยละความก้าวหน้าของการดำเนินงานคิดเป็นร้อยละ 75	ร้อยละความก้าวหน้าของการดำเนินงานคิดเป็นร้อยละ 50	ร้อยละความก้าวหน้าของการดำเนินงานคิดเป็นร้อยละ 25	ร้อยละความก้าวหน้าของการดำเนินงานต่ำกว่าร้อยละ 25

โอกาสการเกิดขึ้นของความเสี่ยง Cyber Security (Likelihood)

ปัจจัย	ระดับโอกาส				
	1=เกิดยาก	**2=ไม่น่าเป็นไปได้**	**3=เป็นไปได้**	**4=มีแนวโน้ม**	**5=มีแนวโน้มสูง**
จุดอ่อนของทรัพย์สินสารสนเทศ (Discoverability (D)) : ผู้ไม่หวังดีสามารถค้นพบจุดอ่อนของทรัพย์สินสารสนเทศ	- สามารถค้นพบได้โดยการ**อ่าน Source Code** - สามารถค้นพบและโจมตีได้จากการ**เข้าถึงด้านกายภาพ (Physical)**	- สามารถค้นพบได้**โดยการเข้าใช้งาน** - สามารถค้นพบและโจมตีได้จากการ**เข้าถึงระบบแบบเครือข่ายเดียวกัน (Local Area Network)**	- สามารถค้นพบได้**โดยตรวจสอบการตอบสนองพฤติกรรม และการสื่อสารของเป้าหมาย (network sniffing)** - สามารถค้นพบและโจมตีได้จาก	- สามารถค้นพบได้จากการ **scan port** - สามารถค้นพบและโจมตีได้จาก**เครือข่ายที่อยู่ใกล้เคียง หรือติดกัน (adjacent subnets or**	- สามารถค้นพบได้จากการ **scan Public Domain** - สามารถค้นพบและโจมตีจาก**เครือข่ายภายนอกได้ (Public Network)**

ปัจจัย	ระดับโอกาส				
	1=เกิดยาก	2=ไม่น่าเป็นไปได้	3=เป็นไปได้	4=มีแนวโน้ม	5=มีแนวโน้มสูง
			ภายในเครือข่ายย่อย (Subnet Addresses) หรือเครือข่ายเดียวกัน (Local Area Network)	**network segment)**	
การโจมตี (Exploitability (E)) : ผู้ไม่หวังดีสามารถใช้ประโยชน์จากจุดอ่อนของระบบหรือ ทรัพย์สินสารสนเทศ	- สามารถทำได้ด้วยการเข้าถึงโดย**ใช้สิทธิ์พิเศษ (Privilege) ของเป้าหมายเช่นระดับสิทธิ Admin/ SYSTEM/Root รวมถึง multi factor authentication** - สามารถทำได้ด้วยเครื่องมือเฉพาะที่**ต้องใช้ความรู้ด้านเทคนิคจากผู้เชี่ยวชาญ** - สามารถเชื่อมโยงไปยังช่องโหว่ของระบบที่อยู่ใกล้เคียง	- สามารถทำได้ด้วยการเข้าถึงโดยใช้**สิทธิ์พิเศษ (Privilege) ของเป้าหมายเช่นระดับสิทธิ Admin/ SYSTEM/ Root** - สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็น**สาธารณะ/เครื่องมือเฉพาะโดยมีความรู้เทคนิคระดับสูง** - สามารถเชื่อมโยงไปยังช่องโหว่ของระบบที่อยู่ใกล้เคียง	- สามารถทำได้ด้วยการเข้าถึงโดย**ใช้สิทธิ์พิเศษ (Privilege) ของเป้าหมายเช่นระดับสิทธิ Admin/SYSTEM/ Root** - สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็น**สาธารณะ โดยมีความรู้เทคนิคระดับปานกลาง**	- สามารถทำได้โดยการ**จำกัดสิทธิ์การเข้าถึงของเป้าหมาย** - สามารถทำได้ด้วยเครื่องมือที่เผยแพร่เป็นสาธารณะ โดย**มีความรู้ขั้นพื้นฐาน**	- สามารถทำได้โดย **ไม่มีสิทธิ์การเข้าถึงของเป้าหมาย** - สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดย**ไม่ต้องมีความรู้ด้านเทคนิค**

ปัจจัย	ระดับโอกาส				
	1=เกิดยาก	2=ไม่น่าเป็นไปได้	3=เป็นไปได้	4=มีแนวโน้ม	5=มีแนวโน้มสูง
การโจมตีหรือบุกรุกซ้ำ(Reproducibility (R)) : ผู้ไม่หวังดีสามารถโจมตีหรือบุกรุกซ้ำบนทรัพย์สินสารสนเทศและผ่านช่องโหว่ที่มีอยู่เดิม	- ไม่สามารถโจมตีหรือบุกรุกซ้ำได้	- ไม่สามารถโจมตีหรือบุกรุกซ้ำได้โดยมีเงื่อนไขเหตุการณ์จากการสุ่มหรือการคาดเดาของผู้บุกรุก - สามารถทำซ้ำได้จากทฤษฎี หรือช่องโหว่ที่มีการพิสูจน์และเผยแพร่สู่สาธารณะ	- สามารถโจมตีหรือบุกรุกซ้ำได้โดยมีเงื่อนไขเหตุการณ์ที่คาดการณ์ได้ - สามารถทำซ้ำได้ด้วยการปรับแต่งช่องโหว่เฉพาะสำหรับเป้าหมาย	- สามารถโจมตีหรือบุกรุกซ้ำโดยไม่มีการกำหนดค่าบางอย่างที่เป้าหมาย - สามารถโจมตีหรือบุกรุกซ้ำได้ด้วยการปรับแต่งช่องโหว่ที่เผยแพร่เล็กน้อย เช่น การเปลี่ยนพารามิเตอร์	- สามารถโจมตีหรือบุกรุกซ้ำโดย ไม่มีการกำหนดค่าหรือเงื่อนไขเหตุการณ์ใด ๆ

หมายเหตุ: **สำหรับกรณี Cyber Security Risk Assessment**

จากตาราง สามารถคำนวณคะแนนระดับโอกาสของสถานการณ์ความเสี่ยง ได้ตามขั้นตอน ดังนี้

1. ให้ค่าคะแนนของแต่ละปัจจัย (จุดอ่อนของทรัพย์สิน (D) การโจมตี (E) และการทำซ้ำ (R))
2. เฉลี่ยคะแนนโดยปัดเศษเป็นจำนวนเต็ม (D+E+R)/3
3. คะแนนที่ปัดเศษแล้วจะเป็นโอกาสของสถานการณ์ความเสี่ยง

เช่น D=3, E=2, R=2 ดังนั้นโอกาสเกิดสถานการณ์ความเสี่ยง = (3+2+2)/3 = 2.3 => ระดับ 2

ระดับความรุนแรงของผลกระทบ (Impact)

ด้านของผลกระทบ	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านภาพลักษณ์/ชื่อเสียง/สิทธิเสรีภาพ (Reputation)	มีผลกระทบน้อยต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล หรือไม่กระทบ	มีผลกระทบต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล สามารถดำเนินการแก้ไขได้	มีผลกระทบต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล ซึ่งคาดว่าไม่สามารถดำเนินการแก้ไขได้ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	มีผลกระทบมากต่อชื่อเสียงของสำนักงาน หรือ หรือสิทธิเสรีภาพของบุคคล และเกิดความไม่พอใจจากบุคคล หรือผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทำให้สำนักงานต้องติดต่อเพื่อขอชี้แจงต่อบุคคลหรือผู้มีส่วนได้ส่วนเสีย หรือประกาศชี้แจงผ่าน Social Media	มีผลกระทบมากต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล และเกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ ทำให้สำนักงานต้องดำเนินการแถลงข่าว
ระดับความสำเร็จในการเชื่อมโยงข้อมูลตาม Agenda Base)	ความสำเร็จในการเชื่อมโยงข้อมูลตาม Agenda Base (ด้านแรงงาน สวัสดิการ และ SME) 3 ด้าน และมีรายงานการใช้ประโยชน์	ความสำเร็จในการเชื่อมโยงข้อมูลตาม Agenda Base (ด้านแรงงาน สวัสดิการ และ SME) 3 ด้าน	ความสำเร็จในการเชื่อมโยงข้อมูลตาม Agenda Base (ด้านแรงงาน สวัสดิการ และ SME) 2 ด้าน	ความสำเร็จในการเชื่อมโยงข้อมูลตาม Agenda Base (ด้านแรงงาน สวัสดิการ และ SME) 1 ด้าน	ไม่สามารถเชื่อมโยงข้อมูลตาม Agenda Base ได้ครบทั้ง 3 ด้าน
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านการเงิน (Finance)	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม)	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 5	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 1 ล้านบาท	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 50 ล้านบาท	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) มากกว่า 100 ล้านบาท

ด้านของผลกระทบ	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
	น้อยกว่า 5 แสนบาท	แสนบาท แต่ไม่เกิน 1 ล้านบาท	แต่ไม่เกิน 50 ล้านบาท	แต่ไม่เกิน 100 ล้านบาท	
จำนวนอัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio)	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) มากกว่า 5.5 เท่า	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) มากกว่า 4.5 เท่า	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) มากกว่า 3.5 เท่า	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) มากกว่า 2.5 เท่า	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) น้อยกว่า 2.5 เท่า
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านผู้ใช้บริการและด้านการดำเนินงาน (User and Operation)	ระบบสามารถให้บริการได้อย่างสมบูรณ์ หรือทุกเหตุการณ์ที่เกิดเหตุขัดข้องสามารถให้บริการในส่วนของฟังก์ชันหลักได้ โดยระยะเวลาที่แก้ไขเฉลี่ยไม่เกิน 4 ชั่วโมงต่อเดือน	ทุกเหตุการณ์ที่เกิดเหตุขัดข้องสามารถให้บริการในส่วนของฟังก์ชันหลักได้ โดยระยะเวลาที่แก้ไขเฉลี่ยตั้งแต่ 4 ชั่วโมง - ไม่เกิน 1 วัน ต่อเดือน	มีบางเหตุการณ์ที่เกิดเหตุขัดข้องและไม่สามารถให้บริการได้ โดยระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าวเฉลี่ย ไม่เกิน 2 ชั่วโมง ต่อเดือน	มีบางเหตุการณ์ที่เกิดเหตุขัดข้อง และไม่สามารถให้บริการได้ โดยระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าวเฉลี่ย 2 - 4 ชั่วโมง ต่อเดือน	มีบางเหตุการณ์ที่เกิดเหตุขัดข้อง และไม่สามารถให้บริการได้ โดยเป็นระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าวเฉลี่ย มากกว่า 4ชั่วโมง ต่อเดือน
	มีผลกระทบต่อจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **น้อยกว่า 1,000**	มีผลกระทบกับจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **ตั้งแต่ 1,000 - 1,999 คน** และไม่	มีผลกระทบกับจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **ตั้งแต่ 2,000 - 4,999 คน โดยอยู่**	มีผลกระทบกับจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **ตั้งแต่ 5,000 - 9,999 คน โดยอยู่ในช่วงระยะเวลาทำการใน**	มีผลกระทบกับจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) **มากกว่า 10,000 คนโดยอยู่ในช่วงระยะเวลาทำ**

ด้านของผลกระทบ	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
	คน และไม่มีผลกระทบต่อภาพลักษณ์ สพร. โดยสามารถจัดการได้ตาม SLA หรือ	**มีผลกระทบต่อภาพลักษณ์ สพร. โดยสามารถจัดการได้ตาม SLA** หรือ	**ในช่วงระยะเวลาทำการในการให้บริการตาม SLA** หรือ	**การให้บริการตาม SLA**หรือ	**การในการให้บริการตาม SLA** หรือ
	ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกาย หรืออนามัย หรือ	มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 100-200 คน หรือ	มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 200 - 500 คน หรือ	มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 500 - 1,000 คน หรือ	มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยมากกว่า 1,000 คน หรือต่อชีวิตตั้งแต่ 1 คนขึ้นไป หรือ
	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบ **เล็กน้อย**ต่อสำนักงาน หรือบุคคล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบ **อย่างจำกัด**ต่อสำนักงาน หรือบุคคล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบ **ปานกลาง**ต่อสำนักงาน บุคคล หรือประเทศชาติ	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบ **ร้ายแรง**ต่อสำนักงาน บุคคล หรือประเทศชาติ	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) หรือการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) หรือการหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบ **ร้ายแรงมาก**ต่อสำนักงาน บุคคล หรือประเทศชาติ

ด้านของผลกระทบ	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
ผลกระทบต่อสำนักงาน หรือบุคคลอื่น ด้านกฎหมายหรือระเบียบข้อบังคับที่สำนักงานต้องปฏิบัติตาม (Compliance)	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบข้อบังคับที่สำนักงานต้องปฏิบัติตาม **แต่ไม่เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญ หรือต่อบุคคลอื่น**	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบ ข้อบังคับที่สำนักงานต้องปฏิบัติตาม **ทำให้เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญ หรือต่อบุคคลอื่น**	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงานหรือข้อตกลง สัญญา หรือกฎหมาย ระเบียบข้อบังคับที่สำนักงานต้องปฏิบัติตาม ทำให้ **เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญ และเกิดความเสียหายต่อสำนักงานหรือต่อบุคคลอื่น**	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบ ข้อบังคับที่สำนักงานต้องปฏิบัติตาม ทำให้ **เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญและไม่เป็นตามเป้าของ ก.พ.ร. และเกิดความเสียหายอย่างร้ายแรงต่อสำนักงานหรือต่อบุคคลอื่นจนเป็นเหตุให้สำนักงานถูกฟ้องร้องดำเนินคดี**	ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับของสำนักงาน หรือข้อตกลง สัญญา หรือ กฎหมาย ระเบียบ ข้อบังคับที่สำนักงานต้องปฏิบัติตาม ทำให้ **เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญและไม่เป็นตามเป้าของ ก.พ.ร. และเกิดความเสียหายอย่างร้ายแรงต่อสำนักงานหรือต่อบุคคลอื่นจนเป็นเหตุให้สำนักงานถูกฟ้องร้องดำเนินคดี**

จากตารางที่เสนอในข้างต้น สำนักงานได้กำหนดค่าระดับความเสี่ยงไว้ ดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ความรุนแรงของเหตุการณ์

ในการพิจารณาความรุนแรงของเหตุการณ์จะต้องพิจารณาจากผลกระทบทั้ง 4 ด้านร่วมกัน เช่น หากความเสี่ยงเรื่องไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่จะมีผลกระทบแต่ละด้าน ได้แก่

5. ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร มีผลกระทบในระดับใด
6. ผลกระทบต่อองค์กรด้านการเงิน มีผลกระทบในระดับใด

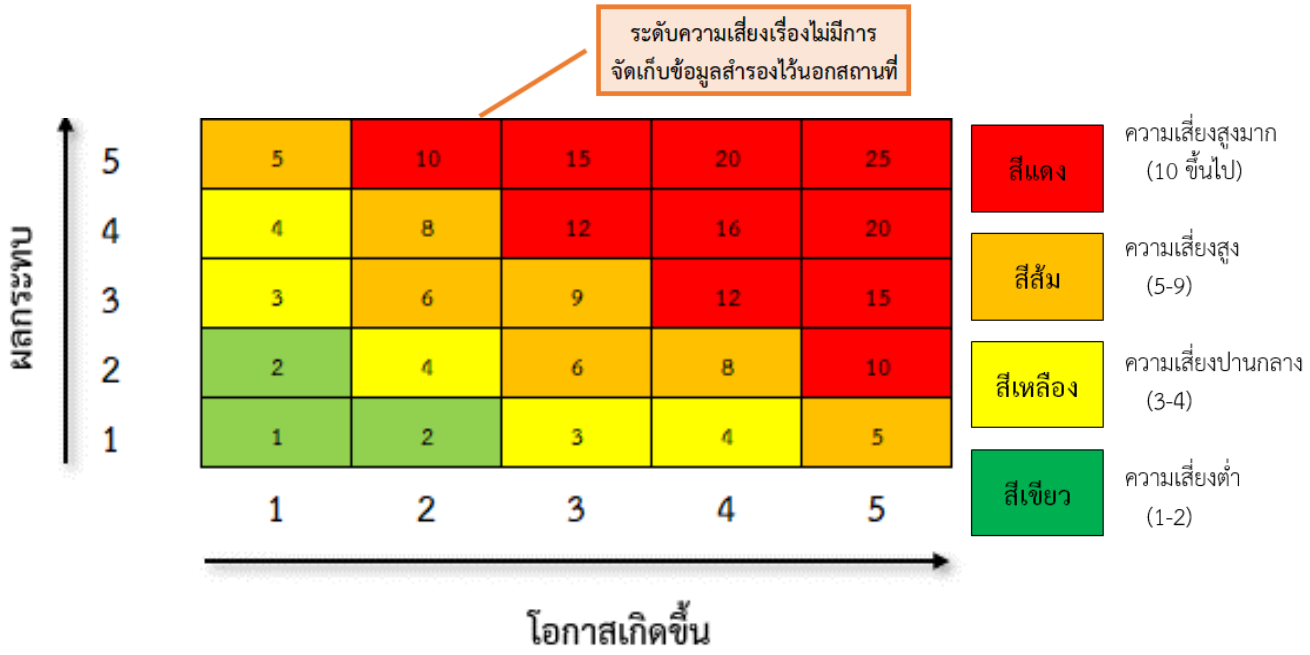
7. ผลกระทบต่อองค์กรด้านผู้ใช้บริการและด้านการดำเนินงาน มีผลกระทบในระดับใด
8. ด้านกฎหมายหรือระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม มีผลกระทบในระดับใด

และใช้ค่าผลกระทบที่มากที่สุดของผลกระทบทั้ง 4 ด้าน เป็นค่าระดับความรุนแรงของเหตุการณ์

ตัวอย่างเช่น ความเสี่ยงเรื่อง ไม่มีการจัดเก็บข้อมูลสำรองไว้นอกสถานที่ เมื่อพิจารณาจากโอกาสการเกิดขึ้นของความเสี่ยงในตารางจะมีค่าเท่ากับ **2** และระดับความรุนแรงของผลกระทบแต่ละด้านคือ

5. ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร มีผลกระทบในระดับ **5**
6. ผลกระทบต่อองค์กรด้านการเงิน มีผลกระทบในระดับ **2**
7. ผลกระทบต่อองค์กรด้านผู้ใช้บริการและด้านการดำเนินงาน มีผลกระทบในระดับ **4**
8. ด้านกฎหมายหรือระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม มีผลกระทบในระดับ **2**

ดังนั้น ระดับความรุนแรงของผลกระทบมากที่สุดจะมีค่าเท่ากับ **5** ทำให้ระดับความเสี่ยงของสำนักงานยังไม่เป็นที่รู้จักในหน่วยงานราชการและประชาชนอย่างทั่วถึง จึงเท่ากับ **10** ตามตาราง 2 มิติ แสดงระดับความเสี่ยงสำหรับทุกค่าที่เป็นไปได้คือ



จากการพิจารณาค่าระดับความเสี่ยงในตารางข้างต้น สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
3-4	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

รายงานผลการวิเคราะห์เปรียบเทียบการบริหารความเสี่ยงระหว่าง ISO 31000:2009 กับ กรอบแนวคิดของ COSO ERM

สารบัญ

หน้า

1. ที่มาของการบริหารความเสี่ยงตามแนวทางของ ISO 31000:2009

จากการประชุมหารือถึง 6 ครั้งในรอบหลายปีของคณะทำงานที่ประกอบด้วยผู้ทรงคุณวุฒิมากกว่า 20 ประเทศ ท้ายที่สุดในเดือนพฤศจิกายน ปี 2009 ที่ผ่านมาคณะทำงานก็เห็นสมควรให้มีการปรับปรุงมาตรฐานเดิมที่ใช้กันอยู่ที่เรียกกันว่า The Australia/New Zealand risk management standard (AS/NZS 4360:2004) เพื่อที่จะสามารถนำไปใช้กับองค์กรต่าง ๆ ให้หลากหลายมากยิ่งขึ้น โดยหลังจากการปรับในเนื้อหาบางส่วนของมาตรฐานเดิมแล้ว มาตรฐานการบริหารความเสี่ยงใหม่ที่ว่าถูกใช้ชื่อว่าการบริหารความเสี่ยง - หลักการและแนวทางในการปฏิบัติ (Risk Management- Principles and Guidelines) หรือที่หลาย ๆ คนรู้จักกันในนาม ISO 31000:2009

มาตรฐานการบริหารความเสี่ยงฉบับใหม่นี้อ้างอิงคำจำกัดความต่าง ๆ ตามเอกสารของ ISO Guide 73 ซึ่งถูกตีพิมพ์ในเดือนพฤศจิกายน ปี 2009 เช่นกัน โดยเอกสาร ISO Guide 73 นั้นเป็นการรวบรวมคำจำกัดความต่าง ๆ ในการบริหารความเสี่ยง

2. หลักการ กรอบแนวคิด และกระบวนการของการบริหารความเสี่ยง ตามแนวทางของ ISO 31000:2009

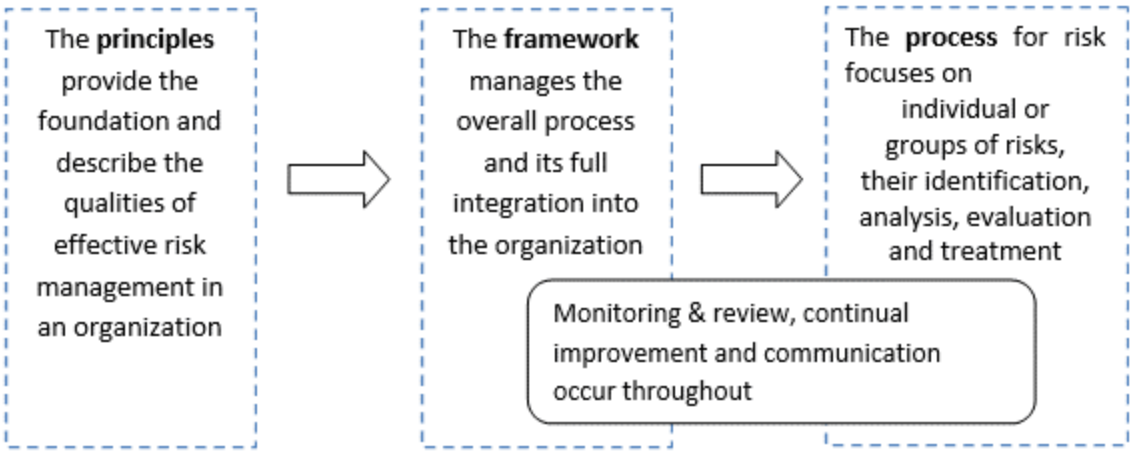
1.1 หลักการ

หลักการเบื้องต้นของการบริหารความเสี่ยงตามกระบวนการบริหารความเสี่ยงของ ISO 31000:2009 นั้นจะเน้นถึงการกำหนดเป้าหมายที่สำคัญของกระบวนการต่าง ๆ โดยที่หลักการจะสนับสนุนมุมมองของการบริหารความเสี่ยงที่ครอบคลุมและประสานกันโดยที่สามารถประยุกต์ใช้ได้ทั้งองค์กร หลักการบริหารความเสี่ยงเป็นการเชื่อมโยงระหว่างกรอบแนวคิด (Framework) และการปฏิบัติจริงที่เกิดขึ้น (Practices) เข้าด้วยกันเพื่อโยงไปยังเป้าหมายกลยุทธ์ขององค์กรผ่านกิจกรรมการบริหารต่าง ๆ ขององค์กร

1.2 กรอบแนวคิด

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

ส่วนประกอบต่าง ๆ ของกรอบแนวคิดการบริหารความเสี่ยงของ ISO 31000:2009 นั้นประกอบไปด้วยการทำความเข้าใจและการกำหนดบริบททั้งภายใน และภายนอกต่าง ๆ ที่กระทบต่อองค์กร การกำหนดนโยบายการบริหารความเสี่ยง การบูรณาการการบริหารความเสี่ยงเข้ากับกระบวนการต่าง ๆ ขององค์กร การรายงานและการสื่อสารต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก การนำกระบวนการบริหารความเสี่ยงไปปฏิบัติ การติดตามและทบทวนกระบวนการบริหารความเสี่ยง และการพัฒนากรอบแนวคิด โดยที่สามารถแสดงถึงแผนผังขั้นตอนของการบริหารความเสี่ยงตามรูปที่ 1

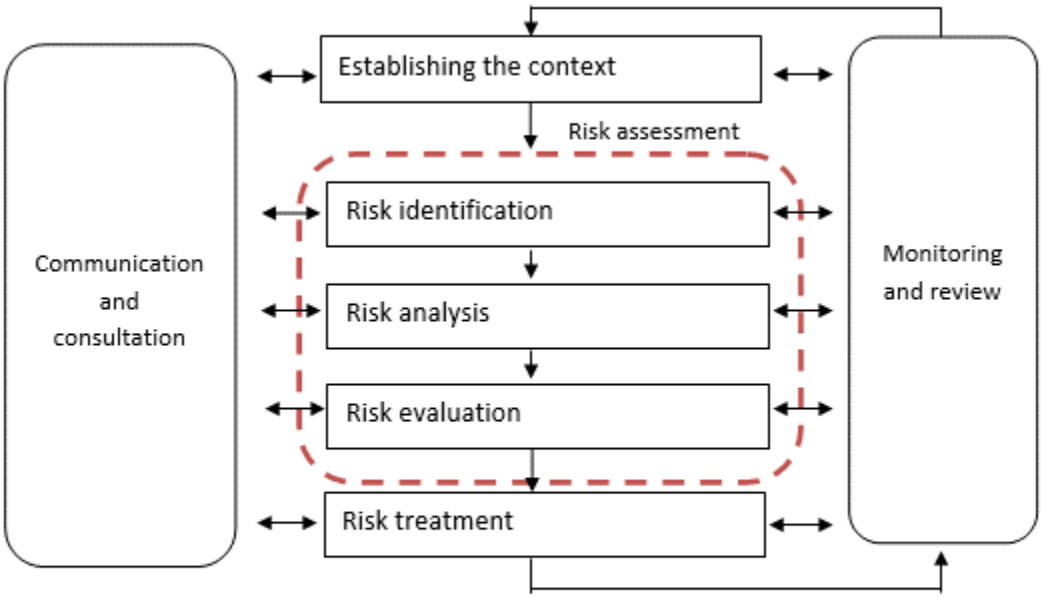


รูปที่ ๑: แผนผังขั้นตอนของการบริหารความเสี่ยง

รูปที่ 1 แสดงให้เห็นถึงขั้นตอนการทำงานของการบริหารความเสี่ยงทั้งหมด กล่าวคือ หลักการของการบริหารความเสี่ยง (principles) ทำให้เราทราบว่าพื้นฐานของการบริหารความเสี่ยงที่ดีนั้นเป็นอย่างไร เมื่อเราทราบหลักการที่ดีแล้วก็จะทำให้เราทราบถึงกรอบแนวคิด (Framework) ในการบริหารความเสี่ยงขององค์กร โดยที่กรอบแนวคิดดังกล่าวเป็นเครื่องมือในการจัดการกระบวนการบริหารความเสี่ยงทั้งหมดให้ถูกบูรณาการเข้ากับการทำงานต่าง ๆ ขององค์กร และขั้นตอนสุดท้ายคือกระบวนการบริหารความเสี่ยงจะเป็นตัวที่ให้ความสำคัญกับที่มาของการระบุปัจจัยเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินความรุนแรงของความเสี่ยง และการจัดการความเสี่ยง

1.3 กระบวนการบริหารความเสี่ยงตามแนวทางของ ISO 31000:2009

กระบวนการบริหารความเสี่ยงตามแนวทางของ ISO 31000:2009 สามารถแบ่งออกได้เป็น 5 กระบวนการหลักด้วยกันที่สอดคล้องกับกระบวนการบริหารความเสี่ยงทั่วไปที่รู้จักกัน ได้แก่ การระบุปัจจัยเสี่ยง/ความเสี่ยง การวิเคราะห์ทางเลือกในการจัดการความเสี่ยง การเลือกการตอบสนองกับความเสี่ยงที่ดีที่สุด การนำแผนบริหารความเสี่ยงไปปฏิบัติ การควบคุมและติดตามผลลัพธ์รวมทั้งการทบทวนปรับปรุงเมื่อจำเป็น ในแบบจำลองของ ISO 31000:2009 กระบวนการบริหารความเสี่ยงที่สำคัญสามารถแสดงได้ตามรูปที่ 2



รูปที่ ๒: กระบวนการบริหารความเสี่ยง

ที่ ม า : ISO 31000:2009 (E) Risk Management - Principles and Guidelines. The International Standards Organization, Geneva, Switzerland

รูปที่ 2 แสดงกระบวนการ 5 กระบวนการได้แก่ 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 และผู้มี

ส่วนได้ส่วนเสียอย่างสม่ำเสมอ (Communication and consultant) โดยที่รายละเอียดของแต่ละกระบวนการของการบริหารความเสี่ยงสามารถแสดงรายละเอียดได้ ดังนี้

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

การกำหนดบริบทต่าง ๆ ที่มีผลต่อเป้าหมายขององค์กรตามแนวทางของ ISO สามารถแบ่งได้เป็น 3 ประเภทย่อย ได้แก่ (1) การกำหนดบริบทภายนอก (Establishing the external context) เช่น กฎระเบียบข้อบังคับ วัฒนธรรม สังคม การเมือง ปัจจัยขับเคลื่อนและกระแสของสังคม และมุมมองจากคนภายนอกต่อองค์กรของเรา (2) การกำหนดบริบทภายใน (Establishing the internal context) เช่น โครงสร้างการบริหาร วัฒนธรรมองค์กร และกลยุทธ์องค์กร เป็นต้น เพื่อที่จะให้การบริหารความเสี่ยงที่เกิดขึ้นเป็นไปตามเป้าหมายขององค์กร (3) การกำหนดบริบทของกระบวนการบริหารความเสี่ยง (Establishing the context of the risk management process) เช่น การกำหนดเป้าหมายของกิจกรรมต่าง ๆ การกำหนดหน้าที่ความรับผิดชอบ การกำหนดขอบเขตของการดำเนินกิจกรรมการบริหารความเสี่ยง เป็นต้น

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

เมื่อการกำหนดบริบททุกด้านครบถ้วนแล้ว องค์กรสามารถนำข้อมูลที่มีอยู่มากำหนดเกณฑ์ในการประเมินความมีนัยสำคัญของความเสี่ยงนั้น (Risk criteria)

2. **การระบุความเสี่ยง/ปัจจัยเสี่ยง (Risk identification) :** เป็นกระบวนการระบุถึงแหล่งที่มาของความเสี่ยงนั้น ๆ ผลกระทบที่จะเกิดขึ้น จุดมุ่งหมายของกระบวนการนี้ต้องให้องค์กรสามารถสร้างชุด

ของรายการความเสี่ยงทั้งหมดซึ่งอยู่บนหลักการที่ว่าความเสี่ยงนั้นสามารถที่จะกระทบต่อการบรรลุเป้าหมายขององค์กรทั้งทางบวกและทางลบ การระบุปัจจัยเสี่ยงควรครอบคลุมทั้งปัจจัยเสี่ยงที่สาเหตุดังกล่าวสามารถจัดการได้ และไม่สามารถจัดการได้ โดยที่การระบุปัจจัยเสี่ยงอาจมาจากข้อมูลในอดีต การวิเคราะห์ทางทฤษฎี การใช้ความเห็นจาก
ผู้เชี่ยวชาญ และความต้องการของผู้มีส่วนได้ส่วนเสีย เป็นต้น อย่างไรก็ตามองค์กรควรประยุกต์ใช้เครื่องมือหรือเทคนิคของการระบุปัจจัยเสี่ยงที่เหมาะสมกับเป้าหมายขององค์กรนั้น ๆ รวมถึงความสามารถของบุคลากรในองค์กร โดยที่การได้มาซึ่งข้อมูลที่มีความถูกต้องและทันต่อเหตุการณ์มีความสำคัญอย่างมากต่อการระบุปัจจัยเสี่ยงที่สมบูรณ์

3. **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 ที่องค์กรมีอยู่ การวิเคราะห์ในส่วนนี้อาจจะเป็นเชิงปริมาณ เชิงคุณภาพ หรือเชิงกึ่งปริมาณก็ได้ ผลที่เกิดสืบเนื่องจากปัจจัยเสี่ยงใด ๆ สามารถแสดงในลักษณะของผลกระทบ (Impact) ที่จับต้องได้ เช่น ตัวเงิน ผลผลิตที่เสียหาย หรือลักษณะของผลกระทบที่จับต้องไม่ได้ เช่น ภาพลักษณ์ที่เสียหายจากมุมมองของผู้มีส่วนได้ส่วนเสีย เป็นต้น

4. **การประเมินความเสี่ยง (Risk evaluation) :** เป็นกระบวนการเพื่อช่วยในการตัดสินใจโดยอาศัยข้อมูลจากผลการวิเคราะห์ความเสี่ยงจากกระบวนการก่อนหน้าเพื่อที่จะใช้ในการพิจารณาว่าปัจจัยเสี่ยงใดที่องค์กรจำเป็นต้องมีการจัดการปัจจัยเสี่ยง (Risk treatment) นั้น รวมถึงการจัดลำดับความสำคัญก่อนหลังในการดำเนินการจัดการลดความเสี่ยงเหล่านั้น กระบวนการประเมินความเสี่ยงเป็นการเปรียบเทียบระดับความเสี่ยง (Risk level) ที่ได้จากการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยง (Risk criteria) ที่ได้มาจากกระบวนการกำหนดบริบทต่าง ๆ ที่มีผลต่อเป้าหมายขององค์กร เพื่อที่จะทำให้ทราบว่าปัจจัยเสี่ยงใดที่องค์กรยอมรับได้ ปัจจัยเสี่ยงใดที่องค์กรยอมรับไม่ได้ซึ่งต้องมีการกำหนดการจัดการความเสี่ยงต่อไป

5. **การจัดการความเสี่ยง (Risk treatment) :** เป็นกระบวนการที่เกี่ยวข้องกับการเลือกทางเลือกใดทางเลือกหนึ่ง หรือหลายทางเลือกสำหรับการลดระดับความเสี่ยง และนำแนวทางหรือทางเลือกนั้นไปปฏิบัติ โดยที่เราสามารถเรียกทางเลือกหรือแนวทางนั้นว่าการควบคุมความเสี่ยง กระบวนการจัดการความเสี่ยงเป็นกระบวนการที่เป็นวงจรหรือวัฏจักร (Cyclical) ของการประเมินการจัดการความเสี่ยง การพิจารณาว่าระดับความเสี่ยงที่เหลืออยู่ (Residual risk level) จากการจัดการความเสี่ยงนั้นยอมรับได้หรือไม่ หากรับ

ไม่ได้การจัดการความเสี่ยงใหม่ที่จะต้องเป็นอย่างไร และรวมถึงการประเมินความมีประสิทธิผลของการจัดการความเสี่ยงที่มีอยู่

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

หลักการในการเลือกแนวทางที่เหมาะสมในการจัดการความเสี่ยงนั้น เราต้องคำนึงถึงการสร้างความสมดุลระหว่างต้นทุนต่าง ๆ ที่เกิดขึ้นจากการนำแนวทางหรือมาตรการจัดการความเสี่ยงไปปฏิบัติกับผลประโยชน์ที่ได้รับเมื่อระดับความเสี่ยงของปัจจัยเสี่ยงนั้นลดลงภายในเงื่อนไขกฎระเบียบข้อบังคับ และความต้องการของผู้มีส่วนได้ส่วนเสีย อย่างไรก็ตามสิ่งที่องค์กรพึงระวังก็คือการดำเนินมาตรการจัดการความเสี่ยงที่ผิดพลาดนั้น นอกจากไม่สามารถลดระดับความเสี่ยงของปัจจัยเสี่ยงนั้นแล้ว ยังอาจก่อให้เกิดปัจจัยเสี่ยงใหม่ตามมาได้ ดังนั้นการติดตามและประเมินประสิทธิผลของการจัดการความเสี่ยงจึงจำเป็นต้องถูกผนวกเข้าเป็นเนื้อเดียวกับแผนการดำเนินงานการจัดการความเสี่ยงเพื่อสร้างความมั่นใจในประสิทธิผลที่เกิดขึ้น

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

3. กระบวนการของการบริหารความเสี่ยงตามแนวทางของ COSO ERM

ที่มา : The Committee of Sponsoring Organization of the Tread way Commission (COSO)

กระบวนการ 8 ขั้นตอนหลักประกอบด้วย

1. สภาพแวดล้อมภายในองค์กร แนวนโยบายโดยทั่วไปของสำนักงาน ซึ่งเป็นพื้นฐานที่สำคัญของกรอบการบริหารความเสี่ยง และการจัดการกับความเสี่ยง
2. การกำหนดวัตถุประสงค์และเป้าหมายที่สอดคล้องกับกลยุทธ์ของสำนักงาน
3. การระบุเหตุการณ์ การบ่งชี้และเข้าใจความเสี่ยงทั้งหมดที่มีผลกระทบต่อวัตถุประสงค์ที่กำหนดไว้
4. การประเมินความเสี่ยง โดยพิจารณาถึงผลกระทบและโอกาสเกิดความเสี่ยง
5. การตอบสนองความเสี่ยง กำหนดการจัดการความเสี่ยงที่มีอยู่ในปัจจุบัน
6. กิจกรรมการควบคุม โดยพิจารณาถึงการควบคุมเพิ่มเติมรวมทั้งความสัมพันธ์ของต้นทุนและผลประโยชน์ที่เกิดขึ้น ผู้บริหารควรนำวิธีการจัดการความเสี่ยงไปปฏิบัติและติดตาม เพื่อให้มั่นใจได้ว่า มีการดำเนินการตามวิธีการที่กำหนดไว้ กิจกรรมการควบคุม คือนโยบายและขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง
7. สารสนเทศและการสื่อการ การสื่อสารเพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่ มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง
8. การติดตามผลและรายงานความมีประสิทธิผลของกระบวนการและระบบการบริหารความเสี่ยง

4. การเปรียบเทียบแนวทางการบริหารความเสี่ยงระหว่าง ISO กับ COSO

การเปรียบเทียบระหว่างแนวทางการบริหารความเสี่ยงแบบ ISO 31000:2009 กับ COSO ERM นั้น สามารถแสดงได้ด้วยความแตกต่างที่สำคัญ ดังนี้

1.1 กรอบแนวคิดในการบริหารความเสี่ยง

กรอบแนวคิดของ COSO ERM นั้นหากเทียบกับกรอบแนวคิดของ ISO นั้นมีความซับซ้อนกว่าและอาศัยขั้นตอนต่าง ๆ ทำให้องค์กรหลายแห่งประสบกับปัญหาการนำกรอบการบริหารความเสี่ยงนี้ไปใช้ในทางปฏิบัติ ในขณะที่ ISO กำหนดกรอบแนวคิดที่ง่ายต่อความเข้าใจมากกว่าตามมุมมองของคณะทำงาน กล่าวคือกรอบแนวคิดของ 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 นั้นจะอิงเข้ากับหลักการของการตรวจสอบภายในที่อาศัยหลักการเฉพาะด้านมากกว่า ข้อดีก็คือมีขั้นตอนที่ค่อนข้างตายตัวอาจจะเหมาะกับองค์กรที่เริ่มในการบริหารความเสี่ยง อย่างไรก็ตามไม่ว่าจะเป็นกรอบแนวคิดแบบใดล้วนมีจุดมุ่งหมายในการบริหารความเสี่ยงเพื่อบรรลุเป้าหมายขององค์กรทั้งสิ้น แต่ข้อดีข้อเสียของแต่ละแนวคิดก็เป็นสิ่งที่องค์กรที่จะต้องเลือกใช้อย่างเหมาะสม

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

1.2 นิยามของคำจำกัดความ

นอกจากกรอบแนวคิดที่แตกต่างกันแล้ว เราสามารถสรุปคำจำกัดความ หรือคำอธิบายที่แตกต่างกันระหว่าง ISO และ COSO ได้ ดังนี้

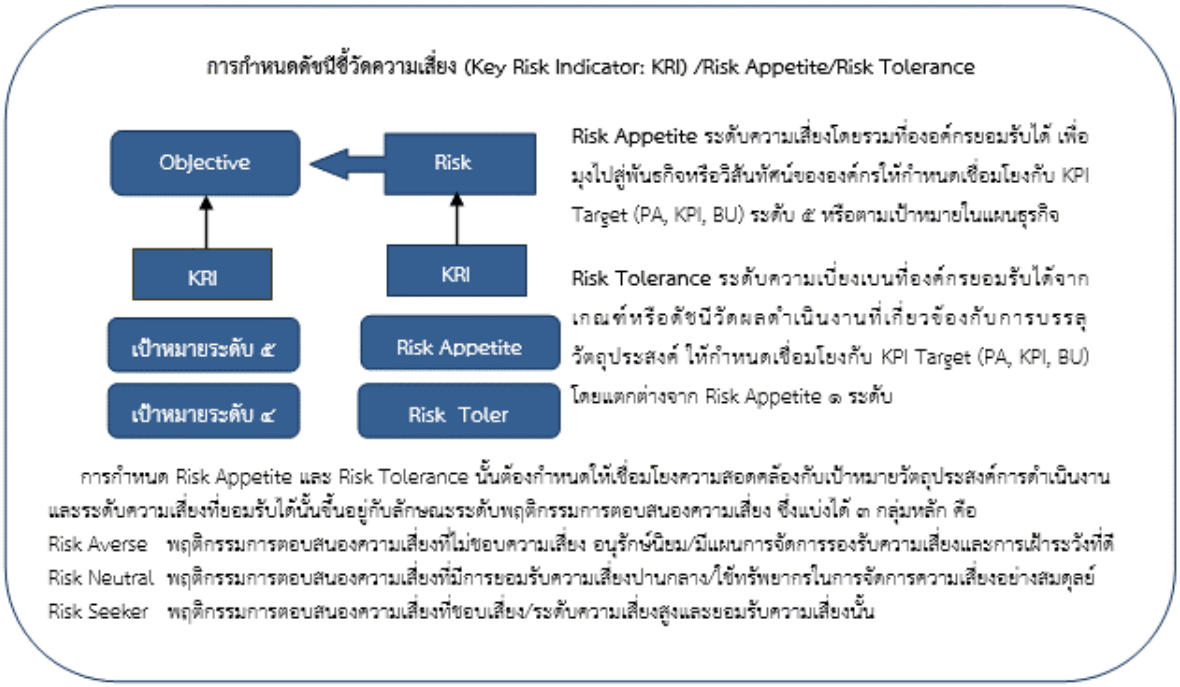
- นิยามความเสี่ยง (Risk definition) ISO ให้ความหมายไว้ว่าเป็นผลของความไม่แน่นอนที่ส่งผลต่อองค์กร ในขณะที่ COSO คือ เหตุการณ์ที่เกิดขึ้นและก่อให้เกิดผลเชิงลบต่อเป้าหมายขององค์กร

ในคู่มือการบริหารความเสี่ยงของ สรอ. ทั้งในภาพรวมและแยกเป็นคู่มือแต่ละด้าน การระบุปัจจัยเสี่ยงที่ยกตัวอย่างในคู่มือแต่ละด้าน จะมองครอบคลุมถึงมุมมองทั้งความไม่แน่นอนที่ส่งผลต่อองค์กร ทั้งนี้ ความไม่แน่นอนดังกล่าวอาจเป็นแนวคิดในเชิงการระบุความเสี่ยงเพื่อเข้าหาโอกาสที่มีอยู่ขององค์กร เช่น ความเสี่ยงด้านการเงิน ในมุมมองของรายได้นอกงบประมาณไม่เป็นไปตามเป้าหมาย ซึ่งรายได้นอกงบประมาณนั้น ไม่ถือว่าเป็นภารกิจหลักขององค์กร แต่เป็นโอกาสทางธุรกิจที่เกิดขึ้นจากการให้บริการหน่วยงานภาครัฐ ดังนั้น ความไม่แน่นอนในเชิงการเข้าหาโอกาส จึงถือเป็นการระบุปัจจัยเสี่ยงอย่างหนึ่ง รวมถึงการระบุปัจจัยเสี่ยงในการทบทวนคู่มือการบริหารความเสี่ยงของสำนักงานทั้งในภาพรวมและแยกเป็นคู่มือแต่ละด้าน พิจารณาถึงเหตุการณ์ที่เกิดขึ้นและก่อให้เกิดผลเชิงลบต่อเป้าหมายขององค์กร เช่น จำนวนหน่วยงานภาครัฐที่มาขอใช้บริการไม่เป็นไปตามเป้าหมาย การพัฒนา Data Center Consolidation ล่าช้ากว่าแผนงานที่กำหนด เป็นต้น ดังนั้น การระบุความเสี่ยงของ สรอ. 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



จากคำนิยามต่าง ๆ ตามรูปที่ 3 สะท้อนให้เห็นถึงทัศนคติต่อความเสี่ยง (Risk attitude) ที่ต่างกันระหว่าง ISO กับ COSO อย่างไรก็ตามการเลือกใช้ขึ้นอยู่กับวิธีการที่เหมาะสมกับองค์กร และความตั้งใจขององค์กรนั้นสำหรับการบริหารความเสี่ยง

Key Term or Description	ISO 31000	COSO
Scope	This International Standard provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.	This definition (of ERM) is purposefully broad. 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 on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.
Risk management, defined.	Coordinated activities to direct and control 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

Key Term or Description	ISO 31000	COSO
		risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
Risk, defined	The effect of uncertainty upon objectives.	The possibility that an event will occur and 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.
Risk assessment, defined.	The overall process of risk identification, risk analysis and risk evaluation.	Risks are analyzed, considering likelihood and 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 • Establish the context • Risk assessment: o Identification o Analysis o Evaluation • Risk treatment Continually & iteratively: Monitor and review	• Internal environment • Objective setting • Event identification • Risk assessment • Risk response • Control activities • Info & communication • Monitoring

รูปที่ 3 ตารางเปรียบเทียบความแตกต่างระหว่าง ISO และ COSO

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.

1.3 กระบวนการบริหารความเสี่ยง

ตามรูปที่ 3 แสดงให้เห็นว่าจุดต่างที่สำคัญซึ่งทำให้กระบวนการบริหารความเสี่ยงตามแนวคิดของ ISO แตกต่างจาก COSO คือ การกำหนดบริบทต่าง ๆ ที่มีผลต่อเป้าหมายขององค์กร (Establishing the context) และกระบวนการวิเคราะห์ความเสี่ยง (Risk assessment) โดยมีรายละเอียด ดังนี้

การกำหนดเป้าหมาย

	ISO	COSO
Establishing The context	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 context) เช่น โครงสร้างการบริหาร วัฒนธรรมองค์กร กลยุทธ์องค์กร และความต้องการของผู้มีส่วนได้ส่วนเสียภายใน (internal stakeholder)	COSO ไม่ได้กล่าวถึงรายละเอียดที่มาของวิธีการในการกำหนดเป้าหมายขององค์กร เพียงแต่มีการอธิบายกระบวนการคร่าว ๆ เท่านั้นว่ากระบวนการบริหารความเสี่ยงที่ดีควรมีการกำหนดเป้าหมายที่ชัดเจนโดยให้การบริหารความเสี่ยงเป็นส่วนช่วยในการบรรลุเป้าหมายนั้น

การดำเนินงานของส่วนบริหารความเสี่ยงสำหรับประเด็นดังกล่าวเพื่อให้คู่มือการบริหารความเสี่ยงของสำนักงานครอบคลุมทั้ง ISO และ COSO ERM :

การกำหนดบริบทขององค์กรในคู่มือการบริหารความเสี่ยงทั้งในภาพรวมและคู่มือการบริหารความเสี่ยงในแต่ละด้าน มีการพิจารณาครอบคลุมทุกด้านทั้งบริบทภายนอก และบริบทภายใน โดยการระบุความเสี่ยงจากบริบทนั้น จะมีการพิจารณาถึงมุมมองของผู้มีส่วนได้เสียขององค์กรประกอบด้วย

การวิเคราะห์ความเสี่ยง

	ISO	COSO
Risk assessment	ISO ให้ความหมายและอธิบายกระบวนการนี้ครอบคลุมรายละเอียดถึง 3 กระบวนการย่อยที่ต่อเนื่องกัน ได้แก่ การระบุความเสี่ยง/ปัจจัยเสี่ยง (Risk identification) เป็นกระบวนการระบุถึงแหล่งที่มาของความเสี่ยงนั้น ๆ ผลกระทบที่จะเกิดขึ้นต่อการบรรลุเป้าหมายขององค์กรทั้งทางบวกและทางลบ การวิเคราะห์ความเสี่ยง (Risk analysis) เป็นการพิจารณาผลกระทบที่สืบเนื่อง (consequence) ทั้งด้านบวกและด้านลบของปัจจัยเสี่ยงดังกล่าว รวมถึงโอกาส (likelihood) ของปัจจัยเสี่ยงที่อาจเกิดขึ้น โดยที่เมื่อเราพิจารณาผลกระทบ และโอกาสเข้าด้วยกันทำให้เราสามารถกำหนดระดับความเสี่ยง (Risk level) ของปัจจัยเสี่ยงนั้น ๆ การประเมินความมีนัยสำคัญของความเสี่ยง (Risk evaluation) เป็นกระบวนการเพื่อช่วยในการตัดสินใจโดยอาศัยข้อมูลจากผลการวิเคราะห์ความเสี่ยงจากกระบวนการก่อนหน้าเพื่อที่จะใช้ในการพิจารณาว่าปัจจัยเสี่ยงใดที่องค์กรจำเป็นต้องมีการจัดการปัจจัยเสี่ยง (Risk treatment)	การวิเคราะห์ความเสี่ยงจะพิจารณาในเรื่องของการกำหนดระดับความรุนแรงผ่านตัวโอกาสและผลกระทบ เพื่อกำหนดมาตรการบริหารความเสี่ยงสำหรับปัจจัยเสี่ยงที่องค์กรยอมรับไม่ได้

การดำเนินงานของส่วนบริหารความเสี่ยงสำหรับประเด็นดังกล่าวเพื่อให้คู่มือการบริหารความเสี่ยงของสำนักงานครอบคลุมทั้ง ISO และ COSO ERM :

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

จากที่กล่าวไว้ข้างต้นถึงรายละเอียดกระบวนการบริหารความเสี่ยงของ ISO นั้น องค์ประกอบหลักของกระบวนการที่ถือว่าทำให้ ISO แตกต่างจาก COSO คือ การกำหนดบริบทที่มีผลต่อเป้าหมายขององค์กร (Establishing the context) ตามกรอบแนวคิดของ ISO ให้ความสำคัญค่อนข้างมากกับองค์ประกอบนี้เนื่องจาก ISO เน้นการบริหารความเสี่ยงที่สามารถนำไปใช้กับองค์กรต่าง ๆ ได้อย่างหลากหลายระดับ ตั้งแต่ระดับภาพรวม ระดับสายงาน ระดับฝ่ายงาน ถึงระดับผลิตภัณฑ์จนกระทั่งถึงตัวปัจเจกบุคคล โดยที่ข้อดีคือการกำหนดบริบทที่ครอบคลุมทำให้การบรรลุเป้าหมายผ่านกระบวนการบริหารความเสี่ยงมีความเป็นไปได้สูง ส่วนข้อเสียคือ ในทางปฏิบัติการได้มาซึ่งข้อมูลหรือบริบทที่ครบถ้วนถือว่าเป็นเรื่องยาก และมีต้นทุนในการได้ข้อมูลดังกล่าวมาค่อนข้างสูง อีกทั้งการกำหนดเป้าหมายที่ลงรายละเอียดตั้งแต่องค์กร สายงาน จนถึงผลิตภัณฑ์อาจทำให้เกิดความซับซ้อนและสูญเสียทรัพยากรอย่างมาก ในขณะที่ COSO ให้ความสำคัญกับการบริหารความเสี่ยงในภาพรวมขององค์กรมากกว่าหน่วยย่อยขององค์กร ข้อดีคือง่ายต่อการบริหารจัดการ แต่ข้อเสียคืออาจทำให้การกำหนดปัจจัยเสี่ยง ไม่ครบถ้วน รวมถึง COSO ยังไม่ได้อธิบายที่มาของการกำหนดเป้าหมายในรายละเอียดเท่ากับ ISO

5. สรุป

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

แหล่งข้อมูลอ้างอิง

หน่วยงานที่เกี่ยวข้อง

1. สำนักงานคณะกรรมการพัฒนาระบบราชการ (สำนักงาน ก.พ.ร.)
2. สำนักงานการตรวจเงินแผ่นดิน
3. สำนักนายกรัฐมนตรี
4. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
5. บริษัท ทริส คอร์ปอเรชั่น จำกัด

กฎหมายที่เกี่ยวข้อง

1. พระราชกฤษฎีกา ว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี (ฉบับที่ 2) พ.ศ. 2562
2. พระราชบัญญัติ ข้อมูลข่าวสารของราชการ พ.ศ. 2540
3. พระราชบัญญัติ องค์การมหาชน (ฉบับที่ 2) พ.ศ. 2559
4. พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562
5. พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
6. พระราชบัญญัติ การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560
7. พระราชบัญญัติ การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
8. พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เว็บไซต์ที่เกี่ยวข้อง

1. www.opdc.go.th
2. www.oag.go.th
3. www.coso.org
4. www.iso.org
5. www.isaca.org
6. www.bot.or.th
7. www.itgthailand.com
8. www.sec.or.th
9. www.set.or.th
10. www.mdes.go.th
11. www.dga.or.th

คำขอบคุณจากคณะผู้จัดทำ
นโยบายและคู่มือบริหารความเสี่ยง
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ในนามของคณะผู้จัดทำนโยบายและคู่มือบริหารความเสี่ยงของสำนักงานพัฒนารัฐบาลดิจิทัล ฉบับนี้ ขอขอบพระคุณคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล คณะอนุกรรมการด้านการบริหารความเสี่ยงสำนักงานพัฒนารัฐบาลดิจิทัล ที่ปรึกษาสำนักงานพัฒนารัฐบาลดิจิทัล คณะผู้บริหาร คณะทำงาน และผู้ที่มีส่วนเกี่ยวข้องทุกท่านในการให้การช่วยเหลือและให้ความร่วมมือจนทำให้นโยบายและคู่มือบริหารความเสี่ยงของสำนักงานสามารถจัดทำขึ้นได้อย่างสมบูรณ์และสำเร็จ เพื่อให้เจ้าหน้าที่ทุกคนในสำนักงาน ใช้เป็นแนวทางในการดูแลและบริหารความเสี่ยงภายใต้ความรับผิดชอบของแต่ละคน และหวังเป็นอย่างยิ่งว่านโยบายและคู่มือบริหารความเสี่ยงฉบับนี้จะมีประโยชน์แก่ผู้ปฏิบัติงานทุกคนและผู้ที่สนใจทุกท่าน

<u>รายนามคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)</u>

1. นายนพรัตน์ เมธาวีกุลชัย ประธานกรรมการ
2. นางกรรณิการ์ งามโสภี กรรมการผู้ทรงคุณวุฒิ
   (ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : ด้านการเงิน การบัญชีและงบประมาณ การตรวจสอบประเมินผล และการบริหารความเสี่ยง)
3. นายประพันธ์ จันทร์วัฒนพงษ์ กรรมการผู้ทรงคุณวุฒิ
   (ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : ด้านการบริหารจัดการและการบริหารทรัพยากรบุคคล)
4. นายสัญญา มิตรเอม กรรมการผู้ทรงคุณวุฒิ
   (ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : ด้านเทคโนโลยีดิจิทัล)
5. นายปิยบุตร บุญอร่ามเรือง กรรมการผู้ทรงคุณวุฒิ
   (ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : ด้านกฎหมายเทคโนโลยีดิจิทัล)
6. นายประเวทย์ ตันติสัจจธรรม กรรมการผู้ทรงคุณวุฒิ
   (ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : ด้านเทคโนโลยีดิจิทัล นวัตกรรม และการเปลี่ยนผ่านสู่ดิจิทัล)
7. ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กรรมการโดยตำแหน่ง
   (นายวิศิษฏ์ วิศิษฏ์สรอรรถ)
8. เลขาธิการคณะกรรมการพัฒนาระบบราชการ กรรมการโดยตำแหน่ง
   (นางสาวอ้อนฟ้า เวชชาชีวะ)
9. ผู้แทนผู้อำนวยการสำนักงบประมาณ กรรมการโดยตำแหน่ง
   (นายกรณินทร์ กาญจโนมัย รองผู้อำนวยการสำนักงบประมาณปฏิบัติราชการแทนผู้อำนวยการสำนักงบประมาณ)
10. นายชัย วุฒิวิวัฒน์ชัย กรรมการโดยตำแหน่ง
    (ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติปฏิบัติการแทนผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ)
11. ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล กรรมการและเลขานุการ
    (นายสุพจน์ เธียรวุฒิ)

รายนามคณะอนุกรรมการบริหารความเสี่ยง

1. นายกรณินทร์ กาญจโนมัย	ประธานอนุกรรมการ
2. พลตรีเจียรนัย วงศ์สอาด	อนุกรรมการ
3. นายประเสริฐ อัครประถมพงศ์	อนุกรรมการ
4. นางสาวรสา กาญจนสาย	อนุกรรมการ
5. นายสุจินดา สุขุม	อนุกรรมการ
6. ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล	อนุกรรมการ
7. ผู้อำนวยการฝ่ายกลยุทธ์องค์กร	เลขานุการ
8. ผู้จัดการส่วนบริหารความเสี่ยง	ผู้ช่วยเลขานุการ

รายนามคณะผู้บริหาร

1. นายสุพจน์ เธียรวุฒิ	ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
2. นางไอรดา เหลืองวิไล	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
3. นางสาวอภิณห์พร อังคกมลเศรษฐ์	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
4. นายณัฐวัชร์ วรนพกุล	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
5. นายอาศิส อัญญะโพธิ์	ผู้ช่วยผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
6. นายชรินทร์ ธีรฐิตยางกูร	ผู้อำนวยการฝ่ายขับเคลื่อนนโยบายรัฐบาลดิจิทัล
7. นางสาวทิสวรรณ ชูปัญญา	ผู้อำนวยการฝ่ายกลยุทธ์องค์กร
8. นายพิชัย ร่วมภูมิสุข	ผู้อำนวยการสำนักเลขานุการผู้อำนวยการ
9. นางคณาพร สนธยานนท์	ผู้อำนวยการฝ่ายบริหารกลาง
10. นายบรรเจิด พรหมโสภา	ผู้อำนวยการฝ่ายบัญชีและการเงิน
11. นายอุสรา วิสารทานนท์	ผู้อำนวยการฝ่ายที่ปรึกษาและบริหารโครงการ
12. นายมนต์ศักดิ์ โซ่เจริญธรรม	ผู้อำนวยการสถาบันนวัตกรรมและธรรมาภิบาลข้อมูล
13. นางสาวอุรัชฎา เกตุพรหม	ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ
14. นายสุพัชรินทร์ กิ่งแก้ว	ผู้อำนวยการฝ่ายพัฒนาแพลตฟอร์มดิจิทัลแลกเปลี่ยนข้อมูล
15. นายปณิธาน เขินอำนวย	ผู้อำนวยการฝ่ายความมั่นคงปลอดภัยทางไซเบอร์
16. นายธนกร ศรีคำดี	ผู้อำนวยการฝ่ายตรวจสอบภายใน
17. นายวิจักขณ์ ซื่อวาจา	ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

18. นายเกียรติศักดิ์ เรืองรอด	ผู้อำนวยการฝ่ายปฏิบัติการดิจิทัล
19. นางสาวณัฏฐ์ฉัตร จันทร์แสงศรี	ผู้อำนวยการฝ่ายวิจัยและพัฒนานวัตกรรมดิจิทัล
20. นายอธิบดี ลิมสัมพันธ์สันติ	รักษาการผู้อำนวยการฝ่ายพัฒนาแพลตฟอร์ม
ดิจิทัล	
	ประชาชน

<u>รายนามคณะผู้จัดทำ</u>

1. นางสาวทิสวรรณ ชูปัญญา	ผู้อำนวยการฝ่ายกลยุทธ์องค์กร
2. นายภัทรพงศ์ วงศ์สุวัฒน์	ผู้จัดการส่วนบริหารความเสี่ยง
3. นางสาวสิรีพิชญ์ สุขผล	นักวิเคราะห์อาวุโส 1

<u>ออกแบบโดย</u>

1. นางสาวทิสวรรณ ชูปัญญา	ผู้อำนวยการฝ่ายกลยุทธ์องค์กร
2. นายภัทรพงศ์ วงศ์สุวัฒน์	ผู้จัดการส่วนบริหารความเสี่ยง
3. นางสาวสิรีพิชญ์ สุขผล	นักวิเคราะห์อาวุโส 1

<u>ปรับปรุง</u> ครั้งที่ 1 เดือนพฤศจิกายน 2557
ครั้งที่ 2 เดือนกันยายน 2558
ครั้งที่ 3 เดือนพฤศจิกายน 2559
ครั้งที่ 4 เดือนตุลาคม 2560
ครั้งที่ 5 เดือนมิถุนายน 2562
ครั้งที่ 6 เดือนกรกฎาคม 2565
ครั้งที่ 7 เดือนเมษายน 2566

สำนักงานพัฒนารัฐบาลดิจิทัล
(องค์การมหาชน)

DIGITAL GOVERNMENT DEVELOPMENT
AGENCY (PUBLIC ORGANIZATION)

WWW.DGA.OR.TH

DGATHAILAND