คู่มือปฏิบัติงาน (Manual)

คู่มือบริหารความเสี่ยงและควบคุมภายใน

(MN-S14-001)

แก้ไขครั้งที่ 0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

Digital Government Development Agency (Public Organization)

การควบคุมเอกสาร

ผู้เรียบเรียง/ผู้จัดทำ	ผู้ตรวจสอบ/ผู้ทบทวน	ผู้อนุมัติ
นายภัทรพงศ์ วงศ์สุวัฒน์	นางสาวทิสวรรณ ชูปัญญา	นางไอรดา เหลืองวิไล
ผจก. ส่วนบริหารความเสี่ยง	ผอ.ฝ่ายกลยุทธ์องค์กร	รอง ผอ.สพร. รักษาการแทน ผอ.สพร.

ครั้งที่	วันที่	รายละเอียดการแก้ไข
0	07/11/2567	ประกาศครั้งแรก - เปลี่ยนแปลงหมายเลขเอกสารจาก SP-S14-001 เป็น MN-S14-001 เพื่อยกระดับความสำคัญของเอกสารให้สอดคล้องตามที่มีการเปลี่ยนแปลงกระบวนการดำเนินงานด้านการบริหารความเสี่ยง และควบคุมภายในของ สพร. - ปรับปรุงเนื้อหาและขั้นตอนปฏิบัติให้เป็นปัจจุบัน - ปรับปรุงเกณฑ์การประเมินความเสี่ยง (โอกาสเกิดและผลกระทบ) รวมทั้งตัวอย่างแบบฟอร์มการประเมินความเพียงพอของการควบคุมภายในและการวิเคราะห์ความเสี่ยง ตามที่ได้รับความเห็นชอบจากคณะกรรมการ สพร. ในคราวประชุม ครั้งที่ 10/2567 เมื่อวันที่ 29 ต.ค. 67

สารบัญ

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 ๙ การบัญชี การรายงานและการตรวจสอบ เพื่อให้การบริหารจัดการความเสี่ยงของหน่วยงานของรัฐมีประสิทธิภาพ รวมถึงยกระดับการบริหารจัดการความเสี่ยงให้สามารถเป็นเครื่องมือสำคัญในการตัดสินใจเชิงกลยุทธ์ (Informed Strategic Decision Making)

อาศัยอำนาจตามความในมาตรา ๒๙ และ ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ๒๕๖๑ ประกอบกับมติที่ประชุมคณะอนุกรรมการด้านการบริหารความเสี่ยง ในการประชุม ครั้งที่ ๓/๒๕๖๔ และการประชุมคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล ครั้งที่ ๗/๒๕๖๔ จึงออกประกาศ ดังต่อไปนี้

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

๒. กำหนดให้มีการดำเนินงานบริหารความเสี่ยงของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ดังนี้

๒.๑ สำนักงานจะดำเนินการจัดวางระบบและกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กร ให้สอดรับกับกลยุทธ์และวัตถุประสงค์ของสำนักงาน 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 ติดตามและสื่อสารให้กับเจ้าหน้าที่และผู้มีส่วนได้ส่วนเสีย

จึงประกาศให้ทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๑๕ ตุลาคม พ.ศ. ๒๕๖๔

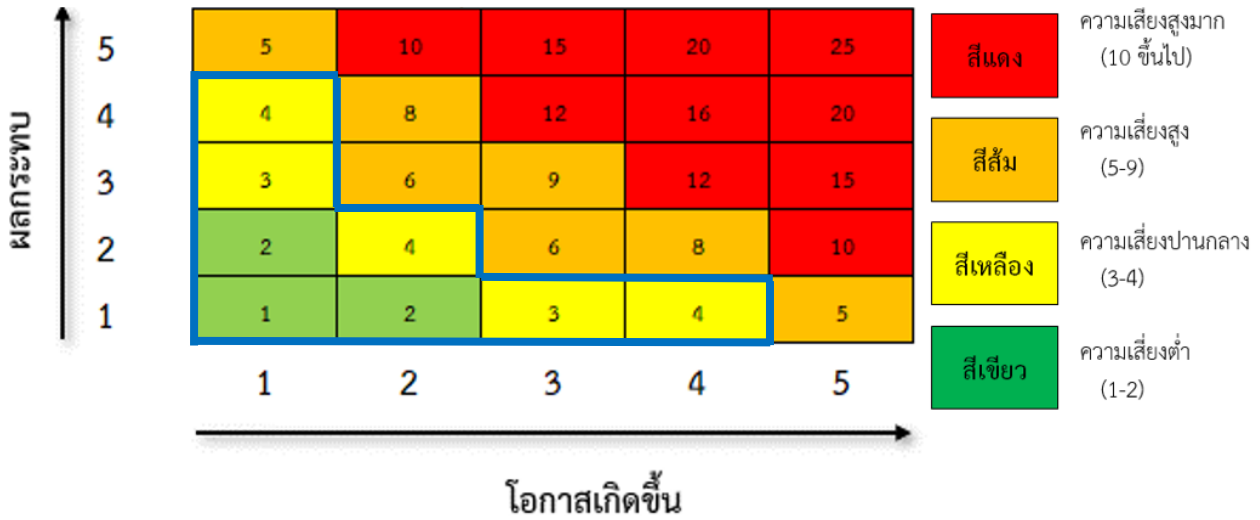
(นายสุพจน์ เธียรวุฒิ)
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ส่วนที่ 1
นโยบายการยอมรับความเสี่ยง (Risk Acceptance)
ของ สพร.

นโยบายการยอมรับความเสี่ยง (Risk Acceptance) ของ สพร.

นโยบายการยอมรับความเสี่ยง (Risk Acceptance) ของ สพร. จะยอมรับความเสี่ยงระดับองค์กรทุกประเภท ได้ที่ระดับความเสี่ยงต่ำและระดับความเสี่ยงปานกลาง และจะยอมรับความเสี่ยงระดับฝ่าย/ส่วนงานทุกประเภทได้ที่ระดับความเสี่ยงต่ำเท่านั้น โดยในกรณีที่มีการประเมินความเพียงพอของการควบคุมภายใน และวิเคราะห์ความเสี่ยงของฝ่าย/ส่วนงาน (การจัดทำ Risk Universe) แล้วผลปรากฏว่า

1. ระดับความเสี่ยงของแผนงาน/โครงการ/กิจกรรม/บริการ ดังกล่าวอยู่ในระดับความเสี่ยงสูงมาก หรือระดับความเสี่ยงสูง จะต้องนำเสนอเพื่อให้ฝ่ายบริหารพิจารณา และหรือนำเสนอต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง พิจารณาให้ความเห็นชอบและกำหนดเป็นปัจจัยเสี่ยงระดับองค์กรเพื่อนำเสนอต่อคณะกรรมการ สพร. พิจารณากำหนดปัจจัยเสี่ยงและแผนบริหารความเสี่ยงระดับองค์กร ซึ่งเจ้าของปัจจัยเสี่ยง (Risk Owner) จะต้องดำเนินการตามแผนบริหารความเสี่ยงของปัจจัยเสี่ยงระดับองค์กร (แผนจัดการความเสี่ยง และแผนการควบคุมภายใน) เพื่อให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้ (ระดับความเสี่ยงต่ำ หรือ ระดับความเสี่ยงปานกลาง)
2. ระดับความเสี่ยงของแผนงาน/โครงการ/กิจกรรม/บริการ ดังกล่าวอยู่ในระดับความเสี่ยงปานกลาง หรือระดับความเสี่ยงต่ำ ฝ่าย/ส่วนงาน ต้องดำเนินการตามแผนจัดการความเสี่ยง และมาตรการปรับปรุงการควบคุมภายใน เพื่อให้ระดับความเสี่ยงอยู่ในระดับที่ฝ่าย/ส่วนงานสามารถยอมรับได้ (ระดับความเสี่ยงต่ำ)



เส้นแบ่งขอบเขตระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ (Risk Boundary Line)

สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 ระดับ ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่ฝ่าย/ส่วนงาน/องค์กร สามารถยอมรับได้ โดยมีแผนจัดการความเสี่ยงหรือไม่มีแผนจัดการความเสี่ยงก็ได้
3-4	ปานกลาง	● ระดับความเสี่ยงที่ฝ่าย/ส่วนงาน ไม่สามารถยอมรับได้ โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น ● ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยให้ฝ่าย/ส่วนงาน นำไปบริหารความเสี่ยง โดยควบคุมและป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและมาตรการปรับปรุงการควบคุมภายใน) ให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้ และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและมาตรการปรับปรุงการควบคุมภายใน) ให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้โดยทันที และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น

หมายเหตุ: นโยบายยอมรับความเสี่ยงของ สพร. ได้รับความเห็นชอบจากคณะกรรมการ สพร. ในการประชุมครั้งที่ 9/2566 เมื่อวันที่ 20 ก.ย. 66

ส่วนที่ 2
หลักการและองค์ประกอบของการบริหารความเสี่ยง และควบคุมภายใน

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 ซึ่งจะก่อให้เกิดความเสี่ยงต่อสำนักงานโดยรวม

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 เจ้าหน้าที่ และลูกจ้างทั่วทั้งสำนักงาน และสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน

4) เพื่อให้ผู้บริหาร เจ้าหน้าที่ และลูกจ้าง ตระหนักและมีความเข้าใจตรงกันถึงเป้าหมาย วัตถุประสงค์ รวมทั้งแนวทางการบริหารความเสี่ยงของสำนักงาน เพื่อร่วมกันสร้างความพึงพอใจให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholders) และสร้างมูลค่าเพิ่มให้องค์กร โดยพิจารณาถึงผลกระทบต่อเป้าหมายการดำเนินงานให้เป็นไปตามหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance) และข้อกำหนดของหน่วยงานที่กำกับดูแลสำนักงาน

ตามคู่มือการบริหารและกำกับดูแลของคณะกรรมการองค์การมหาชน กำหนดให้องค์การมหาชนควรดำเนินการวิเคราะห์และประเมินความเสี่ยงขององค์กรให้ครอบคลุมอย่างน้อย 4 ด้าน ได้แก่ ด้านนโยบายและกลยุทธ์

ด้านการเงินและงบประมาณ ด้านการปฏิบัติงาน และด้านกฎหมาย กฎระเบียบ และสามารถเพิ่มนโยบายการบริหารความเสี่ยงด้านอื่น ๆ ได้ เพื่อให้ครอบคลุมการดำเนินงานของสำนักงาน

ดังนั้น สำนักงานจึงแบ่งประเภทความเสี่ยงออกเป็น 5 ด้าน ดังนี้

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

2) ด้านการดำเนินงาน 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. แนวทางการกำหนดแผนบริหารความเสี่ยง

สำนักงานต้องกำหนดแผนบริหารความเสี่ยงโดยคำนึงถึงสาระสำคัญ ดังนี้

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

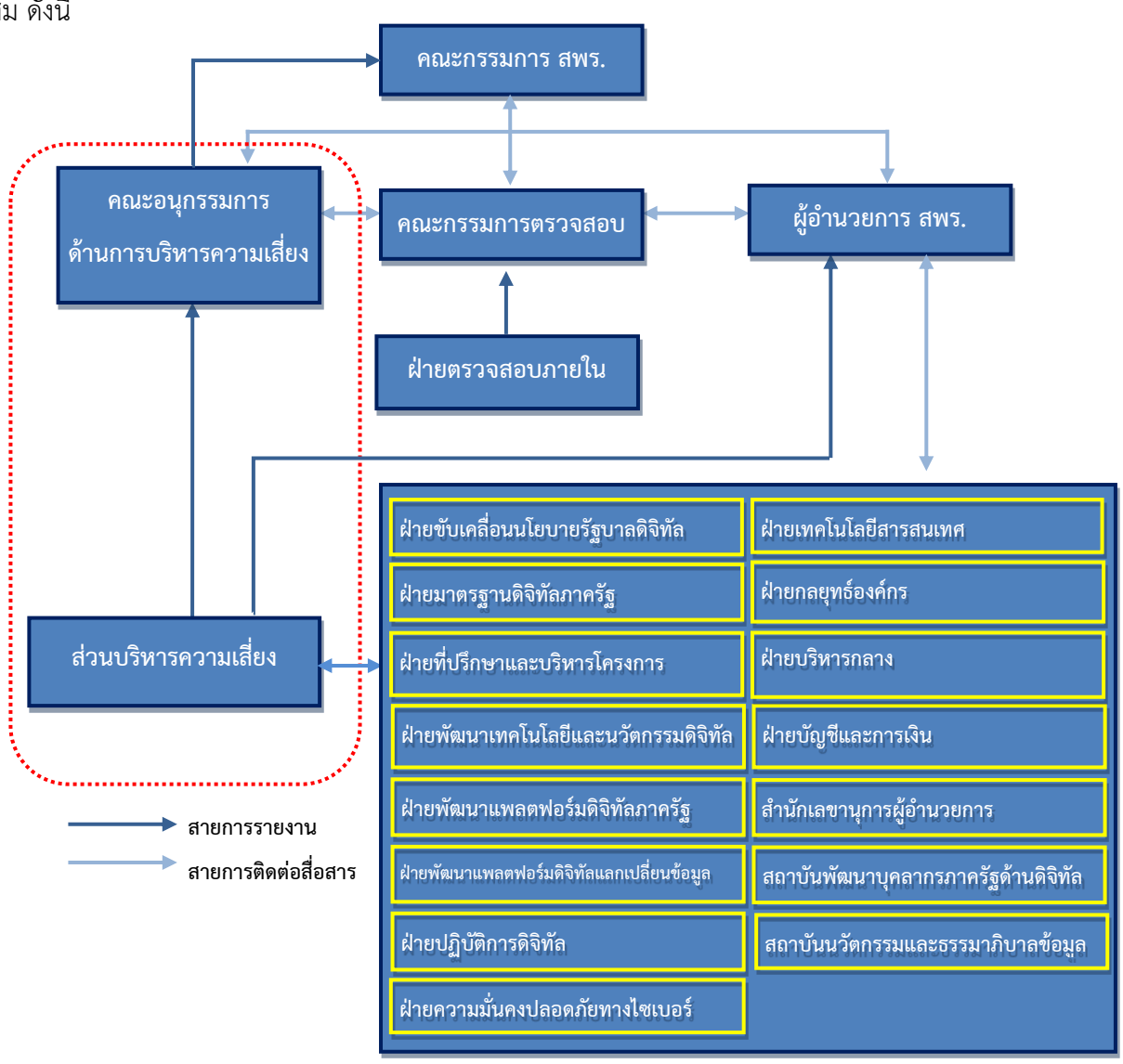
2) ความสอดคล้องกับแนวทางมาตรฐานของหน่วยงานกำกับดูแล ข้อกำหนดของกฎหมาย ระเบียบ ประกาศ หลักเกณฑ์ และแนวทางปฏิบัติที่ดี

3) สำนักงานจะต้องทบทวนแผนบริหารความเสี่ยงอย่างน้อยปีละ 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 ให้คณะอนุกรรมการเชิญบุคคลดังกล่าวเข้าร่วมพิจารณากับคณะอนุกรรมการเป็นคราว ๆไป โดยให้บุคคลดังกล่าวได้รับค่าตอบแทนตามระเบียบสำนักงาน 7) ปฏิบัติงานอื่นใดตามที่คณะกรรมการมอบหมาย
คณะกรรมการตรวจสอบ	1) สอบทาน ให้คำปรึกษา และติดตาม ระบบควบคุมภายใน ระบบการตรวจสอบภายในรายงานผลการตรวจสอบภายใน และรายงานผลการดำเนินงานทางด้านการเงิน และด้านการบริหารงาน 2) สอบทานการบริหารความเสี่ยงจากรายงานผลการตรวจสอบที่เกี่ยวข้องกับระบบการบริหารความเสี่ยงซึ่งอยู่ในแผนการตรวจสอบประจำปี

บทบาท หน้าที่และความรับผิดชอบของผู้บริหาร หน่วยงาน และเจ้าหน้าที่ที่เกี่ยวข้องกับการบริหารความเสี่ยง

หน่วยงาน/ผู้บริหาร/คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
ผู้อำนวยการ เจ้าหน้าที่ และลูกจ้างทุกคนในสำนักงาน	1) มีหน้าที่รับผิดชอบการวิเคราะห์ระบุและประเมินความเสี่ยง กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือแผนบริหารความเสี่ยงของหน่วยงาน/โครงการ หรืองานที่อยู่ในความรับผิดชอบ 2) ติดตามและรายงานความเสี่ยงให้ผู้บังคับบัญชาทราบตามลำดับชั้นตลอดจนคณะอนุกรรมการด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อให้การบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ
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 4) สื่อสาร สนับสนุน ให้คำปรึกษาการบริหารความเสี่ยงในสำนักงาน พร้อมประเมินความเสี่ยงและกำหนดแนวทางในการปรับลดความเสี่ยงของสำนักงาน 5) วัดผล ติดตาม ควบคุม รายงานและให้ข้อเสนอแนะเพิ่มเติมถึงแนวทางในการบริหารและจัดการความเสี่ยงในสำนักงาน 6) สนับสนุนการดำเนินงานของคณะอนุกรรมการด้านการบริหารความเสี่ยง
ฝ่ายตรวจสอบภายใน	1) สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายในและกระบวนการบริหารความเสี่ยงเพื่อให้มั่นใจว่ามีระบบการควบคุมภายในที่เหมาะสมและเพียงพอสำหรับการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ควบคุมได้และเป็นไปตามกระบวนการกำกับดูแลกิจการที่ดี 2) ให้ความเห็นเกี่ยวกับประสิทธิผลของการบริหารจัดการความเสี่ยงด้านการทุจริตและระบบการร้องเรียนของสำนักงาน

หน่วยงาน/ผู้บริหาร/คณะทำงาน	บทบาท/หน้าที่/ความรับผิดชอบ
	3) ติดตามผลการตรวจสอบและการปฏิบัติตามข้อเสนอแนะที่หน่วยรับตรวจต้องดำเนินการเพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพ ประสิทธิผลและประหยัดยิ่งขึ้น
ฝ่าย/ส่วนงาน	1) ควบคุมดูแลการปฏิบัติงานในฝ่าย/ส่วน ให้เป็นไปตามนโยบายและกลยุทธ์การบริหารความเสี่ยง รวมทั้งจัดให้มีระบบบริหารความเสี่ยงที่มีประสิทธิภาพ 2) สร้างความมั่นใจว่าการปฏิบัติงานรายวันมีการประเมินจัดการและรายงานความเสี่ยงอย่างเพียงพอ 3) ส่งเสริมเจ้าหน้าที่ในฝ่ายและส่วนงานให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง 4) สร้างความมั่นใจว่าแผนการบริหารความเสี่ยงได้รับการปฏิบัติอย่างครบถ้วน
Risk Agent	1) รับผิดชอบในการประสานงานกับส่วนบริหารความเสี่ยง รวมทั้งเผยแพร่ความรู้ที่เกี่ยวข้องกับการดำเนินงานส่วนบริหารความเสี่ยง อาทิเช่น การบริหารความเสี่ยง การควบคุมภายใน การประเมินคุณธรรมและความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐ และการส่งเสริมองค์กรคุณธรรม ให้แก่เจ้าหน้าที่ในหน่วยงานของตนเอง 2) ให้คำปรึกษา พร้อมทั้งประสานงานให้หน่วยงานตนเอง ดำเนินการตามกระบวนการบริหารความเสี่ยง โดยมีการระบุปัจจัยเสี่ยง การประเมินความเพียงพอของการควบคุมภายในและวิเคราะห์ความเสี่ยง การจัดทำมาตรการการควบคุมภายใน และการจัดทำแผนการจัดการความเสี่ยงด้านต่าง ๆ ที่อาจเกิดขึ้น เพื่อป้องกันหรือลดระดับความเสี่ยง 3) ช่วยเหลือและสนับสนุนการจัดประชุมเชิงปฏิบัติการที่เกี่ยวข้องกับการดำเนินงานของส่วนบริหารความเสี่ยง 4) บันทึก ติดตาม และรายงานความก้าวหน้าของการบริหารความเสี่ยงและการควบคุมภายใน การประเมินคุณธรรมและความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐ และการส่งเสริมองค์กรคุณธรรม ทั้งระดับองค์กร ระดับฝ่าย/ส่วนงาน

6. ความหมายและคำจำกัดความของการบริหารความเสี่ยงและควบคุมภายใน

ความหมายของความเสี่ยง

การดำเนินงานในองค์กรโดยทั่วไป มีเป้าหมายเพื่อเพิ่มมูลค่าให้แก่ผู้มีส่วนได้ส่วนเสีย ทำให้ทุกองค์กรต้องเผชิญกับความไม่แน่นอน ที่อาจเกิดขึ้นจากปัจจัยภายในและภายนอกหลายประการ เช่น การเปลี่ยนแปลงของกฎระเบียบ 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

ความหมายของการควบคุมภายใน

การควบคุมภายใน หมายถึง กระบวนการปฏิบัติงาน หรือมาตรการต่างๆ ที่ถือปฏิบัติภายในองค์กร และถูกกำหนดร่วมกันโดยคณะกรรมการ/ผู้บริหาร/และบุคลากรขององค์กร เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่า การดำเนินงานขององค์กรจะบรรลุผลสำเร็จตามวัตถุประสงค์ที่กำหนดไว้ โดยกิจกรรมการควบคุมภายใน เป็นกระบวนการที่แทรกอยู่ในกระบวนการทำงานปกติ ซึ่งจะต้องมีการติดตาม และประเมินประสิทธิผลว่ากิจกรรมควบคุมดังกล่าวมีประสิทธิผลหรือไม่

นิยามการควบคุมภายใน

การควบคุมภายใน คือ กระบวนการที่กำหนดให้มีขึ้นเพื่อให้เกิดความมั่นใจในการดำเนินงาน จะบรรลุวัตถุประสงค์ 3 ประการ

- ประสิทธิผล และประสิทธิภาพของการดำเนินงาน
- ความเชื่อถือได้ ของการรายงานทางการเงิน
- การปฏิบัติตามกฎหมาย และระเบียบข้อบังคับ

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 การจัดเก็บระบบงาน โดยจัดการป้องกันให้มีความเหมาะสมและความสำคัญของข้อมูลรวมถึงระบบงานด้วย
ความถูกต้องเชื่อถือได้ของข้อมูล	ข้อมูลที่จะส่งมอบให้กับผู้ใช้ข้อมูล (End User) เป็นข้อมูลที่มีความสมบูรณ์ ถูกต้องครบถ้วน ซึ่งจะทำให้การดำเนินงานและการบริหารงานขององค์กรมีประสิทธิภาพ

ศัพท์เฉพาะ	คำนิยาม
(Data Integrity)	
ความพร้อมใช้งานของระบบงานและข้อมูล (Availability)	การจัดส่งข้อมูลไปให้ผู้ที่ต้องการใช้ข้อมูลได้รวดเร็วทันเวลา และสามารถให้ข้อมูลได้อย่างต่อเนื่องในเวลาที่เหมาะสม เพื่อสนับสนุนการดำเนินงานขององค์กร ทั้งนี้ องค์กรต้องมีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ซึ่งเป็นแผนการดำเนินงานหลักขององค์กร และมีแผนงานรองประกอบแผนงานหลัก ได้แก่ แผนการกู้ระบบกลับคืน (Disaster Recovery Plan) แผนสำรองฉุกเฉิน (Contingency Plan) และแผนรองรับเหตุการณ์ไม่คาดว่าจะเกิดขึ้น (Incident Response Plan)
การควบคุมภายใน (Internal Control)	กระบวนการที่กำหนดให้มีขึ้นเพื่อให้เกิดความมั่นใจในการดำเนินงาน จะบรรลุวัตถุประสงค์ 3 ประการ ● ประสิทธิผล และประสิทธิภาพของการดำเนินงาน ● ความเชื่อถือได้ ของการรายงานทางการเงิน ● การปฏิบัติตามกฎหมาย และระเบียบข้อบังคับ
ระเบียบการควบคุมภายใน	หลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561

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 คือหน่วยงานตรวจสอบภายในทำหน้าที่ในการประเมินความเพียงพอของมาตรการต่าง ๆ โดยอยู่ภายใต้การดูแลของผู้ตรวจสอบภายนอกและทางการ
- ได้รับการสนับสนุนและมีส่วนร่วม จากทุกคนในองค์กรตั้งแต่ระดับคณะกรรมการ ผู้บริหารทุกระดับและเจ้าหน้าที่ทุกคน

7. องค์ประกอบการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงองค์กรตามแนวคิดของ COSO ฉบับปรับปรุงใหม่ COSO ERM 2017 ประกอบด้วยหลักการสำคัญ 5 หลักการ และมี 20 องค์ประกอบที่สัมพันธ์กัน องค์กรควรนำหลักการและองค์ประกอบต่าง ๆ ไปใช้เพื่อให้เกิดการบริหารความเสี่ยงทั่วทั้งองค์กร

ที่มา : Committee of Sponsoring Organizations of the Trading Commission (COSO)

หลักการสำคัญที่ 1 การกำกับดูแลกิจการและวัฒนธรรมองค์กร (Governance and Culture)

การกำกับดูแลกิจการและวัฒนธรรมองค์กร เป็นพื้นฐานขององค์ประกอบทั้งหมดในการบริหารความเสี่ยง เนื่องจากการกำกับดูแลกิจการจะเป็นสิ่งที่กำหนดแนวทางขององค์กรในการให้ความสำคัญและสร้างความรับผิดชอบเกี่ยวกับการบริหารความเสี่ยง และวัฒนธรรมองค์กรจะเกี่ยวข้องกับค่านิยมทางจริยธรรม พฤติกรรมที่พึงประสงค์และความเข้าใจเกี่ยวกับความเสี่ยงขององค์กร ซึ่งจะสะท้อนผ่านการตัดสินใจต่าง ๆ

COSO ถือว่าการกำกับดูแลกิจการและวัฒนธรรมองค์กรเป็นองค์ประกอบที่สำคัญยิ่ง เป็นองค์ประกอบพื้นฐานหลักให้องค์ประกอบอื่น ๆ เกิดขึ้นเสมือนเป็นรากฐานสำคัญให้เกิดการบริหารความเสี่ยงขึ้นในองค์กร มี 5 องค์ประกอบ ดังนี้

1. จัดตั้งคณะกรรมการดูแลความเสี่ยง (Exercises Board Risk Oversight)

คณะกรรมการบริษัทมีหน้าที่กำกับดูแลการดำเนินงานตามกลยุทธ์ต่าง ๆ รวมถึงกำกับดูแลกิจการ เช่น คณะกรรมการควรมีการกำหนดหน้าที่ความรับผิดชอบด้านการบริหารความเสี่ยง มีความรู้และความเชี่ยวชาญในการกำกับการบริหารความเสี่ยง มีความเป็นอิสระ หลีกเลี่ยงความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้น

2. จัดตั้งโครงสร้างการดำเนินงาน (Establishes Operating Structures)

องค์กรควรจัดตั้งโครงสร้างการดำเนินงานที่สอดคล้องกับกลยุทธ์และวัตถุประสงค์ทางธุรกิจ เช่น มีการกำหนดโครงสร้างการดำเนินงานและสายการบังคับบัญชาที่เหมาะสม มีโครงสร้างการบริหารความเสี่ยง การกำหนดอำนาจ หน้าที่ และความรับผิดชอบให้สอดคล้องกับกลยุทธ์

3. ระบุวัฒนธรรมองค์กรที่ต้องการ (Defines Desired Culture)

องค์กรควรระบุพฤติกรรมที่พึงประสงค์ ซึ่งแสดงถึงวัฒนธรรมองค์กรที่ต้องการคณะกรรมการบริหารและฝ่ายบริหารเป็นผู้กำหนดวัฒนธรรมองค์กร ทั้งสำหรับองค์กรในภาพรวมและสำหรับบุคลากรภายใต้วัฒนธรรม

องค์กรที่ให้ความสำคัญกับความเสี่ยง วัฒนธรรมองค์กรเกิดขึ้นจากหลายปัจจัย ปัจจัยภายในที่สำคัญ ได้แก่ ระดับการใช้วิจารณญาณ ความเป็นอิสระในการตัดสินใจของพนักงาน การสื่อสารระหว่างพนักงานและผู้จัดการ มาตรฐานและกฎเกณฑ์ต่าง ๆ แผนผังทางกายภาพของสถานที่ปฏิบัติงานและระบบค่าตอบแทน ปัจจัยภายนอก ได้แก่ ข้อกำหนดด้านกฎหมาย ความคาดหวังของลูกค้า นักลงทุน และองค์ประกอบอื่น ๆ

4. แสดงความมุ่งมั่นในค่านิยมหลัก (Demonstrates Commitment to Core Values)

องค์กรควรแสดงให้เห็นถึงความมุ่งมั่นที่จะปฏิบัติตามค่านิยมหลักขององค์กร เช่น ยึดถือการบริหารความเสี่ยงเป็นส่วนหนึ่งของวัฒนธรรมองค์กร การปฏิบัติตามภาระรับผิดชอบอย่างเคร่งครัด การสร้างความรับผิดชอบต่อตนเอง การกำหนดให้มีการสื่อสารที่เหมาะสม

5. จูงใจ พัฒนา และรักษาบุคลากรที่มีความสามารถ (Attracts, Develops, and Retains Capable Individuals)

องค์กรควรมุ่งมั่นในการสนับสนุนการสร้างทรัพยากรบุคคลควบคู่ไปกับกลยุทธ์และวัตถุประสงค์ทางธุรกิจ เช่น ฝึกอบรมบุคลากรในด้านการบริหารความเสี่ยง ส่งเสริมความสามารถของพนักงาน สร้างแรงจูงใจและผลตอบแทนอื่น ๆ อย่างเหมาะสมสำหรับตำแหน่งงานในทุกระดับ

หลักการสำคัญที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective-Setting)

การบริหารความเสี่ยงสามารถบูรณาการเข้ากับแผนยุทธศาสตร์ขององค์กรได้ ผ่านกระบวนการกำหนดกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยองค์กรควรกำหนดความเสี่ยงที่ยอมรับได้ให้สอดคล้องกับการกำหนดกลยุทธ์ นอกจากนั้น วัตถุประสงค์ทางธุรกิจ จะเป็นสิ่งที่กำหนดแนวทางปฏิบัติตามกลยุทธ์ รวมถึงการดำเนินงานทั่วไป และปัจจัยที่องค์กรให้ความสำคัญและจะเป็นพื้นฐานในการระบุ ประเมิน และการตอบสนองต่อความเสี่ยง หลักการสำคัญที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์มี 4 องค์ประกอบ ดังนี้

6. วิเคราะห์ธุรกิจ (Analyzes Business Context)

องค์กรควรพิจารณาถึงผลกระทบจากการบริหารทางธุรกิจที่อาจเกิดขึ้น และส่งผลต่อระดับความเสี่ยงในภาพรวมขององค์กร เช่น การเข้าใจบริบททางธุรกิจ การคำนึงถึงสภาพแวดล้อมภายนอกและผู้มีส่วนได้เสีย

7. ระบุความเสี่ยงที่ยอมรับได้ (Defines Risk Appetite)

องค์กรควรระบุความเสี่ยงที่ยอมรับได้ เพื่อสร้าง รักษา และส่งเสริมความตระหนักถึงค่านิยม เช่น มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ และสื่อสารความเสี่ยงที่ยอมรับได้ให้ชัดเจน ความเสี่ยงที่ยอมรับได้ไม่มีการกำหนดรูปแบบที่ตายตัวหรือเป็นมาตรฐานที่จะใช้ได้กับทุกองค์กร ผู้บริหารเป็นผู้เลือกความเสี่ยงที่ยอมรับได้ภายใต้บริบททางธุรกิจที่ต่างกันในแต่ละองค์กร

8. ประเมินกลยุทธ์ (Evaluates Alternative Strategies)

องค์กรควรประเมินเพื่อค้นหากลยุทธ์ทางเลือกและผลกระทบที่อาจเกิดขึ้นต่อโปรไฟล์ความเสี่ยงขององค์กร เช่น การวิเคราะห์ SWOT การประเมินมูลค่า การคาดการณ์รายได้ การวิเคราะห์คู่แข่ง และการวิเคราะห์สถานการณ์กลยุทธ์ต้องสนับสนุนพันธกิจและวิสัยทัศน์ รวมถึงสอดคล้องกับค่านิยมหลักและความเสี่ยงที่ยอมรับได้

9. กำหนดวัตถุประสงค์ทางธุรกิจ (Formulates Business Objectives)

ในการกำหนดวัตถุประสงค์ทางธุรกิจ องค์กรควรพิจารณาความเสี่ยงในระดับต่าง ๆ ซึ่งสอดคล้องและสนับสนุนกลยุทธ์ควบคู่ไปด้วย เช่น การกำหนดค่าความเบี่ยงเบนของความเสี่ยงจากผลการดำเนินงาน ซึ่งยังคงอยู่ในช่วงความเสี่ยงที่ยอมรับได้

หลักการสำคัญที่ 3 ผลการดำเนินงาน (Performance)

เริ่มจากการระบุและประเมินความเสี่ยงที่อาจส่งผลต่อความสามารถในการบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยจัดลำดับความสำคัญของความเสี่ยงตามโอกาสและผลกระทบที่อาจเกิดขึ้นและพิจารณาความเสี่ยงที่องค์กรยอมรับได้ จากนั้น องค์กรจะเลือกตอบสนองต่อความเสี่ยงด้วยวิธีต่าง ๆ รวมถึงพิจารณาปริมาณความเสี่ยงในภาพรวม และตรวจสอบผลการดำเนินงานเพื่อเปลี่ยนแปลงแก้ไข ซึ่งจะพัฒนามุมมองในภาพรวมเกี่ยวกับปริมาณความเสี่ยงที่องค์กรอาจเผชิญในการบรรลุเป้าหมายกลยุทธ์ และวัตถุประสงค์ทางธุรกิจในระดับองค์กร มี 5 องค์ประกอบ ดังนี้

10. ระบุความเสี่ยง (Identifies Risk)

องค์กรควรระบุความเสี่ยงที่ส่งผลต่อกลยุทธ์และวัตถุประสงค์ทางธุรกิจ เช่น ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านการเงิน และความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ ความเสี่ยงทั้งหมดจะเก็บไว้ในโปรไฟล์ความเสี่ยง เพื่อนำไปจัดการความเสี่ยงเหล่านี้ต่อไป

11. ประเมินความรุนแรงของความเสี่ยง (Assesses Severity of Risk)

องค์กรควรประเมินความรุนแรงของความเสี่ยง โดยประเมินว่าแต่ละปัจจัยนั้น มีโอกาสที่จะเกิดมากน้อยเพียงใด และหากเกิดขึ้นแล้วจะส่งผลกระทบต่อองค์กรรุนแรงเพียงใด

12. จัดลำดับความสำคัญของความเสี่ยง (Prioritizes Risks)

องค์กรควรคำนวณระดับความเสี่ยง (Risk Exposure) จัดลำดับความสำคัญของความเสี่ยง เพื่อเป็นพื้นฐานในการพิจารณาคัดเลือกวิธีตอบสนองต่อความเสี่ยงต่าง ๆ การคำนวณระดับความเสี่ยงเท่ากับผลคูณของคะแนนระหว่างโอกาสที่จะเกิดกับความเสียหายเพื่อจัดลำดับความสำคัญและใช้ในการตัดสินใจว่าความเสี่ยงใดควรเร่งจัดการก่อน

13. ดำเนินการตอบสนองต่อความเสี่ยง (Implements Risk Responses)

องค์กรควรประเมินความรุนแรงของความเสี่ยง โดยประเมินว่าแต่ละปัจจัยเสี่ยงนั้นมีโอกาสที่จะเกิดมากน้อยเพียงใดและหากเกิดขึ้นแล้วจะส่งผลกระทบต่อองค์กรรุนแรงเพียงใด

14. พัฒนากรอบความเสี่ยงในภาพรวม (Develops Portfolio View)

องค์กรควรพัฒนาและประเมินความเสี่ยงในภาพรวมของทั้งองค์กร เครื่องมือที่นิยมใช้แสดงความเสี่ยงมีชื่อเรียกหลากหลายชื่อได้แก่ Risk Map หรือ Risk Matrix

หลักการสำคัญที่ 4 การทบทวนและปรับปรุงแก้ไข (Review and Revision)

องค์กรควรพิจารณากระบวนการบริหารความเสี่ยงอยู่เป็นระยะ โดยทบทวนความสามารถและแนวทางการบริหารความเสี่ยง ผู้บริหารควรพิจารณาความสามารถและการบริหารความเสี่ยงทั่วทั้งองค์กรว่าเพิ่มคุณค่าให้กับองค์กรมากน้อยเพียงใด และมีสิ่งใดที่ต้องปรับปรุงแก้ไขเพื่อเพิ่มคุณค่าให้กับองค์กรได้ แม้ต้องเผชิญกับความเปลี่ยนแปลงที่สำคัญต่าง ๆ มี 3 องค์ประกอบ ดังนี้

15. ประเมินการเปลี่ยนแปลงที่สำคัญ (Assesses Substantial Change)

องค์กรควรระบุและประเมินการเปลี่ยนแปลงต่าง ๆ ทั้งภายในและภายนอกกิจการที่อาจส่งผลกระทบต่อกลยุทธ์และวัตถุประสงค์ทางธุรกิจที่สำคัญ เช่น ผู้บริหารระดับสูงลาออกจากตำแหน่ง การควบรวมกิจการ การเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยี กฎ ระเบียบ ข้อบังคับต่าง ๆ หรือการเกิดโรคระบาด

16. ทบทวนความเสี่ยงและผลการดำเนินงาน (Reviews Risk and Performance)

องค์กรควรทบทวนผลการดำเนินงานขององค์กร รวมถึงพิจารณาทบทวนความเสี่ยงต่าง ๆ ที่เกี่ยวข้อง เช่น องค์กรมีผลการดำเนินงานตามเป้าหมายแล้วหรือไม่ องค์กรประเมินความเสี่ยงได้แม่นยำหรือไม่ พิจารณาระดับความเสี่ยงได้เหมาะสมกับเป้าหมายหรือไม่ หรือมีความเสี่ยงอื่นใดที่กำลังเกิดขึ้น และอาจส่งผลกระทบต่อองค์กร

17. มุ่งมั่นปรับปรุงการบริหารความเสี่ยงองค์กร (Pursues Improvement in Enterprise Risk Management)

องค์กรควรปรับปรุงการบริหารความเสี่ยงองค์กรอยู่สม่ำเสมอ โดยเฉพาะช่วงเวลาการเปลี่ยนแปลงที่สำคัญ เช่น การปรับโครงสร้างองค์กรหลังการประเมินผลการดำเนินงาน หรือการเปลี่ยนแปลงจากสภาพแวดล้อมภายนอกต่าง ๆ ที่ส่งผลกระทบต่อระบบการบริหารความเสี่ยง

หลักการสำคัญที่ 5 สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication and Reporting)

การสื่อสารเป็นกระบวนการต่อเนื่องในการรวบรวมข้อมูล และแบ่งปันข้อมูลที่จำเป็นจากทั่วทั้งองค์กร ผู้บริหารใช้ข้อมูลที่เกี่ยวข้องทั้งจากแหล่งภายในและภายนอก ซึ่งข้อมูลสารสนเทศดังกล่าวจะมาจากทั้งผู้บริหารและพนักงานในส่วนต่าง ๆ ขององค์กร เพื่อสนับสนุนการบริหารความเสี่ยงทั่วทั้งองค์กร โดยองค์กรจะใช้ประโยชน์จากระบบข้อมูล เพื่อรวบรวม ประมวลผลและจัดการข้อมูลต่าง ๆ ที่สัมพันธ์กับการบริหารความเสี่ยง จากนั้นองค์กรจึงรายงานข้อมูลความเสี่ยง วัฒนธรรมองค์กร และผลการดำเนินการได้มี 3 องค์ประกอบ ดังนี้

18. ยกระดับระบบสารสนเทศ (Leverages Information Systems)

องค์กรควรจัดให้มีสารสนเทศอย่างเพียงพอ เหมาะสมและทันต่อเวลา องค์กรอาจใช้กระบวนการวิเคราะห์กลุ่มข้อมูลขนาดใหญ่ (Big Data Analytics) เพื่อค้นหารูปแบบความสัมพันธ์ของสิ่งเชื่อมโยงข้อมูลเข้าไว้ด้วยกัน นำไปสู่การระบุและจัดการความเสี่ยงได้ดีขึ้น

19. สื่อสารข้อมูลความเสี่ยง (Communicates Risk Information)

องค์กรควรสื่อสารข้อมูลการบริหารความเสี่ยงองค์กรผ่านช่องทางการติดต่อต่าง ๆ ข้อมูลการสื่อสารทั้งระดับบนลงล่าง (Top-down Approach) และระดับล่างขึ้นบน (Bottom-up Approach) การสื่อสารข้อมูลความเสี่ยงควรมีให้เพียงพอทั้งภายในและภายนอกองค์กร

20. รายงานผลความเสี่ยง วัฒนธรรม และผลการดำเนินงาน (Reports on Risk, Culture and Performance)

องค์กรควรรายงานความเสี่ยง วัฒนธรรมองค์กร และผลการดำเนินงานในทุกระดับให้ครอบคลุมทั่วทั้งองค์กร แม้จะมีการมอบหมายหน้าที่ด้านการรายงานผลให้หน่วยงานหรือบุคคลใดแล้วก็ตาม ผู้บริหารก็ยังต้องมีหน้าที่กำกับดูแลด้วย

8. กระบวนการบริหารความเสี่ยงและควบคุมภายใน

กระบวนการบริหารความเสี่ยง เป็นกระบวนการที่ต้องดำเนินการอย่างต่อเนื่องภายในองค์กร และควรผนวกกับกิจกรรมปกติทางธุรกิจ เพื่อให้องค์กรสามารถดำเนินการตามกลยุทธ์ที่กำหนด ส่งผลให้องค์กรบรรลุตามพันธกิจและวัตถุประสงค์ที่ต้องการ

กระบวนการ 7 ขั้นตอนหลัก ประกอบด้วย

1. การระบุปัจจัยเสี่ยงและวิเคราะห์ความเสี่ยง (Risk Identification)
2. การประเมินความเพียงพอของการควบคุมภายใน และการจัดทำมาตรการการปรับปรุงการควบคุมภายใน (Internal Control & Existing Plan)
3. การประเมินความเสี่ยง (Risk Assessment)
4. การจัดลำดับความเสี่ยง (Risk Priority)
5. การจัดทำแผนจัดการความเสี่ยง (Mitigation Plan)
6. สารสนเทศและการสื่อสาร (Information & Communication)
7. การติดตามและประเมินผล (Monitoring)

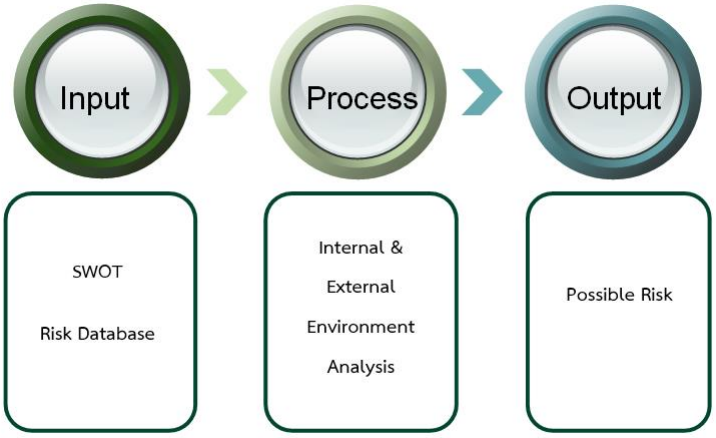
8.1 การระบุปัจจัยเสี่ยงและวิเคราะห์ความเสี่ยง (Risk Identification)

การระบุปัจจัยเสี่ยงและการวิเคราะห์ความเสี่ยง จะเริ่มจากการวิเคราะห์สภาพแวดล้อมภายในและภายนอกองค์กร โดยสภาพแวดล้อมภายในองค์กรครอบคลุมถึงแนวนโยบายโดยทั่วไปของสำนักงาน 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

หลังจากนั้น สำนักงานต้องกำหนดให้หน่วยงานทุกระดับมีการกำหนดวัตถุประสงค์และเป้าหมายการดำเนินงานที่สอดคล้องกับวิสัยทัศน์ พันธกิจ กลยุทธ์ และเป้าหมายโดยรวมของสำนักงาน โดยต้องมีความชัดเจนสามารถวัดหรือประเมินผลได้

ในการกำหนดวัตถุประสงค์ ควรกำหนดให้ครอบคลุมแต่ละประเภทของวัตถุประสงค์ ดังต่อไปนี้

- วัตถุประสงค์ด้านกลยุทธ์ 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)

ความสอดคล้องของวัตถุประสงค์

วัตถุประสงค์ต้องมีความสอดคล้องทั่วทั้งองค์กร เพื่อให้เกิดความมั่นใจว่า หน่วยงาน ผู้บริหาร และเจ้าหน้าที่ ดำเนินการเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

วิสัยทัศน์เป็นจุดเริ่มต้นในการกำหนดทิศทางขององค์กร ผู้บริหารระดับสูงจะทำการกำหนดวัตถุประสงค์ระดับองค์กรขึ้นในการจัดทำแผนประจำปี แต่ละหน่วยงานดำเนินการกำหนดวัตถุประสงค์ของหน่วยงานให้สอดคล้องกับวัตถุประสงค์ที่องค์กรได้กำหนดไว้ และการกำหนดวัตถุประสงค์ของกระบวนการและโครงการต่าง ๆ ต้องคำนึงถึงความสอดคล้องกับวัตถุประสงค์ของหน่วยงานและระดับองค์กร

วัตถุประสงค์อาจเกี่ยวข้องกับองค์กรในหลาย ๆ ด้าน รวมไปถึง ทรัพยากร เทคโนโลยีสารสนเทศ ผลการดำเนินการด้านปฏิบัติการ เป็นต้น

การระบุปัจจัยเสี่ยงหรือความไม่แน่นอนที่อาจเกิดขึ้น จะพิจารณาจากปัจจัยทั้งภายในและภายนอกองค์กรที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร โดยแบ่งประเภทความเสี่ยงออกเป็น 5 ด้าน ดังนี้

1. **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)** เป็นความเสี่ยงที่เกิดจากการกำหนดกลยุทธ์ หรือนโยบายการบริหารงาน ทำให้องค์กรไม่สามารถบรรลุกลยุทธ์และเพิ่มมูลค่าให้องค์กรได้ เช่น การเปลี่ยนแปลงโครงสร้างองค์กร การกำหนดวิสัยทัศน์ หรือกำหนดแผนยุทธศาสตร์ ที่มีความผิดพลาด รวมทั้ง การเปลี่ยนแปลงปัจจัยภายนอกด้านเศรษฐกิจ สังคม การเมือง สภาพการแข่งขัน การเปลี่ยนแปลงของหน่วยงานราชการ เทคโนโลยี และกฎหมายต่าง ๆ เป็นต้น

2. **ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)** เป็นความเสี่ยงที่เกิดจากการปฏิบัติงานปกติในทุก ๆ ขั้นตอน โดยเกี่ยวข้องกับกระบวนการในการปฏิบัติงาน อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากร ซึ่งส่งผล

ต่อประสิทธิภาพและประสิทธิผลในการดำเนินธุรกิจขององค์กร เช่น การบริหารจัดการบุคคลไม่มีประสิทธิภาพ ไม่มีการสร้างความผูกพันต่อองค์กร ความไม่ปลอดภัยในสภาพแวดล้อมการทำงาน ความผิดพลาดจากการปฏิบัติงาน ภัยพิบัติหรือเหตุการณ์อื่น ๆ ความเสียหายของทรัพย์สินสำนักงาน ขาดการติดตามและรายงานผล การบริหารจัดการด้านเอกสารไม่มีประสิทธิภาพ และไม่มีการควบคุมธุรกรรมกับคู่ค้า/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 อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้ ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะมีองค์ประกอบที่สำคัญ 3 ประการ ได้แก่ แผนงานการใช้เทคโนโลยีสารสนเทศ การตัดสินใจในการนำเทคโนโลยีสารสนเทศมาใช้ และการวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน ระบบงาน เหตุการณ์ภายนอก หรือคน (เจ้าหน้าที่ บุคคลภายนอก หรือลูกค้า) ซึ่งส่งผลกระทบต่อการดำเนินงาน

การระบุสาเหตุความเสี่ยง (Root Cause) เป็นการระบุต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการจัดการความเสี่ยง ในภายหลังได้อย่างถูกต้อง

โดยกระบวนการระบุปัจจัยเสี่ยง จะต้องมีความเชื่อมโยงกับกระบวนการในกำหนดวัตถุประสงค์เชิงยุทธศาสตร์ และการวางแผนและการกำหนดเป้าหมายขององค์กร ซึ่งองค์กรจะต้องกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) ต้องสอดคล้องกับเป้าหมายขององค์กรประจำปีที่ระบุไว้ในแผนยุทธศาสตร์และแผนปฏิบัติการ หรือเป็นค่าที่ได้รับความเห็นชอบจากคณะกรรมการ

ความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้ โดยธุรกิจยังคงดำเนินการได้บรรลุตามเป้าหมาย โดยความเสี่ยงที่ยอมรับได้กำหนดขึ้นเพื่อใช้เป็นแนวทางกำหนดกลยุทธ์ขององค์กร ทั้งนี้ ความเสี่ยงที่ยอมรับได้ควรได้รับการกำหนดโดยผู้บริหารและอนุมัติโดยคณะกรรมการ การกำหนดความเสี่ยงที่ยอมรับได้ควรพิจารณาถึงความสมดุลระหว่างการเติบโต ความเสี่ยงและผลตอบแทนขององค์กร ในขณะเดียวกันองค์กรควรบริหารความเสี่ยงที่เกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้

ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) คือ ระดับความเบี่ยงเบนจากความเสี่ยงที่ยอมรับได้ ซึ่งการดำเนินธุรกิจภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ทำให้ผู้บริหารมั่นใจได้ว่าการดำเนินงานขององค์กร อยู่ภายในเกณฑ์หรือระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ซึ่งมีผลให้คณะกรรมการและผู้บริหารขององค์กรมีความมั่นใจมากขึ้นว่าการดำเนินการขององค์กร จะสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ได้

การวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล

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

โดยได้กำหนดแนวทางการวิเคราะห์ความเสี่ยงของแผนงาน/โครงการตามหลักธรรมาภิบาลมี 10 ประเภท ได้แก่

1. **ความเสี่ยงต่อหลักประสิทธิผล (Effectiveness)** ต้องมีวิสัยทัศน์เชิงยุทธศาสตร์ เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกฝ่าย ปฏิบัติตามหน้าที่ตามพันธกิจให้บรรลุวัตถุประสงค์ขององค์กร มีการวางเป้าหมายการปฏิบัติงานที่ชัดเจน และอยู่ในระดับที่ตอบสนองต่อความคาดหวังของประชาชน สร้างกระบวนการปฏิบัติงานอย่างเป็นระบบและมีมาตรฐาน มีการจัดการความเสี่ยงและมุ่งเน้นผลการปฏิบัติงานที่เป็นเลิศ รวมถึงมีการติดตามประเมินผล และพัฒนาปรับปรุงการปฏิบัติงานให้ดีขึ้นอย่างต่อเนื่อง
2. **ความเสี่ยงต่อหลักประสิทธิภาพ (Efficiency)** ในการปฏิบัติงานต้องมีการใช้ทรัพยากรอย่างประหยัด เกิดผลิตภาพ คุ้มค่าการลงทุนและบังเกิดประโยชน์สูงสุดต่อส่วนรวม รวมทั้ง ต้องมีการลด

ขั้นตอนและระยะเวลาในการปฏิบัติงาน เพื่ออำนวยความสะดวกและลดภาระค่าใช้จ่าย ตลอดจนยกเลิกภารกิจที่ล้าสมัย และไม่มีความจำเป็น

3. **ความเสี่ยงต่อหลักการมีส่วนร่วม (Participation)** ต้องรับฟังความคิดเห็นของประชาชน เปิดให้ประชาชนมีส่วนร่วมในการรับรู้ เรียนรู้ ทำความเข้าใจ รวมทั้งแสดงทัศนะ ร่วมเสนอปัญหา/ประเด็นสำคัญที่เกี่ยวข้อง ร่วมคิดแก้ไขปัญหา ร่วมในกระบวนการตัดสินใจและการดำเนินงาน และร่วมตรวจสอบผลการปฏิบัติงาน
4. **ความเสี่ยงต่อหลักความโปร่งใส (Transparency)** ต้องปฏิบัติงานด้วยความซื่อสัตย์สุจริต ตรงไปตรงมา รวมทั้งต้องมีการเปิดเผยข้อมูลข่าวสารที่จำเป็นและเชื่อถือได้ ให้ประชาชนได้รับทราบอย่างสม่ำเสมอ ตลอดจนวางระบบให้การเข้าถึงข้อมูลข่าวสารเป็นไปโดยง่าย
5. **ความเสี่ยงต่อหลักการตอบสนอง (Responsiveness)** ต้องสามารถให้บริการได้อย่างมีคุณภาพ สามารถดำเนินการแล้วเสร็จภายในระยะเวลาที่กำหนด สร้างความเชื่อมั่นไว้วางใจ รวมถึงตอบสนองตามความคาดหวัง/ความต้องการของประชาชนผู้รับบริการ และผู้มีส่วนได้ส่วนเสียที่มีความหลากหลายและมีความแตกต่างกันได้อย่างเหมาะสม
6. **ความเสี่ยงต่อหลักภาระรับผิดชอบ (Accountability)** ในการปฏิบัติงานต้องสามารถตอบคำถามและชี้แจงได้เมื่อมีข้อสงสัย รวมทั้งต้องมีการจัดวางระบบการรายงานความก้าวหน้า และผลสัมฤทธิ์ตามเป้าหมายที่กำหนดไว้ต่อสาธารณะ เพื่อประโยชน์ในการตรวจสอบและการให้คุณให้โทษ ตลอดจนมีการจัดเตรียมระบบการแก้ไขหรือบรรเทาปัญหา และผลกระทบใด ๆ ที่อาจจะเกิดขึ้น
7. **ความเสี่ยงต่อหลักนิติธรรม (Rule of Law)** ต้องใช้อำนาจของกฎหมาย กฎระเบียบ ข้อบังคับในการปฏิบัติงานอย่างเคร่งครัด 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 ระหว่างกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง โดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง จะต้องไม่มีข้อคัดค้านที่หาข้อยุติไม่ได้ ในประเด็นที่สำคัญ

จากแนวคิดธรรมาภิบาลที่เกี่ยวข้อง สามารถแสดงความเชื่อมโยงต่อปัจจัยในการวิเคราะห์ความเสี่ยง เช่น

- ด้านกลยุทธ์ โครงการที่คัดเลือกมานั้น อาจมีความเสี่ยงต่อเรื่องประสิทธิผลและการมีส่วนร่วม
- ด้านการดำเนินงาน อาจมีความเสี่ยงต่อเรื่องประสิทธิภาพและความโปร่งใส
- ด้านการเงิน อาจมีความเสี่ยงต่อหลักนิติธรรมและภาระรับผิดชอบ
- ด้านกฎหมาย กฎระเบียบ อาจมีความเสี่ยงต่อเรื่องนิติธรรมและความเสมอภาค
- ด้านเทคโนโลยีสารสนเทศ อาจมีความเสี่ยงต่อเรื่องประสิทธิภาพและหลักการตอบสนอง

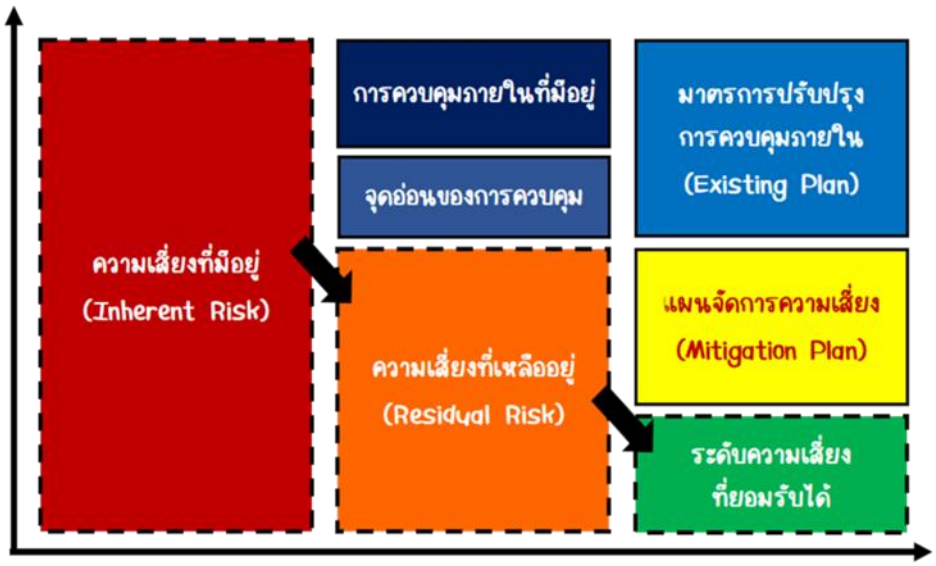
ทั้งนี้สามารถอธิบายความสัมพันธ์ ตามตารางด้านล่างได้ดังนี้

	หลักประสิทธิผล	หลักประสิทธิภาพ	หลักการมีส่วนร่วม	หลักความโปร่งใส	หลักการตอบสนอง	หลักภาระรับผิดชอบ	หลักนิติธรรม	หลักการกระจายอำนาจ	หลักความเสมอภาค	หลักการมุ่งเน้นฉันทามติ
Strategic Risk	✓		✓		✓	✓				
Operational Risk	✓	✓	✓	✓	✓			✓	✓	✓
Financial Risk	✓	✓		✓		✓	✓			
Compliance Risk	✓	✓			✓		✓		✓	
Information Technology Risk	✓	✓		✓	✓				✓	

8.2 การประเมินความเพียงพอของการควบคุมภายใน และการจัดทำมาตรการการปรับปรุงการควบคุมภายใน (Internal Control & Existing Plan)

เป็นการประเมินความเพียงพอของการควบคุมภายในภายใต้แนวคิดของการบริหารความเสี่ยง ว่าระดับของการควบคุมภายในยังอยู่ในระดับที่เพียงพอหรือไม่ ซึ่งจะต้องพิจารณาถึงความครบถ้วน เหมาะสม ของการมีนโยบาย คู่มือการปฏิบัติงาน แผนการปฏิบัติงาน เอกสารที่ใช้สำหรับลงบันทึกผลการทำงานและผลลัพธ์ที่ได้จากการทำงาน แบบฟอร์ม การกำหนดอำนาจการอนุมัติ วิธีปฏิบัติที่ให้เกิดความเชื่อมั่นพอประมาณในเนื้อหาและข้อมูลในการรายงานทั้งการเงินและไม่ใช่การเงิน กระบวนการเก็บรวบรวม ข้อมูลเกี่ยวกับปัจจัยนำเข้า (Input) การดำเนินงาน (Process) และผลการดำเนินงาน (Output) การรายงายผลการดำเนินงาน กิจกรรมการควบคุม งบประมาณ เครื่องและอุปกรณ์ และความเพียงพอของบุคลากร หากพบว่ายังมีจุดอ่อนในการควบคุมภายในก็จำเป็นต้องมีการจัดทำมาตรการปรับปรุงการควบคุมภายใน (Existing Plan) ให้การดำเนินงานของแผนงาน/โครงการ/กิจกรรม/บริการ มีประสิทธิภาพ ดังภาพ

แผนภาพแสดงหลักการบริหารความเสี่ยงและควบคุมภายใน



ทั้งนี้ประเภทของการควบคุมสามารถจัดกลุ่มได้ดังนี้

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 เป็นแผนปฏิบัติการจัดการความเสี่ยง โดยแผนดังกล่าวต้องได้รับความเห็นชอบจากผู้บริหารในระดับที่เกี่ยวข้อง เพื่อให้การสนับสนุนทรัพยากรที่จำเป็นตามที่กำหนดไว้ในแผน เช่น บุคลากร งบประมาณ เป็นต้น ซึ่งจะประกอบด้วย กิจกรรมแสดงขั้นตอนและวิธีการดำเนินงาน ระยะเวลา/วันที่ดำเนินการแล้วเสร็จ และผู้รับผิดชอบ โดยการเลือกกิจกรรมการควบคุม ควรมีการพิจารณาความเกี่ยวข้องเหมาะสมของกิจกรรมควบคุมที่มีต่อการตอบสนองความเสี่ยง และการนำมาใช้เพื่อให้บรรลุวัตถุประสงค์เป็นสำคัญ ไม่ใช่เพื่อให้เห็นว่าต้องมีกิจกรรมการควบคุมเท่านั้น กิจกรรมการควบคุมบางอย่างที่กำหนดอาจช่วยให้องค์กรบรรลุวัตถุประสงค์มากกว่าหนึ่งวัตถุประสงค์

8.3 การประเมินความเสี่ยง (Risk Assessment)

องค์กรต้องกำหนดให้หน่วยงานทุกระดับประเมินความเสี่ยงของทุกปัจจัยเสี่ยงที่ได้ระบุไว้ โดยอ้างอิงจากเกณฑ์วัดระดับความเสี่ยง โอกาสและผลกระทบ ที่องค์กรกำหนด โดยอาจใช้ฐานข้อมูลในอดีตหรือการคาดการณ์ในอนาคตเพื่อประกอบการประเมินระดับความเสี่ยง

การประเมินความเสี่ยงควรพิจารณาถึงความไม่แน่นอนของเหตุการณ์หรือเงื่อนไขต่าง ๆ ใน 2 ปัจจัย ดังต่อไปนี้

- โอกาสที่จะเกิดความเสี่ยง
- ผลกระทบของความเสี่ยง

<u>โอกาสเกิด</u> (Likelihood)

การประเมินโอกาสเกิดของความเสี่ยง โดยทั่วไปการหาข้อมูลมาทำการสนับสนุนการประมาณการที่ถูกต้องเป็นไปได้ยาก ในกรณีที่สามารถหาข้อมูลที่เกี่ยวกับเหตุการณ์ความล้มเหลวหรือความถี่ที่เกิดขึ้นในอดีต ต้องมีความมั่นใจในฐานข้อมูลดังกล่าวว่าสามารถบ่งชี้ถึงความเป็นไปได้ของเหตุการณ์ในอนาคตได้

การประเมินโอกาสเกิดขึ้นอยู่กับระยะเวลาที่นำมาพิจารณา ดังนั้น เมื่อทำการประเมินโอกาสเกิด ผู้บริหารต้องมีความชัดเจนในการกำหนดระยะเวลาที่จะใช้ในการพิจารณา โดยไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นได้ในระยะยาว

การกำหนดระดับของโอกาสเกิด

- กำหนดช่วงเวลาที่ชัดเจนสำหรับการพิจารณาโอกาสเกิด อย่างไรก็ตาม ไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นในระยะยาว
- ประยุกต์คำอธิบายในแต่ละคะแนน โดยระดับคะแนนนี้สามารถเปลี่ยนแปลงได้เช่นเดียวกับระดับคะแนนของผลกระทบ ขึ้นอยู่กับความเหมาะสมกับสถานการณ์ในขณะนั้น

<u>ผลกระทบ</u> (Impact)

การประเมินความเสี่ยงควรพิจารณาถึงผลกระทบทั้งทางด้านการเงิน และที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ผลกระทบสามารถวัดได้ในเชิงของการสูญเสียทางการเงินทั้งทางตรงและทางอ้อม ส่วนการวัดผลการดำเนินงานที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ความพึงพอใจของผู้มีส่วนได้ส่วนเสีย สภาพแวดล้อมและสังคม เป็นต้น

การประเมินผลกระทบของปัจจัยเสี่ยง ควรครอบคลุมทั้งการกำหนดผลกระทบในเชิงการเงินและผลกระทบที่มิใช่ทางการเงิน อย่างไรก็ตาม บางปัจจัยเสี่ยงอาจไม่สามารถกำหนดผลกระทบในเชิงการเงินที่ชัดเจนได้ ดังนั้น ในการประเมินความเสี่ยงเบื้องต้นจึงพิจารณาผลกระทบที่เกิดจากความเสี่ยงในเชิงคุณภาพเป็นส่วนใหญ่ โดยเมื่อพิจารณาระดับความรุนแรงของผลกระทบแล้วนั้น ความเสี่ยงที่มีผลกระทบมากหรือมีโอกาสเกิดสูง จำเป็นต้องได้รับการพิจารณาอย่างละเอียดจากผู้บริหารระดับสูงให้ทันท่วงที โดยกำหนดแผนการบริหารความเสี่ยงที่ท้าทาย และติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ

ตารางด้านล่างแสดงถึงตัวอย่างของผลกระทบที่เกิดจากความเสี่ยงในแบบต่าง ๆ

ประเภทของผลกระทบ	ตัวอย่าง
ด้านกลยุทธ์	• ระดับความสำเร็จในการดำเนินงานตามตัวชี้วัดระดับผลลัพธ์ (Outcome) และผลผลิต (Output) • ระดับความสำเร็จในการจัดทำแผนกลยุทธ์ หรือแผนต่าง ๆ
ด้านการดำเนินงาน	• ร้อยละความสำเร็จของการดำเนินงานตามเป้าหมาย (ประเมินในกรณีที่อยู่ระหว่างการดำเนินงาน) • ระดับความพึงพอใจในการให้บริการ
ด้านการเงิน	• ผลกระทบและความเสียหาย • การจัดหารายได้
ด้านกฎหมาย ระเบียบ	• ผลกระทบจากการไม่ปฏิบัติหรือละเว้น
ด้านเทคโนโลยีสารสนเทศ	• ความสามารถในการแก้ไขบริการเกิดเหตุขัดข้อง • ผลกระทบต่อผู้ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง ซึ่งเกิดจากระบบเทคโนโลยีสารสนเทศ

การกำหนดระดับของผลกระทบ

- กำหนดเงื่อนไขที่จะใช้ในการพิจารณา
- พิจารณาทั้งเงื่อนไขทางการเงินและเงื่อนไขอื่น ๆ ที่ไม่เกี่ยวข้องกับการเงิน เช่น อัตราส่วนเงินทุนหมุนเวียนเร็ว รายได้เทียบกับเป้าหมาย ชื่อเสียง ความสามารถในการบรรลุวัตถุประสงค์ อัตราการลาออกของเจ้าหน้าที่ ความปลอดภัยในชีวิตและทรัพย์สิน และเทคโนโลยีสารสนเทศ
- ทำให้มั่นใจได้ว่าเงื่อนไขนั้นสอดคล้องกับวัตถุประสงค์ขององค์กร
- กำหนดมูลค่าของผลกระทบ ตามระดับคะแนน 1-25 ในการจัดลำดับ โดยระดับคะแนนนี้อาจมีการเปลี่ยนแปลงได้ ขึ้นอยู่กับความเหมาะสมกับสถานการณ์ในขณะนั้น
- ทำให้มั่นใจว่ามูลค่าต่าง ๆ ที่กำหนดเพื่อใช้ในการจัดลำดับสำหรับเงื่อนไขที่ต่างกันมีความสอดคล้องกัน ดังตัวอย่าง ระดับผลกระทบ 3 ของผลกระทบทางการเงิน สามารถเทียบเท่ากับระดับผลกระทบ 3 ของผลกระทบด้านชื่อเสียง เป็นต้น

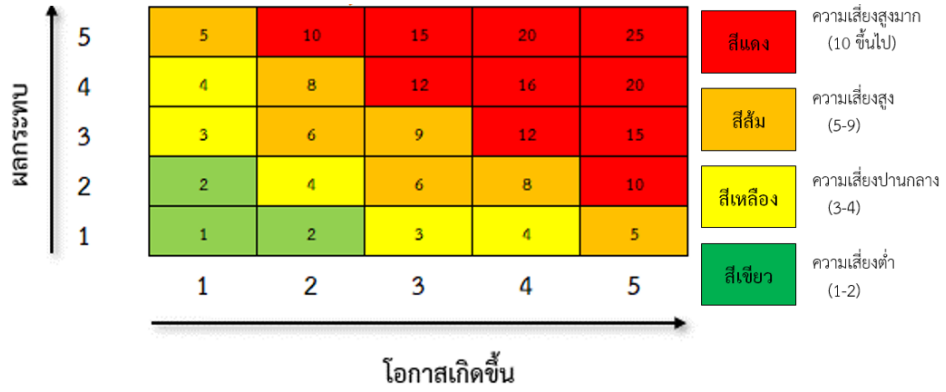
ประโยชน์ของผู้บริหารที่ได้จากการประเมินความเสี่ยงมีดังต่อไปนี้

- การเปรียบเทียบความเสี่ยงกับกลยุทธ์และนโยบายขององค์กร
- กลยุทธ์และนโยบายขององค์กรจัดอยู่ในทิศทางใด กลยุทธ์และนโยบายดังกล่าวยอมรับความเสี่ยงที่เกิดขึ้นได้มากน้อยเพียงใด รวมถึงความเสี่ยงที่สามารถระบุได้นั้น มีความสอดคล้องกับกลยุทธ์และนโยบายขององค์กรเพียงใด
- การบ่งชี้ถึงความเสี่ยงที่ไม่เป็นที่ยอมรับ

- องค์กรสามารถกำหนดระดับความเสี่ยงที่ยอมรับได้ และระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้หรือไม่ และการกำหนดดังกล่าว เป็นการกำหนดโดยภาพรวมหรือเป็นการกำหนดในรายปัจจัยเสี่ยง
- การคัดเลือกและจัดลำดับการดำเนินการที่เหมาะสมในการลดความเสี่ยง

8.4 การจัดลำดับความเสี่ยง (Risk Priority)

การจัดลำดับความเสี่ยง สามารถทำได้โดยการอ้างอิงกับตารางประเมินความเสี่ยง (Risk Assessment Matrix) ซึ่งการพิจารณาว่าความเสี่ยงใดมีนัยสำคัญ ที่ต้องนำมาดำเนินการก่อนหลัง โดยทั่วไปอาจใช้การกำหนดค่าลำดับความเสี่ยงทั้งในด้านของผลกระทบและโอกาสเกิด ทั้งนี้ การกำหนดนัยสำคัญของความเสี่ยงขององค์กร ควรได้รับการพิจารณาจากผู้บริหารระดับสูงและผ่านความเห็นชอบจากคณะอนุกรรมการด้านการบริหารความเสี่ยง หลังจากการประเมินความมีนัยสำคัญของความเสี่ยงเพื่อนำมาใช้ในการกำหนดกลยุทธ์การจัดการความเสี่ยงต่าง ๆ ควรคำนึงถึงประสิทธิผลของต้นทุนที่ต้องใช้ในการจัดการความเสี่ยงนั้น ๆ กับระดับความสำคัญของความเสี่ยงที่ลดลงว่าเหมาะสมเพียงใด ทั้งนี้ ความมีประสิทธิผลของการจัดการความเสี่ยงอาจประเมินได้ในเชิงของการลดลงของโอกาสเกิดและผลกระทบ ดังแสดงในตัวอย่าง ที่ระบุไว้ใน Risk Profile



ปัจจัยเสี่ยงแสดงให้เห็นว่าถึงแม้โอกาสเกิดจะน้อย แต่จะมีผลกระทบสูงมาก เนื่องจากเป็นองค์กรที่ให้บริการเทคโนโลยีสารสนเทศต่อภาครัฐ ภาคประชาชน ระดับประเทศ ทั้งนี้ สพร. ได้แบ่งระดับความเสี่ยงออกเป็น 4 ระดับ ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่ฝ่าย/ส่วนงาน/องค์กร สามารถยอมรับได้ โดยมีแผนจัดการความเสี่ยงหรือไม่มีแผนจัดการความเสี่ยงก็ได้
3-4	ปานกลาง	● ระดับความเสี่ยงที่ฝ่าย/ส่วนงาน ไม่สามารถยอมรับได้ โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
		• ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยให้ฝ่าย/ส่วนงาน นำไปบริหารความเสี่ยง โดยควบคุมและป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและมาตรการปรับปรุงการควบคุมภายใน) ให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้ และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและมาตรการปรับปรุงการควบคุมภายใน) ให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้โดยทันที และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น

8.5 การจัดทำแผนจัดการความเสี่ยง (Mitigation Plan)

เป็นการระบุว่ามีทางเลือกใดบ้างที่สามารถใช้ในการจัดการความเสี่ยง มีความเหมาะสม และนำไปปฏิบัติ เป็นส่วนหนึ่งของการบริหารความเสี่ยงของสำนักงาน ซึ่งจะต้องประเมินผลกระทบที่มีต่อโอกาสที่จะเกิด รวมทั้งต้นทุนและประโยชน์ที่ได้รับ เพื่อให้ความเสี่ยงที่เหลืออยู่ภายในช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ ทั้งนี้ การตอบสนองต่อความเสี่ยงแบ่งเป็น 4 ประการ คือ การยอมรับ (Take) การลด (Treat) การหลีกเลี่ยง/ยกเลิก (Terminate) และการโอนความเสี่ยง (Transfer) ซึ่งสำนักงานต้องจัดให้มีการควบคุมความเสี่ยงและเพดานความเสี่ยงที่เพียงพอและเหมาะสมตามแต่ละประเภทความเสี่ยง และต้องอยู่ภายใต้ระดับความเสี่ยงที่สำนักงานยอมรับได้ รวมทั้งสอดคล้องกับมาตรฐานและหลักเกณฑ์ของหน่วยงานกำกับดูแล แนวทางปฏิบัติที่ดี ตลอดจนนโยบายบริหารความเสี่ยงกับทิศทางและกลยุทธ์การดำเนินงานของสำนักงาน พร้อมทั้งกำหนดกระบวนการปฏิบัติตามการควบคุมความเสี่ยงและเพดานความเสี่ยงที่กำหนดไว้ แนวทางการอนุมัติข้อยกเว้นกรณีจำเป็นหรือเหตุการณ์ไม่ปกติต่าง ๆ รวมถึงการทบทวนการควบคุมความเสี่ยงและเพดานความเสี่ยงดังกล่าวเป็นระยะ เพื่อให้มีประสิทธิภาพในการควบคุมและป้องกันความเสี่ยงให้กับสำนักงาน รวมทั้งผู้บริหารต้องประเมินว่าปัจจุบันการจัดการความเสี่ยงเพียงพอหรือไม่ ทั้งประสิทธิภาพในการลดโอกาสเกิดความเสี่ยง และผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงต่าง ๆ หากไม่มีการจัดการความเสี่ยง หรือการจัดการในปัจจุบันไม่เพียงพอ ควรมีการพิจารณากิจกรรมอื่น ๆ เพิ่มเติมให้เหมาะสมและนำไปปฏิบัติ

<u>วัตถุประสงค์ของการจัดการความเสี่ยง</u>

- ลดโอกาสในการเกิดและผลกระทบของความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้โดยการจัดการสาเหตุของความเสี่ยงอย่างมีประสิทธิภาพ หรือโดยการจัดการผลกระทบที่อาจจะเกิดขึ้นของความเสี่ยง เช่น การมีเจ้าหน้าที่ปฏิบัติการที่พร้อมซ่อมแซมความเสียหายที่เกิดขึ้น เป็นต้น
- การลดผลกระทบของความเสี่ยง ซึ่งโดยมากมักใช้ระบบการเตือนภัย หรือระบบการบริหาร พร้อมด้วยการจัดทำแผนฉุกเฉิน หรือแผนฟื้นฟู

- การเพิ่มโอกาสในการเกิด หรือผลกระทบจากความเสี่ยงที่เป็นโอกาสให้มากที่สุด โดยการปฏิบัติเพื่อสร้างหรือหาโอกาส หรือการจัดการเพื่อให้ได้ผลลัพธ์ที่ดีขึ้น

<u>กลยุทธ์ในการบริหารความเสี่ยง</u>

การยอมรับความเสี่ยง (Take) ความเสี่ยงหลังการควบคุมอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใด ๆ เพิ่มเติมที่มีผลต่อโอกาสเกิด หรือผลกระทบของความเสี่ยง

- ไม่ดำเนินการใด ๆ เพิ่มเติม
- ยอมรับผลที่จะเกิดทั้งหมด
- กำหนดรางวัลเป้าหมายความเสียหาย และระดับการยอมรับ

การลดความเสี่ยง (Treat) การดำเนินการเพิ่มเติมเพื่อลดโอกาสเกิด หรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ตัวอย่างเช่น

- ดำเนินกิจกรรมในเชิงรุกหรือการควบคุมเพื่อลดโอกาสเกิดและผลกระทบ
- การดำเนินการด้านกลยุทธ์ กระบวนการและระบบ
- การพัฒนาบุคลากร ความชำนาญ และโครงสร้างองค์กร
- จัดทำแผนฉุกเฉิน
- พัฒนาแผนฟื้นฟู
- จัดเตรียมแผนรองรับการเสื่อมถอย (Fall-Back)
- การออกแบบใหม่ เช่น กระบวนการทางธุรกิจ ระบบ เครื่องมือ

การหลีกเลี่ยงความเสี่ยง (Terminate) การดำเนินการเพื่อยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง ทั้งนี้ หากทำการใช้กลยุทธ์นี้อาจต้องทำการพิจารณาวัตถุประสงค์ว่าสามารถบรรลุได้หรือไม่ เพื่อทำการปรับเปลี่ยนต่อไป

- ยุติการให้บริการ
- เปลี่ยนหรือปรับเป้าหมาย

การโอนย้ายความเสี่ยง (Transfer) การโอนย้าย หรือการแบ่งความเสี่ยงบางส่วนกับบุคคลหรือองค์กรอื่น

- การประกันภัย
- การร่วมทุน พันธมิตรทางธุรกิจ หุ้นส่วนทางธุรกิจ
- การกระจายความเสี่ยง

<u>แนวทางในการกำหนดกลยุทธ์การจัดการความเสี่ยง</u>

กลยุทธ์การจัดการความเสี่ยงถูกกำหนดขึ้นเพื่อลดระดับของความเสี่ยง ทั้งผลกระทบและโอกาสเกิดให้เป็นไปตามระดับความเสี่ยงที่ยอมรับได้ ในบางกรณีการรวมกลยุทธ์การจัดการความเสี่ยง อาจทำให้เกิดผลที่มีประสิทธิภาพมากขึ้นทั้งทางด้านต้นทุนและการปฏิบัติงาน ดังนั้น ควรต้องมีการพิจารณาการจัดการความเสี่ยงต่าง ๆ ที่อาจมีความเกี่ยวข้องกัน และอาจดำเนินการโดยหลายหน่วยงาน รวมทั้งคำนึงถึงต้นทุนที่อาจเกิดขึ้นในการจัดให้มีการจัดการความเสี่ยงสำหรับกำหนดเป็นกลยุทธ์ในการจัดการความเสี่ยงโดยรวม เพื่อให้เกิดการจัดการความเสี่ยงบูรณาการ

ผู้บริหารอาจพิจารณาปัจจัยในการกำหนดกลยุทธ์การจัดการความเสี่ยง ต่อไปนี้

- การประเมินผลกระทบและโอกาสเกิดจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง

ในการประเมินทางเลือกของแต่ละกลยุทธ์การจัดการความเสี่ยง ผู้บริหารต้องมีความเข้าใจว่า กิจกรรมการจัดการความเสี่ยงอาจส่งผลต่อผลกระทบและโอกาสเกิดของความเสี่ยงต่างกัน ดังนั้นแล้ว การประเมินผลกระทบและโอกาสเกิดของความเสี่ยงที่อาจเปลี่ยนแปลงจากการดำเนินการตามกิจกรรมการจัดการความเสี่ยง จึงควรพิจารณาก่อนการตัดสินใจเลือกกลยุทธ์ เพื่อให้ระดับความเสี่ยงสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ขององค์กร ทั้งนี้ การประเมินผลกระทบและโอกาสเกิดหลังจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยงสามารถอ้างอิงข้อมูลได้จากเหตุการณ์ในอดีต แนวโน้มของเหตุการณ์ที่อาจเกิดขึ้น และวิเคราะห์การเปลี่ยนแปลงที่อาจเกิดขึ้นในอนาคต ความเสี่ยงสามารถถูกระบุได้ทั้งอันตรายหรือโอกาสที่อาจเกิดขึ้น การกำหนดกลยุทธ์การจัดการความเสี่ยงจึงสามารถทำได้จากการประเมินปัจจัยหลัก 2 ประการ ดังนี้

1. ประเมินต้นทุนและผลตอบแทนของการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง

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

2. การประเมินความเป็นไปได้ที่จะประสบผลสำเร็จในการจัดการความเสี่ยง

เนื่องจากกิจกรรมการจัดการความเสี่ยงที่องค์กรจะกำหนดขึ้นนั้น ต้องประกอบด้วยปัจจัยหลายประเภทที่สนับสนุนให้การดำเนินการประสบความสำเร็จ ดังนั้น การประเมินความเป็นไปได้ที่กิจกรรมการจัดการความเสี่ยงจะประสบความสำเร็จจึงมีความจำเป็น โดยควรพิจารณาถึงปัจจัยต่าง ๆ เช่น ความรู้ความเข้าใจของบุคลากร งบประมาณที่ใช้ในการจัดการ ระยะเวลาแล้วเสร็จ เป็นต้น หากพิจารณาแล้วพบว่า กิจกรรมดังกล่าวมีแนวโน้มที่จะไม่ประสบความสำเร็จ ควรพิจารณาถึงกลยุทธ์การจัดการความเสี่ยงด้วยวิธีการอื่น เพื่อใช้เป็นทางเลือกหรือปรับปรุงแผนการจัดการความเสี่ยงที่มีอยู่ให้เหมาะสมยิ่งขึ้น

หลังจากได้ทำการประเมินเพื่อกำหนดกลยุทธ์การจัดการความเสี่ยงที่มีประสิทธิผลจากแนวทางที่ได้กล่าวมาแล้วข้างต้น ผู้บริหารต้องทำการกำหนดแผนการปฏิบัติงาน (Implementation Plan) หรือขั้นตอนในการปฏิบัติ (Procedure) โดยต้องระบุระยะเวลาแล้วเสร็จเพื่อให้มั่นใจได้ว่า จะมีการดำเนินงานตามกลยุทธ์เพื่อให้เกิดโอกาสตามที่คาดหวังไว้จริง และได้รับการดำเนินการโดยเจ้าของความเสี่ยง

- ความรับผิดชอบในการบริหารความเสี่ยง หรือ “การเป็นเจ้าของความเสี่ยง” (Risk Owner) คือ หน่วยงาน หรือบุคคลที่รับผิดชอบให้การดำเนินการจัดการความเสี่ยงบรรลุวัตถุประสงค์หรือประสบความสำเร็จ โดยทั่วไปเจ้าของความเสี่ยงจะต้องรับผิดชอบในการตัดสินใจ เกี่ยวกับแผนการบริหารความเสี่ยง และแผนการปรับปรุงที่เหมาะสมสำหรับความเสี่ยงที่ไม่สามารถยอมรับได้ เมื่อแผนได้ถูกอนุมัติและได้รับการเห็นชอบ เจ้าของความเสี่ยงจะต้องรับผิดชอบต่อการนำแผนไปปฏิบัติและติดตามผลการดำเนินงานของแผนนั้น และต้องแสดงให้ผู้บริหารเห็นความสำเร็จในการทำหน้าที่ของตนเกี่ยวกับการบริหารความเสี่ยง
- การพัฒนาการจัดการความเสี่ยงสำหรับความเสี่ยงที่ซับซ้อนอาจเกี่ยวข้องกับผู้บริหารระดับสูงและเจ้าหน้าที่หลายส่วนงาน ดังนั้น การสื่อสารที่ดีจึงเป็นสิ่งจำเป็นเพื่อให้แน่ใจว่าบุคคลที่เกี่ยวข้องภายในองค์กรได้ตระหนักถึงสิ่งที่กำลังดำเนินการ และบทบาทที่ต้องเกี่ยวข้องหรือปฏิบัติ

8.6 สารสนเทศและการสื่อสาร (Information & Communication)

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

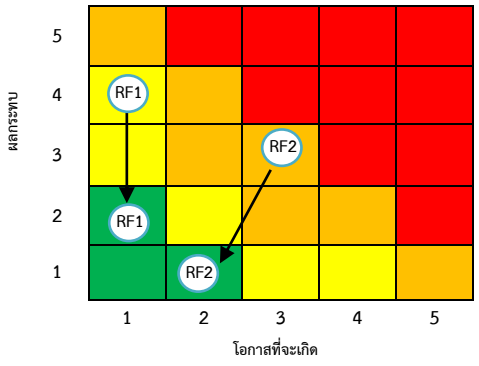
สารสนเทศที่ใช้ในการปฏิบัติงาน ได้มาจากแหล่งภายในและภายนอก ทั้งในรูปแบบเชิงปริมาณ และคุณภาพ ทั้งที่เป็นสารสนเทศทางการเงิน และที่มิใช่การเงิน ที่มีความเกี่ยวข้องกับวัตถุประสงค์ขององค์กรหลาย ๆ ประเภท

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

การสื่อสาร เป็นการสื่อสารข้อมูลที่จัดทำไว้แล้ว ส่งไปถึงผู้ที่ควรจะได้รับ หรือมีไว้พร้อมสำหรับผู้ที่ควรใช้สารสนเทศนั้น เพื่อให้ผู้ที่ได้รับใช้ข้อมูลดังกล่าวให้เกิดประโยชน์ในการตัดสินใจด้านต่าง ๆ และเพื่อสนับสนุนให้เกิดความเข้าใจ ตลอดจนมีการดำเนินงานตามวัตถุประสงค์ โดยระบบการสื่อสารต้องประกอบด้วยการสื่อสารภายในองค์กรและระบบการสื่อสารภายนอกองค์กร ซึ่งการสื่อสารแบ่งเป็น

- การสื่อสารภายในองค์กร ควรเป็นการสื่อสารหลายทาง เพื่อให้มีการดำเนินงานตามวัตถุประสงค์ของการควบคุมภายใน กระบวนการ และความรับผิดชอบในทุกระดับขององค์กร เช่น การสื่อสารจากระดับบนลงล่าง (Top-Down) หรือจากล่างขึ้นบน (Bottom-up) การสื่อสารในระดับเดียวกัน (Horizontal) โดยมีเทคนิคหรือเครื่องมือที่นำมาใช้สื่อสารระหว่างกัน ได้แก่ ระบบ MS Teams, Intranet, Video/Telephone Conference เป็นต้น
- สื่อสารภายนอกองค์กร เป็นการสื่อสารกับแหล่งข้อมูลภายนอกโดยทำอย่างเป็นทางการ เป็นระยะ ๆ อย่างสม่ำเสมอหรืออาจทำเป็นมีเหตุจำเป็นเป็นครั้งคราวก็ได้ เช่น การติดต่อทางโทรศัพท์ การเชิญพบปะ หารือ 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 A

ปัจจัยเสี่ยง A			
สถานะความเสี่ยง	**โอกาสเกิด**	**ผลกระทบ**	**ระดับความเสี่ยง**
ก่อนบริหารความเสี่ยง	3	5	15
ระดับความเสี่ยงที่คาดหวัง	2	2	4
ระดับความเสี่ยง Q1	2	5	10
ระดับความเสี่ยง Q2	2	4	8
ระดับความเสี่ยง Q3	2	2	4
ระดับความเสี่ยง Q4	1	2	2

ทั้งนี้ องค์กรจะต้องมีการสื่อสารเพื่อให้คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่ มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติ และกระบวนการบริหารความเสี่ยง นอกจากนี้ ควรมีการประเมินประสิทธิภาพและประสิทธิผลของการสื่อสาร เป็นระยะ ๆ เพื่อให้การสื่อสารเป็นส่วนหนึ่งของการควบคุมภายใน ที่เป็นประโยชน์สูงสุดต่อองค์กร

8.7 การติดตามและประเมินผล (Monitoring)

การติดตามและการรายงานผลเป็นกิจกรรมที่ใช้เพื่อติดตามและสอบทานแผนการจัดการความเสี่ยง เพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงมีประสิทธิภาพและเหมาะสม หรือควรปรับเปลี่ยน หากแผนนั้นไม่มีประสิทธิภาพเพียงพอ โดยกำหนดข้อมูลที่ต้องติดตาม และความถี่ในการสอบทาน และควรกำหนดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อประเมินว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้วหรือมีความเสี่ยงใหม่เพิ่มขึ้น

การติดตามผลโดยทั่วไปมักจะดำเนินการโดยผู้บริหารและบุคลากรภายในองค์กรเอง อย่างไรก็ตามอาจให้บุคคลภายนอก เช่น ที่ปรึกษา หรือผู้เชี่ยวชาญอิสระ ช่วยในการติดตามการจัดการความเสี่ยงเป็นครั้งคราวได้ ความเสี่ยงและการจัดการต่อความเสี่ยงอาจมีการเปลี่ยนแปลงตลอดเวลา การจัดการต่อความเสี่ยงที่เคยมีประสิทธิผล อาจเปลี่ยนเป็นกิจกรรมที่ไม่เหมาะสม กิจกรรมการควบคุมอาจมีประสิทธิผลน้อยลง หรือไม่ควรดำเนินการต่อไป 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 ยังควรสามารถบ่งชี้หรือพยากรณ์ให้ผู้บริหารหน่วยงาน และผู้บริหารสายงานสามารถคาดคะเนถึงความเสี่ยงที่อาจจะเกิดขึ้นในอนาคต (Forward Looking/Leading Indicators) ได้อีกด้วย

ตารางแสดง ตัวอย่างดัชนีชี้วัดความเสี่ยง (KRIs)

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

แนวทางการรายงานผลการดำเนินงาน มีดังนี้

1. คณะอนุกรรมการด้านการบริหารความเสี่ยง

1.1 รายงานต่อคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

- รายงานแผนการบริหารความเสี่ยงประจำปี รวมทั้งแผนปฏิบัติการเพื่อการจัดการความเสี่ยง ปีละ 1 ครั้ง
- รายงานผลการดำเนินการและความคืบหน้าการจัดการความเสี่ยงที่สำคัญระดับองค์กร ต่อคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ไตมาสละ 1 ครั้ง

1.2 รายงานต่อคณะกรรมการตรวจสอบ

- รายงานผลการดำเนินงานอย่างน้อยปีละ 1 ครั้ง

2. ผู้ประสานงานด้านการบริหารความเสี่ยง (Risk Agent)

2.1 รายงานต่อฝ่ายที่เกี่ยวข้อง /รองผู้อำนวยการ สพร. /ผู้อำนวยการ สพร. /คณะอนุกรรมด้านการบริหารความเสี่ยง

2.2 รายงานความเสี่ยงระดับองค์กรในส่วนที่รับผิดชอบและแผนปฏิบัติการการจัดการความเสี่ยง ตลอดจนความคืบหน้าในการจัดการความเสี่ยงตามแผน พร้อมทั้งปัญหาและอุปสรรค ไตรมาสละ 1 ครั้ง

3. ส่วนบริหารความเสี่ยง

3.1 รายงานต่อคณะอนุกรรมการด้านการบริหารความเสี่ยง

3.2 รายงานความเสี่ยงที่สำคัญระดับองค์กร รวมทั้งรายละเอียดการจัดการความเสี่ยง ตลอดจนความคืบหน้าของแผนปฏิบัติการและประเด็นสำคัญเพื่อการพิจารณาของคณะอนุกรรมการด้านการบริหารความเสี่ยงทุกครั้ง ที่มีการประชุมคณะอนุกรรมการด้านการบริหารความเสี่ยง

3.3 รายงานเหตุการณ์ที่เกิดขึ้นใหม่ทั้งที่เป็นโอกาสและความเสี่ยงที่มีผลต่อสำนักงานจากสภาพแวดล้อมที่เปลี่ยนแปลงไปเป็นการเฉพาะกิจ

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

สำนักงานต้องสนับสนุนให้เกิดการสื่อสารในเชิงรุกและให้มีการสื่อสารอย่างสม่ำเสมอ ช่องทางในการสื่อสารอย่างเป็นทางการที่ใช้ในการพิจารณาความเสี่ยง การควบคุม และแผนการดำเนินการ ได้แก่ การประชุมทั่วไปของผู้บริหาร การประชุมคณะทำงาน รายงานประจำเดือนสำหรับผู้บริหาร การประชุมคณะอนุกรรมการด้านการบริหารความเสี่ยง เป็นต้น การสื่อสารอย่างต่อเนื่องจะช่วยให้มีข้อมูลความเสี่ยงที่เพียงพอและได้รับการนำเสนอเพื่อใช้ในการตัดสินใจอย่างทันท่วงที ในบางกรณีการจัดการกับความเสี่ยงด้วยวิธีการที่เร่งด่วน เช่น การประสานงานทางโทรศัพท์ อาจมีความเหมาะสมกว่ารอการจัดทำรายงานอย่างเป็นทางการ ผู้ที่เกี่ยวข้องต้องรายงานความเสี่ยงที่มีระดับความเสี่ยงสูงให้แก่ผู้บังคับบัญชาทราบอย่างสม่ำเสมอและทันท่วงที พร้อมทั้งอธิบายวิธีการจัดการความเสี่ยงเหล่านั้น นอกจากนี้ ผู้บริหารในแต่ละหน่วยงานควรพิจารณาและนำเสนอความเสี่ยงที่มีระดับความเสี่ยงสูงของหน่วยงาน หรือความเสี่ยงที่ควรจะต้องได้รับการจัดการในระดับที่สูงกว่าขึ้นไปยังผู้บริหารในสายบังคับบัญชาเพื่อทำการพิจารณาความเสี่ยงและหาแนวทางการจัดการความเสี่ยงในระดับงานที่สูงขึ้นต่อไป

9. ปัจจัยสำเร็จในการบริหารความเสี่ยงขององค์กร

การบริหารความเสี่ยงที่ประสบความสำเร็จต้องมีปัจจัยสำคัญ ซึ่งประกอบทั้งด้านทรัพยากรและโครงสร้างพื้นฐานที่จำเป็นเพื่อให้เกิดการบริหารความเสี่ยงที่ประสบผลสำเร็จและยั่งยืน ดังนี้

1. **ความมุ่งมั่นของผู้บริหารในการจัดให้มีระบบการบริหารความเสี่ยง**

การปฏิบัติตามกรอบการบริหารความเสี่ยงขององค์กร จะประสบความสำเร็จเพียงใดขึ้นอยู่กับเจตนารมย์ การสนับสนุน การมีส่วนร่วม และความเป็นผู้นำของผู้บริหารระดับสูงในองค์กร คณะกรรมการและผู้บริหารระดับสูงต้องให้ความสำคัญและสนับสนุนให้ทุกคนในองค์กรเข้าใจความสำคัญในคุณค่าของการบริหารความเสี่ยงต่อองค์กร มิฉะนั้นแล้ว การบริหารความเสี่ยงไม่สามารถเกิดขึ้นได้ การบริหารความเสี่ยงต้องเริ่มต้นจากผู้นำสูงสุดขององค์กรต้องการให้เกิดระบบขึ้น โดยกำหนดนโยบายให้มีการปฏิบัติ รวมถึงการกำหนดให้ผู้บริหารต้องใช้ข้อมูลเกี่ยวกับความเสี่ยงในการตัดสินใจและบริหารงาน

2. **ความเข้าใจเกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงในทางเดียวกัน**

การใช้คำนิยามเกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงแบบเดียวกัน จะทำให้มีประสิทธิภาพในการกำหนดวัตถุประสงค์ นโยบาย กระบวนการ เพื่อใช้ในการบ่งชี้และประเมินความเสี่ยง และกำหนดวิธีการจัดการความเสี่ยงที่เหมาะสม

องค์กรที่จัดทำนโยบาย และกรอบ การบริหารความเสี่ยง ที่มีคำอธิบายองค์ประกอบในกรอบการบริหารความเสี่ยงอย่างชัดเจน จะทำให้ผู้บริหารและเจ้าหน้าที่ทุกคนเข้าใจความเสี่ยงในแนวทางเดียวกัน และมีจุดหมายร่วมกันในการบริหารความเสี่ยง

3. **กระบวนการบริหารการเปลี่ยนแปลง**

ในการนำเอากระบวนการและระบบบริหารแบบใหม่มาใช้ องค์กรจำเป็นต้องมีการบริหารการเปลี่ยนแปลงเหล่านี้ การพัฒนาการบริหารความเสี่ยงก็เช่นเดียวกัน ต้องมีการชี้แจงให้ผู้บริหารและเจ้าหน้าที่ทุกคนรับทราบถึงการเปลี่ยนแปลง และผลที่องค์กรและแต่ละบุคคลจะได้รับจากการเปลี่ยนแปลงเหล่านั้น

4. **การกำหนดกระบวนการบริหารความเสี่ยงที่ต่อเนื่อง**

องค์กรที่ประสบความสำเร็จในการปฏิบัติตามกระบวนการบริหารความเสี่ยง คือ องค์กรที่สามารถนำกระบวนการบริหารความเสี่ยงมาปฏิบัติอย่างทั่วถึงทั้งองค์กร และกระทำอย่างต่อเนื่องสม่ำเสมอ

5. **การสื่อสาร การเรียนรู้ และการอบรมที่มีประสิทธิภาพ**

วัตถุประสงค์ของการสื่อสารอย่างมีประสิทธิผลนั้น เพื่อให้มั่นใจได้ว่า

- ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา
- ผู้บริหารสามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่
- มีการติดตามแผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กรและจัดการความเสี่ยงต่าง ๆ เพื่อให้องค์กรมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด โดยที่การสื่อสารเกี่ยวกับกลยุทธ์ การบริหารความเสี่ยงและวิธีปฏิบัติมีความสำคัญอย่างมาก เพราะการสื่อสารจะเน้นให้เห็นถึงความเชื่อมโยงระหว่างการบริหารความเสี่ยงกับกลยุทธ์องค์กร การชี้แจงทำความเข้าใจต่อเจ้าหน้าที่ทุกคนถึงความรับผิดชอบแต่ละบุคคลต่อกระบวนการบริหารความเสี่ยง จะช่วยให้เกิดการยอมรับในกระบวนการและนำมาซึ่ง

ความสำเร็จในการพัฒนาการบริหารความเสี่ยง 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 และความรับผิดชอบของแต่ละบุคคลในการจัดการความเสี่ยง และสื่อสารข้อมูลเกี่ยวกับความเสี่ยง การฝึกอบรมในองค์กรควรคำนึงถึงประเด็นดังต่อไปนี้

- ความแตกต่างกันของระดับความรับผิดชอบในการบริหารความเสี่ยง
- ความรู้ที่เกี่ยวกับความเสี่ยงและการบริหารความเสี่ยงที่มีอยู่แล้วในองค์กร

ระบบการประเมินผลการดำเนินงาน ถือเป็นเครื่องมือสำคัญที่ใช้ในการส่งเสริมความรับผิดชอบของแต่ละบุคคล โดยความรับผิดชอบเกี่ยวกับการบริหารความเสี่ยงควรกำหนดรวมอยู่ในงานที่แต่ละบุคคลรับผิดชอบและในคำอธิบายลักษณะงาน (Job Description) การประเมินผลการดำเนินงานส่วนที่เกี่ยวกับการบริหารความเสี่ยงมีประเด็นที่ควรประเมินดังต่อไปนี้

- ความรับผิดชอบและการสนับสนุนกระบวนการบริหารความเสี่ยงและกรอบการบริหารความเสี่ยงที่แต่ละบุคคลมีต่อองค์กร
- การวัดระดับของความเสี่ยงที่บุคคลนั้นเป็นผู้รับผิดชอบว่าความเสี่ยงได้รับการจัดการอย่างมีประสิทธิผลเพียงใด

8. กระบวนการติดตามการบริหารความเสี่ยง

ขั้นตอนสุดท้ายของปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง คือ การกำหนดวิธีที่เหมาะสมในการติดตามการบริหารความเสี่ยง

การติดตามกระบวนการบริหารความเสี่ยง

- การนำแผนตอบสนองความเสี่ยงไปปฏิบัติ และระดับความเสี่ยงที่เหลืออยู่หลังการปฏิบัติตามแผน
- การรายงานและการสอบทานตามขั้นตอนตามกระบวนการบริหารความเสี่ยง
- ความชัดเจนและสม่ำเสมอของการมีส่วนร่วมและความมุ่งมั่นของผู้บริหารระดับสูง
- บทบาทของผู้นำในการสนับสนุนและติดตามการบริหารความเสี่ยง
- การประยุกต์ใช้เกณฑ์การประเมินผลการดำเนินงานที่เกี่ยวข้องกับการบริหารความเสี่ยง

ส่วนที่ 3
การบริหารความเสี่ยงด้านกลยุทธ์ ด้านการดำเนินงาน ด้านการเงิน ด้านกฎหมาย ระเบียบ และด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ (S-O-F-C-IT)

1. การบริหารความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

1.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการกำหนดนโยบายต่าง ๆ เช่น นโยบายระดับรัฐจนถึงนโยบายในระดับผู้บริหาร แผนกลยุทธ์ แผนดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับสภาพแวดล้อมภายใน และปัจจัยภายนอก ทำให้มีโอกาสที่จะไม่ประสบความสำเร็จตามทิศทางที่กำหนดไว้ ซึ่งจะส่งผลกระทบต่อตัวชี้วัดผลการปฏิบัติงานของสำนักงาน

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

แผนธุรกิจ (Business Plan) หมายถึง แผนที่กำหนดกรอบการดำเนินงานโดยรวมของสำนักงาน เพื่อสนับสนุนการปฏิบัติงานให้สำเร็จตามแผนกลยุทธ์ และเป็นแนวทาง ให้แก่ หน่วยงานต่าง ๆ ในการกำหนดแผนปฏิบัติการ (Action Plan) โดยทั่วไปจะเป็นแผนระยะสั้นไม่เกิน 1 ปี ประกอบด้วย เป้าหมาย ผลดำเนินการ หน่วยงานที่รับผิดชอบ ปริมาณทรัพยากรที่ใช้ กรอบเวลาการดำเนินงาน และเกณฑ์ในการติดตามผลการปฏิบัติงาน ซึ่งควรสอดคล้องกับงบประมาณของสำนักงานด้วย

1.2 ที่มาของความเสี่ยงด้านกลยุทธ์ สามารถจำแนกได้ 2 ประเภท ดังนี้

1.2.1 ปัจจัยความเสี่ยงภายนอก หมายถึง ปัจจัยที่สำนักงาน ไม่สามารถควบคุมได้ หรือควบคุมได้ยาก ซึ่งจะส่งผลกระทบหรือเป็นอุปสรรคต่อการจัดทำแผนกลยุทธ์ แผนดำเนินงานของสำนักงาน และการปฏิบัติ เพื่อให้บรรลุเป้าหมายที่วางไว้ของสำนักงาน

(1) การได้รับนโยบายต่าง ๆ จากหน่วยงานภายนอกที่กำกับดูแลสำนักงานนั้น ซึ่งสำนักงานจะต้องสามารถสื่อสารสู่เจ้าหน้าที่ได้อย่างถูกต้องตามที่ได้รับนโยบายมา เพื่อที่หน่วยงานต่าง ๆ ของสำนักงาน จะได้นำไปกำหนดในแผนกลยุทธ์และแผนดำเนินงานได้อย่างสอดคล้องตามนโยบายที่ได้รับ

(2) การเปลี่ยนแปลงนโยบายระดับรัฐ อาจทำให้สภาวะการทำงานหยุดชะงัก หรือต้องวางกลยุทธ์และแผนการดำเนินงานใหม่

(3) การเปลี่ยนแปลงพฤติกรรมของกลุ่มลูกค้าเป้าหมาย การเปลี่ยนแปลงของโครงสร้างประชากรและความต้องการของลูกค้า จะมีผลต่อฐานลูกค้าของสำนักงาน ซึ่งสำนักงานต้องมีการกำหนดกลุ่มลูกค้าเป้าหมายที่มีศักยภาพ และวิธีการเสนอบริการที่ดีให้แก่ลูกค้าเหล่านั้น เพื่อป้องกันความเสี่ยงที่จะสูญเสียส่วนแบ่งตลาด

(4) การเลือกใช้เทคโนโลยีเป็นความเสี่ยงที่มีความสำคัญต่อการดำเนินงานของสำนักงานอย่างมาก ดังนั้น สำนักงานต้องมีการจัดการความเสี่ยงจากการเลือกใช้เทคโนโลยี

เพื่อตอบสนองต่อนโยบายที่ได้รับ และสนับสนุนต่อแผนกลยุทธ์ แผนดำเนินงานของสำนักงาน

(5) การเกิดภัยพิบัติจากธรรมชาติ เช่น อุทกภัยปี พ.ศ. 2554 ภัยจากการประท้วงจนก่อให้เกิดการจลาจล แต่ระดับความรุนแรงของผลกระทบดังกล่าวขึ้นอยู่กับขอบเขตการดำเนินงานที่เกี่ยวข้องกับเหตุการณ์หรือภัยพิบัติ และความสามารถในการปรับตัวของสำนักงาน

(6) กฎหมาย มติคณะรัฐมนตรี ข้อบังคับ ระเบียบ ประกาศ และคำสั่ง ตลอดจนระเบียบของหน่วยงานที่กำกับดูแล อาจเป็นอุปสรรคในการดำเนินงาน อันส่งผลกระทบต่อการปฏิบัติตามแผนกลยุทธ์ และแผนดำเนินงานให้บรรลุเป้าหมาย และจำเป็นต้องปรับเปลี่ยนแผนกลยุทธ์ และแผนดำเนินงานให้สอดคล้องกับกฎหมาย ฯลฯ

1.2.2 ปัจจัยความเสี่ยงภายใน หมายถึง ปัจจัยที่สำนักงานสามารถควบคุมได้ แต่สามารถส่งผลกระทบ หรือเป็นอุปสรรคต่อการดำเนินงานตามแผนกลยุทธ์เพื่อให้บรรลุเป้าหมาย ได้แก่

(1) นโยบายของคณะกรรมการ สพร. และผู้บริหาร สพร. เป็นปัจจัยสำคัญในการกำหนดแนวทาง หรือบทบาทของ สพร.

(2) การขับเคลื่อนแผนยุทธศาสตร์ และแผนปฏิบัติการของ สพร. เป็นปัจจัยสำคัญในการเพิ่มประสิทธิภาพ และการปรับเปลี่ยนการบริหารงานภาครัฐให้อยู่ในรูปแบบดิจิทัล

(3) การดำเนินงานตามตัวชี้วัดขององค์กร ซึ่งเป็นตัวชี้วัดของ สพร.

(4) กระบวนการสื่อสารภายในองค์กร สำนักงานต้องจัดให้มีกระบวนการสื่อสารองค์กรในเรื่องแผนกลยุทธ์ และแผนดำเนินงานขององค์กรสู่เจ้าหน้าที่อย่างทั่วถึงทุกระดับและต่อเนื่อง

(5) โครงสร้างองค์กร การจัดโครงสร้างองค์กร มีความสำคัญต่อการปฏิบัติตามแผนกลยุทธ์และแผนดำเนินงานให้บรรลุเป้าหมายและมีประสิทธิภาพ หากสำนักงานไม่มีการทบทวนการแบ่งแยกหน้าที่ความรับผิดชอบตามนโยบาย หรือภารกิจที่ได้รับจากรัฐบาลเป็นรายปี หรือรายเฉพาะกิจจะทำให้เกิดปัญหาในการจัดการ เพื่อบรรลุต่อเป้าหมายที่ต้องการ

(6) ความเพียงพอของข้อมูล ผู้บริหารของสำนักงาน จะต้องได้รับข้อมูลที่เหมาะสมเพื่อใช้ในการบริหารความเสี่ยงด้านนโยบายและกลยุทธ์ การได้รับข้อมูลไม่เพียงพอ ไม่เหมาะสม ไม่ถูกต้องและไม่ทันกาล จะเป็นอุปสรรคต่อการเข้าใจสภาวการณ์ และส่งผลต่อการวางแผนกลยุทธ์ และแผนดำเนินงานการกำหนดเป้าหมาย และการบริหารงานของสำนักงาน

ตัวอย่างปัจจัยเสี่ยงทางด้านกลยุทธ์

ตัวอย่างปัจจัยเสี่ยงด้านกลยุทธ์	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การดำเนินงานตามแผนกลยุทธ์ในบางกลยุทธ์ที่สำคัญไม่เป็นไปตามเป้าหมาย	1. โครงสร้างองค์กรไม่เหมาะสมกับการตอบสนองของภารกิจ และกลยุทธ์ที่สำคัญ 2. ขาดการติดตามการเปลี่ยนแปลงนโยบายภาครัฐระหว่างปีงบประมาณ	✓	✓
ขาดการบูรณาการกลยุทธ์ในระดับองค์กรและฝ่ายงาน	1. ไม่มีการกำหนดเป้าประสงค์ที่เป็นรูปธรรมสำหรับยุทธศาสตร์ในระดับองค์กร และเป็นที่ยอมรับทั่วทั้งองค์กร 2. ขาดการติดตามการดำเนินงานผลความสำเร็จของเป้าประสงค์ในยุทธศาสตร์หลัก และเชื่อมโยงกับผลความสำเร็จของโครงการ	✓ ✓	

2. การบริหารความเสี่ยงด้านการดำเนินงาน (Operational Risk)

2.1 ความเสี่ยงด้านการดำเนินงาน (Operational Risk)

หมายถึง ความเสี่ยงที่ทำให้เกิดความเสียหาย อันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดี หรือขาดธรรมาภิบาลในองค์กร และขาดการควบคุมดูแลที่เหมาะสม โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน คน (เจ้าหน้าที่ บุคคลภายนอก หรือลูกค้า) ระบบงาน หรือเหตุการณ์ภายนอก ซึ่งส่งผลกระทบต่อการดำเนินงานของสำนักงาน

ความเสี่ยงด้านการดำเนินงาน ยังครอบคลุมถึงเหตุการณ์ความเสียหาย (Loss Incidents) ที่อาจเกิดขึ้นเนื่องจากการดำเนินงานผิดพลาดของหน่วยงานใด ๆ ในสำนักงาน และสามารถเกิดขึ้นได้กับการปฏิบัติงานในทุกระดับชั้น นอกจากนี้ ความเสี่ยงด้านการดำเนินงานที่เกิดขึ้นกับหน่วยงานหนึ่ง อาจส่งผลกระทบและก่อให้เกิดความเสียหายแก่หน่วยงานอื่น ๆ ต่อเนื่องกันไปได้ ดังนั้น จึงมีความจำเป็นที่ในแต่ละหน่วยงานของสำนักงานต้องมีระบบการบริหารความเสี่ยงด้านการดำเนินงานที่มีประสิทธิภาพ และเหมาะสมกับสภาวะแวดล้อมในการดำเนินธุรกิจ เพื่อให้มั่นใจว่าสำนักงานสามารถจัดการความเสี่ยงด้านการดำเนินงานได้ และลดความสูญเสียให้อยู่ในระดับต่ำที่สุด

2.2 ที่มาของความเสี่ยงด้านการปฏิบัติงาน สามารถจำแนกได้ 8 ประเภท ดังนี้

2.2.1 การยกระดับศักยภาพและการเพิ่มประสิทธิภาพในการดำเนินงาน ซึ่งอยู่ในส่วนของขั้นตอน หรือกระบวนการที่ขาดประสิทธิภาพ หรือความเหมาะสม

2.2.2 การบริหารจัดการ Supply Chain ทั้งในส่วนของการดำเนินงานตาม Core Business Process อาทิเช่น การดำเนินงานมีความล่าช้า ขาดการบูรณาการการทำงานร่วมกัน และการดำเนินงานตาม Supporting Process ของการติดตาม ประเมินผล ซึ่งมีสาเหตุมาจากการที่กระบวนการมีความซับซ้อน หรือขาดการศึกษาวิเคราะห์ และกำหนดกระบวนงานไม่เพียงพอ

2.2.3 การบริหารจัดการทรัพยากรบุคคล เช่น การรักษาบุคลากร อัตรากำลังคนไม่เพียงพอ หรือขาดแรงจูงใจ และความผูกพันกับองค์กร

2.2.4 การให้บริการ ไม่ว่าจะเป็นความพึงพอใจต่ำ การมีข่าวเชิงลบ หรือการไม่สามารถแก้ไขบริการที่เกิดเหตุขัดข้องได้ เป็นต้น

2.2.5 การบริหารจัดการ SLA ซึ่งอาจเกิดจากการที่ไม่สามารถแก้ไข Incident ได้ตาม SLA ที่กำหนด หรือขาดการจัดลำดับความสำคัญในการแก้ไข Incident

2.2.6 ความต่อเนื่องในการดำเนินธุรกิจ/โครงการ โดยทบทวนการหยุดชะงักของการดำเนินงาน ซึ่งมีเหตุมาจากการขาดงบประมาณในการดำเนินงาน ขาดบุคลากร รวมทั้งการดำเนินงานขาดความคุ้มค่า

2.2.7 การทบทวนของเทคโนโลยี รวมทั้ง อุปกรณ์ เครื่องมือเครื่องใช้ต่าง ๆ ที่ล้าสมัยไม่เป็นปัจจุบัน ซึ่งอาจส่งผลในการดำเนินงานมีความผิดพลาด

2.2.8 การบริหาร Outsource/Vendor เช่น การที่ Outsource/Vendor ไม่สามารถส่งมอบงานได้ทันตามกำหนด หรือมีการยกเลิกการให้บริการ

ตัวอย่างปัจจัยเสี่ยงด้านการดำเนินงาน

ตัวอย่างปัจจัยเสี่ยงด้านการดำเนินงาน	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
กระบวนการประเมินผลการปฏิบัติงานยังล่าช้า	1. วิธีการประเมิน รวมทั้งแบบฟอร์มการประเมิน และวิธีการประมวลผลมีความซับซ้อน 2. ขาดการสื่อสารระบบประเมินผลการปฏิบัติงานให้พนักงานรับทราบ	✓ ✓	
การดำเนินงานโครงการมีความล่าช้า	1. ไม่มีการสรุปประเด็นปัญหา และกำหนดระยะเวลาในการแก้ไขที่ชัดเจน 2. ไม่ได้รับการจัดสรรงบประมาณในการดำเนินงานโครงการ	✓	✓

3. การบริหารความเสี่ยงด้านการเงิน (Financial Risk)

3.1 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 โดยไม่สามารถบริหารเงินทุนหมุนเวียนให้มีสภาพคล่อง เพื่อให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่อง

โดยรายงานทางการเงินที่มีส่วนสนับสนุนในการวิเคราะห์ความเสี่ยงทางด้านการเงิน ได้แก่

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

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

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

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

3.2 ที่มาของความเสี่ยงด้านการเงิน สามารถจำแนกเป็นปัจจัยเสี่ยงได้ 2 ประเภท ดังนี้

3.2.1 ปัจจัยความเสี่ยงภายนอก ได้แก่

(1) ความเสี่ยงจากความไม่ตระหนักถึงความสำคัญของภารกิจของสำนักงาน หรือการที่งบประมาณของประเทศมีจำกัด ทำให้สำนักงาน ได้รับจัดสรรงบประมาณไม่สอดคล้องกับความจำเป็น และแผนงานที่กำหนดไว้

(2) ความเสี่ยงจากการเปลี่ยนแปลงกฎระเบียบ กฎหมาย หรือกฎเกณฑ์ด้านการเงินต่าง ๆ ของรัฐบาล ที่มีผลกระทบต่อการปฏิบัติงานด้านการเงิน และงบประมาณของสำนักงาน

(3) ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของสิ่งแวดล้อมภายนอกต่าง ๆ ทั้งภายในประเทศและภายนอกประเทศ ที่ทำให้เกิดความผันผวนของค่าเงิน อัตราแลกเปลี่ยน อัตราดอกเบี้ย ฯลฯ ที่มีผลกระทบต่อการบริหารด้านการเงินของสำนักงาน

3.2.2 ปัจจัยความเสี่ยงภายใน ได้แก่

(1) การเปลี่ยนแปลง และความไม่ชัดเจนของนโยบายและกลยุทธ์ระดับองค์กร ซึ่งส่งผลต่อกลยุทธ์ในระดับปฏิบัติการ และมีผลกระทบทั้งทางตรงและทางอ้อมต่อแผนการปฏิบัติงานด้านการเงิน และงบประมาณ เช่น การจัดหารายได้ไม่เป็นไปตามเป้าหมาย

(2) การเปลี่ยนแปลงโครงสร้างองค์กร อาจทำให้มีผลกระทบต่อค่าใช้จ่ายทางการเงิน และการใช้จ่ายเงินงบประมาณของสำนักงาน

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

ตัวอย่างปัจจัยเสี่ยงทางด้านการเงิน

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

4. การบริหารความเสี่ยงด้านกฎหมาย ระเบียบ (Compliance Risk)

4.1 ความเสี่ยงด้านกฎหมาย ระเบียบ (Compliance Risk)

หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการ หรือการปฏิบัติงานที่ไม่เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง ทำให้มีผลกระทบต่อธรรมาภิบาลหรือต่อสำนักงาน และเจ้าหน้าที่ ทั้งนี้ ความเสี่ยงด้านกฎหมาย ระเบียบ ยังรวมถึงความเสี่ยงจากการตีความกฎหมาย การไม่ทราบ การไม่เข้าใจกฎระเบียบที่ไม่สอดคล้องตรงกันของหน่วยงานต่าง ๆ หรือการละเว้นการดำเนินการ หรือการปฏิบัติงานให้เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง

4.2 ที่มาของความเสี่ยงด้านกฎหมาย ระเบียบ สามารถแบ่งจำแนกปัจจัยเสี่ยงได้ 2 ประเภท คือ

4.2.1 การดำเนินการตามกฎหมาย ซึ่งอาจเกิดจากการไม่สามารถปรับกระบวนการทำงานได้ตามกฎหมายสำคัญ หรือกระบวนการปรับเปลี่ยนตามระเบียบ ข้อบังคับ ของสำนักงาน รวมทั้ง การกระทำทุจริตต่าง ๆ

4.2.2 การปฏิบัติตามมาตรฐาน อาทิเช่น ไม่สามารถจัดทำมาตรฐานที่สำคัญขององค์กร หรือการไม่ดำเนินการจัดทำมาตรฐานที่สำคัญ เป็นต้น

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย ระเบียบ

ตัวอย่างปัจจัยเสี่ยงทางด้านกฎหมาย ระเบียบ	สาเหตุที่อาจเกิดขึ้น	ปัจจัยภายใน	ปัจจัยภายนอก
การปฏิบัติงานไม่เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ และสัญญา ที่ทำไว้กับหน่วยงานภายนอก	ไม่มีการเผยแพร่กฎหมาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับองค์กร ทั้งในอดีตและปัจจุบันที่ยังมีผลบังคับใช้ให้เจ้าหน้าที่รับทราบและปฏิบัติ		✓
การปฏิบัติงานไม่เป็นไปตามคำสั่ง ประกาศ ระเบียบข้อบังคับขององค์กร	1. ไม่มีการเผยแพร่คำสั่ง ประกาศ ระเบียบข้อบังคับขององค์กร 2. ไม่มีการทบทวน/ปรับปรุงให้เป็นปัจจุบันเป็นประจำทุกปี 3. ไม่มีการสื่อสารให้หน่วยงานที่เกี่ยวข้องทราบ หากมีการเปลี่ยนแปลงแก้ไขหลักเกณฑ์/วิธีปฏิบัติงาน	✓ ✓ ✓	

5. การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

การดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ได้มีการนำมาตรฐาน ISO/IEC 27001:2022 ซึ่งเป็นมาตรฐานที่กำลังได้รับความนิยมอย่างแพร่หลายในปัจจุบัน และกล่าวถึงข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS (Information Security Management System) ให้กับองค์กร ซึ่งวัตถุประสงค์ของมาตรฐานนี้ เพื่อให้องค์กรสามารถบริหารจัดการทางด้านความปลอดภัยได้อย่างมีระบบ และเพียงพอเหมาะสมต่อการดำเนินธุรกิจขององค์กร มาร่วมกำหนดเป็นประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วย โดยสามารถกำหนดกรอบการบริหาร ดังนี้

5.1 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

หมายถึง 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

5.2 ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Type of Risk) สามารถจำแนกออกได้เป็น 2 ประเภท ดังนี้

5.2.1 ปัจจัยเสี่ยงภายใน IT Risk Management and Cyber Security ได้แก่ 1) การรักษาความลับ และความมั่นคงปลอดภัย (Confidentiality & Security) 2) ความถูกต้องเชื่อถือได้ของระบบ และข้อมูล (Integrity) และ 3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability)

5.2.2 ปัจจัยเสี่ยงภายนอก IT/Cyber Outsourcing ได้แก่ 1) การรักษาความลับ และความมั่นคงปลอดภัย (Confidentiality & Security) 2) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และ 3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability)

ทั้งนี้ สามารถวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ได้จากทรัพย์สินที่เสียหายได้ 5 ประเภท ดังนี้

1) ความเสี่ยงที่เกิดจากข้อมูล (Information Risk) หมายถึง ความเสี่ยงที่เกิดจากข้อมูลต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบ และรัดกุมเพียงพอ (Access Risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้เกิดการฟ้องร้องได้ หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงาน

หยุดชะงักได้ โดยความเสี่ยงนี้ อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์ และป้องกันความเสียหายอย่างเพียงพอ ยังรวมไปถึงความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back Up) ที่สำคัญคือ เพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูลสำรอง (Information Back-Up) การกู้คืนข้อมูล (Information Recovery) ซึ่งเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และแผนกู้คืนข้อมูล (Disaster Recovery Plan)

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

3) ความเสี่ยงที่เกิดจากโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากการเลือกใช้ หรือความเสี่ยงจากการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้องการถูก ผู้ไม่หวังดีทำลายระบบ (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) ความเสี่ยงที่เกิดจากบุคลากร (People Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ในเรื่องของการกำหนดโครงสร้าง การมอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ทั้งนี้ ยังรวมถึงการที่ขาดแผนการฝึกอบรมด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่ของสำนักงานอย่างทั่วถึง ทั้งในส่วนของผู้ดูแลระบบ (Administration) ผู้พัฒนาระบบ (Developer/Programmer) และผู้ใช้งานทั่วไป (User) อย่างสม่ำเสมอ

5) ความเสี่ยงที่เกิดจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้าง หรือจัดจ้างผู้ให้บริการภายนอก เพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้ เป็นต้น

ตัวอย่างปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ

ตัวอย่างปัจจัยเสี่ยง ด้านเทคโนโลยีสารสนเทศ	สาเหตุที่อาจเกิดขึ้น	ปัจจัย ภายใน	ปัจจัย ภายนอก
นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (IS Policy) ไม่เป็นปัจจุบัน	ขาดการทบทวน/ปรับปรุง ให้มีความสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง	✓	
ผู้รับจ้างช่วงจากผู้ให้บริการภายนอกเข้าถึงทรัพย์สินสารสนเทศของสำนักงานโดยไม่ได้รับอนุญาต	1. ขาดการควบคุม ติดตาม และระบุเงื่อนไขในสัญญาจ้าง 2. ผู้ให้บริการภายนอกกระทำผิดสัญญา	✓	✓

6. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงจะพิจารณาปัจจัยการประเมินความเสี่ยง 2 ด้าน คือ การประเมินโอกาสเกิด (Likelihood) และผลกระทบ (Impact) จากการเกิดเหตุการณ์ความเสี่ยง เพื่อทราบระดับความรุนแรงของความเสี่ยง ทั้งนี้ ความเสี่ยงด้านกลยุทธ์ ด้านการดำเนินงาน ด้านการเงิน ด้านกฎหมาย กฎระเบียบ และด้านเทคโนโลยีสารสนเทศ สามารถประเมินได้จากเกณฑ์การประเมินโอกาสเกิด และเกณฑ์การประเมินผลกระทบในแต่ละด้าน ซึ่งเกณฑ์ดังกล่าว อาจวัดจากโอกาสเกิดเหตุการณ์ในอดีต หรือการคาดการณ์เหตุการณ์ในอนาคต รวมทั้ง การประเมินผลกระทบอาจใช้ระดับความสำเร็จของเป้าหมายการดำเนินงานที่กำหนดไว้ หรือระดับความรุนแรงหรือความเสียงหายที่อาจเกิดเหตุการณ์ โดย สพร. ได้กำหนดเกณฑ์การประเมินโอกาสเกิดและผลกระทบในแต่ละประเภทความเสี่ยง ดังนี้

6.1 ประเภทความเสี่ยงด้าน S-O-F-C-IT ยกเว้น Cyber Security ดังรายละเอียดดังนี้

คำนิยาม และเกณฑ์การประเมินโอกาสเกิด (Likelihood) ของ S-O-F-C-IT ยกเว้น Cyber Security

เกณฑ์ที่ใช้ในการประเมิน	1 = โอกาสเกิดขึ้นยากที่สุด	2 = โอกาสเกิดขึ้นยาก	3 = โอกาสเกิดขึ้นปานกลาง	4 = โอกาสเกิดขึ้นง่าย	5 = โอกาสเกิดขึ้นง่ายที่สุด
ความถี่/จำนวนครั้งของการเกิดเหตุการณ์	แทบจะไม่เกิดหรืออย่างมาก ปีละ 1 ครั้ง	โอกาสเกิดน้อยหรืออย่างมากไม่เกินปีละ 2 ครั้ง	ปานกลาง หรือปีละ 3-5 ครั้ง	ค่อนข้างบ่อยหรือปีละ 6-10 ครั้ง	เกิดเป็นประจำหรืออย่างน้อยเดือนละ 1 ครั้ง
ข้อบ่งชี้หรือหลักฐานของการเกิดเหตุการณ์	เป็นไปไม่ได้ที่จะเกิดเหตุการณ์นี้ขึ้น	ไม่มีข้อบ่งชี้หรือหลักฐาน แต่มีความเป็นไปได้ยากที่จะเกิดเหตุการณ์นี้ขึ้น	มีข้อบ่งชี้หรือหลักฐานที่แสดงถึงความเป็นไปได้ที่จะเกิดเหตุการณ์นี้ขึ้น	มีข้อบ่งชี้หรือหลักฐานที่คาดว่าจะเกิดเหตุการณ์นี้ขึ้น ในระยะอันใกล้	มีความแน่นอนที่จะเกิดเหตุการณ์นี้ขึ้น
โอกาสเกิดเหตุการณ์ที่จะกระทำผิด	ไม่มีโอกาสเกิดขึ้นแม้ไม่มีมาตรการควบคุม	เกิดขึ้นยากมากแม้ไม่มีมาตรการควบคุม	มีโอกาสเกิดหากไม่มีมาตรการควบคุม	มีโอกาสเกิดขึ้นง่ายมากแม้ไม่มีมาตรการควบคุม	มีโอกาสเกิดขึ้นง่ายมาก แม้จะมีมาตรการควบคุม
ระดับความสำเร็จของแผนงาน/โครงการ/กิจกรรมในอดีตที่ผ่านมา (ประเมินในกรณีที่ใช้ความสำเร็จในอดีต)	ผลการดำเนินงานดีกว่าเป้าหมายทุกปีตลอดระยะเวลา 3 ปีย้อนหลัง	ผลการดำเนินงานเป็นไปตามเป้าหมายทุกปีและมีบางปีที่ผลการดำเนินงานดีกว่าเป้าหมายตลอดระยะเวลา 3 ปีย้อนหลัง	ผลการดำเนินงานเป็นไปตามเป้าหมายทุกปีและไม่มีปีใดที่ผลการดำเนินงานดีกว่าเป้าหมายตลอดระยะเวลา 3 ปีย้อนหลัง	ผลการดำเนินงานต่ำกว่าเป้าหมายบางปีตลอดระยะเวลา 3 ปีย้อนหลัง	ผลการดำเนินงานต่ำกว่าเป้าหมายทุกปีตลอดระยะเวลา 3 ปีย้อนหลัง

เกณฑ์ที่ใช้ในการประเมิน	1 = โอกาสเกิดขึ้นยากที่สุด	2 = โอกาสเกิดขึ้นยาก	3 = โอกาสเกิดขึ้นปานกลาง	4 = โอกาสเกิดขึ้นง่าย	5 = โอกาสเกิดขึ้นง่ายที่สุด
ร้อยละของระดับความสำเร็จของการดำเนินงานตามแผน/แผนปฏิบัติการ สพร./แผน DG/แผนการย้ายสำนักงาน/นโยบายรัฐบาล/KPI ก.พ.ร. (กิจกรรมที่ดำเนินการ)	ดำเนินการได้ตามแผน คิดเป็นร้อยละ 100	ดำเนินการได้ตามแผน ไม่น้อยกว่าร้อยละ 75	ดำเนินการได้ตามแผน ไม่น้อยกว่าร้อยละ 50	ดำเนินการได้ตามแผน ไม่น้อยกว่าร้อยละ 25	ดำเนินการได้ตามแผน น้อยกว่าร้อยละ 25
ร้อยละของจำนวนองค์การบริหารส่วนท้องถิ่นที่สมัครเข้าร่วมโครงการท้องถิ่นดิจิทัล	ร้อยละ 100	ไม่น้อยกว่าร้อยละ 75	ไม่น้อยกว่าร้อยละ 50	ไม่น้อยกว่าร้อยละ 25	น้อยกว่าร้อยละ 25
จำนวนชุดข้อมูล Domain ที่สำคัญ	15 ชุดข้อมูล	12 ชุดข้อมูล	9 ชุดข้อมูล	6 ชุดข้อมูล	3 ชุดข้อมูล
ร้อยละของอัตราการทดแทนตำแหน่งว่างจากกรอบอัตรากำลัง	อัตราการทดแทนตำแหน่งงานว่างไม่น้อยกว่าร้อยละ 90	อัตราการทดแทนตำแหน่งงานว่างไม่น้อยกว่าร้อยละ 80	อัตราการทดแทนตำแหน่งงานว่างไม่น้อยกว่าร้อยละ 70	อัตราการทดแทนตำแหน่งงานว่างไม่น้อยกว่าร้อยละ 60	อัตราการทดแทนตำแหน่งงานว่างต่ำกว่าร้อยละ 60
ร้อยละของการใช้จ่ายเงินนอกงบประมาณที่ใช้ตามแผนงานบุคลากรภาครัฐแผนงบประมาณรายจ่ายประจำปี	ไม่เกินร้อยละ 80	ไม่เกินร้อยละ 85	ไม่เกินร้อยละ 90	ไม่เกินร้อยละ 95	มากกว่าร้อยละ 95

เกณฑ์ที่ใช้ในการประเมิน	1 = โอกาสเกิดขึ้นยากที่สุด	2 = โอกาสเกิดขึ้นยาก	3 = โอกาสเกิดขึ้นปานกลาง	4 = โอกาสเกิดขึ้นง่าย	5 = โอกาสเกิดขึ้นง่ายที่สุด
จำนวนของการเกิดเหตุการณ์ที่ไม่ปฏิบัติตามหรือปฏิบัติตามล่าช้า	แทบจะไม่เกิดหรืออย่างมาก ปีละ 1 ครั้ง	โอกาสเกิดน้อยหรืออย่างมากไม่เกินปีละ 2 ครั้ง	ปานกลาง หรือปีละ 3-5 ครั้ง	ค่อนข้างบ่อยหรือปีละ 6-10 ครั้ง	เกิดเป็นประจำหรืออย่างน้อยเดือนละ 1 ครั้ง
ร้อยละของบริการตาม Service Catalog ที่สามารถปิดช่องโหว่ได้ตามนโยบาย	ร้อยละ 100	ร้อยละ 97.5	ร้อยละ 95	ร้อยละ 92.5	ต่ำกว่าร้อยละ 92.5
ร้อยละของเหตุการณ์ด้าน Cyber Security ที่มีระดับความรุนแรงสูงหรือวิกฤต (High, Critical)	ร้อยละ 100	ร้อยละ 97.5	ร้อยละ 95	ร้อยละ 92.5	ต่ำกว่าร้อยละ 92.5
ร้อยละการแก้ไข Incident ตาม SLA	ร้อยละ 100	ร้อยละ 97.5	ร้อยละ 95	ร้อยละ 92.5	ต่ำกว่าร้อยละ 92.5

คำนิยาม และเกณฑ์การประเมินผลกระทบ (Impact) ของ S-O-F-C-IT ยกเว้น Cyber Security

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ด้านกลยุทธ์: ระดับความสำเร็จในการดำเนินงานตามแผน/แผนปฏิบัติการ สพร./แผน DG/แผนการย้ายสำนักงาน/นโยบายรัฐบาล/KPI ก.พ.ร. (ผลผลิต/ผลลัพธ์ตามเป้าหมาย)	ร้อยละ 100	ไม่น้อยกว่าร้อยละ 90	ไม่น้อยกว่าร้อยละ 80	ไม่น้อยกว่าร้อยละ 50	น้อยกว่าร้อยละ 50

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ด้านกลยุทธ์: ระดับความสำเร็จในการจัดทำแผนกลยุทธ์หรือแผนต่าง ๆ	สามารถดำเนินการได้แล้วเสร็จตามองค์ประกอบและระยะเวลาที่กำหนด	สามารถดำเนินการได้แล้วเสร็จตามองค์ประกอบแต่มีความล่าช้ากว่าระยะเวลาที่กำหนด โดยไม่มีผลกระทบต่อการดำเนินงาน	สามารถดำเนินการได้แล้วเสร็จตามองค์ประกอบแต่มีความล่าช้ากว่าระยะเวลาที่กำหนด โดยส่งผลกระทบต่อการดำเนินงาน	ไม่สามารถดำเนินการได้ตามองค์ประกอบรวมทั้ง มีความล่าช้ากว่าระยะเวลาที่กำหนด โดยส่งผลกระทบต่อการดำเนินงาน ซึ่งจะต้องแก้ไขโดยฝ่ายบริหาร	ไม่สามารถดำเนินการได้ตามองค์ประกอบรวมทั้งมีความล่าช้ากว่าระยะเวลาที่กำหนด โดยส่งผลกระทบต่อการดำเนินงาน ซึ่งจะต้องแก้ไขโดยคณะกรรมการ
ด้านกลยุทธ์: ชื่อเสียงและภาพลักษณ์	มีผลกระทบน้อยต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล หรือไม่กระทบ	มีผลกระทบต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล สามารถดำเนินการ แก้ไขได้	มีผลกระทบต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล ซึ่งคาดว่าไม่สามารถดำเนินการแก้ไขได้ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	มีผลกระทบมากต่อชื่อเสียงของสำนักงาน หรือสิทธิเสรีภาพของบุคคล และเกิดความไม่พอใจจากบุคคล หรือ ผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทำให้สำนักงานต้องติดต่อเพื่อขอชี้แจงต่อบุคคลหรือผู้มีส่วนได้ส่วนเสีย หรือประกาศชี้แจงผ่าน Social Media	มีผลกระทบมากต่อชื่อเสียงของสำนักงานหรือสิทธิเสรีภาพของบุคคล และเกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ ทำให้สำนักงานต้องดำเนินการแถลงข่าว

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ด้านกลยุทธ์: ประสิทธิภาพในการบริหารจัดการองค์กรในภาพรวม	สามารถดำเนินการได้อย่างมีประสิทธิภาพ โดยไม่มีผลกระทบต่อการบริหารจัดการองค์กรในภาพรวม	สามารถดำเนินการได้อย่างมีประสิทธิภาพ โดยมีผลกระทบต่อการบริหารจัดการองค์กรในภาพรวมเพียงเล็กน้อย ซึ่งอาจต้องปรับรูปแบบวิธีการทำงาน	สามารถดำเนินการได้โดยมีผลกระทบต่อการบริหารจัดการองค์กร ทั้งในส่วนของรูปแบบวิธีการทำงาน และงบประมาณ	ไม่สามารถดำเนินการได้ และมีผลกระทบต่อการบริหารจัดการองค์กรในระดับสูง และเกิดความเสียหายบางอย่าง (รูปแบบวิธีการทำงาน/งบประมาณ/ขวัญกำลังใจ) ซึ่งจะต้องแก้ไขโดยฝ่ายบริหาร	ไม่สามารถดำเนินการได้ และมีผลกระทบต่อการบริหารจัดการองค์กรในระดับสูงมาก และเกิดความเสียหายในภาพรวม (รูปแบบวิธีการทำงาน/งบประมาณ/ขวัญกำลังใจ) ซึ่งจะต้องแก้ไขโดยคณะกรรมการ
ด้านกลยุทธ์: ปริมาณการใช้ประโยชน์จากบริการดิจิทัลผ่าน Super App	มากกว่า 10 ล้านรายการ	10 ล้านรายการ	7.5 ล้านรายการ	5 ล้านรายการ	น้อยกว่า 5 ล้านรายการ
ด้านกลยุทธ์: จำนวนบริการดิจิทัลที่สามารถให้บริการผ่าน Super App	มากกว่า 10 บริการ (บริการใหม่)	10 บริการ (บริการใหม่)	8 บริการ (บริการใหม่)	6 บริการ (บริการใหม่)	น้อยกว่า 6 บริการ (บริการใหม่)
ด้านกลยุทธ์: จำนวน Transaction ที่ลดลงจากปีที่ผ่านมาของบริการ GDX (ร้อยละ)	จำนวนเพิ่มขึ้น	จำนวนไม่ลดลงจากปีที่ผ่านมา	จำนวนลดลงไม่เกินร้อยละ 10	จำนวนลดลงไม่เกินร้อยละ 20	จำนวนลดลงมากกว่าร้อยละ 20
ด้านกลยุทธ์: จำนวนของผู้ใช้บริการที่ลดลงจากปีที่ผ่านมา (ร้อยละ)	จำนวนเพิ่มขึ้น	จำนวนไม่ลดลงจากปีที่ผ่านมา	จำนวนลดลงไม่เกินร้อยละ 10	จำนวนลดลงไม่เกินร้อยละ 20	จำนวนลดลงมากกว่าร้อยละ 20

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ด้านการดำเนินงาน: ระดับความพึงพอใจในการให้บริการ	ระดับความพึงพอใจไม่น้อยกว่าร้อยละ 95	ระดับความพึงพอใจไม่น้อยกว่าร้อยละ 90	ระดับความพึงพอใจไม่น้อยกว่าร้อยละ 85	ระดับความพึงพอใจไม่น้อยกว่าร้อยละ 80	ระดับความพึงพอใจน้อยกว่าร้อยละ 80
ด้านการดำเนินงาน: การตอบสนองผู้รับบริการ	สามารถให้บริการแก่ผู้รับบริการได้ตามปกติ	เกิดข้อร้องเรียนจากผู้รับบริการแต่สามารถแก้ไขและชี้แจงข้อร้องเรียนได้อย่างรวดเร็ว	เกิดข้อร้องเรียนจากผู้รับบริการและไม่สามารถแก้ไขและชี้แจงข้อร้องเรียนได้ตามระยะเวลาที่กำหนด และเริ่มส่งผลกระทบต่อความพึงพอใจของผู้รับบริการ	ผู้รับบริการขาดความเชื่อมั่นในการให้บริการ	ผู้รับบริการขาดความเชื่อมั่นในการให้บริการและมีการร้องเรียนที่ส่งผลกระทบต่อภาพลักษณ์และชื่อเสียงของ สพร.
ด้านการดำเนินงาน: การส่งมอบงานของ Vendor/Outsource	สามารถส่งมอบงานได้ตามเงื่อนไขและระยะเวลาที่กำหนด	สามารถส่งมอบงานได้ตามระยะเวลาที่กำหนด แต่ต้องมีการปรับปรุงแก้ไขและไม่ส่งผลกระทบต่อการดำเนินงาน	ไม่สามารถส่งมอบงานได้ตามเงื่อนไขหรือระยะเวลาที่กำหนด ต้องมีการปรับปรุงแก้ไขและส่งผลกระทบต่อการดำเนินงาน	ไม่สามารถส่งมอบงานได้และมีการยกเลิกสัญญา	ไม่สามารถส่งมอบงานได้ตามสัญญาและมีการฟ้องร้องดำเนินคดี
ด้านการดำเนินงาน: การหยุดชะงักหรือการขาดความต่อเนื่องของโครงการ/ธุรกิจ	ไม่มีการหยุดชะงักและการดำเนินงานของโครงการ/ธุรกิจมีความต่อเนื่อง	มีการหยุดชะงักของโครงการ/ธุรกิจเล็กน้อย แต่ยังสามารถดำเนินการแก้ไขให้กลับมาดำเนินการได้ภายใน 1 วัน	มีการหยุดชะงักของโครงการ/ธุรกิจในระดับปานกลาง แต่ยังสามารถดำเนินการแก้ไขให้กลับมาดำเนินการได้โดยใช้ระยะเวลาในการปรับปรุงแก้ไขภายใน 7 วัน	มีการหยุดชะงักของโครงการในระดับสูง แต่ยังสามารถดำเนินการแก้ไขให้กลับมาดำเนินการได้โดยใช้ระยะเวลาในการปรับปรุงแก้ไขมากกว่า 7 วัน	มีการหยุดชะงักของโครงการในระดับสูงมากและไม่สามารถดำเนินการแก้ไขได้ ต้องยกเลิกโครงการ/ธุรกิจ

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ด้านการดำเนินงาน: ระดับผลกระทบจากการย้ายสำนักงานล่าช้า	มีสำนักงานประจำในการปฏิบัติงานภายใน ไตรมาส 2/2568	มีสำนักงานประจำในการปฏิบัติงานภายใน ไตรมาส 3/2568	มีสำนักงานประจำในการปฏิบัติงานภายใน ไตรมาส 4/2568 และไม่ต้องเช่าใช้สำนักงานชั่วคราวในไตรมาส 4/2568	ไม่มีสำนักงานประจำในการปฏิบัติงาน ในปีงบประมาณ พ.ศ. 2568 ต้องเช่าใช้สำนักงานชั่วคราว ตลอดทั้งปีงบประมาณ พ.ศ. 2568	ไม่มีสำนักงานประจำในการปฏิบัติงาน ในปีงบประมาณ พ.ศ. 2568 ต้องเช่าใช้สำนักงานชั่วคราวไปถึงปีงบประมาณ พ.ศ. 2569
ด้านการเงิน: ร้อยละของจำนวนบุคลากร เมื่อเทียบกับกรอบอัตรากำลัง	ไม่น้อยกว่าร้อยละ 90	ไม่น้อยกว่าร้อยละ 80	ไม่น้อยกว่าร้อยละ 70	ไม่น้อยกว่าร้อยละ 60	น้อยกว่าร้อยละ 60
ด้านการเงิน: ผลกระทบและความเสียหาย	ผลกระทบที่เกิดขึ้น ประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) น้อยกว่า 5 แสนบาท	ผลกระทบที่เกิดขึ้นประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 5 แสนบาท แต่ไม่เกิน 1 ล้านบาท	ผลกระทบที่เกิดขึ้นประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 1 ล้านบาท แต่ไม่เกิน 50 ล้านบาท	ผลกระทบที่เกิดขึ้นประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) ตั้งแต่ 50 ล้านบาท แต่ไม่เกิน 100 ล้านบาท	ผลกระทบที่เกิดขึ้นประเมินเป็นมูลค่าความเสียหายทางการเงิน (ทั้งทางตรงและทางอ้อม) มากกว่า 100 ล้านบาท
ด้านการเงิน: การจัดหารายได้ตามเป้าหมายสะสม	ร้อยละ 100	ไม่น้อยกว่าร้อยละ 90	ไม่น้อยกว่าร้อยละ 80	ไม่น้อยกว่าร้อยละ 70	น้อยกว่าร้อยละ 70
ด้านการเงิน: ร้อยละค่าใช้จ่ายด้านบุคลากรเทียบกับงบประมาณประจำปี	ไม่เกินร้อยละ 27.5	ไม่เกินร้อยละ 30	ไม่เกินร้อยละ 32.5	ไม่เกินร้อยละ 35	มากกว่าร้อยละ 35
ด้านการเงิน: จำนวนอัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio)	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) ไม่น้อยกว่า 3.5 เท่า	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) ไม่น้อยกว่า 2.5 เท่า	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) ไม่น้อยกว่า 1.5 เท่า	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) ไม่น้อยกว่า 1 เท่า	อัตราส่วนเงินทุนหมุนเวียนเร็ว (Quick Ratio) น้อยกว่า 1 เท่า

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ด้านการเงิน: ร้อยละของงบประมาณจากแหล่งอื่นที่ได้รับเมื่อเทียบกับคำขอตั้งงบประมาณ	ร้อยละ 100	ไม่น้อยกว่าร้อยละ 90	ไม่น้อยกว่าร้อยละ 80	ไม่น้อยกว่าร้อยละ 80	น้อยกว่าร้อยละ 70
ด้านการปฏิบัติตามกฎหมาย ระเบียบ: ผลกระทบจากการไม่ปฏิบัติหรือปฏิบัติล่าช้าในการดำเนินการตามกฎหมายหรือมาตรฐานที่สำคัญ	การไม่ปฏิบัติหรือปฏิบัติล่าช้าในการดำเนินการตามกฎหมาย หรือมาตรฐานที่สำคัญแต่ไม่เกิดผลกระทบต่อการดำเนินงานของสำนักงานหรือต่อบุคคลอื่น	การไม่ปฏิบัติหรือปฏิบัติล่าช้าในการดำเนินการตามกฎหมาย หรือมาตรฐานที่สำคัญ ทำให้เกิดผลกระทบต่อการดำเนินงานของสำนักงาน หรือต่อบุคคลอื่น แต่สามารถดำเนินการแก้ไขได้	การไม่ปฏิบัติหรือปฏิบัติล่าช้าในการดำเนินการตามกฎหมายหรือมาตรฐานที่สำคัญ ทำให้เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญ และเกิดความเสียหายต่อสำนักงานหรือต่อบุคคลอื่น ซึ่งคาดว่าไม่สามารถดำเนินการแก้ไขได้ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	การไม่ปฏิบัติหรือปฏิบัติล่าช้าในการดำเนินการตามกฎหมายหรือมาตรฐานที่สำคัญ ทำให้เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญและไม่เป็นตามเป้าของ ก.พ.ร. และเกิดความเสียหายอย่างร้ายแรงต่อสำนักงานหรือต่อบุคคลอื่นจนเป็นเหตุให้สำนักงานถูกร้องเรียน	การไม่ปฏิบัติหรือปฏิบัติล่าช้าในการดำเนินการตามกฎหมายหรือมาตรฐานที่สำคัญ ทำให้เกิดผลกระทบต่อการดำเนินงานของสำนักงานที่มีนัยสำคัญและไม่เป็นตามเป้าของ ก.พ.ร. และเกิดความเสียหายอย่างร้ายแรงต่อสำนักงานหรือต่อบุคคลอื่นจนเป็นเหตุให้ สำนักงานถูกฟ้องร้องดำเนินคดี
ด้านเทคโนโลยีสารสนเทศ: ความสามารถในการแก้ไขบริการเกิดเหตุขัดข้อง	ระบบสามารถให้บริการได้อย่างสมบูรณ์หรือทุกเหตุการณ์ที่เกิดเหตุขัดข้อง ในส่วนของฟังก์ชันหลักได้ โดยระยะเวลาที่แก้ไขเฉลี่ย ไม่เกิน 4 ชั่วโมงต่อเดือน	ทุกเหตุการณ์ที่เกิดเหตุขัดข้องสามารถให้บริการในส่วนของฟังก์ชันหลักได้ โดยระยะเวลาที่แก้ไขเฉลี่ยตั้งแต่ 4 ชั่วโมง – ไม่เกิน 1 วันต่อเดือน	มีบางเหตุการณ์ที่บริการเกิดเหตุขัดข้อง และไม่สามารถให้บริการได้ โดยระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าวเฉลี่ย ไม่เกิน 2 ชั่วโมง ต่อเดือน	มีบางเหตุการณ์ที่เกิดเหตุขัดข้องและไม่สามารถให้บริการได้โดยระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าว เฉลี่ย 2 - 4 ชั่วโมง ต่อเดือน	มีบางเหตุการณ์ที่บริการเกิดเหตุขัดข้อง และไม่สามารถให้บริการได้ โดยเป็นระยะเวลาที่แก้ไขเหตุการณ์ดังกล่าวเฉลี่ยมากกว่า 4ชั่วโมงต่อเดือน

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ด้านเทคโนโลยีสารสนเทศ: ผลกระทบต่อผู้ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง ซึ่งเกิดจากระบบเทคโนโลยีสารสนเทศขัดข้อง	มีผลกระทบต่อจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) น้อยกว่า 1,000 คน	มีผลกระทบกับจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) ตั้งแต่ 1,000 - 1,999 คน	มีผลกระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) ตั้งแต่ 2,000 - 4,999 คน	มีผลกระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) ตั้งแต่ 5,000 - 9,999 คน	มีผลกระทบกับจำนวนผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย ที่ใช้บริการพร้อมกัน ณ ช่วงเวลาหนึ่ง (Concurrent transaction) มากกว่า 10,000 คน
ด้านเทคโนโลยีสารสนเทศ: ผลกระทบจากการถูกบุกรุก/โจมตีความมั่นคงปลอดภัย การละเมิดข้อมูลส่วนบุคคล และระบบสารสนเทศของสำนักงาน รวมทั้งข้อมูลรั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต	ระบบไม่ถูกโจมตี/บุกรุก รวมทั้ง ข้อมูลรั่วไหล และสามารถแก้ไขและให้บริการได้อย่างสมบูรณ์ ไม่เกิดความเสียหาย	ระบบถูกโจมตี/บุกรุก รวมทั้ง ข้อมูลรั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต แต่ยังสามารถแก้ไขและให้บริการได้อย่างสมบูรณ์ หรือมีความเสียหายเล็กน้อย	ระบบถูกโจมตี/บุกรุก รวมทั้ง ข้อมูลรั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งไม่สามารถแก้ไขได้ทั้งหมด แต่ยังให้บริการในส่วนของฟังก์ชันหลักได้ หรือมีความเสียหายปานกลาง	ระบบถูกโจมตี/บุกรุก รวมทั้ง ข้อมูลรั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งไม่สามารถแก้ไขและให้บริการในส่วนของฟังก์ชันหลักได้ รวมทั้งเกิดความเสียหายต่อสำนักงาน หรือต่อบุคคลอื่น จนเป็นเหตุให้ถูกร้องเรียน	ระบบถูกโจมตี/บุกรุก รวมทั้ง ข้อมูลรั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งไม่สามารถแก้ไขได้ รวมทั้งเกิดความเสียหายต่อสำนักงาน หรือต่อบุคคลอื่น จนเป็นเหตุให้ถูกฟ้องร้องดำเนินคดี
ด้านเทคโนโลยีสารสนเทศ: ร้อยละการให้บริการอย่างต่อเนื่อง ตาม SLA ที่กำหนด	สูงกว่าร้อยละ 99.5	ร้อยละ 99.5	ร้อยละ 99.4	ไม่น้อยกว่าร้อยละ 99	ต่ำกว่าร้อยละ 99

จากตารางที่เสนอในข้างต้น สำนักงานได้กำหนดค่าระดับความเสี่ยงไว้ ดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ความรุนแรงของเหตุการณ์

ในการพิจารณาความรุนแรงของเหตุการณ์ ซึ่งไม่ได้กำหนดคำนิยามตามเกณฑ์การประเมินผลกระทบของปัจจัยเสี่ยง สามารถพิจารณาได้จากผลกระทบของประเภทความเสี่ยงที่สอดคล้อง เช่น หากเป็นปัจจัยเสี่ยงเกี่ยวกับการพ้นสภาพของเจ้าหน้าที่ที่สำคัญ (Key Successor) ให้พิจารณาว่าเป็นปัจจัยเสี่ยงด้านใด ซึ่งในกรณีดังกล่าวเกี่ยวข้องกับบุคลากร จึงกำหนดให้เป็นปัจจัยเสี่ยงด้านการดำเนินงาน ดังนั้น จากตัวอย่างจึงสามารถนำเกณฑ์การประเมินผลกระทบด้านการดำเนินงาน การหยุดชะงักหรือการขาดความต่อเนื่องของโครงการ/ธุรกิจ เนื่องจากผลกระทบจากการพ้นสภาพของเจ้าหน้าที่ที่สำคัญ คือการทำให้กระบวนการมีการหยุดชะงัก เป็นต้น ดังกรณีตัวอย่าง

กรณีตัวอย่าง

ในช่วงปีงบประมาณ พ.ศ. 2566 มีเจ้าหน้าที่ที่สำคัญพ้นสภาพจำนวน 3 ราย ซึ่งส่งผลให้การดำเนินงานเกิดการหยุดชะงัก ไม่สามารถดำเนินการได้เป็นระยะเวลา 7 วัน ดังนั้น จึงสามารถประเมินโอกาสเกิด และผลกระทบได้จากคำนิยาม ดังนี้

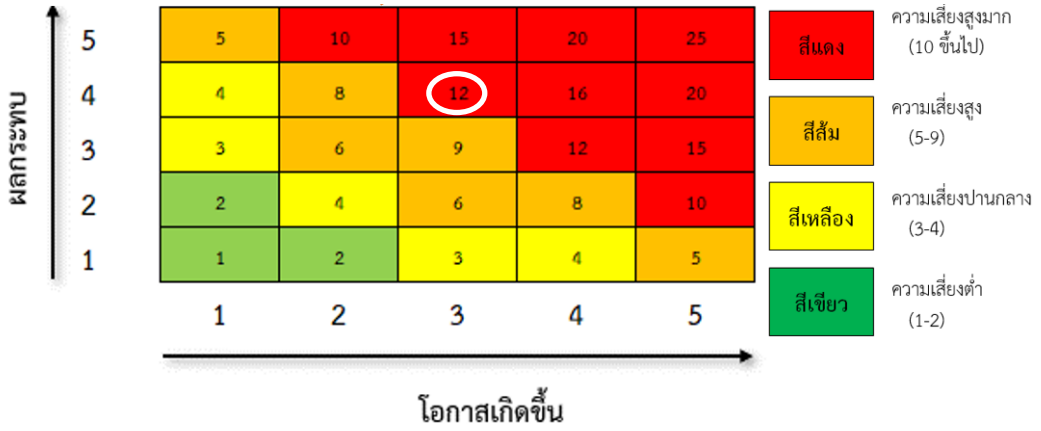
โอกาสเกิด

เกณฑ์ที่ใช้ในการประเมิน	1 = โอกาสเกิดขึ้นยากที่สุด	2 = โอกาสเกิดขึ้นยาก	3 = โอกาสเกิดขึ้นปานกลาง	4 = โอกาสเกิดขึ้นง่าย	5 = โอกาสเกิดขึ้นง่ายที่สุด
ความถี่/จำนวนครั้งของการเกิดเหตุการณ์	แทบจะไม่เกิดหรืออย่างมากปีละ 1 ครั้ง	โอกาสเกิดน้อยหรืออย่างมากไม่เกินปีละ 2 ครั้ง	ปานกลาง หรือปีละ 3-5 ครั้ง	ค่อนข้างบ่อยหรือปีละ 6-10 ครั้ง	เกิดเป็นประจำหรืออย่างน้อยเดือนละ 1 ครั้ง

ผลกระทบ

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ด้านการดำเนินงาน: การหยุดชะงักหรือการขาดความต่อเนื่องของโครงการ/ธุรกิจ	ไม่มีการหยุดชะงัก และการดำเนินงานของโครงการ/ธุรกิจมีความต่อเนื่อง	มีการหยุดชะงักของโครงการ/ธุรกิจเล็กน้อยแต่ยังสามารถดำเนินการแก้ไขให้กลับมาดำเนินการได้ภายใน 1 วัน	มีการหยุดชะงักของโครงการ/ธุรกิจในระดับปานกลางแต่ยังสามารถดำเนินการแก้ไขให้กลับมาดำเนินการได้โดยใช้ระยะเวลาในการปรับปรุงแก้ไขภายใน 7 วัน	มีการหยุดชะงักของโครงการในระดับสูงแต่ยังสามารถดำเนินการแก้ไขให้กลับมาดำเนินการได้โดยใช้ระยะเวลาในการปรับปรุงแก้ไขมากกว่า 7 วัน	มีการหยุดชะงักของโครงการในระดับสูงมากและไม่สามารถดำเนินการแก้ไขได้ ต้องยกเลิกโครงการ/ธุรกิจ

ดังนั้น จึงสามารถประเมินระดับความรุนแรงของความเสี่ยงได้เท่ากับ โอกาสเกิด (3) x ผลกระทบ (4) = ระดับความเสี่ยงสูงมาก (12) ดังภาพ



จากการพิจารณาค่าระดับความเสี่ยงในตารางข้างต้น สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 ระดับ ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่ฝ่าย/ส่วนงาน/องค์กร สามารถยอมรับได้ โดยมีแผนจัดการความเสี่ยงหรือไม่มีแผนจัดการความเสี่ยงก็ได้
3-4	ปานกลาง	● ระดับความเสี่ยงที่ฝ่าย/ส่วนงาน ไม่สามารถยอมรับได้ โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น ● ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยให้ฝ่าย/ส่วนงาน นำไปบริหารความเสี่ยง โดยควบคุม และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและมาตรการปรับปรุงการควบคุมภายใน) ให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้ และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและมาตรการปรับปรุงการควบคุมภายใน) ให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้โดยทันที และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น

ดังนั้น ปัจจัยเสี่ยงดังกล่าวจะต้องนำไปเสนอต่อที่ประชุมฝ่ายบริหาร รวมทั้งคณะอนุกรรมการด้านการบริหารความเสี่ยงพิจารณาให้ความเห็นชอบ ก่อนนำเสนอคณะกรรมการ สพร. พิจารณาอนุมัติให้เป็นปัจจัยเสี่ยงระดับองค์กรต่อไป

6.2 ประเภทความเสี่ยงด้าน IT เฉพาะ Cyber Security ดังรายละเอียดดังนี้

คำนิยาม และเกณฑ์การประเมินโอกาสเกิด (Likelihood) ของ IT เฉพาะที่เป็น Cyber Security

เกณฑ์ที่ใช้ในการประเมิน	1 = โอกาสเกิดขึ้นยากที่สุด	2 = โอกาสเกิดขึ้นยาก	3 = โอกาสเกิดขึ้นปานกลาง	4 = โอกาสเกิดขึ้นง่าย	5 = โอกาสเกิดขึ้นง่ายที่สุด
จุดอ่อนของทรัพย์สินสารสนเทศ (Discoverability (D)) : ผู้ไม่หวังดีสามารถค้นพบจุดอ่อนของทรัพย์สินสารสนเทศ	- สามารถค้นพบได้โดยการอ่าน Source Code - สามารถค้นพบและโจมตีได้จากการเข้าถึงด้านกายภาพ (Physical)	- สามารถค้นพบได้โดยการเข้า ใช้งาน - สามารถค้นพบและโจมตีได้จากการเข้าถึงระบบแบบ เครือข่ายเดียวกัน (Local Area Network)	- สามารถค้นพบได้โดยตรวจสอบการตอบสนองพฤติกรรม และการสื่อสารของเป้าหมาย Network Sniffing) - สามารถค้นพบและโจมตีได้จากภายในเครือข่ายย่อย (Subnet Addresses) หรือเครือข่ายเดียวกัน (Local Area Network)	- สามารถค้นพบได้จากการ Scan Port - สามารถค้นพบและโจมตีได้จากเครือข่ายที่อยู่ใกล้เคียง หรือติดกัน (Adjacent Subnets or Network Segment)	- สามารถค้นพบได้จากการ Scan Public Domain - สามารถค้นพบและโจมตีจากเครือข่ายภายนอกได้ (Public Network)
การโจมตี (Exploitability (E)) : ผู้ไม่หวังดีสามารถใช้ประโยชน์จากจุดอ่อนของระบบหรือ ทรัพย์สินสารสนเทศ	- สามารถทำได้ด้วยการเข้าถึงโดยใช้สิทธิ์พิเศษ (Privilege) ของเป้าหมายเช่น ระดับสิทธิ Admin/SYSTEM/ Root รวมถึง Multi Factor Authentication - สามารถทำได้ด้วยเครื่องมือเฉพาะที่ต้องใช้ความรู้ด้านเทคนิคจากผู้เชี่ยวชาญ	- สามารถทำได้ด้วยการเข้าถึงโดยใชสิทธิ์พิเศษ (Privilege) ของเป้าหมาย เช่น ระดับสิทธิ Admin/SYSTEM/ Root - สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ/ เครื่องมือเฉพาะโดยมีความรู้เทคนิคระดับสูง	- สามารถทำได้ด้วยการเข้าถึงโดยใชสิทธิ์พิเศษ (Privilege) ของเป้าหมาย เช่น ระดับสิทธิ Admin/SYSTEM/ Root - สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยมีความรู้เทคนิคระดับปานกลาง	- สามารถทำได้โดยการจำกัดสิทธิ์การเข้าถึงของเป้าหมาย - สามารถทำได้ด้วยเครื่องมือที่เผยแพร่เป็นสาธารณะ โดยมีความรู้ขั้นพื้นฐาน	- สามารถทำได้โดยไม่มีสิทธิ์การเข้าถึงของเป้าหมาย - สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยไม่ต้องมีความรู้ด้านเทคนิค

เกณฑ์ที่ใช้ในการประเมิน	1 = โอกาสเกิดขึ้นยากที่สุด	2 = โอกาสเกิดขึ้นยาก	3 = โอกาสเกิดขึ้นปานกลาง	4 = โอกาสเกิดขึ้นง่าย	5 = โอกาสเกิดขึ้นง่ายที่สุด
การโจมตีหรือบุกรุกซ้ำ (Reproducibility (R)) : ผู้ไม่หวังดีสามารถโจมตีหรือบุกรุกซ้ำบนทรัพย์สินสารสนเทศและผ่านช่องโหว่ที่มีอยู่เดิม	- ไม่สามารถโจมตีหรือบุกรุกซ้ำได้	- ไม่สามารถโจมตีหรือบุกรุกซ้ำได้โดยมีเงื่อนไขเหตุการณ์จากการสุ่มหรือการคาดเดาของผู้บุกรุก - สามารถทำซ้ำได้จากทฤษฎี หรือช่องโหว่ที่มีการพิสูจน์และเผยแพร่สู่สาธารณะ	- สามารถโจมตีหรือบุกรุกซ้ำได้โดยมีเงื่อนไขเหตุการณ์ที่คาดการณ์ได้ - สามารถทำซ้ำได้ด้วยการปรับแต่งช่องโหว่เฉพาะสำหรับเป้าหมาย	- สามารถโจมตีหรือบุกรุกซ้ำโดยไม่มีการกำหนดค่าบางอย่างที่เป้าหมาย -สามารถโจมตีหรือบุกรุกซ้ำได้ด้วยการปรับแต่งช่องโหว่ที่เผยแพร่เล็กน้อย เช่น การเปลี่ยนพารามิเตอร์	- สามารถโจมตีหรือบุกรุกซ้ำโดยไม่มีการกำหนดค่าหรือเงื่อนไขเหตุการณ์ใด 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

คำนิยาม และเกณฑ์การประเมินผลกระทบ (Impact) ของ IT เฉพาะ Cyber Security

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ความสามารถในการรักษาความลับของข้อมูล (Confidentiality: C)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) อาจส่งผลกระทบเล็กน้อยต่อสำนักงาน หรือบุคคล โดยไม่จำเป็นต้องดำเนินการแก้ไข	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) อาจส่งผลกระทบอย่างจำกัดต่อสำนักงาน หรือบุคคล โดยสามารถดำเนินการแก้ไขได้	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) อาจส่งผลกระทบปานกลางต่อสำนักงาน บุคคล หรือประเทศชาติ ซึ่งคาดว่าไม่สามารถดำเนินการแก้ไขได้ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) ส่งผลกระทบร้ายแรงต่อสำนักงาน บุคคล หรือประเทศชาติ ส่งผลให้เกิดความไม่พอใจจากบุคคลหรือผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทำให้สำนักงานต้องติดต่อเพื่อขอชี้แจงต่อบุคคลหรือผู้มีส่วนได้ส่วนเสีย หรือประกาศชี้แจงผ่าน Social Media	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) อาจส่งผลกระทบร้ายแรงมากต่อสำนักงาน บุคคล หรือประเทศชาติ เกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ ทำให้สำนักงานต้องดำเนินการแถลงข่าว

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ความถูกต้องและความสมบูรณ์ของข้อมูล (Integrity: I)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) อาจส่งผลกระทบเล็กน้อยต่อสำนักงาน หรือบุคคล โดยไม่จำเป็นต้องดำเนินการแก้ไข	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) อาจส่งผลกระทบอย่างจำกัดต่อสำนักงาน หรือบุคคล โดยสามารถดำเนินการแก้ไขได้	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) อาจส่งผลกระทบปานกลางต่อสำนักงาน บุคคล หรือประเทศชาติ ซึ่งคาดว่าไม่สามารถดำเนินการแก้ไขได้ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) อาจส่งผลกระทบร้ายแรงต่อสำนักงาน บุคคล หรือประเทศชาติ ส่งผลให้เกิดความไม่พอใจจากบุคคล หรือผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทำให้สำนักงานต้องติดต่อเพื่อขอชี้แจงต่อบุคคลหรือผู้มีส่วนได้ส่วนเสีย หรือประกาศชี้แจงผ่าน Social Media	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (I) อาจส่งผลกระทบร้ายแรงมากต่อสำนักงาน บุคคล หรือประเทศชาติ เกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ ทำให้สำนักงานต้องดำเนินการแถลงข่าว

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ความพร้อมใช้งานของข้อมูล (Availability: A)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบเล็กน้อยต่อสำนักงาน หรือบุคคล โดยไม่จำเป็นต้องดำเนินการแก้ไข	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบอย่างจำกัดต่อสำนักงาน หรือบุคคล โดยสามารถดำเนินการแก้ไขได้	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบปานกลางต่อสำนักงาน บุคคล หรือประเทศชาติ ซึ่งคาดว่าไม่สามารถดำเนินการแก้ไขได้ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบร้ายแรงต่อสำนักงาน บุคคล หรือประเทศชาติ ส่งผลให้เกิดความไม่พอใจจากบุคคลหรือผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทำให้สำนักงานต้องติดต่อเพื่อขอชี้แจงต่อบุคคลหรือผู้มีส่วนได้ส่วนเสีย หรือประกาศชี้แจงผ่าน Social Media	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์ (A) อาจส่งผลกระทบร้ายแรงมากต่อสำนักงาน บุคคล หรือประเทศชาติ เกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ ทำให้สำนักงานต้องดำเนินการแถลงข่าว

หมายเหตุ: **สำหรับกรณี Cyber Security Risk Assessment**

จากตาราง สามารถคำนวณคะแนนระดับผลกระทบของสถานการณ์ความเสี่ยง ได้โดยการพิจารณาระดับผลกระทบความสามารถในการรักษาความลับของข้อมูล (Confidentiality: C)) ความถูกต้องและความสมบูรณ์ของข้อมูล (Integrity: I)) ความพร้อมใช้งานของข้อมูล (Availability: A)

จากตารางที่เสนอในข้างต้น สำนักงานได้กำหนดค่าระดับความเสี่ยงไว้ ดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ความรุนแรงของเหตุการณ์

กรณีตัวอย่าง

เกิดเหตุการณ์ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาตระหว่างการส่งข้อความทางอิเล็กทรอนิกส์ เช่น อีเมล์ และ Social media อื่น ๆ โดยผู้ไม่หวังดี โดยส่งผลกระทบเล็กน้อยต่อสำนักงาน และไม่ต้องดำเนินการแก้ไข ดังนั้น จึงสามารถประเมินโอกาสเกิดและผลกระทบได้จากคำนิยาม ดังนี้

พิจารณาโอกาสเกิดของปัจจัยเสี่ยง โดยดำเนินการดังนี้

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

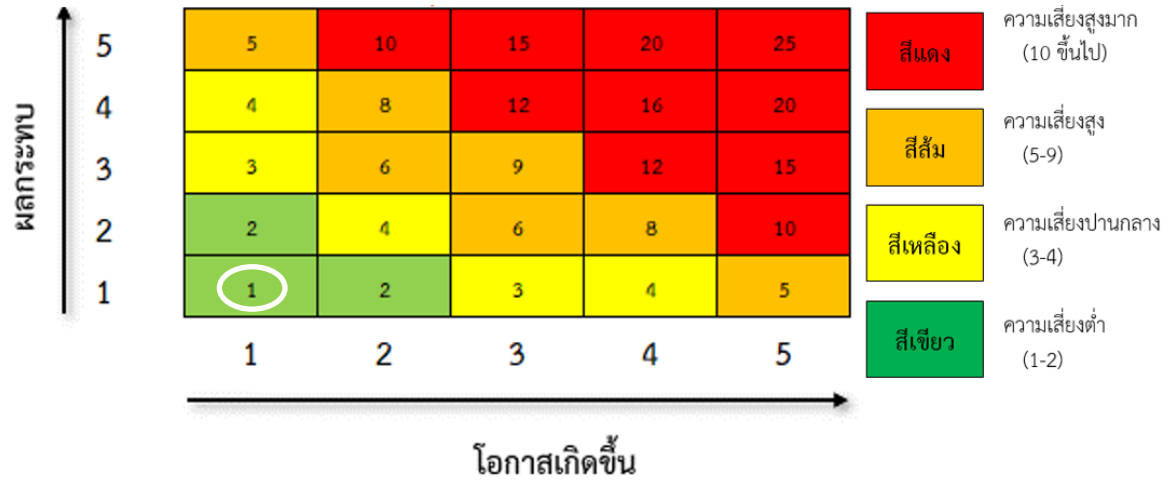
3. คะแนนที่ปัดเศษแล้วจะเป็นโอกาสของสถานการณ์ความเสี่ยง

ดังนั้น จากปัจจัยเสี่ยงข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาตระหว่างการส่งข้อความทางอิเล็กทรอนิกส์ เช่น อีเมล์ และ Social media อื่น ๆ พิจารณาแล้ว พบว่า D=1, E=2, R=1 ดังนั้น โอกาสเกิดสถานการณ์ความเสี่ยง = (3+2+2)/3 = 1.3 => ระดับ 1

และเมื่อพิจารณาถึงผลกระทบของปัจจัยเสี่ยง จะมีความเกี่ยวข้องกับการรักษาความลับ จึงเลือกใช้ความสามารถในการรักษาความลับของข้อมูล (Confidentiality: C)) ซึ่งสอดคล้องกับค่าระดับที่ 1

เกณฑ์ที่ใช้ในการประเมิน	1 = ผลกระทบน้อยที่สุด	2 = ผลกระทบน้อย	3 = ผลกระทบปานกลาง	4 = ผลกระทบมาก	5 = ผลกระทบมากที่สุด
ความสามารถในการรักษาความลับของข้อมูล (Confidentiality: C))	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) อาจส่งผลกระทบเล็กน้อยต่อสำนักงานหรือบุคคล โดยไม่จำเป็นต้องดำเนินการแก้ไข	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) อาจส่งผลกระทบอย่างจำกัดต่อสำนักงาน หรือบุคคล โดยสามารถดำเนินการแก้ไขได้	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) อาจส่งผลกระทบปานกลางต่อสำนักงาน บุคคล หรือประเทศชาติ ซึ่งคาดว่าไม่สามารถดำเนินการแก้ไขได้ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) ส่งผลกระทบร้ายแรงต่อสำนักงาน บุคคลหรือประเทศชาติ ส่งผลให้เกิดความไม่พอใจจากบุคคล หรือผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทำให้สำนักงานต้องติดต่อเพื่อขอชี้แจงต่อบุคคล หรือผู้มีส่วนได้ส่วนเสีย หรือประกาศชี้แจงผ่าน Social Media	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (C) อาจส่งผลกระทบร้ายแรงมากต่อสำนักงาน บุคคลหรือประเทศชาติ เกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ ทำให้สำนักงานต้องดำเนินการแถลงข่าว

ดังนั้น ระดับความเสี่ยงของปัจจัยเสี่ยง ข้อมูลสำคัญถูกเข้าถึง โดยไม่ได้รับอนุญาตระหว่างการส่งข้อความทางอิเล็กทรอนิกส์ เช่น อีเมล์ และ Social media อื่น ๆ จึงเท่ากับ **1** แสดงระดับความเสี่ยงดังภาพ



จากการพิจารณาค่าระดับความเสี่ยงในตารางข้างต้น สำนักงานได้แบ่งบริเวณของระดับความเสี่ยงออกเป็น 4 โซน ดังแสดงในตาราง ดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำ	ระดับความเสี่ยงที่ฝ่าย/ส่วนงาน/องค์กร สามารถยอมรับได้ โดยมีแผนจัดการความเสี่ยงหรือไม่มีแผนจัดการความเสี่ยงก็ได้
3-4	ปานกลาง	● ระดับความเสี่ยงที่ฝ่าย/ส่วนงาน ไม่สามารถยอมรับได้ โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น ● ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยให้ฝ่าย/ส่วนงาน นำไปบริหารความเสี่ยง โดยควบคุม และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น
5-9	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและมาตรการปรับปรุงการควบคุมภายใน) ให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้ และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น
10 ขึ้นไป	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ โดยต้องจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและมาตรการปรับปรุงการควบคุมภายใน) ให้ระดับความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้โดยทันที และป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น

ดังนั้น ปัจจัยเสี่ยงดังกล่าวเป็นปัจจัยเสี่ยงระดับส่วนงาน สามารถยอมรับได้ โดยมีแผนจัดการความเสี่ยงหรือไม่มีแผนจัดการความเสี่ยงก็ได้

แบบฟอร์มการรายงานผลและการติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยง และแผนการควบคุมภายใน)

เหตุการณ์ความเสี่ยง :	
เจ้าของปัจจัยเสี่ยง :	
Leading KRI	
Lagging KRI	
เป้าหมายการบริหารความเสี่ยง	
ยุทธศาสตร์ :	
การควบคุมภายในที่มีอยู่ :	
ความเสี่ยงที่ยังคงเหลือ (ปัจจัยภายใน) :	
ความเสี่ยงที่ยังคงเหลือ (ปัจจัยภายนอก) :	

แผนการควบคุมภายใน				
ที่	มาตรการปรับปรุงการควบคุมภายใน	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ	ผลผลิต

แผนจัดการความเสี่ยง				
ที่	แผนจัดการความเสี่ยงเพื่อป้องกันความเสี่ยงใหม่	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ	ผลผลิต
ที่	แผนจัดการความเสี่ยงเพื่อลดผลกระทบ	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ	ผลผลิต

แผนการควบคุมภายใน							
มาตรการปรับปรุงการควบคุมภายใน	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ	ผลผลิต	ร้อยละความก้าวหน้า	ผลการดำเนินงาน	ปัญหา/อุปสรรค	แนวทางการแก้ไข
สรุปผลการดำเนินงานประจำไตรมาส							

แผนจัดการความเสี่ยง							
แผนจัดการความเสี่ยงเพื่อป้องกันความเสี่ยงใหม่	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ	ผลผลิต	ร้อยละความก้าวหน้า	ผลการดำเนินงาน	ปัญหา/อุปสรรค	แนวทางการแก้ไข
สรุปผลการดำเนินงานประจำไตรมาส							

แผนจัดการความเสี่ยงเพื่อลดผลกระทบ	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ	ผลผลิต	ร้อยละความก้าวหน้า	ผลการดำเนินงาน	ปัญหา/อุปสรรค	แนวทางการแก้ไข
สรุปผลการดำเนินงานประจำไตรมาส							

เหตุการณ์ความเสี่ยง xx			
สถานะความเสี่ยง	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง
ระดับความเสี่ยงก่อนบริหาร			
ระดับความเสี่ยงที่คาดหวัง			
ระดับความเสี่ยง Q1			
ระดับความเสี่ยง Q2			
ระดับความเสี่ยง Q3			
ระดับความเสี่ยง Q4			

แบบฟอร์มประเมินความเพียงพอของการควบคุมภายใน และการวิเคราะห์ความเสี่ยง

1. กระบวนการ/กิจกรรม/โครงการ/บริการ (ตามข้อบังคับคณะกรรมการ 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 *(เฉพาะ IT Risk)	6. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 2 *(เฉพาะ IT Risk)	7. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 3 *(เฉพาะ IT Risk)	8. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 4 *(เฉพาะ IT Risk)	9. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 5 *(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	Supplier	Top Secret	Secret	Confidential	Internal Use	Public	Policy	WM / PC / WI	Action Plan	Format	Approve	Check&Balance	Monitoring	Report	Activity	Budget	Equipment	Man Power					

ประเภทความเสี่ยงด้าน IT Risk						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	27. ผลกระทบ	28. ระดับความเสี่ยง		Take	Treat	Transfer	Terminate			
			#DIV/0!		#DIV/0!			0								

ตัวอย่าง 1

1. กระบวนการ/กิจกรรม/โครงการ/บริการ (ตามข้อบังคับคณะกรรมการ สพร. ว่าด้วยแบ่งส่วนงานและขอบเขตหน้าที่ของส่วนงานฯ)	ประเภทความเสี่ยงด้าน S-O-F-C			ประเภทความเสี่ยงด้าน IT Risk					10. เป็นความเสี่ยงที่มีผลกระทบต่อข้อมูลส่วนบุคคลและได้จัดทำ DPIA Identification	11. ชื่อปัจจัยเสี่ยง/ประเด็นความเสี่ยง (เก้ยคุกคามและช่องโหว่)
	2. Risk Type	3. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 1	4. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 2	5. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 1 *(เฉพาะ IT Risk)	6. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 2 *(เฉพาะ IT Risk)	7. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 3 *(เฉพาะ IT Risk)	8. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 4 *(เฉพาะ IT Risk)	9. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 5 *(เฉพาะ IT Risk)		
3. การขับเคลื่อนสู่การเป็นองค์กรคุณธรรมต้นแบบ	Strategic Risk	1. External Factors	1.1 การเปลี่ยนแปลงของกฎหมายที่เกี่ยวข้องกับการดำเนินงาน ของ สพร.						✖	ผลการประเมินองค์กรคุณธรรมต้นแบบไม่เป็นไปตามเป้าหมาย

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	Supplier	Top Secret	Secret	Confidential	Internal Use	Public	Policy	WM / PC / WI	Action Plan	Format	Approve	Check&Balance	Monitoring	Report	Activity	Budget	Equipment	Man Power					
										✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	ไม่มี	เพียงพอ	ไม่มี	ไม่มี	ไม่มี

ประเภทความเสี่ยงด้าน IT Risk						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	27. ผลกระทบ	28. ระดับความเสี่ยง		Take	Treat	Transfer	Terminate			
			#DIV/0!		#DIV/0!	3	3	9	1. คณะทำงานฯ และผู้ที่เกี่ยวข้อง ไม่ทราบหลักเกณฑ์และขั้นตอนการประเมินองค์กรคุณธรรม 2. การดำเนินงานต้องอาศัยความร่วมมือของทุกฝ่าย/ส่วนงาน		✓			1. ประชุมคณะทำงานฯ และผู้เกี่ยวข้อง เพื่อชี้แจงทำความเข้าใจ รวมทั้งกำหนดแนวทางการดำเนินงานหลังจากได้รับคู่มือการประเมินองค์กรคุณธรรมประจำปีงบประมาณ จากกรมการศาสนา 2.1 จัดเตรียมข้อมูลและแบบรายงาน เพื่ออำนวยความสะดวกให้กับทุกฝ่าย/ส่วนงาน ในการจัดทำแผนและรายงานผลตามเกณฑ์การประเมินองค์กรคุณธรรม 2.2 จัดกิจกรรม หรือจัดทำ PR ประชาสัมพันธ์ เพื่อสร้างการรับรู้และความตระหนักให้แก่เจ้าหน้าที่ทุกระดับในองค์กร	ม.ค. 68 ม.ค. - มิ.ย. 68 ม.ค. - มิ.ย. 68	ผจก. CSR เจ้าหน้าที่ส่วน CSR เจ้าหน้าที่ส่วน CSR

ตัวอย่าง 2

1. กระบวนการ/กิจกรรม/โครงการ/บริการ (ตามข้อบังคับคณะกรรมการ สพร. ว่าด้วยแบ่งส่วนงานและขอบเขตหน้าที่ของส่วนงานฯ)	ประเภทความเสี่ยงด้าน S-O-F-C			ประเภทความเสี่ยงด้าน IT Risk					10. เป็นความเสี่ยงที่มีผลกระทบต่อข้อมูลส่วนบุคคลและได้จัดทำ DPIA Identification	11. ชื่อปัจจัยเสี่ยง/ประเด็นความเสี่ยง (เกี่ยวกับและช่องโหว่)
	2. Risk Type	3. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 1	4. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 2	5. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 1 *(เฉพาะ IT Risk)	6. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 2 *(เฉพาะ IT Risk)	7. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 3 *(เฉพาะ IT Risk)	8. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 4 *(เฉพาะ IT Risk)	9. รายการของเหตุการณ์ความเสี่ยง (Risk Event Categories) LEVEL 5 *(เฉพาะ IT Risk)		
1. การบริหารความเสี่ยงและควบคุมภายใน	IT Risk			1. IT Risk Management and Cybersecurity	1.1 การรักษาความลับและความมั่นคงปลอดภัย (Confidentiality & Security)	1.1.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)	1.1.4.2 การจัดชั้นความลับของข้อมูล (Information classification)	1.1.4.2.1 ชั้นความลับของสารสนเทศ (Classification of information)	✗	ข้อมูลสำคัญถูกเข้าถึง/เปิดเผย/แก้ไขเปลี่ยนแปลง

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	Supplier	Top Secret	Secret	Confidential	Internal Use	Public	Policy	WM / PC / WI	Action Plan	Format	Approve	Check&Balance	Monitoring	Report	Activity	Budget	Equipment	Man Power					
✓	✓							✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	ไม่มี	เพียงพอ	ไม่มี	ไม่มี	ไม่มี

ประเภทความเสี่ยงด้าน IT Risk						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	27. ผลกระทบ	28. ระดับความเสี่ยง		Take	Treat	Transfer	Terminate			
1	1	1	1	2	2				มีผู้ไม่หวังดีเข้ามาขโมยข้อมูล	✓				เนื่องจาก สพร. ได้มีการกำหนด IS Policy เพื่อให้เจ้าหน้าที่ถือปฏิบัติตามอย่างเคร่งครัด รวมทั้ง ส่วน CSR ได้ชี้แจงและสร้างความตระหนักในการจัดชั้นความลับและการบริหารจัดการข้อมูล/เอกสารที่ชัดเจนให้แก่เจ้าหน้าที่ส่วน CSR	ไม่มี	ไม่มี

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 การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560
5. พระราชบัญญัติ การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560
6. พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562
7. พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
8. พระราชบัญญัติ การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
9. พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
10. พระราชบัญญัติ ปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565

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

ภาคผนวก

Governance Risk management & Compliance (GRC)

Governance Risk management & Compliance (GRC)

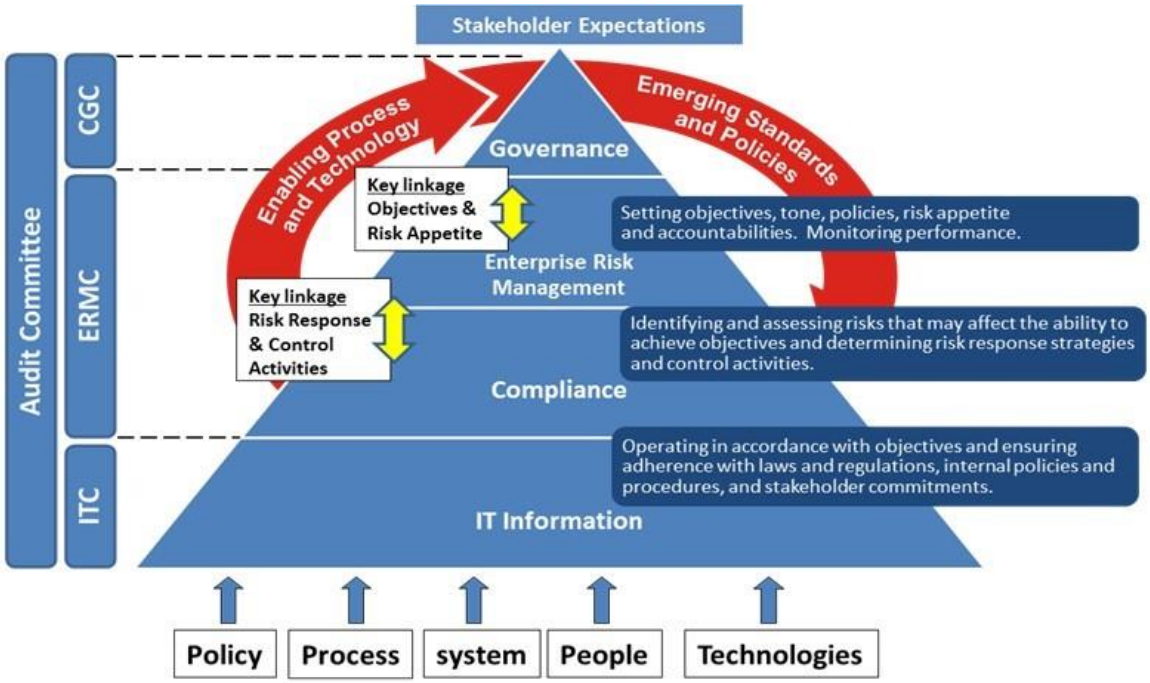
GRC คือ แนวคิดในการเชื่อมโยง และบูรณาการนิยามของสามองค์ประกอบ ได้แก่

Governance หมายถึง นโยบาย วัฒนธรรมองค์กร กระบวนการขั้นตอนการปฏิบัติงานที่ถูกกำหนดออกมาอย่างชัดเจนในการบริหารจัดการ และกำกับดูแลองค์กร โดยผู้บริหารระดับสูง เพื่อการบริหารองค์กรที่โปร่งใส ซึ่งรวมถึงความสัมพันธ์ และบทบาทของทุกคนในองค์กร ตลอดจนกำหนดเป้าหมายหลักที่เน้นเรื่องความโปร่งใสในการบริหารจัดการของผู้บริหารระดับสูงในองค์กร

Risk Management หมายถึง การบริหารจัดการความเสี่ยงที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ที่ตั้งไว้ โดยใช้กระบวนการเชิงระบบของการประเมินสถานะ และระดับของความเสี่ยงที่เกี่ยวข้องกับธุรกิจ ในลักษณะที่ทำให้การดำเนินงานไม่บรรลุผลตามเป้าหมาย โดยจะต้องหาทางระบุความเสี่ยง จัดลำดับความเสี่ยงตามความสำคัญ และบริหารจัดการหรือป้องกันหรือลดโอกาสเกิด และผลกระทบของปัจจัยเสี่ยงที่ไม่คาดหวัง (Risk) ด้วยทางเลือกที่เหมาะสม ทบทวนระดับความเสี่ยงที่เหลือ และดำเนินการบริหารจัดการเพิ่มเติมจนกระทั่งความเสี่ยงลดระดับลงมาอยู่ในเกณฑ์ที่ยอมรับได้ขององค์กร และรวมถึงใช้ประโยชน์จากเหตุการณ์ในเชิงบวก (Opportunity) ได้อย่างรวดเร็วและมีประสิทธิภาพเพื่อสร้างมูลค่าเพิ่มให้องค์กร

Compliance หมายถึง การดำเนินงานกำกับเพื่อให้มั่นใจว่า การปฏิบัติการทุกอย่างอยู่ภายใต้กฎเกณฑ์อย่างเหมาะสม ไม่มีการฝ่าฝืนใด ๆ เกิดขึ้น โดยกฎเกณฑ์ที่ว่านี้รวมทั้งระเบียบ ข้อบังคับ กฎหมาย คำสั่งภายในองค์กร พันธะที่ผูกพันไว้กับผู้มีส่วนได้เสีย คู่สัญญาทุกภาคส่วน ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความปลอดภัยขององค์กรอย่างถูกต้องตามมาตรฐาน การปฏิบัติตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็กทรอนิกส์ เป็นต้น การดำเนินงานในส่วนของการปรับปรุงประสิทธิภาพ และประสิทธิผลในการกำกับการปฏิบัติตามกฎเกณฑ์ ในลักษณะที่ติดตาม เฝ้าระวังการเปลี่ยนแปลงในด้านกฎเกณฑ์และระเบียบเพื่อทำความเข้าใจ การศึกษาผลกระทบของกฎเกณฑ์ภายนอกต่อการดำเนินงานภายใน และความจำเป็นในการปรับนโยบาย ระเบียบ ประกาศ กระบวนการปฏิบัติงานและสื่อสารเพื่อมิให้เกิดการฝ่าฝืน ซึ่งถือเป็นส่วนหนึ่งของการกำกับดูแลที่ดี

การพัฒนาแนวคิดจากการบริหารแบบ Silo มาเป็นกรอบแนวคิดที่บูรณาการ GRC เข้าด้วยกัน โดยแนวคิด GRC นั้นไม่ได้เป็นการพยายามที่จะรวบเอางาน 3 ด้าน มาไว้ที่ศูนย์กลางเพียงจุดเดียว หากแต่ต้องการที่จะนำองค์ประกอบทั้ง 3 มาปฏิบัติร่วมกันในรูปแบบของการทำงานเป็นทีม เป็นการแสวงหาแนวทาง การเชื่อมโยงบูรณาการงาน 3 ด้านเข้าด้วยกันในเชิงนโยบาย กระบวนการดำเนินงาน ขั้นตอนการปฏิบัติ และระบบการควบคุม แบ่งปันข้อมูลซึ่งกันและกัน มีการเปิดกว้างทางความคิดที่จะปรับปรุงองค์กรจากข้อมูล และแนวทางจากผู้บริหารของหลาย ๆ ฝ่าย โดยต้องได้รับการสนับสนุนจากองค์ประกอบพื้นฐานหลัก 5 ประการขององค์กร ได้แก่ กลยุทธ์ กระบวนการ ระบบ บุคลากร เทคโนโลยี ดังรูปความสัมพันธ์ และความเชื่อมโยงตามภาพ ตัวอย่าง เช่น



- การรณรงค์ปลูกฝัง ปรับเปลี่ยนวัฒนธรรมขององค์กร เพื่อนำบุคคลภายในองค์กรไปสู่วัตถุประสงค์และเป้าหมายด้านวัฒนธรรมองค์กรที่คาดหวัง เพื่อเพิ่มประสิทธิภาพ สนับสนุน หรือผลักดันให้การดำเนินงานขององค์กรบรรลุตามวัตถุประสงค์ได้ดีขึ้น ทั้งยังทำให้เกิดผลลัพธ์เชิงวัฒนธรรมองค์กรที่พึงประสงค์ด้วย

- กลยุทธ์/กระบวนการ/ระบบ : การส่งเสริมให้คณะกรรมการสามารถกำกับดูแลองค์กร และให้คำแนะนำแก่ผู้บริหาร เพื่อดำเนินงานให้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องได้อย่างมั่นใจ โดยผู้บริหารต้องจัดให้มีการบริหารความเสี่ยงที่เป็นระบบ มุ่งเน้นความเสี่ยงที่ตรงประเด็น และสามารถจัดกระบวนการทำงานเพื่อให้มีการปฏิบัติตามระเบียบ หรือการควบคุมภายในได้อย่างเหมาะสม ภายใต้ต้นทุนการดำเนินงานที่สมเหตุสมผล รวมถึงการนำเทคโนโลยีมาสนับสนุนการทำงานให้มีประสิทธิภาพ และการสื่อสารข้อมูลอย่างถูกต้องเหมาะสมทันเวลาต่อผู้เกี่ยวข้องทุกระดับ

- การที่บุคลากรมีความมุ่งมั่น ยึดถือ และส่งเสริมวัฒนธรรมของการดำเนินธุรกิจอย่างมีศักดิ์ศรี และคุณค่าทางจริยธรรม รับผิดชอบในผลงานของตน มีมุมมองที่เป็นหนึ่งเดียวกับองค์กร และต่อต้านการทำกิจกรรมที่ต่างคนต่างทำตามอำนาจหน้าที่เฉพาะตัว เน้นการทำงานเป็นทีมโดยคำนึงถึงประโยชน์ขององค์กรเป็นหลัก

- การควบคุมภายในที่เพียงพอในการลดความเสี่ยงของบุคคล ช่วยกำกับคนมากขึ้น เช่น การกำกับติดตาม (Monitoring) การใช้ระบบควบคุมการตรวจสอบคุณภาพงาน และการทดสอบผลงานว่าใช้งานได้จริงอย่างสม่ำเสมอ และมีประสิทธิผล 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 ส่งผลให้ลูกค้าเกิดความเชื่อถือ และความมั่นใจในการใช้บริการต่าง ๆ ขององค์กร

ภาคผนวก

ข้อกำหนดมาตรฐาน ISO/IEC 27001 : 2022

ระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

(Information Security Management System: ISMS)

ตาราง A.1 — การควบคุมความมั่นคงปลอดภัยสารสนเทศ

5 มาตรการควบคุมด้านองค์กร

5.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุม : นโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายเฉพาะเรื่องต้องมีการกำหนด อนุมัติโดยผู้บริหาร, เผยแพร่, สื่อสาร แก่บุคลากร และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องรับทราบ และทบทวนตามรอบระยะเวลาที่กำหนด และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น

5.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุม : บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศต้องถูกกำหนด และมอบหมายงานตามความต้องการขององค์กร

5.3 การแบ่งงานและหน้าที่ความรับผิดชอบ

มาตรการควบคุม : หน้าที่ที่ขัดแย้งกันและพื้นที่ความรับผิดชอบที่ขัดแย้งกันต้องแบ่งแยกออกจากกัน

5.4 หน้าที่ความรับผิดชอบของผู้บริหาร

มาตรการควบคุม : ผู้บริหารต้องกำหนดให้บุคลากรทุกคนใช้ความมั่นคงปลอดภัยสารสนเทศตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายเฉพาะเรื่อง และขั้นตอนปฏิบัติขององค์กรที่จัดทำขึ้น

5.5 การติดต่อหน่วยงานผู้มีอำนาจ

มาตรการควบคุม : องค์กรต้องจัดทำและรักษาไว้ซึ่งการติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้อง

5.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ

มาตรการควบคุม : องค์กรต้องจัดทำและรักษาไว้ซึ่งการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันหรือกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย และสมาคมวิชาชีพ

5.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม

มาตรการควบคุม : ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศจะถูกรวบรวมและวิเคราะห์เพื่อสร้างข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม

5.8 ความมั่นคงปลอดภัยสารสนเทศในการบริการโครงการ

มาตรการควบคุม : ความมั่นคงปลอดภัยสารสนเทศจะถูกผนวกรวมเข้ากับการบริหารจัดการโครงการ

5.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ

มาตรการควบคุม : บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น รวมถึงความเป็นเจ้าของ ต้องได้รับการจัดทำและรักษาให้คงไว้

5.10 การใช้งานข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆอย่างเหมาะสม

มาตรการควบคุม : หลักเกณฑ์การใช้งานอย่างเหมาะสมและขั้นตอนปฏิบัติสำหรับการจัดการข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ จะต้องถูกกำหนด จัดทำเป็นเอกสาร และนำไปปฏิบัติ

5.11 การคืนทรัพย์สิน

มาตรการควบคุม : บุคลากรและผู้มีส่วนได้ส่วนเสียตามความเหมาะสม ต้องคืนทรัพย์สินทั้งหมดขององค์กรที่ตนถือครองไว้ เมื่อมีการเปลี่ยนแปลงหรือสิ้นสภาพการว่าจ้างงาน สิ้นสุดสัญญาหรือข้อตกลง

5.12 การจัดหมวดหมู่ของสารสนเทศ

มาตรการควบคุม : สารสนเทศต้องได้รับการแยกหมวดหมู่ตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ตามการรักษาความลับ ความถูกต้องสมบูรณ์ ความพร้อมใช้งาน และข้อกำหนดของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

5.13 การทำป้ายชี้บ่งสารสนเทศ

มาตรการควบคุม : ชุดขั้นตอนปฏิบัติงานที่เหมาะสมสำหรับการทำป้ายชี้บ่งสารสนเทศ ต้องจัดทำและนำไปปฏิบัติตามให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้

5.14 การถ่ายโอนข้อมูล

มาตรการควบคุม : หลักเกณฑ์การถ่ายโอนข้อมูล, ขั้นตอนปฏิบัติ, หรือข้อตกลงในการถ่ายโอนข้อมูลต้องถูกนำมาใช้สำหรับการถ่ายโอนข้อมูลทุกประเภทภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก

5.15 การควบคุมการเข้าถึง

มาตรการควบคุม : ข้อบังคับในการควบคุมการเข้าถึงสารสนเทศและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ทางกายภาพและทางตรรกะ จะต้องจัดทำขึ้น และนำไปปฏิบัติตามข้อกำหนดทางธุรกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

5.16 การบริหารจัดการด้านเอกลักษณ์

มาตรการควบคุม : วงจรชีวิตของเอกลักษณ์ต่าง ๆ จะต้องได้รับการบริหารจัดการ

5.17 ข้อมูลในการพิสูจน์ตัวตน

มาตรการควบคุม : การจัดสรรและการจัดการข้อมูลในการพิสูจน์ตัวตนจะต้องถูกควบคุมโดยกระบวนการบริหารจัดการ รวมถึงการให้คำแนะนำบุคลากรในการจัดการข้อมูลการพิสูจน์ตัวตนอย่างเหมาะสม

5.18 สิทธิ์การเข้าถึง

มาตรการควบคุม : สิทธิ์การเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ จะต้องมีการให้สิทธิ์ การทบทวน การแก้ไข และการถอดถอนตามนโยบายเฉพาะขององค์กร และข้อบังคับสำหรับการควบคุมการเข้าถึง

5.19 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก

มาตรการควบคุม : กระบวนการและขั้นตอนปฏิบัติจะต้องกำหนดและนำไปปฏิบัติ เพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข่องกับการใช้ผลิตภัณฑ์ หรือบริการของผู้ให้บริการภายนอก

5.20 การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงของผู้ให้บริการภายนอก

มาตรการควบคุม : ข้อกำหนดที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดทำขึ้น และตกลงร่วมกันกับผู้ให้บริการภายนอกแต่ละรายตามประเภทของความสัมพันธ์กับผู้ให้บริการภายนอก

5.21 การจัดการด้านความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)

มาตรการควบคุม : กระบวนการและขั้นตอนปฏิบัติจะต้องกำหนด และนำไปปฏิบัติเพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับห่วงโซ่อุปทานของผลิตภัณฑ์และบริการด้าน ICT

5.22 การติดตาม การทบทวน และการเปลี่ยนแปลงการจัดการบริการของผู้ให้บริการภายนอก

มาตรการควบคุม : องค์กรต้องเฝ้าติดตาม ทบทวน ประเมิน และบริหารจัดการการเปลี่ยนแปลงไว้ในแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอก และการส่งมอบบริการอย่างสม่ำเสมอ

5.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์

มาตรการควบคุม : กระบวนการในการจัดหา การใช้ การจัดการ และการยกเลิกการใช้บริการคลาวด์จะต้องจัดทำขึ้นตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

5.24 การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุม : องค์กรต้องวางแผนและเตรียมพร้อมสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศโดยการกำหนด จัดทำ และสื่อสารกระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึง บทบาท และความรับผิดชอบ

5.25 การประเมินและการตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุม : องค์กรต้องประเมินและตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ถ้าเหตุการณ์ดังกล่าวถูกจัดหมวดหมู่เป็นเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

5.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุม : เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ต้องได้รับการตอบสนองตามเอกสารขั้นตอนปฏิบัติ

5.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุม : ความรู้ที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ต้องถูกนำไปใช้เพื่อเสริมสร้างความแข็งแกร่ง และปรับปรุงมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ

5.28 การเก็บรวบรวมหลักฐาน

มาตรการควบคุม : องค์กรต้องจัดทำและดำเนินการตามขั้นตอนปฏิบัติ ในการระบุ การเก็บรวบรวม การจัดหา การเก็บรักษาหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

5.29 ความมั่นคงปลอดภัยสารสนเทศระหว่างการหยุดชะงัก

มาตรการควบคุม : องค์กรต้องวางแผนถึงวิธีการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับที่เหมาะสมระหว่างการหยุดชะงัก

5.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ

มาตรการควบคุม : ความพร้อมด้าน ICT จะต้องวางแผน ดำเนินการ รักษาไว้ และทดสอบตามวัตถุประสงค์ความต่อเนื่องทางธุรกิจและข้อกำหนดความต่อเนื่องด้าน ICT

5.31 กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญา

มาตรการควบคุม : กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และวิธีการขององค์รเพื่อให้เป็นไปตามข้อกำหนดดังกล่าวจะต้องได้รับการระบุ จัดทำเป็นเอกสาร และปรับปรุงให้เป็นปัจจุบัน

5.32 สิทธิในทรัพย์สินทางปัญญา

มาตรการควบคุม : องค์กรต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อปกป้องสิทธิในทรัพย์สินทางปัญญา

5.33 การป้องกันบันทึก

มาตรการควบคุม : บันทึกต้องได้รับการป้องกันการสูญหาย การทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่ออกไปโดยไม่ได้รับอนุญาต

5.34 ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (PII)

มาตรการควบคุม : องค์กรต้องระบุและปฏิบัติตามข้อกำหนดที่เกี่ยวกับการรักษาความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (PII) ตามกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดตามสัญญา

5.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ

มาตรการควบคุม : วิธีการขององค์กรที่ใช้เพื่อบริการจัดการความมั่นคงปลอดภัยสารสนเทศ และการนำไปปฏิบัติรวมถึงบุคลากร กระบวนการ และเทคโนโลยีจะต้องได้รับการทบทวนอย่างเป็นอิสระตามช่วงเวลาที่วางแผนไว้ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคม : การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร นโยบายเฉพาะกฎระเบียบ และมาตรฐาน ต้องได้รับการทบทวนอย่างสม่ำเสมอ

5.37 เอกสารขั้นตอนการปฏิบัติงาน

มาตรการควบคุม : ขั้นตอนการปฏิบัติสำหรับสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศจะต้องจัดทำเป็นเอกสาร และมีพร้อมใช้แก่ผู้ใช้งานทุกคนที่จำเป็นต้องใช้

6. มาตรการควบคุมด้านบุคลากร

6.1 การคัดกรอง

มาตรการควบคุม : การตรวจสอบประวัติความเป็นมาของผู้สมัครงานทั้งหมด เพื่อเป็นพนักงานต้องดำเนินการก่อนเข้าร่วมองค์กร และดำเนินการอย่างต่อเนื่องโดยให้สอดคล้องตามกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้องและเหมาะสมต่อข้อกำหนดทางธุรกิจ ชั้นความลับข้อมูลที่จะเข้าถึง และความเสี่ยงที่เกี่ยวข้อง

6.2 ข้อตกลงและเงื่อนไขการจ้างงาน

มาตรการควบคุม : ข้อตกลงในสัญญาจ้างงานต้องกล่าวถึงหน้าที่ความรับผิดชอบของบุคลากร และขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศ

6.3 ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุม : บุคลากรขององค์กรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องจะต้องได้รับการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ การให้ความรู้ การฝึกอบรม และการปรับปรุงอย่างสม่ำเสมอถึงนโยบายขององค์กร นโยบายเฉพาะ และขั้นตอนปฏิบัติ ที่เกี่ยวกับด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่เกี่ยวข้องกับงานที่รับผิดชอบอย่างสม่ำเสมอ

6.4 กระบวนการทางวินัย

มาตรการควบคุม : กระบวนการทางวินัยจะต้องเป็นทางการและสื่อสารให้รับทราบ เพื่อลงโทษบุคลากรและผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่ฝ่าฝืน ละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ

6.5 ความรับผิดชอบหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน

มาตรการควบคุม : ความรับผิดชอบและหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศที่ยังคงหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน ต้องกำหนดไว้ บังคับใช้ และสื่อสารกับบุคลากรที่เกี่ยวข้องและผู้มีส่วนได้ส่วนเสียอื่น ๆ ทราบ

6.6 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ

มาตรการควบคุม : ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับสะท้อนให้เห็นถึงความต้องการขององค์กรในการปกป้องข้อมูล จะต้องกำหนด จัดทำเป็นเอกสาร ทบทวนอย่างสม่ำเสมอ และลงนามโดยบุคลากรและผู้มีส่วนได้ส่วนเสียอื่น ๆ

6.7 การปฏิบัติงานจากระยะไกล

มาตรการควบคุม : มาตรการรักษาด้านความมั่นคงปลอดภัยจะต้องนำไปปฏิบัติ เมื่อบุคลากรปฏิบัติงานจากระยะไกล เพื่อปกป้องข้อมูลที่ถูกเข้าถึง การประมวลผล หรือจัดเก็บจากภายนอกองค์กร

6.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุม : องค์กรต้องจัดให้มีกลไกสำหรับบุคลากรในการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่สังเกตพบ หรือต้องสงสัยผ่านช่องทางที่เหมาะสมในเวลาที่เหมาะสม

7 มาตรการควบคุมด้านกายภาพ

7.1 อาณาเขตความมั่นคงปลอดภัยทางกายภาพ

มาตรการควบคุม : อาณาเขตความมั่นคงปลอดภัย ต้องถูกกำหนด และนำไปใช้เพื่อปกป้องพื้นที่ที่มีสารสนเทศและทรัพย์สินที่เกี่ยวข้องอื่น ๆ

7.2 การเข้า-ออกพื้นที่

มาตรการควบคุม : บริเวณที่ต้องรักษาความมั่นคงปลอดภัยต้องได้รับการปกป้องโดยมาตรการควบคุมการเข้า-ออก และจุดที่เข้าถึงได้อย่างเหมาะสม

7.3 ความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก

มาตรการควบคุม : ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกต่าง ๆ ต้องได้รับการออกแบบ และนำไปประยุกต์ใช้

7.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ

มาตรการควบคุม : สถานที่จะต้องได้รับการเฝ้าติดตามสำหรับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตอย่างต่อเนื่อง

7.5 การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม

มาตรการควบคุม : การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม เช่น ภัยพิบัติทางธรรมชาติ และทางกายภาพอื่น ๆ โดยตั้งใจหรือไม่ตั้งใจ

7.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย

มาตรการควบคุม : มาตรการรักษาด้านความมั่นคงปลอดภัยสำหรับการทำงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัยต้องได้รับการออกแบบ และนำไปประยุกต์ใช้

7.7 การจัดเก็บโต๊ะทำงาน และจัดการหน้าจอ

มาตรการควบคุม : กฎเกณฑ์การจัดเก็บโต๊ะทำงานสำหรับกระดาษและสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ และกฎเกณฑ์การจัดการหน้าจอสำหรับสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องกำหนดและบังคับใช้อย่างเหมาะสม

7.8 การจัดวางและการป้องกันอุปกรณ์

มาตรการควบคุม : อุปกรณ์ต้องได้รับการจัดวางอย่างปลอดภัยและได้รับการป้องกัน

7.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสำนักงาน

มาตรการควบคุม : ทรัพย์สินที่นำออกไปใช้งานนอกสำนักงานจะต้องได้รับการป้องกัน

7.10 สื่อบันทึกข้อมูล

มาตรการควบคุม : สื่อบันทึกข้อมูลต้องได้รับการบริหารจัดการตลอดวงจรชีวิตของการจัดหา การใช้งาน การขนส่ง และการจำหน่ายตามการจัดระดับชั้นความลับขององค์กรและข้อกำหนดในการจัดการ

7.11 ระบบสาธารณูปโภคสนับสนุน

มาตรการควบคุม : สิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องได้รับการป้องกันจากความล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากความผิดพลาดของระบบสาธารณูปโภคสนับสนุน

7.12 ความมั่นคงปลอดภัยของการเดินสาย

มาตรการควบคุม : สายเคเบิลที่นำไฟฟ้า,ข้อมูล หรือสนับสนุนบริการทางข้อมูลจะต้องได้รับการปกป้องจากการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย

7.13 การบำรุงรักษาอุปกรณ์

มาตรการควบคุม : อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มั่นใจถึงความพร้อมใช้งาน ความถูกต้องในการทำงาน และการรักษาความลับของข้อมูล

7.14 การจำหน่ายหรือนำอุปกรณ์มาใช้ซ้ำอย่างมั่นคงปลอดภัย

มาตรการควบคุม : อุปกรณ์ที่มีสื่อบันทึกข้อมูลจะต้องได้รับการตรวจสอบ เพื่อให้มั่นใจว่าข้อมูลที่ละเอียดอ่อนและซอฟต์แวร์ลิขสิทธิ์ที่ติดตั้งอยู่ ได้ถูกลบออก หรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนนำไปจำหน่าย หรือนำมาใช้ซ้ำ

8. มาตรการควบคุมด้านเทคโนโลยี

8.1 อุปกรณ์ระดับผู้ใช้งาน

มาตรการควบคุม : ข้อมูลที่จัดเก็บ ประมวลผล หรือเข้าถึงได้ผ่านอุปกรณ์ปลายทางของผู้ใช้ ต้องได้รับการปกป้อง

8.2 สิทธิพิเศษในการเข้าถึง

มาตรการควบคุม : การจัดสรรและใช้สิทธิ์การเข้าถึงที่เป็นสิทธิพิเศษต้องถูกจำกัด และบริหารจัดการ

8.3 การจำกัดการเข้าถึงข้อมูล

มาตรการควบคุม : การเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ต้องถูกจำกัดตามนโยบายเฉพาะที่จัดทำไว้ในการควบคุมการเข้าถึง

8.4 การเข้าถึงซอร์สโค้ด

มาตรการควบคุม : การเข้าถึงซอร์สโค้ดโดยการอ่านและเขียน เครื่องมือในการพัฒนา และซอฟต์แวร์ไลบรารีต้องได้รับการจัดการอย่างเหมาะสม

8.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย

มาตรการควบคุม : เทคโนโลยีของการพิสูจน์ตัวตนอย่างมั่นคงปลอดภัยและขั้นตอนปฏิบัติ ต้องดำเนินการตามข้อจำกัดการเข้าถึงสารสนเทศและนโยบายเฉพาะเกี่ยวกับการควบคุมการเข้าถึง

8.6 การบริหารจัดการขีดความสามารถของทรัพยากร

มาตรการควบคุม : การใช้ทรัพยากรต้องได้รับการเฝ้าระวัง และปรับให้สอดคล้องกับความต้องการในปัจจุบันและที่คาดการณ์ไว้

8.7 การป้องกันจากโปรแกรมไม่พึงประสงค์

มาตรการควบคุม : การป้องกันจากโปรแกรมไม่พึงประสงค์จะต้องดำเนินการและสนับสนุนโดยการสร้างความตระหนักแก่ผู้ใช้งานอย่างเหมาะสม

8.8 การบริหารจัดการช่องโหว่ทางเทคนิค

มาตรการควบคุม : ต้องได้รับข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งาน, ช่องโหว่ดังกล่าวขององค์กร ต้องได้รับการประเมินและระบุมาตรการที่เหมาะสม

8.9 การจัดการการตั้งค่า

มาตรการควบคุม : องค์ประกอบ รวมถึงความมั่นคงปลอดภัยขององค์ประกอบ ของฮาร์ดแวร์ ซอฟต์แวร์ บริการและเครือข่าย ต้องจัดทำ ทำเป็นเอกสาร นำไปปฏิบัติ เฝ้าติดตาม และทบทวน

8.10 การลบข้อมูล

มาตรการควบคุม : ข้อมูลที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์หรือสื่อบันทึกข้อมูลอื่น ๆ ต้องถูกลบออก เมื่อไม่มีความจำเป็นต้องใช้งานข้อมูลนั้นอีก

8.11 การซ่อนข้อมูล

มาตรการควบคุม : การปิดบังข้อมูล ต้องใช้ตามนโยบายเฉพาะขององค์กรที่เกี่ยวกับการควบคุมการเข้าถึงและนโยบายเฉพาะอื่น ๆ ที่เกี่ยวข้อง และข้อกำหนดทางธุรกิจ โดยนำกฎหมายที่บังคับใช้มาพิจารณา

8.12 การป้องกันข้อมูลรั่วไหล

มาตรการควบคุม : มาตรการป้องกันข้อมูลรั่วไหล ต้องนำไปใช้กับระบบ เครือข่าย และอุปกรณ์อื่น ๆ ที่ใช้ประมวลผล จัดเก็บ หรือมีการส่งข้อมูลที่ละเอียดอ่อน

8.13 การสำรองข้อมูล

มาตรการควบคุม : การสำรอง ข้อมูลสารสนเทศ, ซอฟต์แวร์ และระบบ ต้องได้รับการบำรุงรักษาและทดสอบอย่างสม่ำเสมอ สอดคล้องกับนโยบายเฉพาะที่ตกลงกันในการสำรองข้อมูล

8.14 ระบบทดแทน

มาตรการควบคุม : สิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องดำเนินการสำรองไว้อย่างเพียงพอ เพื่อให้เป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน

8.15 การบันทึกกิจกรรม

มาตรการควบคุม : ล็อกที่บันทึกกิจกรรม ข้อยกเว้น ข้อผิดพลาด และเหตุการณ์ที่เกี่ยวข้องอื่น ๆ จะต้องมีการจัดทำขึ้น จัดเก็บ ป้องกัน และวิเคราะห์

8.16 การเฝ้าติดตามกิจกรรม

มาตรการควบคุม : เครือข่าย ระบบ และแอปพลิเคชัน ต้องได้รับการเฝ้าติดตามพฤติกรรมที่ผิดปกติ และการดำเนินการที่เหมาะสม เพื่อประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น

8.17 การตั้งค่านาฬิกาให้ตรงกัน

มาตรการควบคุม : นาฬิกาของระบบประมวลผลสารสนเทศที่องค์กรใช้งาน ต้องได้รับการตั้งค่าเวลาให้ตรงกับแหล่งเทียบเวลาที่ได้รับการรับรอง

8.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ

มาตรการควบคุม : การใช้งานโปรแกรมยูทิลิตี้ ที่สามารถข้ามผ่านมาตรการควบคุมของระบบและแอปพลิเคชันได้ต้องถูกจำกัด และควบคุมอย่างเคร่งครัด

8.19 การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ

มาตรการควบคุม : ต้องดำเนินการตามขั้นตอนปฏิบัติและมาตรการ เพื่อจัดการการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการอย่างมั่นคงปลอดภัย

8.20 ความมั่นคงปลอดภัยของเครือข่าย

มาตรการควบคุม : เครือข่ายและอุปกรณ์เครือข่ายต้องได้รับการรักษาความมั่นคงปลอดภัย บริหารจัดการ และควบคุมเพื่อปกป้องข้อมูลในระบบและแอปพลิเคชัน

8.21 ความมั่นคงปลอดภัยของบริการเครือข่าย

มาตรการควบคุม : กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของบริการเครือข่าย ต้องได้รับการระบุ นำไปปฏิบัติ และเฝ้าติดตาม

8.22 การแบ่งแยกเครือข่าย

มาตรการควบคุม : กลุ่มบริการข้อมูลสารสนเทศ ผู้ใช้ และระบบสารสนเทศต่าง ๆ ต้องได้รับการแบ่งแยกออกจากเครือข่ายขององค์กร

8.23 การกรองเว็บ

มาตรการควบคุม : การเข้าถึง การเปิดเว็บไซต์ภายนอก ต้องได้รับการจัดการ เพื่อลดปัจจัยเสี่ยงในการเข้าถึงเนื้อหาที่เป็นอันตราย

8.24 การเข้ารหัสข้อมูล

มาตรการควบคุม : หลักเกณฑ์สำหรับการใช้งานการเข้ารหัสข้อมูลอย่างมีประสิทธิภาพ รวมถึงการบริหารจัดการกุญแจการเข้ารหัสข้อมูล ต้องได้รับการกำหนดและนำไปปฏิบัติ

8.25 วงจรการพัฒนาอย่างมั่นคงปลอดภัย

มาตรการควบคุม : หลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบอย่างมั่นคงปลอดภัย ต้องได้รับการกำหนดและนำไปปฏิบัติ

8.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน

มาตรการควบคุม : หลักเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศจะต้องกำหนด ระบุ และอนุมัติเมื่อพัฒนาหรือจัดหาแอปพลิเคชัน

8.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย

มาตรการควบคุม : หลักการด้านความมั่นคงปลอดภัยทางวิศวกรรมระบบ ต้องจัดทำ ทำเป็นเอกสาร บำรุงรักษา และนำไปประยุกต์ใช้กับทุกกิจกรรมของการพัฒนาระบบสารสนเทศ

8.28 การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย

มาตรการควบคุม : หลักการในการเขียนชุดคำสั่งอย่างมั่นคงปลอดภัยเข้ารหัสที่ ต้องนำไปใช้กับการพัฒนาซอฟต์แวร์

8.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาและการยอมรับ

มาตรการควบคุม : การทดสอบความมั่นคงปลอดภัย ต้องได้รับการกำหนดและนำไปประยุกต์ใช้ในวงจรชีวิตของการพัฒนา

8.30 การพัฒนาโดยหน่วยงานภายนอก

มาตรการควบคุม : องค์กรต้องกำกับดูแล เฝ้าติดตาม และทบทวนกิจกรรมที่เกี่ยวข้องกับการพัฒนาระบบจากหน่วยงานภายนอก

8.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงออกจากกัน

มาตรการควบคุม : สภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงต้องถูกแบ่งแยกออกจากกัน และรักษาความมั่นคงปลอดภัย

8.32 การบริหารจัดการการเปลี่ยนแปลง

มาตรการควบคุม : การเปลี่ยนแปลงถึงสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ และระบบสารสนเทศต้องเป็นไปตามขั้นตอนการจัดการการเปลี่ยนแปลง

8.33 ข้อมูลในการทดสอบ

มาตรการควบคุม : ข้อมูลในการทดสอบต้องได้รับการคัดเลือก ปกป้อง และบริหารจัดการอย่างเหมาะสม

8.34 การปกป้องระบบสารสนเทศระหว่างการทดสอบในการตรวจประเมิน

มาตรการควบคุม : การทดสอบในการตรวจประเมิน และกิจกรรมการรับประกันอื่น ๆ ที่เกี่ยวข้องกับการตรวจประเมินระบบปฏิบัติการ ต้องมีการวางแผน และตกลงร่วมกันระหว่างผู้ทดสอบและผู้บริหารอย่างเหมาะสม

<u>รายนามคณะกรรมการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)</u>

1. นายณปกรณ์ ธนสุวรรณเกษม ประธานกรรมการ
2. นายธนา โพธิกำจร กรรมการผู้ทรงคุณวุฒิ
   (ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : ด้านเทคโนโลยีดิจิทัล)
3. นายอภิรัต ศิรินาวิน กรรมการผู้ทรงคุณวุฒิ
   (ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : ด้านเทคโนโลยีดิจิทัล)
4. นายฉัตรชัย ธนาฤดี กรรมการผู้ทรงคุณวุฒิ
   (ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้าน : ด้านการเงิน การบัญชีและงบประมาณ การตรวจสอบ ประเมินผล และการบริหารความเสี่ยง)
5. ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กรรมการโดยตำแหน่ง
   (นายวิศิษฏ์ วิศิษฏ์สรอรรถ)
6. เลขาธิการคณะกรรมการพัฒนาระบบราชการ กรรมการโดยตำแหน่ง
   (นางสาวอ้อนฟ้า เวชชาชีวะ)
7. ผู้แทนผู้อำนวยการสำนักงบประมาณ กรรมการโดยตำแหน่ง
   (นายกรณินทร์ กาญจโนมัย รองผู้อำนวยการสำนักงบประมาณปฏิบัติราชการแทน ผู้อำนวยการสำนักงบประมาณ)
8. นายชัย วุฒิวิวัฒน์ชัย กรรมการโดยตำแหน่ง
   (ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติปฏิบัติการแทน ผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ)

รายนามคณะผู้บริหาร

1. นางไอรดา เหลืองวิไล	รองผู้อำนวยการ รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
2. นางสาวอภิณห์พร อังคกมลเศรษฐ์	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
3. นายณัฐวัชร์ วรนพกุล	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
4. นายอาศิส อัญญะโพธิ์	ผู้ช่วยผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
5. นายชรินทร์ ธีรฐิตยางกูร	ผู้อำนวยการฝ่ายขับเคลื่อนนโยบายรัฐบาลดิจิทัล
6. นางสาวทิสวรรณ ชูปัญญา	ผู้อำนวยการฝ่ายกลยุทธ์องค์กร
7. นายพิชัย ร่วมภูมิสุข	ผู้อำนวยการสำนักเลขานุการผู้อำนวยการ
8. นางคณาพร สนธยานนท์	ผู้อำนวยการฝ่ายบริหารกลาง
9. นายบรรเจิด พรหมโสภา	ผู้อำนวยการฝ่ายบัญชีและการเงิน
10. นายอุสรา วิสารทานนท์	ผู้อำนวยการฝ่ายที่ปรึกษาและบริหารโครงการ
11. นางสาวอุรัชฎา เกตุพรหม	ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ
12. นายสุพัชรินทร์ กิ่งแก้ว	ผู้อำนวยการฝ่ายพัฒนาแพลตฟอร์มดิจิทัลแลกเปลี่ยนข้อมูล
13. นายปณิธาน เขินอำนวย	ผู้อำนวยการฝ่ายความมั่นคงปลอดภัยทางไซเบอร์
14. นายธนกร ศรีคำดี	ผู้อำนวยการฝ่ายตรวจสอบภายใน
15. นายวิจักขณ์ ซื่อวาจา	ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ
16. นายเกียรติศักดิ์ เรืองรอด	ผู้อำนวยการฝ่ายปฏิบัติการดิจิทัล
17. นางสาวณัฏฐ์ฉัตร จันทร์แสงศรี	ผู้อำนวยการพัฒนาเทคโนโลยีและนวัตกรรมดิจิทัล
18. นายอธิบดี ลิมสัมพันธ์สันติ	ผู้อำนวยการฝ่ายพัฒนแพลตฟอร์มดิจิทัลประชาชน
19. นางสาวมณฑา ชยากรวิกรม	ผู้อำนวยการสถาบันนวัตกรรมและธรรมาภิบาลข้อมูล

รายนามคณะผู้จัดทำ

1. นางสาวทิสวรรณ ชูปัญญา	ผู้อำนวยการฝ่ายกลยุทธ์องค์กร
2. นายภัทรพงศ์ วงศ์สุวัฒน์	ผู้จัดการส่วนบริหารความเสี่ยง
3. นางสาวสุชาวลี ดวงมณี	นักวิเคราะห์ 2
4. นางสาวปุณยนุช พงศ์พานิช	นักวิเคราะห์

ออกแบบโดย

1. นางสาวทิสวรรณ ชูปัญญา	ผู้อำนวยการฝ่ายกลยุทธ์องค์กร
2. นายภัทรพงศ์ วงศ์สุวัฒน์	ผู้จัดการส่วนบริหารความเสี่ยง
3. นางสาวปุณยนุช พงศ์พานิช	นักวิเคราะห์

ปรับปรุง

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
ครั้งที่ 8 เดือนกันยายน 2566
ครั้งที่ 9 เดือนมิถุนายน 2567
ครั้งที่ 10 เดือนกันยายน 2567