



คู่มือการบริหารความเสี่ยงของ สสว.
ประจำปี 2566

สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.)
The Office of Small and Medium Enterprises Promotion (OSMEP)

คำนำ

สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.) ตระหนักและให้ความสำคัญต่อการทบทวนและนำแนวคิดการบริหารความเสี่ยงทั่วทั้งองค์กรตามมาตรฐานสากลที่เป็นปัจจุบันมาประยุกต์ใช้งานภายในองค์กร โดยมีวัตถุประสงค์ที่จะสร้างประสิทธิผลของการดำเนินงานด้านการบริหารความเสี่ยงให้เกิดขึ้นในทุกระดับขององค์กรและจัดทำนโยบายบริหารความเสี่ยงเพื่อใช้เป็นกรอบแนวทางการพัฒนาระบบการบริหารความเสี่ยง แล้วจึงจัดทำคู่มือการบริหารความเสี่ยงขององค์กรขึ้นเพื่อให้ผู้บริหารและผู้ปฏิบัติงานทุกระดับได้ศึกษาและสร้างความรู้ ความเข้าใจที่ถูกต้องต่อกระบวนการบริหารความเสี่ยงตามมาตรฐานสากล ก่อนนำไปประยุกต์ใช้ในการปฏิบัติงานในทุกบทบาทหน้าที่ที่ได้รับมอบหมายให้สอดคล้องกันทั่วทั้งองค์กร โดยมุ่งหวังให้เป็นวัฒนธรรมการบริหารความเสี่ยงในการปฏิบัติงานซึ่งจะช่วยเพิ่มมูลค่า (Value Added) และสร้างสรรค์มูลค่า (Value Creation) ให้แก่องค์กรและสร้างความมั่นใจให้กับผู้มีส่วนได้เสียว่าการดำเนินงานของสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.) จะบรรลุผลตามภารกิจที่ได้รับมอบหมายและมีความยั่งยืนสืบไป

ส่วนบริหารความเสี่ยงและควบคุมภายใน

ฝ่ายกลยุทธ์องค์กร

สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

พฤศจิกายน 2565

สารบัญ

	หน้า
บทที่ 1 บทนำองค์กร	6
1.1 ความเป็นมาของ สสว.	6
1.2 แผนปฏิบัติการของ สสว. ประจำปี 2566	6
บทที่ 2 หลักเกณฑ์การบริหารความเสี่ยง	8
2.1 กรอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2017	8
2.2 กรอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2004	10
2.3 กรอบหลักเกณฑ์การบริหารความเสี่ยงของทุนหมุนเวียน ประจำปีบัญชี 2566	10
บทที่ 3 กรอบการบริหารความเสี่ยงของ สสว.	13
โครงสร้างการบริหารความเสี่ยง	14
3.1 โครงสร้างการบริหารความเสี่ยงของ สสว.	14
3.2 บทบาทความรับผิดชอบด้านการบริหารความเสี่ยง	15
สภาพแวดล้อมภายในองค์กร	17
3.3 นโยบายการบริหารความเสี่ยง	17
3.4 วัตถุประสงค์การบริหารความเสี่ยง	18
3.5 กลยุทธ์การบริหารความเสี่ยง	18
3.6 วัฒนธรรมการบริหารความเสี่ยง	18
3.7 นิยามศัพท์การบริหารความเสี่ยง	19
กระบวนการบริหารความเสี่ยง	24
3.8 กำหนดแหล่งที่มาของความเสี่ยง	25
3.9 ระบุปัจจัยเสี่ยง	25
3.10 ประเมินประสิทธิผลของการควบคุมที่มีอยู่	27
3.11 ระบุระดับความรุนแรง	28
3.12 จัดลำดับความเสี่ยง	30
3.13 คัดเลือกวิธีจัดการความเสี่ยง	32
3.14 สื่อสารความเสี่ยงแบบบูรณาการ	36
3.15 รายงานผลบริหารความเสี่ยง	37
ปัจจัยสนับสนุนการบริหารความเสี่ยง	33
3.16 ระบบรายงานผลและปรับปรุงผลการบริหารความเสี่ยง	38
3.17 สารสนเทศและการสื่อสารด้านบริหารความเสี่ยง	38

ภาคผนวก	40
ตารางเปรียบเทียบองค์ประกอบของคู่มือการบริหารความเสี่ยงที่ดีตามเกณฑ์ประเมินผล	41
ประวัติการปรับปรุงคู่มือการบริหารความเสี่ยงของ สสว.	42
ตัวอย่างแบบพิมพ์การประเมินความเสี่ยงและจัดทำแผนบริหารความเสี่ยงระดับองค์กร	43

สารบัญภาพ

	หน้า
ภาพที่ 1 ภาพรวมแผนปฏิบัติการของ สสว. ประจำปี 2566	7
ภาพที่ 2 องค์ประกอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2017	8
ภาพที่ 3 องค์ประกอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2004	10
ภาพที่ 4 กรอบการบริหารความเสี่ยงของ สสว.	13
ภาพที่ 5 โครงสร้างการบริหารความเสี่ยง	14
ภาพที่ 6 แผนผังกระบวนการบริหารความเสี่ยงของ สสว.	24
ภาพที่ 7 ความสัมพันธ์ของความเสี่ยงและกิจกรรมการควบคุม	27
ภาพที่ 8 ตารางหลักเกณฑ์การประเมินประสิทธิผลการควบคุมภายในที่มีอยู่	27
ภาพที่ 9 สูตรการคำนวณค่าระดับความเสี่ยง	28
ภาพที่ 10 การติดตามความก้าวหน้าของการจัดการความเสี่ยงในแต่ละความเสี่ยง	29
ภาพที่ 11 ตารางตัวอย่างการกำหนดค่าโอกาสเกิดความเสี่ยง	29
ภาพที่ 12 ตารางตัวอย่างการกำหนดค่าผลกระทบจากความเสี่ยง	30
ภาพที่ 13 ตารางจัดระดับความรุนแรงของความเสี่ยง (Risk Matrix)	31
ภาพที่ 14 แสดงแนวคิดความคาดหวังของการจัดการความเสี่ยงในแต่ละความเสี่ยง	33
ภาพที่ 15 ตารางแสดงเกณฑ์ความสามารถในการยอมรับความเสี่ยง	33
ภาพที่ 16 ตารางแสดงตัวอย่างวิเคราะห์ Cost - Benefit ของมาตรการจัดการความเสี่ยง	36

บทที่ 1

บทนำ

1.1 ความเป็นมาของ สสว.

สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม จัดตั้งตามพระราชบัญญัติส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม พ.ศ. 2543 และพระราชบัญญัติส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (ฉบับที่ 2) พ.ศ. 2561 แก้ไขเพิ่มเติม มีสถานะเป็นหน่วยงานของรัฐภายใต้การกำกับดูแลของนายกรัฐมนตรี และดำเนินการบริหารจัดการกองทุนโดยคณะกรรมการ 2 คณะ ประกอบด้วย

คณะกรรมการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

มีอำนาจหน้าที่ในการกำหนดนโยบายและแผนการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อมรวมทั้งกำกับการดำเนินงานของคณะกรรมการบริหารสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม โดยมีนายกรัฐมนตรีเป็นประธานกรรมการ และผู้อำนวยการสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (ผอ.สสว.) เป็นกรรมการและเลขานุการ (มาตรา 6)


คณะกรรมการบริหารสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

มีอำนาจหน้าที่วางนโยบาย บริหารงาน ควบคุม กำกับดูแลและรับผิดชอบในกิจการของ สสว. โดยมีประธานกรรมการและกรรมการบริหารฯ ผู้มีความรู้ ความเชี่ยวชาญ มีประสบการณ์เกี่ยวกับวิสาหกิจขนาดกลางและขนาดย่อมที่ได้รับการแต่งตั้งจากคณะกรรมการส่งเสริมฯ โดยมีผู้อำนวยการสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (ผอ.สสว.) เป็นกรรมการและเลขานุการ (มาตรา 18)

1.2 แผนปฏิบัติการของ สสว. ประจำปี 2566

สำหรับปี 2566 ได้กำหนดวิสัยทัศน์ พันธกิจและยุทธศาสตร์ ไว้ดังนี้

วิสัยทัศน์ พันธกิจ ค่านิยมองค์กร และแผนปฏิบัติการของ สสว.

 วิสัยทัศน์

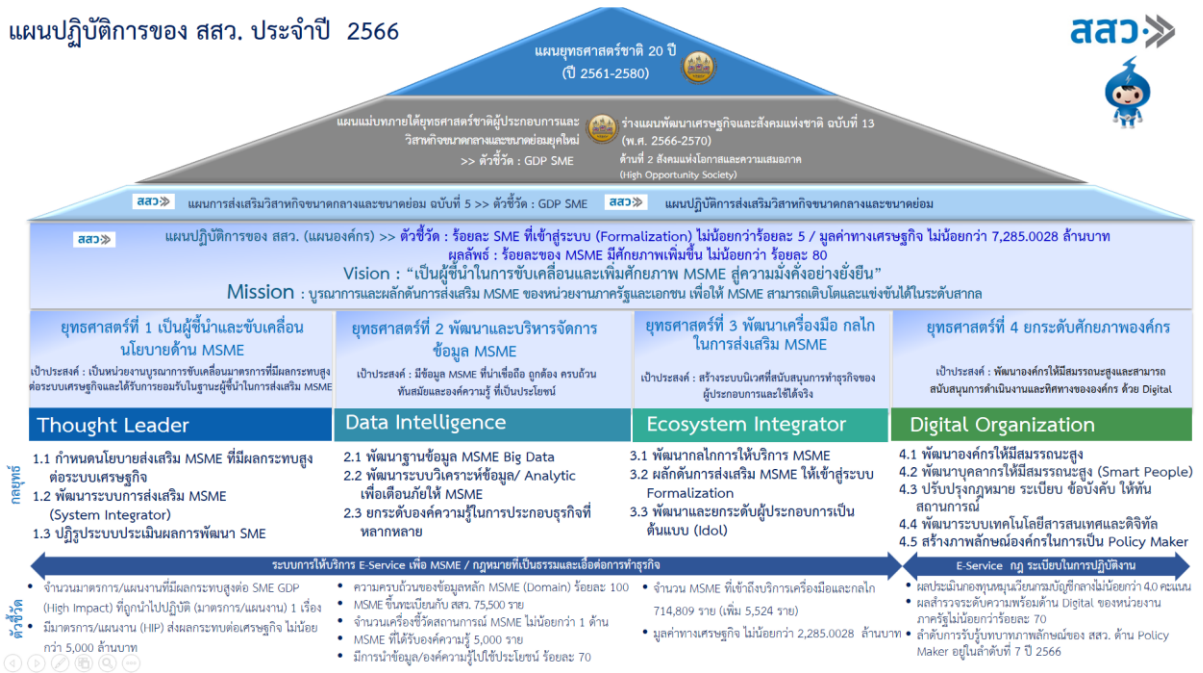
“เป็นผู้นำในการขับเคลื่อน
และเพิ่มศักยภาพ MSME
สู่ความมั่งคั่งอย่างยั่งยืน”

 พันธกิจ

“บูรณาการและผลักดันการ
ส่งเสริม MSME ของหน่วยงาน
ภาครัฐและเอกชน เพื่อให้
MSME สามารถเติบโตและ
แข่งขันได้ในระดับสากล”



แผนปฏิบัติการของ สสว. ประจำปี 2566



ภาพที่ 1 ภาพรวมแผนปฏิบัติการของ สสว.ประจำปี 2566

ดังนั้น เพื่อให้การดำเนินงานของ สสว. บรรลุวัตถุประสงค์ของการจัดตั้งและเพื่อให้เกิดความตระหนักและคำนึงถึงการพัฒนาปรับปรุงหรือเพิ่มประสิทธิภาพการบริหารจัดการ สามารถตรวจสอบสถานภาพหรือความสามารถในการบริหารจัดการองค์กร เพื่อประโยชน์ในการบริหารและพัฒนาองค์กรในปัจจุบันและอนาคตได้ จึงจำเป็นต้องมีการติดตามและประเมินผลการดำเนินงานในเรื่องดังกล่าว โดยคณะรัฐมนตรีได้มีมติให้หน่วยงานต่าง ๆ มีการกำหนดระบบการติดตามประเมินผลที่เป็นมาตรฐานสากล รวมทั้งกรมบัญชีกลาง กระทรวงการคลัง ในฐานะผู้กำกับดูแลการดำเนินงานของกองทุนและเงินหมุนเวียนได้ทำบันทึกข้อตกลงการประเมินผลการดำเนินงานกองทุนส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อมตั้งแต่ปีบัญชี 2548 จนถึงปัจจุบัน โดยภายใต้กรอบหลักเกณฑ์การประเมินผลฯ การบริหารความเสี่ยงได้ถูกกำหนดให้เป็นตัววัดระดับความสำเร็จในการเพิ่มประสิทธิภาพด้านการบริหารจัดการองค์กรของ สสว. ตามตัวชี้วัดที่ 4.1 การบริหารความเสี่ยงและการควบคุมภายใน ข้อ 2 การกำหนดวัตถุประสงค์การบริหารความเสี่ยง ประเด็นย่อย (1) การจัดทำ/ทบทวนคู่มือการบริหารความเสี่ยง ซึ่ง สสว. จะต้องดำเนินการให้เป็นไปตามที่กรมบัญชีกลางกำหนด

บทที่ 2

หลักเกณฑ์การบริหารความเสี่ยง

เนื่องจากการดำเนินงานของ สสว. ต้องเผชิญกับเหตุการณ์ไม่แน่นอนและความเสี่ยงจากสภาพแวดล้อมที่เปลี่ยนแปลงตลอดเวลา ทั้งจากปัจจัยภายในและภายนอกจนอาจกลายเป็นสถานการณ์ความเสี่ยงที่ส่งผลกระทบต่อการบรรลุเป้าหมายตามภารกิจ จึงจำเป็นต้องจัดให้มีการบริหารความเสี่ยงทั่วทั้งองค์กร (ERM: Enterprise Risk Management) อย่างเป็นระบบเพื่อบูรณาการการจัดการ การตอบสนองและหรือการหลีกเลี่ยงจากความเสี่ยงที่เผชิญอยู่อย่างเหมาะสม (Optimal Risk Taking) และเพื่อช่วยสนับสนุนการตัดสินใจของผู้บริหารในการที่จะปกป้องผลประโยชน์ขององค์กรจากความเสี่ยงที่ค้นพบให้สามารถดำเนินงานได้สำเร็จตามความคาดหวัง (Expected Enterprise Value) ของผู้มีส่วนได้ส่วนเสีย และสร้างความยั่งยืนให้องค์กรต่อไป

สสว. ได้พัฒนากระบวนการบริหารความเสี่ยงอย่างต่อเนื่อง โดยนำขั้นตอนการดำเนินงานตามมาตรฐานสากลของ COSO (Committee of Sponsoring Organization of the Treadway Commission) โดยนำกรอบแนวคิดด้านการบริหารความเสี่ยงที่ COSO กำหนดทั้ง 2 เวอร์ชันมาประยุกต์ใช้ในระบบการบริหารความเสี่ยงของ สสว. เพื่อสร้างประสิทธิภาพการบริหารจัดการความเสี่ยงในภาพรวมให้ดียิ่งขึ้น เพื่อรักษาความสามารถ และสร้างความยั่งยืนให้กับองค์กร ประกอบด้วย

2.1 กรอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2017 (Enterprise Risk Management- Integrating with Strategy and Performance) มีพื้นฐานแนวคิดการบริหารความเสี่ยง คือ

- (1) การบริหารความเสี่ยงเป็นกระบวนการที่ต้องดำเนินการอย่างต่อเนื่อง
- (2) เป็นหน้าที่ของบุคลากรทุกคนทั้งฝ่ายบริหารและผู้ปฏิบัติงาน
- (3) มุ่งเน้นการระบุและประเมินความเสี่ยงในกระบวนการกำหนดกลยุทธ์
- (4) ระบุเหตุการณ์ที่สำคัญที่จะกระทบต่อเป้าหมายขององค์กรและจัดการให้อยู่ในระดับที่ยอมรับได้
- (5) ช่วยให้ฝ่ายบริหารมีข้อมูลประกอบการตัดสินใจที่ดีที่สุด เพื่อบรรลุวัตถุประสงค์องค์กรที่ตั้งไว้ได้



ภาพที่ 2 องค์ประกอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2017

และมีหลักการด้านการบริหารความเสี่ยง จำนวน 5 หัวข้อ และในแต่ละหัวข้อนั้น สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ได้กำหนดเป็นประเด็นแนะนำให้หน่วยงานที่เป็นรัฐวิสาหกิจหรือหน่วยงานอื่น นำไปประยุกต์ ใช้ในปี 2565 ตามความเหมาะสม ตามรายละเอียด ดังต่อไปนี้

หัวข้อที่ 1 ธรรมาภิบาลและวัฒนธรรมองค์กร ได้แก่

- 1.1 บทบาทคณะกรรมการในกำกับติดตามการบริหารความเสี่ยงและการพัฒนาระบบการควบคุมภายใน
- 1.2 โครงสร้างและบทบาทหน้าที่
- 1.3 บรรยากาศและวัฒนธรรมสนับสนุนการบริหารความเสี่ยง
- 1.4 ความมุ่งมั่นต่อค่านิยมองค์กร
- 1.5 แรงจูงใจ การพัฒนาและการรักษาบุคลากร

หัวข้อที่ 2 การกำหนดยุทธศาสตร์และวัตถุประสงค์ / เป้าประสงค์เชิงยุทธศาสตร์ ได้แก่

- 2.1 การวิเคราะห์ธุรกิจ ในหัวข้อการวางแผนเชิงกลยุทธ์
- 2.2 การระบุเป้าหมายการบริหารความเสี่ยง
- 2.3 การประเมินทางเลือกและกำหนดยุทธศาสตร์
- 2.4 การกำหนดวัตถุประสงค์ในการดำเนินธุรกิจเพื่อสร้างมูลค่าเพิ่มให้กับองค์กร

หัวข้อที่ 3 กระบวนการบริหารความเสี่ยง (Performance) ได้แก่

- 3.1 การระบุปัจจัยเสี่ยง
- 3.2 การกำหนดกิจกรรมการควบคุมที่ตอบสนองต่อความเสี่ยงองค์กร
- 3.3 การประเมินระดับความรุนแรงของปัจจัยเสี่ยง
- 3.4 การจัดลำดับความเสี่ยง
- 3.5 การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยงที่ระบุไว้
- 3.6 การบริหารความเสี่ยงแบบบูรณาการ Risk Correlation Map และ Portfolio View of Risk

หัวข้อที่ 4 การทบทวนการบริหารความเสี่ยง ได้แก่

- 4.1 การทบทวนและปรับปรุงผลการบริหารความเสี่ยง
- 4.2 การกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยง
- 4.3 การประเมินการเปลี่ยนแปลงที่มีนัยสำคัญ ในหัวข้อการวางแผนเชิงกลยุทธ์

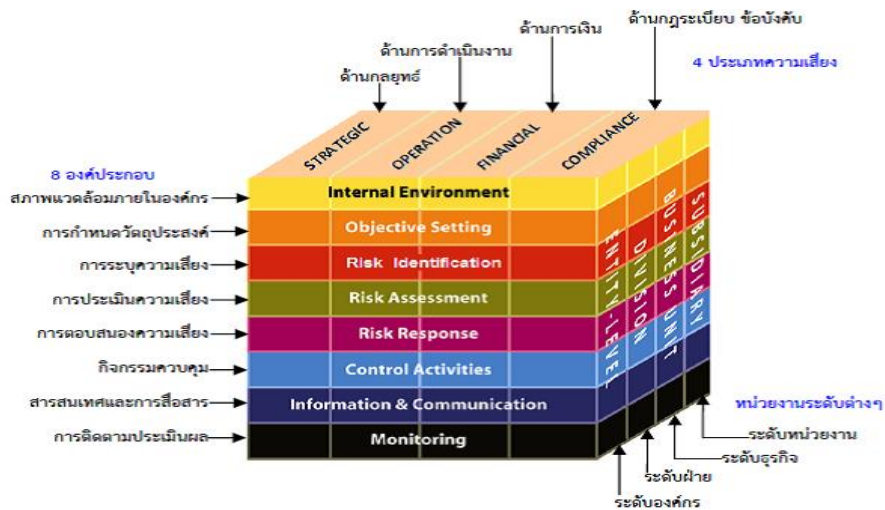
หัวข้อที่ 5 ข้อมูลสารสนเทศ การสื่อสาร และการรายงาน ได้แก่

- 5.1 ข้อมูลสารสนเทศ การสื่อสาร และการรายงานผล
- 5.2 การติดตามและรายงานผลการบริหารความเสี่ยง การควบคุมภายใน วัฒนธรรมและผลการดำเนินงาน
- 5.3 ข้อมูลและเทคโนโลยีในการสนับสนุนการบริหารความเสี่ยง
- 5.4 กระบวนการบริหารความต่อเนื่องทางธุรกิจ

2.2 กรอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2004 (Enterprise Risk Management)

มีพื้นฐานแนวคิดการบริหารความเสี่ยงแบ่งเป็น 3 ด้าน คือ

- ด้านที่ 1 องค์กรสามารถนำหลักเกณฑ์การบริหารความเสี่ยงไปใช้งานได้ตั้งแต่ระดับหน่วยงาน ระดับธุรกิจ ระดับฝ่ายงานและระดับองค์กร
- ด้านที่ 2 หน่วยงานสามารถนำองค์ประกอบทั้ง 8 ของกระบวนการบริหารความเสี่ยง ประยุกต์ใช้งานให้เหมาะสมกับสภาพองค์กร
- ด้านที่ 3 ความเสี่ยง 4 ประเภทที่อาจเกิดขึ้นในองค์กร คือ ด้านกลยุทธ์ (Strategic Risk) ด้านการดำเนินงาน (Operational Risk) ด้านการเงิน (Financial Risk) และด้านกฎ ระเบียบ ข้อบังคับ (Compliance Risk)



ภาพที่ 3 องค์ประกอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2004

2.3 กรอบหลักเกณฑ์การบริหารความเสี่ยงของทุนหมุนเวียน ประจำปีบัญชี 2566 ของกรมบัญชีกลาง โดย บริษัท ทริส คอร์ปอเรชั่น จำกัด เป็นที่ปรึกษา ได้ชี้แจงกรอบหลักเกณฑ์การประเมินดังกล่าว เมื่อวันที่ 20 กรกฎาคม 2565 โดยได้กำหนดเกณฑ์ประเมินผลฯ ด้านที่ 4 การบริหารจัดการทุนหมุนเวียน ในหัวข้อ 4.1 การบริหารความเสี่ยงและการควบคุมภายใน ที่มีแนวทางของตัวชี้วัดไว้สอดคล้องกับหลักการด้านการบริหาร ความเสี่ยง จำนวน 8 หัวข้อตามหลักเกณฑ์ COSO ERM 2004 ดังต่อไปนี้

องค์ประกอบที่ 1 Internal Environment หรือ สภาพแวดล้อมการควบคุมภายใน ซึ่งถือเป็น พื้นฐานขององค์ประกอบอื่น ๆ ทั้งหมด ที่ประกอบด้วยนโยบาย บทบาทหน้าที่ของฝ่ายบริหารหน่วยงานและ บุคลากรที่เกี่ยวข้องกับการบริหารความเสี่ยงและการควบคุมภายใน และมุ่งเน้นที่การมีระบบการจัดการเรื่อง ร้องเรียน

องค์ประกอบที่ 2 Objective Setting หรือ การกำหนดวัตถุประสงค์การบริหารความเสี่ยง ที่มุ่งเน้นการแสดงผ่านคู่มือการบริหารความเสี่ยงที่มีองค์ประกอบที่ตีกรอบถ้วน (ประกอบด้วย โครงสร้างการบริหารความเสี่ยงขององค์กร นโยบาย วัตถุประสงค์ของการบริหารความเสี่ยง การระบุความเสี่ยง การระบุถึงระดับความรุนแรงและการจัดลำดับความเสี่ยงจากผลการวิเคราะห์ความเสียหายข้างต้น การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยงที่ระบุไว้ โดยพิจารณาถึงผลกระทบและโอกาสที่จะเกิดค่าใช้จ่ายและผลประโยชน์ที่ได้ (Cost-Benefit) และระดับความเสี่ยงที่ยอมรับได้ของความเสี่ยงที่เหลืออยู่ (Residual Risk) ขององค์กร การทำรายงานการบริหารความเสี่ยงและการประเมินผลการบริหารความเสี่ยง โดยกำหนดให้มีการทบทวนคู่มือการบริหารความเสี่ยงทุกปีหรือกรณีที่มีการเปลี่ยนแปลงด้านการบริหารความเสี่ยง มีการสื่อสารให้ผู้บริหาร/พนักงานทุกระดับผ่านช่องทางที่หลากหลาย เนื้อหาที่เหมาะสมกับช่องทางการสื่อสารและช่องทางการสื่อสารที่มีประสิทธิภาพ ตลอดจนมีการตรวจสอบความรู้ความเข้าใจของพนักงานที่มีต่อคู่มือและการนำไปใช้ด้วย)

องค์ประกอบที่ 3 Event Identification หรือ การระบุความเสี่ยงระดับองค์กร โดยเน้นให้มีการกำหนดเกณฑ์การพิจารณาระบบการควบคุมภายในที่เพียงพอควบคู่ไปกับการระบุความเสี่ยงระดับองค์กร และการพิจารณาระดับความเสี่ยงที่คงเหลืออยู่ (Residual Risk) หลังจากการควบคุมภายใน (มุ่งเน้น ปัจจัยเสี่ยงระดับองค์กรต้องสะท้อนตัวชี้วัดที่สำคัญหรือยุทธศาสตร์ที่สำคัญของทุนหมุนเวียน หากไม่สะท้อนจะถูกปรับลดคะแนน 0.5000 คะแนน) และปัจจัยเสี่ยงระดับองค์กรมีความเชื่อมโยงกับเป้าหมายประจำปีของทุนหมุนเวียนในทุกยุทธศาสตร์ นอกจากนี้ ควรระบุความเสี่ยงให้ครบทั้ง 4 ประเภทที่อาจเกิดขึ้นในองค์กร ซึ่งประกอบด้วย ด้านกลยุทธ์ (Strategic Risk: S) ด้านการดำเนินงาน (Operational Risk) ด้านการเงิน (Financial Risk) และด้านกฎ ระเบียบ ข้อบังคับ (Compliance Risk)

องค์ประกอบที่ 4 Risk Assessment หรือ การประเมินระดับความรุนแรงของความเสี่ยงระดับองค์กร โดยการประเมินระดับความรุนแรงทั้งโอกาสและผลกระทบของปัจจัยเสี่ยงที่เกิดต่อความเสี่ยงระดับองค์กร รวมทั้งการนำฐานข้อมูลมาใช้ในการพิจารณากำหนดระดับความรุนแรง

องค์ประกอบที่ 5 Risk Response หรือ การตอบสนองความเสี่ยง การกำหนดแผนการบริหารความเสี่ยงระดับองค์กรครบทุกปัจจัยเสี่ยง โดยมีการวิเคราะห์ Cost – Benefit (มุ่งเน้นในแต่ละทางเลือกของแต่ละปัจจัยเสี่ยงในการจัดการ และมุ่งเน้นการวิเคราะห์การบริหารความเสี่ยงแบบบูรณาการเพื่อนำมาจัดทำแผนการบริหารความเสี่ยง โดยผ่านความเห็นชอบจากคณะกรรมการบริหารทุนหมุนเวียน)

องค์ประกอบที่ 6 Control Activities หรือ กิจกรรมการควบคุม แนวทางการปฏิบัติงานในการควบคุม ที่ฝ่ายบริหารกำหนดขึ้นเพื่อให้มั่นใจว่าแผนบริหารความเสี่ยงที่กำหนดขึ้นนั้น ได้มีการปฏิบัติตามแนวทางที่กำหนดอย่างมีประสิทธิภาพ มีการกำหนดผู้รับผิดชอบและระยะเวลาในการดำเนินงานไว้อย่างชัดเจน และมุ่งเน้นการสอบทานรายงานทางการเงินและมีใช้การเงินโดยผู้บริหารและผู้บริหารระดับรอง การจัดทำทะเบียนทรัพย์สินและการตรวจนับเพื่อเทียบกับทะเบียนทรัพย์สิน/หลักฐานทางบัญชี

องค์ประกอบที่ 7 Information and Communication หรือ สารสนเทศและการสื่อสาร เป็นการใช้ระบบสารสนเทศเพื่อสนับสนุนการติดตาม การดำเนินกิจกรรมตามแผนบริหารความเสี่ยง โดยพิจารณาผ่านการดำเนินงานตามแผนบริหารความเสี่ยงได้ครบถ้วนและความเสี่ยงระดับองค์กรสามารถลดระดับความรุนแรงได้ตามเป้าหมายที่กำหนด (มุ่งเน้นการลดระดับความรุนแรงลงได้ตามเป้าหมาย คิดเป็นร้อยละ 50 ของปัจจัยเสี่ยงทั้งหมด)

องค์ประกอบที่ 8 Monitoring หรือ การติดตามผลและประเมินผล มุ่งเน้นการประเมินผล การควบคุมภายในตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายใน สำหรับหน่วยงานของรัฐ พ.ศ. 2561 (มุ่งเน้นการส่งรายงานการประเมินผลการควบคุมภายในตามหลักเกณฑ์ กระทรวงการคลัง ได้ทันตามกำหนดเวลา คือ ภายใน 90 วัน นับตั้งแต่วันสิ้นปีบัญชี)

ทั้งนี้ สสว. ได้นำกรอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2017 การบริหารความเสี่ยง ตามหลักเกณฑ์ COSO ERM 2004 และกรอบหลักเกณฑ์การประเมินผลการดำเนินงานทุนหมุนเวียน ประจำปีบัญชี 2566 ของกรมบัญชีกลาง ช่างต้น มาประยุกต์ร่วมกันเป็นแนวทางในการจัดการระบบการบริหาร ความเสี่ยงขององค์กรต่อไป

บทที่ 3

กรอบการบริหารความเสี่ยงของ สสว.

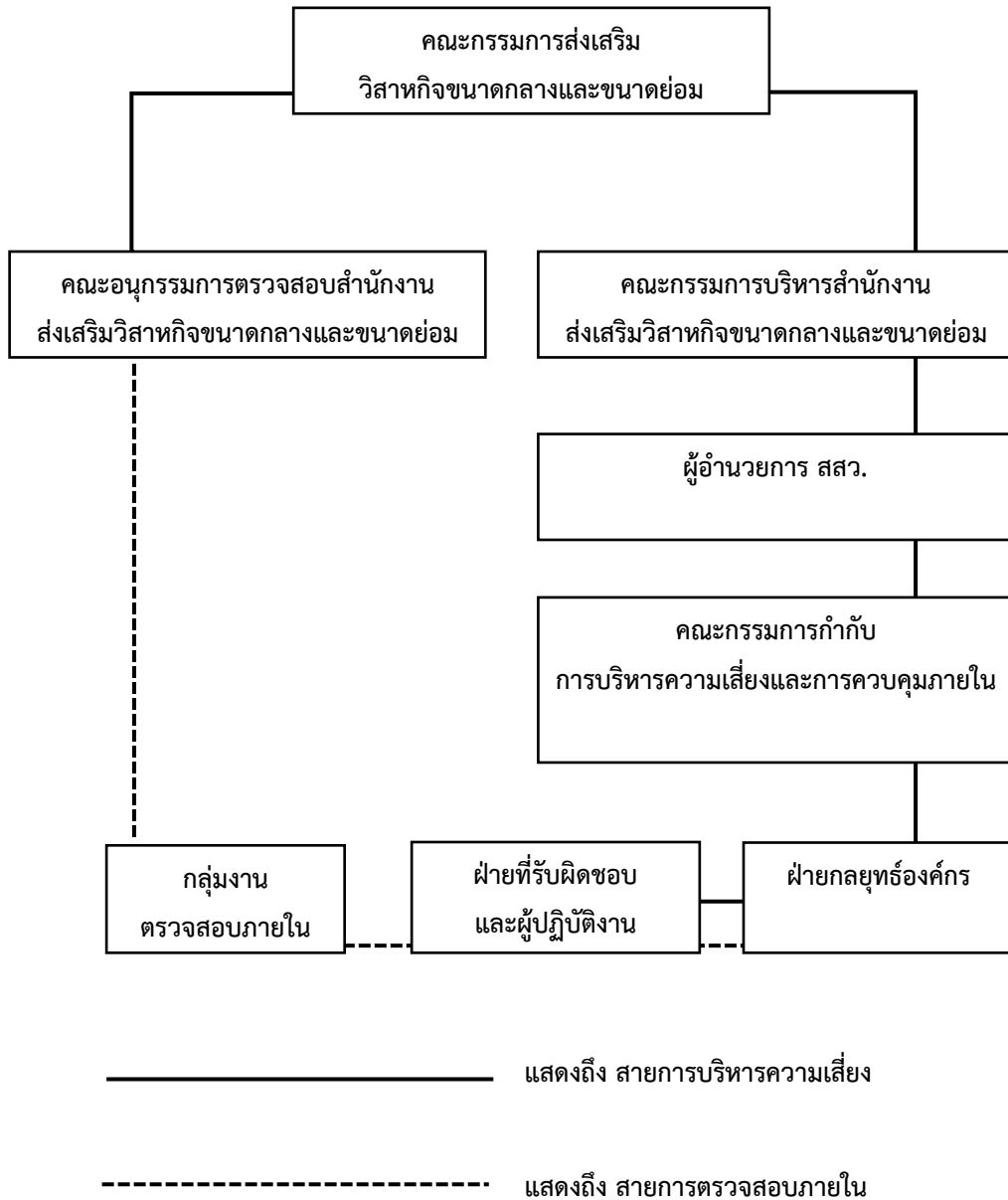
สสว. ได้กำหนดกรอบการบริหารความเสี่ยงขององค์กรขึ้น เพื่อมุ่งเน้นการมีส่วนร่วมของหน่วยงานที่เกี่ยวข้องให้นำไปสู่การปฏิบัติด้านการบริหารความเสี่ยงระดับองค์กรอย่างมีประสิทธิภาพตามเป้าหมายที่กำหนดไว้ โดยการดำเนินงานในแต่ละส่วนของกรอบการบริหารความเสี่ยงนั้น จะมุ่งเน้นการปรึกษาหารือสื่อสารผลการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่องในทุก ๆ ขั้นตอนงาน ตามกรอบการบริหารความเสี่ยง ดังต่อไปนี้



ภาพที่ 4 กรอบการบริหารความเสี่ยงของ สสว.

สำหรับรายละเอียดการดำเนินงานในแต่ละส่วนของกรอบการบริหารความเสี่ยง มีดังนี้

3.1 โครงสร้างการบริหารความเสี่ยงของ สสว.



ภาพที่ 5 โครงสร้างการบริหารความเสี่ยงของ สสว.

3.2 บทบาท/ความรับผิดชอบด้านการบริหารความเสี่ยง

สสว. ได้กำหนดบทบาท / ความรับผิดชอบของบุคลากรและหน่วยงานต่าง ๆ ด้านการบริหารความเสี่ยงและการควบคุมภายในตามโครงสร้างการบริหารความเสี่ยงของ สสว. ไว้ ดังนี้

1. คณะกรรมการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

กำกับดูแลดำเนินงานของคณะกรรมการบริหารสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

2. คณะกรรมการบริหารสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

- ส่งเสริมให้มีระบบการควบคุมภายในและการบริหารจัดการความเสี่ยงที่มีประสิทธิภาพ
- กำกับดูแลการควบคุมภายในตามหลักเกณฑ์ที่กระทรวงการคลังกำหนด
- กำกับดูแลการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- พิจารณาให้ความเห็นชอบแผนบริหารความเสี่ยงระดับองค์กร
- ติดตามผลและให้ข้อเสนอแนะการควบคุมภายในและการบริหารจัดการความเสี่ยง

3. คณะอนุกรรมการตรวจสอบสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

- ให้ข้อเสนอแนะและข้อสังเกตต่อผลการควบคุมภายในและการบริหารความเสี่ยงของ สสว.

4. ผู้อำนวยการสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

- สนับสนุนให้มีการบริหารความเสี่ยงและการควบคุมภายในอย่างมีประสิทธิภาพและมีความต่อเนื่องจนเป็นวัฒนธรรมองค์กรตามนโยบายการบริหารความเสี่ยง
- ติดตามการบริหารความเสี่ยงในปัจจุบันที่สำคัญ เพื่อให้มั่นใจว่ามีการตอบสนองต่อความเสี่ยงที่สำคัญอย่างเหมาะสมและควบคุมความเสี่ยงอยู่ในระดับที่ยอมรับได้
- บริหารจัดการให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในระบบการบริหารความเสี่ยงและมีการบูรณาการร่วมกับระบบงานอื่นอย่างเหมาะสม

5. คณะกรรมการกำกับการบริหารความเสี่ยงและการควบคุมภายใน

- อำนวยการในการจัดวางระบบและประเมินผลการควบคุมภายในของ สสว.
- กำหนดแนวทาง ประสานงานประเมินผลการควบคุมภายในกับหน่วยงานในสังกัด
- รวบรวม พิจารณาและสรุปผลการประเมินการควบคุมภายในในภาพรวมของ สสว.
- จัดทำรายงานการประเมินผลการควบคุมภายในของหน่วยงานของรัฐ
- ติดตามประเมินผลการบริหารจัดการความเสี่ยงระดับองค์กร
- จัดทำแผนการบริหารจัดการความเสี่ยงระดับองค์กร
- จัดทำรายงานผลการบริหารจัดการความเสี่ยงระดับองค์กร
- พิจารณาทบทวนปัจจัยเสี่ยงและผลการบริหารจัดการความเสี่ยงระดับองค์กร

6. ฝ่ายกลยุทธ์องค์กร

- ศึกษาและวิเคราะห์หลักเกณฑ์และประสานงานให้มีการประเมินผลการควบคุมภายในตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561
- ศึกษาและวิเคราะห์ปัจจัยความเสี่ยงที่มีผลกระทบต่อองค์กร และมีการสื่อสารให้ผู้อำนวยการ สสว. คณะกรรมการกำกับการบริหารความเสี่ยงและการควบคุมภายใน และคณะกรรมการบริหาร สสว. รับทราบอย่างสม่ำเสมอ เพื่อใช้เป็นข้อมูลในการจัดทำเป็นนโยบายและกรอบการบริหารความเสี่ยงที่เหมาะสม
- จัดทำร่างนโยบาย คู่มือและแผนบริหารความเสี่ยงระดับองค์กร
- ให้คำแนะนำและสนับสนุนในการบริหารจัดการความเสี่ยงของหน่วยงานต่าง ๆ
- ติดตาม วิเคราะห์ และจัดทำรายงานผลการบริหารความเสี่ยงเสนอต่อฝ่ายบริหารตามระยะเวลาที่กำหนด
- ส่งเสริมและสนับสนุนการให้ความรู้เรื่องการบริหารความเสี่ยงและการควบคุมภายในให้กับหน่วยงานต่าง ๆ
- เป็นเลขานุการของคณะกรรมการกำกับการบริหารความเสี่ยงและการควบคุมภายใน
- ศึกษา ติดตาม และพัฒนาองค์ความรู้ รวมทั้งวิเคราะห์ และพัฒนาเทคนิคใหม่ ๆ ในการบริหารความเสี่ยงและการควบคุมภายใน

7. ฝ่ายที่รับผิดชอบและผู้ปฏิบัติงาน

- จัดวางระบบการควบคุมภายในและประเมินผลการควบคุมภายในของฝ่าย โดยการระบุความเสี่ยง ประเมินความเพียงพอของการควบคุมที่มีอยู่ กำหนดแผนการป้องกันและควบคุมความเสี่ยงในแต่ละกระบวนการตามหน้าที่ความรับผิดชอบรวมถึงการควบคุมและติดตามการดำเนินงานเป็นไปตามแผนที่กำหนด
- สนับสนุนให้ผู้ปฏิบัติงานมีส่วนร่วมในกระบวนการบริหารความเสี่ยง ตั้งแต่การระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความรุนแรงของความเสี่ยง จัดทำและนำเสนอแผนบริหารความเสี่ยง การนำแผนไปปฏิบัติ การติดตามและรายงานผล
- ส่งเสริมให้พนักงานในฝ่ายตระหนักถึงความสำคัญของการบริหารความเสี่ยงและนำมาประยุกต์ใช้ให้เป็นส่วนหนึ่งของการปฏิบัติงานจนเป็นวัฒนธรรมองค์กร

8. กลุ่มงานตรวจสอบภายใน

- สอบทานการควบคุมภายในของหน่วยงาน เพื่อรายงานความเชื่อมั่นต่อการจัดวางระบบการควบคุมภายในและการประเมินผลการควบคุมภายในของ สสว.
- ประเมินผลการระบุความเสี่ยง การตอบสนองความเสี่ยง ผลการดำเนินงานตามแผนบริหารความเสี่ยง
- รายงานการสอบทานและประเมินผลระบบการควบคุมภายในและการบริหารจัดการความเสี่ยงของ สสว. ต่อคณะอนุกรรมการตรวจสอบสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

สภาพแวดล้อมภายในองค์กร

3.3 นโยบายการบริหารความเสี่ยง

- 1) ผู้บริหารระดับสูง ส่งเสริม สนับสนุน และผลักดันให้ สสว. มีระบบการบริหารจัดการที่ดี มีประสิทธิภาพเป็นระบบแบบแผน และมีการนำการบริหารความเสี่ยงมาใช้เป็นเครื่องมือในการดำเนินงานขององค์กร โดยมีองค์ประกอบหลักของการบริหารความเสี่ยงที่ดี สมบูรณ์ และครบถ้วน
- 2) จัดให้มีและส่งเสริมการบริหารความเสี่ยงทั่วทั้งองค์กรแบบบูรณาการ โดยมีการบริหารจัดการอย่างเป็นระบบและมีการดำเนินการต่อเนื่อง
- 3) มีการกำหนดกระบวนการบริหารความเสี่ยงที่เป็นระบบมาตรฐานเดียวกันทั้งองค์กร โดยจัดให้มีการอบรมหรือสร้างความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงให้แก่ผู้บริหารและพนักงานทุกระดับ
- 4) จัดตั้งคณะกรรมการกำกับการบริหารความเสี่ยงและการควบคุมภายในของ สสว. เพื่อพิจารณากำหนด ทบทวนนโยบายและแนวทางการบริหารความเสี่ยงของ สสว.
- 5) ให้มีการจัดตั้งหน่วยงานบริหารความเสี่ยงที่ทำหน้าที่กำกับ สนับสนุน และติดตามให้กระบวนการบริหารความเสี่ยงดำเนินไปอย่างมีประสิทธิภาพ
- 6) ให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานปกติ โดยผู้บริหารและพนักงานทุกระดับจะต้องตระหนักถึงการสร้างมูลค่าเพิ่มให้กับองค์กร งานบริการลูกค้า ประชาชน และภารกิจที่ได้รับมอบหมายจากภาครัฐ ตลอดจนให้ความสนใจระมัดระวังในเหตุการณ์หรือการกระทำที่จะส่งผลกระทบต่อให้เกิดความเสียหายหรือทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กร
- 7) สสว. จะมีการทบทวนนโยบายเมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อองค์กร และหรือเมื่อครบรอบระยะเวลาตามปีบัญชี

3.4 วัตถุประสงค์การบริหารความเสี่ยง

1) เพื่อบริหารจัดการให้ สสว. มีผลการดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้ โดยระบุปัจจัยเสี่ยงที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร เพื่อวิเคราะห์สาเหตุที่แท้จริงสำหรับบริหารจัดการระดับความรุนแรงของความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้ ควบคุมได้ และติดตามได้

2) เพื่อให้ บุคลากรของ สสว. นำแนวทางการบริหารความเสี่ยง มาใช้เป็นเครื่องมือช่วยในการบริหารและการดำเนินงานอย่างมีประสิทธิภาพ ประสิทธิผล และมีการบริหารจัดการที่เป็นไปตามหลักการกำกับดูแลกิจการที่ดี

3) เพื่อให้ สสว. ดำเนินการให้สอดคล้องกับพระราชบัญญัติการเงินการคลังของรัฐ พ.ศ. 2561 มาตรา 79 ให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

3.5 กลยุทธ์การบริหารความเสี่ยง

เมื่อนโยบายการบริหารความเสี่ยงได้ถูกกำหนดขึ้นแล้ว ผู้บริหารและผู้มีส่วนเกี่ยวข้องกับการบริหารความเสี่ยงได้ร่วมกันกำหนด และทบทวนแผนกลยุทธ์ เพื่อใช้เป็นแผนปฏิบัติการ (Action Plan) ในการบริหารความเสี่ยงในระดับองค์กร และระดับหน่วยงานต่างๆ โดยแผนกลยุทธ์ที่จัดทำขึ้นนั้นจะกำหนดรายละเอียดของวัตถุประสงค์ ขอบเขตงาน ผู้มีหน้าที่รับผิดชอบ งบประมาณ หรือทรัพยากรที่ต้องการ รวมถึงระยะเวลาของแผนที่ชัดเจน

3.6 วัฒนธรรมการบริหารความเสี่ยง

คณะกรรมการบริหาร สสว. และผู้บริหารระดับสูงเป็นผู้นำในการสร้างวัฒนธรรมองค์กร โดยสื่อสารเรื่องแนวคิดในการบริหารจัดการความเสี่ยงให้แก่เจ้าหน้าที่ที่เกี่ยวข้องในทุกๆระดับ เพื่อปลูกจิตสำนึก สร้างความรู้ ความเข้าใจ ตลอดจนให้เกิดการตระหนักถึงหน้าที่ความรับผิดชอบในเรื่องดังกล่าวว่าการบริหารจัดการความเสี่ยงนั้น มิใช่เป็นเพียงหน้าที่ของหน่วยงานบริหารความเสี่ยงหรือบุคคลหนึ่งบุคคลใดเท่านั้น แต่เป็นหน้าที่และความรับผิดชอบของทุกคนในองค์กร

นอกจากนี้ ควรกำหนดแนวทางปฏิบัติในการบริหารความเสี่ยง ซึ่งครอบคลุมถึงการกำหนดหลักเกณฑ์ในการระบุความเสี่ยง (Risk Identification) การประเมินความเสี่ยง (Risk Assessment) การจัดการความเสี่ยง (Risk Response) กิจกรรมการควบคุม (Control Activities) สารสนเทศและการติดต่อสื่อสาร (Information and Communication) การติดตามและการรายงานผล (Monitoring/Reporting) และกระตุ้นให้มีการนำไปถือปฏิบัติทั่วทั้งองค์กร (Wide Enterprise Risk Management) ต่อไป

3.7 นิยามศัพท์การบริหารความเสี่ยง

เพื่อให้ผู้บริหาร และพนักงานทุกระดับ มีความเข้าใจที่ตรงกันในเรื่องของความหมายและประเภทของความเสี่ยง ซึ่งขึ้นอยู่กับขอบเขตการดำเนินงาน ลักษณะ และสถานะแวดล้อมในการดำเนินงาน โดยครอบคลุมความเสี่ยงที่สำคัญที่อาจเกิดขึ้นและส่งผลกระทบต่อการทำงานของ สสว. และนำไปใช้ได้ อย่างมีประสิทธิภาพ จึงกำหนดให้มีคำศัพท์และคำจำกัดความเพื่อให้เกิดความเข้าใจในแบบเดียวกัน ดังนี้

ลำดับ	คำศัพท์	คำจำกัดความ
1	แหล่งที่มาของความเสี่ยง (Risk Universe)	การระบุปัจจัยเสี่ยงต้องระบุให้ครอบคลุมแหล่งที่มาทั้งปัจจัยภายใน ปัจจัยภายนอก วัตถุประสงค์เชิงยุทธศาสตร์และเป้าหมายที่สำคัญขององค์กร จุดอ่อน โอกาส (ตามที่ระบุใน SWOT) ความต้องการของผู้มีส่วนได้ส่วนเสีย ตัวชี้วัดที่สำคัญขององค์กร
2	ปัจจัยเสี่ยง (Risk Factor: RF)	<ul style="list-style-type: none"> - ความไม่แน่นอนที่หากเกิดขึ้นแล้ว จะกระทบเชิงลบต่อเป้าหมายขององค์กร (Risk) - ความไม่แน่นอนที่หากเกิดขึ้นแล้ว จะกระทบเชิงบวกต่อเป้าหมายขององค์กร (Opportunity) - ทั้งนี้ ปัจจัยเสี่ยงระดับองค์กรที่มีคุณภาพครบถ้วน อย่างน้อยต้องแสดงความเชื่อมโยงกับเป้าหมายตามยุทธศาสตร์และตัวชี้วัดตามบันทึกข้อตกลง ตัวชี้วัดที่สำคัญขององค์กรได้ทั้งหมด และสอดคล้องกับแหล่งที่มาของความเสี่ยง (Risk Universe) ที่องค์กรกำหนด (Connect Risks to Strategic Goals)
3	สาเหตุความเสี่ยง (Root cause: Rc)	<ul style="list-style-type: none"> - เหตุการณ์ใด ๆ ที่เป็นสาเหตุทำให้เกิดปัจจัยความเสี่ยง (Risk Factor) ทั้งนี้ ควรมีการระบุให้ครบทั้งสาเหตุหลักและสาเหตุรอง - การระบุสาเหตุที่แท้จริง (Root-Cause Analysis) และผลต่อเนื้อง (Outcome) ที่ชัดเจนให้เพียงพอที่จะสามารถกำหนดแผนจัดการความเสี่ยง (Mitigation)
4	กิจกรรมการควบคุมที่มีอยู่ (Existing Control)	กิจกรรม มาตรการ การดำเนินงานต่าง ๆ ที่มีอยู่ในปัจจุบันเพื่อควบคุมจัดการความเสี่ยง
5	ประสิทธิภาพของการควบคุมภายใน	ความเพียงพอของการควบคุมภายในที่มีการกำหนดหลักเกณฑ์หรือแนวทางในการพิจารณาความเพียงพอที่ชัดเจน (Links Risk to Control)
6	ความเสี่ยงก่อนการบริหารจัดการ (Inherent Risk : IR)	ความเสี่ยงก่อนการดำเนินกิจกรรมการควบคุม/จัดการความเสี่ยงนั้น

ลำดับ	คำศัพท์	คำจำกัดความ
7	ความเสี่ยงที่เหลืออยู่ (Residual Risk: RR)	<ul style="list-style-type: none"> - ปัจจัยเสี่ยงที่เหลืออยู่หลังจากพิจารณาประสิทธิภาพของการควบคุมภายในที่จะเปลี่ยนแปลงโอกาสที่จะเกิดหรือผลกระทบของความเสี่ยงนั้น - ปัจจัยเสี่ยงที่ผ่านการประเมินประสิทธิภาพความเพียงพอของกิจกรรมการควบคุมแล้ว สามารถจำแนกได้เป็น 3 กลุ่ม คือ <ol style="list-style-type: none"> 1. กลุ่มที่การควบคุมภายในที่มีอยู่มีประสิทธิภาพเพียงพอ 2. กลุ่มที่การควบคุมภายในที่มีอยู่มีประสิทธิภาพไม่เพียงพอ 3. กลุ่มที่ไม่มีกิจกรรมการควบคุม
8	เจ้าของความเสี่ยง (Risk Owner)	หน่วยงาน/ผู้รับผิดชอบต่อผลกระทบจากความเสี่ยงและหรือต่อการบริหารความเสี่ยง
9	ระดับความเสี่ยง (Level of Risk)	<ul style="list-style-type: none"> - การแบ่งความรุนแรงของความเสี่ยงออกเป็นระดับต่าง ๆ ด้วยผลลัพธ์การคูณ 2 มิติของ ค่าคะแนนโอกาสเกิด (Likelihood) และค่าคะแนนผลกระทบ (Impact) : Standardize Assessment Scale & Criteria - การจัดลำดับความเสี่ยงโดยการนำค่าระดับความเสี่ยงมาจัดเรียงตามลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยง และผลกระทบของความเสี่ยงที่ประเมินได้ โดยค่าระดับความเสี่ยงมีทั้งหมด 4 ระดับ ดังนี้ สูงมาก (สีแดง) สูง (สีส้ม) ปานกลาง (สีเหลือง) และ ต่ำ (สีเขียว) - ทั้งนี้ ควรใช้ข้อมูลเชิงปริมาณที่เชื่อมโยงกับฐานข้อมูลองค์กรผ่านระบบเทคโนโลยีดิจิทัล - ผลของการระบุค่าระดับความเสี่ยง ควรกำหนดให้แสดงผลได้ครบทั้ง 4 ค่าในทุกปัจจัยเสี่ยง ประกอบด้วย <ol style="list-style-type: none"> 1. ค่าระดับหลังประเมินกิจกรรมการควบคุม (Residual Risk: RR) 2. ค่าระดับเป้าหมายที่คาดหวัง (Target Risk: TR) 3. ค่าระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) 4. ค่าระดับหลังบริหารจัดการความเสี่ยง (Risk Mitigation: RM)
10	ผลกระทบ (Impact: I)	ความเสียหายหรือความรุนแรงที่จะเกิดขึ้นและส่งผลกระทบต่อเป้าหมายหรือวัตถุประสงค์ขององค์กรในมุมมองต่าง ในลักษณะของ Lagging Indicator เช่น จำนวนเงิน ระยะเวลา ชื่อเสียง ภาพลักษณ์หรือเป้าหมายขององค์กรในด้านต่าง ๆ
11	โอกาสเกิด (Likelihood: L)	ความเป็นไปได้ที่จะทำให้ปัจจัยเสี่ยงที่ระบุไว้เกิดขึ้น ซึ่งจะเป็โอกาสในลักษณะของ Leading Indicators เช่น ความถี่ หรือความก้าวหน้าของการดำเนินงาน หรือมุมมองอื่น ๆ ที่ทำให้เหตุการณ์ความเสี่ยงเกิดขึ้นได้
12	ตัวชี้วัดความเสี่ยง (Key Risk Indicator)	ปัจจัย ตัวแปรหรือผลลัพธ์จากเหตุการณ์ที่สามารถใช้เป็นสัญญาณเตือนภัยล่วงหน้า (Early Warning) หรือใช้ติดตาม (Monitor) หรือ ใช้บังคับ (Trigger) ถึงการเปลี่ยนแปลงของระดับความเสี่ยงที่เฝ้าระวังได้

ลำดับ	คำศัพท์	คำจำกัดความ
13	เป้าหมายความเสี่ยง (Risk Target: TR)	ค่าเป้าหมายของระดับความเสี่ยงที่คาดหวังจากผลการบริหารความเสี่ยง
14	ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA)	จำนวนของความเสี่ยงที่เป็นพื้นฐานกว้าง ๆ ซึ่งองค์กรเต็มใจยอมรับในการมุ่งไปสู่เป้าหมาย วัตถุประสงค์ พันธกิจหรือวิสัยทัศน์ขององค์กร
15	ช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance: RT)	ค่าหรือช่วงซึ่งแสดงถึงขอบเขตที่องค์กรจะยอมให้ผลลัพธ์จากการบริหารความเสี่ยงเบี่ยงเบนไปจาก Risk Appetite ที่กำหนดไว้
16	แผนภาพความเสี่ยง (Risk Profile)	แผนภาพแสดงปัจจัยเสี่ยงระดับองค์กรหรือระดับสายงาน ที่ได้มีการวิเคราะห์และประเมินระดับความรุนแรงผ่านแผนภาพ ที่สะท้อนการจัดลำดับความเสี่ยง และแสดงขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) มีการกำหนดระดับความเสี่ยง (สูง ปานกลาง ต่ำ) กับเป้าประสงค์และวัตถุประสงค์เชิงยุทธศาสตร์ขององค์กรและค่าความเสี่ยงที่ยอมรับได้ (Risk Appetite)
17	กลยุทธ์การจัดการความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง คือ วิธีการ / คัดเลือกแนวทางการเพื่อลดผลกระทบหรือลดโอกาสที่จะเกิด โดยกำหนดหลักเกณฑ์ในการประเมินค่าใช้จ่ายและผลประโยชน์ที่ได้ (Cost Benefit) ในการจัดการความเสี่ยงในแต่ละทางเลือกของความเสี่ยงที่เหลืออยู่ (Residual Risk) และสรุปเป็นแผนงาน ทั้งนี้ ทางเลือกที่จะประกอบการวิเคราะห์และตัดสินใจควรมีทางเลือกมากกว่า 1 ทางเลือกในการตัดสินใจเสมอ โดยทั่วไป คือ -Take: กลยุทธ์การยอมรับความเสี่ยง -Treat: กลยุทธ์การยอมรับความเสี่ยงการจัดการ -Transfer: กลยุทธ์การยอมรับความเสี่ยงการถ่ายโอน -Terminate: กลยุทธ์การยอมรับความเสี่ยงการหลีกเลี่ยง
18	ภาพรวมของความเสี่ยง (Portfolio View of Risk)	การวิเคราะห์ถึงช่วงเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ในแต่ละปัจจัยเสี่ยง กับช่วงเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ในระดับองค์กร และการจัดทำแบบจำลองที่เหมาะสม/นำแบบจำลองดังกล่าวไปใช้ในการบริหารความเสี่ยงในภาพรวม เพื่อสะท้อนถึงช่วงเบี่ยงเบนที่ยังอยู่ในวิสัยที่องค์กรสามารถจัดการได้
19	การให้ความเชื่อมั่นอย่างสมเหตุสมผล (Reasonable Assurance)	แนวคิดที่ว่า ไม่ว่าการบริหารความเสี่ยงขององค์กรจะได้รับการออกแบบมาดีหรือนำมาใช้ได้ดีเพียงใด ก็ไม่สามารถรับประกันการบรรลุวัตถุประสงค์ขององค์กรได้ทั้งหมด ทั้งนี้ เนื่องมาจากข้อจำกัดต่าง ๆ ที่มีอยู่ตามธรรมชาติของการบริหารความเสี่ยงขององค์กรนั่นเอง

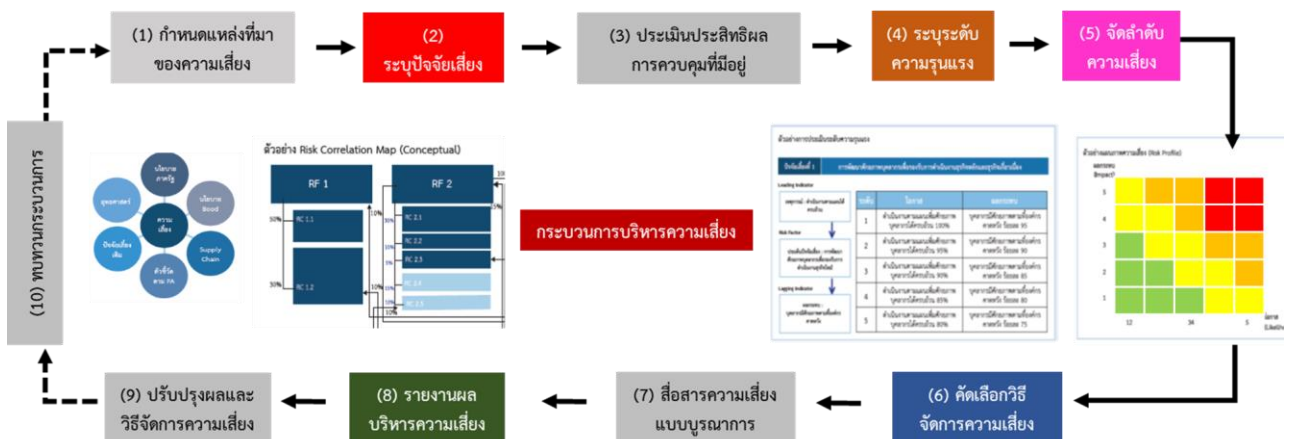
ลำดับ	คำศัพท์	คำจำกัดความ
20	แผนจัดการความเสี่ยง (Risk Mitigation Plan)	<p>- วิธีการ/แผนงานจัดการความเสี่ยงเพื่อลดผลกระทบหรือลดโอกาสที่จะเกิด โดยกำหนดหลักเกณฑ์ในการประเมินค่าใช้จ่ายและผลประโยชน์ที่ได้ (Cost Benefit) ในการจัดการความเสี่ยงในแต่ละทางเลือกของความเสี่ยงที่เหลืออยู่ (Residual Risk) และสรุปเป็นแผนงาน ทั้งนี้ ทางเลือกที่จะประกอบการวิเคราะห์และตัดสินใจควรมีทางเลือกมากกว่า 1 ทางเลือกในการตัดสินใจเสมอ</p> <p>- เงื่อนไข แผนจัดการความเสี่ยง ต้องแสดงให้เห็นว่า การดำเนินงานตามแผนงานดังกล่าวครบถ้วน จะสามารถลดระดับโอกาสเกิด หรือระดับความรุนแรงได้ กรณีที่ดำเนินงานตามกิจกรรมของแผนจัดการความเสี่ยงได้ครบถ้วน แต่ไม่สามารถลดระดับความรุนแรงได้นั้น ถือว่าการจัดทำแผนจัดการความเสี่ยงไม่มีคุณภาพ และถือว่าไม่สามารถจัดทำแผนการจัดการความเสี่ยงได้อย่างครบถ้วน</p> <p>- อนึ่ง แผนบริหารความเสี่ยงที่ดี ควรมีการระบุให้ครบถ้วนถึง</p> <ol style="list-style-type: none"> 1. เป้าประสงค์องค์กรที่อาจได้รับผลกระทบ 2. ประเภทความเสี่ยง ปัจจัยเสี่ยงและผลกระทบที่อาจเกิดขึ้น 3. สาเหตุความเสี่ยง โดยวิเคราะห์โอกาสเกิดและผลกระทบ ทั้งสาเหตุหลัก/สาเหตุรอง และค่าน้ำหนักของสาเหตุ 4. กิจกรรมการควบคุมภายในที่มีอยู่ (Existing Control) 5. ประเมินประสิทธิภาพการควบคุมที่มีอยู่ 6. แผนบริหารจัดการความเสี่ยงเพิ่มเติมจากมาตรการควบคุมที่มีอยู่ (Existing Control) จำแนกตามสาเหตุความเสี่ยง 7. การทบทวนกิจกรรมการควบคุมระหว่างปี ถือว่าเป็นส่วนหนึ่งของแผนบริหารจัดการความเสี่ยง 8. ควรใช้แผนผังการบริหารความเสี่ยงแบบบูรณาการ (Risk Correlation Map) มาประกอบการคัดเลือก/กำหนดวิธีจัดการความเสี่ยง
21	แผนผังความเสี่ยงหรือแผนผังการบริหารความเสี่ยงแบบบูรณาการ (Risk Correlation Map)	<p>- ภาพรวมความสัมพันธ์ของความเสี่ยงและผลกระทบที่มีระหว่างหน่วยงานต่าง ๆ ภายในองค์กร</p> <p>- องค์ประกอบของ Risk Correlation Map ควรครบถ้วนในประเด็น ดังนี้</p> <ol style="list-style-type: none"> 1) กำหนดสาเหตุของความเสี่ยงในทุกปัจจัยเสี่ยงและกำหนดระดับความรุนแรงของแต่ละสาเหตุในทุกปัจจัยเสี่ยง โดยพิจารณาพร้อมกับ Risk Owner 2) วิเคราะห์ความสัมพันธ์ระหว่างปัจจัยเสี่ยงในระดับองค์กรและความสัมพันธ์ของสาเหตุ โดยพิจารณาพร้อมกับ Risk Owner 3) วิเคราะห์ผลกระทบทั้งเชิงปริมาณและมีใช้เชิงปริมาณระหว่างปัจจัยเสี่ยงและสาเหตุ และระหว่างปัจจัยเสี่ยงต่อปัจจัยเสี่ยงระดับองค์กรด้วยกัน โดยพิจารณาพร้อมกับ Risk Owner

ลำดับ	คำศัพท์	คำจำกัดความ
		<p>4) นำ Risk Correlation Map ไปใช้ในการกำหนดแผนการบริหารความเสี่ยง โดยมีการบริหารถึงสาเหตุความเสี่ยงหลัก และปัจจัยเสี่ยงอื่นที่มีค่าระดับความรุนแรงสูงและส่งผลกระทบต่อปัจจัยเสี่ยงดังกล่าว รวมถึงมีการประเมินความสำเร็จของเป้าหมายในการบริหารความเสี่ยงของปัจจัยเสี่ยง ว่าเป็นผลมาจากการบริหารปัจจัยเสี่ยงที่เป็นสาเหตุหรือการบริหารความเสี่ยงที่มีผลกระทบสูง</p> <p>5) สร้างความเข้าใจในเรื่อง Risk Correlation Map ให้กับบุคลากรในองค์กรและ Risk Owners</p>
22	รายงานผลการบริหารความเสี่ยง	<p>กำหนดให้มีองค์ประกอบ ดังต่อไปนี้</p> <ol style="list-style-type: none"> 1) รายงานระดับความรุนแรง และ RA ของแต่ละปัจจัยเสี่ยงรายไตรมาส เทียบกับเป้าหมายที่คาดหวัง 2) รายงานความคืบหน้าการดำเนินงานตามมาตรการบริหารความเสี่ยงที่กำหนดและกิจกรรมในแผนบริหารความเสี่ยง (Mitigation Plan) และกิจกรรมการควบคุม (Existing Control) ที่กำหนดครบถ้วน รายงานผลได้ทุกไตรมาส 3) วิเคราะห์ถึงปัญหา/อุปสรรค และแนวทางที่จะบรรลุถึงเป้าหมาย <p>นอกจากนี้</p> <p>ควรพิจารณาให้มีความสอดคล้องกับความคืบหน้าของการติดตามผลตามแผนปฏิบัติการประจำปีที่เกี่ยวข้องและรายงานผลพร้อมการรายงานผลการดำเนินงานขององค์กร (Performance) และเชื่อมโยงกับระบบสารสนเทศและระบบดิจิทัลขององค์กรในการติดตามรายงานผลและมีระบบสนับสนุนกระบวนการ ERM และ EWS และต้องดูแลการจัดทำรายงานการประเมินผลการควบคุมภายในระดับหน่วยงานของรัฐ ประจำปีบัญชี เสนอหน่วยงานกำกับภายใน 90 วันด้วย</p>

ลำดับ	คำศัพท์	คำจำกัดความ
23	คู่มือการบริหารความเสี่ยงที่ดี	ประกอบด้วย <ol style="list-style-type: none"> 1) โครงสร้างการบริหารความเสี่ยงขององค์กร 2) นโยบาย วัตถุประสงค์ของการบริหารความเสี่ยง 3) การระบุความเสี่ยง 4) การระบุถึงระดับความรุนแรงและการจัดลำดับความเสี่ยงจากผลการวิเคราะห์ความเสียหาย 5) การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยงที่ระบุไว้ โดยพิจารณาถึงผลกระทบและโอกาสที่จะเกิด ค่าใช้จ่ายและผลประโยชน์ที่ได้ (Cost-Benefit) และระดับความเสี่ยงที่ยอมรับได้ของความเสี่ยงที่เหลืออยู่ (Residual Risk) ขององค์กร 6) การทำรายงานการบริหารความเสี่ยงและการประเมินผลการบริหารความเสี่ยง โดยกำหนดให้มีการทบทวนคู่มือการบริหารความเสี่ยงทุกปีหรือกรณีที่มีการเปลี่ยนแปลงด้านการบริหารความเสี่ยง ทั้งนี้ ต้องมีการสื่อสารให้ผู้บริหาร/พนักงานทุกระดับผ่านช่องทางที่หลากหลาย เนื้อหาที่เหมาะสมกับช่องทางการสื่อสารและช่องทางการสื่อสารที่มีประสิทธิภาพ ตลอดจนมีการตรวจสอบความรู้ความเข้าใจของพนักงานที่มีต่อคู่มือและการนำไปใช้ด้วย

กระบวนการบริหารความเสี่ยง

สสว. ได้นำกรอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2017 การบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2004 และกรอบหลักเกณฑ์การประเมินผลการดำเนินงานทุนหมุนเวียนประจำปีบัญชี 2566 ของกรมบัญชีกลาง ที่กำหนดเกณฑ์ตัวชี้วัดประเมินผลฯ ด้านที่ 4 การบริหารจัดการทุนหมุนเวียน ในหัวข้อ 4.1 การบริหารความเสี่ยงและการควบคุมภายใน มาประยุกต์ใช้ร่วมกัน ตามแผนผังกระบวนการบริหารความเสี่ยง ตามรายละเอียด ดังต่อไปนี้



ภาพที่ 6 แผนผังกระบวนการบริหารความเสี่ยงของ สสว.

3.8 กำหนดแหล่งที่มาของความเสี่ยง

การเริ่มต้นการบริหารความเสี่ยงนั้น ต้องเริ่มด้วยการกำหนดแหล่งที่มาของความเสี่ยง (Risk Universe) ให้ครอบคลุมทั้งปัจจัยภายใน ปัจจัยภายนอก วัตถุประสงค์เชิงยุทธศาสตร์และเป้าหมายที่สำคัญขององค์กร จุดอ่อน โอกาส (ตามที่ระบุใน SWOT) ความต้องการของผู้มีส่วนได้ส่วนเสีย ตัวชี้วัดที่สำคัญขององค์กร (Inherent Risk) จะช่วยให้สามารถระบุความเสี่ยงที่อาจเกิดผลกระทบต่อองค์กรได้อย่างครบถ้วน

3.9 ระบุปัจจัยเสี่ยง

ในขั้นตอนการระบุความเสี่ยง ต้องทบทวนวัตถุประสงค์ของการบริหารความเสี่ยง เพื่อระบุเป้าประสงค์ที่ชัดเจนขององค์กรในมุมมองต่าง ๆ หรือตามเป้าหมายกระบวนการงาน วัตถุประสงค์ที่ดีจะมีความชัดเจน วัดผลได้ ปฏิบัติได้ มีเหตุผล และมีกรอบระยะเวลาแน่นอน ซึ่งเป็นไปตามหลักการ “SMART” ได้แก่

Specific	- มีความเฉพาะเจาะจง ทุกคนเข้าใจตรงกัน
Measurable	- สามารถวัดได้ทั้งเชิงปริมาณหรือเชิงคุณภาพ
Attainable	- สามารถทำให้บรรลุผลได้
Relevant	- มีความสัมพันธ์กับนโยบายหลักในระดับสูง
Time constrained	- มีกำหนดเวลา/กรอบเวลาในการดำเนินงาน

โดยทั่วไปวัตถุประสงค์แบ่งออกได้เป็น 2 ระดับ คือ

วัตถุประสงค์ระดับองค์กร (Entity-Level Objectives) เป็นวัตถุประสงค์ของการดำเนินงานในภาพรวมขององค์กร โดยทั่วไปวัตถุประสงค์ในระดับองค์กรจะระบุไว้ในแผนกลยุทธ์และแผนปฏิบัติงานประจำปีขององค์กร

วัตถุประสงค์ในระดับกิจกรรม (Activity-Level Objectives) เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจงลงไปสำหรับแต่ละกิจกรรม/โครงการ ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การระบุความเสี่ยง ต้องระบุความเป็นไปได้ของเหตุการณ์ความเสี่ยงให้ครอบคลุมแหล่งที่มา (Risk Universe) ทั้งปัจจัยภายใน ปัจจัยภายนอก วัตถุประสงค์เชิงยุทธศาสตร์และเป้าหมายที่สำคัญขององค์กร จุดอ่อน โอกาส (ตามที่ระบุใน SWOT) ความต้องการของผู้มีส่วนได้ส่วนเสีย ตัวชี้วัดที่สำคัญขององค์กร (Inherent Risk)

ทั้งนี้ ปัจจัยเสี่ยงระดับองค์กรที่มีคุณภาพครบถ้วน อย่างน้อยต้องแสดงความเชื่อมโยงกับเป้าหมายตามยุทธศาสตร์และตัวชี้วัดตามบันทึกข้อตกลง ตัวชี้วัดที่สำคัญขององค์กรได้ทั้งหมด และสอดคล้องกับแหล่งที่มาของความเสี่ยง (Risk Universe) ที่องค์กรกำหนด

ปัจจัยเสี่ยง (Risk Factor: RF) คือ ความไม่แน่นอนที่หากเกิดขึ้นแล้ว มีผลกระทบเชิงลบต่อเป้าหมายขององค์กร จัดว่าเป็นความเสี่ยง (Risk) แต่ถ้าความไม่แน่นอนนั้น เมื่อเกิดขึ้นแล้วมีผลกระทบเชิงบวกต่อเป้าหมายขององค์กร จัดว่าเป็นโอกาส (Opportunity)

ประเภทความเสี่ยง ควรจัดแบ่งความเสี่ยง ออกเป็น 4 ประเภท คือ

ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: S) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบายเป้าหมาย กลยุทธ์ โครงสร้างองค์กร ทรัพยากร การปฏิบัติตามแผน และสภาพแวดล้อมอันส่งผลกระทบต่อองค์กร

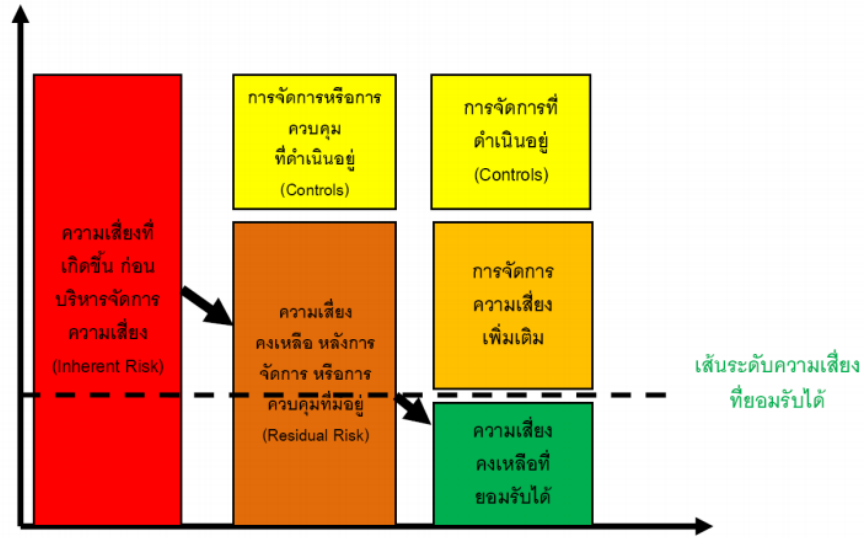
ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk: O) หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงานทุก ๆ ขั้นตอน โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ ระบบงาน ขั้นตอนการทำงาน อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากร ซึ่งจะส่งผลกระทบต่อประสิทธิภาพและประสิทธิผลในการดำเนินงาน

ความเสี่ยงด้านการเงิน (Financial Risk: F) หมายถึง ความเสี่ยงที่เกิดจากความไม่พร้อมในเรื่องงบประมาณ การเงิน เช่น ความผิดพลาดในการเบิกจ่าย สภาพคล่องทางการเงิน เป็นต้น ตลอดจนความเสี่ยงจากการขาดการจัดการข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงาน เพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้อง เหมาะสม ทำให้ขาดประสิทธิภาพ และไม่ทันต่อสถานการณ์ ซึ่งจะส่งผลกระทบต่อฐานะการเงินขององค์กร

ความเสี่ยงด้านการปฏิบัติตามกฎหมายหรือกฎระเบียบที่เกี่ยวข้อง (Compliance Risk: C) หมายถึง ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎหมาย กฎระเบียบ ที่เกี่ยวข้องได้ หรือกฎหมาย กฎระเบียบที่มีอยู่ไม่เหมาะสม ล้าสมัย เป็นอุปสรรคต่อการปฏิบัติงาน

3.10 ประเมินประสิทธิผลของการควบคุมที่มีอยู่

เพื่อประเมินถึงมาตรการควบคุมที่มีอยู่แล้วในปัจจุบันร่วมด้วย เนื่องจากมาตรการดังกล่าวอาจทำให้ระดับโอกาส และ/หรือระดับผลกระทบของความเสียหายลดลงได้ตามแนวคิดในแผนภาพที่แสดง



ภาพที่ 7 ความสัมพันธ์ของความเสี่ยงและกิจกรรมการควบคุม

หลักเกณฑ์การประเมินประสิทธิผลของการควบคุมภายในที่มีอยู่ นั้น สามารถประเมินได้ด้วยหลักเกณฑ์ต่าง ๆ เช่น ผลงานในอดีต กระบวนการ การรายงานและปรับปรุงผล เป็นต้น

การประเมินประสิทธิผลการควบคุมภายในที่มีอยู่ (เงื่อนไข กรณีเพียงพอ 1) ต้องมีคะแนนเกณฑ์ประเมินรวม ไม่ต่ำกว่าระดับ 6 คะแนน และ 2) ต้องไม่มีเกณฑ์ข้อใดต่ำกว่าระดับ 2 คะแนน			
ระดับคะแนน ประสิทธิภาพ	1 ผลงานในอดีต	2 กระบวนการ	3 การรายงานและ ปรับปรุงผล
3 มีประสิทธิภาพ	ดีกว่าเป้าหมาย	มีการสื่อสาร , มีแผนการทำงาน , ระบุความเสี่ยง , มีจุดควบคุม	นำข้อสังเกตไปปรับปรุงการควบคุม และมีผลการดำเนินงานดีขึ้น
2 เป็นระบบ	เท่ากับเป้าหมาย	มีขั้นตอนงาน , มีจุดควบคุม	รายงานผลและติดตามรายไตรมาส
1 เบื้องต้น	ต่ำกว่าเป้าหมาย	มีขั้นตอนงาน	มีการรายงานแต่ไม่ต่อเนื่องเป็นระบบ

ภาพที่ 8 ตารางหลักเกณฑ์การประเมินประสิทธิผลของการควบคุมภายในที่มีอยู่

การกำหนดกิจกรรมการควบคุมควรคำนึงถึง การกระทำได้เร็ว ใช้งบประมาณน้อย และมีประสิทธิภาพในการลด ควบคุม หรือป้องกันความเสี่ยงได้อย่างเห็นผล ทั้งนี้กิจกรรมที่กำหนดขึ้นต้องไม่ก่อให้เกิดความเสียหายอื่นตามมา หรือทำให้งานหยุดชะงัก และจะต้องพิจารณาความคุ้มค่ากับผลลัพธ์ที่จะเกิดขึ้นจากการดำเนินการนั้นด้วย

ประเภทกิจกรรมการควบคุมแบ่งเป็น 4 ลักษณะ ได้แก่

1) การควบคุมเชิงป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่เริ่มต้นดำเนินการ เช่น การแบ่งแยกหน้าที่ การควบคุมการเข้าถึงเอกสารข้อมูล เป็นต้น

2) การควบคุมเชิงค้นพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การสอบทาน การยืนยันยอด และการรายงานข้อบกพร่อง

3) การควบคุมเชิงแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีก เช่น การสำรองข้อมูลไว้ในที่ปลอดภัย การซ่อมหนีไฟ เป็นต้น

4) การควบคุมเชิงส่งเสริม (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การสร้างแรงจูงใจ เป็นต้น

3.11 ระบุระดับความรุนแรง

เมื่อระบุความเสี่ยงและประเมินประสิทธิผลของการควบคุมภายในที่มีอยู่แล้ว เจ้าของความเสี่ยง (Risk Owner) ต้องทำการประเมินความเสี่ยงที่คงเหลืออยู่ ด้วยการวิเคราะห์ระดับความรุนแรง/ค่าระดับความเสี่ยงของปัจจัยเสี่ยง ในแบบ 2 มิติ คือ

- 1) ค่าโอกาสเกิดความเสี่ยง (Likelihood: L)
- 2) ค่าผลกระทบจากความเสี่ยง (Impact: I)

การคำนวณค่าระดับความเสี่ยง คำนวณด้วยสูตร ดังต่อไปนี้

ค่าระดับความเสี่ยง =	ค่าคะแนนของโอกาส เกิดความเสียหาย	×	ค่าคะแนนจากผลกระทบ ของความเสี่ยง
----------------------	-------------------------------------	---	-------------------------------------

ภาพที่ 9 สูตรการคำนวณค่าระดับความเสี่ยง

ทั้งนี้ การประเมินค่าระดับความเสี่ยงจะใช้ประกอบการติดตามความก้าวหน้าของการบริหารจัดการความเสี่ยงของทุกรายการความเสี่ยง / ปัจจัยเสี่ยง จากหน่วยงานที่เกี่ยวข้องเป็นรายไตรมาส ซึ่งจะประกอบไปด้วยค่าระดับความเสี่ยง ดังนี้

1. ค่าระดับความเสี่ยงก่อนบริหารจัดการ (Inherent Risk : IR)
2. ค่าระดับความเสี่ยงคงเหลือภายหลังมีการควบคุม (Residual Risk : RR)
3. ค่าระดับความเสี่ยงเป้าหมาย (Target Risk : TR)
4. ค่าระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite : RA)
5. ค่าระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance : RT)
6. ค่าระดับความเสี่ยงหลังจัดการตามแผนความเสี่ยง (Risk Mitigation : RM)

ค่าระดับความเสี่ยงก่อนบริหารจัดการ (IR : Inherent Risk)			ค่าระดับความเสี่ยงคงเหลือ (RR : Residual Risk)					
โอกาส (L)	ผลกระทบ (I)	ผลคูณ L x I	โอกาส (L)	ผลกระทบ (I)	ผลคูณ L x I			
ค่าระดับความเสี่ยงเป้าหมายที่คาดหวัง (TR : Target Risk) / ค่าระดับความเสี่ยงที่ยอมรับได้ (RA : Risk Appetite)			ค่าระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (RT : Risk Tolerance)			ค่าระดับความเสี่ยงหลังการบริหาร (RM : Risk Mitigation)		
โอกาส (L)	ผลกระทบ (I)	ผลคูณ L x I	โอกาส (L)	ผลกระทบ (I)	ผลคูณ L x I	โอกาส (L)	ผลกระทบ (I)	ผลคูณ L x I

ภาพที่ 10 การติดตามความก้าวหน้าของการจัดการความเสี่ยงในแต่ละความเสี่ยง

ค่าโอกาสเกิดความเสี่ยง (Likelihood Scale: L)

คือ การประเมินความเป็นไปได้ในเชิงปริมาณหรือแนวโน้มของเหตุการณ์ความเสี่ยงที่อาจจะเกิดขึ้นภายในเวลาของแผนธุรกิจหรือตามฐานข้อมูลจริงที่มีอยู่ สำหรับเชิงคุณภาพอาจพิจารณาจากความคิดเห็นของผู้ที่เกี่ยวข้องเพื่อประเมินโอกาสที่อาจจะเกิดความเสียหายขึ้น โดยกำหนดค่าคะแนนและคำอธิบายระดับความน่าจะเป็น (Likelihood: L) เป็น 5 ระดับ (5 Points Scale) โดยกำหนดได้ ดังนี้

ระดับคะแนน ค่าโอกาสเกิด	โอกาสที่จะเกิด	ความถี่ที่จะเกิดเหตุการณ์ โดยเฉลี่ย
1 โอกาสเกิดขึ้นน้อยมาก	คาดว่าจะมีโอกาสดังเกิดขึ้นในอนาคตน้อยมาก (Probability < 1%) หรืออาจเกิดขึ้นใน สถานการณ์ที่ไม่ปกติ	5 ปีต่อครั้ง
2 โอกาสเกิดขึ้นน้อย	คาดว่าจะมีโอกาสดังเกิดขึ้นในอนาคตน้อย (Probability 1 - 2%)	2-3 ปีต่อครั้ง
3 โอกาสเกิดขึ้นปานกลาง	คาดว่าจะมีโอกาสดังเกิดขึ้นในอนาคตปานกลาง (Probability 2 - 3%)	1 ปีต่อครั้ง
4 โอกาสเกิดขึ้นสูง	คาดว่าจะมีโอกาสดังเกิดขึ้นในอนาคตค่อนข้างบ่อย (Probability 3 - 5%)	1 - 6 เดือนต่อครั้ง แต่ไม่เกิน 5 ครั้ง
5 โอกาสเกิดขึ้นสูงสุด	คาดว่าจะมีโอกาสดังเกิดขึ้นในอนาคตบ่อยมาก (Probability > 5%)	1 เดือนต่อครั้ง หรือมากกว่า

หมายเหตุ: การกำหนดระดับโอกาสที่จะเกิดความเสียหาย (Likelihood Scale) สามารถปรับได้ตามความเหมาะสมกับความเสี่ยงที่พบ

ภาพที่ 11 ตารางตัวอย่างการกำหนดค่าโอกาสเกิดความเสี่ยง

ค่าผลกระทบจากความเสียหาย (Impact Scale: I)

คือ การประเมินความเสียหายหรือความรุนแรงที่องค์กรได้รับเมื่อความเสี่ยงเกิดขึ้น โดยพิจารณาจากจำนวนมูลค่าของเงินที่สูญเสียหรือความล่าช้าของงาน สำหรับเชิงคุณภาพพิจารณาจากระดับความผิดตามกฎระเบียบ ข้อบังคับหรือระดับความสำคัญของงานว่า เป็นงานประจำวัน งานประจำเดือน งานสำคัญตามแผนวิสาหกิจ หรือระดับความสำคัญของบัญชี เป็นต้น โดยกำหนดค่าคะแนนและคำอธิบายระดับผลกระทบ (Impact: I) เป็น 5 ระดับ (5 Points Scale) โดยกำหนดได้ ดังนี้

ระดับคะแนน	ด้านการเงิน	ด้านการปฏิบัติงาน	ด้านชื่อเสียง/ภาพลักษณ์
1 เสียหายน้อยมาก	ค่าความเสียหายน้อยกว่า 10,000 บาท	เกิดความล่าช้าของโครงการ ไม่เกิน 1.5 เดือน	ไม่มีผลกระทบต่อชื่อเสียงและ ภาพลักษณ์ของ สสว. หรือมีผลกระทบน้อยมาก
2 เสียหายน้อย	ค่าความเสียหาย 10,000 – 50,000 บาท	เกิดความล่าช้าของโครงการ 1.5 - 3 เดือน	มีผลกระทบต่อชื่อเสียงและ ภาพลักษณ์ของ สสว. น้อย
3 เสียหายปานกลาง	ค่าความเสียหาย 50,000 – 250,000 บาท	เกิดความล่าช้าของโครงการ 3 - 4.5 เดือน	มีผลกระทบต่อชื่อเสียงและ ภาพลักษณ์ของ สสว. ปานกลาง
4 เสียหายสูง	ค่าความเสียหาย 250,000 - 10,000,000 บาท	เกิดความล่าช้าของโครงการ 4.5 - 6 เดือน	มีผลกระทบต่อชื่อเสียงและ ภาพลักษณ์ของ สสว. อย่างมีนัยสำคัญ
5 เสียหายสูงสุด	ค่าความเสียหายมากกว่า 10,000,000 บาท	เกิดความล่าช้าของโครงการ มากกว่า 6 เดือน	มีผลกระทบอย่างร้ายแรง ต่อชื่อเสียงและภาพลักษณ์ ของ สสว.

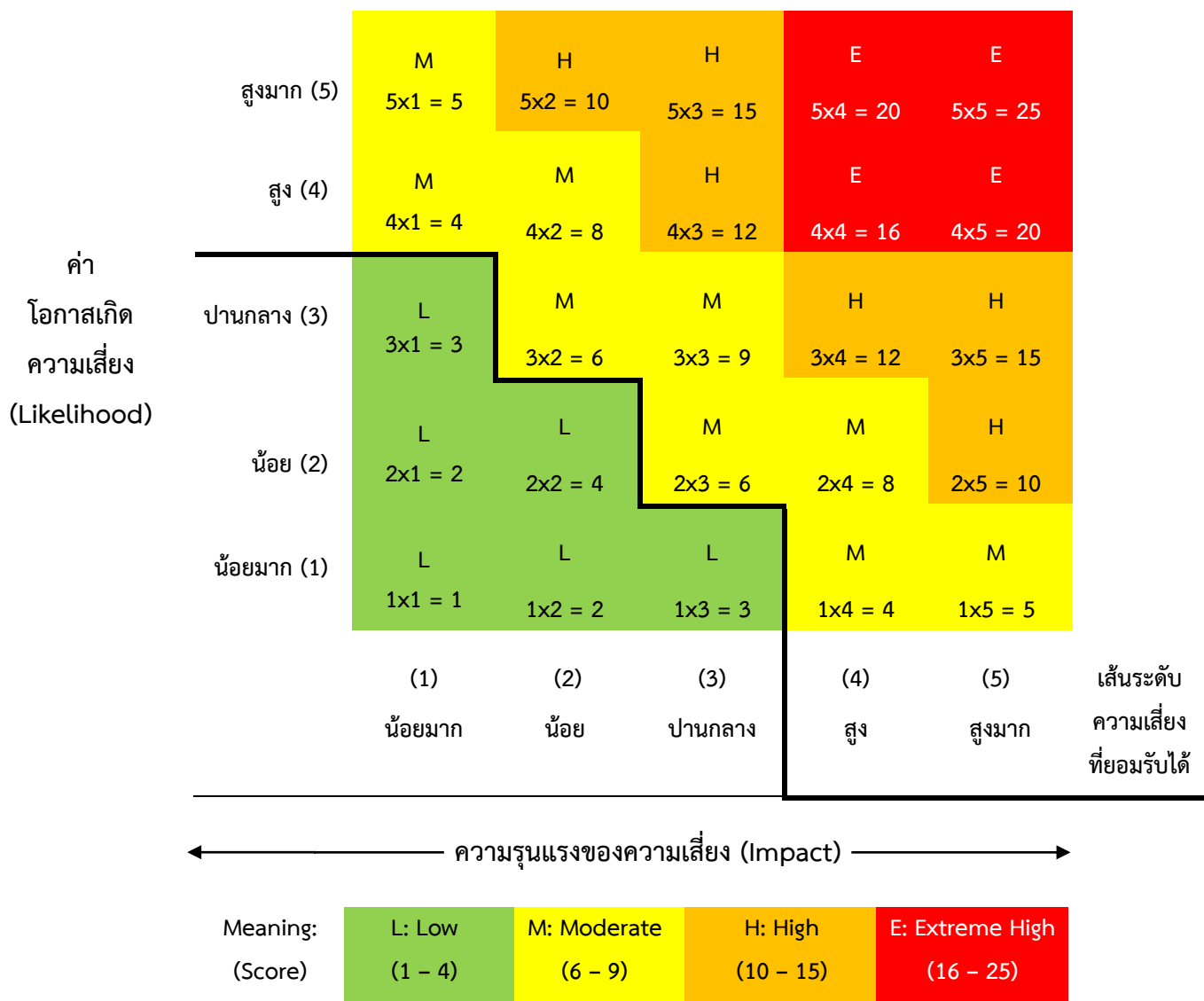
หมายเหตุ : การกำหนดค่าผลกระทบจากความเสียหาย (Impact Scale) สามารถปรับได้ตามความเหมาะสมกับลักษณะความเสี่ยงที่พบ

ภาพที่ 12 ตารางตัวอย่างการกำหนดค่าผลกระทบจากความเสียหาย

3.12 จัดลำดับความเสี่ยง

การจัดลำดับความเสี่ยงโดยการนำค่าระดับความเสี่ยงมาจัดเรียงตามลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยง และผลกระทบของความเสี่ยงที่ประเมินได้ โดยระดับความสำคัญของความเสี่ยงมีทั้งหมด 4 ระดับ เพื่อคัดเลือกความเสี่ยงที่มีความสำคัญสูง – สูงมาก ไปจัดลำดับความเร่งด่วน (Prioritize Risks) ในการจัดการความเสี่ยงและพิจารณากลยุทธ์การตอบสนองความเสี่ยงเพื่อจัดทำแผนบริหารความเสี่ยงต่อไป ตามตารางดังต่อไปนี้ โดยสามารถสรุปเป็นแผนภาพแสดงระดับความรุนแรงของความเสี่ยง (Risk Matrix) ได้ดังนี้

แผนภาพแสดงระดับความรุนแรงของความเสี่ยง (Risk Matrix)



ภาพที่ 13 ตารางจัดลำดับความรุนแรงของความเสี่ยง (Risk Matrix)

การแปลความค่าสี

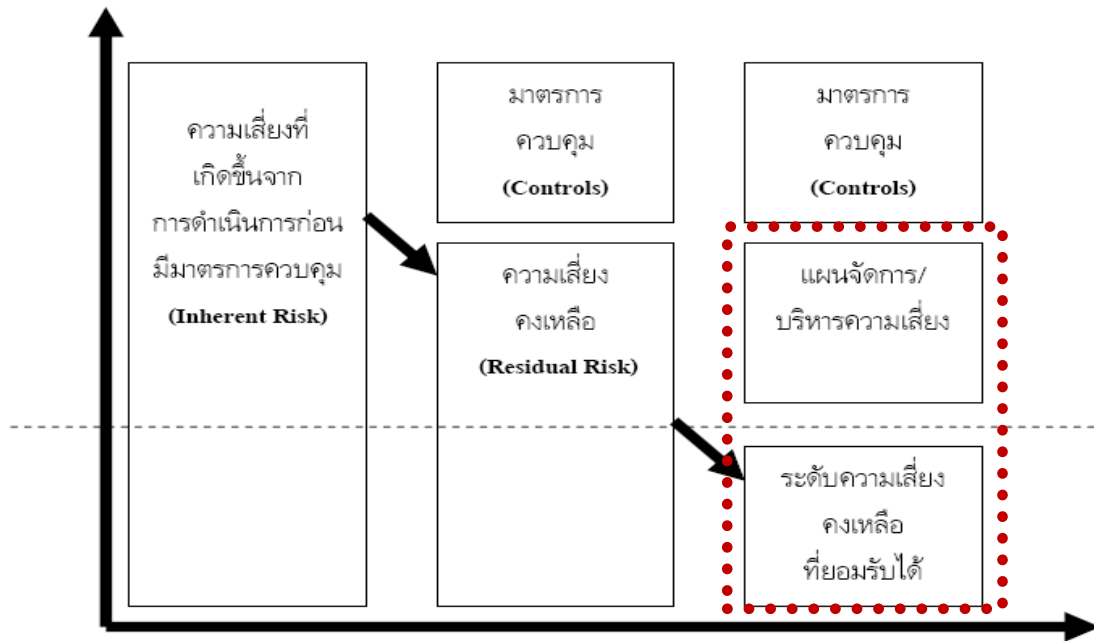
- ระดับความเสี่ยงสูงมาก ต้องกำหนดมาตรการติดตามอย่างใกล้ชิดและดำเนินงานตามแผนทันที
- ระดับความเสี่ยงสูง กำหนดมาตรการเฝ้าระวังและวางแผนบริหารความเสี่ยงเพิ่มเติม
- ระดับความเสี่ยงปานกลาง ระบุผู้รับผิดชอบและแจ้งเตือนหากระดับความเสี่ยงเปลี่ยนแปลง
- ระดับความเสี่ยงต่ำ อยู่ในระดับความเสี่ยงที่ยอมรับได้ อาจไม่จำเป็นต้องมีมาตรการใด ๆ

หมายเหตุ

- ค่าระดับความเสี่ยงของแต่ละปัจจัยเสี่ยงจะถูกนำมาใช้เพื่อจัดลำดับความสำคัญของความเสี่ยงในองค์กร และเป็นเกณฑ์ในการคัดเลือกความเสี่ยงมาจัดการตามลำดับความรุนแรงอย่างเหมาะสม โดยความเสี่ยงที่มีคะแนนค่าระดับสูง ควรถูกพิจารณาจัดการก่อนความเสี่ยงที่มีค่าระดับต่ำกว่า
- กรณีที่พบว่าปัจจัยเสี่ยงหลายปัจจัยเกิดขึ้นพร้อมกัน การใช้ตารางจัดระดับความเสี่ยงอาจช่วยให้รับผิดชอบความเสี่ยงพิจารณาเลือกความเสี่ยงที่จะต้องบริหารจัดการได้ง่ายขึ้น
- เป้าหมายของระดับความเสี่ยงในแต่ละรายการ กำหนดให้รายการความเสี่ยงที่อยู่สูงกว่า Risk Appetite Boundary จะต้องบริหารจัดการเพื่อลดระดับความเสี่ยงลงอยู่ในค่าเป้าหมาย (โอกาสการเกิดและผลกระทบ) ค่าใดค่าหนึ่ง ดังนี้ (1, 3) (2, 3) (3, 2) และ (4, 1) หรือในกรณีที่รายการความเสี่ยงใด ณ ตอนต้นปีอยู่ในระดับค่าเป้าหมายอยู่แล้ว จะต้องควบคุมระดับความเสี่ยง ณ สิ้นปี ไม่ให้เพิ่มสูงขึ้นไปจากค่าเป้าหมายที่เป็นอยู่
- ระดับความเสี่ยงสูงมาก อยู่สูงกว่าเส้น Risk Appetite Boundary องค์กรจะต้องกำหนดแผนการบริหารความเสี่ยงและมีการติดตามอย่างใกล้ชิดจากผู้บริหารระดับสูง
- ระดับความเสี่ยงสูง อยู่สูงกว่าเส้น Risk Appetite Boundary องค์กรควรจะต้องกำหนดแผนงานในการบริหารความเสี่ยง แต่ทั้งนี้ ในกรณีที่คณะกรรมการ / คณะอนุกรรมการบริหารความเสี่ยงที่เกี่ยวข้องพิจารณาแล้วเห็นว่าความเสี่ยงดังกล่าวมีแนวโน้มของระดับความเสี่ยงลดลง และสามารถจัดการควบคุมได้ ก็สามารถลดระดับจากความเสี่ยงระดับองค์กรเป็นการควบคุมภายในแทนได้
- ระดับความเสี่ยงปานกลาง อยู่ต่ำกว่าเส้น Risk Appetite Boundary สามารถจัดการในระดับควบคุมภายในได้ แต่ทั้งนี้ ในกรณีที่คณะกรรมการ / คณะอนุกรรมการบริหารความเสี่ยงที่เกี่ยวข้องพิจารณาแล้วเห็นว่าความเสี่ยงนั้นมีความสำคัญต่อการดำเนินงานขององค์กร และมีแนวโน้มของระดับความเสี่ยงสูงขึ้นก็อาจสามารถยกระดับให้เป็นการบริหารความเสี่ยงระดับองค์กรได้
- ระดับความเสี่ยงต่ำ อยู่ต่ำกว่าเส้น Risk Appetite Boundary สามารถบริหารจัดการในระดับควบคุมภายในได้

3.13 คัดเลือกวิธีจัดการความเสี่ยง

การจัดการความเสี่ยงเป็นขั้นตอนในการประเมินทางเลือกและกำหนดแนวทางการดำเนินการเพื่อลดระดับความรุนแรงของความเสี่ยง โดยนำผลจากการประเมินความเสี่ยงที่ได้จากขั้นตอนที่ 3 : การประเมินความเสี่ยง มาจัดทำแผนจัดการ/บริหารความเสี่ยงตามลำดับความสำคัญของความเสี่ยง โดยวิเคราะห์หาวิธีการจัดการกับความเสี่ยงวิธีการใดวิธีการหนึ่งหรือหลายวิธีรวมกัน เพื่อลดโอกาส (Likelihood) ที่จะเกิดความเสี่ยง และ/หรือลดระดับความรุนแรงของผลกระทบที่จะเกิดขึ้น (Impact) ให้อยู่ในระดับที่ยอมรับได้ (ดูแผนภาพประกอบ)



ภาพที่ 14 แสดงแนวคิดความคาดหวังของการจัดการความเสี่ยงในแต่ละความเสี่ยง

เกณฑ์หรือระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เป็นการกำหนดสถานการณ์ที่องค์กรยอมรับได้กับสถานการณ์ที่เกินกว่าระดับที่องค์กรยอมรับได้ เพื่อว่าบุคลากรทุกคนภายในองค์กรจะได้ออกมาช่วยกันควบคุมความเสี่ยงที่เกิดจริงมิให้เกินกว่าเกณฑ์ระดับที่ยอมรับได้

เกณฑ์ความสามารถในการยอมรับความเสี่ยง

ระดับความเสี่ยง	ความหมาย
สูงมาก	ระดับที่ไม่สามารถยอมรับได้ ต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
สูง	ระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ทันที
ปานกลาง	ระดับที่ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้เคลื่อนไปยังระดับที่ยอมรับไม่ได้
ต่ำ	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

ภาพที่ 15 ตารางแสดงเกณฑ์ความสามารถในการยอมรับความเสี่ยง

คัดเลือกความเสี่ยงที่สำคัญ

ให้ผู้ประเมินนำผลการประเมินความเสี่ยงที่ได้จากขั้นตอนที่ 3 (การประเมินความเสี่ยง) มาจัดลำดับตามระดับความสำคัญ (ระดับความเสี่ยง) และคัดเลือกกิจกรรมที่มีระดับความเสี่ยงสูงกว่าระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อนำไปพิจารณากำหนดวิธีการ/แนวทางในการจัดการความเสี่ยงที่เหมาะสมต่อไป

ทั้งนี้ สสว. กำหนดระดับความเสี่ยงที่ยอมรับได้ไว้ที่ระดับความเสี่ยงระดับต่ำ ดังนั้นผู้ประเมินจะคัดเลือกกิจกรรมที่มีระดับความเสี่ยงในระดับสูงมาก สูง และปานกลาง มาเพื่อพิจารณากำหนดวิธีการจัดการความเสี่ยง ส่วนกิจกรรมที่มีระดับความเสี่ยงในระดับต่ำ ซึ่งเป็นความเสี่ยงที่ยอมรับได้ แต่ควรต้องติดตามดูแลและทบทวนเป็นประจำอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าความเสี่ยงดังกล่าวยังคงอยู่ในระดับที่ยอมรับได้

ประเมินทางเลือกเพื่อกำหนดวิธีจัดการความเสี่ยง

เมื่อพิจารณาคัดเลือกความเสี่ยงที่มีความสำคัญในข้อ 1. เสร็จสิ้น ผู้ประเมินต้องประเมินทางเลือกเพื่อกำหนดวิธีการในการจัดการความเสี่ยงเหล่านั้น โดยทางเลือกในการจัดการ/บริหารความเสี่ยงโดยทั่วไปมี 4 ทางเลือก (SARA) ดังนี้

1. การแบ่งปัน (Sharing) คือ การแบ่งความรับผิดชอบให้ผู้อื่นร่วมรับความเสี่ยง เช่น การทำประกัน การใช้บริการภายนอก (Outsource) เป็นต้น
2. การหลีกเลี่ยง (Avoiding) คือ การดำเนินการหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง เช่น หลีกเลี่ยงหรือหยุดทำธุรกิจและสินค้าหรือบริการที่ไม่ถนัด การเปลี่ยนวัตถุประสงค์ เป็นต้น
3. การควบคุม (Reducing) คือ การลดหรือควบคุมความเสี่ยงโดยใช้กระบวนการควบคุมภายใน เพื่อลดโอกาสที่จะเกิดความเสี่ยงและลดผลกระทบที่เกิดจากความเสี่ยง เช่น การจัดทำแผนฉุกเฉิน การปรับปรุงแก้ไขกระบวนการดำเนินงาน การจัดอบรมเพิ่มทักษะให้กับพนักงาน การจัดทำคู่มือการปฏิบัติงาน เป็นต้น
4. การยอมรับ (Accepting) คือ การยอมรับความเสี่ยงนั้นในกรณีที่ยังคงมีระบบการควบคุมภายในที่มีประสิทธิภาพ มีระบบข้อมูลที่เพียงพอที่จะใช้ในการตัดสินใจ และมีความเข้าใจความเสี่ยงเป็นอย่างดี รวมทั้งประโยชน์ที่ได้รับจากการจัดการความเสี่ยงอาจน้อยกว่าต้นทุนที่ต้องเสียไป

ซึ่งในการพิจารณาทางเลือกและกำหนดวิธีการในการจัดการความเสี่ยง ผู้ประเมินควรต้องพิจารณาประเด็นต่าง ๆ ดังต่อไปนี้

วัตถุประสงค์ในการจัดการความเสี่ยง มีอยู่ 2 ประการ คือ

เพื่อลดโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง (Reduce Likelihood) วิธีการจัดการความเสี่ยงประเภทนี้มุ่งเน้นการลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย ซึ่งเหมาะกับความเสี่ยงที่เกิดจากปัจจัยภายในที่สามารถควบคุมได้ หรือลักษณะงานที่ต้องปฏิบัติบ่อยครั้งหรือปฏิบัติเป็นประจำ/ต่อเนื่อง เช่น การจัดให้มีแผนบำรุงรักษาอุปกรณ์คอมพิวเตอร์อย่างต่อเนื่อง เพื่อลดโอกาสในการเกิดปัญหาขัดข้อง หรือการปรับปรุงกระบวนการทำงาน เพื่อลดความซับซ้อนและข้อผิดพลาดที่อาจเกิดขึ้น หรือการกำหนดให้มี Checklist เพื่อตรวจสอบความถูกต้อง ครบถ้วนของการทำงานในแต่ละขั้นตอน เป็นต้น

เพื่อลดขนาดผลกระทบของความเสียหาย (Reduce Impact) วิธีการจัดการความเสี่ยงประเภทนี้มุ่งเน้นการลดขนาดผลกระทบของความเสียหายเมื่อความเสี่ยงเกิดขึ้นแล้ว ซึ่งเหมาะกับความเสี่ยงที่เกิดจากปัจจัยภายนอกที่ควบคุมได้ยาก โดยผู้ประเมินอาจจะใช้วิธีการกระจายความเสี่ยง เพื่อไม่ให้เกิดการกระจุกตัวของความเสี่ยง เช่น การจำกัดขนาดของธุรกรรม หรือปริมาณธุรกรรมโดยรวมไว้ในระดับต่ำ เป็นต้น แต่หากว่าความเสี่ยงอยู่นอกเหนือความสามารถที่จะควบคุม หรือไม่สามารถลดการกระจุกตัวได้ อาจจะเลือกการจัดการความเสี่ยงโดยการจัดทำแผนการดำเนินการเพื่อรองรับเมื่อเกิดเหตุการณ์ความเสียหาย และลดผลกระทบจากเหตุการณ์ดังกล่าว เช่น การจัดทำแผนฉุกเฉิน หรือการทำประกันภัย เพื่อให้บุคคลอื่นช่วยรับผลกระทบของความเสียหายที่จะเกิดขึ้น เป็นต้น

ต้นทุน (Costs) และผลประโยชน์ (Benefits)

ผู้ประเมินต้องพิจารณาความเป็นไปได้ในการจัดการ รวมทั้งต้องเปรียบเทียบค่าใช้จ่ายหรือต้นทุน (Costs) ที่คาดว่าจะเกิดขึ้นในการดำเนินการตามวิธีการจัดการ/บริหารความเสี่ยงแต่ละวิธี ทั้งที่เป็นจำนวนเงินและไม่เป็นจำนวนเงิน เช่น ต้นทุนด้านทรัพยากรบุคคล ด้านเวลา เป็นต้น กับผลประโยชน์ (Benefits) ที่คาดว่าจะได้รับจากการดำเนินการตามวิธีการดังกล่าวว่าคุ้มค่าหรือไม่ และวิธีการ/แนวทางใดให้ประสิทธิผลและประโยชน์สูงสุด



ตัวอย่าง การวิเคราะห์ Cost-Benefit

มาตรการจัดการความเสี่ยง		Cost		Benefit	
มาตรการ	ประเภท	เชิงปริมาณ	เชิงคุณภาพ	เชิงปริมาณ	เชิงคุณภาพ
พัฒนาระบบความปลอดภัยของระบบสารสนเทศ	แบ่งปัน - โอน (Sharing)	ไม่สามารถถ่ายโอนความเสี่ยงได้			
	ยอมรับ (Accepting)	ความเสียหายที่ข้อมูลสารสนเทศรั่วไหล ประมาณ xxx ลบ.	ชื่อเสียงของบริษัทที่อาจได้รับผลกระทบและสมาชิกขาดความเชื่อมั่นใน กบข.		
	การจัดการ - ควบคุม (Reducing)	ค่าพัฒนาระบบ xxx ลบ. (รวมต้นทุนค่าแรงงานแล้ว)	ระบบ xxx ป้องกันความปลอดภัยของระบบสารสนเทศ	ระดับความเชื่อมั่นในความปลอดภัยของระบบสารสนเทศเพิ่มขึ้น xx%	ยกระดับความปลอดภัยสารสนเทศของศูนย์คอมพิวเตอร์ ในส่วนของ Physical Control ให้มีความปลอดภัยมากขึ้น และผ่านการรับรองมาตรฐาน ISO 27001
	หลีกเลี่ยง (Avoiding)	ไม่สามารถยกเลิกกระบวนการนี้ได้ เพราะปัจจุบันองค์กรถูกจัดอันดับเป็นประเภท Critical Infra. ดังนั้นจึงจำเป็นต้องรับ Certificate ISO 27001			
สรุป	องค์กรเลือกการลดความเสี่ยง ด้วยการพัฒนาความปลอดภัยของระบบสารสนเทศ				

ภาพที่ 16 ตารางแสดงตัวอย่างวิเคราะห์ Cost - Benefit ของมาตรการจัดการความเสี่ยง

3.14 สื่อสารความเสี่ยงแบบบูรณาการ

หลังจากประเมินทางเลือกการจัดการความเสี่ยง จะคัดเลือกทางเลือกและกำหนดวิธีการจัดการที่เหมาะสมที่สุดสำหรับแต่ละความเสี่ยง ให้ใช้แผนผังการบริหารความเสี่ยงแบบบูรณาการ (Risk Correlation Map) มาประกอบการกำหนดวิธีการจัดการความเสี่ยง / จัดทำแผนบริหารความเสี่ยง โดยหารือร่วมกับหน่วยงานรับผิดชอบหลักของการบริหารความเสี่ยง (Risk Owner) เพื่อดำเนินการรวบรวมข้อมูลกิจกรรมการควบคุมที่มีหรือที่เกี่ยวข้อง เพื่อนำมาใช้ประกอบการจัดทำเป็นแผนบริหารความเสี่ยงของแต่ละความเสี่ยงและในภาพรวมองค์กรในเชิงบูรณาการ (Integration) ซึ่งจะมีการกำหนดวิธีการดำเนินการ ผู้รับผิดชอบและกำหนดเวลาดำเนินการ เพื่อประโยชน์ในการติดตามและประเมินผลการจัดการความเสี่ยงต่อไป ทั้งนี้ การจัดทำแผนบริหารความเสี่ยงขององค์กรให้นำเสนอแผนบริหารความเสี่ยงต่อคณะกรรมการบริหารของ สสว. เพื่อขอความเห็นชอบในการดำเนินการตามแผนบริหารความเสี่ยงต่อไป (ใช้แบบพิมพ์พร้อมคำอธิบายตามที่ปรากฏอยู่ในภาคผนวก)

เงื่อนไขของแผนจัดการความเสี่ยง ต้องแสดงให้เห็นว่า การดำเนินงานตามแผนงานดังกล่าวครบถ้วน จะสามารถลดระดับโอกาสเกิด หรือระดับความรุนแรงได้ กรณีที่ดำเนินงานตามกิจกรรมของแผนจัดการความเสี่ยงได้ครบถ้วน แต่ไม่สามารถลดระดับความรุนแรงได้นั้น ถือว่าการจัดทำแผนจัดการความเสี่ยงไม่มีคุณภาพ และถือว่าไม่สามารถจัดทำแผนการจัดการความเสี่ยงได้อย่างครบถ้วน

แผนบริหารความเสี่ยงที่ดี ควรมีการระบุให้ครบถ้วนถึง

1. เป้าประสงค์องค์กรที่ได้อาจได้รับผลกระทบ
2. ประเภทความเสี่ยง ปัจจัยเสี่ยงและผลกระทบที่อาจเกิดขึ้น
3. สาเหตุความเสี่ยง โดยวิเคราะห์โอกาสเกิดและผลกระทบ ทั้งสาเหตุหลัก/สาเหตุรอง และค่าน้ำหนักของสาเหตุ
4. กิจกรรมการควบคุมภายในที่มีอยู่ (Existing Control)
5. ประเมินประสิทธิผลการควบคุมที่มีอยู่
6. แผนบริหารจัดการความเสี่ยงเพิ่มเติมจากมาตรการควบคุมที่มีอยู่ (Existing Control) จำแนกตามสาเหตุความเสี่ยง
7. การทบทวนกิจกรรมการควบคุมระหว่างปี ถือว่าเป็นส่วนหนึ่งของแผนบริหารจัดการความเสี่ยง
8. ให้ใช้แผนผังการบริหารความเสี่ยงแบบบูรณาการ (Risk Correlation Map) มาประกอบการกำหนดวิธีจัดการความเสี่ยง / จัดทำแผนบริหารความเสี่ยง

3.15 รายงานผลบริหารความเสี่ยง

เมื่อจัดทำแผนบริหารความเสี่ยงขององค์กรแล้ว ให้แต่ละหน่วยงานผู้รับผิดชอบนำแผนบริหารความเสี่ยงดังกล่าวไปปฏิบัติตามวิธีการและระยะเวลาที่กำหนด พร้อมทั้งรายงานความก้าวหน้าและผลดำเนินงานเป็นระยะตามที่กำหนดให้มีองค์ประกอบ ดังนี้

1. รายงานระดับความรุนแรง และ RA ของแต่ละปัจจัยเสี่ยงรายไตรมาส เทียบกับเป้าหมายที่คาดหวัง
2. รายงานความคืบหน้าการดำเนินงานตามมาตรการบริหารความเสี่ยงที่กำหนดและ (กิจกรรมในแผนบริหารความเสี่ยง: Mitigation Plan) และกิจกรรมการควบคุม (Existing Control) ที่กำหนดให้ครบถ้วน
3. วิเคราะห์ถึงปัญหา/อุปสรรค และแนวทางที่จะบรรลุถึงเป้าหมาย

นอกจากนี้ควรพิจารณาให้มีความสอดคล้องกับความคืบหน้าของการติดตามผลตามแผนปฏิบัติการประจำปีที่เกี่ยวข้องและรายงานผลพร้อมการรายงานผลการดำเนินงานขององค์กร (Performance) และเชื่อมโยงกับระบบสารสนเทศและระบบดิจิทัลขององค์กรในการติดตามรายงานผลและมีระบบสนับสนุนกระบวนการบริหารความเสี่ยงและระบบการเตือนภัยล่วงหน้าด้วย (EWS ; Early Warning System) และดูแลการจัดทำรายงานการประเมินผลการควบคุมภายใน ระดับหน่วยงานของรัฐประจำปีบัญชี ที่ต้องนำเสนอหน่วยงานกำกับภายใน 90 วันด้วย

ปัจจัยสนับสนุนการบริหารความเสี่ยง

3.16 ระบบรายงานผลและปรับปรุงผลการบริหารความเสี่ยง

หลังจากจัดทำแผนบริหารความเสี่ยงของ สสว. และมีการดำเนินงานตามแผนแล้ว จะต้องมีการติดตามและรายงานผล เพื่อให้เกิดความมั่นใจว่า มาตรการหรือแนวทางการจัดการความเสี่ยง ได้มีการดำเนินการอย่างเหมาะสม ถูกต้อง เพียงพอ สามารถลดและควบคุมความเสี่ยงที่เกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้หรือต้องจัดหามาตรการหรือตัวควบคุมอื่นเพิ่มเติม เพื่อให้ความเสี่ยงที่ยังเหลืออยู่ หลังมีการจัดการ (Risk Management) อยู่ในระดับที่ยอมรับได้

โดยหน่วยงานผู้รับผิดชอบหลักของการบริหารความเสี่ยง รวบรวมและจัดทำรายงานผลการบริหารความเสี่ยงโดยใช้แบบรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงของ สสว. ประจำปี ซึ่งต้องระบุผลของการดำเนินการในแต่ละกิจกรรมตามที่ระบุในแผนบริหารความเสี่ยง ว่าสามารถจัดการ กับปัจจัยเสี่ยงต่าง ๆ ได้มากน้อยเพียงใด สามารถลดหรือควบคุมให้อยู่ในระดับที่ยอมรับได้หรือไม่ หรือจะต้องกำหนดแนวทางการแก้ไขเพิ่มเติมต่อไป และเพื่อจัดเก็บเป็นข้อมูลใช้ประกอบ แก้ไข พัฒนาและปรับปรุงกระบวนการบริหารความเสี่ยงในปีต่อ ๆ ไปให้มีประสิทธิภาพยิ่งขึ้นด้วย

3.17 สารสนเทศและการสื่อสารด้านบริหารความเสี่ยง

การสื่อสารถือได้ว่าเป็นหัวใจของการบริหารความเสี่ยงในทุก ๆ ขั้นตอน มีวัตถุประสงค์ เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง โดยมีการเปิดช่องทางการสื่อสาร ข้อมูลด้านการบริหารความเสี่ยงให้กับผู้บริหาร คณะทำงาน และบุคลากรของหน่วยงานได้เข้าถึง และรับทราบข้อมูลด้านการบริหารความเสี่ยงผ่านช่องทางต่าง ๆ เช่น ระบบอินทราเน็ต หนังสือเวียน การประชุมชี้แจงโดยผู้บริหาร หรือการฝึกอบรม เป็นต้น การบริหารความเสี่ยงที่ประสบความสำเร็จต้องอาศัยการติดต่อ สื่อสาร อย่างสม่ำเสมอและมีประสิทธิผล โดยวัตถุประสงค์หลักของการติดต่อสื่อสาร อย่างมีประสิทธิภาพนั้น เพื่อให้มั่นใจได้ว่าผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงที่ถูกต้องและทันเวลา สามารถจัดการกับความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลง ซึ่งการติดตาม แผนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อให้องค์กรมีโอกาสนในการบรรลุวัตถุประสงค์ได้มากที่สุด

นอกจากนี้ ควรมีการพิจารณาสนับสนุนระบบเทคโนโลยีสารสนเทศ เฉพาะด้าน เพื่อใช้ในการบริหารจัดการความเสี่ยงให้มีประสิทธิภาพมากยิ่งขึ้น ในด้านของ

ระบบสารสนเทศและการสื่อสารที่ใช้สนับสนุนการบริหารความเสี่ยง

ระบบการจัดเก็บและการใช้ฐานข้อมูลในอดีตเป็นข้อมูลประกอบการกำหนดค่าโอกาส และผลกระทบดัชนีตัวชี้วัดความสำเร็จ ค่าเป้าหมายในการบริหารความเสี่ยง ค่าระดับความเสี่ยงที่ยอมรับได้ ช่วงเบี่ยงเบนของค่าระดับความเสี่ยงที่ยอมรับได้ของทุกปัจจัยเสี่ยง

ระบบการติดตามและรายงานผลการบริหารความเสี่ยง โดยใช้ Application ที่เหมาะสมที่สามารถนำข้อมูลดิบมาจัดทำ / ประมวลผลข้อมูลให้อยู่ในแบบที่ต้องการ เชื่อถือได้และใช้ประกอบการตัดสินใจได้

ระบบการติดตามค่าดัชนีชี้วัดความเสี่ยงหลัก (Key Risk Indicator) ผ่านระบบเทคโนโลยีสารสนเทศขององค์กรในบางส่วนที่มีความสำคัญและมีความพร้อม

บทสรุป

ระบบการบริหารความเสี่ยงที่ดีและประสบความสำเร็จนั้น ขึ้นอยู่กับปัจจัยดังต่อไปนี้ คือ

ปัจจัยที่ 1: สร้างวัฒนธรรมให้การบริหารความเสี่ยงเป็นส่วนหนึ่งในงานที่ต้องตัดสินใจ

ปัจจัยที่ 2: ได้รับการสนับสนุนจากผู้บริหารระดับสูงอย่างต่อเนื่อง

ปัจจัยที่ 3: มีการสร้างความรู้ ความเข้าใจที่ตรงกันในเรื่องการบริหารความเสี่ยง

ปัจจัยที่ 4: ส่งเสริมให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างต่อเนื่อง

ปัจจัยที่ 5: ในการบริหารการเปลี่ยนแปลงที่เกิดขึ้นต้องมีการชี้แจงอย่างทั่วถึง

ปัจจัยที่ 6: มีการสื่อสารด้านการบริหารความเสี่ยงอย่างต่อเนื่องและมีประสิทธิภาพ

ปัจจัยที่ 7: มีการวัดผลการบริหารความเสี่ยงและนำไปปรับปรุงอย่างจริงจัง

ภาคผนวก

ตารางเปรียบเทียบองค์ประกอบของคู่มือการบริหารความเสี่ยงที่ดี
ตามเกณฑ์การประเมินผลการดำเนินงานทุนหมุนเวียน กรมบัญชีกลาง กระทรวงการคลัง
ตัวชี้วัดที่ 4.1 (2) การกำหนดวัตถุประสงค์ของการบริหารความเสี่ยง

ลำดับที่	องค์ประกอบของคู่มือการบริหารความเสี่ยง	สสว.	ตัวชี้วัดที่ TRIS กำหนด
1	บทนำองค์กร	✓	
2	วิสัยทัศน์ พันธกิจ และยุทธศาสตร์	✓	
3	กรอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2017	✓	
4	กรอบการบริหารความเสี่ยงตามหลักเกณฑ์ COSO ERM 2004	✓	
5	กรอบหลักเกณฑ์การบริหารความเสี่ยงของทุนหมุนเวียน ประจำปีบัญชี 2565	✓	
6	โครงสร้างการบริหารความเสี่ยงของ สสว.	✓	✓
7	บทบาทความรับผิดชอบด้านการบริหารความเสี่ยง	✓	
8	นโยบายการบริหารความเสี่ยง	✓	✓
9	วัตถุประสงค์การบริหารความเสี่ยง	✓	✓
10	กลยุทธ์การบริหารความเสี่ยง	✓	
11	วัฒนธรรมการบริหารความเสี่ยง	✓	
12	นิยามศัพท์การบริหารความเสี่ยง	✓	
13	แหล่งที่มาของความเสี่ยง	✓	
14	ระบุความเสี่ยง	✓	✓
15	ระบุระดับความรุนแรง	✓	✓
16	จัดลำดับความเสี่ยง	✓	
17	คัดเลือกวิธีจัดการความเสี่ยง	✓	✓
18	รายงานผลบริหารความเสี่ยง	✓	✓
19	ระบบติดตามและรายงานผล	✓	
20	สารสนเทศและการสื่อสารความเสี่ยง	✓	
21	การทบทวนคู่มือการบริหารความเสี่ยงทุกปี	✓	✓

ประวัติการปรับปรุงคู่มือการบริหารความเสี่ยงของ สสว.

ลำดับ ที่	รายการ	ฉบับเดิม ปี 2565	ฉบับปรับปรุง ปี 2566	รายการปรับปรุง ที่สำคัญ	รายละเอียด
องค์ประกอบของคู่มือการบริหารความเสี่ยงตามกรอบหลักเกณฑ์ TRIS					
1.	โครงสร้างการบริหารความเสี่ยง ขององค์กร	/	/		
2	นโยบาย วัตถุประสงค์ของการ บริหารความเสี่ยง	/	/	เพิ่มหัวข้อย่อย ลำดับที่ 7 ทบทวนนโยบายเมื่อมี เหตุการณ์ที่ส่งผลกระทบต่อองค์กร	เพื่อให้องค์กรสามารถ ปรับตัวตามสถานการณ์ที่ ส่งผลกระทบต่อเป้าหมาย
3	นิยามศัพท์	/	/	เพิ่มนิยามศัพท์ ความเสี่ยงก่อนการบริหารจัดการ (Inherent Risk : IR)	เพื่อให้สอดคล้องกับ ประเด็นการระบุความ รุนแรง
4	การระบุความเสี่ยง	/	/	ปรับปรุงหลักเกณฑ์การประเมิน ประสิทธิผลการควบคุมภายในที่มีอยู่	เพื่อให้หลักเกณฑ์สามารถ สะท้อนประสิทธิผลได้ดียิ่งขึ้น
5	การระบุถึงระดับความรุนแรงและ การจัดลำดับความเสี่ยงจากผลการ วิเคราะห์ความเสียหายข้างต้น	/	/	เพิ่มความเสี่ยงก่อนการบริหารจัดการ (Inherent Risk : IR) ในการประเมินระดับความรุนแรง	เพื่อให้สอดคล้องกับ เกณฑ์ประเมินผล และ นิยามศัพท์
6	การกำหนด/คัดเลือกวิธีการจัดการ ต่อความเสี่ยงที่ระบุไว้	/	/		
7	การทำรายงานการบริหารความ เสี่ยงและการประเมินผลการ บริหารความเสี่ยง	/	/	ปรับปรุงแบบพิมพ์ เพิ่มความเสี่ยงก่อนการบริหารจัดการ (Inherent Risk : IR)	เพื่อให้สอดคล้องกับ เกณฑ์ประเมินผล และ การระบุความรุนแรงฯ
เนื้อหาอื่น ๆ					
1	กรอบการบริหารความเสี่ยง สสว.	/	/		
2	หลักเกณฑ์ COSO 2017	/	/		
3	หลักเกณฑ์ COSO 2004	/	/		
4	การเปรียบเทียบกับคู่มือฯ ที่ดี	/	/		
5	ประวัติการปรับปรุงคู่มือการ บริหารความเสี่ยงของ สสว.	/	/		

ตัวอย่างแบบพิมพ์

การประเมินความเสี่ยงและจัดทำแผนบริหารความเสี่ยงระดับองค์กร

RF		การระบุและวิเคราะห์ความเสี่ยงระดับองค์กร ประจำปี..(1).....					แบบ บส.1				
1 แหล่งที่มาของความเสี่ยง (Risk Universe) (2)		4 ปัจจัยเสี่ยง (Risk Factor: RF) และ วงเล็บประเภทความเสี่ยง [S – O – F – C] (5)			6 ค่าระดับความเสี่ยงและค่าสีความเสี่ยง			7 แผนภาพสถานะความเสี่ยง			
2 เป้าหมายเชิงปริมาณ/คุณภาพ (KPI) (3)		5 ผลกระทบจากความเสี่ยง (Impact) ที่มีต่อเป้าหมาย (KPI ในข้อ 2) (6)			ให้ใช้ค่าโอกาสและค่าผลกระทบ ที่อ้างอิงไว้ในตาราง A			Risk Profile (13)			
3 เจ้าของความเสี่ยง (Risk Owner) (4)		5.1 สัญญาณเตือนก่อนเกิดความเสี่ยง (Trigger) (7)			6.1 Inherent Risk : IR (ค่าระดับความเสี่ยงก่อนบริหารจัดการ) (8)						
					6.2 Residual Risk : RR (ค่าความเสี่ยงคงเหลือภายหลังมีการควบคุม) (9)						
					6.3 Target Risk: TR / Risk Appetite : RA (ค่าความเสี่ยงเป้าหมายและที่ยอมรับได้) (10)						
					6.4 Risk Tolerance : RT (ค่าความเสี่ยงที่ยอมให้เบี่ยงเบนได้) (11)						
					6.5 Risk Management: RM (ค่าความเสี่ยงหลังจัดการตามแผนความเสี่ยง) (12)						
8 ระบุสาเหตุความเสี่ยง (Root causes: RC) และประเมินน้ำหนักของสาเหตุที่มีผลต่อปัจจัยเสี่ยง (14)		9 ระบุแผนงานโครงการ งานหรือการควบคุมที่มีอยู่ในปัจจุบัน (Existing Control) (15)		10 ประเมินความเพียงพอข้อ 9 (16) (ใช้หลักเกณฑ์การให้คะแนนตามตาราง B)				11 แผนบริหารความเสี่ยง			
				10.1 ผลงานในอดีต : เป้า (คะแนน 1 – 2 - 3) (17)	10.2 มีกระบวนการทำงานชัดเจน (คะแนน 1 – 2 - 3) (18)	10.3 มีการติดตามรายงานผล (คะแนน 1 – 2 - 3) (19)	10.4 ความเพียงพอ (20)	11.1 ทางเลือกจัดการความเสี่ยง (ใช้ผลตาราง C) (21)	11.2 มาตรการที่จะใช้จัดการความเสี่ยงหรือแผนฉุกเฉินเมื่อความเสี่ยงได้เกิดขึ้น (22)	11.3 เพื่อลดโอกาส (/) (23)	11.4 เพื่อลดผลกระทบ (/) (24)
8.1 สาเหตุหลัก (%)											
8.2 สาเหตุรอง (%)											

ตาราง A การวิเคราะห์ค่าระดับความเสี่ยง (L / I)
 เพื่อแสดงค่าโอกาสเกิดความเสี่ยง (Likelihood: L) และค่าผลกระทบ (Impact: I)

Leading Indicator (เนื่องจาก) (25) Risk Factor (ทำให้เกิดความเสี่ยง) (26) Lagging Indicator (ส่งผลให้) (27)	(28)		
	ระดับ	โอกาส (L) (29)	ผลกระทบ (I) (30)
	5		
	4		
	3		
	2		
	1		

ตาราง B การวิเคราะห์ความเพียงพอของกิจกรรมการควบคุมที่มีอยู่ในปัจจุบัน

การประเมินประสิทธิภาพการควบคุมภายในที่มีอยู่ (เงื่อนไข กรณีเพียงพอ 1) ต้องมีคะแนนเกณฑ์ประเมินรวม ไม่ต่ำกว่าระดับ 6 คะแนน และ 2) ต้องไม่มีเกณฑ์ข้อใดต่ำกว่าระดับ 2 คะแนน			
ระดับคะแนน ประสิทธิภาพ	1 ผลงานในอดีต	2 กระบวนการ	3 การรายงานและ ปรับปรุงผล
3	มีประสิทธิภาพ ดีกว่าเป้าหมาย	มีการสื่อสาร , มีแผน การทำงาน , ระบุ ความเสี่ยง , มีจุดควบคุม	นำข้อสังเกตไปปรับปรุง การควบคุม และ มีผลการดำเนินงานดีขึ้น
2	เป็นระบบ เท่ากับเป้าหมาย	มีขั้นตอนงาน , มีจุดควบคุม	รายงานผลและติดตาม รายไตรมาส
1	เบื้องต้น ต่ำกว่าเป้าหมาย	มีขั้นตอนงาน	มีการรายงานแต่ไม่ ต่อเนื่องเป็นระบบ

ตาราง C การวิเคราะห์ Cost & Benefit
 เพื่อระบุทางเลือกที่เหมาะสมในการบริหารจัดการความเสี่ยง

(31)					
สาเหตุ	วิธีการจัดการ ความเสี่ยง	Cost		Benefit	
		เชิงปริมาณ	เชิงคุณภาพ	เชิงปริมาณ	เชิงคุณภาพ
(32)	แบ่งปัน (Sharing)				
	ยอมรับ (Accepting)				
	ควบคุม (Reducing)				
	หลีกเลี่ยง (Avoiding)				
สรุป : ทางเลือกที่เหมาะสม คือ (33)					

RF		แผนบริหารความเสี่ยงและการรายงานผลการบริหารความเสี่ยง ปี 2566 ณ				แบบ บส.2		
1 แหล่งที่มาของความเสี่ยง / Owner:		4 ปัจจัยเสี่ยง (Risk Factor: RF)		6 ค่าระดับความเสี่ยงและค่าสีความเสี่ยง			7 แผนภาพสถานะความเสี่ยง	
				ให้ใช้ค่าโอกาสและค่าผลกระทบ ที่อ้างอิงไว้ในตาราง A	ค่าระดับ (X= L x I)	ค่าสี	Risk Profile 	
2 เป้าหมายเชิงปริมาณ/คุณภาพ (KPI)		5 ผลกระทบจากความเสี่ยง (Impact)		6.1 Inherent Risk : IR (ค่าระดับความเสี่ยงก่อนบริหารจัดการ)				
				6.2 Residual Risk : RR (ค่าความเสี่ยงคงเหลือหลังมีการควบคุม)				
				6.3 Target Risk: TR / Risk Appetite : RA (ค่าความเสี่ยงเป้าหมายและที่ยอมรับได้)				
3 ผลงานที่ทำได้		5.1 สัญญาณเตือนก่อนเกิดความเสี่ยง (Trigger)		6.4 Risk Tolerance : RT (ค่าความเสี่ยงที่ยอมรับได้)				
				6.4 Risk Management: RM (ค่าความเสี่ยงหลังจัดการตามแผนความเสี่ยง)				
8 ระบุสาเหตุความเสี่ยง (Root causes: RC)		9 งานหรือ การควบคุม ที่มีอยู่ใน ปัจจุบัน (Existing Control)		11 แผนบริหารความเสี่ยงและผลการดำเนินงาน				
		10 ผลการดำเนินงานตามข้อ 9 และปัญหาอุปสรรค (ถ้ามี) (34)		11.1 มาตรการ ฯ หรือแผนฉุกเฉิน ที่จะใช้จัดการเมื่อความเสี่ยงเกิดขึ้น (แสดงช่วงเวลาตามแผน ←→) (35)		11.2 ระยะเวลาดำเนินการ Q 1 (36) Q 2 (37) Q 3 (38) Q 4 (39)		11.3 ผลการดำเนินงาน (แสดงช่วงเวลาทำจริง ←---→) (40)
8.1 สาเหตุหลัก (%)								
8.2 สาเหตุรอง (%)								

คำอธิบาย

การระบุและวิเคราะห์ความเสี่ยงระดับองค์กร (แบบ บส.1)

- (1) ระบุปีที่ทำการประเมินความเสี่ยง
- (2) แหล่งที่มาของความเสี่ยงที่ สสว. กำหนด
- (3) เป้าหมายเชิงปริมาณ/คุณภาพ (KPI)
- (4) ใส่ชื่อหน่วยงานที่รับผิดชอบแผนบริหารความเสี่ยงนี้ (Risk Owner)
- (5) ชื่อปัจจัยเสี่ยงที่ระบุขึ้นไว้ และ ประเภทความเสี่ยงระดับองค์กร คือ S – O – F – C
- (6) ผลกระทบจากความเสี่ยง (Impact) ที่มีต่อเป้าหมาย
- (7) ใส่สัญญาณเตือนก่อนเกิดความเสี่ยง (Trigger)
- (8) ค่าระดับความเสี่ยงก่อนบริหารจัดการ (IR)
- (9) ค่าระดับความเสี่ยงคงเหลือภายหลังมีการควบคุม (RR)
- (10) ค่าระดับความเสี่ยงเป้าหมายและที่ยอมรับได้ (TR) / (RA)
- (11) ค่าระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (RT)
- (12) ค่าระดับความเสี่ยงหลังจัดการตามแผนความเสี่ยง (RM)
(8) – (12) กำหนดให้มีวิธีการคำนวณแบบเดียวกัน คือ ค่าระดับความเสี่ยง (L x I) คือ การนำค่า L (1-2-3-4-5) และการนำค่า I (1-2-3-4-5) ที่ได้จากการประเมินในตาราง A มาทำการคูณกันและใส่ผลลัพธ์ไว้หลังเครื่องหมาย (=) ด้วย หลังจากนั้น ให้ทำการใส่สี ซึ่งวิเคราะห์ด้วยผลคูณที่ได้กับตาราง Risk Profile (13)
- (14) ระบุสาเหตุของความเสี่ยงที่ทำการวิเคราะห์ไว้ พร้อมทั้งใส่น้ำหนักของสาเหตุความเสี่ยงที่มีต่อปัจจัยเสี่ยง
- (15) ระบุการควบคุมภายในที่มีไว้แล้ว สำหรับควบคุมสาเหตุความเสี่ยง
- (16) ประเมินประสิทธิภาพการควบคุมภายในที่มีอยู่ตามเกณฑ์การให้คะแนนตาราง B
- (17) ผลงานในอดีต ให้ระบุค่าตัวเลข 1-2-3 ซึ่งนำมาจากการประเมินในตาราง B
- (18) กระบวนการทำงาน ให้ระบุค่าตัวเลข 1-2-3 ซึ่งนำมาจากการประเมินในตาราง B
- (19) รายงานผล ให้ระบุค่าตัวเลข 1-2-3 ซึ่งนำมาจากการประเมินในตาราง B
- (20) ความเพียงพอ ให้ใส่เครื่องหมาย ✓ หรือ X โดยเป็นการวิเคราะห์ตามเงื่อนไขที่ระบุอยู่ในตาราง B
- (21) ทางเลือกจัดการความเสี่ยง ให้ระบุทางเลือกในการจัดการความเสี่ยงแบบใดแบบหนึ่ง โดยวิเคราะห์ทางเลือกในการจัดการในตาราง C
- (22) ระบุมาตรการในการจัดการความเสี่ยง และระบุเครื่องหมาย ✓ ว่ามาตรการที่ระบุสามารถลดโอกาส (23) หรือลดผลกระทบ (24) ของปัจจัยเสี่ยง
- (25) ให้ระบุสาเหตุของความเสี่ยง Leading Indicator (เนื่องจาก)
- (26) ให้ระบุ Risk Factor (ทำให้เกิดความเสี่ยง)
- (27) ให้ระบุผลกระทบจากความเสี่ยง Lagging Indicator (ส่งผลให้)

- (28) ใ้ชื่อปัจจัยเสี่ยง (29) ระบุนิยามของโอกาสเกิดความเสี่ยง และ (30) ระบุนิยามของผลกระทบจากความเสี่ง
- (31) ใ้ชื่อปัจจัยเสี่ยง และนำสาเหตุของปัจจัยเสี่ยงมาใ้ในช่อง (32) เพื่อวิเคราะห์ทางเลือกในการจัดการ (การแบ่งปัน – การยอมรับ – การควบคุม – การหลีกเลี่ยง) โดยในแต่ละทางเลือกจะต้องทำการวิเคราะห์ต้นทุนและผลประโยชน์ที่ได้รับ เป็นเชิงปริมาณและเชิงคุณภาพ หลังจากวิเคราะห์ทางเลือกในการจัดการความเสี่ยง ใ้แนวทางเลือกที่เหมาะสมมาใ้ในช่อง (33)

แผนบริหารความเสี่ยงและการรายงานผลการบริหารความเสี่ยง (แบบ บส.2)

การกรอกข้อมูลในแบบ บส.2 สามารถอ้างอิงตามแบบ บส.1 และมีเพิ่มเติมในส่วนของการรายงานผลการดำเนินงาน

- (34) รายงานผลการดำเนินงานของการควบคุมภายในที่มีอยู่ พร้อมปัญหาอุปสรรค (ถ้ามี)
- (35) ใ้กิจกรรมการดำเนินงานของมาตรการหรือแผนฉุกเฉินที่จะใ้จัดการความเสี่ยง โดยแสดงระยะเวลาดำเนินการในช่อง Q1 (36) , Q2 (37) , Q3 (38) และ Q4 (39)
- (40) รายงานผลการดำเนินงานของมาตรการหรือแผนฉุกเฉินที่จะใ้จัดการความเสี่ยง

