

คู่มือ

การบริหารความเสี่ยงและควบคุมภายใน ประจำปี 2565



ส่วนบริหารความเสี่ยงและพัฒนาระบบองค์กร
สำนักบริหาร
องค์การสวนพฤกษศาสตร์

สารบัญ

	หน้า
1. ส่วนที่ 1 หลักการและเกณฑ์การประเมินผลด้านการบริหารความเสี่ยงและควบคุมภายใน	1
1.1 เกณฑ์การประเมินผล (Enablers)	2
1.2 นโยบายการบริหารความเสี่ยงและควบคุมภายใน	4
1.3 การบูรณาการการกำกับดูแลที่ดี การบริหารความเสี่ยงและการปฏิบัติตามกฎหมาย กฎระเบียบ (Governance Risk Management & Compliance : GRC)	5
2. ส่วนที่ 2 ด้านการบริหารความเสี่ยง (Risk Management : RM)	6
2.1 ความหมายของการบริหารความเสี่ยง	7
2.2 ความสำคัญและประโยชน์ของการบริหารความเสี่ยง	7
2.3 แนวทางการบริหารจัดการความเสี่ยงของ อ.ส.พ.	7
2.4 บทบาทและความรับผิดชอบหลักของผู้เกี่ยวข้องโดยตรงกับการบริหารความเสี่ยง	8
2.5 แหล่งที่มาของการเกิดความเสี่ยง	9
2.6 ประเภทความเสี่ยง	9
2.7 การบริหารความเสี่ยง อ.ส.พ.	10
2.8 องค์ประกอบการบริหารความเสี่ยง	11
2.9 กระบวนการบริหารความเสี่ยง	13
2.10 แผนที่ความเสี่ยง (Risk Map)	26
2.11 การบริหารความต่อเนื่องทางธุรกิจ	27
2.12 การเตรียมความพร้อมของหน่วยงานต่อสภาวะวิกฤต	29
2.13 ปัจจัยสำคัญการบริหารความเสี่ยงให้ประสบความสำเร็จ	30
3. ส่วนที่ 3 ด้านการควบคุมภายใน (Internal Control : IC)	31
3.1 ความหมายของการควบคุมภายใน	32
3.2 ความสำคัญและประโยชน์ของการควบคุมภายใน	32
3.3 แนวคิดของการควบคุมภายใน	33
3.4 มาตรฐานการควบคุมภายใน	34
3.5 การจัดวางระบบควบคุมภายใน	35
3.6 การประเมินประสิทธิผลของการควบคุมภายใน	36
3.7 การสรุปประเมินการควบคุมภายในด้วยตนเอง (CSA)	38
3.8 แนวทางปฏิบัติเกี่ยวกับการควบคุมภายในของ อ.ส.พ.	38
3.9 คณะกรรมการและคณะทำงานเกี่ยวกับการควบคุมภายในของ อ.ส.พ.	40
3.10 แผนการดำเนินการเกี่ยวกับการควบคุมภายในประจำปี	41
3.11 ข้อจำกัดของการควบคุมภายใน	42

ส่วนที่ **1**



หลักการและเกณฑ์การประเมินผล
ด้านการบริหารความเสี่ยงและควบคุมภายใน

ส่วนที่ 1 :

หลักการและเกณฑ์การประเมินผลด้านการบริหารความเสี่ยงและควบคุมภายใน

1.1 เกณฑ์การประเมินผล (Enablers)

กระทรวงการคลังโดยสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ ได้กำหนดหลักเกณฑ์การประเมินผลการดำเนินงานของรัฐวิสาหกิจใหม่ (ระบบ SE-AM) โดยเริ่มใช้กับรัฐวิสาหกิจในปี 2563 โดยมีหลักเกณฑ์ที่เกี่ยวข้องกับการบริหารความเสี่ยงและควบคุมภายใน ที่ต้องนำมาปรับปรุงแนวทางการบริหารความเสี่ยงขององค์กรฯ ที่เกี่ยวข้องมีดังนี้

1) เกณฑ์ด้านการบริหารความเสี่ยงและการควบคุมภายใน (RM&IC)

1.1) การทบทวนและปรับปรุงผลการบริหารความเสี่ยง (Reviews Risk Performance) อย่างสม่ำเสมอตามสภาพแวดล้อมที่เปลี่ยนแปลงไป โอกาสที่เกิดขึ้น หรือในกรณีที่ผลการบริหารความเสี่ยงไม่เป็นไปตามเป้าหมายที่กำหนด การกำหนดเป้าหมายการบริหารความเสี่ยง ค่าเป้าหมาย พร้อมทั้งรายงานผลการดำเนินงานเพื่อให้สามารถวิเคราะห์ประเด็นความเสี่ยงที่อาจเกิดขึ้นใหม่ รวมทั้งการประเมินประสิทธิผลของการทบทวนและปรับปรุงผลการบริหารความเสี่ยงและนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

1.2) การกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยง (Pursues Improvement in Enterprise Risk Management) การกำหนดขั้นตอนในการปรับปรุงกระบวนการบริหารความเสี่ยงขององค์กร ทั้งในเชิงกระบวนการบริหารความเสี่ยง และการสร้างวัฒนธรรม ความตระหนักในองค์กร ทั้งศักยภาพบุคลากรในด้าน การบริหารความเสี่ยง มีการประเมินประสิทธิผลของการกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยงและนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการ

2) เกณฑ์ด้านการกำกับดูแลกิจการที่ดี (CG) รัฐวิสาหกิจติดตามผลการดำเนินงานด้านการบริหารความเสี่ยงและควบคุมภายในตามแนวทางที่กำหนดครบถ้วนสมบูรณ์ โดยมีความถี่อย่างน้อยเป็นรายไตรมาส

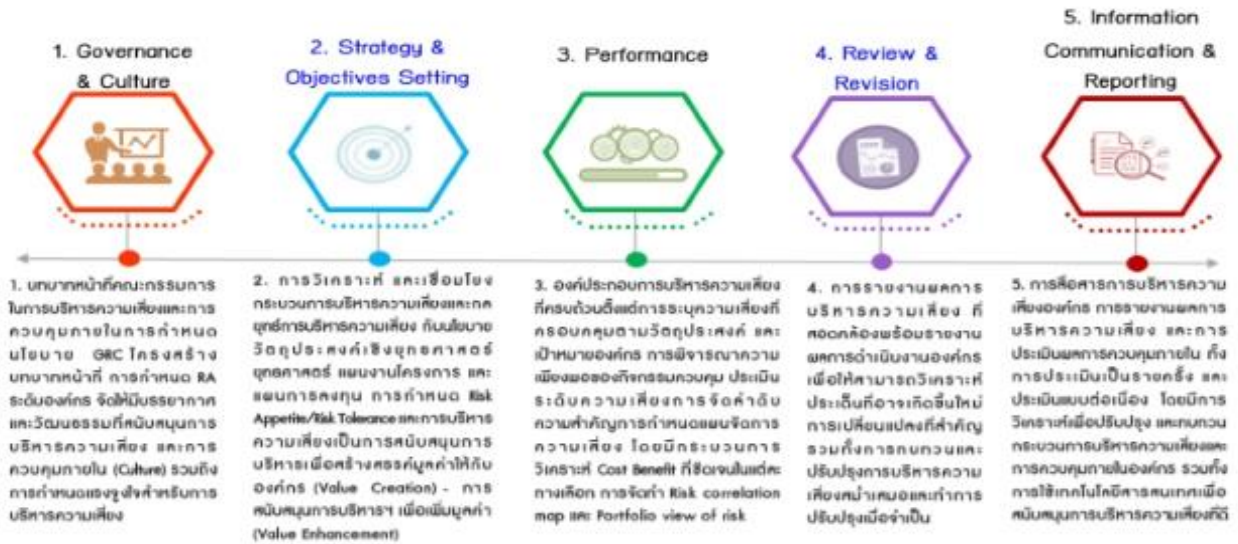
3) หลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ.2561 ในประเด็น

3.1) การประเมินความเสี่ยง เป็นกระบวนการที่ดำเนินการอย่างต่อเนื่องและเป็นประจำ เพื่อระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อ การบรรลุวัตถุประสงค์ของหน่วยงานของรัฐ รวมถึงกำหนดวิธีการจัดการความเสี่ยง นั้น ฝ่ายบริหารควรคำนึงถึงการเปลี่ยนแปลงของสภาพแวดล้อมภายนอกและ การปฏิบัติงานในทั้งหมดที่มีผลต่อการบรรลุวัตถุประสงค์ของหน่วยงานของรัฐ

3.2) กิจกรรมการควบคุม เป็นการปฏิบัติที่กำหนดไว้ในนโยบายและ กระบวนการดำเนินงาน เพื่อให้มั่นใจว่าการปฏิบัติตามคำสั่งการของฝ่ายบริหาร จะลดหรือควบคุมความเสี่ยงให้สามารถบรรลุวัตถุประสงค์ กิจกรรมการควบคุม ควรได้รับการนำไปปฏิบัติที่ทุกระดับของหน่วยงานของรัฐ ในกระบวนการ ปฏิบัติงาน ขั้นตอนการดำเนินงานต่างๆ รวมถึงการนำเทคโนโลยีมาใช้ในการดำเนินงาน



หลักเกณฑ์การประเมินผลการบริหารความเสี่ยงและการควบคุมภายในปี 2565



หัวข้อ	น้ำหนัก	ประเด็นย่อย
1. ธรรมาภิบาลและวัฒนธรรมองค์กร	15	1.1 บทบาทคณะกรรมการในการกำกับติดตามการบริหารความเสี่ยงและการพัฒนาระบบการควบคุมภายใน 4% 1.2 โครงสร้างและบทบาทหน้าที่ 3% 1.3 บรรยากาศและวัฒนธรรมสนับสนุนการบริหารความเสี่ยง 4% 1.4 ความมุ่งมั่นต่อค่านิยมองค์กร 2% 1.5 แรงจูงใจ การพัฒนาและรักษาบุคลากร 2%
2. การกำหนดยุทธศาสตร์และวัตถุประสงค์เชิงยุทธศาสตร์	15	2.1 การวิเคราะห์ธุรกิจ 0% 2.2 การระบุเป้าหมายการบริหารความเสี่ยง 5% 2.3 การประเมินทางเลือกกำหนดยุทธศาสตร์ 0% 2.4 การกำหนดวัตถุประสงค์ในการดำเนินธุรกิจเพื่อสร้างมูลค่าเพิ่มให้กับองค์กร 10%
3. กระบวนการบริหารความเสี่ยง	35	3.1 การระบุปัจจัยเสี่ยง 5% 3.2 การกำหนดกิจกรรมการควบคุมที่ตอบสนองต่อความเสี่ยงองค์กร 5% 3.3 การประเมินระดับความรุนแรงของปัจจัยเสี่ยง 5% 3.4 การจัดลำดับความเสี่ยง 3% 3.5 การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยงที่ระบุไว้ 5% 3.6 การบริหารความเสี่ยงแบบบูรณาการ 12%
4. การทบทวนการบริหารความเสี่ยง	15	4.1 การทบทวนและปรับปรุงผลการบริหารความเสี่ยง 10% 4.2 การกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยง 5% 4.3 การประเมินการเปลี่ยนแปลงที่มีนัยสำคัญ 0%
5. ข้อมูลสารสนเทศ การสื่อสารและการรายงานผล	20	5.1 ข้อมูลสารสนเทศ การสื่อสาร และการรายงานผล 5% 5.2 การติดตาม ประเมินผลและรายงานผลการบริหารความเสี่ยง การควบคุมภายใน วัฒนธรรมและผลการดำเนินงาน 5% 5.3 ข้อมูลและเทคโนโลยีในการสนับสนุนการบริหารความเสี่ยง 6% 5.4 กระบวนการบริหารความเสี่ยงต่อเนื่องทางธุรกิจ 4%

1.2 นโยบายการบริหารความเสี่ยงและควบคุมภายใน

คณะกรรมการองค์การสวนพฤกษศาสตร์ในฐานะผู้นำในการกำกับดูแลองค์กรฯ ได้ตระหนักถึงการพัฒนางค์กรอย่างยั่งยืน จึงได้กำหนดนโยบายในการกำกับดูแลกิจการที่ดีและการนำองค์กร ติดตามการบริหารความเสี่ยง และการพัฒนาระบบการควบคุมภายใน โดยบูรณาการหลักการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง จริยธรรม จรรยาบรรณและมีคุณธรรมในการดำเนินธุรกิจ รวมถึงการปฏิบัติตามกฎหมาย เพื่อสร้างมูลค่าเพิ่ม และประโยชน์สูงสุดแก่ผู้มีส่วนได้ส่วนเสีย ดังนี้

1) คณะกรรมการองค์การสวนพฤกษศาสตร์กำหนดนโยบาย กำกับดูแลและส่งเสริมให้มีการ บูรณาการการทำงานด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎ ระเบียบ (GRC) ตลอดจนมุ่งมั่นพัฒนาการดำเนินงานสู่มาตรฐานสากล

2) คณะกรรมการองค์การสวนพฤกษศาสตร์ปฏิบัติหน้าที่ด้วยความทุ่มเทและรับผิดชอบ มีความเป็นอิสระและมีการจัดแบ่งบทบาทหน้าที่ไว้ชัดเจน โดยกำกับดูแลกิจการเพื่อประโยชน์สูงสุดขององค์กร และคำนึงถึงบทบาทของผู้มีส่วนได้ส่วนเสียทุกกลุ่ม

3) คณะกรรมการองค์การสวนพฤกษศาสตร์ และผู้บริหารทุกระดับ ต้องเป็นผู้นำต้นแบบที่ดีในการปฏิบัติงานอย่างมีคุณธรรม จริยธรรมและจรรยาบรรณ ตลอดจนตระหนักถึงการบริหารความเสี่ยงการปฏิบัติตามกฎ ระเบียบ โดยสนับสนุนการมีส่วนร่วมของพนักงานในทุกระดับ และไม่ยอมให้บุคคลใดกระทำการทุจริตคอร์รัปชันในทุกรูปแบบ (Zero Tolerance)

4) คณะกรรมการองค์การสวนพฤกษศาสตร์ ผู้บริหารและพนักงานทุกระดับ มุ่งมั่นปฏิบัติตามหลักการ และแนวทางการกำกับดูแลกิจการที่ดีในรัฐวิสาหกิจของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.)

5) องค์การสวนพฤกษศาสตร์จัดให้มีการบริหารจัดการแบบบูรณาการโดยใช้ทรัพยากรที่มีอยู่ให้เกิดประโยชน์สูงสุด เพื่อให้สามารถบรรลุวัตถุประสงค์เชิงยุทธศาสตร์และวัตถุประสงค์อื่นๆ ได้อย่างมีประสิทธิภาพและประสิทธิผล ตลอดจนสร้างโอกาสและมูลค่าเพิ่มให้แก่องค์กร

6) องค์การสวนพฤกษศาสตร์จัดให้มีการบริหารความเสี่ยงและการควบคุมภายในทุกระดับอย่างทั่วถึง กระตุ้นให้พนักงานทุกคนตระหนักถึงความสำคัญของการบริหารความเสี่ยงในทุกการตัดสินใจ

7) องค์การสวนพฤกษศาสตร์กำกับดูแลและติดตามการปฏิบัติงาน เพื่อให้มั่นใจว่าองค์กรมีการดำเนินงานภายใต้ขอบเขตกฎหมาย สัญญา นโยบาย ระเบียบ และข้อบังคับ อย่างเคร่งครัดและมีประสิทธิผล

8) องค์การสวนพฤกษศาสตร์กำหนดให้มีการเปิดเผยข้อมูลสารสนเทศอย่างเพียงพอ เชื่อถือได้และทันต่อสถานการณ์ เพื่อให้ผู้มีส่วนได้ส่วนเสียรับข้อมูลสารสนเทศอย่างเท่าเทียมกัน

9) องค์การสวนพฤกษศาสตร์จัดให้มีระบบเทคโนโลยีสารสนเทศรองรับฐานข้อมูลด้าน GRC ที่เป็นปัจจุบัน เพื่อให้สามารถใช้ข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ

10) องค์การสวนพฤกษศาสตร์สื่อสารนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการปฏิบัติตามกฎ ระเบียบ (GRC) แก่ผู้เกี่ยวข้องทุกระดับทั้งภายในและภายนอก เพื่อใช้ในการพัฒนากระบวนการปฏิบัติงาน และส่งเสริมให้เป็นวัฒนธรรมขององค์กร

1.3 การบูรณาการการกำกับดูแลที่ดี การบริหารความเสี่ยงและการปฏิบัติตาม

กฎหมาย ฎระเบียบ (Governance Risk Management & Compliance : GRC)

“GRC” เป็นการรวม 3 องค์ประกอบเข้าด้วยกัน ได้แก่ Governance, Risk Management และ Compliance การกำหนดนิยามของคำว่า “GRC” นั้น มาจากนิยามของทั้งสามองค์ประกอบ ได้แก่

1) **Governance** หมายถึง นโยบาย วัฒนธรรมองค์กร กระบวนการขั้นตอนการปฏิบัติงานที่ถูกกำหนดออกมาอย่างชัดเจนในการบริหารจัดการและกำกับดูแลองค์กร โดยผู้บริหารระดับสูงเพื่อการบริหารองค์กรที่โปร่งใส ตรวจสอบได้

2) **Risk Management** หมายถึง การบริหารจัดการความเสี่ยงที่มีเป้าหมายในการลดผลกระทบและโอกาสเกิดความเสี่ยงขึ้นในองค์กร

3) **Compliance** หมายถึง การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ และกฎหมาย ตลอดจนการปฏิบัติตามนโยบายขององค์กรอย่างถูกต้อง

GRC คือการนำองค์ประกอบทั้ง 3 มาปฏิบัติร่วมกันในรูปแบบของการทำงานเป็นทีม มีการบูรณาการข้อมูล โดยเชื่อมโยงข้อมูลระหว่างกัน เพื่อให้ผู้บริหารใช้ประกอบการบริหารงานและกำหนดทิศทางขององค์กรได้อย่างมีประสิทธิภาพ โปร่งใส และตรวจสอบได้ เป็นองค์กรที่มีธรรมาภิบาล (Good Governance) เสริมสร้างภาพลักษณ์ที่ดีให้กับองค์กร นอกจากนี้ ยังทำให้องค์กรเกิดความสามารถในการแข่งขัน (Competitive Advantage) ในระยะยาวอีกด้วย รวมทั้งสร้างจิตสำนึกในการปฏิบัติงานที่ดีให้กับพนักงานทุกคน ส่งผลให้ผู้มีส่วนได้ส่วนเสียต่อองค์กร (Stakeholder) เกิดความเชื่อถือและความมั่นใจในการบริหารงานและการให้บริการต่างๆ ขององค์กร

โดยการบูรณาการ การกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎหมาย ฎระเบียบ ข้อบังคับ จะก่อให้เกิดประโยชน์ต่อการบริหารจัดการองค์กร ดังนี้

1) ทำให้ อ.ส.พ. มีบุคลากร (People) กระบวนการทำงาน (Process) และเทคโนโลยี (Technology) ที่ช่วยสนับสนุนการดำเนินงานตามนโยบายที่ได้รับ ให้บรรลุเป้าหมายได้ตามแผนที่วางไว้

2) ทำให้ อ.ส.พ. สามารถระบุความเสี่ยงได้ครอบคลุม ประเมินความเสี่ยงและจัดการความเสี่ยงต่างๆ ให้อยู่ในระดับที่ยอมรับได้โดยจัดสรรทรัพยากรได้อย่างเหมาะสมตามลำดับความสำคัญ

3) ทำให้ อ.ส.พ. สามารถติดตามได้ว่า การควบคุมภายในได้รับการออกแบบอย่างเหมาะสม ได้รับการนำไปปฏิบัติโดยผู้บริหารและพนักงานทุกระดับของ อ.ส.พ. ไม่มีการละเมิดกฎระเบียบข้อบังคับต่างๆ และการดำเนินงานเป็นไปตามความคาดหวังของผู้มีส่วนได้เสีย

4) ทำให้การสอบทานโดยสำนักตรวจสอบภายใน ครอบคลุมทั้งเรื่อง การกำกับดูแลกิจการ (Governance : G) การบริหารความเสี่ยง (Risk Management : R) การปฏิบัติตามกฎระเบียบ (Compliance : C) การควบคุมภายใน (Internal Control) และการปฏิบัติตามหลักจริยธรรมและจรรยาบรรณ (Ethics)

ส่วนที่

2



ด้านการบริหารความเสี่ยง
(RISK MANAGEMENT : RM)

ส่วนที่ 2 : การบริหารความเสี่ยง (Risk Management : RM)

2.1 ความหมายของการบริหารความเสี่ยง

“ความเสี่ยง (Risk)” หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบต่อหรือสร้างความเสียหายหรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ทั้งในระดับองค์กร ส่วนงาน และบุคคลได้

“การบริหารความเสี่ยง (Risk Management)” หมายถึง การบริหารปัจจัยเสี่ยงและควบคุมกิจกรรมทั้งกระบวนการ การดำเนินงานต่างๆ โดยลดมูลเหตุแต่ละโอกาสที่องค์กรจะเกิดความเสียหายเพื่อให้ระดับและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมและตรวจสอบได้อย่างมีระบบโดยคำนึงถึงการบรรลุเป้าหมายขององค์กรเป็นสำคัญ

2.2 ความสำคัญและประโยชน์ของการบริหารความเสี่ยง

- 1) ช่วยให้ผู้บริหารพิจารณาระดับความเสี่ยงที่ยอมรับได้ที่สอดคล้องกับกลยุทธ์ขององค์กร สามารถป้องกันและใช้ประโยชน์จากเหตุการณ์ในเชิงบวกได้มีประสิทธิภาพมากขึ้น
- 2) สนับสนุนให้องค์กรสามารถป้องกันเหตุการณ์ ประเมินความเสี่ยงและจัดการความเสี่ยงให้สอดคล้องกับวัตถุประสงค์ด้านการเติบโตและผลตอบแทนของธุรกิจ
- 3) สร้างคุณค่าให้การทำงาน สร้างมูลค่าเพิ่มให้แก่องค์กร และสร้างภาพลักษณ์ที่ดีให้องค์กร
- 4) ช่วยพัฒนาการบริหารจัดการให้มีประสิทธิภาพและประสิทธิผล

2.3 แนวทางการบริหารจัดการความเสี่ยงของ อ.ส.พ.

องค์การสวนพฤกษศาสตร์ได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงขององค์กร จึงมุ่งมั่นให้มีการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management) ที่เป็นไปตามหลักสากล โดยกำหนดแนวทางการบริหารจัดการความเสี่ยงเพื่อใช้ในการขับเคลื่อนองค์กรให้ดำเนินการตามวิสัยทัศน์ พันธกิจ และยุทธศาสตร์ ดังนี้

1) มุ่งมั่นพัฒนาการบริหารความเสี่ยงขององค์การสวนพฤกษศาสตร์ให้เป็นไปตามหลักปฏิบัติและมาตรฐานที่ดี สามารถขับเคลื่อนภารกิจและโครงการสำคัญขององค์กร เพื่อให้เกิดประสิทธิภาพ ประสิทธิผลสูงสุด รวมถึงเป็นเครื่องมือสำคัญในการกำหนดนโยบายที่สอดคล้องกับสถานการณ์ การบูรณาการร่วมกันหน่วยงานทั้งภายในและภายนอกองค์กร การป้องกันและลดผลกระทบที่อาจเกิดจากการดำเนินงานตามภารกิจขององค์กร ทั้งในระยะสั้นและระยะยาว

2) ให้ความสำคัญกับการควบคุมภายในและการบริหารความเสี่ยง เพื่อให้การดำเนินงานขององค์กรเป็นไปตามกฎหมายที่เกี่ยวข้อง โดยมุ่งเน้นให้มีการดำเนินงานที่ครอบคลุมในทุกกิจกรรมอย่างเพียงพอ เหมาะสมกับการดำเนินการตามภารกิจขององค์กร

3) มุ่งเน้นดำเนินการควบคุมภายในและบริหารจัดการความเสี่ยง เพื่อสร้างความยั่งยืนให้แก่องค์กร โดยนำระบบเทคโนโลยีสารสนเทศมาบูรณาการใช้ในการสนับสนุน เพื่อรวบรวมข้อมูล วิเคราะห์ และประเมินผล พร้อมทั้งติดตามความเสี่ยงขององค์กรอย่างเป็นระบบ

2.4 บทบาทและความรับผิดชอบของผู้เกี่ยวข้องโดยตรงกับการบริหารความเสี่ยง

ผู้เกี่ยวข้อง	บทบาทและความรับผิดชอบหลัก
คณะกรรมการ	<ul style="list-style-type: none"> - มีความเข้าใจถึงความเสี่ยงที่อาจมีผลกระทบต่อองค์กร และทำให้มั่นใจว่ามีการดำเนินการที่เหมาะสมเพื่อจัดการความเสี่ยงนั้นๆ
คณะกรรมการตรวจสอบ	<ul style="list-style-type: none"> - ทำให้มั่นใจว่ามีการควบคุมภายในที่เหมาะสมเพื่อจัดการความเสี่ยงทั่วทั้งองค์กร - กำกับดูแลและติดตามการบริหารความเสี่ยงอย่างเป็นอิสระ - ติดตามประสิทธิภาพการทำงานของหน่วยงานตรวจสอบภายใน - รายงานต่อคณะกรรมการและผู้ถือหุ้นเกี่ยวกับประสิทธิภาพและประสิทธิผลของการควบคุมภายใน - สื่อสารกับคณะกรรมการบริหารความเสี่ยง เพื่อให้เข้าใจความเสี่ยงที่สำคัญและเชื่อมโยงกับระบบการควบคุมภายใน
คณะอนุกรรมการขับเคลื่อนนโยบายฯ	<ul style="list-style-type: none"> - พิจารณา และอนุมัตินโยบายและกรอบการบริหารความเสี่ยง - ติดตามการพัฒนากรอบการบริหารความเสี่ยง - ประเมินและอนุมัติแผนการจัดการความเสี่ยง - รายงานต่อคณะกรรมการเกี่ยวกับความเสี่ยงและการจัดการความเสี่ยง - สื่อสารกับคณะกรรมการตรวจสอบ เกี่ยวกับความเสี่ยงที่สำคัญ
ผู้อำนวยการ อ.ส.พ.	<ul style="list-style-type: none"> - ติดตามความเสี่ยงที่สำคัญทั้งองค์กร และทำให้มั่นใจได้ว่ามีแผนการจัดการที่เหมาะสม - ส่งเสริมนโยบายการบริหารความเสี่ยง และทำให้มั่นใจว่ากระบวนการบริหารความเสี่ยงได้รับการปฏิบัติทั่วทั้งองค์กร
รองผู้อำนวยการ	<ul style="list-style-type: none"> - ติดตามความเสี่ยงทางกลยุทธ์และความเสี่ยงด้านการปฏิบัติการที่สำคัญ และทำให้มั่นใจได้ว่ามีแผนการจัดการความเสี่ยงที่เหมาะสม - ส่งเสริมวัฒนธรรมการบริหารความเสี่ยง และทำให้มั่นใจ ผู้อำนวยการสำนักให้ความสำคัญกับการบริหารความเสี่ยงในหน่วยงานของตน
ผู้อำนวยการสำนัก, หัวหน้าส่วน	<ul style="list-style-type: none"> - ทำให้มั่นใจว่าการปฏิบัติงานรายวันมีการประเมินจัดการและรายงานความเสี่ยงอย่างเพียงพอ - ส่งเสริมพนักงานในฝ่ายงานให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง
หัวหน้างานหรือพนักงาน	<ul style="list-style-type: none"> - ระบุและรายงานความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานต่อผู้อำนวยการสำนักและเข้าร่วมในการจัดทำแผนจัดการความเสี่ยง และนำแผนไปปฏิบัติหน่วยงานหรือผู้รับผิดชอบ - ปฏิบัติหน้าที่ประจำวันแทนคณะกรรมการบริหารความเสี่ยง
หน่วยงานหรือผู้รับผิดชอบการบริหารความเสี่ยง	<ul style="list-style-type: none"> - จัดทำนโยบายความเสี่ยง กรอบและกระบวนการ เสนอคณะอนุกรรมการฯ ที่คณะกรรมการ อ.ส.พ. มอบหมาย เพื่อพิจารณาอนุมัติ - ให้การสนับสนุนและแนะนำกระบวนการบริหารความเสี่ยงแก่หน่วยงานต่างๆ ภายในองค์กรตามที่มีการร้องขอ
ผู้ตรวจสอบภายใน	<ul style="list-style-type: none"> - ทำให้มั่นใจว่ามีการควบคุมภายในที่เหมาะสมต่อการจัดการความเสี่ยง และการควบคุมเหล่านั้นได้รับการปฏิบัติตามภายในองค์กร - ทำให้มั่นใจว่าได้มีการนำระบบการบริหารความเสี่ยงมาปรับใช้อย่างเหมาะสมและมีการปฏิบัติตามทั่วทั้งองค์กร - สอบทานการปฏิบัติงานของหน่วยงานการบริหารความเสี่ยง - สื่อสารกับหน่วยงานการบริหารความเสี่ยงเพื่อทำความเข้าใจเกี่ยวกับความเสี่ยงและดำเนินการตรวจสอบภายในตามแนวความเสี่ยง (Risk based auditing)

2.5 แหล่งที่มาของการเกิดความเสี่ยง

แหล่งที่มาของการเกิดความเสี่ยง เกิดจากปัจจัย 2 ปัจจัย ดังนี้

1) ปัจจัยภายใน เช่น วัตถุประสงค์ขององค์กร, นโยบายและกลยุทธ์, การดำเนินงาน, กระบวนการทำงาน, โครงสร้างองค์กร และระบบการบริหารงาน, การเงิน, วัฒนธรรมองค์กร และเทคโนโลยีสารสนเทศ

2) ปัจจัยภายนอก เช่น นโยบายของรัฐ สภาวะเศรษฐกิจ/สังคมการเมือง การดำเนินการของหน่วยงานภายนอกที่เกี่ยวข้อง, การแข่งขัน (คู่แข่งทางการดำเนินธุรกิจ), ผู้ขายหรือผู้ส่งมอบสินค้า/บริการและภัยธรรมชาติต่างๆ เป็นต้น

โดยในกระบวนการระบุปัจจัยเสี่ยง (Risk Identification) ต้องมีการระบุปัจจัยเสี่ยงทั้งภายในและภายนอก ยุทธศาสตร์ และเป้าหมายที่สำคัญขององค์กร จุดอ่อน ความต้องการ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย ตัวชี้วัดที่สำคัญขององค์กร (Inherent Risk) เพื่อกำหนดเป็น Risk Universe



รูปภาพที่ 1 : การระบุปัจจัยความเสี่ยง (Risk Identification) ที่ครอบคลุม

2.6 ประเภทความเสี่ยง

1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: SR) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์หรือนโยบายการบริหารงาน และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย, เป้าหมาย, กลยุทธ์, โครงสร้างองค์กร, ภาวะการแข่งขัน, ทรัพยากรและสภาพแวดล้อมอันส่งผลกระทบต่อวัตถุประสงค์หรือเป้าหมายองค์กร

2) ความเสี่ยงด้านการดำเนินงาน (Operational Risk : OR) เป็นความเสี่ยงที่เกี่ยวข้องกับประเด็นในการปฏิบัติงานประจำวัน หรืออาจเกิดจากการดำเนินงานปกติที่องค์กรต้องเผชิญเพื่อให้บรรลุวัตถุประสงค์เชิงกลยุทธ์ ความเสี่ยงด้านนี้มักเกี่ยวข้องกับประสิทธิภาพ และประสิทธิผลขององค์กร เช่น อุปกรณ์เทคโนโลยีสารสนเทศ บุคลากร ซึ่งส่งผลกระทบต่อประสิทธิภาพและประสิทธิผลในการดำเนินธุรกิจขององค์กร เช่น โครงการล่าช้า ขาดอุปกรณ์หรือเครื่องมือที่มีประสิทธิภาพ ขาดการติดตามการบริหารสัญญา บุคลากรขาดแรงจูงใจในการปฏิบัติงาน เป็นต้น

- ความเสี่ยงจากการปฏิบัติงาน ได้แก่ การปฏิบัติงานไม่เป็นไปตามแผนปฏิบัติ ไม่เหมาะสมกับลักษณะงาน โครงการล่าช้า พนักงานไม่มีประสิทธิภาพ การพัฒนาผลิตภัณฑ์ไม่มีประสิทธิภาพ

- ความเสี่ยงจากการมอบอำนาจ การกระจายอำนาจภายในองค์กรอาจช่วยเพื่อประสิทธิภาพในการทำงานให้สะดวกรวดเร็วขึ้นได้ แต่ก็อาจสร้างปัญหาในการทำงานได้เช่นกัน หากสายบังคับบัญชาไม่ชัดเจนภาวะผู้นำของการมอบอำนาจ หรือเครื่องมือสร้างแรงจูงใจในการปฏิบัติงานไม่เพียงพอต่ออำนาจที่ได้รับ

- ความเสี่ยงจากเทคโนโลยีที่เปลี่ยนแปลง ส่งผลให้อาจเกิดปัญหาต่อการดำเนินการขององค์กร ได้แก่ การปรับเปลี่ยนอุปกรณ์คอมพิวเตอร์และโปรแกรมใหม่ การเปลี่ยนแปลงขั้นตอนการทำงาน การพัฒนาผลิตภัณฑ์ใหม่ การปลดระวางเครื่องมือและโปรแกรมเก่า การจัดการฐานข้อมูล

3) ความเสี่ยงด้านการเงิน (Financial Risk : FR) หมายถึง ความเสี่ยงเกี่ยวกับสภาพคล่องทางการเงิน การบริหารทางการเงินและงบการเงิน หรือการขาดข้อมูลการวิเคราะห์ วางแผนการควบคุม และจัดทำรายงานเพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้อง เหมาะสม ส่งผลต่อสถานะทางการเงินขององค์กร เช่น แผนการลงทุนไม่มีความชัดเจนเพียงพอที่จะนำไปใช้ในการวิเคราะห์เพื่อคาดการณ์ด้านการเงินได้ สภาพคล่องทางการเงิน ความเสี่ยงจากการจัดสรรงบประมาณไม่เหมาะสม ตั้งงบประมาณผิดพลาด และใช้งบประมาณเกิน ไม่มีแหล่งรายได้ใหม่ รวมทั้งความเสี่ยงจากความผันผวนของปัจจัยทางการตลาด(Market Risk) และความเสี่ยงจากการที่คู่สัญญาไม่ปฏิบัติตามภาระผูกพัน (Credit Risk)

4) ความเสี่ยงด้าน กฎหมาย และข้อกำหนดผูกพันองค์กร (Compliance Risk: CR) หมายถึง ความเสี่ยงจากการที่หน่วยงานต่างๆ ต้องปฏิบัติตามกฎหมายและข้อกำหนดผูกพันองค์กร เช่น ความเสี่ยงจากการผิดสัญญาข้อผูกพัน ความเสี่ยงจากการขาดการรายงานตามกฎระเบียบ หรือการไม่ปฏิบัติตามกฎหมายระเบียบและข้อบังคับ

2.7 การบริหารความเสี่ยง อ.ส.พ.

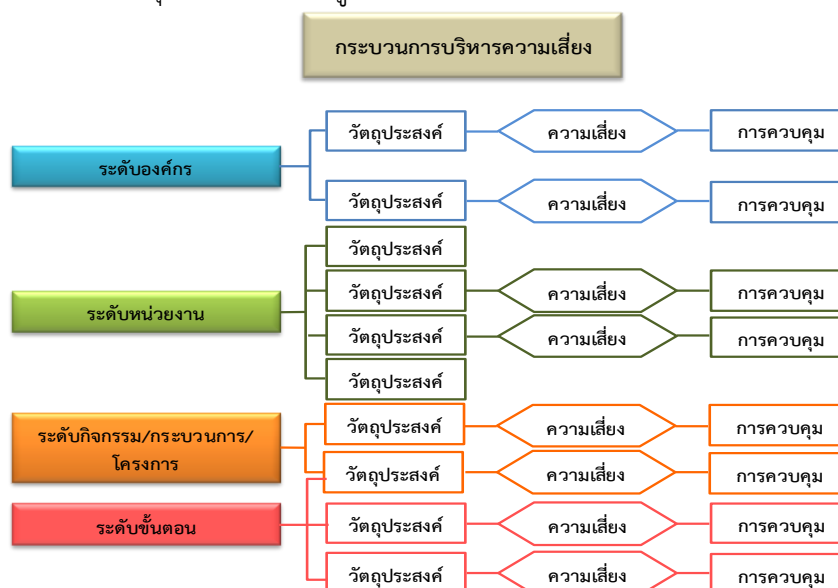
การบริหารความเสี่ยงสามารถดำเนินงานได้ในทุกๆ ส่วนขององค์กร ตั้งแต่การบริหารความเสี่ยงของ อ.ส.พ. ที่เกี่ยวข้องกับทุกส่วนงานลงไปถึงระดับของแต่ละขั้นตอนของการทำงานซึ่งสามารถแบ่งเป็น 4 ระดับ ดังนี้

1) การบริหารความเสี่ยงระดับองค์กร เป็นการบริหารความเสี่ยงที่มีผลกระทบต่อวิสัยทัศน์ วัตถุประสงค์ หรือเป้าหมายการดำเนินงานของ อ.ส.พ. รวมทั้งมีผลกระทบต่อเป้าหมายการดำเนินงานตามบันทึกข้อตกลง ประเมินผลการดำเนินงานของ อ.ส.พ.

2) การบริหารความเสี่ยงระดับหน่วยงานย่อย เป็นการบริหารความเสี่ยงที่เกิดขึ้นจากการดำเนินงานของแต่ละหน่วยงาน โดยความเสี่ยงที่เกิดขึ้นสามารถบริหารจัดการได้โดยอำนาจหน้าที่ของผู้อำนวยการสำนัก เป็นความเสี่ยงที่ไม่เกิดผลกระทบต่อวัตถุประสงค์และเป้าหมายในการดำเนินงานของ อ.ส.พ.

3) การบริหารความเสี่ยงระดับกิจกรรม/กระบวนการ/โครงการ

4) การบริหารความเสี่ยงระดับขั้นตอนโดยในทุกๆ ระดับจะต้องมีการกำหนดวัตถุประสงค์ของการบริหารความเสี่ยง และการควบคุมความเสี่ยง ดังรูปภาพ 2



รูปภาพที่ 2 กระบวนการบริหารความเสี่ยง เป็น 4 ระดับ

2.8 องค์ประกอบการบริหารความเสี่ยง

การบริหารความเสี่ยงที่มีประสิทธิผลตามแนวทางของ COSO (The Committee of Sponsoring Organization of the Treadway Commission) ประกอบด้วยองค์ประกอบ 8 ประการซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงานและการบริหารความเสี่ยงดังนี้

1) **สภาพแวดล้อมภายในองค์กร (Internal Environment)** สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญในการกำหนดกรอบการบริหารความเสี่ยงและเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กร ประกอบด้วยหลายประการ เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติของบุคลากรกระบวนการทำงาน ระบบสารสนเทศ เป็นต้น

2) **การกำหนดวัตถุประสงค์ (Objective Setting)** องค์กรจะต้องพิจารณาการกำหนดวัตถุประสงค์ในการบริหารความเสี่ยงให้มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม

3) **การระบุความเสี่ยง (Risk Identification)** เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งปัจจัยเสี่ยงที่เกิดขึ้นจากปัจจัยภายในและปัจจัยภายนอกองค์กร และเมื่อเกิดขึ้นแล้วส่งผลให้องค์กรไม่บรรลุวัตถุประสงค์หรือเป้าหมาย เช่น นโยบายการบริหารงาน บุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบข้อบังคับ เป็นต้น ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้นๆ และเพื่อนำให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้เป็นอย่างดี

4) **การประเมินความเสี่ยง (Risk Assessment)** การประเมินความเสี่ยง เป็นการวัดระดับความรุนแรงของความเสี่ยงเพื่อพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

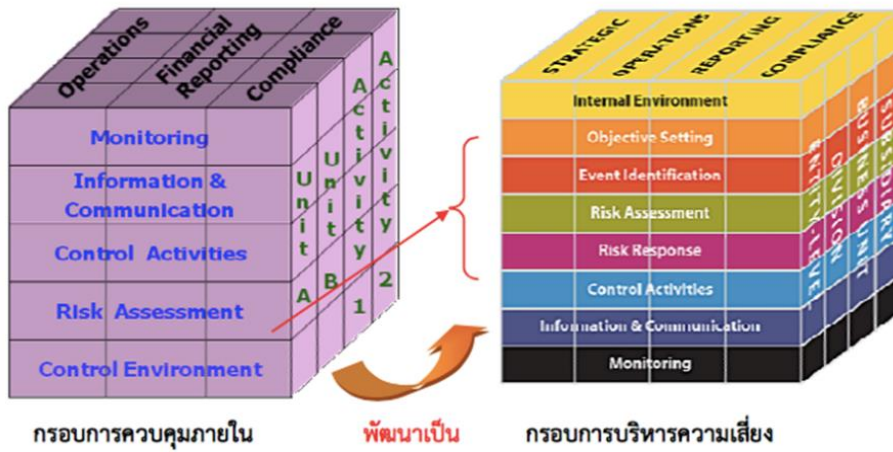
5) **การตอบสนองความเสี่ยง (Risk Response)** เป็นการดำเนินการหลังจากที่องค์กรสามารถระบุความเสี่ยงขององค์กรและประเมินระดับความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการเพื่อลดโอกาสที่จะเกิดความเสี่ยงและลดระดับความรุนแรงของผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้ ด้วยวิธีจัดการความเสี่ยงที่เหมาะสมที่สุดและคุ้มค่ากับการลงทุน

6) **กิจกรรมควบคุม (Control Activities)** การกำหนดกิจกรรมและการปฏิบัติต่างๆ เพื่อช่วยลดหรือควบคุมความเสี่ยงเพื่อสร้างความมั่นใจจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้องและทำให้การดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ป้องกันและลดระดับความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

7) **สารสนเทศและการสื่อสาร (Information and Communication)** องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงต่อไปตามกรอบขั้นตอนการปฏิบัติที่องค์กรกำหนด

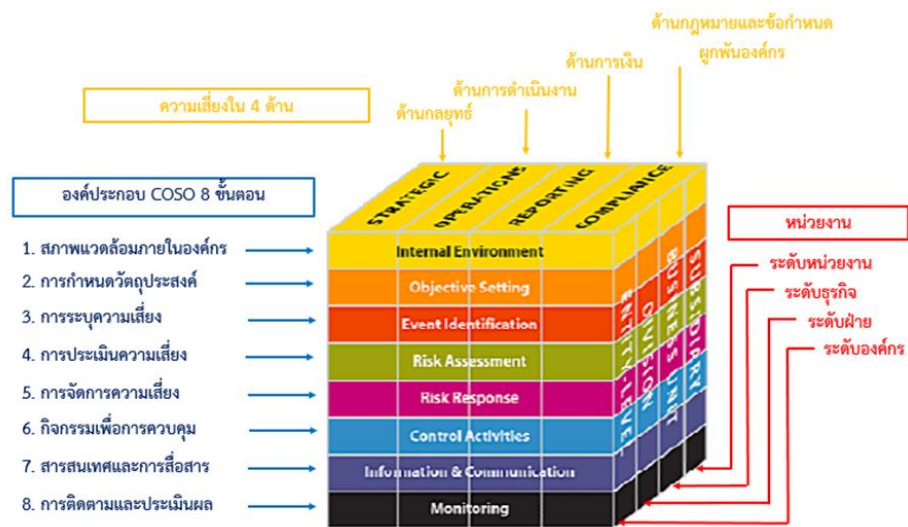
8) **การติดตามประเมินผล (Monitoring)** องค์กรจะต้องมีการติดตามผลเพื่อให้ทราบถึงผลการดำเนินงานว่าเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

อ.ส.พ. ได้ดำเนินการบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงขององค์กรที่ได้รับว่าเป็นแนวทางในการส่งเสริมการบริหารความเสี่ยงและเป็นหลักปฏิบัติที่เป็นสากล คือกรอบการบริหารความเสี่ยงระดับองค์กรของคณะกรรมการ COSO (The Committee of Sponsoring Organization of the Treadway Commission) สำหรับองค์กร (Enterprise Risk Management Framework) ตามรูปภาพที่ 2 ซึ่ง COSO ประกาศใช้กรอบงานการบริหารความเสี่ยงระดับองค์กร (ERM) โดยพัฒนาจากกรอบงานการควบคุมภายในและได้เพิ่มแนวคิดหลักการและองค์ประกอบสำคัญเพื่อให้ตรงความต้องการเกี่ยวกับการบริหารความเสี่ยงในการบริหารงานยุคใหม่ในการเพิ่มมูลค่าให้กับองค์กร โดยให้สอดคล้องกับหลักการกำกับดูแลที่ดี และสามารถใช้เป็นเกณฑ์อ้างอิงในการบริหารความเสี่ยงอย่างเป็นสากล



รูปภาพที่ 3 กรอบงานการควบคุมภายในและกรอบงานการบริหารความเสี่ยงตามแนวทางของ COSO

องค์ประกอบของกรอบการบริหารความเสี่ยงตามแนว COSO มี 8 องค์ประกอบที่มีความสัมพันธ์กัน ตามรูปภาพที่ 4



รูปภาพที่ 4 แสดงการบริหารความเสี่ยงตามแนวทางของ COSO

องค์ประกอบการบริหารความเสี่ยงข้างต้นมีกระบวนการที่ต้องดำเนินงานอย่างต่อเนื่อง 6 ขั้นตอน ได้แก่

- การกำหนดวัตถุประสงค์ (ขั้นตอน 2)
- การระบุความเสี่ยง (ขั้นตอน 3)
- การประเมินความเสี่ยง (ขั้นตอน 4)
- การจัดการความเสี่ยง (ขั้นตอน 5)
- กิจกรรมเพื่อการควบคุม (ขั้นตอน 6)
- การติดตามและประเมินผล (ขั้นตอน 8)

กระบวนการบริหารความเสี่ยง

โดยมีขั้นตอนสภาพแวดล้อมภายในองค์กร (ขั้นตอน 1) และสารสนเทศและการสื่อสาร (ขั้นตอน 7) เป็นองค์ประกอบเสริมให้กระบวนการบริหารความเสี่ยงทั้ง 6 ขั้นตอนมีประสิทธิภาพ ตามรูปภาพที่ 4

2.9 กระบวนการบริหารความเสี่ยง

องค์การสวนพฤกษศาสตร์ ได้ยึดถือนโยบายในการบริหารบริหารความเสี่ยง 4 ประการ มาดำเนินกระบวนการบริหารความเสี่ยง ดังนี้

1) การบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันทั้งองค์กร : ทุกภาคส่วนในองค์กร ตั้งแต่คณะกรรมการองค์การสวนพฤกษศาสตร์จนถึงระดับปฏิบัติการ ควรมีส่วนร่วมในกระบวนการบริหารจัดการความเสี่ยง โดยระบุ วิเคราะห์ และประเมินความเสี่ยง ที่อาจส่งผลกระทบต่อวัตถุประสงค์องค์กร เป็นประจำทุกปีและเมื่อจำเป็น เพื่อให้สอดคล้องกับสถานการณ์สภาพแวดล้อมที่เปลี่ยนแปลงไป เพื่อบริหารจัดการให้ความเสี่ยงอยู่ในระดับที่องค์กรยอมรับได้

2) การบริหารความเสี่ยงอย่างบูรณาการ : ควรจัดให้มีกระบวนการบริหารความเสี่ยงอย่างเชื่อมโยงบูรณาการในองค์กร โดยรวมอยู่ในกระบวนการหลักทางธุรกิจและการวางแผนกลยุทธ์ ทั้งนี้ กระบวนการบริหารความเสี่ยงควรมีรูปแบบการบริหารเป็นเชิงรุกและครอบคลุมถึงโอกาสทางธุรกิจ ทั้งนี้ เพื่อบรรลุเป้าหมายขององค์กรร่วมกัน

3) กระบวนการบริหารความเสี่ยงควรได้รับการพัฒนาอย่างต่อเนื่อง : ซึ่งอาจพิจารณาข้อเสนอแนะความคิดเห็น จากผู้มีส่วนได้เสียทั้งภายในและภายนอก ร่วมในการระบุ วิเคราะห์ ประเมินความเสี่ยงตามความจำเป็น และควรพิจารณาในการนำเทคโนโลยีสารสนเทศสนับสนุนการบริหารความเสี่ยงอย่างเหมาะสม

4) การกำกับดูแลการบริหารความเสี่ยงอย่างสม่ำเสมอ : ควรจัดให้มีการประชุมคณะอนุกรรมการบริหารความเสี่ยง อย่างสม่ำเสมอ หรือเมื่อมีเหตุการณ์อันทำให้ระดับความเสี่ยงเปลี่ยนแปลงไป เพื่อติดตามประเมินผลการบริหารความเสี่ยงให้เกิดความมั่นใจว่าความเสี่ยงที่สำคัญขององค์กรได้รับการบริหารจัดการอย่างเหมาะสมทันเวลา

5) การสร้างให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กร : สนับสนุนให้คณะกรรมการองค์การสวนพฤกษศาสตร์ ผู้บริหาร และพนักงานทุกระดับสามารถเข้าถึงแหล่งข้อมูลข่าวสารการบริหารความเสี่ยงอย่างทั่วถึง โดยผ่านกิจกรรม และช่องทางต่างๆ รวมถึงการอบรมสัมมนา เพื่อปลูกฝังให้เกิดความตระหนักว่าการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการปฏิบัติงานปกติขององค์กร

กระบวนการบริหารความเสี่ยงของ อ.ส.พ.



รูปภาพที่ 5 กระบวนการบริหารความเสี่ยงของ อ.ส.พ.

กระบวนการบริหารความเสี่ยงของ อ.ส.พ. แบ่งเป็น 8 ขั้นตอน ดังต่อไปนี้

กระบวนการที่ 1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

องค์กรในที่นี้ หมายถึง อ.ส.พ. หน่วยงานย่อยในที่นี้ หมายถึง งาน หรือ กิจกรรม ที่แต่ละหน่วยงานมีแผนหรือกิจกรรมในการดำเนินงานอยู่แล้วสามารถนำมาวิเคราะห์ ประเมินผลอย่างอิสระได้

สภาพแวดล้อมภายใน

สภาพแวดล้อมการทำงานภายใน อ.ส.พ. อาจจะเป็นสภาพแวดล้อมการทำงานภายนอกของหน่วยงานย่อยของ อ.ส.พ. ได้ หากอยู่นอกเหนือการควบคุมของหน่วยงานนั้น ๆ เช่น นโยบายของ อ.ส.พ. หรือ นโยบายของผู้บริหาร เนื่องจากสิ่งเหล่านั้นล้วนกำหนดมาเพื่อเป็นทิศทางให้หน่วยงานย่อยดำเนินการ ซึ่งการกำหนดนั้นจะส่งผลต่อความสำเร็จหรือไม่สำเร็จของหน่วยงานย่อยได้ แต่หน่วยงานย่อยไม่สามารถควบคุม กำหนด แก้ไขหรือปรับปรุงได้ แต่ถ้าเป็นสภาพแวดล้อมการทำงานภายนอกของ อ.ส.พ. ย่อมเป็นสภาพแวดล้อมการทำงานภายนอกของหน่วยงานย่อยโดยไม่ต้องวิเคราะห์อีกแล้วไม่ว่าจะด้วยสาเหตุใดก็ตามเป็นสิ่งที่ อ.ส.พ. ควบคุมไม่ได้ย่อมเป็นสิ่งที่หน่วยงานภายใน อ.ส.พ. ควบคุมไม่ได้เช่นเดียวกัน

การวิเคราะห์สภาพแวดล้อมภายใน เป็นการศึกษาค้นหาและระบุว่าองค์กรจะต้องบริหารงานและดำเนินงานเพื่อนำปัจจัยขององค์กรมาใช้เพื่อสร้างความได้เปรียบในการแข่งขันจากจุดแข็งและโอกาส ตลอดจนเพื่อหลีกเลี่ยงจุดอ่อนและอุปสรรคที่จะเกิดขึ้น การวิเคราะห์สภาพแวดล้อมภายในขององค์กรสามารถทำได้หลายวิธี ที่นิยมกัน ดังนี้

- การวิเคราะห์ตามหน้าที่ (Function Analysis)
- การวิเคราะห์ปัจจัย 7 ประการของ McKinsey (McKinsey 7-S Framework)
- การวิเคราะห์สายโซ่แห่งคุณค่า (Value Chain Analysis)

ดังนั้น จึงเป็นสิ่งที่ผู้บริหารสามารถควบคุมได้ (Controllable Factor) การวิเคราะห์สภาพแวดล้อมภายในมีการวิเคราะห์ได้หลายวิธีที่นิยมกัน ได้แก่ การวิเคราะห์ตามหน้าที่ (Function Analysis) การวิเคราะห์ปัจจัย 7 ประการของ McKinsey (McKinsey 7-S Framework) และวิธีที่สาม การวิเคราะห์สายโซ่แห่งคุณค่า (Value Chain Analysis)

สภาพแวดล้อมภายนอก

สภาพแวดล้อมภายนอก เป็นปัจจัยที่อยู่เหนือการควบคุมขององค์กร มีการเปลี่ยนแปลงอยู่ตลอดเวลา เป็นไปไม่ได้ที่จะติดตามการเปลี่ยนแปลงของสภาพแวดล้อมได้ทุกอย่าง ผู้บริหารควรจะมีแผนเฉพาะปัจจัยทางสภาพแวดล้อมที่สำคัญเท่านั้น โดยทั่วไป สภาพแวดล้อมภายนอก มีอยู่ 2 ส่วน คือ

1) **สภาพแวดล้อมการดำเนินงาน (Task Environment)** เป็นปัจจัยที่มีผลกระทบโดยตรง ต่อการดำเนินงานของกิจการ ประกอบไปด้วย ผู้มีส่วนได้เสียกับองค์กร เช่น รัฐบาล ชุมชน คู่แข่งขัน ลูกค้า ผู้จำหน่าย วัตถุดิบ เจ้าหนี้ แรงงาน กลุ่มผลประโยชน์

2) **สภาพแวดล้อมโดยทั่วไป (General Environment)** เป็นปัจจัยที่ไม่มีผลกระทบต่อการดำเนินงานระยะสั้นขององค์กร แต่มีผลต่อการตัดสินใจในระยะยาว ได้แก่ เศรษฐกิจ สังคม วัฒนธรรม การเมือง กฎหมาย เทคโนโลยี ภูมิศาสตร์ และปัจจัยระหว่างประเทศ

การเปลี่ยนแปลงของสภาพแวดล้อมภายนอก ก่อให้เกิดการเปลี่ยนแปลงลักษณะของอุตสาหกรรม ซึ่งสร้างโอกาส อุปสรรค และปัจจัยแห่งความสำเร็จที่สำคัญใหม่ๆ ขึ้นมา ผู้บริหารจึงต้องประเมินทรัพยากรและความสามารถขององค์กร โดยการวิเคราะห์สภาพแวดล้อมภายในด้วย ทั้งนี้ เพื่อทราบถึงจุดแข็งและจุดอ่อนขององค์กรด้วยสภาพแวดล้อมภายในองค์กร (Internal Environment Analysis) เป็นปัจจัยภายในที่ขึ้นกับทรัพยากรและความสามารถขององค์กรเอง

กระบวนการที่ 2 การกำหนดวัตถุประสงค์ (Objective setting)

ความเสี่ยงจะกำหนดวัตถุประสงค์ตามภารกิจหลักของ อ.ส.พ. และเป้าหมายตามแผนวิสาหกิจและแผนปฏิบัติงาน โดยให้สอดคล้องกับงบประมาณรายจ่ายในแต่ละปี ของ อ.ส.พ. เพื่อให้ทราบขอบเขตการดำเนินงานในแต่ละระดับ และสามารถวิเคราะห์ความเสี่ยงที่คาดว่าจะเกิดขึ้นได้อย่างครบถ้วน ในการบริหารความเสี่ยงของหน่วยงาน / องค์กรให้บรรลุเป้าหมายในภาพรวม การกำหนดวัตถุประสงค์ที่ดี ในการกำหนดวัตถุประสงค์ ควรกำหนดให้ครอบคลุมแต่ละประเภทของวัตถุประสงค์ ดังต่อไปนี้

1) **วัตถุประสงค์ด้านกลยุทธ์ (Strategic Objectives)** เป็นวัตถุประสงค์ในระดับสูง ซึ่งเชื่อมโยงและสนับสนุนภารกิจขององค์กร โดยองค์กรกำหนดวัตถุประสงค์ด้านกลยุทธ์เพื่อแสวงหาทางเลือกหรือวิธีการสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้เสีย

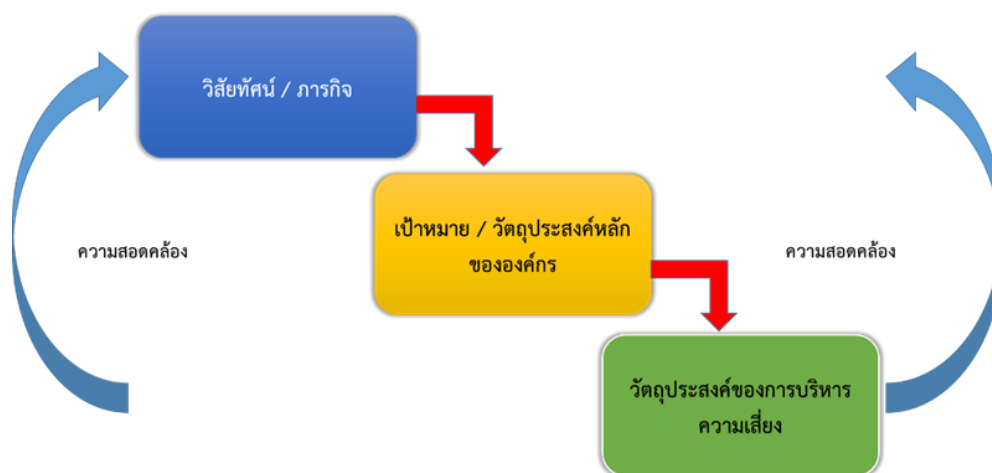
2) **วัตถุประสงค์ด้านการดำเนินงาน (Operations Objectives)** เป็นวัตถุประสงค์ในระดับของการปฏิบัติงานที่มุ่งเน้นการใช้ทรัพยากรอย่างมีประสิทธิภาพและประสิทธิผล

3) **วัตถุประสงค์ด้านการเงิน (Financial Objectives)** เป็นวัตถุประสงค์ที่เกี่ยวข้องกับการบริหารการเงิน ขององค์กรในทุกด้าน ได้แก่ ประสิทธิภาพในการเบิกจ่ายงบประมาณ ประสิทธิภาพในการบริหารค่าใช้จ่าย ความน่าเชื่อถือและความทันเวลาของการรายงานข้อมูลทางการเงินและข้อมูลที่ไม่ใช่ทางการเงิน ทั้งภายในและภายนอกองค์กร

4) **วัตถุประสงค์ด้านกฎหมาย กฎระเบียบ (Compliance Objectives)** เป็นวัตถุประสงค์ที่มุ่งเน้นเกี่ยวกับการปฏิบัติตามกฎหมายและกฎระเบียบต่าง ๆ การปฏิบัติตามกฎระเบียบเกี่ยวข้องกับความสอดคล้องของวัตถุประสงค์

วิสัยทัศน์เป็นจุดเริ่มต้นในการกำหนดทิศทางขององค์กร ผู้บริหารระดับสูงจะทำการกำหนดวัตถุประสงค์ระดับองค์กรขึ้นในการจัดทำแผนประจำปี แต่ละหน่วยงานดำเนินการกำหนดวัตถุประสงค์ของหน่วยงานให้สอดคล้องกับวัตถุประสงค์ที่องค์กรได้กำหนดไว้ และการกำหนดวัตถุประสงค์ของกระบวนการและโครงการต่างๆ ต้องคำนึงถึงความสอดคล้องกับวัตถุประสงค์ของหน่วยงานและระดับองค์กร

วัตถุประสงค์อาจเกี่ยวข้องกับองค์การในหลายๆ ด้าน รวมไปถึง ทรัพยากร เทคโนโลยีสารสนเทศ ผลการดำเนินงาน ด้านการปฏิบัติการ เป็นต้น



รูปภาพที่ 6 การกำหนดวัตถุประสงค์/เป้าหมาย

กระบวนการที่ 3 การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยง คือ การระบุเหตุการณ์ความเสี่ยงหรือความไม่แน่นอนที่อาจเกิดขึ้น โดยพิจารณาจากปัจจัยทั้งภายในและภายนอกสำนักงาน ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของสำนักงาน

การค้นหาค่าความเสี่ยงและสาเหตุหรือปัจจัยของความเสี่ยงในงาน โครงการ กิจกรรม หรือกระบวนการปฏิบัติงาน เป็นการพิจารณาว่ามีสิ่งใดหรือเหตุการณ์ใดที่อาจจะเป็นอุปสรรคและทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์หรือเป้าหมาย ทั้งในระดับองค์กรและระดับกิจกรรม

กระบวนการที่มีความสำคัญและเป็นงานหลักขององค์กร โดยศึกษาจากข้อมูลสถิติของความเสี่ยงที่เคยเกิดขึ้น การสำรวจในปัจจุบันหรือคาดว่าจะเกิดขึ้นในอนาคต จากวิธีการดังนี้

- 1) การระดมความคิดเห็นของบุคลากรภายในองค์กร
- 2) การแจกแบบสอบถามด้านความตระหนัก เรื่องการบริหารความเสี่ยง
- 3) การจัดอบรมบุคลากรเกี่ยวกับการบริหารความเสี่ยง

การประเมินความเสี่ยง (Risk Assessment) คือ กระบวนการในการระบุระดับความรุนแรงและการจัดลำดับความสำคัญของปัจจัยเสี่ยงโดยประเมินจากโอกาสที่จะเกิดขึ้น (Likelihood) และผลกระทบ (Impact) ที่จะเกิดขึ้น

โอกาส (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงขึ้น

ผลกระทบ (Impact) หมายถึง ความรุนแรงของความเสียหาย หรือผลที่เกิดขึ้นตามมาจากผลสืบเนื่องของเหตุการณ์ ความเสี่ยง

ระดับความเสี่ยง (Degree of risk) หมายถึง สถานะของความเสี่ยงที่ได้รับจากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่ง เป็น 5 ระดับ สูงมาก สูง ปานกลาง น้อยและน้อยมาก

กระบวนการที่ 4 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงควรพิจารณาถึงความไม่แน่นอนของเหตุการณ์หรือเงื่อนไขต่างๆ ใน 2 ปัจจัย ดังต่อไปนี้

- ผลกระทบของความเสี่ยง
- โอกาสที่จะเกิดความเสี่ยง

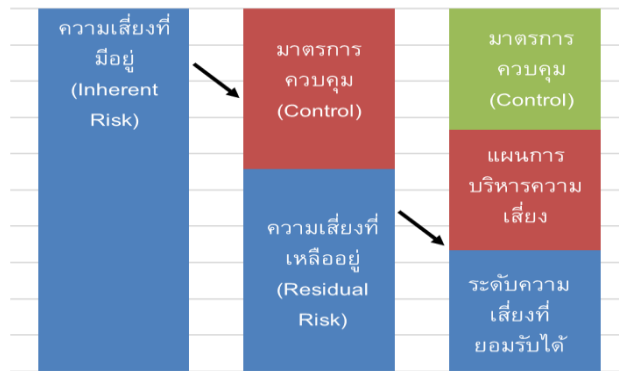
โอกาส (Likelihood)

การประเมินโอกาสเกิดของความเสี่ยง โดยทั่วไปการหาข้อมูลมาทำการสนับสนุนการประมาณการที่ถูกต้องเป็นไปได้ยาก ในกรณีที่สามารถหาข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความล้มเหลวหรือความถี่ที่เกิดขึ้นในอดีต ต้องมีความมั่นใจในฐานข้อมูลดังกล่าวว่าสามารถบ่งชี้ถึงความเป็นไปได้ของเหตุการณ์ในอนาคตได้

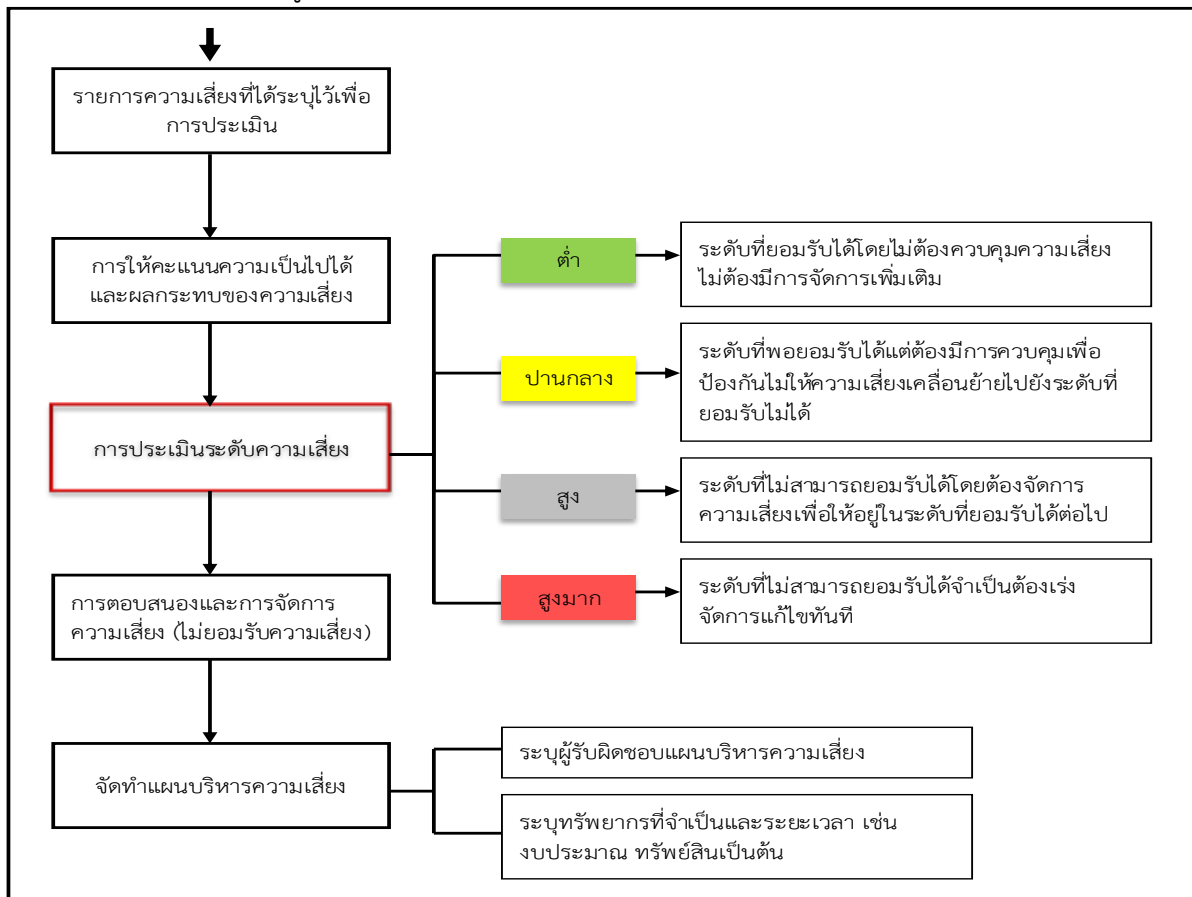
ผลกระทบ (Impact)

การประเมินความเสี่ยงควรพิจารณาถึงผลกระทบทั้งทางด้านการเงิน และที่ไม่ใช่ทางด้านการเงิน ตัวอย่างเช่น ผลกระทบสามารถวัดได้ในเชิงของการสูญเสียทางการเงินทั้งทางตรงและทางอ้อม การวัดผลการดำเนินงานที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น ความพึงพอใจของผู้มีส่วนได้ส่วนเสีย สภาพแวดล้อมและสังคม เป็นต้น

หลังจากได้ระบุความเสี่ยงที่อาจเกิดขึ้นแล้วในขั้นตอนที่ 3 ขั้นตอนต่อไป คือการประเมินความเสี่ยง ซึ่งเป็นการคาดคะเนโอกาสและผลกระทบที่จะเกิดขึ้นจากความเสี่ยงนั้น ๆ และประเมินว่าความเสี่ยงที่จะเกิดขึ้นนั้นมี ความรุนแรงอยู่ในระดับใด เพื่อจะได้นำมาจัดลำดับความสำคัญโดยในการประเมินความเสี่ยงจะทำการประเมินระดับความเสี่ยงก่อนการบริหารจัดการความเสี่ยง (Inherent Risk) และประเมินระดับความเสี่ยงที่เปลี่ยนแปลง หลังการควบคุม/การบริหารจัดการที่มีอยู่ (Residual Risk) ซึ่งหากความเสี่ยงยังคงสูงกว่าระดับที่ยอมรับได้ ดังแสดงในรูปภาพที่ 4-8 และขั้นตอนการประเมินในรูปภาพที่ 7-12



รูปภาพที่ 7 ความเสี่ยงก่อน/หลังการบริหารจัดการความเสี่ยง



รูปภาพที่ 8 ขั้นตอนการประเมินความเสี่ยง

การประเมินความเสี่ยงจะพิจารณาจากองค์ประกอบ 2 ประการ ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) การนำองค์ประกอบทั้งสองมาพิจารณาร่วมกันจะทำให้ทราบถึงระดับความเสี่ยง (Level of Risk) ซึ่งเป็นตัวชี้วัดความสำคัญของความเสี่ยงนั้น แสดงถึงระดับความสำคัญในการบริหารความเสี่ยง โดยค่าระดับความเสี่ยงได้จากการนำโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงมาพิจารณาร่วมกัน ดังนี้

$$\text{ระดับความเสี่ยง (R)} = \text{ระดับโอกาสที่จะเกิดความเสี่ยง (L)} \times \text{ระดับผลกระทบที่เกิดขึ้น (I)}$$

ตารางการประเมินระดับคะแนนความเสี่ยง (Risk Assessment Matrix)

Risk Assessment Matrix			ความเป็นไปได้				
			ต่ำมาก/ น้อยมาก	ต่ำ/น้อย	ปานกลาง	สูง/บ่อย	สูงมาก/ บ่อยมาก
			1	2	3	4	5
ผลกระทบ / ความรุนแรง (I)	สูงมาก/หายนะ	5	5 (5×1)	10 (5×2)	15 (5×3)	20 (5×4)	25 (5×5)
	สูง/วิกฤต	4	4 (4×1)	8 (4×2)	12 (4×3)	16 (4×4)	20 (4×5)
	ปานกลาง	3	3 (3×1)	6 (3×2)	9 (3×3)	12 (3×4)	15 (3×5)
	ต่ำ / น้อย	2	2 (2×1)	4 (2×2)	6 (2×3)	8 (2×4)	10 (2×5)
	ไม่เป็นสาระสำคัญ / น้อยมาก	1	1 (1×1)	2 (1×2)	3 (1×3)	4 (1×4)	5 (1×5)
			ระดับของความเสี่ยง (L)				

จาก Risk Assessment Matrix นำรายการความเสี่ยงของแต่ละระดับความเสี่ยงที่ได้จัดเรียงลำดับไว้ (Risk Ranking) มาวิเคราะห์เปรียบเทียบกับเกณฑ์ความสามารถในการยอมรับความเสี่ยง (Criteria for Acceptability Risk)

การกำหนดมาตรการตอบสนองต่อความเสี่ยงจะเป็นการกำหนดวิธีการจัดการความเสี่ยงที่เกิดขึ้นให้ลดลง โดยนำระดับความเสี่ยงมากำหนดลงในแผนผังเมทริกซ์แสดงระดับความเสี่ยง (Risk Matrix) ซึ่งแบ่งระดับของความเสี่ยง ได้ดังนี้

เกณฑ์ความสามารถในการยอมรับความเสี่ยง

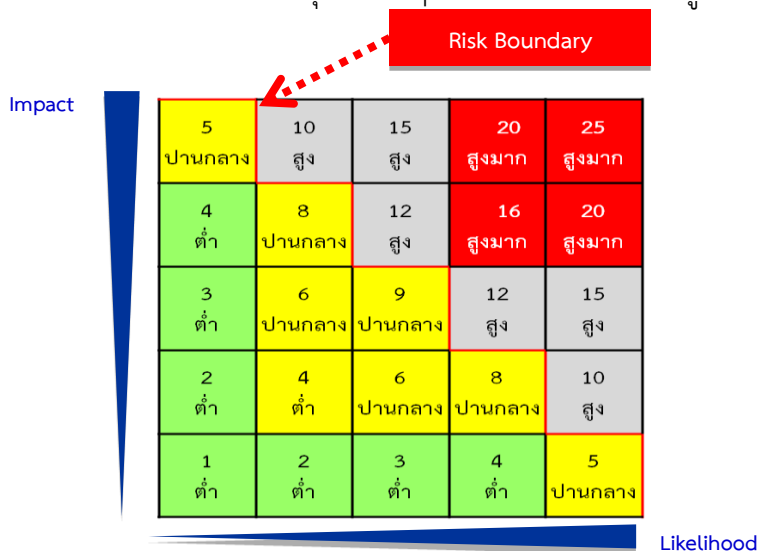
ระดับความเสี่ยง	ระดับคะแนน	ความหมาย
สูงมาก (VH) (สีแดง)	16-25	Intolerable or Immediate Attention Require/High Risk - ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
สูง (H) (สีเทา)	10-15	Intolerable or Attention Required/High Risk - ระดับที่ไม่สามารถยอมรับได้ - โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
ปานกลาง (M) (สีเหลือง)	5-9	Tolerable but caution or Management Discretion/Medium Risk - ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
ต่ำ (L) (สีเขียว)	1-4	Acceptable or limited Focus - ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยงไม่ต้องมีการจัดการเพิ่มเติม

** ระดับความเสี่ยงปานกลาง การควบคุมความเสี่ยงต้องมีการติดตามผลและประเมินผลต่อความเสี่ยงที่เกิดขึ้นจริงอย่างมีประสิทธิภาพ/ประสิทธิผล และมีผู้รับผิดชอบโดยตรง เช่น มีแผนปฏิบัติ คู่มือปฏิบัติ มีการมอบหมายที่ชัดเจนฯ

- **ความเสี่ยงที่อยู่ในโซนสีแดง** (โอกาส X ผลกระทบ ระดับคะแนนความเสี่ยงที่อยู่ระหว่าง 16-25 คะแนน) จะต้องมีการกำหนดมาตรการในการจัดการความเสี่ยงเพิ่มเติมโดยทันที โดยใช้กลยุทธ์การลด/ควบคุมความเสี่ยง (Treat) กระจาย/โอนความเสี่ยง (Transfer) หรือหลีกเลี่ยงความเสี่ยง (Terminate) พร้อมกำหนดผู้รับผิดชอบและกรอบระยะเวลาที่ชัดเจน
- **ความเสี่ยงที่อยู่ในโซนสีเทา** (โอกาส X ผลกระทบ ระดับคะแนนความเสี่ยงที่อยู่ระหว่าง 5-9 คะแนน) เป็นความเสี่ยงที่อยู่ในระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยงเพื่ออยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์การลด/ควบคุมความเสี่ยง (Treat) กระจาย/โอนความเสี่ยง (Transfer) หรือหลีกเลี่ยงความเสี่ยง (Terminate) พร้อมกำหนดผู้รับผิดชอบและกรอบระยะเวลาที่ชัดเจน โดยระดับความสำคัญในการดำเนินงานให้น้อยกว่าโซนสีแดง
- **ความเสี่ยงที่อยู่ในโซนสีเหลือง** (โอกาส X ผลกระทบ ระดับคะแนนความเสี่ยงที่อยู่ระหว่าง 10-15 คะแนน) เป็นความเสี่ยงที่อยู่ในระดับพอยอมรับได้ แต่ต้องมีการควบคุม โดยกำหนดผู้รับผิดชอบและกรอบระยะเวลาที่ชัดเจน ทั้งนี้ต้องมีการปฏิบัติตามรับการควบคุมภายใน อย่างเคร่งครัด เพื่อไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่รับไม่ได้
- **ความเสี่ยงที่อยู่ในโซนสีเขียว** (โอกาส X ผลกระทบ ระดับคะแนนความเสี่ยงที่อยู่ระหว่าง 1-4 คะแนน) เป็นความเสี่ยงที่อยู่ในระดับที่ยอมรับได้ ไม่จำเป็นต้องมีมาตรการจัดการเพิ่มเติมใดๆ กับความเสี่ยงที่เกิดขึ้น ในทางกลับกันอาจมีการทบทวนระบบควบคุมภายในใหม่เพื่อผ่อนคลายการควบคุมได้ระดับหนึ่ง

การกำหนดขอบเขตของระดับความเสี่ยง (Risk Boundary)

หมายถึง ขอบเขตของคะแนนระดับความเสี่ยงที่องค์กรยอมรับได้ คือ ระดับคะแนนตั้งแต่ 1-9 กับ ความเสี่ยงที่มีระดับคะแนน 10-25 คะแนนระดับความรุนแรง Impact x Likelihood ดังรูปภาพที่ 9



รูปภาพที่ 9 ขอบเขตของระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Boundary)

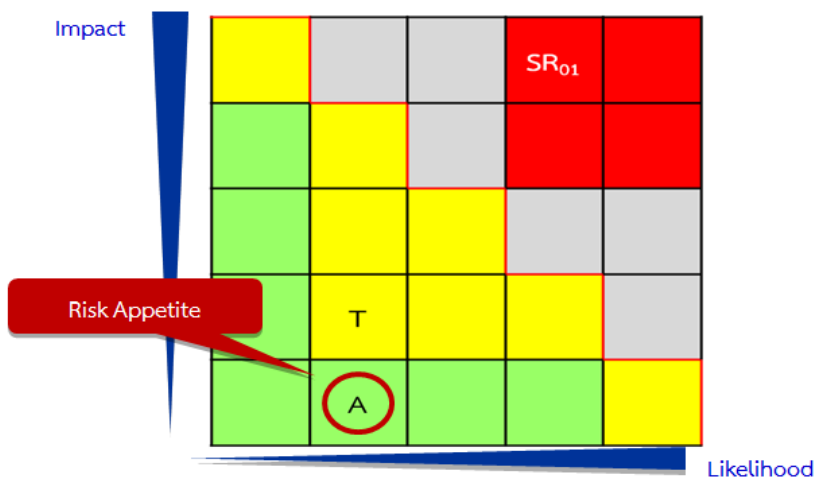
การวิเคราะห์ระดับความเสี่ยง ความเสี่ยงที่ยอมรับได้ (Risk Appetite) และช่วงของความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ (Risk Tolerance)

การกำหนดความเสี่ยงที่ยอมรับได้ถือเป็นส่วนหนึ่งในการกำหนดกลยุทธ์การดำเนินงานขององค์กรโดยรวม เนื่องจากการดำเนินงานต่าง ๆ ขององค์กรมีความเสี่ยงเป็นอุปสรรคที่จะทำให้ไม่บรรลุเป้าหมายที่ได้

กำหนดไว้ หากมีความเสี่ยงที่เกิดขึ้นในระดับหนึ่งโดยองค์กรยังสามารถดำเนินงานให้บรรลุเป้าหมายที่กำหนดได้ ระดับความเสี่ยงที่เกิดขึ้นนั้นเรียกว่า ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

ความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ค่าความเสี่ยงโดยรวมที่องค์กรยอมรับเพื่อให้องค์กรบรรลุเป้าหมาย ซึ่งความเสี่ยงที่องค์กรยอมรับได้จะระบุเป็นเป้าหมายค่าเดียวหรือระบุเป็นช่วงก็ได้ ขึ้นอยู่กับความเหมาะสมของแต่ละปัจจัยเสี่ยง เป็นระดับของความเสี่ยงที่คณะกรรมการหรือผู้บริหารยอมรับได้ในการดำเนินการ เพื่อให้บรรลุวัตถุประสงค์หรือนโยบายขององค์กร โดยคณะกรรมการหรือผู้บริหารควรกำหนดยุทธศาสตร์ขององค์กรที่สอดคล้องกับความเสี่ยงที่ยอมรับได้ หรือความเสี่ยงที่องค์กรยอมรับได้ เป็นระดับความเสี่ยงที่ยอมรับได้ เพื่อสร้างมูลค่า (Value) ให้กับองค์กร โดยวัดระดับเป็นสูง กลาง ต่ำ หรืออาจวัดเป็นเชิงปริมาณ

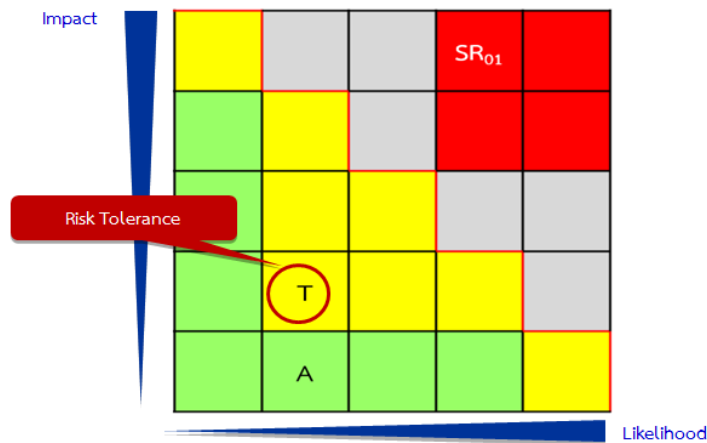
การทำ Risk Appetite ของแต่ละความเสี่ยงสามารถหาได้เมื่อทราบถึงปริมาณความเสี่ยงที่เกิดขึ้นแล้วว่าความเสี่ยงอยู่ในระดับสูงหรือสูงมาก จำเป็นต้องลดความเสี่ยงนั้น อ.ส.พ. พิจารณาว่าจะลดความเสี่ยงนั้นให้ต่ำที่สุดในระดับใดที่องค์กรสามารถยอมรับให้มีความเสี่ยงอยู่ในการดำเนินงานของ อ.ส.พ. ในกรณีที่ไม่สามารถกำจัดความเสี่ยงนั้นได้ กล่าวโดยสรุปคือ Risk Appetite คือระดับความเสี่ยงที่มีอยู่ของ อ.ส.พ. ที่ยอมให้เกิดขึ้นแต่จะต้องไม่ทำให้เป้าหมายหรือวัตถุประสงค์ของการดำเนินขององค์กรได้รับความเสียหายหรือไม่บรรลุวัตถุประสงค์



รูปภาพที่ 10 ตำแหน่งความเสี่ยงที่ยอมรับได้ (Risk Appetite)

ช่วงของความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ช่วงของความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ เป็นระดับของความเบี่ยงเบนของผลลัพธ์ ออกจากเป้าหมายของวัตถุประสงค์ การดำเนินงานที่อยู่ภายในระดับของความเสี่ยงที่ยอมรับได้ จะช่วยเป็นหลักประกันให้แก่ฝ่ายบริหารได้ว่า มีความเป็นไปได้สูงที่องค์กรจะสามารถดำเนินการ และบรรลุวัตถุประสงค์ได้ ซึ่งส่วนมากจะอยู่ในระดับสูงกว่า Risk Appetite

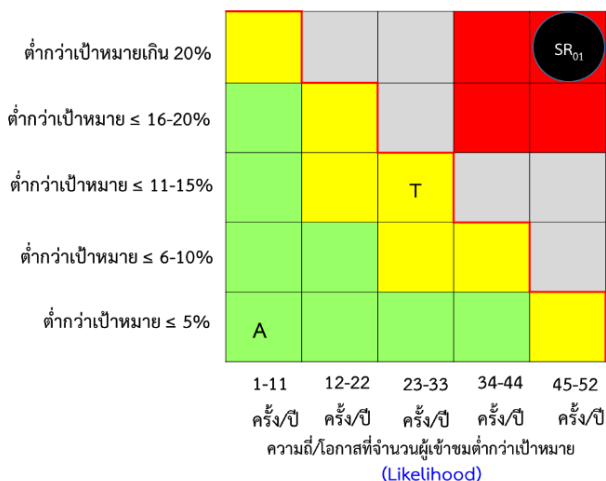
Risk Tolerance เป็นเครื่องมือในการกำกับผลดำเนินงานในมุมมองของการบรรลุผลสำเร็จตามวัตถุประสงค์ ภายใต้ความเสี่ยงที่ทำให้เกิดค่าเบี่ยงเบนของผลดำเนินงานจริงให้ต่ำกว่าค่าเป้าหมายในเกณฑ์ที่กิจการยังพอยอมรับได้



รูปภาพที่ 11 ตำแหน่งช่วงของความเป็ยงเบนของความเสี่ยงที่ยอมรับได้ (Risk Tolerance)

สถานภาพปัจจัยเสี่ยง/ผลการดำเนินงานที่ผ่านมา คือ ตำแหน่งสถานภาพของการประเมินความเสี่ยงในแต่ละปัจจัยเสี่ยงก่อน *สถานะภาพปัจจัยเสี่ยง* หมายถึง สถานภาพที่ อ.ส.พ. ประเมินว่าอยู่ในระดับใดของการทำงาน หากอยู่ในโซนที่เกินระดับคะแนน (Impact × Likelihood) 10 หรือระดับคะแนนเกิน 10 ในโซนสีเทา และสีแดง อ.ส.พ. จะต้องทำการบริหาร หรือจัดการความเสี่ยง หากมีระดับคะแนน (Impact × Likelihood) ตั้งแต่ 9 คะแนนลงมา ปัจจัยเสี่ยงนั้นก็อยู่ในระดับที่ต้องทำการเฝ้าระวัง โดยไม่ต้องมีการบริหารความเสี่ยงก็ได้

ร้อยละที่จำนวนผู้เข้าชมต่ำกว่าเป้าหมาย



รูปภาพที่ 12 ตัวอย่างตำแหน่งสถานภาพปัจจัยเสี่ยง /ผลการดำเนินงานที่ผ่านมา

กระบวนการที่ 5 การจัดการความเสี่ยง (Risk Response)

การจัดการความเสี่ยงและการจัดทำแผนบริหารความเสี่ยงระบุแนวทางที่เหมาะสมในการตอบสนองต่อความเสี่ยง พิจารณาทางเลือกโดยคำนึงถึงความเสี่ยงที่ยอมรับได้และต้นทุน (Cost) กับประโยชน์ (Benefit) ที่ได้รับ การเลือกการตอบสนองต่อความเสี่ยงขึ้นอยู่กับผลการประเมินความเสี่ยงโดยรวมขององค์กร

การจัดการความเสี่ยง ในการจัดการความเสี่ยงจะต้องวิเคราะห์ถึงสาเหตุของความเสี่ยงในแต่ละประเด็น เพื่อนำไปสู่การหามาตรการจัดการกับปัจจัยความเสี่ยงให้ตรงจุดโดยการเลือกรายการความเสี่ยงจาก Risk Assessment Matrix ที่มีความสำคัญที่สุดมาดำเนินการก่อน การจัดการความเสี่ยง คือ การดำเนินการเพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยวิธีแนวทางในการจัดการบริหารความเสี่ยงทฤษฎีการบริหารความเสี่ยง (4T'Strategies: 4Ts) ได้แก่ Terminate, Transfer, Treat, Take

1) Terminate - การหลีกเลี่ยง/กำจัดความเสี่ยง (Risk Avoidance) : ไม่ยอมรับความเสี่ยง เป็นการกำจัดความเสี่ยงออกไปหรือหลีกเลี่ยงความเสี่ยง เนื่องจากมีโอกาสเกิดขึ้นสูงและมีผลกระทบสูง เช่น

- เปลี่ยนวัตถุประสงค์
- หยุดดำเนินกิจการ/ระงับ/ยกเลิก
- จุดขึ้นตอนที่ไม่น่าเป็นและจะนำมาซึ่งความเสี่ยง
- ปรับเปลี่ยนรูปแบบการทำงาน หรือลดขอบเขตการดำเนินการ
- ไม่ดำเนินการกิจกรรมนั้น ๆ เมื่อวิเคราะห์ความเสี่ยงแล้วอยู่ในระดับไม่ยอมรับความเสี่ยง เช่น การลงทุนในโครงการขนาดใหญ่ เป็นต้น

ข้อเสีย ของการหลีกเลี่ยงความเสี่ยง คืออาจส่งผลกระทบต่อให้เกิดการเปลี่ยนแปลงในแผนงานขององค์กรมากจนเกินไป จนไม่สามารถมุ่งไปสู่เป้าหมายที่วางไว้ได้

2) Transfer – การถ่ายโอน/การกระจายความเสี่ยง (Risk Sharing/Spreading): เป็นการลดโอกาสที่จะเกิดความเสี่ยง และ/ หรือลดผลกระทบที่จะเกิดขึ้นจากความเสี่ยง โดยการถ่ายโอนหรือแบ่งภาระบางส่วนให้ผู้อื่นรับผิดชอบ เช่น

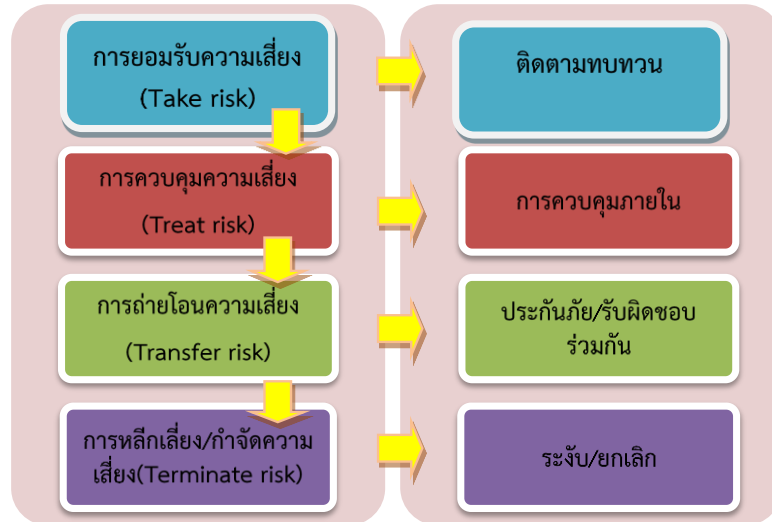
- การทำประกัน (Insurance) คือการจ่ายเงินเพื่อป้องกันตนเองและสินทรัพย์จากเหตุการณ์ที่ไม่คาดคิด เป็นการโอนความเสี่ยงไปยังบริษัทประกัน เช่น การทำประกันภัย ประกันชีวิต ประกันอัตราแลกเปลี่ยน เป็นต้น
- การทำสัญญา (Contracts) คือการทำข้อตกลงต่าง ๆ ทั้งในปัจจุบันและอนาคต เช่น การทำสัญญาซื้อขายล่วงหน้า การจัดจ้างหน่วยงานอื่นให้ดำเนินการแทน
- การรับประกัน (Warranties) ผู้ขายให้สัญญากับผู้ซื้อว่าสินค้าจะสามารถใช้งานได้ตามคุณสมบัติที่ระบุไว้ภายในระยะเวลาที่กำหนด หากไม่เป็นไปตามสัญญาผู้ขายพร้อมที่จะรับผิดชอบต่อสิ่งที่ตกลงกัน จึงเป็นลักษณะของการแบ่งปันความเสี่ยง
- การทำสำเนาเอกสารไว้หลายชุด
- การกระจายที่เก็บทรัพย์สินมีค่า
- การจ้างบุคคลภายนอกดำเนินการแทน ฯลฯ

3) Treat – การลด/การควบคุมความเสี่ยง (Risk Reduction/Control): ดำเนินการเพิ่มเติมเพื่อลดโอกาสที่อาจเกิดขึ้นหรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยการเพิ่มเติมหรือเปลี่ยนแปลงขั้นตอนบางส่วนของกิจกรรมหรือโครงการที่นำไปสู่เหตุการณ์ที่เป็นความเสี่ยง ลดความน่าจะเป็นที่เหตุการณ์ที่เป็นความเสี่ยงจะเกิดขึ้น และลดระดับความรุนแรงของผลกระทบเมื่อเหตุการณ์ที่เป็นความเสี่ยงเกิดขึ้น ได้แก่ การหามาตรการในการป้องกันความเสี่ยงอย่างเต็มรูปแบบ เช่น การจัดซื้ออุปกรณ์เพื่อป้องกันอันตรายจากการทำงาน หรือการจัดหาอุปกรณ์เพิ่มเติมจากเดิมการปรับปรุงแก้ไขกระบวนการงาน การจัดทำแผนฉุกเฉิน การจัดทำมาตรฐานความปลอดภัย การฝึกอบรมบุคลากรให้มีความรู้เพียงพอ การกำหนดผู้จัดจ้างและผู้มอบงานให้แยกออกจากกัน การสำรองข้อมูลเป็นระยะ การมี Server สำรอง เป็นต้น

4) Take - การยอมรับความเสี่ยง (Risk Acceptance): เป็นการยอมรับให้ความเสี่ยงเกิดขึ้น กลยุทธ์นี้จะไม่มีการดำเนินการใดเพื่อลดโอกาสหรือผลกระทบเนื่องจากระดับความเสี่ยงที่เหลือน้อยอยู่ในระดับต่ำ หรืออยู่ในระดับที่ยอมรับได้ หรือมีค่าใช้จ่ายในการบริหารจัดการความเสี่ยงสูงกว่าผลลัพธ์ที่จะได้ แต่ควรมีมาตรการติดตามอย่างใกล้ชิดเพื่อรองรับผลที่จะเกิดขึ้น

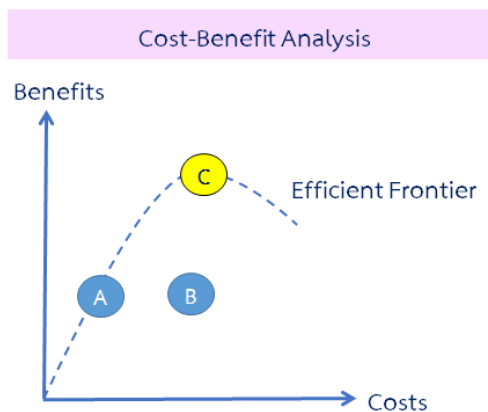
- ตั้งใจที่จะดำเนินการต่อไป
- ยอมรับทั้งหมด
- กำหนดรางวัล/ เป้าหมายความเสียหาย และระดับการยอมรับ

- กำหนด และติดตามตัวบ่งชี้ความเสี่ยงที่สำคัญ
- คิตรายการสูงขึ้น
- กิจกรรมการตรวจสอบและติดตาม
- จัดหาเงินทุนสำรองเพื่อรองรับผลที่อาจเกิดขึ้น
- จัดเตรียมแผนรองรับการเสื่อมถอย



รูปภาพที่ 13 แผนผังวิธีการจัดการความเสี่ยง นำทฤษฎีการบริหารความเสี่ยง (4Ts) มาควบคุมจัดการได้

การตัดสินใจเลือกกลยุทธ์ในการบริหารจัดการความเสี่ยงจะต้องคำนึงถึงปัจจัยเสี่ยงซึ่งเป็นสาเหตุทำให้เกิดความเสี่ยง ที่มาของสาเหตุ ผลกระทบ เลือกวิธีการจัดการความเสี่ยง โดยทำการวิเคราะห์ต้นทุนและผลประโยชน์ (Cost – Benefit Analysis) เพื่อเปรียบเทียบกันในแต่ละทางเลือกในการบริหารความเสี่ยง เพื่อนำไปสู่การตัดสินใจเลือกทางเลือกในการบริหารความเสี่ยงที่ดีที่สุด และเกิดความคุ้มค่าในการดำเนินโครงการหรือกิจกรรมในทางเลือกนั้น



รูปภาพที่ 14 การวิเคราะห์ต้นทุนและผลประโยชน์ภายใต้ข้อจำกัดให้เกิดประสิทธิภาพสูงสุด

Costs หมายถึง การประมาณการต้นทุน/ค่าใช้จ่ายในการดำเนินการแผนบริหารความเสี่ยง

Benefits หมายถึง การประมาณการมูลค่าของผลกระทบจากความเสียหายที่ลดลง เมื่อเทียบกับไม่ได้ดำเนินการใด ๆ (Ability to Mitigate Overall Risks)

Efficient Frontier หมายถึง เส้นประสิทธิภาพสูงสุด โดยมีจุด C เป็นจุดที่เหมาะสมที่สุด

เส้นปะ หมายถึง ข้อจำกัดงบประมาณ (Budget Constraint)

Source: Enterprise Risk Management, John Fraser and Betty J. Simkins, Editors

เมื่อเลือกกลยุทธ์ในการจัดการความเสี่ยงที่เหมาะสมได้แล้ว ส่วนงานที่เกี่ยวข้องกับความเสี่ยงนั้นๆ จะต้องดำเนินการจัดทำแผนบริหารความเสี่ยง เพื่อให้สามารถติดตามและประเมินผลการจัดการความเสี่ยงได้

การจัดการความเสี่ยง ต้องมีการนำแผนผังความเสี่ยง (Risk Assessment Matrix) มาพิจารณาจัดลำดับค่าความเสี่ยงจากสูงมากถึงต่ำ โดยเลือกรายการความเสี่ยงที่มีค่าระดับความเสี่ยงสูงมาก/สูง ซึ่งอยู่ในเกณฑ์ความเสี่ยงที่ยอมรับไม่ได้มาจัดการความเสี่ยงต่อไป

การจัดทำแผนบริหารความเสี่ยงหลังจากที่ได้ประเมินความเสี่ยงแล้ว ผู้ประเมินจะเลือกวิธีการจัดการกับความเสี่ยงที่เหมาะสมและดำเนินการจัดทำเป็นแผนบริหารความเสี่ยง เพื่อให้สามารถติดตามและประเมินผลการจัดการความเสี่ยงได้ โดยแผนบริหารความเสี่ยงมีองค์ประกอบดังนี้

- วิธีการดำเนินงาน/มาตรการควบคุมความเสี่ยง
- หน่วยงานผู้รับผิดชอบ
- กำหนดระยะเวลาดำเนินการของแผนบริหารความเสี่ยง
- วิธีประเมินผล/วิธีวัดตัวชี้วัด

กระบวนการที่ 6 กิจกรรมเพื่อการควบคุม (Control Activities)

หมายถึง นโยบายและกระบวนการปฏิบัติงานที่ทำให้มั่นใจว่าได้มีการจัดการความเสี่ยงอย่างเหมาะสม กิจกรรมการควบคุมเกิดขึ้นในทุกส่วนขององค์กร และกำหนดผู้รับผิดชอบที่ชัดเจน ตัวอย่าง กิจกรรมการควบคุม (Control Activities) ซึ่งรวมถึง

- การกำหนดนโยบายและวิธีปฏิบัติงาน เช่น การจัดทำคู่มือปฏิบัติงาน
- การอนุมัติ/ รับรอง/ ให้ความเห็นชอบงาน
- การสอบทานผลการปฏิบัติงาน
- การรักษาความปลอดภัย/ การเข้าถึงข้อมูลระบบเทคโนโลยีสารสนเทศ
- การแบ่งแยกหน้าที่ความรับผิดชอบงาน/การมอบหมายงาน

องค์การสวนพฤกษศาสตร์ (อ.ส.พ.) ได้มีการกำหนดกิจกรรมควบคุมอย่างชัดเจน โดยมีการจัดทำนโยบายและวิธีปฏิบัติงานบริหารความเสี่ยงตามคู่มือบริหารความเสี่ยง กำหนดผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยง โดยในการบริหารความเสี่ยงระดับปฏิบัติการ ผู้อำนวยการฝ่าย/ สำนัก เป็นผู้พิจารณา กำหนดความรับผิดชอบ ส่วนการบริหารความเสี่ยงในระดับองค์กร ผู้อำนวยการ จะเป็นผู้กำหนดว่าส่วนงานใดเป็นผู้รับผิดชอบหลัก มีการกำหนดระยะเวลาดำเนินการแล้วเสร็จและมีการรายงานผลการปฏิบัติตามแผนบริหารความเสี่ยงเพื่อเป็นการสอบทานเป็นระยะด้วย

กระบวนการที่ 7 สารสนเทศและการสื่อสาร (information and communication)

หมายถึง การจัดให้มีการสื่อสารและระบบสารสนเทศความเสี่ยงที่ดี เพื่อให้มั่นใจว่าผู้บริหาร และพนักงานทุกคนเข้าใจกระบวนการและบทบาทหน้าที่ความรับผิดชอบของตนเองเกี่ยวกับการบริหารความเสี่ยง

สารสนเทศและการสื่อสารที่ดีจะเกิดขึ้นได้ ต้องมีข้อมูลที่เกี่ยวข้องกับการดำเนินงานนั้นได้มีการบ่งชี้ รวบรวมและชี้แจงให้แก่บุคคลที่ควรทราบ โดยผ่านทางรูปแบบและเวลาการสื่อสารที่เหมาะสมข้อมูลที่มีประโยชน์ต่อการตัดสินใจ การบริหารจัดการ และการปฏิบัติงานนั้น อาจเป็นได้ทั้งข้อมูลที่เกี่ยวข้องกับการดำเนินงาน การเงิน และการปฏิบัติตามกฎระเบียบต่างๆ โดยแหล่งข้อมูลอาจมาจากภายในหรือภายนอกองค์กร

กระบวนการที่ 8 การติดตามและประเมินผล (Monitoring)

จำเป็นอย่างยิ่งที่ต้องมีกลไกในการติดตามและประเมินผล เพื่อให้มั่นใจว่าได้มีการปฏิบัติการควบคุมภายในนั้นอย่างสม่ำเสมอ และการปฏิบัตินั้นยังมีความเหมาะสมกับลักษณะการดำเนินงานและการเปลี่ยนแปลงที่เกิดขึ้น เพราะอย่าลืมว่า การเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นอาจมีผลกระทบต่อความเสี่ยงในการดำเนินงาน และความเสี่ยงที่เปลี่ยนแปลงไป

1) **การติดตามผล** เป็นการติดตามผลภายหลังจากการได้ดำเนินการตามแผนการบริหารความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งสาเหตุของความเสี่ยงที่มีผลต่อความสำเร็จ ความรุนแรงของผลกระทบ วิธีการบริหารจัดการกับความเสี่ยง รวมถึงค่าใช้จ่ายของการควบคุม มีความเหมาะสมกับสถานการณ์การเปลี่ยนแปลง โดยมีเป้าหมายในการติดตามผลคือ

- เป็นการประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการดำเนินการไปแล้ว ว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่
- เป็นการตรวจสอบความคืบหน้าของมาตรการควบคุมที่มีการทำเพิ่มเติมมาแล้วเสร็จตามกำหนดหรือไม่ สามารถลดโอกาสหรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้หรือไม่
- การรายงานและติดตามผล มีความจำเป็นและมีประโยชน์ต่อการบริหารความเสี่ยงเพราะจะทำให้ทราบว่า
- แผนจัดการความเสี่ยงได้ถูกนำไปใช้อย่างถูกต้องและมีประสิทธิภาพเพียงใด
- ทำให้ทราบถึงข้อผิดพลาดที่อาจเกิดขึ้นหลังจากใช้แผนจัดการความเสี่ยง
- ทำให้สามารถปรับปรุงแก้ไขแผนจัดการความเสี่ยงให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป หรือกรณีที่แผนเดิมไม่มีประสิทธิภาพ
- มีการรายงานต่อผู้บริหารที่ได้รับมอบหมายเป็นรายไตรมาส

2) **การประเมินผล** สามารถแบ่งออกเป็น 2 ลักษณะ คือ

2.1) **การประเมินผลระหว่างการปฏิบัติงาน (Ongoing Monitoring)** โดยจะประเมินผลการปฏิบัติงานตามแผนการบริหารความเสี่ยง เพื่อติดตามว่ากระบวนการต่าง ๆ ได้มีการดำเนินการตามมาตรการ/กิจกรรมควบคุมที่ได้กำหนดไว้หรือไม่ และสามารถลดความเสี่ยงที่เกิดขึ้นหรืออาจจะเกิดขึ้นได้หรือไม่ หรือมีเหตุการณ์/สถานการณ์ความเปลี่ยนแปลงเกิดขึ้นนอกเหนือจากที่ได้คาดการณ์ไว้แล้วนำเสนอคณะกรรมการบริหารความเสี่ยงและผู้บริหาร เพื่อปรับแผนบริหารความเสี่ยงและดำเนินการปรับแก้ไขได้อย่างทันท่วงที โดยความถี่ในการติดตามและประเมินผลจากกิจกรรมควบคุมดำเนินการเป็นรายไตรมาส และในกรณีพิเศษหากพบว่าการเปลี่ยนแปลงที่มีสาระสำคัญอาจจะจัดให้มีการประชุมคณะกรรมการบริหารความเสี่ยงเป็นกรณีพิเศษขึ้นมา

2.2) **การประเมินผลเป็นรายครั้ง (Separate Evaluation)** เป็นการประเมินผลโดยการรายงานเมื่อสิ้นสุดระยะเวลาที่กำหนดไว้ หรือในกรณีพิเศษ การติดตามและประเมินผลอาจจะดำเนินการในลักษณะของการประเมินตนเอง (Self Appraisal) หรืออาจให้บุคคลภายนอกเป็นผู้ประเมิน (Independent Appraisal)

โดยหน่วยงานที่รับผิดชอบบริหารจัดการประเด็นความเสี่ยงใด หน่วยงานนั้นจะเป็นผู้รับผิดชอบในการประเมินประสิทธิภาพการบริหารความเสี่ยงของตนเอง และผู้ตรวจสอบภายในจะเป็นอีกหน่วยงานหนึ่งที่จะทำการติดตามตรวจสอบตามหน้าที่ประจำของแต่ละหน่วยงาน หรืออาจจะทำการตรวจสอบตามคำสั่งของคณะกรรมการตรวจสอบ หรือคณะกรรมการบริหารความเสี่ยง ซึ่งขอบเขตความถี่ในการประเมินจะขึ้นอยู่กับผลการประเมินความเสี่ยง และประสิทธิภาพของการติดตามผลระหว่างการปฏิบัติงาน ในการประเมินคณะกรรมการจะประเมินผลดังนี้

- มีการปฏิบัติตามมาตรการ/กิจกรรมควบคุมที่ได้กำหนดไว้อย่างครบถ้วนสมบูรณ์ หรือไม่
- การปฏิบัติตามกิจกรรมควบคุมนั้น สามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพ และประสิทธิผลหรือไม่
- มีข้อบกพร่องหรือสถานการณ์ใดๆ ที่มีผลกระทบต่อการบริหารความเสี่ยงที่ควรได้รับความสนใจ แก้ไขหรือปรับปรุงให้ดีขึ้นหรือไม่

จากนั้นคณะกรรมการบริหารความเสี่ยง อ.ส.พ. จะเสนอรายงานการประเมินผลการบริหารความเสี่ยงต่อผู้บริหารและคณะกรรมการ อ.ส.พ. เพื่อนำผลการประเมินที่ได้ปรับปรุงการจัดทำระบบบริหารความเสี่ยงในปีต่อไปให้มีประสิทธิภาพ ประสิทธิผลและคุ้มค่ายิ่งขึ้น

2.10 แผนที่ความเสี่ยง (Risk Map)

การดำเนินงานการบริหารความเสี่ยงเป็นการดำเนินงานในระดับองค์กร โดยมีการพิจารณาถึงความสัมพันธ์ของความเสี่ยงและผลกระทบของแต่ละปัจจัยเสี่ยงที่มีระหว่างหน่วยงานต่างๆ ภายในองค์กร ซึ่งสามารถอธิบายได้ด้วยแผนที่ความเสี่ยง (Risk Map)

แผนที่ความเสี่ยง (Risk Map) เป็นเครื่องมือที่ช่วยในการบริหารจัดการความเสี่ยง โดยมีการพิจารณาถึงความสัมพันธ์ (Correlation) ของความเสี่ยงและผลกระทบที่มีระหว่างหน่วยงานต่างๆ ภายในองค์กรและช่วยให้องค์กรสามารถจัดการความเสี่ยงที่ต้นเหตุได้อย่างชัดเจน

องค์ประกอบที่สำคัญของแผนที่ความเสี่ยง (Risk Map)

1) การกำหนดสาเหตุของความเสี่ยง **น้ำหนักของสาเหตุและระดับความรุนแรงของสาเหตุ** การระบุสาเหตุ (Root Cause) ในแต่ละปัจจัยเสี่ยงสามารถระบุเบื้องต้นทั้งหมดของสาเหตุ เมื่อหาความสัมพันธ์จะเห็นสาเหตุร่วม (Common)

2) การวิเคราะห์ความสัมพันธ์ระหว่างปัจจัยเสี่ยงระดับองค์กร และความสัมพันธ์ของสาเหตุ เป็นการพิจารณาถึงความสัมพันธ์ระหว่างปัจจัยเสี่ยงและสาเหตุ โดยพิจารณาจากสาเหตุทางตรงและทางอ้อม

3) การวิเคราะห์ผลกระทบระหว่างปัจจัยเสี่ยงในระดับองค์กร และผลกระทบของสาเหตุ แผนที่ความเสี่ยง (Risk Map) จะต้องมีการประเมินผลกระทบทั้งในเชิงปริมาณและคุณภาพ โดยมีการจับคู่ผลกระทบเพื่อระบุผลกระทบที่จะเกิดขึ้นอย่างชัดเจน

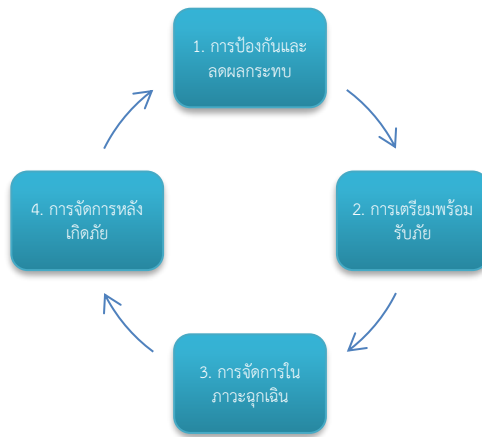
การวิเคราะห์ Risk map เพื่อแสดงความสัมพันธ์กับการกำหนดมาตรการตอบสนองความเสี่ยง (Risk Response) โดยพิจารณาระดับความรุนแรงของสาเหตุ รวมถึงความสัมพันธ์ทั้งแนวดิ่งและข้ามปัจจัยเสี่ยง และมาตรการตอบสนองความเสี่ยง (Risk Response) โดยพิจารณาเพิ่มเติมจากมาตรการควบคุมภายใน

4) การนำ Risk Correlation Map ไปใช้ในการกำหนดแผนการบริหารความเสี่ยง แผนบริหารความเสี่ยงครอบคลุมถึงทุกสาเหตุความเสี่ยงของปัจจัยเสี่ยงนั้นๆ รวมถึงผลกระทบจากปัจจัยเสี่ยงอื่นๆ จะต้องมีแผนกิจกรรมจัดการรองรับ โดยกำหนดผู้รับผิดชอบ โดยแผนบริหารความเสี่ยงต้องครอบคลุมถึงสาเหตุของความเสี่ยงทุกสาเหตุ รวมถึงปัจจัยเสี่ยงหรือสาเหตุของปัจจัยเสี่ยงอื่นที่มีความสัมพันธ์และส่งผลกระทบมายังปัจจัยเสี่ยงนั้นๆ

2.11 การบริหารความต่อเนื่องทางธุรกิจ

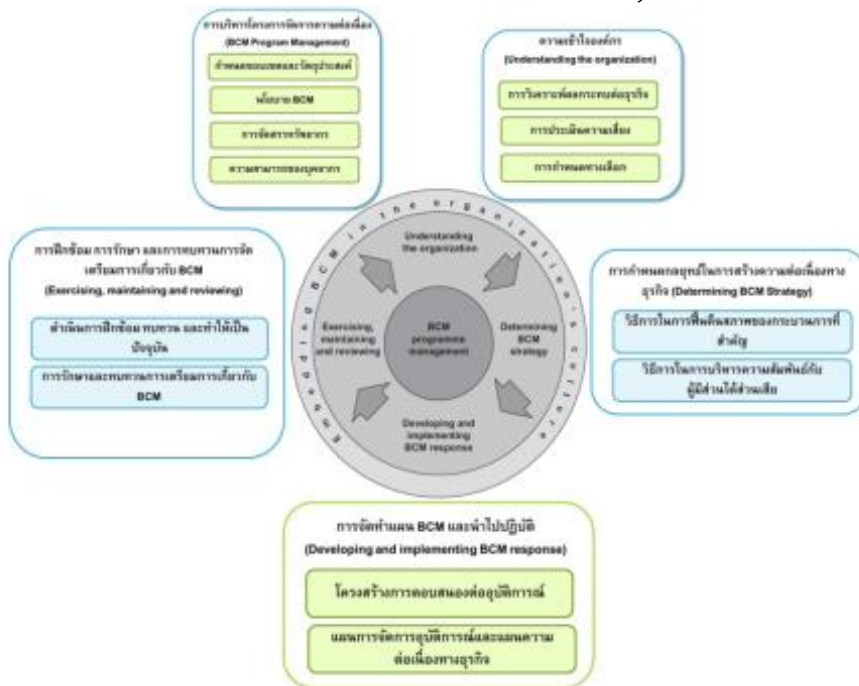
การบริหารความต่อเนื่องทางธุรกิจ หรือ Business Continuity Management (BCM) หมายถึง การบริหารจัดการแบบองค์รวมที่มีการระบุถึงภัยคุกคามที่มีต่อองค์กร รวมถึงผลกระทบของภัยคุกคามนั้นๆ และ ให้แนวทางในการสร้างขีดความสามารถให้องค์กรมีความยืดหยุ่น (Resilience) เพื่อการตอบสนองและปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสียหลัก รวมถึงชื่อเสียง ภาพลักษณ์ และกิจกรรมที่สร้างคุณค่าขององค์กร

การบริหารความต่อเนื่องทางธุรกิจ แบ่งวัฏจักรการบริหารจัดการออกเป็น 4 ขั้นตอน คือ 1) การป้องกันและลดผลกระทบ 2) การเตรียมพร้อมรับภัย 3) การจัดการในภาวะฉุกเฉิน และ 4) การจัดการหลังเกิดภัย ดังนั้น ความรู้ ความเข้าใจ เกี่ยวกับการบริหารความพร้อมต่อสภาวะวิกฤต ตามวัฏจักรข้างต้นเป็นเรื่องจำเป็นทั้งต่อบุคลากรภายในหน่วยงานและประชาชนที่ได้รับผลกระทบต่อสภาวะวิกฤต เพื่อให้เกิดความตระหนัก มีความรอบคอบไม่ตื่นตระหนกต่อสถานการณ์



รูปภาพที่ 15 แผนผังวิธีการจัดการความเสี่ยง นำทฤษฎีการบริหารความเสี่ยง (4Ts) มาควบคุมจัดการได้

การบริหารความต่อเนื่องทางธุรกิจของ อ.ส.พ. ได้อ้างอิงมาตรฐาน Business Continuity Standard (BS25999) ซึ่งกำหนดโดย British Standards Institution : BSI ผลิตภัณฑ์อุตสาหกรรม มอก.22301:2019 โดยมี 6 องค์ประกอบหลัก เป็นวงจรการบริหารความต่อเนื่อง (BCM Life Cycle) ดังนี้



รูปภาพที่ 16 วงจรการบริหารความต่อเนื่อง (BCM Life Cycle)

1) การบริหารโครงการจัดการความต่อเนื่อง (BCM Program Management) โครงการจัดการความต่อเนื่อง ถือเป็นองค์ประกอบหลักและเป็นขั้นตอนแรกของการบริหารความต่อเนื่อง เป็นการจัดทำกรอบนโยบาย BCM โครงสร้าง BCM หน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้อง ตั้งแต่ผู้บริหารระดับสูงลงมาถึงเจ้าหน้าที่ระดับต่างๆ รวมถึงการจัดตั้งทีมงานด้าน BCM การกำหนดตัวชี้วัดผลการดำเนินงานของเจ้าหน้าที่ ขั้นตอนการปรับระดับของเหตุการณ์ (Incident Escalation Process) วิธีการบริหารโครงการจัดการความต่อเนื่อง และการติดตามพร้อมทั้งรายงานความคืบหน้า

2) การศึกษาและทำความเข้าใจองค์กร (Understanding the Organization) การเข้าใจองค์กรเป็นกระบวนการทำความเข้าใจกับหน่วยงาน ซึ่งหมายถึงความรู้และความเข้าใจในสภาพและการดำเนินงานของหน่วยงานว่าจะรับผลกระทบหรือความเสี่ยงอย่างไร ผ่านวิธีการวิเคราะห์ผลกระทบทางธุรกิจ หรือผลกระทบต่อกระบวนการทำงานหรือการให้บริการ (Business Impact Analysis – BIA) และการประเมินความเสี่ยง (Risk Assessment – RA) เพื่อระบุความเร่งด่วนของกิจกรรมต่างๆ และระดับความสามารถที่ต้องการ เพื่อนำไปเป็นข้อมูลในการจัดระดับความสำคัญของกระบวนการ การกำหนดแนวทาง และการกำหนดกลยุทธ์ในข้อต่อไป

3) การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง (Determining BCM strategy) แนวทางในการตอบสนองต่อการหยุดชะงักของการดำเนินงานขององค์กร ได้แก่ กลยุทธ์กู้คืนการดำเนินงาน (Recovery Strategy) ซึ่งเป็นขั้นตอนที่ต้องจัดทำก่อนการพัฒนาและเตรียมการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉิน และกลยุทธ์ด้านการจัดการทรัพยากรที่เหมาะสม ตามข้อมูลที่ได้จากผลกระทบต่อกระบวนการทำงานหรือการให้บริการ (BIA) โดยต้องกำหนดในเรื่อง บุคลากร (People) สถานที่ปฏิบัติงาน (Premise) อุปกรณ์และเครื่องมือ (Equipment) เทคโนโลยี (Technology) ข้อมูล (Information) และผู้ผลิตสินค้าหรือผู้ให้บริการ (Suppliers)

4) การพัฒนาและเตรียมการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉิน (Developing and Implementing BCM Response) ภายหลังจากการกำหนดกลยุทธ์แล้ว จะต้องจัดทำแผนงานเตรียมตอบสนองต่อภาวะฉุกเฉินให้เป็นไปตามกรอบยุทธศาสตร์ที่กำหนดไว้ โดยจัดทำแผนดังต่อไปนี้

4.1) Incident Management Plans (IMP) เพื่อจัดการกับวิกฤติฉุกเฉินที่เกิดขึ้น

4.2) Emergency/Crisis Management Plan (CMP) เพื่อจัดการกับวิกฤติฉุกเฉินที่เกิดขึ้น และผลกระทบที่ขยายไปในวงกว้าง

4.3) Business Continuity Plans (BCP) เพื่อบริหารภารกิจอย่างต่อเนื่อง โดยมุ่งทำขั้นตอนงานที่สำคัญต่อภารกิจและใช้ทรัพยากรหลักอย่างเหมาะสม พร้อมทั้งเตรียมแผนรับผลกระทบจากสถานการณ์

4.4) Recovery Plans (RP) แผนกู้คืนภารกิจหลังภัยพิบัติผ่านพ้นไป

5) การทดสอบ ปรับปรุง และทบทวนแผน (Exercising Maintaining and Reviewing) เป็นขั้นตอนที่สำคัญ เนื่องจากเป็นกระบวนการที่ทำให้แน่ใจได้ว่า BCM ที่ได้จัดทำขึ้นสามารถใช้ได้จริง รวมทั้งเพื่อเตรียมความพร้อม ตลอดจนตรวจสอบความสามารถของบุคลากร และประสิทธิภาพของแผนในการตอบสนองต่อวิกฤติการณ์ โดยรูปแบบการทดสอบอาจมีตั้งแต่ระดับง่ายไปหายาก ดังนี้

- Call Tree คือ การข้อมการแจ้งเหตุฉุกเฉินให้กับสมาชิกทีมงานที่เกี่ยวข้องตามผังรายชื่อทางโทรศัพท์ หรือช่องทางอื่นๆ ที่สามารถติดต่อและยืนยันการรับแจ้งเหตุได้อย่างทันการณ์
- Tabletop Testing คือ การประชุมแลกเปลี่ยนความคิดเห็นกับทุกหน่วยที่เกี่ยวข้อง โดยจำลองโจทย์สถานการณ์ขึ้นมา และทดลองนำแผน BCP มาพิจารณาว่าใช้ตอบโต้แต่ละขั้นตอนนี้ได้หรือไม่
- Simulation คือ การทดสอบโดยจำลองสถานการณ์เสมือนจริง และทดลองนำแผน BCP มาประยุกต์ใช้
- Full BCP Exercise คือ การทดสอบเต็มรูปแบบและใกล้เคียงสถานการณ์จริงมากที่สุด

6) การปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร (Embedding BCM in the Organization's Culture) การทำให้ BCM ผสมกลมกลืนเข้าจนเป็นวัฒนธรรมองค์กร เป็นเรื่องที่ต้องใช้เวลาและจิตวิทยาที่จะทำให้เจ้าหน้าที่ทุกคนได้ซึ่งสามและเข้าใจถึงความสำคัญของ BCM ตลอดจนบทบาทหน้าที่ที่ทุกคนพึงมีเพื่อให้ภารกิจสามารถดำเนินการต่อไปได้ในยามที่เกิดเหตุวิกฤต

2.12 การเตรียมความพร้อมของหน่วยงานต่อสภาวะวิกฤต

ตามมาตรฐาน BS25999 ข้างต้น ควรกำหนดกลุ่มผู้รับผิดชอบและโครงสร้างของการจัดการความต่อเนื่องขององค์กรฯ ดังนี้

ขั้นตอนตามแนวทาง BS25999	ผู้รับผิดชอบ	หมายเหตุ
1) การบริหารโครงการจัดการความต่อเนื่อง	- ผู้อำนวยการ อ.ส.พ. - ผู้อำนวยการสำนัก/ส่วนงานต่างๆ - ประธานคณะกรรมการ และ คณะทำงานฯ	ผู้อำนวยการ อ.ส.พ. หรือกับผู้อำนวยการสำนัก/ส่วนงานต่างๆ และกำหนดโครงสร้าง ผู้รับผิดชอบ และคณะทำงานฯ รวมถึงบทบาทความรับผิดชอบ ในโครงการจัดการความต่อเนื่อง
2) ศึกษาและทำความเข้าใจองค์กร	- ประธานคณะกรรมการและ คณะทำงานฯ - ผู้อำนวยการสำนัก/ส่วนงานต่างๆ	ประธานคณะกรรมการและคณะทำงานฯ จัดการความต่อเนื่อง ร่วมกับผู้อำนวยการสำนัก/ส่วนงานต่างๆ ทำการศึกษาและวิเคราะห์ผลกระทบต่อกิจกรรมการทำงานหรือการให้บริการ (BIA) การประเมินความเสี่ยง/ภัยคุกคาม (RA) และกำหนดแนวทางเลือก
3) กำหนดกลยุทธ์ BCM	- ผู้อำนวยการ อ.ส.พ. - ผู้อำนวยการสำนัก/ส่วนงานต่างๆ - ประธานคณะกรรมการ และ คณะทำงานฯ	ประธานคณะกรรมการ และคณะทำงานจัดการความต่อเนื่อง หรือร่วมกับผู้อำนวยการสำนัก/ส่วนงานต่างๆ และกำหนดแนวทาง/กลยุทธ์นำเสนอต่อผู้อำนวยการ อ.ส.พ. พิจารณาและอนุมัติ
4) พัฒนาและเตรียมการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉิน	- ประธานคณะกรรมการ และ คณะทำงานฯ - ส่วนงานต่างๆ	ประธานคณะกรรมการ และคณะทำงานจัดการความต่อเนื่องร่วมกับตัวแทนจากส่วนงานต่างๆ พัฒนาและจัดทำแผนการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉินและแผนดำเนินธุรกิจอย่างต่อเนื่อง
5) การทดสอบ ปรับปรุง และทบทวนแผน	- ประธานคณะกรรมการ และ คณะทำงานฯ - ผู้บริหารและตัวแทนจากส่วนงานต่างๆ	ประธานคณะกรรมการและคณะทำงานจัดการความต่อเนื่อง ร่วมกับผู้บริหารและตัวแทนจากส่วนงานต่างๆ ดำเนินการทดสอบแผนที่ได้มีการจัดทำขึ้น
6) ปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร	- ผู้อำนวยการ อ.ส.พ. - ผู้บริหารและตัวแทนส่วนงานต่างๆ - ประธานคณะกรรมการ และ คณะทำงานฯ	ประธานคณะกรรมการและคณะทำงานจัดการความต่อเนื่อง ร่วมกับผู้บริหารและตัวแทนจากส่วนงานต่างๆ นำเสนอแนวทางการปลูกฝัง BCM แก่ผู้อำนวยการ อ.ส.พ. และเผยแพร่ให้ทุกหน่วยงานนำไปปฏิบัติ

2.13 ปัจจัยสำคัญการบริหารความเสี่ยงให้ประสบความสำเร็จ

1) การสนับสนุนจากผู้บริหารระดับสูง การปฏิบัติตามกรอบการบริหารความเสี่ยงขององค์กร จะประสบความสำเร็จเพียงใดขึ้นอยู่กับเจตนาธรรมณ์ การสนับสนุน การมีส่วนร่วม และความเป็นผู้นำของผู้บริหารระดับสูงในองค์กร โดยต้องให้ความสำคัญและสนับสนุนให้ทุกคนในองค์กรเข้าใจความสำคัญในคุณค่าของการบริหารความเสี่ยงต่อองค์กร โดยกำหนดให้มีการปฏิบัติ รวมถึงการกำหนดให้ผู้บริหารต้องใช้ข้อมูลเกี่ยวกับความเสี่ยงในการตัดสินใจและบริหารงาน เป็นต้น

2) การใช้คำให้เกิดความเข้าใจแบบเดียวกัน การใช้คำนิยามเกี่ยวกับความเสี่ยง และการบริหารความเสี่ยงแบบเดียวกัน จะทำให้เกิดประสิทธิภาพในการกำหนดวัตถุประสงค์ นโยบาย กระบวนการ เพื่อใช้ในการบ่งชี้และประเมินความเสี่ยง และกำหนดวิธีการจัดการความเสี่ยงที่เหมาะสม องค์กรที่ได้มีการจัดทำกรอบและนโยบายการบริหารความเสี่ยงที่มีคำอธิบายองค์ประกอบในกรอบการบริหารความเสี่ยงอย่างชัดเจน จะทำให้ผู้บริหารและพนักงานทุกคนใช้ภาษาความเสี่ยงในทิศทางเดียวกันและมีจุดหมายร่วมกันในการบริหารความเสี่ยง

3) การปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างต่อเนื่อง องค์กรที่ประสบความสำเร็จในการปฏิบัติตามกระบวนการบริหารความเสี่ยง คือ องค์กรที่สามารถนำกระบวนการบริหารความเสี่ยงมาปฏิบัติอย่างทั่วถึงทั้งองค์กร และกระทำอย่างต่อเนื่องสม่ำเสมอ

4) กระบวนการในการบริหารการเปลี่ยนแปลง ในการนำเอากระบวนการและระบบบริหารแบบใหม่มาใช้ องค์กรจำเป็นต้องมีการบริหารการเปลี่ยนแปลง การพัฒนาการบริหารความเสี่ยงก็เช่นเดียวกันต้องมีการชี้แจงให้ผู้บริหารและพนักงานทุกคนรับทราบถึงการเปลี่ยนแปลงและผลที่องค์กรและแต่ละบุคคลจะได้รับจากการเปลี่ยนแปลงนั้น

5) การสื่อสารอย่างมีประสิทธิภาพ วัตถุประสงค์ของการสื่อสารอย่างมีประสิทธิภาพเพื่อให้มั่นใจว่าได้ว่า

- ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงอย่างถูกต้องและทันเวลา
- ผู้บริหารสามารถจัดการความเสี่ยงตามลำดับความสำคัญ หรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่
- มีการติดตามแผนการจัดการความเสี่ยงต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารองค์กรและจัดการความเสี่ยงต่างๆ เพื่อให้องค์กรมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด

6) การวัดผลการบริหารความเสี่ยง การวัดผลการบริหารความเสี่ยงประกอบด้วย 2 รูปแบบ ดังนี้

- การวัดความเสี่ยงในรูปแบบของผลกระทบและโอกาสที่อาจเกิดขึ้น การบริหารความเสี่ยงที่ประสบความสำเร็จ จะช่วยให้ความเสี่ยงอยู่ในระดับที่องค์กรยอมรับได้
- การวัดความสำเร็จของการบริหารความเสี่ยง โดยอาศัยดัชนีวัดผลการดำเนินงานซึ่งอาจกำหนดเป็นระดับองค์กร ฝ่ายงาน หรือของแต่ละบุคคล การใช้ดัชนีวัดผลการดำเนินงานนี้อาจปฏิบัติร่วมกับกระบวนการด้านทรัพยากรบุคคล

7) การฝึกอบรมและกลไกด้านทรัพยากรบุคคล กรรมการ ผู้บริหาร และพนักงานทุกคนในองค์กรควรต้องได้รับการฝึกอบรมเพื่อให้เข้าใจกรอบการบริหารความเสี่ยงและความรับผิดชอบของแต่ละบุคคลในการจัดการความเสี่ยงและสื่อสารข้อมูลเกี่ยวกับความเสี่ยง

8) การติดตามกระบวนการบริหารความเสี่ยง ควรพิจารณาประเด็นดังต่อไปนี้

- การรายงานและการสอบทานขั้นตอนตามกระบวนการบริหารความเสี่ยง
- ความชัดเจนและสม่ำเสมอของการมีส่วนร่วมและความมุ่งมั่นของผู้บริหารระดับสูง
- บทบาทของผู้นำในการสนับสนุนและติดตามการบริหารความเสี่ยง
- การประยุกต์ใช้เกณฑ์การประเมินผลการดำเนินงานที่เกี่ยวกับการบริหารความเสี่ยง

ส่วนที่

3



ด้านการควบคุมภายใน
(INTERNAL CONTROL : IC)

ส่วนที่ 3 ด้านการควบคุมภายใน (Internal Control : IC)

3.1 ความหมายของการควบคุมภายใน

“การควบคุมภายใน (Internal control)” หมายความว่า กระบวนการปฏิบัติงานที่ผู้กำกับดูแลฝ่ายบริหารและพนักงาน อ.ส.พ. ทุกระดับของส่วนงานกำหนดให้มีขึ้น เพื่อให้มีความมั่นใจอย่างสมเหตุสมผลว่าการดำเนินงานจะบรรลุผลสำเร็จตามวัตถุประสงค์ของการควบคุมภายในอย่างสมเหตุสมผล ในเรื่องดังต่อไปนี้

การดำเนินการ (Operation : O) หมายถึง การบริหารจัดการการใช้ทรัพยากรให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล รวมถึงการดูแลป้องกันรักษาสินทรัพย์ การป้องกันหรือลดข้อผิดพลาดในการปฏิบัติงาน การใช้ทรัพยากรอย่างคุ้มค่า และการป้องกันการทุจริต

การรายงาน (Report : R) หมายถึง ความถูกต้อง เชื่อถือได้ และทันกาลของรายงานทางการเงินและมีใช้การเงิน ที่จัดทำขึ้นเพื่อใช้ภายในและภายนอกองค์กร

การปฏิบัติตามกฎหมายและระเบียบข้อบังคับ (Compliance : C) ได้แก่ การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมติคณะรัฐมนตรีที่เกี่ยวข้อง รวมทั้งการปฏิบัติตามนโยบาย และวิธีการปฏิบัติงานที่องค์กรกำหนด

3.2 ความสำคัญและประโยชน์ของการควบคุมภายใน

การควบคุมภายในเป็นเครื่องมือในการบริหารจัดการ และสนับสนุนการดำเนินงาน เพื่อให้สามารถดำเนินกิจการได้อย่างมั่นคงต่อเนื่อง เพิ่มความเชื่อมั่นในการบรรลุวัตถุประสงค์ขององค์กรอย่างมีประสิทธิภาพและประสิทธิผล นอกจากนี้ยังสามารถลดความสูญเสีย และสร้างมูลค่าเพิ่มได้อย่างเป็นรูปธรรม

ประโยชน์ที่ผู้บริหารพึงคาดหวังได้จากการควบคุมภายในที่ดี มีดังนี้

1) การควบคุมภายในที่ดี ที่ได้รับการปฏิบัติตามอย่างมีประสิทธิภาพ จะมีส่วนช่วยให้การดำเนินงานขององค์กรมีประสิทธิภาพและบรรลุวัตถุประสงค์ที่วางไว้ ซึ่งหมายถึง การดำเนินการได้ตามเป้าหมายที่ผู้บริหารกำหนด

2) ช่วยป้องกันไม่ให้เกิดการใช้ทรัพยากรเป็นไปอย่างสิ้นเปลือง และป้องกันความสูญเสีย สูญเปล่าของทรัพยากรที่นำไปใช้ในการดำเนินงานด้านต่างๆ

3) ช่วยทำให้เกิดความมั่นใจตามควรว่ารายงานทางการเงิน ทั้งรายงานที่ใช้เพื่อการภายในและรายงานที่เสนอต่อบุคคลภายนอก มีความถูกต้องสมบูรณ์และเชื่อถือได้

4) ช่วยกำกับให้การปฏิบัติการด้านต่างๆ สอดคล้องกับกฎหมาย และระเบียบที่ใช้บังคับกับองค์กร ซึ่งเป็นการป้องกันมิให้องค์กรเสียหายชื่อเสียง หรือเกิดความเสียหายด้านการเงิน หรือด้านอื่นๆ ที่อาจเกิดขึ้นหากมีการกระทำที่ผิดกฎหมาย หรือผิดระเบียบ

ประโยชน์ของการควบคุมภายในกับฝ่ายงาน

ฝ่ายบริหาร	ระบบการควบคุมภายในที่ดีจะเป็นเครื่องมือช่วยให้ผู้บริหารมีความมั่นใจว่า พนักงานและลูกจ้างได้ปฏิบัติงานอย่างถูกต้อง รายงานต่างๆ ที่จัดทำขึ้นถูกต้อง เชื่อถือได้ และทันเวลาที่กำหนด ตลอดจนมีการป้องกันความผิดพลาดและการทุจริตหรือการสูญหายของทรัพย์สินไว้อย่างรัดกุม
พนักงานและลูกจ้าง	ระบบการควบคุมภายในจะเป็นเครื่องชี้นำแนวทางการปฏิบัติงานที่ถูกต้องและเป็นไปตามนโยบายที่ผู้บริหารวางไว้ เป็นเครื่องช่วยเพิ่มประสิทธิภาพในการปฏิบัติงาน
ผู้สอบบัญชีและผู้ตรวจสอบภายใน	ผู้สอบบัญชีและผู้ตรวจสอบภายในจะใช้ประสิทธิภาพของระบบการควบคุมภายในเป็นปัจจัยสำคัญในการกำหนดขอบเขตการปฏิบัติงานตรวจสอบ ช่วยให้การทำงานของผู้สอบบัญชี และผู้ตรวจสอบภายในรวดเร็ว และมีประสิทธิภาพมากขึ้น
คณะกรรมการตรวจสอบ	หน้าที่หลักประการหนึ่งของคณะกรรมการตรวจสอบ คือ การพิจารณาระบบควบคุมภายในของกิจการว่ามีประสิทธิภาพ ประสิทธิผลเพียงพอหรือไม่ กิจการที่มีระบบการควบคุมภายในที่ดีจะช่วยเพิ่มความมั่นใจในการปฏิบัติงานของคณะกรรมการตรวจสอบได้

3.3 แนวคิดของการควบคุมภายใน

1) การควบคุมภายในถือเป็นส่วนหนึ่งของขั้นตอนการปฏิบัติงานในทุกตำแหน่ง และทุกระดับของส่วนงาน การควบคุมภายในเป็นกระบวนการ (Process) ที่มีการปฏิบัติอย่างต่อเนื่อง ซึ่งกำหนดไว้ในกระบวนการปฏิบัติงาน (Built in) ตามปกติของหน่วยรับตรวจ ดังนั้น ฝ่ายบริหารจึงควรนำการควบคุมภายในมาใช้โดยรวมเป็นส่วนหนึ่งของกระบวนการบริหารงาน ได้แก่ การวางแผน (Planning) การดำเนินงาน (Executing) และการติดตามผล (Monitoring)

2) การควบคุมภายในเกิดขึ้นได้โดยบุคลากรของหน่วยรับตรวจ ผู้บริหารเป็นผู้รับผิดชอบกำหนดและจัดให้มีระบบการควบคุมภายในที่มีประสิทธิผล ด้วยการสร้างบรรยากาศสิ่งแวดล้อม การควบคุม กำหนดทิศทาง กลไกการควบคุมและกิจกรรมต่างๆ รวมทั้งการติดตามผลการควบคุมภายใน บุคลากรทุกระดับรับผิดชอบในการปฏิบัติตามที่ผู้บริหารกำหนด

3) การควบคุมภายในให้ความมั่นใจอย่างสมเหตุสมผลว่าการปฏิบัติงานจะบรรลุวัตถุประสงค์ที่กำหนด แม้ว่าการควบคุมภายในจะออกแบบไว้ให้มีประสิทธิผลเพียงใด ก็ไม่สามารถให้ความมั่นใจว่าจะทำให้การดำเนินงานบรรลุผลสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ได้อย่างสมบูรณ์ เพราะการควบคุมภายในมีข้อจำกัด เช่น โอกาสที่จะเกิดข้อผิดพลาด การสมรู้ร่วมคิดกัน หรือการปฏิบัติผิดกฎหมายระเบียบข้อบังคับที่กำหนดไว้ ที่สำคัญที่สุดคือ การที่ผู้บริหารหลีกเลี่ยงขั้นตอนของระบบการควบคุมภายในหรือใช้อำนาจในทางที่ผิด นอกจากนี้การวางระบบควบคุมภายในจะต้องคำนึงถึงต้นทุนและผลประโยชน์ที่เกี่ยวข้องด้วยว่า ผลประโยชน์ที่ได้รับจากการควบคุมภายในจะคุ้มค่างกับต้นทุนที่เกิดขึ้น

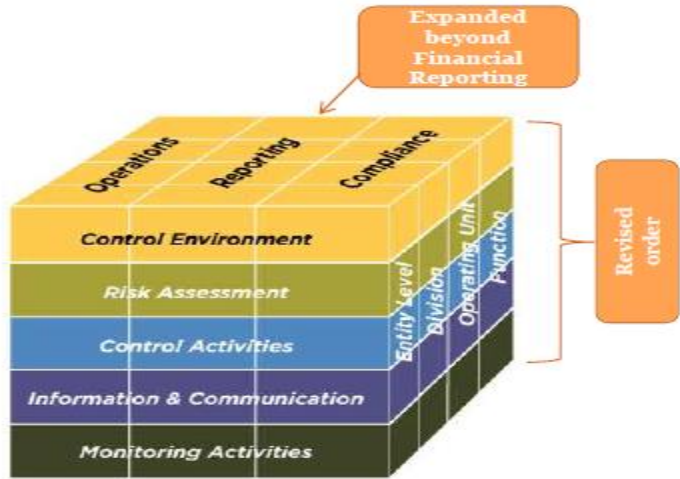
3.4 มาตรฐานการควบคุมภายใน

การสร้างระบบการควบคุมภายในที่เป็นไปตามมาตรฐานการควบคุมภายในที่มีความเชื่อมโยงและเกื้อกูลกันตามองค์ประกอบของมาตรฐานการควบคุมภายในของกระทรวงการคลัง ประกอบด้วย 5 องค์ประกอบดังต่อไปนี้

- 1) **สภาพแวดล้อมของการควบคุม (Control Environment)** เป็นเรื่องพื้นฐานที่สำคัญที่สุดของการบริหารองค์กร ผู้กำกับดูแล ฝ่ายบริหาร และบุคลากร ต้องสร้างสภาพแวดล้อมให้บุคลากรทุกระดับมีทัศนคติที่ดีต่อการควบคุมภายใน โดยส่งเสริมให้บุคลากรทุกคนเกิดจิตสำนึกในเรื่องความซื่อสัตย์ จริยธรรม ความรับผิดชอบต่อนหน้าที่ได้รับมอบหมาย และความสำคัญของประสิทธิผลการควบคุมภายใน
- 2) **การประเมินความเสี่ยง (Risk Assessment)** ฝ่ายบริหารต้องให้ความสำคัญกับการประเมินความเสี่ยงและประเมินความเสี่ยงที่มีผลกระทบต่อผลสำเร็จตามวัตถุประสงค์ขององค์กรที่เกิดจากปัจจัยภายในและภายนอกด้วยวิธีการที่เป็นระบบอย่างเพียงพอและเหมาะสม
- 3) **กิจกรรมการควบคุม (Control Activities)** ได้แก่ นโยบายและระเบียบ วิธีปฏิบัติ รวมถึงมาตรการต่างๆ ที่ฝ่ายบริหารกำหนดหรือออกแบบขึ้น เพื่อให้บุคลากรนำไปปฏิบัติเพื่อลดหรือควบคุมความเสี่ยงอย่างมีประสิทธิภาพและประสิทธิผล ฝ่ายบริหารต้องจัดให้มีกิจกรรมการควบคุมเพื่อป้องกันหรือลดความเสียหายความผิดพลาดที่อาจเกิดขึ้น และให้สามารถบรรลุผลสำเร็จตามวัตถุประสงค์ของการควบคุมภายใน ตัวอย่างกิจกรรมการควบคุม เช่น การสอบทานงาน การดูแลป้องกันทรัพย์สิน และการแบ่งแยกหน้าที่ เป็นต้น
- 4) **สารสนเทศและการสื่อสาร (Information and Communication)** เป็นส่วนสนับสนุนที่สำคัญต่อประสิทธิภาพและประสิทธิผลในการกำหนดกลยุทธ์ประเมินความเสี่ยงและกิจกรรมควบคุม ฝ่ายบริหารต้องจัดให้มีสารสนเทศอย่างเพียงพอ เหมาะสม เชื่อถือได้ และสื่อสารให้ฝ่ายบริหารและบุคลากรอื่นๆ ที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร ซึ่งจำเป็นต้องใช้สารสนเทศนั้นในรูปแบบที่เหมาะสมและทันเวลา
- 5) **การติดตามประเมินผล (Monitoring)** เป็นวิธีการที่ช่วยให้ฝ่ายบริหารมีความมั่นใจว่าระบบการควบคุมภายในมีการปฏิบัติตามหรือไม่ ฝ่ายบริหารต้องจัดให้มีการติดตามประเมินผลทั้งในระหว่างการปฏิบัติงานอย่างต่อเนื่อง และสม่ำเสมอ และการประเมินผลเป็นรายครั้ง (การประเมินการควบคุมด้วยตนเอง (Control Self-Assessment : CSA) และการประเมินการควบคุมอย่างเป็นอิสระ) เพื่อให้เกิดความมั่นใจว่าระบบการควบคุมภายในที่กำหนดหรือออกแบบไว้เหมาะสมมีประสิทธิภาพ หรือต้องปรับปรุงระบบการควบคุมภายใน

องค์ประกอบทั้ง 5 ประการ มีความเกี่ยวเนื่องสัมพันธ์กันโดยมีสภาพแวดล้อมของการควบคุมเป็นรากฐานที่สำคัญขององค์ประกอบอื่นๆ องค์ประกอบทั้ง 5 นี้ เป็นสิ่งจำเป็นที่มีอยู่ในการดำเนินงานตามภารกิจขององค์กร เพื่อให้การปฏิบัติงานบรรลุผลสำเร็จตามวัตถุประสงค์ขององค์กรทั้ง 3 ประการ คือ

- การดำเนินงานเกิดประสิทธิผลและประสิทธิภาพ
- รายงานทางการเงินและมีใช้การเงินน่าเชื่อถือ
- มีการปฏิบัติตามกฎระเบียบและข้อบังคับที่เกี่ยวข้อง



รูปภาพที่ 17 องค์ประกอบของการควบคุมภายใน

3.5 การจัดวางระบบการควบคุมภายใน

การกำหนดหรือออกแบบระบบการควบคุมภายในที่มีประสิทธิผล ควรมี 7 ขั้นตอน ดังนี้

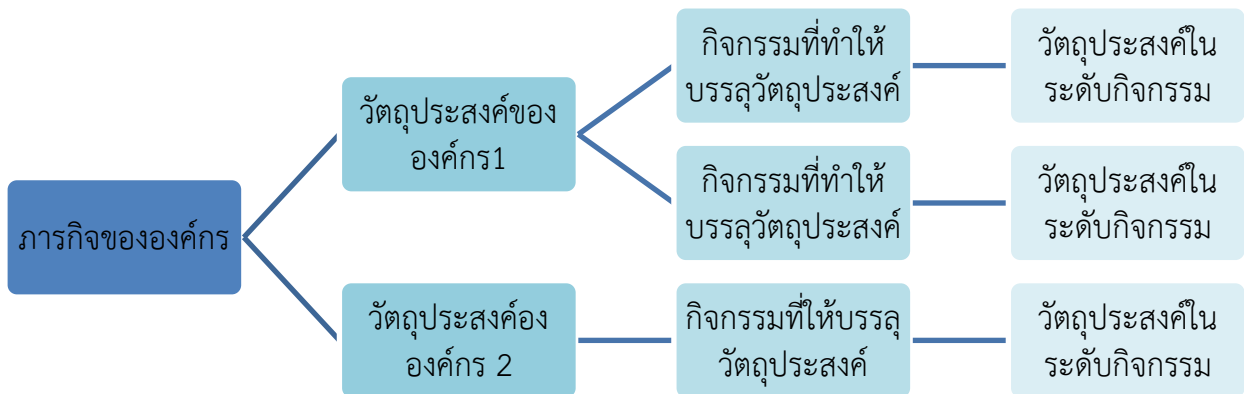
1) กำหนดวัตถุประสงค์ในการดำเนินงาน องค์กรจำเป็นต้องกำหนดวัตถุประสงค์หรือเป้าหมายทั้งในระยะสั้นและระยะยาว สิ่งสำคัญอย่างหนึ่ง ที่จะช่วยให้ผู้บริหารดำเนินงานให้บรรลุวัตถุประสงค์ได้ คือ การสร้างระบบการควบคุมภายในที่ดี ช่วยทำให้ผู้บริหารมั่นใจในระดับที่สมเหตุสมผลว่าจะสามารถควบคุมดูแล การดำเนินงานให้บรรลุวัตถุประสงค์ที่ตั้งไว้ได้ โดยวัตถุประสงค์ขององค์กร แบ่งเป็น 2 ระดับ คือ

(1) วัตถุประสงค์ในระดับองค์กร (Entity – Level Objectives) เป็นวัตถุประสงค์การดำเนินงานในภาพรวมขององค์กร

(2) วัตถุประสงค์ในระดับกิจกรรม (Activity – Level Objectives) เป็นวัตถุประสงค์การดำเนินงานที่เฉพาะเจาะจงลงไป สำหรับแต่ละกิจกรรมของระดับส่วนงานย่อย ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การกำหนดวัตถุประสงค์ขององค์กร ควรมีลำดับขั้นตอนดังต่อไปนี้

- (1) กำหนดภารกิจขององค์กร
- (2) กำหนดวัตถุประสงค์ในระดับองค์กรให้สอดคล้องกับภารกิจที่กำหนดไว้
- (3) กำหนดกิจกรรมที่ทำให้บรรลุวัตถุประสงค์ในระดับองค์กร
- (4) กำหนดวัตถุประสงค์ในระดับกิจกรรม



รูปภาพที่ 18 การกำหนดวัตถุประสงค์ของการควบคุมภายใน

- 2) ค้นหาความเสี่ยงต่างๆ ที่มีนัยสำคัญ ที่อาจทำให้การดำเนินงานไม่บรรลุผลสำเร็จตามวัตถุประสงค์
- 3) พิจารณาการควบคุมที่มีอยู่แล้วว่า ป้องกันหรือลดความเสี่ยงได้ในระดับใด
- 4) ระบุกิจกรรมการควบคุมใหม่ เพื่อป้องกันหรือลดความเสี่ยงที่เหลือให้อยู่ในระดับที่ยอมรับได้
- 5) ประเมินการต้นทุนที่ใช้ในการจัดให้มีและดำรงรักษาไว้ซึ่งกิจกรรมการควบคุม ต้นทุนหรือค่าใช้จ่ายต้องไม่สูงกว่าประโยชน์ที่จะได้รับจากการมีกิจกรรมการควบคุม
- 6) จัดทำแผนในการนำกิจกรรมการควบคุมนั้นมาใช้
- 7) นำกิจกรรมการควบคุมไปปฏิบัติ และติดตามผล

3.6 การประเมินประสิทธิผลของการควบคุมภายใน

การประเมินประสิทธิผลของการควบคุมภายในจะเป็นการประเมินขั้นสุดท้าย โดยอาศัยหลักฐานที่รวบรวมไว้จากการประเมินในขั้นต้น แล้วขยายผลการประเมิน โดยจะขยายผลการประเมินให้ครอบคลุมรอบการประเมินประสิทธิผลของการควบคุมภายใน 4 ด้าน ได้แก่ 1. ระดับการควบคุม 2. ผลการดำเนินงานเมื่อเทียบกับเป้าหมาย 3. กระบวนการควบคุม 4. การติดตามและกำกับดูแล โดยทั้ง 4 ด้านจะต้องมีค่าระดับการควบคุมไม่ต่ำกว่าระดับ 3 ดังนี้

	1. ระดับการควบคุม (ร้อยละ 30)	2. ผลการดำเนินงานเมื่อเทียบกับเป้าหมาย (ร้อยละ 30)	3. กระบวนการควบคุม (ร้อยละ 20)	4. การติดตามและกำกับดูแล (ร้อยละ 20)
1	เบื้องต้น	ผลการดำเนินงานต่ำกว่าเป้าหมายมาก (น้อยกว่าร้อยละ 70 หรืออยู่ที่ค่าเกณฑ์ 1)	ไม่มีมาตรฐานที่ชัดเจน	ไม่มีการติดตาม
2	ไม่เป็นทางการ	ผลการดำเนินงานต่ำกว่าเป้าหมาย (ร้อยละ 71-80 หรืออยู่ที่ค่าเกณฑ์ 2)	มีการควบคุมเป็นมาตรฐาน แต่ยังไม่นำออกมาใช้	มีการควบคุมแต่ไม่มีการติดตาม
3	เป็นระบบ	ผลการดำเนินงานเป็นไปตามเป้าหมาย (ร้อยละ 81-90 หรืออยู่ที่ค่าเกณฑ์ 3)	มีการควบคุมเป็นมาตรฐานของแต่ละหน่วยงาน	มีการติดตามแต่ไม่มีการรายงานให้ผู้บริหารทราบ
4	บูรณาการ	ผลการดำเนินงานดีกว่าเป้าหมาย (ร้อยละ 91-100 หรืออยู่ที่ค่าเกณฑ์ 4)	มีการกำหนดเป็นมาตรฐานขององค์กร	มีการติดตามและมีการรายงานให้ผู้บริหารทราบเป็นระยะ
5	ใช้ให้เกิดประโยชน์สูงสุด	ผลการดำเนินงานดีกว่าเป้าหมายมาก (มากกว่าร้อยละ 100 หรืออยู่ที่ค่าเกณฑ์ 5)	มีการกำหนดเป็นมาตรฐานขององค์กร และเทียบเคียงกับ Best Practice	มีการระบุระยะเวลาการติดตามและรายงานผลที่ชัดเจน

หลักเกณฑ์การประเมินประสิทธิผลของความเพียงพอของการควบคุม

ในการประเมินประสิทธิผลของความเพียงพอของการควบคุมภายในได้กำหนด เป็น 4 ด้าน และมีหลักเกณฑ์ในการประเมิน ดังนี้

หลักเกณฑ์	น้ำหนักร้อยละ
1. ระดับการควบคุม ประเมินจากการควบคุมว่าได้ผลตามวัตถุประสงค์หรือความเสี่ยงที่กำหนดหรือไม่ โดยพิจารณาจาก	30
1.1 การควบคุมที่กำหนดมีความสอดคล้องกับวัตถุประสงค์หรือความเสี่ยงที่กำหนด	15
1.2 ความคุ้มค่า ไม่เสียเวลาและค่าใช้จ่ายในการประเมินผลมากเกินไปจนความจำเป็น	8
1.3 สามารถปฏิบัติได้โดยผู้ประเมินมีความรู้ทักษะที่จำเป็น หรือโดยอาศัยความรู้และทักษะจากผู้เชี่ยวชาญและที่ปรึกษา	7
2. ผลการดำเนินงานเมื่อเทียบกับเป้าหมาย ประเมินจากผลการดำเนินงานตามภารกิจของหน่วยงานที่สอดคล้องกับแผนการดำเนินงานที่สำคัญขององค์กรฯ	30
2.1 ผลการดำเนินงานตามบันทึกข้อตกลงการประเมินผลหรือตามแผนยุทธศาสตร์	15
2.2 ผลการดำเนินงานตามแผนงานโครงการของหน่วยงาน	8
2.3 ผลสำเร็จของการเบิกจ่ายงบประมาณ	7
3. กระบวนการควบคุม	20
3.1 การกำหนดกิจกรรมการควบคุม	8
3.2 การกำหนดความถี่ในการปฏิบัติตามกิจกรรมควบคุม	4
3.3 การสื่อสาร	8
4. การติดตามและกำกับดูแล	20
4.1 การติดตามให้เป็นไปตามกระบวนการควบคุม	8
4.2 ความถี่ในการปฏิบัติจริง	6
4.3 การทบทวนและปรับปรุงกิจกรรมให้สัมฤทธิ์ผล	6
รวมน้ำหนัก	100

วิธีปฏิบัติ

ในการประเมินประสิทธิผลของความเพียงพอของการควบคุมภายในได้กำหนดวิธีการปฏิบัติสำหรับหน่วยงานไว้ ดังนี้

- 1) ระบุผู้รับผิดชอบในการดำเนินการประเมินการควบคุมภายในด้วยตนเอง สำหรับแต่ละหน่วยงาน
- 2) กำหนดขอบเขตของการดำเนินการประเมินการควบคุมภายในด้วยตนเอง เช่น รายการของกระบวนการปฏิบัติงานที่จะต้องทำการประเมิน
- 3) ระบุวัตถุประสงค์ของกระบวนการ ความเสี่ยงของกิจกรรมที่สำคัญ ระบุการควบคุมที่มีในปัจจุบัน และที่ควรมีสำหรับความเสี่ยงที่สำคัญของกระบวนการ
- 4) จัดทำแบบสอบถามการควบคุมภายใน
- 5) ประเมินการควบคุมภายใน ระบุความเสี่ยงที่การควบคุมยังไม่เพียงพอ และจัดทำแผนปรับปรุงการควบคุมสำหรับการควบคุมที่ยังไม่เพียงพอ
- 6) จัดประชุมเชิงปฏิบัติการ CSA (CSA Workshop) เพื่อหาข้อสรุปผลการประเมินการควบคุมและแผนปรับปรุง
- 7) จัดทำรายงานสรุปผลการประเมินการควบคุมภายในด้วยตนเอง และนำเสนอต่อผู้บริหารตามลำดับชั้น

- 8) จัดทำรายงานตามระเบียบของคณะกรรมการตรวจเงินแผ่นดิน
- 9) ติดตามการปฏิบัติตามแผนปรับปรุงการควบคุม

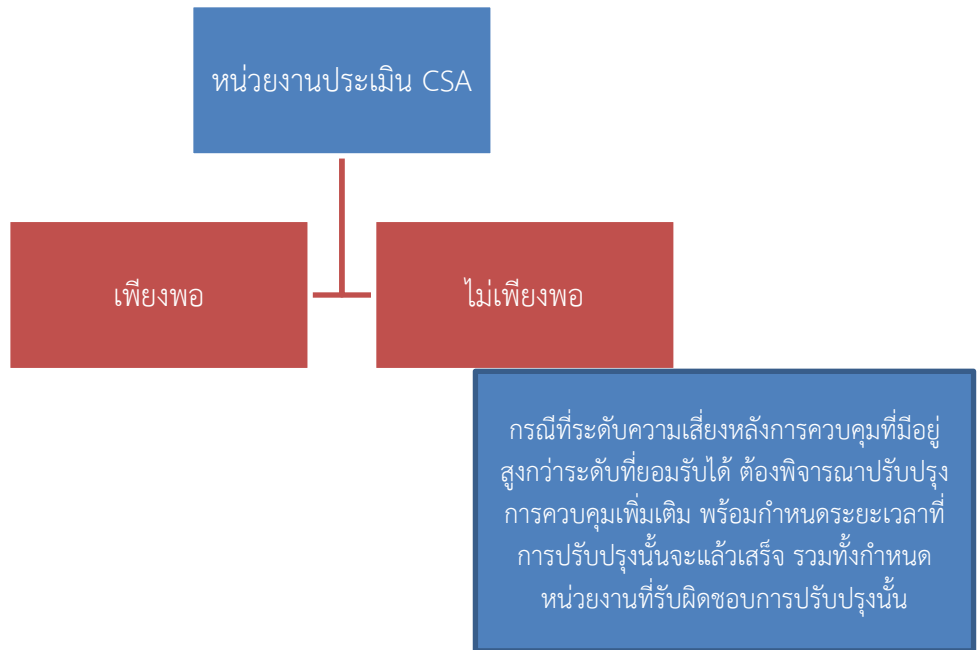
3.7 การสรุปประเมินการควบคุมภายในด้วยตนเอง (CSA)

CSA ย่อมาจาก Control Self Assessment หรือ การประเมินการควบคุมด้วยตนเอง เป็นเครื่องมือช่วยพัฒนาสมรรถภาพขององค์กรให้สามารถบรรลุวัตถุประสงค์ขององค์กรได้ง่ายขึ้น โดยอาจทำออกมาในรูปแบบของการประชุมเชิงปฏิบัติการ (Workshop) ซึ่งเกิดขึ้นจากบุคลากรที่มีหน้าที่รับผิดชอบโดยตรงต่อการปฏิบัติงาน

สิ่งที่ต้องคำนึงถึงในการ Workshop

- 1) วัตถุประสงค์และขอบเขตของระบบงานนั้น
- 2) ขั้นตอนในการทำงานและวัตถุประสงค์ของขั้นตอน
- 3) ความเสี่ยงและสาเหตุที่ทำให้เกิดความเสี่ยงนั้นๆ
- 4) การควบคุมที่มีอยู่เพื่อลดระดับความเสี่ยง

โดยพิจารณาว่าการควบคุมที่มีอยู่นั้น ทำให้ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้หรือไม่ โดยประเมินระดับความเสี่ยงจาก “เกณฑ์ประเมินความเสี่ยงระดับหน่วยงาน” ซึ่งประเมินจาก โอกาส (Likelihood) และผลกระทบ (Impact)



รูปภาพที่ 19 กระบวนการประเมินการควบคุมภายในด้วยตนเอง (CSA) ซึ่งต้องกระทำโดยบุคลากรภายในหน่วยงานเป็นประจำอย่างสม่ำเสมอ

3.8 แนวทางปฏิบัติเกี่ยวกับการควบคุมภายในของ อ.ส.พ.

- 1) มุ่งเน้นให้การควบคุมภายในถือเป็นส่วนหนึ่งของขั้นตอนการปฏิบัติงานในทุกตำแหน่ง และทุกระดับของส่วนงาน
- 2) ผู้บริหารเป็นผู้รับผิดชอบกำหนดและจัดให้มีระบบการควบคุมภายในที่มีประสิทธิภาพ ด้วยการสร้างบรรยากาศสิ่งแวดล้อม การควบคุม กำหนดทิศทาง กลไกการควบคุมและกิจกรรมต่างๆ รวมทั้งการติดตามผลการควบคุมภายใน พนักงานและลูกจ้าง อ.ส.พ. ทุกระดับมีหน้าที่รับผิดชอบในการนำระบบการควบคุมภายในไปปฏิบัติตามที่ผู้บริหารกำหนด

3) การควบคุมภายในเป็นการสร้างความมั่นใจอย่างสมเหตุสมผลว่าการปฏิบัติงานจะบรรลุวัตถุประสงค์ที่กำหนด โดยต้องคำนึงถึงต้นทุนและผลประโยชน์ที่เกี่ยวข้องด้วยว่า ผลประโยชน์ที่ได้รับจากการควบคุมภายในจะคุ้มค่างับต้นทุนที่เกิดขึ้น

4) สร้างระบบการควบคุมภายในที่เป็นไปตามมาตรฐานการควบคุมภายในที่มีความเชื่อมโยงและเกื้อกูลกันภายใต้ 5 องค์ประกอบ ดังต่อไปนี้

- (1) สภาพแวดล้อมของการควบคุม (Control Environment)
- (2) การประเมินความเสี่ยง (Risk Assessment)
- (3) กิจกรรมการควบคุม (Control Activities)
- (4) สารสนเทศและการสื่อสาร (Information and Communication)
- (5) การติดตามประเมินผล (Monitoring)

5) ให้มีการติดตามผลระหว่างการปฏิบัติงาน (Ongoing Monitoring) อย่างต่อเนื่องและสม่ำเสมอ โดยมีการประเมินผลเป็นรายครั้ง (Separate Evaluation) ซึ่งแยกเป็นการประเมินการควบคุมด้วยตนเอง (Control Self-Assessment : CSA) ปีละครั้ง ตามระเบียบคณะกรรมการตรวจเงินแผ่นดิน ว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน

ดังนั้น เพื่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลว่าจะบรรลุวัตถุประสงค์ด้านการดำเนินงาน ด้านการรายงานและด้านการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับ ตามตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ รวมทั้งสอดคล้องกับหลักการตามกรอบการดำเนินงานด้าน Governance, Risk and Compliance (GRC) จึงได้กำหนดแนวทางปฏิบัติเกี่ยวกับการควบคุมภายใน ดังนี้

1) กรณีมีการปรับปรุงโครงสร้างและลักษณะงาน ให้หน่วยงานจัดวางระบบการควบคุมภายในทุกระบบงานตามโครงสร้างและลักษณะงานหลักที่ได้รับมอบหมายให้สอดคล้องกับ

- ยุทธศาสตร์ขององค์กรฯ
- นโยบายกำกับดูแลกิจการและจริยธรรมการดำเนินงานขององค์กรฯ
- หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ.2561

2) ให้หน่วยงานตามข้อ 1) และหน่วยงานที่จัดวางระบบการควบคุมภายในไว้แล้ว จัดทำแผนการประเมินการควบคุมด้วยตนเอง (แผน CSA) และทำการประเมินตามแผน พร้อมทั้งจัดทำรายงานเกี่ยวกับการควบคุมภายในให้แล้วเสร็จภายในระยะเวลาที่กำหนด

3) ให้ทุกหน่วยงาน ทบทวน/ปรับปรุงแนวทางปฏิบัติและคู่มือการปฏิบัติงานให้เป็นปัจจุบัน นำเสนอขอความเห็นชอบจากผู้บริหารสูงสุดของสายงาน รวมทั้งนำคู่มือปฏิบัติงานส่วนที่มีข้ความลับไว้ในระบบเอกสารอิเล็กทรอนิกส์เพื่อเป็นองค์ความรู้เผยแพร่ภายในองค์กร

4) ให้หัวหน้างานทุกหน่วยงานสื่อสารการดำเนินการเกี่ยวกับการควบคุมภายในให้บุคลากรในสังกัดทราบ และติดตามควบคุมให้บุคลากรถือปฏิบัติในส่วนที่เกี่ยวข้องอย่างเคร่งครัด

3.10 แผนการดำเนินการเกี่ยวกับการควบคุมภายในประจำปี

กิจกรรม	กำหนดเสร็จ (โดยประมาณ)
ต้นปีงบประมาณ	
1) หน่วยงานระดับงาน/ส่วน ประเมินความเสี่ยงที่ยังมีอยู่จากปีก่อนและความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงานในปี เพื่อจัดทำแผนการปรับปรุงการควบคุมภายใน ตามแบบรายงานการประเมินผลการควบคุมภายใน (แบบ ปค.5)	สัปดาห์ที่ 4 ของเดือน ก.ย.
ระหว่างปีงบประมาณ	
1) รายงานผลการติดตามการประเมินผลการควบคุมภายในตามแบบติดตาม ปค.5 ต่อคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน ทุกไตรมาส	สัปดาห์สุดท้ายของแต่ละไตรมาส
2) หน่วยงานหารือการบริหารความเสี่ยงและแผนการควบคุมภายในของส่วนงานกับผู้บังคับบัญชาตามสายงาน	สัปดาห์ที่ 1 ของเดือน ต.ค.
3) คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน จัดส่งรายงานผลการติดตามการประเมินผลการควบคุมภายใน แบบ ติดตาม ปค.5 รายไตรมาส ต่อผู้ตรวจสอบภายใน เพื่อประกอบการพิจารณาสอบทานการประเมินผลการควบคุมภายใน	ภายหลังจากการประชุมคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน แต่ละไตรมาส
สิ้นปีงบประมาณ	
1) หน่วยงานระดับงาน/ส่วน จัดทำรายงานการประเมินผลการควบคุมภายใน สำหรับระยะเวลาการดำเนินงานสิ้นสุด 30 กันยายน (แบบ ปค.5)	สัปดาห์ที่ 1 ของเดือน ต.ค.
2) ผู้แทนหน่วยงานระดับงาน/ส่วน เสนอรายงานการประเมินผลการควบคุมภายใน ต่อผู้อำนวยการสำนักหรือผู้บังคับบัญชาตามสายงาน เพื่อพิจารณาลงนามรับรองการประเมินผลการควบคุมภายใน และจัดส่งให้คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน	สัปดาห์ที่ 3 ของเดือน ต.ค.
3) คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน จัดทำรายงานการประเมินผลการควบคุมภายใน ในภาพรวมของ อ.ส.พ. จัดส่งให้ผู้ตรวจสอบภายใน	สัปดาห์ที่ 3 ของเดือน พ.ย.
4) ผู้อำนวยการสำนักตรวจสอบภายใน รายงานการสอบทานการประเมินผลการควบคุมภายใน เสนอต่อผู้อำนวยการองค์การสวนพฤกษศาสตร์	สัปดาห์ที่ 1 ของเดือน ธ.ค.
5) ผู้อำนวยการองค์การสวนพฤกษศาสตร์ พิจารณาลงนามรายงานการประเมินผลการควบคุมภายในของ อ.ส.พ. ตามหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ จัดส่งให้กระทรวงต้นสังกัด	สัปดาห์ที่ 3 ของเดือน ธ.ค.

3.11 ข้อจำกัดของการควบคุมภายใน

ข้อจำกัดของการควบคุมภายใน (ปัจจัยความสำเร็จและอุปสรรค) มีดังนี้

- 1) การตัดสินใจใช้ดุลยพินิจของฝ่ายบริหารแทนระบบการควบคุมภายใน
- 2) การก้าวท้าวของฝ่ายบริหาร หรือผู้บริหารอาจสั่งการ หรือยกเว้นกฎเกณฑ์ในสิ่งที่ตนสั่งการให้ปฏิบัติ
- 3) การไม่ปฏิบัติตามระบบการควบคุมภายในที่องค์การกำหนดไว้ของผู้ปฏิบัติงานแต่ละคน
- 4) พนักงานสมคบกันฉ้อโกง หรือหลีกเลี่ยงการควบคุมที่มีอยู่
- 5) ผู้ปฏิบัติงานขาดความเข้าใจกลไกของการควบคุมที่จัดขึ้น
- 6) ค่าใช้จ่ายในการจัดให้มีระบบการควบคุมภายในก่อให้เกิดต้นทุนสูงกว่าค่าเสียหายที่อาจเกิดขึ้น ซึ่งไม่

คุ้มกับประโยชน์ที่ได้รับ