คู่มือ การบริหารความเสี่ยง

แผน บริหารจัดการความเสี่ยง

Risk Management Guide & Risk management plan

รอบปีงบประมาณ 2567

สำนักงานตรวจสอบภายใน

มหาวิทยาลัยราชภัฏเชียงใหม่

คำนำ

ตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 มาตรา 79 กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด อีกทั้งมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ.2562 (ว 23) ข้อ 2.4 การบริหารจัดการความเสี่ยงต้องดำเนินการในทุกระดับของหน่วยงานของรัฐ รวมทั้งมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ.2561 (ว 105) ซึ่งมีผลบังคับใช้ในปัจจุบันแล้วนั้น

สำนักงานตรวจสอบภายในได้จัดทำคู่มือและแผนการบริหารจัดการความเสี่ยง รอบปีงบประมาณ 2567 ฉบับนี้ขึ้น โดยมีเนื้อหาเป็นไปตามกฎ/ระเบียบดังกล่าวข้างต้น ได้แก่ มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ.2562 (ว 23) และมาตรฐานการควบคุมภายใน สำหรับหน่วยงานของรัฐ พ.ศ.2561 (ว 105) อีกทั้งได้มีการประยุกต์ใช้แนวคิดเรื่องกรอบการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management-Integrated Framework : ERM) หรือเรียกว่า COSO : ERM 2004 & 2017

คู่มือและแผนการบริหารจัดการความเสี่ยง รอบปีงบประมาณ 2567 ฉบับนี้ ได้นำเข้าที่ประชุมทบทวนแผนยุทธศาสตร์และแผนปฏิบัติการ รอบปีงบประมาณ 2566 เมื่อวันที่ 31 พฤษภาคม 2566 ณ ห้องประชุมริมใต้ อาคารอำนวยการและบริหารกลาง ศูนย์แม่ริม เพื่อให้มีการปรับปรุงแก้ไข และพัฒนา โดยมีกรอบโครงสร้างสำคัญอยู่ 3 ส่วน ได้แก่ 1. ข้อมูลทั่วไป 2. แนวทางการบริหารความเสี่ยง 3. คู่มือการบริหารความเสี่ยง และ 4. แผนการบริหารจัดการความเสี่ยง ซึ่งเป็นแนวทางการบริหารจัดการความเสี่ยงของสำนักงานตรวจสอบภายใน

สำนักงานตรวจสอบภายใน หวังว่าคู่มือและแผนการบริหารจัดการความเสี่ยง รอบปีงบประมาณ 2567 ฉบับนี้ จะเป็นกรอบแนวทางการปฏิบัติงานในการดำเนินงานการบริหารความเสี่ยงของสำนักงานตรวจสอบภายใน โดยทุกคนในหน่วยงานให้ถือปฏิบัติ เพื่อให้ความเสี่ยงต่างๆ ลดลงอยู่ในระดับที่ยอมรับได้ต่อไป

สำนักงานตรวจสอบภายใน
กันยายน 2566

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

ส่วนที่ 1
ข้อมูลทั่วไป

ประวัติความเป็นมา

สำนักงานตรวจสอบภายใน เป็นหน่วยงานที่ทำหน้าที่ตรวจสอบภายใน เริ่มแรกเป็นส่วนหนึ่งของงานประกันคุณภาพที่มหาวิทยาลัยมอบให้ ผู้ช่วยศาสตราจารย์กมล รักสวน รองอธิการบดีฝ่ายบริหารทั่วไป รับผิดชอบร่วมกับคณะกรรมการตรวจสอบภายใน ที่ตั้งขึ้นเฉพาะกิจ ภายหลังจึงริเริ่มดำเนินการจัดตั้งอย่างเป็นทางการโดยใช้ชื่อว่า “หน่วยตรวจสอบภายใน” เมื่อปีงบประมาณ 2546 ต่อมาในปี พ.ศ.2557 สภามหาวิทยาลัยราชภัฏเชียงใหม่ได้มีมติให้เปลี่ยนเป็น “สำนักงานตรวจสอบภายใน” โดยอาศัยอำนาจตามความในมาตรา 18 (2) แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ.2557 สภามหาวิทยาลัยราชภัฏเชียงใหม่ ในคราวประชุมครั้งที่ 12/2557 เมื่อวันที่ 29 ตุลาคม พ.ศ.2557

ปรัชญา (Philosophy)

“การตรวจสอบต้องมีคุณภาพและเป็นที่เชื่อถือ (Quality Audit for all, All for quality)”

วิสัยทัศน์ (Vision)

“ตรวจสอบอย่างโปร่งใส บริการที่เที่ยงธรรม แนะนำและให้คำปรึกษาที่มีคุณค่า”

พันธกิจ (Mission)

1) ประเมินประสิทธิภาพและประสิทธิผลหน่วยรับตรวจ ให้ตรงกับวัตถุประสงค์ และสอดคล้องกับนโยบายทุกระดับ
2) สอบทานระบบการปฏิบัติงานของหน่วยรับตรวจตามมาตรฐาน กฎหมาย ระเบียบ ข้อบังคับ ประกาศและคำสั่งของทางราชการ
3) ตรวจสอบระบบดูแลทรัพย์สินของหน่วยงานรับตรวจ
4) วิเคราะห์และประเมินการมีประสิทธิภาพ-ประสิทธิผล ความประหยัดและความคุ้มค่าในการใช้ทรัพยากรของหน่วยรับตรวจ
5) ประสานการตรวจสอบกับหน่วยรับการตรวจ และหน่วยงานที่เกี่ยวข้อง เพื่อสร้างองค์ความรู้ที่เข้มแข็ง มีระบบงานการตรวจสอบร่วมกัน เพื่อช่วยเหลือแนะนำ และให้คำปรึกษา
6) ประเมินและให้คำแนะนำการวางระบบการควบคุมภายในของมหาวิทยาลัย เพื่อให้หน่วยงานในสังกัดมีการควบคุมภายใน เพื่อลดความเสี่ยง

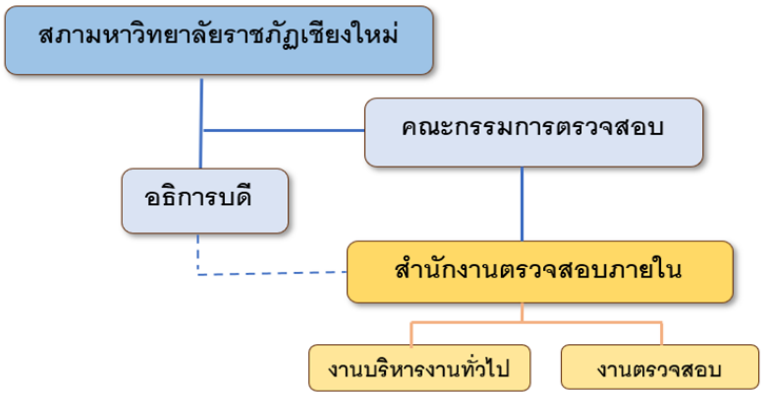
หน้าที่ความรับผิดชอบ

สำนักงานตรวจสอบภายใน มีหน้าที่ในการบริการให้ความเชื่อมั่น (Assurance Services) และการบริการให้คำปรึกษา (Consulting Services) เพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานอย่างมีประสิทธิภาพ ประสิทธิผล และคุ้มค่า โดยมีประเด็นการบริการให้ความเชื่อมั่น และการให้คำปรึกษา ดังนี้

1) การตรวจสอบทางการเงิน (Financial Auditing)
2) การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Auditing)
3) การตรวจสอบการปฏิบัติงาน (Operational Auditing)
4) การตรวจสอบผลการดำเนินงาน (Performance Auditing)
5) การตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Auditing)
6) การตรวจสอบการบริหาร (Management Auditing)
7) การบริการให้คำปรึกษา (Consulting)

โครงสร้างการบริหาร

สำนักงานตรวจสอบภายใน เป็นหน่วยงานภายใต้มหาวิทยาลัยราชภัฏเชียงใหม่ มีโครงสร้างหน่วยงานขึ้นตรงต่ออธิการบดี ตามข้อบังคับมหาวิทยาลัยราชภัฏเชียงใหม่ ว่าด้วย สำนักงานตรวจสอบภายใน พ.ศ. 2557 ข้อ 5 และข้อ 7 ประกอบกับสภามหาวิทยาลัยราชภัฏเชียงใหม่ ได้แต่งตั้งคณะกรรมการตรวจสอบ ตามคำสั่งสภามหาวิทยาลัยราชภัฏเชียงใหม่ ที่ 33/2565 เรื่องแต่งตั้งคณะกรรมการตรวจสอบ สั่ง ณ วันที่ 7 ตุลาคม 2565 และมีหน้าที่ตามข้อบังคับมหาวิทยาลัยราชภัฏเชียงใหม่ว่าด้วย คณะกรรมการตรวจสอบ พ.ศ. 2565 ตามข้อ 9 มีผลให้สำนักงานตรวจสอบภายในขึ้นตรงต่อคณะกรรมการตรวจสอบ ซึ่งเป็นไปตามแนบท้ายหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ (ฉบับที่ 2) 2562 (ภาพที่ 1)



ภาพที่ 1 โครงสร้างบริหารงานสำนักงานตรวจสอบภายใน มหาวิทยาลัยราชภัฏเชียงใหม่

คณะกรรมการตรวจสอบและบุคลากรสำนักงานตรวจสอบภายใน

คณะกรรมการตรวจสอบ

เพื่อให้การดำเนินงานเป็นไปตามหลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ.2561 สภามหาวิทยาลัยราชภัฏเชียงใหม่ ได้แต่งตั้งคณะกรรมการตรวจสอบ ตามคำสั่งสภามหาวิทยาลัยราชภัฏเชียงใหม่ ที่ 33/2565 เรื่องแต่งตั้งคณะกรรมการตรวจสอบ สั่ง ณ วันที่ 7 ตุลาคม 2565 และมีหน้าที่ตามข้อบังคับมหาวิทยาลัยราชภัฏเชียงใหม่ว่าด้วยคณะกรรมการตรวจสอบ พ.ศ. 2565 ตามข้อ 9 จำนวน 5 คน ดังนี้

ภาพที่ 2 คณะกรรมการตรวจสอบ สำนักงานตรวจสอบภายใน

บุคลากรสำนักงานตรวจสอบภายใน

มีบุคลากรปฏิบัติงานภายในหน่วยงานทั้งสิ้น จำนวน 5 คน (ภาพที่ 3) ดังนี้

ภาพที่ 3 บุคลากรสำนักงานตรวจสอบภายใน

ส่วนที่ 2
แนวทางการบริหารจัดการความเสี่ยง

นโยบายการบริหารความเสี่ยง

นโยบายการบริหารความเสี่ยง เป็นกรอบการดำเนินงานของสำนักงานตรวจสอบภายใน ที่ได้ประยุกต์ใช้หลักการบริหารความเสี่ยงองค์กร (Enterprise Risk Management : ERM) เพื่อกำหนดแนวทางในการดำเนินการบริหารจัดการความเสี่ยงและควบคุมภายในองค์กรให้บรรลุเป้าหมายกลยุทธ์ โดยประกาศนโยบายการบริหารความเสี่ยง ประจำปีงบประมาณ โดยสื่อสารผ่านทางการประชุมสำนักงานตรวจสอบภายใน (ภาพที่ 4) คือ

1) ให้มีบริหารความเสี่ยงทั่วทั้งหน่วยงาน (Enterprise Risk Management : ERM) โดยจะยอมรับความเสี่ยงในระดับปานกลางและความเสี่ยงในระดับน้อยในการปฏิบัติงาน
2) ให้ปฏิเสธที่จะยอมรับความสี่ยงที่เกี่ยวข้องกับการทุจริตทุกกรณี (Anti-Corruption) และจะเป็นแบบอย่างที่ดี มุ่งมั่นสร้างระบบการควบคุม ป้องกัน ตรวจสอบ ให้เกิดความเชื่อมั่นในองค์กร
3) ให้ผู้บริหาร/บุคลากรทุกคนมีส่วนร่วมในการบริหารความเสี่ยง (Participation)
4) ให้นำระบบเทคโนโลยีสารสนเทศที่ทันสมัยมาใช้ในกระบวนการบริหารความเสี่ยง และสนับสนุนให้เจ้าหน้าที่ทุกระดับเข้าถึงสารสนเทศการบริหารความเสี่ยง (IT Support)
5) ให้ติดตามทบทวนความเสี่ยงให้สอดคล้องกับสภาวะแวดล้อมที่เปลี่ยนแปลง (Adapt to Change)
6) ส่งเสริม/กระตุ้นให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กร โดยให้เจ้าหน้าที่ทุกคนตระหนักความสำคัญของการบริหารความเสี่ยง (Risk Awareness Culture)
7) ดำเนินการ/สนับสนุนให้การบริหารความเสี่ยง โดยใช้ทรัพยากรที่มีอย่างจำกัด ให้เกิดประสิทธิภาพเพื่อสามารถจัดการความเสี่ยงได้อย่างเหมาะสม (Efficient under limited resource)

ภาพที่ 4 นโยบายการบริหารความเสี่ยง

หลักการและความจำเป็นของการบริหารความเสี่ยงและควบคุมภายใน

การบริหารความเสี่ยง

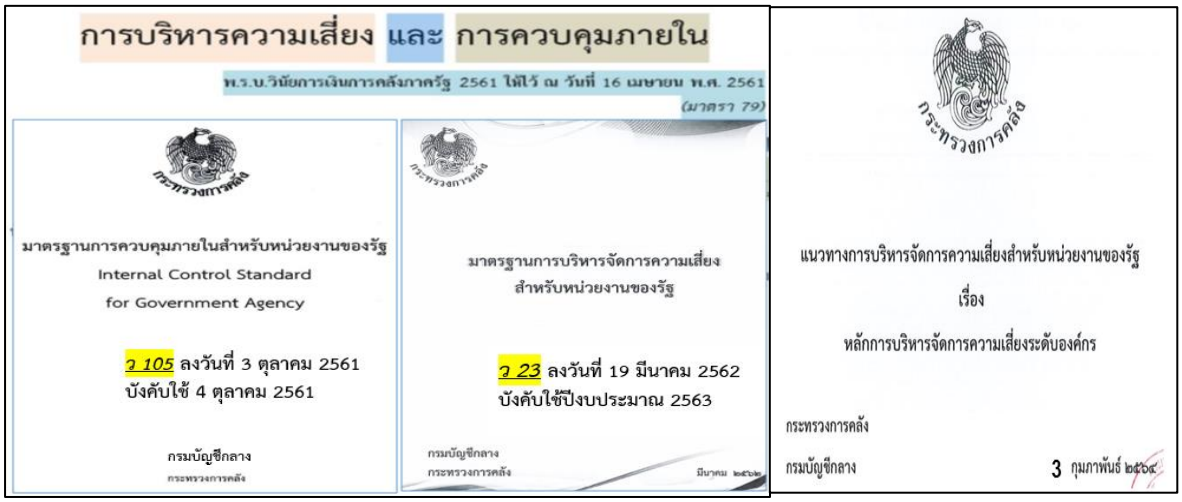
สำนักงานตรวจสอบภายใน ต้องปฏิบัติตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 ตามหนังสือ กค 0409.4/ว 23 ลงวันที่ 19 มีนาคม 2562 ตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ.2562 มาตรา 79 บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด (ภาพที่ 5)

การควบคุมภายใน

สำนักงานตรวจสอบภายใน ต้องปฏิบัติตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2562 ตามหนังสือ กค 0409.3/ว 105 ลงวันที่ 5 ตุลาคม 2561 ตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2562 มาตร 79 บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด (ภาพที่ 5)

แนวทางบริหารการบริหารความเสี่ยง

สำนักงานตรวจสอบภายใน ยึดแนวทางบริหารการบริหารความเสี่ยงสำหรับหน่วยงานภาครัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร ตามหนังสือ กค 0409.3/ว 36 ลงวันที่ 3 กุมภาพันธ์ 2564 ซึ่งเป็นกรอบที่กำหนดโดยกรมบัญชีกลาง



ภาพที่ 5 มาตรฐานฯ การบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ พ.ศ. 2562 (ว 23)
มาตรฐานฯ การควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2562 (ว 105)
แนวทางบริหารการบริหารความเสี่ยงสำหรับหน่วยงานภาครัฐ (ว 36)

โครงสร้างการบริหารความเสี่ยง

สำนักงานตรวจสอบภายใน กำหนดให้การบริหารความเสี่ยงเป็นหน้าที่และความรับผิดชอบของทุกคนในองค์กร ตามคำสั่งสำนักงานตรวจสอบภายในที่ 1/2566 เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน สั่ง ณ วันที่ 15 มีนาคม 2566 โดยกำหนดโครงสร้างการบริหารความเสี่ยงของสำนักงานตรวจสอบภายใน ตามโครงสร้างการบริหารหน่วยงาน ซึ่งอยู่ในรูปแบบของคณะกรรมการบริหารความเสี่ยงและควบคุมภายในของสำนักงานตรวจสอบภายใน โดยมีโครงสร้างคณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน ดังภาพด้านล่างนี้

ภาพที่ 6 โครงสร้างคณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน สำนักงานตรวจสอบภายใน

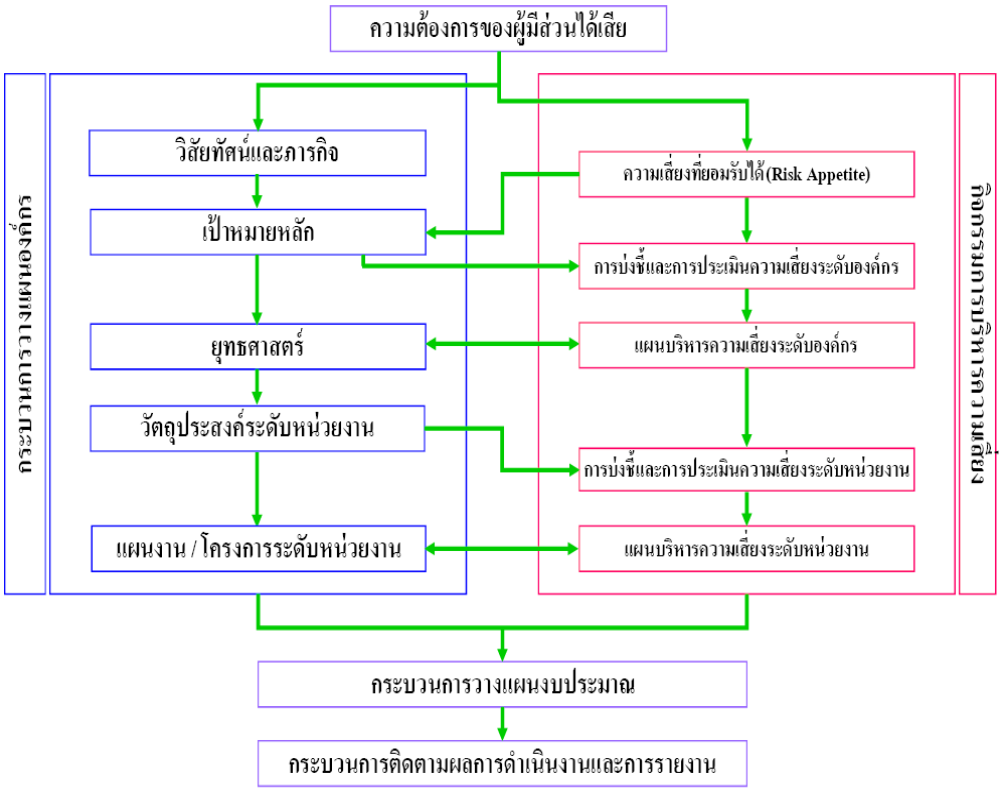
หน้าที่ความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

หน้าที่ความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง ตามคำสั่งสำนักงานตรวจสอบภายในที่ 1/2566 เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน ได้กำหนดความรับผิดชอบของคณะกรรมการบริหารความเสี่ยงและการควบคุมภายในไว้ ดังนี้

1. จัดทำแผนการบริหารจัดการความเสี่ยง
2. ติดตามประเมินผลการบริหารจัดการความเสี่ยง
3. จัดทำรายงานผลตามแผนบริหารจัดการความเสี่ยง
4. พิจารณาทบทวนแผนการบริหารจัดการความเสี่ยง
5. จัดให้มีระบบการควบคุมภายใน

ความเชื่อมโยงระหว่างการบริหารความเสี่ยงกับยุทธศาสตร์ของหน่วยงาน

ความเชื่อมโยงระหว่างการบริหารความเสี่ยงกับยุทธศาสตร์ของหน่วยงานการบริหารความเสี่ยงระดับหน่วยงานมีส่วนในการสนับสนุนการดำเนินงานตามยุทธศาสตร์ขององค์กร โดยจัดให้มีการประเมินความเสี่ยงที่อาจส่งผลต่อการบรรลุวัตถุประสงค์ เชิงยุทธศาสตร์ พร้อมทั้งดำเนินการจัดทำแผนบริหารความเสี่ยง เพื่อจัดการกับความเสี่ยงที่มีค่าความเสี่ยงสูง ซึ่งมีการติดตามการดำเนินงานโดยหน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยงทั้งระดับหน่วยงานและระดับองค์กรการบริหารความเสี่ยงระดับหน่วยงานเป็นหน้าที่ความรับผิดชอบของหน่วยงานคณะ/สำนัก/ศูนย์สำนัก/สำนักงานต่างๆ เพื่อดำเนินการระบุและประเมินความเสี่ยงที่อาจส่งผลกระทบต่อวัตถุประสงค์ของสายงานและหน่วยงานในสังกัด (ภาพที่ 6)



ภาพที่ 7 ความเชื่อมโยงระหว่างการบริหารความเสี่ยงกับยุทธศาสตร์ของหน่วยงาน

ที่มา : องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย (2563: 22)

ภาพที่ 8 ความเชื่อมโยงระหว่างการบริหารความเสี่ยงกับยุทธศาสตร์ พันธกิจ และวิสัยทัศน์

หลักเกณฑ์ประเมินด้านการบริหารความเสี่ยงและควบคุมภายใน

หลักเกณฑ์ประเมินด้านการบริหารความเสี่ยงและควบคุมภายใน ประกอบด้วย 5 หลักเกณฑ์ ดังนี้

- หลักเกณฑ์ 1 ธรรมาภิบาลและวัฒนธรรมองค์กร (Governance and Culture)
- หลักเกณฑ์ 2 การกำหนดยุทธศาสตร์และวัตถุประสงค์/เป้าประสงค์เชิงยุทธศาสตร์ (Strategy & Objectives Setting)
- หลักเกณฑ์ 3 กระบวนการบริหารความเสี่ยง (Performance)
- หลักเกณฑ์ 4 การทบทวนการบริหารความเสี่ยง (Review & Revision)
- หลักเกณฑ์ 5 ข้อมูลสารสนเทศการสื่อสารและการรายงานผล (Information Communication & Reporting)

หลักเกณฑ์ 1 ธรรมาภิบาลและวัฒนธรรมองค์กร (Governance and Culture)

1) Exercises Board Risk Oversight and the development and performance of internal control (บทบาทคณะกรรมการในการกากับติดตามการบริหารความเสี่ยงและการพัฒนาระบบการควบคุมภายใน)

กระบวนการกำหนดนโยบายและการกำกับดูแลด้านการบริหารความเสี่ยงและการควบคุมภายในแบบบูรณาการ (GRC 1) การกำหนดโครงร่างและบทบาทหน้าที่ที่เกี่ยวข้องกับการบริหารความเสี่ยงและการควบคุมภายใน การกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite : RA) ระดับหน่วยงาน กระบวนการจัดทำคู่มือและการ

สื่อสารคู่มือที่เป็นแนวปฏิบัติที่ดีและชัดเจน การสร้างบรรยากาศ วัฒนธรรม ความตระหนักในการบริหารความเสี่ยง และมีการติดตามประเมินระดับการรับรู้ ความเข้าใจ ความตระหนักที่เป็นระบบ รวมทั้งการพัฒนาและสร้างแรงจูงใจในการบริหาร ความเสี่ยงกับผลการดำเนินงานของหน่วยงานที่เป็นรูปธรรมการกำหนดนโยบายที่บูรณาการในเรื่องกำกับดูแลกิจการที่ดีการบริหารความเสี่ยงและการควบคุมภายใน (GRC) รวมทั้งการกำหนดหลักการในการกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite : RA) ระดับหน่วยงาน โดยคณะกรรมการบริหารความเสี่ยงของหน่วยงาน

1. การเผยแพร่นโยบาย กำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน (GRC) แก่บุคลากรในหน่วยงาน และผู้มีส่วนได้เสียอย่างทั่วถึง

2. นำนโยบายที่บูรณาการในเรื่องกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) ไปปฏิบัติอย่างเป็นรูปธรรม

3. การทบทวนนโยบายกากับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) เพื่อให้เหมาะสมกับ นโยบายอื่นๆ ที่เกี่ยวข้องของหน่วยงาน

4. การปรับปรุงนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) ให้สอดคล้องกับบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ และมาตรฐานสากลที่เปลี่ยนแปลงไป

.....

1 GRC ย่อมาจาก “Governance Risk and Compliance” เป็นแนวคิดใหม่ที่รวมองค์ประกอบ 3 องค์ประกอบเข้าด้วยกัน ได้แก่ องค์ประกอบที่ 1 Governance, องค์ประกอบที่ 2 Risk Management และ องค์ประกอบที่ 3 Regulatory Compliance

2) โครงสร้างและบทบาทหน้าที่ (Establishes Operating structures)

1. การมีหน่วยงานเพื่อจัดการความเสี่ยงและการควบคุมภายในที่ชัดเจนโดยกำหนด โครงสร้างบทบาทหน้าที่ของมีผู้ที่ที่รับผิดชอบการบริหารจัดการความเสี่ยง และการควบคุมภายในที่ชัดเจน

2. การกำหนดและสรรหาบุคลากรที่มีคุณสมบัติ และความรู้ความสามารถในการบริหารความเสี่ยงและการควบคุมภายใน อีกทั้งมีการทำงานที่เป็นรูปธรรมอย่างจริงจัง รวมทั้งกำหนดบทบาท อำนาจหน้าที่ และกระบวนการในการดำเนินงานที่ชัดเจนเป็นรูปธรรม (มีการกำหนดหน้าที่งาน Job Description : JD มีโครงสร้างความรับผิดชอบ มีแผนงานรองรับ) และการกำหนดแผนงานของการดำเนินงานตามโครงสร้างผู้รับผิดชอบที่ชัดเจน รวมถึงสามารถบรรลุเป้าหมายในแผนงานได้ครบถ้วน และกระบวนการจัดทำคู่มือการบริหารความเสี่ยงที่มีองค์ประกอบที่ครบถ้วน เพื่อให้สามารถนำไปปฏิบัติได้อย่างชัดเจน

3. โครงสร้างหน่วยงานและคณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน มีการทำงานที่เป็นรูปธรรมอย่างจริงจัง

4. โครงสร้างและบทบาทหน้าที่ด้านการบริหารความเสี่ยงและการควบคุมภายในสอดคล้องกับการกำหนดโครงสร้างและบทบาทหน้าที่ของกระบวนการทำงานอื่น รวมทั้งมีการสื่อสาร ผู้บริหารมีการติดตามผลการดำเนินงานของหน่วยงาน/คณะทางานที่รับผิดชอบฯ โดยสามารถดำเนินงานตามแผนงานของหน่วยงาน และ

สามารถบรรลุเป้าหมายตามแผนการปฏิบัติงานนั้นได้ครบถ้วน และมีกระบวนการในการตรวจสอบถึงความเข้าใจของผู้บริหารและบุคลากรในหน่วยงาน

5. การประเมินประสิทธิผลของการกำหนดโครงสร้างและบทบาทหน้าที่ โดยมีการติดตามผลการดำเนินงานของหน่วยงาน/คณะทำงานที่รับผิดชอบ และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการปฏิบัติงาน กำหนดโครงสร้างและบทบาทหน้าที่ รวมทั้งกระบวนการจัดทำแผนปฏิบัติการของปีต่อไป เพื่อให้เกิดกระบวนการจัดการความเสี่ยงที่บูรณาการจากภายในหน่วยงานและการทบทวน /ปรับปรุง คู่มือการบริหารความเสี่ยง

3) บรรยากาศและวัฒนธรรม สนับสนุนการบริหารความเสี่ยง (Defines Desired Culture)

1. จัดให้มีบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยง (Culture)

2. การกำหนดกระบวนการ/ดำเนินการสร้างความตระหนักเกี่ยวกับความสำคัญ หรือความรู้ความเข้าใจของการบริหารความเสี่ยงในหน่วยงาน โดยครอบคลุมทั้งผู้บริหารและบุคคลากรในหน่วยงาน

3. ทำการฝึกอบรม/ ชี้แจง/ ทำความเข้าใจถึงพื้นฐานด้านการบริหารความเสี่ยง โดยมีเกิดความรู้แก่ผู้บริหารและบุคคลากรที่เกี่ยวข้อง (Risk Owner) และประเมินความรู้ความเข้าใจ

4. กระบวนการ / ดำเนินการสร้างความตระหนักเกี่ยวกับความสำคัญ / ความรู้ความเข้าใจของการบริหารความเสี่ยงในหน่วยงาน ให้มีความสอดคล้องกับกระบวนการพัฒนาบุคลากร และหัวข้ออื่นที่เกี่ยวข้อง เช่น แผนพัฒนาบุคลากร ซึ่งเป็นแผนด้านทรัพยากรบุคคล (Human Resource : HR) เป็นต้น

5. การสำรวจทัศนคติของบุคลากรในเรื่องการบริหารความเสี่ยงขององค์กร และสามารถสรุปผลการสำรวจเสนอผู้บริหารในสายงานที่เกี่ยวข้อง โดยมีแผนงานในการปรับปรุงจากข้อสังเกตที่ได้จากการสำรวจ รวมถึงผลการสำรวจต้องดีขึ้นจากปีที่ผ่านมา หรือจากผลการสำรวจครั้งล่าสุด

4) ความมุ่งมั่นต่อค่านิยมองค์กร (Demonstrates Commitment to Core Values)

1. การกำหนดกระบวนการในการสร้างวัฒนธรรมองค์กรด้านความเสี่ยงที่มุ่งตอบสนอง และส่งเสริมค่านิยมองค์กร

2. การทบทวนสถานการณ์ความเสี่ยงที่จะช่วยให้ทุกคนเข้าใจถึงความสัมพันธ์และผลกระทบของความเสี่ยงก่อนตัดสินใจของคณะกรรมการบริหารความเสี่ยงและการควบคุมภายในของหน่วยงาน อีกทั้งกระบวนการในการกระตุ้นให้เกิดการรับรู้ถึงความเสี่ยงในหน่วยงานและการสร้างบรรยากาศและวัฒนธรรมสนับสนุนการบริหารความเสี่ยง

3. การพัฒนาและสร้างพฤติกรรมในการสร้างวัฒนธรรมองค์กรด้านความเสี่ยงที่มุ่งตอบสนองและส่งเสริมค่านิยมองค์กร โดยครอบคลุมทั้งคณะกรรมการบริหารความเสี่ยงและการควบคุมภายในของหน่วยงาน

4. กระบวนการสร้างความตระหนักเกี่ยวกับความสำคัญ ความรู้ความเข้าใจของการบริหารความเสี่ยงในหน่วยงาน มีความสอดคล้องกับกระบวนการพัฒนาบุคลากร และหัวข้ออื่นที่เกี่ยวข้อง เช่น แผนพัฒนาบุคลากร ซึ่งเป็นแผนด้านทรัพยากรบุคคล (Human Resource: HR) เป็นต้น

5. การสำรวจทัศนคติ/พฤติกรรมของพนักงานในเรื่องการส่งเสริมพฤติกรรมในการสร้างวัฒนธรรมองค์กรด้านความเสี่ยงที่มุ่งตอบสนองค่านิยมองค์กร และสามารถสรุปผลการสำรวจเสนอผู้บริหารในสายงานที่เกี่ยวข้อง โดยมีแผนงานในการปรับปรุงจากข้อสังเกตที่ได้จากการสำรวจ รวมถึงผลการสำรวจต้องดีขึ้นจากปีที่ผ่านมา หรือจากผลการสำรวจครั้งล่าสุด

5) แรงจูงใจ การพัฒนาและการรักษาบุคลากร (Attracts, Develops, and Retains Capable Individuals)

1. การกำหนดแผนงานในการเชื่อมโยงผลการประเมินเฉพาะการบริหารความเสี่ยงกับผลตอบแทน/แรงจูงใจในการประเมินผู้บริหารแต่ละระดับอย่างชัดเจน (Incentive)

2. ดำเนินการได้จริงในการเชื่อมโยงผลการประเมินเฉพาะการบริหารความเสี่ยงกับผลตอบแทน/แรงจูงใจในการประเมินผู้บริหารแต่ละระดับอย่างชัดเจน

3. การถ่ายทอดตัวชี้วัดระดับองค์กรลงสู่ระดับสายงาน โดยเฉพาะตัวชี้วัดการบริหารความเสี่ยงทั้งในลักษณะของปัจจัยเสี่ยงของสายงาน และกิจกรรมที่สายงานต้องสนับสนุนการบริหารความเสี่ยง โดยทุกฝ่ายงาน/สายงานที่องค์กรต้องมีการจัดทำ Risk Profile ของแต่ละสายงานและสามารถผูกแรงจูงใจในแต่ละขั้นกับ Risk Profile ของฝ่ายงานในแต่ละระดับที่สามารถลดระดับความรุนแรงลงได้ครบถ้วน

4. กระบวนการเชื่อมโยงผลการประเมินเฉพาะการบริหารความเสี่ยง มีความเชื่อมโยงกับกระบวนการบริหารทุนมนุษย์ ในการประเมินผลการดำเนินงาน และการถ่ายทอดความเสี่ยงระดับสายงานสอดคล้องกับการวิเคราะห์แผนงานโครงการ และการประเมินความเสี่ยงแผนงานของแต่ละสายงาน

5. การทบทวนแนวทางการกำหนดการเชื่อมโยงผลการประเมินเฉพาะการบริหารความเสี่ยงกับผลตอบแทน/แรงจูงใจในการประเมิน

หลักเกณฑ์ 2 การกำหนดยุทธศาสตร์และวัตถุประสงค์/เป้าประสงค์เชิงยุทธศาสตร์ (Strategy & Objectives Setting)

กระบวนการในการกำหนดวัตถุประสงค์เชิงยุทธศาสตร์ และยุทธศาสตร์การวางแผนการลงทุนที่สำคัญที่เชื่อมโยงกับการกระบวนการบริหารความเสี่ยงหน่วยงาน รวมทั้งการกำหนดเป้าหมายการบริหารความเสี่ยง (Risk Appetite) ที่สอดคล้องกับเป้าประสงค์/เป้าหมายของหน่วยงาน รวมทั้งการสร้างมูลค่าเพิ่มองค์กรด้วยการบริหารความเสี่ยง Value Creation และ Value Enhancement เพื่อให้สามารถตอบสนองและเชื่อมโยงกับวัตถุประสงค์เชิงยุทธศาสตร์และสร้างมูลค่าเพิ่มให้กับมหาวิทยาลัยราชภัฏเชียงใหม่ได้

1) Analyzes Business Context (การวิเคราะห์ธุรกิจ)

ประเมินในหัวข้อการวางแผนเชิง กลยุทธ์-การวิเคราะห์ธุรกิจการวางแผนเชิงกลยุทธ์หัวข้อย่อย-การวิเคราะห์สภาพแวดล้อม (Environmental Scanning)

2) การระบุเป้าหมายการบริหารความเสี่ยง (Risk Appetite : RA) (Defines Risk Appetite)

1. กระบวนการในการกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) ในลักษณะของระดับที่เป็นเป้าหมาย (ค่าเดียว) หรือช่วง (Risk Appetite) และการกำหนดช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance : RT)

2. การระบุ Risk Appetite และ Risk Tolerance โดยสามารถแสดงให้เห็นถึงความเชื่อมโยง/ความสอดคล้องกับเป้าหมาย/วัตถุประสงค์ของหน่วยงานได้อย่างชัดเจน (Business Objective) และคำนึงถึงความต้องการของผู้มีส่วนได้เสียทุกกลุ่มต้องมีการถ่ายทอด Risk Appetite/ Risk Tolerance ที่ถ่ายทอดจากวัตถุประสงค์เชิงธุรกิจ Business Objective โดยสามารถระบุได้ว่าเป็น Strategic Risk/Operational Risk/ Financial Risk และ Compliance Risk (S-O-F-C) หรือประเภทความเสี่ยงตามที่กำหนด

3. มีกระบวนการในการสื่อสารและถ่ายทอดความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance: RT) ต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องที่สอดคล้องตามสาเหตุของแต่ละปัจจัยเสี่ยงที่กำหนด

4. การดำเนินการกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) ต้องสอดคล้องกับเป้าหมายขององค์กรประจำปีบัญชี (Business Objective) ที่ระบุในแผนยุทธศาสตร์ (แผนระยะยาว) และแผนปฏิบัติการประจำปี และมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance: RT) โดยมีความสอดคล้องกับระดับขององค์กรที่ยอมให้เบี่ยงเบนได้ที่ระบุในแผนปฏิบัติการประจำปี หรือเป็นค่าที่ผ่านการอนุมัติจากคณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน

5. มีการประเมินประสิทธิผลของการกำหนดค่าความเสี่ยงที่ยอมรับได้ (Risk Appetite: RA) และระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance: RT) ที่สอดคล้องกับเป้าหมายองค์กร (Business Objective) ที่มีการเปลี่ยนแปลงระหว่างปีได้ทันกาล และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการบริหารจัดการความเสี่ยง

3) การประเมินทางเลือกและกำหนดยุทธศาสตร์ (Evaluates Alternative Strategies)

ประเมินในหัวข้อการวางแผนเชิงกลยุทธ์ หัวข้อย่อย-การกำหนดยุทธศาสตร์/กลยุทธ์ (Strategic Formulation)

4) การกำหนดวัตถุประสงค์ในการดำเนินธุรกิจเพื่อสร้างมูลค่าเพิ่มให้กับองค์กร (Formulates Business Objectives)

ในส่วนการกำหนด Business Objectives ประเมินในหัวข้อการวางแผนเชิงกลยุทธ์ หัวข้อย่อย-การกำหนดวัตถุประสงค์เชิงยุทธศาสตร์ (Strategic Objective)

1. การทำ Value Creation และ Value Enhancement เพื่อให้เชื่อมโยงกับวัตถุประสงค์เชิงยุทธศาสตร์ในการนำมาบริหารและสร้างมูลค่าเพิ่มให้กับองค์กรได้

2. การระบุเหตุการณ์ที่เป็นโอกาสของธุรกิจ ซึ่งมีความสัมพันธ์กับการระบุโอกาส (Opportunity) ใน SWOT ขององค์กร และได้มีการวิเคราะห์ถึงปัจจัยเสี่ยงของเหตุการณ์ดังกล่าว และนำมาเข้ากระบวนการบริหารความเสี่ยง จนสามารถทำให้ระดับความรุนแรงของปัจจัยเสี่ยงดังกล่าวลดลงด้วยการวิเคราะห์สภาพแวดล้อมทั้งภายในและภายนอกธุรกิจอีกครั้ง

3. การกำหนดแผนบริหารความเสี่ยงสาหรับความเสี่ยงที่ส่งผลในการที่สร้างความมั่นใจถึงการเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) และได้ดำเนินการตามแผนการบริหารความเสี่ยงดังกล่าวครบถ้วน ระดับความรุนแรงของความเสี่ยงที่ส่งผลในการที่สร้างความมั่นใจถึงการเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ลดลงได้ตามเป้าหมายที่กำหนด

4. กระบวนการ/ดำเนินการทำ Value Creation และ Value Enhancement มีความสอดคล้องกับกระบวนการกำหนดตำแหน่งเชิงยุทธศาสตร์ วัตถุประสงค์เชิงยุทธศาสตร์ แผนยุทธศาสตร์องค์กร รวมถึงแผนแม่บทที่เกี่ยวข้อง เช่น แผนงาน KM เป็นต้น

5. มีการประเมินประสิทธิผลของการทำ Value Creation และ Value Enhancement เพื่อให้เชื่อมโยงกับวัตถุประสงค์เชิงยุทธศาสตร์ ในการนำมาบริหารและสร้างมูลค่าเพิ่มให้กับองค์กรที่สอดคล้องกับเป้าหมายองค์กร (Business Objective) รวมทั้งวัตถุประสงค์เชิงยุทธศาสตร์ และยุทธศาสตร์ที่มีการเปลี่ยนแปลงระหว่างปีได้ทันกาล และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการบริหารจัดการความเสี่ยง

หลักเกณฑ์ 3 กระบวนการบริหารความเสี่ยง (Performance)

การระบุขั้นตอนในการระบุความเสี่ยงระดับหน่วยงานที่สอดคล้องกับประเภทความเสี่ยงที่องค์กรกำหนด โดยต้องพิจารณาว่ามี ความเสี่ยงใดบ้างที่เกี่ยวข้องกับยุทธศาสตร์ ทิศทาง และการดำเนินกิจการขององค์กร (Risk Universe) การกำหนด/ประเมินกิจกรรมการควบคุมภายในที่ครอบคลุมกิจกรรมขององค์กร การประเมินระดับความรุนแรงของความเสี่ยงโดยการใช้ฐานข้อมูลในอดีตในการพิจารณา การจัดลำดับความสำคัญ ในการจัดการความเสี่ยงระดับองค์กร จนสามารถนาไปกำหนด แผนในการจัดการ/ตอบสนองความเสี่ยงที่เชื่อมโยงกับกิจกรรมการควบคุมภายในที่มีอยู่ และสัมพันธ์ตามสาเหตุที่ได้กำหนดในการจัดทาการบริหารความเสี่ยงเชิงบูรณาการ (Risk Correlation Map) รวมทั้งการพัฒนาเป็น Portfolio View of Risk) เพื่อให้รู้จักองค์กรสามารถวิเคราะห์และบริหารความเสี่ยงได้ครบกระบวนการที่ดี ที่สามารถสร้างความมั่นใจการบรรลุเป้าหมายองค์กร

1) การระบุปัจจัยเสี่ยง (Identifies Risk)

1. การระบุความเสี่ยงระดับหน่วยงานที่สอดคล้องกับประเภทความเสี่ยงที่หน่วยงานกำหนด โดยต้องพิจารณาว่า มีความเสี่ยงใดบ้างที่เกี่ยวข้องกับการดำเนินกิจการของหน่วยงาน โดยต้องมีการพิจารณาที่มาที่ครอบคลุม ทั้งจากปัจจัยภายใน ปัจจัยภายนอก ยุทธศาสตร์และเป้าหมายที่สำคัญขององค์กรจุดอ่อน ความต้องการ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย ตัวชี้วัดที่สำคัญของหน่วยงาน (Inherent Risk) เพื่อกำหนด Risk Universe

2. กำหนดประสิทธิผลของความเพียงพอของการควบคุม รวมทั้งการพิจารณาถึงระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) หลังจากพิจารณาประสิทธิผลของการควบคุมภายใน โดยมีความเชื่อมโยงกับเป้าหมายประจำปีของหน่วยงาน และสามารถแสดงถึงความเชื่อมโยงระหว่างปัจจัยเสี่ยงที่เหลืออยู่ในปีก่อนหน้ากับปีที่ประเมินได้ชัดเจน มีการประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด มีการสื่อสารปัจจัยเสี่ยงที่มีการระบุต่อ ผู้รับผิดชอบ (Risk Owner) ที่เกี่ยวข้อง

3. กระบวนการในการถ่ายทอดความเสี่ยงระดับหน่วยงานให้กับสายงานที่รับผิดชอบ และมีการระบุความเสี่ยงในระดับสายงานที่รองรับความเสี่ยงหน่วยงานและยุทธศาสตร์หน่วยงาน และแผนงานของสายงาน

4. การดำเนินการระบุความเสี่ยงองค์กรที่สอดคล้องกับกระบวนการและกิจกรรมควบคุมภายใน กระบวนการประเมินประสิทธิผลการควบคุมภายใน รวมทั้งการพิจารณาถึงระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) หลังจากการควบคุมภายใน โดยมีความเชื่อมโยงกับเป้าหมาย ประจำปีของหน่วยงานและสามารถแสดงถึงความเชื่อมโยงระหว่างปัจจัยเสี่ยงที่เหลืออยู่ในปีก่อนหน้ากับปีที่ประเมินได้ชัดเจน

5. มีการประเมินประสิทธิผลของการระบุความเสี่ยงระดับหน่วยงาน และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการบริหารจัดการความเสี่ยง

2) การกำหนดกิจกรรมการควบคุม (Selects and Develops Control Activities)

1. การกำหนดและพัฒนากิจกรรมการควบคุม เพื่อควบคุมความเสี่ยงในแต่ละกิจกรรมของหน่วยงาน

2. มีกระบวนการในการประเมินความเพียงพอของระบบการควบคุมภายใน ประกอบการระบุปัจจัยเสี่ยงระดับหน่วยงาน และทุกสายงาน มีการประเมินกิจกรรมการควบคุมประกอบการวิเคราะห์ปัจจัยเสี่ยงระดับสายงานได้ครบถ้วนทุกสายงาน

3. ทุกสายงานมีการประเมินกิจกรรมการควบคุมประกอบการวิเคราะห์ ปัจจัยเสี่ยงระดับสายงานได้ครบถ้วนทุกสายงาน การประเมิน ประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย, กระบวนการ, ผลผลิต, ระยะเวลาที่แล้วเสร็จ)

4. กิจกรรมการควบคุมที่กำหนด มีการบูรณาการกับกระบวนการพัฒนา เทคโนโลยีดิจิทัลในการนาระบบเทคโนโลยีดิจิทัลมาพัฒนากิจกรรม การควบคุม และกิจกรรมการควบคุมสอดคล้องกับแผนงาน/แผนปฏิบัติการประจาปีที่เกี่ยวข้อง

5. มีการทบทวนกิจกรรมการควบคุมระหว่างปี เพื่อให้กิจกรรมการควบคุมเป็นส่วนหนึ่งของแผนงานจัดการความเสี่ยงที่สนับสนุนให้ความเสี่ยงบรรลุตามเป้าหมายที่กำหนด

3) การประเมินระดับความรุนแรงของปัจจัยเสี่ยง (Assesses Severity of Risk)

1. การกำหนดเกณฑ์ประเมินระดับความรุนแรงทั้งในเชิงโอกาสและผลกระทบโดยแยกปัจจัยเสี่ยง

2. การกำหนดเกณฑ์ประเมินระดับความรุนแรง โดยการใช้ฐานข้อมูลในอดีต หรือการคาดการณ์ในอนาคต เพื่อประกอบกับการกำหนดระดับความรุนแรงของแต่ละปัจจัยเสี่ยง ทั้งนี้การกำหนดระดับความรุนแรง (โอกาสและผลกระทบ) ต้องสัมพันธ์กับขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) เพื่อจัดลำดับ ความเสี่ยงและกำหนดเป้าหมายในเชิงระดับความรุนแรงที่คาดหวังของทุกปัจจัยเสี่ยงได้อย่างชัดเจน การดำเนินการประเมินระดับความรุนแรงรายปัจจัยเสี่ยงได้ ครบถ้วนตามกระบวนการที่กำหนด

3. มีการสื่อสารเกณฑ์การประเมินระดับความรุนแรงของแต่ละปัจจัยเสี่ยงต่อผู้รับผิดชอบ (Risk Owner) ที่เกี่ยวข้อง

4. การกำหนดระดับความรุนแรง มีความเชื่อมโยงกับฐานข้อมูลองค์กรในการใช้ระบบเทคโนโลยีดิจิทัล ในการนำระบบเทคโนโลยีดิจิทัล มาพัฒนาการกำหนดเกณฑ์วัดระดับ ความรุนแรง เพื่อกำหนดเป็นฐานข้อมูล

5. การรายงานผลระดับความรุนแรงของแต่ละปัจจัยเสี่ยงรายไตรมาส เทียบกับเป้าหมายที่คาดหวัง พร้อมวิเคราะห์ถึงปัญหา/อุปสรรค และแนวทางที่จะบรรลุถึง เป้าหมาย และมีการประเมินประสิทธิผลของการกำหนดเกณฑ์ประเมินระดับความ รุนแรง ทั้งในเชิงโอกาส และผลกระทบและนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

4) การจัดลำดับความเสี่ยง (Prioritizes Risks)

1. การกำหนดขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) การกำหนดระดับความเสี่ยง (สูง ปานกลาง ต่ำ) และการจัดลำดับความเสี่ยงของแต่ละปัจจัยเสี่ยง และการจัดทำแผนภาพความเสี่ยง (Risk Profile)

2. การดำเนินการตามขั้นตอนที่สำคัญครบถ้วนและทุกขั้นตอนสามารถเป็นไปตามกระบวนการที่กำหนด

3. การแสดงผลการจัดลำดับความเสี่ยง และรายงานผลรายไตรมาส

4. การบูรณาการกำหนดขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) การกำหนดระดับความเสี่ยง (สูง ปานกลาง ต่ำ) กับเป้าประสงค์ และวัตถุประสงค์เชิงยุทธศาสตร์ขององค์กรและค่าความเสี่ยงที่ยอมรับได้ (Risk Appetite)

5. การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย, กระบวนการ, ผลผลิต, ระยะเวลาที่แล้วเสร็จ) การประเมินประสิทธิผลของการกำหนดขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) และการจัดลำดับความเสี่ยง ของแต่ละปัจจัยเสี่ยง การจัดทำแผนภาพความเสี่ยง (Risk Profile) และนาข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

5) การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยงที่ระบุไว้ (Implements Risk Responses)

1. การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยง (Mitigation) ที่ระบุไว้

2. พิจารณาถึงวิธีการ/แผนงานจัดการความเสี่ยงเพื่อลดผลกระทบ หรือลดโอกาสที่จะเกิดรวมทั้งกระบวนการและหลักเกณฑ์ในการประเมินค่าใช้จ่ายและผลประโยชน์ที่ได้ (Cost Benefit) ในการจัดการความเสี่ยง

ในแต่ละทางเลือกในทุกความเสี่ยงที่เหลืออยู่ (Residual Risk) ที่ผ่านการจัดลำดับความเสี่ยงในการกำหนดเป็นความเสี่ยงระดับองค์กร และสรุปเป็นแผนงานจัดการความเสี่ยงในแต่ละความเสี่ยงระดับองค์กร

3. การกำหนดเกณฑ์ในการพิจารณาแผนงาน/กิจกรรมการควบคุม (ประสิทธิผลการควบคุมภายใน) ร่วมกับการพิจารณาเพื่อกำหนด/คัดเลือก วิธีการจัดการความเสี่ยงในการคัดเลือกวิธีการจัดการความเสี่ยงที่ชัดเจน

4. การบูรณาการ การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยง (Mitigation) กับการวิเคราะห์ความเสี่ยงเชิงบูรณาการ (Risk Correlation Map) และกระบวนการอื่น เช่น การกำหนดกิจกรรมการควบคุมแผนปฏิบัติการต่างๆ ที่เกี่ยวข้อง รวมทั้งการออกแบบระบบงาน (Work System) และกระบวนการ (Work Process) ในการดำเนินงานขององค์กร เป็นต้น

5. มีการประเมินประสิทธิผลของการกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยง (Mitigation) และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

6) การบริหารความเสี่ยงแบบบูรณาการ (Develops Portfolio View) Risk Correlation Map และการจัดทา Portfolio View of Risk

1. การกำหนดกระบวนการในการพิจารณาถึงความสัมพันธ์ของความเสี่ยงและผลกระทบที่ มีระหว่างหน่วยงานต่างๆ ภายในองค์กร โดย Risk Correlation Map ขององค์กร ที่มีการกำหนดสาเหตุของความเสี่ยงในทุกปัจจัยเสี่ยง และสามารถกำหนดระดับความรุนแรงของแต่ละสาเหตุในทุกปัจจัยเสี่ยงการวิเคราะห์ความสัมพันธ์ของปัจจัยเสี่ยง และสาเหตุการวิเคราะห์ผลกระทบทั้งในเชิงปริมาณและเชิงคุณภาพระหว่างปัจจัยเสี่ยงและผลกระทบของสาเหตุ และกระบวนการในการแสดงผลดังกล่าวผ่านแผนภาพ Risk Correlation Map และนำไปกำหนดแผนจัดการความเสี่ยง

2. การดำเนินการจัดทำ Risk Correlation Map ของหน่วยงาน ได้ตามกระบวนการครบถ้วนและดำเนินงานร่วมกันเจ้าของความเสี่ยง (Risk Owner)

3. การกำหนดกระบวนการในการวิเคราะห์ถึงภาพรวมของความเสี่ยง (Portfolio View of Risk) โดยผ่านการวิเคราะห์ถึงในช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ในแต่ละปัจจัยเสี่ยง กับช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ในระดับองค์กร และการจัดทำแบบจำลองที่เหมาะสม/นำแบบจาลองดังกล่าวไปใช้ในการบริหารความเสี่ยงในภาพรวม เพื่อสะท้อนถึงช่วงเบี่ยงเบนที่ยังอยู่ในวิสัยที่องค์กรสามารถจัดการได้

4. การสื่อสารและสร้างความเข้าใจกับ Risk Owner ในการพิจารณาถึงความสัมพันธ์ของความเสี่ยงและผลกระทบที่มีระหว่างหน่วยงานต่างๆ ภายในองค์กรโดย Risk Correlation Map ของหน่วยงาน

5. มีการประเมินประสิทธิผลของการกำหนดการพิจารณาถึงความสัมพันธ์ของความเสี่ยงและผลกระทบที่มีระหว่างหน่วยงานต่างๆ ภายในหน่วยงานโดย Risk Correlation Map และการวิเคราะห์ถึงภาพรวมของความเสี่ยง (Portfolio View of Risk) ของหน่วยงาน และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการบริหารความเสี่ยง

หลักเกณฑ์ 4 การทบทวนการบริหารความเสี่ยง (Review & Revision)

การรายงานผลการบริหารความเสี่ยงที่สอดคล้องพร้อมรายงานผลการดำเนินงานหน่วยงานเพื่อให้สามารถวิเคราะห์ประเด็นที่อาจเกิดขึ้นใหม่ การเปลี่ยนแปลงที่สำคัญ รวมทั้งการทบทวนและปรับปรุงการ บริหารความเสี่ยงสม่ำเสมอ และทำการปรับปรุงเมื่อจำเป็น

1) การทบทวนและปรับปรุงผลการบริหารความเสี่ยง (Reviews Risk and Performance)

1. การกำหนดกระบวนการในการทบทวนและปรับปรุงผลความเสี่ยง สม่ำเสมอตามสภาพแวดล้อมที่เปลี่ยนแปลงไป โอกาสที่เกิดขึ้น หรือในกรณีที่ผลการบริหารความเสี่ยงไม่เป็นไปตามเป้าหมายที่กำหนด

2. การบริหารและประเมินผลการบริหารความเสี่ยงที่เกิดขึ้นจริงโดยการติดตามผลการดำเนินงานตามกิจกรรมในแผนบริหารความเสี่ยง รวมทั้งเป้าหมายการบริหารความเสี่ยงทั้งในเชิงของระดับความรุนแรง และค่าเป้าหมาย (Risk Appetite) ที่กำหนด พร้อมรายงานผลการดำเนินงานขององค์กร (Performance) เพื่อให้สามารถวิเคราะห์ประเด็นความเสี่ยงที่อาจเกิดขึ้นใหม่ จากการเปลี่ยนแปลงที่สำคัญ

3. การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย, กระบวนการ, ผลผลิต, ระยะเวลาที่แล้วเสร็จ)

4. การทบทวนและปรับปรุงผลความเสี่ยง และผลการบริหารความเสี่ยงที่เกิดขึ้นจริง มีความเชื่อมโยงกับกระบวนการปรับเปลี่ยนแผนงาน (ตามปกติ และสถานการณ์เปลี่ยนแปลงอย่างรวดเร็ว) วัตถุประสงค์เชิงยุทธศาสตร์ขององค์กร วิสัยทัศน์และตัวชี้วัดที่สำคัญ และกระบวนการติดตามผลการดำเนินงานตามแผนงานและตัวชี้วัดที่สำคัญขององค์กร เช่น แผนปฏิบัติการ แผนการบริหารทรัพยากรบุคคล เป็นต้น

5. มีการประเมินประสิทธิผลของการทบทวนและปรับปรุงผลการบริหารความเสี่ยง และนาข้อมูลไปใช้เพื่อปรับปรุงกระบวนการบริหารจัดการความเสี่ยง

2) การกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยง (Pursues Improvement in Enterprise Risk Management)

1. การกำหนดขั้นตอนในการปรับปรุงกระบวนการบริหารความเสี่ยงองค์กร ทั้งในเชิงกระบวนการบริหารความเสี่ยงและการสร้างวัฒนธรรม ความตระหนักในองค์กร รวมทั้งศักยภาพบุคลากรในด้านการบริหารความเสี่ยง

2. การดำเนินงานปรับปรุงและพัฒนากระบวนการบริหารความเสี่ยงองค์กร ตามขั้นตอนที่กำหนดได้ครบทุกขั้นตอน

3. การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย, กระบวนการ, ผลผลิต, ระยะเวลาที่แล้วเสร็จ)

4. การทบทวนกระบวนการของการกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยงมีความเชื่อมโยงกับกระบวนการปรับเปลี่ยนแผนงาน วัตถุประสงค์เชิงยุทธศาสตร์ขององค์กร วิสัยทัศน์ และตัวชี้วัดที่สำคัญ และกระบวนการติดตามผลการดำเนินงานตามแผนงานและตัวชี้วัดที่สำคัญขององค์กร

5. มีการประเมินประสิทธิผลของการกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยงและนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

3) การประเมินการเปลี่ยนแปลงที่มีนัยสำคัญ (Assesses Substantial Change)

ประเมินในหัวข้อการวางแผนเชิงกลยุทธ์ หัวข้อย่อย-กระบวนการติดตาม ผลสำเร็จตามแผนปฏิบัติการและปรับเปลี่ยนแผนงาน (Monitoring & Review)

หลักเกณฑ์ 5 ข้อมูลสารสนเทศการสื่อสารและการรายงานผล (Information Communication & Reporting)

เกณฑ์การประเมินผลมีประเด็นของการพิจารณาเพิ่มเติมจาก 3 องค์ประกอบย่อยข้างต้น รวมในส่วนของการรายงานความเสี่ยง ในส่วนของการพิจารณาการประเมินผลการควบคุมภายใน ทั้งการประเมินเป็นรายครั้ง และประเมินแบบต่อเนื่อง (Control Self Assessment)

1) การสื่อสารการบริหารความเสี่ยงองค์กร (Communicates Risk Information)

1. การกำหนดกระบวนการและช่องทางในการสื่อสารการบริหารความเสี่ยงหน่วยงาน ในการสร้างความรู้ความเข้าใจ ความตระหนักเรื่องการบริหารความเสี่ยงรวมทั้งกระบวนการสำรวจระดับการรับรู้ความตระหนักและทัศนคติของพนักงานในเรื่องการบริหารความเสี่ยงและการควบคุมภายใน

2. การสื่อสารและสร้างความรู้ความเข้าใจ ความตระหนักเรื่องการบริหารความเสี่ยงและการควบคุมภายในครอบคลุมทุกกลุ่มบุคลากร และหน่วยงานเจ้าของความเสี่ยง (Risk Owner) และผู้บริหารเกิดขึ้นจริง

3. การสื่อสารและสร้างความรู้ความเข้าใจ ความตระหนักเรื่องการบริหาร ความเสี่ยงและการควบคุมภายในฯ มีผลของระดับความรู้ความเข้าใจและ ความตระหนักเป็นไปตามเป้าหมายที่กำหนด และดีกว่าปีที่ผ่านมา

4. การทบทวนและปรับปรุงช่องทางในการสื่อสาร มีความเชื่อมโยงกับกระบวนการพัฒนาบุคลากร และการพัฒนาเทคโนโลยีดิจิทัล เช่น แผนการบริหารทรัพยากรบุคคล เป็นต้น

5. การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย, กระบวนการ, ผลผลิต, ระยะเวลาที่ แล้วเสร็จ)

2) การติดตาม ประเมินผลและรายงานผล การบริหารความเสี่ยงการควบคุมภายใน วัฒนธรรมและผลการดำเนินงาน (Reports on Risk, Internal Control, Culture, and Performance)

1. มีกระบวนการรายงานผลการบริหารความเสี่ยงตามแผนจัดการความเสี่ยง (Mitigation Plan) และกิจกรรมการควบคุม (Existing Control) ที่กำหนด ครบถ้วน โดยรายงานผลต่อผู้บริหารสายงานคณะกรรมการบริหาร และ คณะกรรมการบริหารความเสี่ยงเป็นรายไตรมาส และนำส่งรายงานการประเมินผลการควบคุมภายในตามหลักเกณฑ์การปฏิบัติการควบคุมภายใน สำหรับหน่วยงานของรัฐ ได้ครบถ้วนและเป็นไปตามระยะเวลาที่กำหนด

2. แนวทางแก้ไขเพื่อให้มั่นใจว่าจะบรรลุเป้าหมายการบริหารความเสี่ยงได้ตามแผนงานที่กำหนดโดยรายงานผลต่อคณะกรรมการบริหารความเสี่ยงเป็นรายไตรมาส ครบทุกไตรมาส

3. กระบวนการรายงานผลการบริหารความเสี่ยงสามารถเชื่อมโยงกับการพัฒนา ระบบสารสนเทศ/ระบบดิจิทัลของหน่วยงานในการติดตามและรายงานผลการดำเนินงาน

4. การรายงานผลการบริหารความเสี่ยงมีองค์ประกอบครบถ้วน และรายงานผลได้ครบทุกไตรมาส โดยมีความเชื่อมโยงและสอดคล้องกับความคืบหน้าของการติดตามผลตามแผนปฏิบัติการประจาปีที่เกี่ยวข้อง และรายงานผลพร้อมการรายงานผลการดำเนินงานขององค์กร (Performance) และเชื่อมโยงกับการ พัฒนาระบบเทคโนโลยีดิจิทัลที่สนับสนุนกระบวนการบริหารความเสี่ยง และ ระบบเตือนภัยล่วงหน้า (Early Warning System: EWS)

5. มีการทบทวน/ปรับปรุง กระบวนการรายงานผลการบริหารความเสี่ยง

3) ข้อมูลและเทคโนโลยีในการสนับสนุนการบริหารความเสี่ยง (Leverages Information and Technology)

1. การกำหนดกระบวนการพัฒนาระบบเทคโนโลยีดิจิทัล ที่สนับสนุนกระบวนการบริหาร ความเสี่ยง และกระบวนการพัฒนาระบบเตือนภัยล่วงหน้า (Early Warning System: EWS) ที่เชื่อมโยงกับเป้าหมายหน่วยงาน

2. ดำเนินการพัฒนาระบบเทคโนโลยีสารสนเทศที่สนับสนุนการเก็บรวบรวมข้อมูลการรายงานและวิเคราะห์ระดับความรุนแรง และระบบ Early Warning System รวมทั้ง กระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และใช้งานระบบได้จริงรวมทั้งข้อมูลมีความทันกาล

3. พัฒนาระบบเทคโนโลยีสารสนเทศที่สนับสนุนการเก็บรวบรวมข้อมูล การรายงานและวิเคราะห์ระดับความรุนแรง และระบบ Early Warning System รวมทั้งกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และใช้งานระบบได้จริง รวมทั้งข้อมูลมีความทันกาล และมีการสื่อสารให้หน่วยงานที่เกี่ยวข้องใช้งานระบบได้อย่างครบถ้วน

4. การพัฒนาระบบเทคโนโลยีสารสนเทศที่สนับสนุนการเก็บรวบรวมข้อมูล การรายงาน และวิเคราะห์ระดับความรุนแรง และระบบ Early Warning System รวมทั้ง กระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) มีความเชื่อมโยงและสอดคล้องกับแผนปฏิบัติการดิจิทัล รวมทั้งการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation)

5. มีการประเมินประสิทธิผลของ การกำหนดกระบวนการพัฒนาระบบเทคโนโลยีดิจิทัล ที่สนับสนุนกระบวนการบริหารความเสี่ยง และนาข้อมูลไปใช้ เพื่อปรับปรุงกระบวนการบริหารจัดการความเสี่ยง

นิยามของการบริหารความเสี่ยง

เพื่อให้การใช้คำที่เกี่ยวกับความเสี่ยงเป็นที่เข้าใจในแนวทางเดียวกันและใช้ร่วมกันหน่วยงาน จึงกำหนดคำนิยามเกี่ยวกับความเสี่ยงไว้ ดังนี้

1) ความเสี่ยง (Risk) หมายถึง ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ของหน่วยงาน

2) ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทาให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไรและทำไม

ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้องปัจจัยเสี่ยงพิจารณาได้จาก

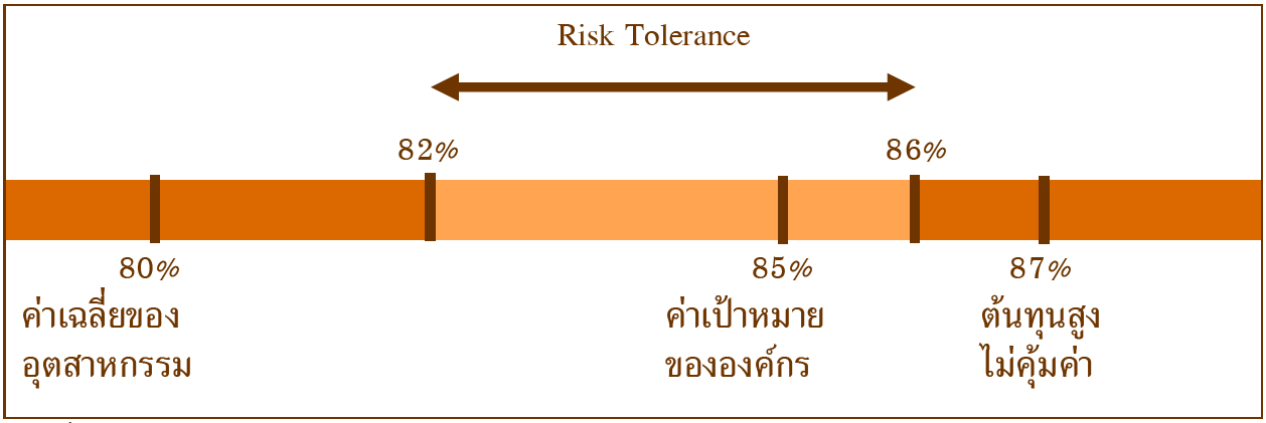
1) ปัจจัยภายนอก เช่น เศรษฐกิจ สังคม การเมือง กฎหมาย ฯลฯ

2) ปัจจัยภายใน เช่น กฎ ระเบียบ ข้อบังคับภายในองค์กร ประสบการณ์เจ้าหน้าที่ระบบการทางาน ฯลฯ

3) การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน รวมถึงเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

4) การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการที่ใช้ในการวิเคราะห์และจัดลาดับความเสี่ยงที่ส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรซึ่งการกำหนดระดับความเสี่ยงจะพิจารณาจากผลกระทบ (Impact/Impact) และโอกาสที่จะเกิด (Likelihood/Frequency)

5) ความเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับความเบี่ยงเบนจากเกณฑ์หรือประเภทของความเสี่ยงที่ยอมรับได้ ซึ่งค่าความเบี่ยงเบนจะเป็นช่วงที่ยอมให้ผลการดำเนินงานเบี่ยงเบนหรือคลาดเคลื่อนไปจากเป้าหมายที่กำหนดโดยจะต้องมีความสัมพันธ์กับระดับความเสี่ยงที่ยอมรับได้



ภาพที่ 9 ตัวอย่างการกำหนด Risk Tolerance

ที่มา : คู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน, กระทรวงการคลัง (2555: 133)

6) ความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ประเภทและเกณฑ์ของความเสี่ยงหรือความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้โดยยังคงให้องค์กรสามารถบรรลุเป้าหมาย ซึ่งความเสี่ยงที่ยอมรับได้นั้น จะต้องสอดคล้องกับเป้าหมายขององค์กร ไม่ด้อยกว่าค่าเป้าหมายค่าเดียวหรือระบุเป็นช่วงก็ได้ ทั้งนี้ ขึ้นอยู่กับความเหมาะสมของปัจจัยเสี่ยงแต่ละตัว

7) แผนภูมิความเสี่ยง (Risk Map) หรือ (Risk Profile) หมายถึง แผนภูมิแสดงสถานะของระดับความรุนแรงของปัจจัยเสี่ยงโดยรวม โดยแสดงเป็นพิกัดของโอกาสและผลกระทบ โดยใช้ระดับสีแทนระดับความรุนแรง ทั้งนี้ Risk Profile จะแสดงให้เห็นภาพรวมในการกระจายตัวของปัจจัยเสี่ยงขององค์การ และแสดงให้เห็นถึงขอบเขตของความรุนแรงที่องค์การยอมรับได้ (Risk Boundary) เพื่อให้องค์การได้กำหนดเป็นเป้าหมายในภาพรวมว่าจะต้องบริหารความเสี่ยงจนมีระดับความรุนแรงลดลงจนอยู่ในระดับดังกล่าว

8) เจ้าของความเสี่ยง (Risk Owner) หมายถึง ฝ่าย/สำนักงาน/ศูนย์/กอง/บุคคลหรือกลุ่มบุคคลที่มีความรับผิดชอบโดยตรงต่อการบริหารความเสี่ยงโดยเจ้าของความเสี่ยงจะระบุปัจจัยเสี่ยงและจัดทำแผนจัดการความเสี่ยงซึ่งอาจต้องประสานกับหน่วยงาน/บุคคลที่เกี่ยวข้องกับปัจจัยเสี่ยงนั้นๆอเพื่อลดหรือควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

9) ระดับความเสี่ยง (Degree of Risks) หมายถึงระดับความสำคัญในการบริหารความเสี่ยง โดยพิจารณาจากผลคูณของระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) กับระดับความรุนแรงของผลกระทบ (Impact) ของความเสี่ยงแต่ละสาเหตุ (โอกาส X ผลกระทบ)

10) GRC : Corporate Governance - Risk management - Compliance หมายถึง การกำกับดูแลกิจการ การบริหารความเสี่ยงและการปฏิบัติตามกฎระเบียบ (Corporate Governance, Risk Management & Compliance: GRC) คือ การจัดให้มีบุคลากรที่มีความรู้และคุณสมบัติเหมาะสม (People) ขั้นตอนการทำงานที่โปร่งใส และมีการควบคุมภายในที่ดี (Process) การบริหารจัดการข้อมูลให้ถูกต้องเหมาะสม ทันเวลา (Information) และการใช้เทคโนโลยีอย่างมีประสิทธิภาพ (Technology) เพื่อช่วยให้องค์กรมีการกำกับดูแลกิจการที่ดี มีการบริหารความความเสี่ยงอย่างเป็นระบบ และสามารถปฏิบัติตามกฎระเบียบ ที่เกี่ยวข้องได้อย่างครบถ้วน ทั้งนี้ เพื่อช่วยเพิ่มความมั่นใจว่าองค์กรจะสามารถบรรลุวัตถุประสงค์หรือเป้าหมายที่ตั้งไว้อย่างสมเหตุสมผล

11) ระดับความเสี่ยงก่อนการควบคุม (Inherent Risk) หมายถึง ระดับความเสี่ยงที่เกิดขึ้นจากการดำเนินกิจกรรมต่างๆ ขององค์กร โดยที่ผู้บริหารยังไม่ได้ดำเนินการใดๆ เพื่อลดผลกระทบหรือโอกาสเกิดของความเสี่ยงนั้น การประเมินระดับความเสี่ยงก่อนการควบคุมจะทำให้ผู้บริหารสามารถประมาณการทรัพยากรที่ต้องใช้และระดับการควบคุมที่ต้องมีในการจัดการความเสี่ยง

12) ความเสี่ยงหลังการควบคุม (Residual Risk) หมายถึง ระดับความเสี่ยงคงเหลือหลังจากที่ได้พิจารณาถึงการควบคุมต่างๆ ที่ผู้บริหารกำหนดให้มีในปัจจุบัน การประเมินระดับความเสี่ยงหลังการควบคุม ทำให้ผู้บริหารสามารถพิจารณาได้ว่ามาตรการจัดการความเสี่ยงที่มีอยู่ในปัจจุบันมีประสิทธิภาพเพียงพอหรือไม่ หรือมีการควบคุมเกินความจำเป็น หากระดับความเสี่ยงหลังการควบคุมอยู่ในระดับที่สูงเกินกว่าระดับที่องค์กรยอมรับได้ ผู้บริหารจะต้องกำหนดแผนจัดการความเสี่ยงและดำเนินการตามแผนดังกล่าว_

13) ดัชนีชี้วัดความเสี่ยงหลัก (Key Risk Indicator: KRI) หมายถึง เครื่องมือวัดกิจกรรมที่อาจทำให้หน่วยงานมีความเสี่ยงที่เพิ่มขึ้น เช่น อัตราความพึงพอใจของหน่วยรับตรวจ หรืออัตราการร้องเรียนจากหน่วยรับตรวจที่อาจส่งผลต่อการสุ่มเสี่ยงต่อการไม่ปฏิบัติตามกฎระเบียบ เป็นต้น

14) ความเสี่ยงที่จะเกิดใหม่ (Emerging Risk) หมายถึง ความเสี่ยงที่จะเกิดใหม่เป็นความสูญเสียที่เกิดขึ้นจากความเสี่ยงที่ยังไม่ได้ปรากฏขึ้นในปัจจุบันแต่อาจจะเกิดขึ้นได้ในอนาคตเนื่องจากสภาวะแวดล้อมที่เปลี่ยนไป ความเสี่ยงประเภทนี้เป็นความเสี่ยงที่เกิดขึ้นอย่างช้าๆ ยากที่จะระบุได้ มีความถี่ของการเกิดต่ำแต่เมื่อเกิดขึ้นแล้วจะส่งผลกระทบอย่างรุนแรง ความเสี่ยงที่จะเกิดใหม่นี้มักจะถูกระบุขึ้นมาจากการคาดการณ์บนพื้นฐานของการศึกษาจากหลักฐานที่มีปรากฏอยู่ ความเสี่ยงที่จะเกิดใหม่นี้มักจะเป็นผลมาจากการเปลี่ยนแปลงทางการเมือง กฎหมาย สังคม เทคโนโลยี สภาพแวดล้อมทางกายภาพ หรือการเปลี่ยนแปลงตามธรรมชาติ บางครั้ง

ผลกระทบของความเสี่ยงประเภทนี้อาจจะไม่สามารถระบุได้ในปัจจุบันตัวอย่าง เช่น ปัญหาที่เกิดขึ้นจากนาโนเทคโนโลยี หรือการเปลี่ยนแปลงของสภาวะภูมิอากาศ เป็นต้น

15) ความเสี่ยงด้านทรัพยากร (Resources Risk) หมายถึง ความเสี่ยงที่เกิดจากความไม่พร้อมหรือขาดประสิทธิภาพในการดำเนินงานด้านการเงิน งบประมาณ การควบคุมค่าใช้จ่าย ระบบสารสนเทศด้านอาคารสถานที่

16) ความเสี่ยงด้านยุทธศาสตร์/กลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการวางแผนกลยุทธ์หรือแผนปฏิบัติราชการ รวมถึงการนำไปปฏิบัติที่ไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยต่างๆ ทั้งที่เป็นปัจจัยภายในและภายนอกองค์การ ซึ่งอาจส่งผลกระทบต่อทิศทางการพัฒนาและการบรรลุผลตามเป้าหมายและวัตถุประสงค์ขององค์การ

17) ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ/ข้อบังคับ (Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบหรือข้อบังคับที่เกี่ยวข้องได้ หรือกฎระเบียบที่มีอยู่ไม่เหมาะสม เป็นอุปสรรคต่อการปฏิบัติงาน หรือไม่สามารถปฏิบัติได้ทันตามเวลาที่กำหนด และอาจมีผลต่อการลงโทษตามกฎหมายที่เกี่ยวข้อง ตลอดจนการติดตามผลการปฏิบัติตามกฎระเบียบหรือข้อบังคับที่เกี่ยวข้อง

18) ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk) หมายถึง ความเสี่ยงที่เกิดขึ้นในกระบวนการทำงานตามปกติทุกขั้นตอนไม่ว่าจะเป็นเรื่องของกระบวนการบริหารหลักสูตร การบริหารงานวิจัย ระบบงานระบบประกันคุณภาพว่ามีการดำเนินงานตามขั้นตอนอย่างถูกต้องเหมาะสมและมีระบบควบคุม ตรวจสอบที่ดีเพียงใด ถ้าไม่ดีพอองค์การต้องหาวิธีการในการจัดการไม่ให้ความเสี่ยงนั้นเกิดขึ้นมิฉะนั้นอาจจะส่งผลกระทบต่อความสำเร็จของการดำเนินงานตามแผนปฏิบัติราชการหรือแผนกลยุทธ์ขององค์การ

19) ความเสี่ยงด้านบุคลากรและความเสี่ยงด้านธรรมาภิบาล (Human and Good Governance Risk) หมายถึง ความเสี่ยงที่เกิดจากการขาดประสิทธิภาพในการกำหนดกรอบอัตรากำลังการสรรหาบุคลากรการบรรจุแต่งตั้ง การฝึกอบรม การโยกย้ายและไม่ได้จัดทำข้อกำหนดด้านจริยธรรมไว้อย่างชัดเจนในด้านต่าง ๆ

20) ความเสี่ยงจากเหตุการณ์ภายนอก (External Environment Risk) หมายถึง ความเสี่ยงที่เกิดขึ้นจากสภาพแวดล้อมที่มีการเปลี่ยนแปลงตลอดเวลาและอาจส่งผลกระทบทำให้องค์การไม่สามารถดำเนินการได้สำเร็จตามเป้าหมาย

หลักธรรมาภิบาลของการบริหารบ้านเมืองที่ดี

หลักธรรมาภิบาล (Good Governance) ในการวิเคราะห์ความเสี่ยงนั้น นอกจากส่วนราชการจะพิจารณาปัจจัยเสี่ยงจากด้านต่างๆ แล้วส่วนราชการต้องนาแนวคิดเรื่องธรรมาภิบาลที่เกี่ยวข้องในแต่ละด้านมาเป็นปัจจัยในการวิเคราะห์ความเสี่ยง เช่น (กรมอนามัย, 2558: 2-3)

- ด้านยุทธศาสตร์ โครงการที่คัดเลือกมานั้นอาจมีความเสี่ยงต่อเรื่องประสิทธิผล และการมีส่วนร่วม
- ด้านการดำเนินการ อาจมีความเสี่ยงต่อเรื่องประสิทธิภาพ และความโปร่งใส
- ด้านการเงิน อาจมีความเสี่ยงต่อเรื่องนิติธรรม และภาระรับผิดชอบ
- ด้านกฎ ระเบียบ อาจมีความเสี่ยงต่อเรื่องนิติธรรม และความเสมอภาค

ทั้งนี้ ความเสี่ยงเรื่องธรรมาภิบาลที่อาจเกิดขึ้นจากการดำเนินแผนงาน/โครงการเพื่อให้เป็นไปตามหลักธรรมาภิบาล (Good Governance) (ภาพที่ 9) ได้แก่

1. ประสิทธิผล (Effectiveness)
2. ประสิทธิภาพ (Efficiency)
3. การมีส่วนร่วม (Participation)
4. ความโปร่งใส (Transparency)
5. การตอบสนอง (Responsiveness)
6. ภาระรับผิดชอบ (Accountability)
7. นิติธรรม (Rule of Law)
8. การกระจายอำนาจ (Decentralization)
9. ความเสมอภาค (Equity)
10. การมุ่งเน้นฉันทามติ (Consensus Oriented)

ภาพที่ 10 หลักธรรมาภิบาลของการบริหารบ้านเมืองที่ดี 10 ประการ

ที่มา : https://www.prokfa.go.th/

ส่วนที่ 3
คู่มือการบริหารความเสี่ยง

ที่มาและความสำคัญ

มีข้อกำหนดเกี่ยวกับการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐไว้ในกฎหมายอย่างน้อย 5 ฉบับ ได้แก่

1. พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561
2. มาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายใน สำหรับหน่วยงานของรัฐ พ.ศ.2561 (ว 105)
3. มาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยง สำหรับหน่วยงานของรัฐ พ.ศ.2562 (ว 23)
4. ระเบียบกระทรวงการคลังว่าด้วยการตรวจสอบภายในของส่วนราชการ พ.ศ.2551
5. แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่องหลักการบริหารจัดการความเสี่ยงระดับองค์กร (ว 36)

1. พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561

ตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 ในหมวด 4 มาตรา 79 มีข้อกำหนดเกี่ยวกับการบริหารจัดการความเสี่ยงไว้ใน (ภาพที่ 10) ดังนี้

มาตรา 79 ให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด


หน้า ๑
เล่ม ๑๓๕ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๙ เมษายน ๒๕๖๑

พระราชบัญญัติ
วินัยการเงินการคลังของรัฐ
พ.ศ. ๒๕๖๑

หมวด ๔
การบัญชี การรายงาน และการตรวจสอบ

มาตรา ๗๙ ให้หน่วยงานของรัฐจัดให้มี❶การตรวจสอบภายใน ❷การควบคุมภายในและ
❸การบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

ภาพที่ 11 ข้อกำหนดการบริหารจัดการความเสี่ยงในพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ.2561

2. มาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายใน สำหรับหน่วยงานของรัฐ พ.ศ.2561

มาตรา 79 ให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด และได้จัดทำขึ้นตามมาตรฐานสากล เพื่อเป็นกรอบแนวทางกำหนด ประเมินและปรับปรุงระบบการควบคุมภายในของหน่วยงานภาครัฐ

บทนำ

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ มาตรา ๖๒ วรรคสาม บัญญัติให้รัฐต้องรักษาวินัยการเงินการคลังเพื่อให้ฐานะการเงินการคลังมีเสถียรภาพมั่นคงและยั่งยืน โดยกฎหมายว่าด้วยวินัยการเงินการคลังต้องมีบทบัญญัติเกี่ยวกับกรอบการดำเนินการการคลัง งบประมาณ วินัยรายได้ รายจ่าย ทั้งเงินงบประมาณและเงินนอกงบประมาณ การรับทรัพย์สิน เงินคงคลังและหนี้สาธารณะ ดังนั้น จึงได้กำหนดพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ หมวด ๔ การบัญชี การรายงาน และการตรวจสอบ มาตรา ๗๙ ให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายใน และการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด ซึ่งการควบคุมภายในถือเป็นปัจจัยสำคัญที่จะช่วยให้การดำเนินงานตามภารกิจมีประสิทธิผล ประสิทธิภาพ ประหยัด และช่วยป้องกันหรือลดความเสี่ยงจากการผิดพลาด ความเสียหาย ความสิ้นเปลือง ความสูญเปล่าของการใช้ทรัพย์สิน หรือการกระทำอันเป็นการทุจริต

มาตรฐานการควบคุมภายในสำหรับหน่วยงานของรัฐนี้ ได้จัดทำขึ้นตามมาตรฐานสากลของ The Committee of Sponsoring Organizations of the Treadway Commission : COSO 2013 โดยปรับให้เหมาะสมกับบริบทของระบบการบริหารราชการแผ่นดิน เพื่อใช้เป็นกรอบแนวทางในการกำหนด ประเมินและปรับปรุงระบบการควบคุมภายในของหน่วยงานของรัฐ อันจะทำให้การดำเนินงาน และการบริหารงานของหน่วยงานของรัฐบรรลุผลสำเร็จตามวัตถุประสงค์ เป้าหมาย และมีการกำกับดูแลที่ดี

ภาพที่ 12 บทนำการบริหารจัดการความเสี่ยงในมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายใน สำหรับหน่วยงานของรัฐ พ.ศ.2561

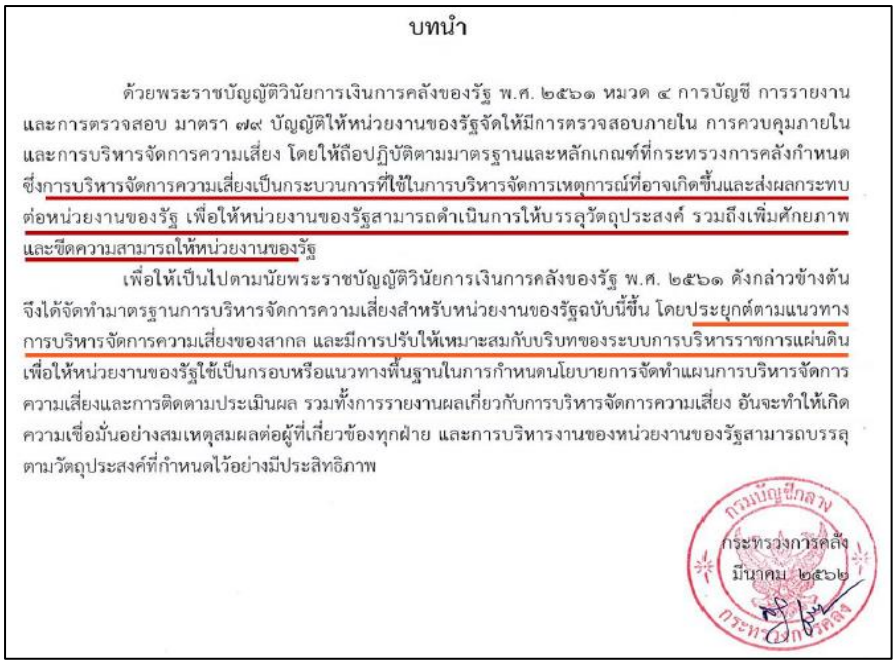
3. มาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ.2562

มาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ.2562 เป็นกฎเกณฑ์ที่ประกาศใช้ในปีงบประมาณ 2562 และเริ่มบังคับใช้ในปีงบประมาณ 2563 ข้อความตอนหนึ่งในบทนำของมาตรฐานฯ ได้กล่าวถึงความสำคัญของการบริหารจัดการความเสี่ยงไว้ (ภาพที่ 12) ดังนี้

> ...การบริหารจัดการความเสี่ยงเป็นกระบวนการที่ใช้ในการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินการให้บรรลุวัตถุประสงค์รวมถึงเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

อีกทั้งยังได้มีการระบุแนวทางการจัดทามาตรฐานฯ ไว้ดังนี้

> ...มีการประยุกต์ตามแนวทางการบริหารจัดการความเสี่ยงของสากล และมีการปรับให้เหมาะสมกับบริบทของระบบการบริหารราชการแผ่นดิน...



บทนำ

ด้วยพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ หมวด ๔ การบัญชี การรายงาน และการตรวจสอบ มาตรา ๗๙ บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายใน และการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด ซึ่งการบริหารจัดการความเสี่ยงเป็นกระบวนการที่ใช้ในการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินการให้บรรลุวัตถุประสงค์ รวมถึงเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

เพื่อให้เป็นไปตามนัยพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ ดังกล่าวข้างต้น จึงได้จัดทำมาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐฉบับนี้ขึ้น โดยประยุกต์ตามแนวทางการบริหารจัดการความเสี่ยงของสากล และมีการปรับให้เหมาะสมกับบริบทของระบบการบริหารราชการแผ่นดิน เพื่อให้หน่วยงานของรัฐใช้เป็นกรอบหรือแนวทางพื้นฐานในการกำหนดนโยบายการจัดทำแผนการบริหารจัดการความเสี่ยงและการติดตามประเมินผล รวมทั้งการรายงานผลเกี่ยวกับการบริหารจัดการความเสี่ยง อันจะทำให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลต่อผู้ที่เกี่ยวข้องทุกฝ่าย และการบริหารงานของหน่วยงานของรัฐสามารถบรรลุตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ

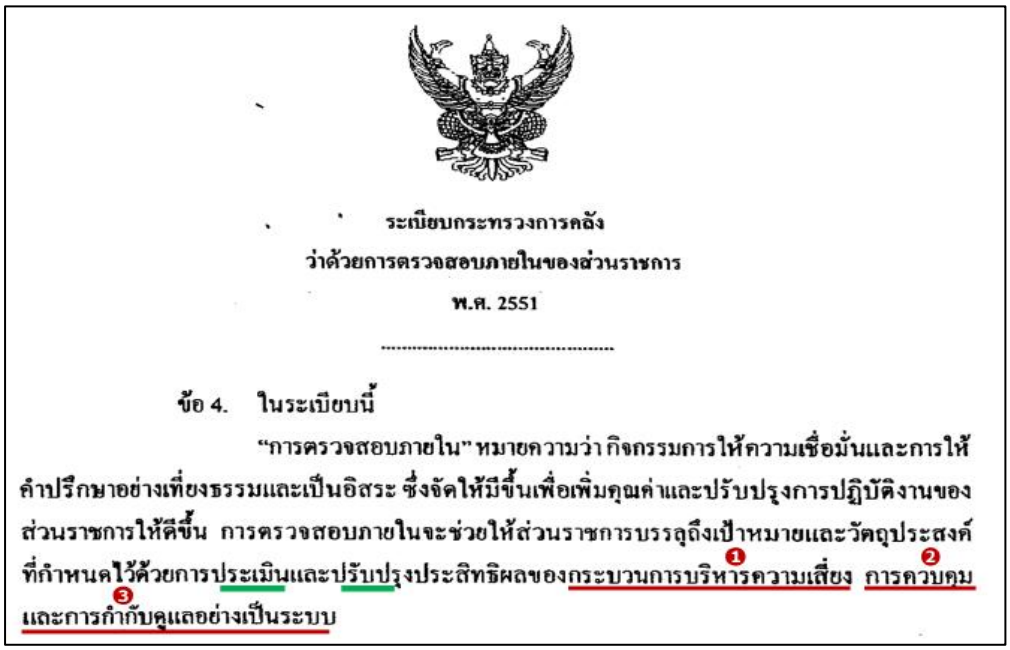
กรมบัญชีกลาง กระทรวงการคลัง มีนาคม ๒๕๖๒

ภาพที่ 13 บทนำในมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ.2562

4. ระเบียบกระทรวงการคลังว่าด้วยการตรวจสอบภายในของส่วนราชการ พ.ศ.2551

ตามระเบียบกระทรวงการคลังว่าด้วยการตรวจสอบภายในของส่วนราชการ พ.ศ.2551 ได้ระบุถึงความสำคัญของการบริหารจัดการความเสี่ยงไว้ (ภาพที่ 13) ดังนี้

> ...การตรวจสอบภายในจะช่วยให้ส่วนราชการบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ ด้วย**การประเมิน**และ**ปรับปรุง**ประสิทธิผลของ**กระบวนการบริหารความเสี่ยง** การควบคุมและการกำกับดูแลอย่างเป็นระบบ



ระเบียบกระทรวงการคลัง
ว่าด้วยการตรวจสอบภายในของส่วนราชการ
พ.ศ. 2551

ข้อ 4. ในระเบียบนี้

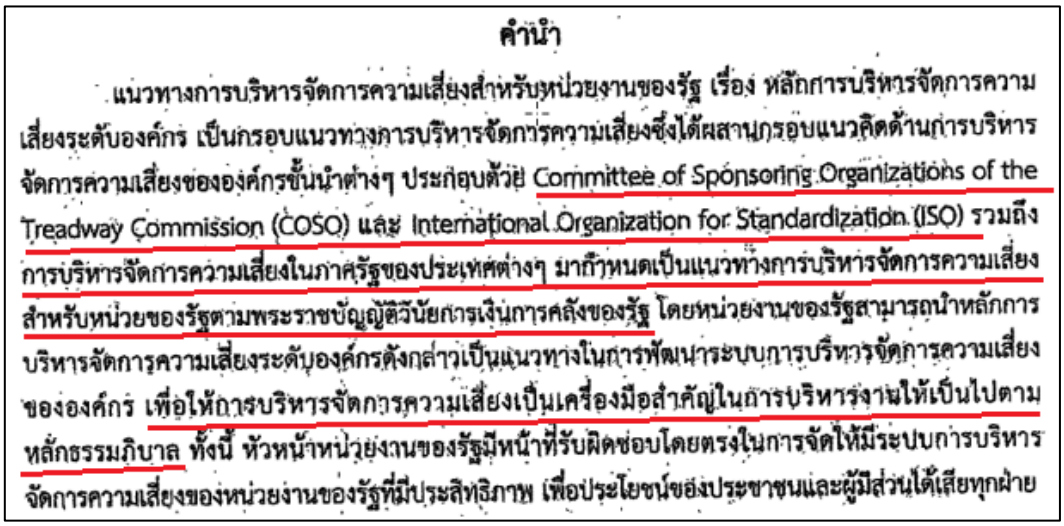
"การตรวจสอบภายใน" หมายความว่า กิจกรรมการให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานของส่วนราชการให้ดีขึ้น การตรวจสอบภายในจะช่วยให้ส่วนราชการบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ

ภาพที่ 14 ระเบียบกระทรวงการคลังว่าด้วยการตรวจสอบภายในของส่วนราชการ พ.ศ.2551

จากข้อมูลข้างต้น สรุปได้ว่าการตรวจสอบภายในด้วยการ**ประเมิน**และ**ปรับปรุง**ประสิทธิผลของกระบวน**การบริหารจัดการความเสี่ยง** การควบคุมและการกำกับดูแล ซึ่งจะช่วยให้ส่วนราชการบรรลุถึงเป้าหมายและวัตถุประสงค์

5. แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่องหลักการบริหารจัดการความเสี่ยงระดับองค์กร

ตามแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ ภายใต้พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ.2561 ได้ผสานแนวคิดเป็นกรอบการบริหารจัดการความเสี่ยงขององค์กรประกอบด้วย COSO และ ISO เพื่อให้การบริหารความเสี่ยงเป็นเครื่องมือในการบริหารงานตามหลักธรรมาภิบาล (ภาพที่ 14)



คำนำ

แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร เป็นกรอบแนวทางการบริหารจัดการความเสี่ยงซึ่งได้ผสานกรอบแนวคิดด้านการบริหารจัดการความเสี่ยงขององค์กรชั้นนำต่างๆ ประกอบด้วย Committee of Sponsoring Organizations of the Treadway Commission (COSO) และ International Organization for Standardization (ISO) รวมถึงการบริหารจัดการความเสี่ยงในภาครัฐของประเทศต่างๆ มากำหนดเป็นแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยของรัฐตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ โดยหน่วยงานของรัฐสามารถนำหลักการบริหารจัดการความเสี่ยงระดับองค์กรดังกล่าวเป็นแนวทางในการพัฒนาระบบการบริหารจัดการความเสี่ยงขององค์กร เพื่อให้การบริหารจัดการความเสี่ยงเป็นเครื่องมือสำคัญในการบริหารงานให้เป็นไปตามหลักธรรมภิบาล ทั้งนี้ หัวหน้าหน่วยงานของรัฐมีหน้าที่รับผิดชอบโดยตรงในการจัดให้มีระบบการบริหารจัดการความเสี่ยงของหน่วยงานของรัฐที่มีประสิทธิภาพ เพื่อประโยชน์ของประชาชนและผู้มีส่วนได้เสียทุกฝ่าย

ภาพที่ 15 บทนำแนวทางการบริหารจัดการความเสี่ยง สำหรับหน่วยงานภาครัฐ

มาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ.2562

มาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ.2562 ซึ่งประกาศใช้ในปีงบประมาณ 2562 และเริ่มบังคับใช้ในปีงบประมาณ 2563

มาตรฐานการจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ หรืออาจเรียกตามเลขที่หนังสือเวียนที่ออกเรียกว่า “ว 23” ประกาศใช้ในปีงบประมาณ 2562 ซึ่งเป็นการประกาศใช้ภายหลังจากมาตรฐานการควบคุมภายในสำหรับหน่วยงานของรัฐ หรือเรียกว่า “ว 105” ที่มีการประกาศใช้ในปีงบประมาณ พ.ศ. 2561 และแนวทางบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ “ว 36” (ภาพที่ 15)

ภาพที่ 16 ลำดับการประกาศใช้มาตรฐานการควบคุมภายในสำหรับหน่วยงานของรัฐ และมาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

เนื้อหาสาระของมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ มี ดังนี้

การบริหารจัดการความเสี่ยง หมายความว่า กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน รวมถึงเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ได้กำหนดจำนวน 9 ข้อ ดังนี้

มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

2. มาตรฐาน

2.1 หน่วยงานของรัฐต้องจัดให้มีการบริหารจัดการความเสี่ยง เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลแก่ผู้มีส่วนได้ส่วนเสียของหน่วยงานว่าหน่วยงานได้ดำเนินการบริหารจัดการความเสี่ยงอย่างเหมาะสม

2.2 ฝ่ายบริหารของหน่วยงานของรัฐต้องจัดให้มีสภาพแวดล้อมที่เหมาะสมต่อการบริหารจัดการความเสี่ยงภายในองค์กร อย่างน้อยประกอบด้วย การมอบหมายผู้รับผิดชอบเรื่องการบริหารจัดการความเสี่ยง การกำหนดวัฒนธรรมของหน่วยงานของรัฐที่ส่งเสริมการบริหารจัดการความเสี่ยง รวมถึงการบริหารทรัพยากรบุคคล

2.3 หน่วยงานของรัฐต้องการกำหนดวัตถุประสงค์เพื่อใช้ในการบริหารจัดการความเสี่ยงที่เหมาะสม รวมถึงมีการสื่อสารการบริหารจัดการความเสี่ยงของวัตถุประสงค์ด้านต่างๆ ต่อบุคลากรที่เกี่ยวข้อง

2.4 การบริหารจัดการความเสี่ยงต้องดำเนินการในทุกระดับของหน่วยงานของรัฐ

2.5 การบริหารจัดการความเสี่ยง อย่างน้อยต้องประกอบด้วย การระบุความเสี่ยง การประเมินความเสี่ยง และการตอบสนองความเสี่ยง

2.6 หน่วยงานของรัฐต้องจัดทำแผนบริหารจัดการความเสี่ยงอย่างน้อยปีละครั้งและต้องมีการสื่อสารแผนบริหารจัดการความเสี่ยงกับผู้ที่เกี่ยวข้องทุกฝ่าย

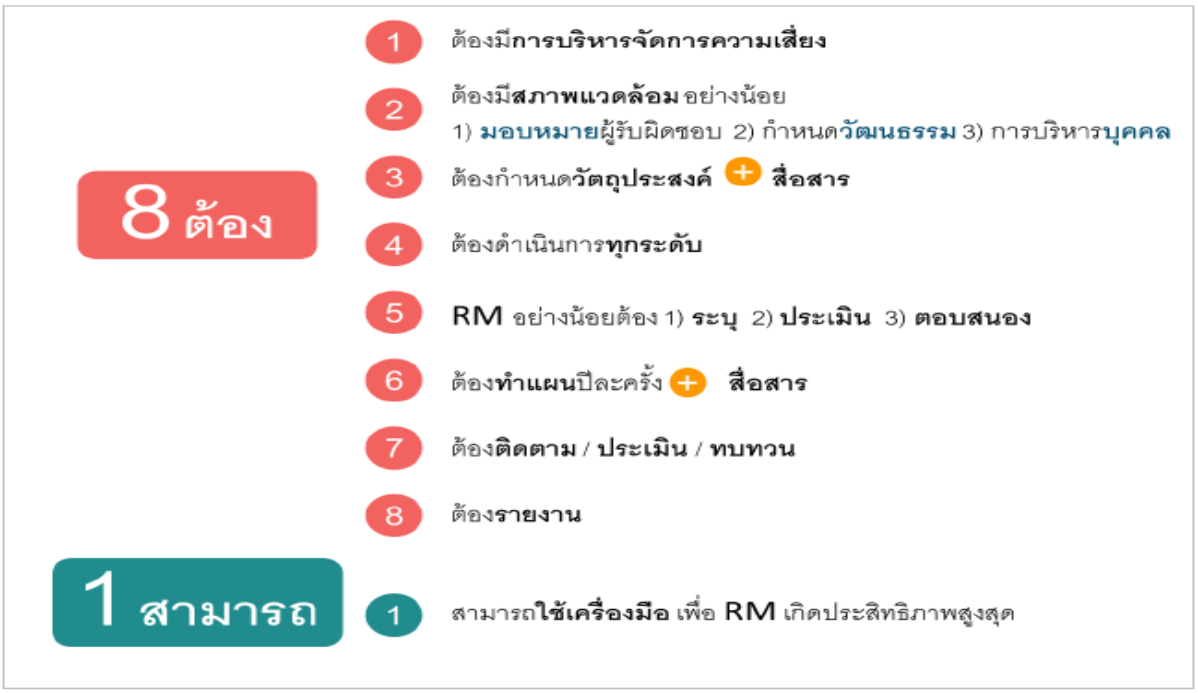
2.7 หน่วยงานของรัฐต้องมีการติดตามประเมินผลการบริหารจัดการความเสี่ยงและทบทวนแผนการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ

2.8 หน่วยงานของรัฐต้องมีการรายงานการบริหารจัดการความเสี่ยงของหน่วยงานต่อผู้ที่เกี่ยวข้อง

2.9 หน่วยงานของรัฐสามารถพิจารณานำเครื่องมือการบริหารความเสี่ยงที่เหมาะสมมาประยุกต์ใช้กับหน่วยงาน เพื่อให้การบริหารจัดการความเสี่ยงของหน่วยงานเกิดประสิทธิภาพสูงสุด

ที่มา : มาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ พ.ศ. 2562 (ว 23)

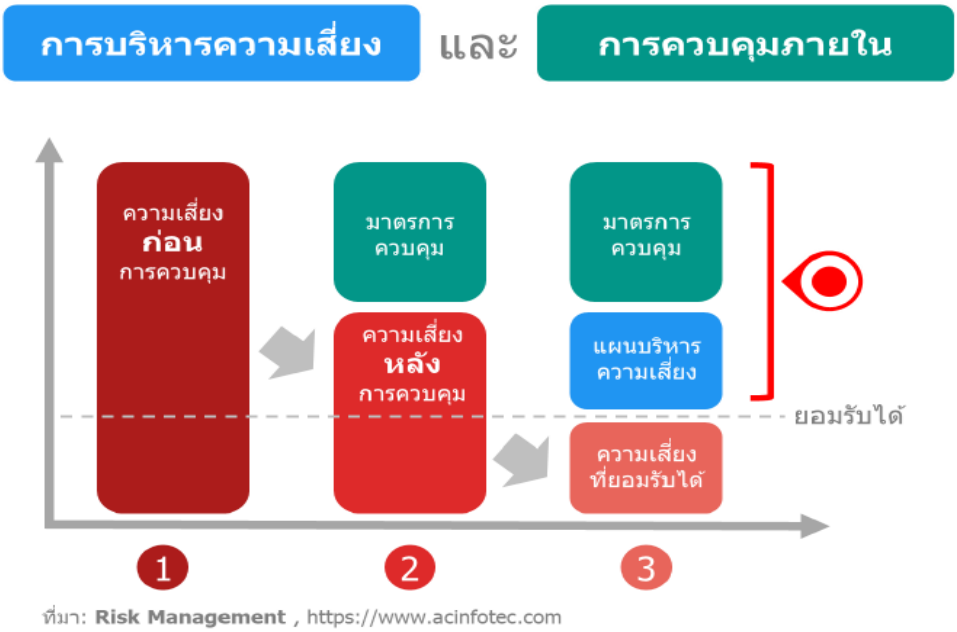
จากมาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ 9 ข้อข้างต้น สามารถสรุปสาระสำคัญได้ (ภาพที่ 16) ดังนี้



ภาพที่ 17 สรุปสาระสำคัญ 9 ข้อ มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

แนวคิดการบริหารความเสี่ยง

ในการพิจารณาว่าการควบคุมภายในที่ปฏิบัติอยู่นั้น มีประสิทธิภาพและประสิทธิผลเพียงพอหรือไม่หรือต้องออกแบบมาตรการในการจัดการความเสี่ยงเพิ่มเติมอีกมากเพียงใด หน่วยงานต้องพิจารณาร่วมกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) กล่าวคือ มาตรการในการควบคุมดังกล่าว เมื่อนำไปปฏิบัติแล้ว ควรจะลดความเสี่ยงลงมาให้อยู่ในระดับที่ยอมรับได้ (ภาพที่ 17)



ภาพที่ 18 แนวคิดการบริหารความเสี่ยง และการควบคุมภายใน

คำนิยามความเสี่ยงและการบริหารความเสี่ยง

ตามมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ พ.ศ.2562 (ว 23) ได้ให้คำนิยามของความเสี่ยงไว้ ดังนี้

“ความเสี่ยง” หมายความว่า ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ของหน่วยงาน

จากคำนิยามคำว่าความเสี่ยงข้างต้นสามารถสรุปได้ว่ามี 2 องค์ประกอบ ได้แก่

1. เป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ของหน่วยงาน และ 2. เป็นเหตุการณ์ที่อาจเกิดขึ้นในอนาคต ตามมาตรฐานฯ ดังกล่าวข้างต้น ได้ให้คำนิยามคำว่า การบริหารจัดการความเสี่ยงไว้ ดังนี้

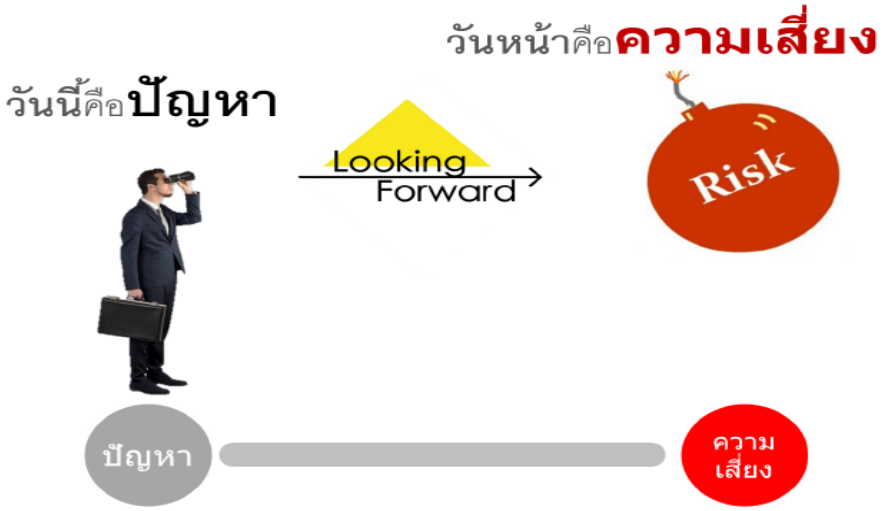
“การบริหารจัดการความเสี่ยง” หมายความว่า กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน รวมถึงเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

จากคำนิยามคำว่าการบริหารจัดการความเสี่ยง จึงสรุปได้ว่า เป็นกระบวนการจัดการความเสี่ยงที่อาจเกิดขึ้น เพื่อให้หน่วยงานของรัฐสามารถบรรลุวัตถุประสงค์ได้ รวมถึงเพิ่มศักยภาพและขีดความสามารถ

ภาพที่ 19 การสื่อสารด้วยภาพของคำว่าความเสี่ยง และการบริหารจัดการความเสี่ยง

มุมมอง Looking Forward

มุมมองในการมองความเสี่ยงควรใช้ **มุมมองไปข้างหน้า (**Looking Forward**)** คือการมองอุปสรรคที่จะเกิดขึ้นในวันหน้า (ภาพที่ 19)



ภาพที่ 20 มุมมองในการมองความเสี่ยง (Looking Forward)

ตัวอย่างข้อแตกต่างระหว่างปัญหาและความเสี่ยง ด้วยมุมมอง Looking Forward (ตารางที่ 1)

ตารางที่ 1 แสดงตัวอย่างความแตกต่างระหว่างปัญหาและความเสี่ยง

ปัญหา	ความเสี่ยง
1. ตำแหน่งทางวิชาการของอาจารย์ประจำ ยังไม่เป็นไปตามเกณฑ์มาตรฐานการ ประกันคุณภาพการศึกษา	หลักสูตรไม่ได้การรับรอง
2. จำนวนนักศึกษาลดลง	ปิดหลักสูตร
3. เขียนโครงร่างวิจัยไม่ถูกต้อง	งานวิจัยไม่มีคุณภาพ / ไม่ได้รับการตีพิมพ์

ประเภทความเสี่ยง

จากคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน, กระทรวงการคลัง (2555 : 45-46) ได้ระบุว่า กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ และเกณฑ์ประเมินผลการดำเนินงานรัฐวิสาหกิจ ด้านการบริหารจัดการองค์กร กระทรวงการคลัง ได้แบ่งประเภทของความเสี่ยงเป็น 4 ประเภท ดังนี้

1. ความเสี่ยงด้านกลยุทธ์
2. ความเสี่ยงด้านการปฏิบัติงาน
3. ความเสี่ยงด้านการเงิน
4. ความเสี่ยงด้านกฎระเบียบ/ข้อบังคับ

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : SR) คือ ความเสี่ยงที่อาจก่อให้เกิดการสูญเสียทางการเงินหรือศักยภาพในการแข่งขัน อันเนื่องมาจากกระบวนการตัดสินใจเชิงกลยุทธ์ที่ไม่เหมาะสม ตัวอย่างความเสี่ยงด้านกลยุทธ์ เช่น

- การเปลี่ยนแปลงทางการเมือง
- ไม่สามารถเพิ่มรายได้และลดค่าใช้จ่ายได้ตามเป้าหมายที่กำหนด
- การเปลี่ยนแปลงความต้องการของลูกค้า

2. ความเสี่ยงด้านการปฏิบัติการ (Operational Risk : OR) คือ ความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานขององค์กร อันเนื่องมาจากความผิดพลาดที่เกิดจากการปฏิบัติงานของบุคลากร ระบบหรือกระบวนการต่างๆ ตัวอย่างความเสี่ยงด้านการปฏิบัติการ เช่น

- ขาดบุคลากรที่มีคุณภาพ
- การก่อการร้าย อุทกภัย วินาศภัย ฯลฯ
- การใช้งานระบบเทคโนโลยีสารสนเทศไม่เต็มประสิทธิภาพ

3. ความเสี่ยงด้านการเงิน (Financial Risk : FR) คือ ความเสี่ยงที่เกิดจากความผันผวนของตัวแปรทางการเงิน เช่น อัตราแลกเปลี่ยน อัตราดอกเบี้ย สภาพคล่องทางการเงิน และราคาสินค้าโภคภัณฑ์ (Commodity) เป็นต้น ซึ่งก่อให้เกิดการสูญเสียทางการเงิน ตัวอย่างความเสี่ยงด้านการเงิน เช่น

- ความเสี่ยงด้านเครดิต
- ความเสี่ยงด้านสภาพคล่อง
- การขาดทุนจากอัตราแลกเปลี่ยน
- ความผันผวนของราคาวัตถุดิบ

4. ความเสี่ยงด้านกฎระเบียบ/ข้อบังคับ (Compliance Risk : CR) หรืออาจใช้คาว่า Regulatory Risk คือ ความเสี่ยงที่เกิดจากการละเมิดหรือไม่ปฏิบัติตามนโยบาย กระบวนการ หรือการควบคุมต่างๆ ที่กำหนดขึ้นเพื่อให้สอดคล้องกับกฎระเบียบ ข้อบังคับ ข้อสัญญา และข้อกฎหมายที่เกี่ยวข้องกับการดำเนินงานขององค์กร ตัวอย่างความเสี่ยงด้านกฎระเบียบ/ข้อบังคับ เช่น

- การทุจริต
- การถูกฟ้องร้อง ร้องเรียนจากผู้มีส่วนได้ส่วนเสีย
- การไม่ปฏิบัติตามกฎ ระเบียบ ที่เกี่ยวข้องกับรัฐวิสาหกิจแต่ละแห่ง

แนวคิดการบริหารความเสี่ยงองค์กร

ในปี พ.ศ.2535 คณะกรรมการชุดหนึ่ง เรียกว่า COSO ย่อมากจาก The Committee of Sponsoring Organizations of the Treadway Commission ซึ่งเป็นคณะกรรมการของสถาบันวิชาชีพ 5 สถาบัน ในสหรัฐอเมริกา อันได้แก่

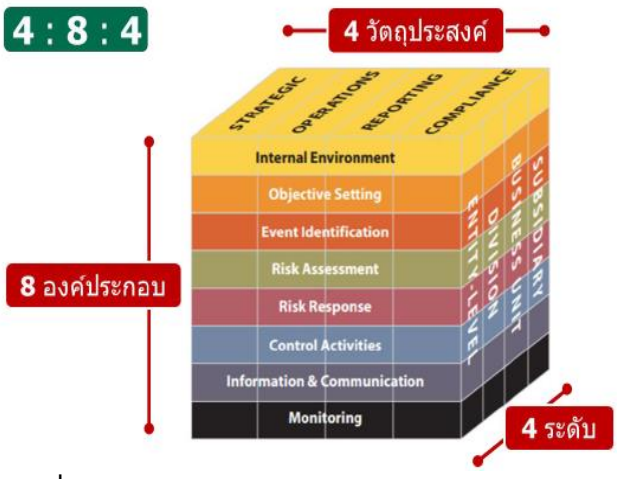
1. สมาคมผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา (The American Institute of Certified Public Accountants หรือ AICPA)
2. สมาคมผู้ตรวจสอบภายใน (The Institute of Internal Auditor หรือ IIA)
3. สมาคมผู้บริหารการเงิน (The Financial Executives Institute หรือ FEI)
4. สมาคมนักบัญชีแห่งสหรัฐอเมริกา (The American Accounting Association หรือ AAA)
5. สมาคมนักบัญชีเพื่อการบริหาร (Institute of Management Accountants หรือ IMA)

COSO ได้ร่วมกันศึกษาวิจัย และพัฒนาแนวคิดของการควบคุมภายใน

ในปี ค.ศ.2004 COSO ได้มีการนำเสนอแนวคิดเรื่อง กรอบการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management-Integrated Framework : ERM) หรือเรียกว่า **COSO : ERM**

COSO : ERM ได้ขยายขอบเขตการควบคุมภายในให้กว้างขวางมากขึ้นกว่าเดิม หลังจากในปี ค.ศ.1992 COSO เคยเสนอกรอบการควบคุมภายใน (Internal Control – An Integrated Framework) หรือเรียกย่อว่า COSO : IC

COSO : ERM Model มีองค์ประกอบคือ **4 : 8 : 4** คือ **4 วัตถุประสงค์ 8 องค์ประกอบ 4 ระดับ**ดัง**ภาพที่ 20** ด้านล่างนี้ ซึ่งรายละเอียดจะกล่าวไปลำดับถัดไป



ภาพที่ 21 COSO ERM Model

ที่มา : https://www.coso.org/

วัตถุประสงค์ของการบริหารความเสี่ยง

COSO ERM Model (ภาพที่ 21) ได้กำหนดการบริหารความเสี่ยงมีวัตถุประสงค์ที่สำคัญ 4 ด้าน หรือเรียกว่า **4 วัตถุประสงค์** ได้แก่ 1. วัตถุประสงค์เชิงกลยุทธ์ 2. วัตถุประสงค์การดำเนินงาน 3. วัตถุประสงค์การรายงาน และ 4. วัตถุประสงค์การปฏิบัติตามกฎระเบียบ (จันทนา สาขากร และคณะ, 2557)

ภาพที่ 22 COSO ERM Model - 4 Objectives

ที่มา : https://www.coso.org/

1. วัตถุประสงค์เชิงกลยุทธ์ (Strategic : S) เป็นวัตถุประสงค์ระดับสูง และสัมพันธ์กับการสนับสนุนพันธกิจขององค์กร

2. วัตถุประสงค์การดำเนินงาน (Operation : O) เป็นวัตถุประสงค์ของการใช้ทรัพยากรขององค์กรอย่างมีประสิทธิภาพ ประสิทธิผลและคุ้มค้า

3. วัตถุประสงค์การรายงาน (Reporting : R) เป็นวัตถุประสงค์เพื่อความเชื่อถือได้ของรายงาน

4. วัตถุประสงค์การปฏิบัติตามกฎระเบียบ (Compliance : C) เป็นวัตถุประสงค์ที่มุ่งให้องค์กรปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับองค์กรเมื่อเปรียบเทียบวัตถุประสงค์ของการควบคุมภายในและการบริหารความเสี่ยง (COSO : IC และ COSO : ERM) จะเห็นได้ว่ามีข้อแตกต่างกัน 2 ประการ คือ

1. COSO : ERM มีวัตถุประสงค์เพิ่มจาก COSO : IC คือ วัตถุประสงค์เชิงกลยุทธ์

2. COSO : IC มีวัตถุประสงค์การรายงานทางการเงิน (Financial) ต่อมา COSO : ERM มีวัตถุประสงค์การรายงาน (Reporting : R) โดยได้ขยายกว้างกว่า ไม่เน้นแต่เฉพาะการรายงานทางการเงินเท่านั้น แต่ให้ครอบคลุมถึงความเชื่อถือได้ของรายงานทุกประเภท

องค์ประกอบของการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงขององค์การที่ได้รับการยอมรับว่าเป็นแนวทางในการส่งเสริมการบริหารความเสี่ยงและเป็นหลักปฏิบัติที่เป็นสากลคือ กรอบการบริหารความเสี่ยงสำหรับองค์กรของคณะกรรมการ COSO (The

Committee of Sponsoring Organization of the Treadway Commission) หรือCOSO-ERMประกอบด้วย 8 องค์ประกอบ (ภาพที่ 22) ดังนี้

1. สภาพแวดล้อมภายในองค์กร (Internal Environment)
2. การกำหนดวัตถุประสงค์ (Objective Setting)
3. การบ่งชี้เหตุการณ์ (Event Identification)
4. การประเมินความเสี่ยง (Risk Assessment)
5. การตอบสนองความเสี่ยง (Risk Response)
6. กิจกรรมการควบคุม (Control Activities)
7. สารสนเทศและการสื่อสาร (Information and Communication)
8. การติดตามประเมินผล (Monitoring)

ภาพที่ 23 COSO ERM Model - 8 Components

ที่มา : https://www.coso.org/

1) สภาพแวดล้อมภายในองค์กร

สภาพแวดล้อมภายใน (Internal Environment) สภาพแวดล้อมขององค์การเป็นองค์ประกอบที่สำคัญในการกาหนดกรอบการบริหารความเสี่ยง และเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์การ การวิเคราะห์สภาพแวดล้อมภายในองค์การจะสะท้อนการดำเนินงานชัดเจนขึ้น เมื่อพิจารณาให้ครอบคลุมถึงปัจจัยภายในและปัจจัยภายนอกที่อาจมีผลกระทบต่อองค์การ

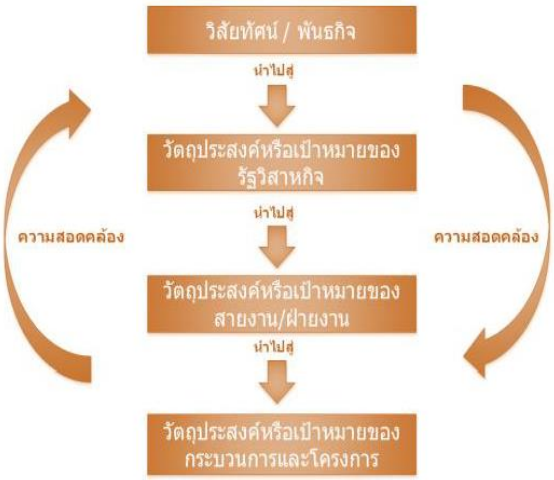
☐ ปัจจัยภายใน เช่น โครงสร้างองค์การ กระบวนการและวิธีการปฏิบัติงาน วัฒนธรรมองค์การปรัชญาการบริหารความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้ของผู้บริหาร

☐ ปัจจัยภายนอก เช่น ภาวะเศรษฐกิจ การเมืองทั้งในประเทศและต่างประเทศ ความก้าวหน้าทางเทคโนโลยี กฎเกณฑ์การกำกับดู แลของหน่วยงานที่เกี่ยวข้อง

2) การกำหนดวัตถุประสงค์

การกำหนดวัตถุประสงค์ (Objective Setting) องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ให้มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์การยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์การได้อย่างชัดเจนและเหมาะสม โดยการกำหนดวัตถุประสงค์ควรครอบคลุมวัตถุประสงค์

ด้านกลยุทธ์ (Strategic Objectives) วัตถุประสงค์ด้านการปฏิบัติงาน (Operations Objectives) วัตถุประสงค์ด้านการรายงาน (Reporting Objectives) วัตถุประสงค์ด้านการปฏิบัติตามกฎระเบียบ (Compliance Objectives) (ภาพที่ 23)



ภาพที่ 24 ความเชื่อมโยงวิสัยทัศน์/พันธกิจกับวัตถุประสงค์ด้านต่างๆ

ที่มา : คู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน, กระทรวงการคลัง (2555 : 33)

3) การบ่งชี้เหตุการณ์

การบ่งชี้เหตุการณ์ (Event Identification) เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงานทั้งปัจจัยเสี่ยงที่เกิดจากปัจจัยภายในและปัจจัยภายนอกองค์การและเมื่อเกิดขึ้นแล้วส่งผลให้องค์การไม่บรรลุวัตถุประสงค์หรือเป้าหมาย โดยความเสี่ยงแบ่งออกเป็น 4 ด้าน ได้แก่ ความเสี่ยงด้านกลยุทธ์(Strategic Risk) ความเสี่ยงด้านการปฏิบัติงาน (Operation Risk) ความเสี่ยงด้านการเงิน (Financial Risk) และความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk)

4) การประเมินความเสี่ยง

การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงเป็นการวัดระดับความรุนแรงของความเสี่ยง เพื่อพิจารณาจัดลาดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) ซึ่งขึ้นอยู่กับระยะเวลาที่นามาพิจารณา ผู้บริหารต้องมีความชัดเจนในการกำหนดระยะเวลาที่ใช้ในการพิจารณา ไม่ควรละเลยความเสี่ยงที่อาจเกิดขึ้นในระยะยาวและผลกระทบ (Impact) เป็นการพิจารณาถึงผลกระทบทั้งทางด้านการเงิน เช่น การลดลงของรายได้และด้านที่ไม่ใช่การเงิน เช่น ด้านกลยุทธ์ การดำเนินงานที่ไม่บรรลุวัตถุประสงค์ขององค์การ หรือด้านทรัพยากรบุคคล การลาออกพนักงาน การสูญเสียพนักงานในตำแหน่งที่สำคัญ เป็นต้น

5) การตอบสนองความเสี่ยง

การตอบสนองต่อความเสี่ยง (Risk Response) เป็นการดำเนินการหลังจากที่องค์การสามารถระบุความเสี่ยงขององค์การและประเมินระดับของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการเพื่อลดโอกาสที่จะเกิดความเสี่ยงและลดระดับความรุนแรงของผลกระทบให้อยู่ในระดับที่องค์การยอมรับได้ ด้วยวิธีจัดการควบคุมความเสี่ยงที่เหมาะสมที่สุดและคุ้มค่ากับการลงทุนการตอบสนองต่อความเสี่ยงแบ่งเป็น 4 ประการ ได้แก่

การยอมรับ (Accept)

การลด (Reduce)

การหลีกเลี่ยง/การยกเลิก (Avoid/Terminate)

การโอนความเสี่ยง (Transfer)

ผู้บริหารอาจทำการพิจารณาปัจจัยในการกำหนดกลยุทธ์การจัดการความเสี่ยงโดยการประเมินผลกระทบและโอกาสเกิดจากการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง หรือการประเมินต้นทุนและผลตอบแทนของการดำเนินการตามกลยุทธ์การจัดการความเสี่ยง หรือการประเมินความเป็นไปได้ที่จะประสบความสำเร็จในการจัดการความเสี่ยง

6) กิจกรรมการควบคุม

กิจกรรมควบคุม (Control Activities) การกำหนดกิจกรรมและการปฏิบัติต่างๆ เพื่อช่วยลดหรือควบคุมความเสี่ยง เพื่อสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้อง และทำให้การดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายขององค์การ อีกทั้งป้องกันและลดระดับความเสี่ยงให้อยู่ในระดับที่องค์การยอมรับได้

การควบคุมแบ่งออกเป็น 4 แบบ ได้แก่

การควบคุมแบบป้องกัน (Preventive Control)

การควบคุมแบบค้นหา (Detective Control)

การควบคุมแบบแก้ไข (Corrective Control)

การควบคุมแบบส่งเสริม(Directive Control)

7) สารสนเทศและการสื่อสาร

สารสนเทศและการสื่อสาร (Information & Communication) องค์การจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนาไปพิจารณาดำเนินการบริหารความเสี่ยงต่อไปตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

- สารสนเทศ หมายถึง ข้อมูลที่ได้ผ่านการประมวลผลและถูกจัดให้อยู่ในรูปแบบที่เหมาะสมมีความหมายและเป็นประโยชน์ต่อการใช้งาน ซึ่งข้อมูลสารสนเทศหมายรวมถึงข้อมูลทางการเงินและการดำเนินงานในด้านอื่นๆ โดยเป็นข้อมูลทั้งจากแหล่งภายในและภายนอกองค์การ
- การสื่อสาร เป็นการสื่อสารข้อมูลที่จัดทำไว้แล้ว ส่งไปถึงผู้ที่ควรจะได้รับ หรือมีไว้พร้อมสำหรับผู้ที่ควรใช้สารสนเทศนั้น เพื่อให้ผู้ที่ได้รับใช้ข้อมูลดังกล่าวให้เกิดประโยชน์ในการตัดสินใจด้านต่างๆ และเพื่อสนับสนุนให้เกิดความเข้าใจ ตลอดจนมีการดำเนินงานตามวัตถุประสงค์ โดยระบบการสื่อสารต้องประกอบด้วยการสื่อสาร

ภายในองค์การและระบบการสื่อสารภายนอกองค์การ ทั้งนี้องค์กรจะต้องมีการสื่อสารเพื่อให้คณะกรรมการ ผู้บริหารและพนักงาน มีความตระหนักและเข้าใจในนโยบาย แนวปฏิบัติและกระบวนการบริหารความเสี่ยง นอกจากนี้ควรมีการประเมินประสิทธิภาพ และประสิทธิผลของการสื่อสารเป็นระยะๆ เพื่อให้การสื่อสารเป็นส่วนหนึ่งของการควบคุมภายใน ที่เป็นประโยชน์สูงสุดต่อองค์การ

8) การติดตามประเมินผล

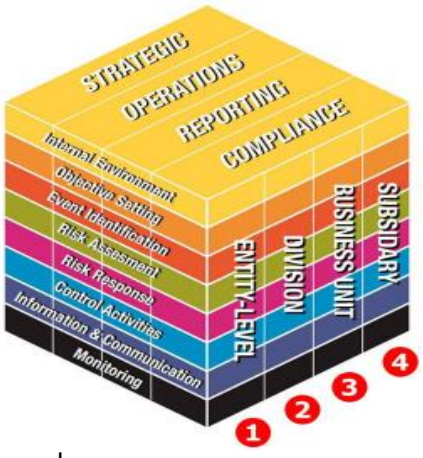
การติดตามประเมินผล (Monitoring) เป็นกิจกรรมที่ใช้ติดตามและสอบทานแผนบริหารความเสี่ยง เพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีประสิทธิภาพและเหมาะสม หรือควรปรับเปลี่ยน โดยกำหนดข้อมูลที่ต้องติดตามและความถี่ในการสอบทาน และควรกำหนดให้มีการประเมินความเสี่ยงซ้ำอย่างน้อยปีละ 1 ครั้ง เพื่อประเมินว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้ว หรือมีความเสี่ยงใหม่เพิ่มขึ้น

ทั้งนี้ ความเสี่ยงและการจัดการต่อความเสี่ยงอาจมีการเปลี่ยนแปลงตลอดเวลา การจัดการต่อความเสี่ยงที่เคยมีประสิทธิผล อาจเปลี่ยนเป็นกิจกรรมที่ไม่เหมาะสม กิจกรรมการควบคุมอาจมีประสิทธิผลน้อยลง หรือไม่ควรดำเนินการต่อไป หรืออาจมีการเปลี่ยนแปลงในวัตถุประสงค์หรือกระบวนการต่างๆ ดังนั้น ผู้บริหารควรประเมินกระบวนการบริหารความเสี่ยงเป็นประจำเพื่อให้มั่นใจว่าการบริหารความเสี่ยงมีประสิทธิผลเสมอ

ระดับหน่วยงานในองค์กร

ระดับหน่วยงานในองค์กร (Entity's Units) แบ่งออกได้ 4 ระดับ (ภาพที่ 24)

1. ระดับทั่วทั้งองค์กร (Entity – Level : EL)
2. ระดับส่วนงาน (Division : D)
3. ระดับหน่วยงาน (Business Unit : BU)
4. ระดับหน่วยงานย่อย (Subsidiary : S)



ภาพที่ 25 COSO ERM Model - 4 Entity Unit

ที่มา : https://www.coso.org/

ตามมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ พ.ศ.2562 (ว 23) ได้กำหนดใน ข้อ 2.4 การบริหารจัดการความเสี่ยงต้องดำเนินการในทุกระดับของหน่วยงานของรัฐ

กรอบการบริหารความเสี่ยง COSO-ERM 2017

กรอบการบริหารความเสี่ยงองค์กร (Enterprise Risk Management, ERM) จึงได้ถูกนำเสนอโดย COSO ในปี ค.ศ.2004 หลังจากเหตุนั้น ในชื่อของ COSO-ERM Integrated Framework-2004 ซึ่งองค์กรต่างๆ ทั่วโลกนำมาปรับใช้เป็นแนวทางในการบริหารความเสี่ยงองค์กร รวมถึงหน่วยงานรัฐที่มีหน้าที่กำกับดูแลกิจการประเภทต่างๆ ในประเทศด้วย

กรอบการบริหารความเสี่ยง COSO-ERM นี้ได้ถูกใช้มามากกว่า 10 ปี (ตั้งแต่ปี 2004) ท่ามกลางการใช้อย่างแพร่หลายมากขึ้นเรื่อยๆ และสภาพแวดล้อมทั้งในระดับมหาภาค และระดับองค์กรที่เปลี่ยนแปลงไป โดย COSO ได้ดำเนินการทบทวนปรับปรุงใหม่จนแล้วเสร็จ เผยแพร่ในเดือนมิถุนายน ปี 2017 ที่ผ่านมา และใช้ชื่อกรอบการบริหารความเสี่ยงใหม่นี้ว่า Enterprise Risk Management-Integrating with Strategy and Performance หรือเรียกว่า COSO – ERM 2017 (Enterprise Risk Management-Integrating with Strategy and Performance)

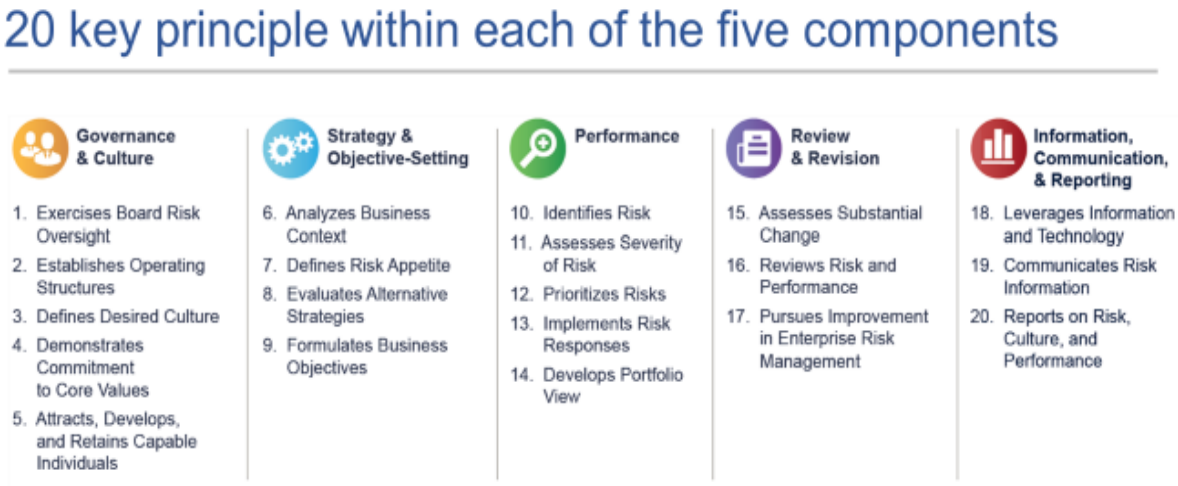
การจัดกลุ่มองค์ประกอบของกระบวนการบริหารความเสี่ยงองค์กรเป็น 5 องค์ประกอบ (ภาพที่ 25) คือ

1. การกำกับดูแลกิจการและวัฒนธรรมองค์กร (Governance and Culture)
2. กลยุทธ์และวัตถุประสงค์องค์กร (Strategy & Objective Setting)
3. เป้าหมายผลการดำเนินงาน (Performance)
4. การทบทวนและปรับปรุง (Review & Revision) และ
5. สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication & Reporting)

ภาพที่ 26 กรอบการบริหารความเสี่ยงองค์กร COSO ERM 2017

ที่มา : The Committee of Sponsoring Organization of the Tread way Commission (COSO, 2017)

การจัดกลุ่มองค์ประกอบของกระบวนการบริหารความเสี่ยงองค์กร ให้มีน้อยลงจากเดิม 8 องค์ประกอบ เหลือเพียง 5 องค์ประกอบ แต่เพิ่มประเด็นหลักการในแต่ละองค์ประกอบให้ชัดเจนมากขึ้นรวม 20 หลักการ



ภาพที่ 27 องค์ประกอบ COSO ERM 2017

ที่มา : The Committee of Sponsoring Organization of the Tread way Commission (COSO, 2017)

องค์ประกอบสำคัญของการบริหารความเสี่ยงตามแนวคิดของ COSO ERM 2017 แบ่งออกเป็น 5 องค์ประกอบ โดยองค์ประกอบเหล่านี้ต้องมีความเกี่ยวเนื่องและมีความสัมพันธ์ต่อกัน เพื่อให้เกิดการบรรลุวัตถุประสงค์ของการบริหารความเสี่ยง ดังนี้ (ภณิดา วรทวีธำรง, 2561: 12-16)

องค์ประกอบที่ 1 การกำกับดูแลกิจการและวัฒนธรรมองค์กร (Governance and Culture)

การกำกับดูแลกิจการและวัฒนธรรมองค์กรเป็นพื้นฐานในการบริหารความเสี่ยงเนื่องจากการกำกับดูแลกิจการเป็นสิ่งที่ใช้ในการกำหนดแนวทางขององค์กรเกี่ยวกับการให้ความสำคัญและความรับผิดชอบในการบริหารความเสี่ยงวัฒนธรรมองค์กรจะเกี่ยวข้องกับค่านิยม ทางจริยธรรมพฤติกรรมที่พึงประสงค์ และความเข้าใจเกี่ยวกับความเสี่ยงขององค์กร ซึ่งจะสะท้อนผ่านการตัดสินใจต่างๆ ซึ่งประกอบด้วยกรอบแนวทางปฏิบัติ 5 หลักการ ดังนี้

หลักการที่ 1 จัดตั้งคณะกรรมการดูแลความเสี่ยง (Exercises Board Risk Oversight)

คณะกรรมการบริษัทมีหน้าที่กำกับดูแลการดำเนินงานตามกลยุทธ์ รวมถึงกำกับดูแลกิจการ เช่น คณะกรรมการควรมีหน้าที่ความรับผิดชอบด้านการบริหารความเสี่ยง คณะกรรมการควรมีความอิสระหลีกเลี่ยงความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้น

หลักการที่ 2 จัดตั้งโครงสร้างการดำเนินงาน (Establishes Operating Structures)

องค์กรควรจัดตั้งโครงสร้างการดำเนินงานที่สอดคล้องกับกลยุทธ์และวัตถุประสงค์ทางธุรกิจ

หลักการที่ 3 ระบุวัฒนธรรมองค์กรที่ต้องการ (Defines Desired Culture)

องค์กรควรระบุพฤติกรรมที่พึงประสงค์ ซึ่งแสดงถึงวัฒนธรรมองค์กรที่ต้องการคณะกรรมการบริหารและฝ่ายบริหารเป็นผู้กำหนดวัฒนธรรมองค์กรในภาพรวมและสำหรับบุคลากรภายใต้วัฒนธรรมองค์กรที่ให้ความสำคัญกับความเสี่ยง วัฒนธรรมองค์กรเกิดขึ้นจากหลายปัจจัย ปัจจัยภายในที่สำคัญ ได้แก่ ระดับการใช้วิจารณญาณ ความเป็นอิสระในการตัดสินใจของพนักงาน การสื่อสารระหว่างพนักงาน และผู้จัดการ

ปัจจัยภายนอก ได้แก่ ข้อกำหนดด้านกฎหมาย ความคาดหวังของลูกค้าและองค์ประกอบอื่นๆ

หลักการที่ 4 แสดงความมุ่งมั่นในค่านิยมหลัก (Demonstrates Commitment to Core Values)

องค์กรควรแสดงให้เห็นถึงความมุ่งมั่นที่จะปฏิบัติตามค่านิยมหลักขององค์กร เช่น ยึดถือการบริหารความเสี่ยงเป็นส่วนหนึ่งของวัฒนธรรมองค์กร การปฏิบัติตามหน้าที่และความรับผิดชอบอย่างเคร่งครัด การกำหนดให้มีการสื่อสารที่เหมาะสม

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

องค์กรควรมุ่งมั่นในการสนับสนุนการสร้างทรัพยากรบุคคลควบคู่ไปกับกลยุทธ์และวัตถุประสงค์ทางธุรกิจ เช่น ฝึกอบรมบุคลากรในด้านการบริหารความสี่ยงการส่งเสริมความรู้ความสามารถของพนักงาน การสร้างแรงจูงใจและผลตอบแทนอื่นๆ อย่างเหมาะสมสำหรับตำแหน่งงานในทุกระดับ

องค์ประกอบที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective-Setting)

การบริหารความเสี่ยงสามารถบูรณาการเข้ากับแผนยุทธศาสตร์ขององค์กรได้ ผ่านกระบวนการกำหนดกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยองค์กรควรกำหนดความเสี่ยงที่ยอมรับได้ให้สอดคล้องกับการกำหนดกลยุทธ์ นอกจากนั้นวัตถุประสงค์ทางธุรกิจจะเป็นสิ่งที่กำหนดแนวทางปฏิบัติตามกลยุทธ์รวมถึงการดำเนินงานทั่วไปและปัจจัยที่องค์กรให้ความสำคัญโดยจะเป็นพื้นฐานในการระบุประเมิน และการตอบสนองต่อความเสี่ยง ซึ่งประกอบด้วยกรอบแนวทางปฏิบัติ 4 หลักการดังนี้

หลักการที่ 6 วิเคราะห์ธุรกิจ (Analyzes Business Context)

องค์กรควรพิจารณาถึงผลกระทบจากบริบททางธุรกิจที่อาจเกิดขึ้นและส่งผลต่อระดับความเสี่ยงในภาพรวมขององค์กร เช่น การเข้าใจบริบททางธุรกิจ การคำนึงถึงสภาพแวดล้อมภายนอกและผู้มีส่วนได้ส่วนเสีย

หลักการที่ 7 ระบุความเสี่ยงที่ยอมรับได้ (Defines Risk Appetite)

องค์กรควรระบุความเสี่ยงที่ยอมรับได้ เพื่อสร้างดำรงไว้ และส่งเสริมความตระหนักถึงค่านิยมความเสี่ยงที่ยอมรับได้ไม่มีการกำหนดรูปแบบตายตัว หรือเป็นมาตรฐานที่จะใช้ได้กับทุกองค์กรผู้บริหารเป็นผู้เลือกความเสี่ยงที่ยอมรับได้ภายใต้บริบททางธุรกิจที่ต่างกันในแต่ละองค์กร

หลักการที่ 8 ประเมินกลยุทธ์ทางเลือก (Evaluates Alternative Strategies)

องค์กรควรประเมินเพื่อค้นหากลยุทธ์ทางเลือกและผลกระทบที่อาจเกิดขึ้นต่อโปรไฟล์ความเสี่ยงขององค์กร เช่น การวิเคราะห์ SWOT และการวิเคราะห์สถานการณ์กลยุทธ์ต้องสนับสนุนพันธกิจและวิสัยทัศน์ รวมถึงสอดคล้องกับค่านิยมหลักและความเสี่ยงที่ยอมรับได้

หลักการที่ 9 กำหนดวัตถุประสงค์ทางธุรกิจ (Formulates Business Objectives)

ในการกำหนดวัตถุประสงค์ทางธุรกิจ องค์กรควรพิจารณาถึงความเสี่ยงในระดับต่างๆ ตลอดจนความสอดคล้องและการสนับสนุนกลยุทธ์ควบคู่ไปด้วย เช่น การกำหนดค่าความเบี่ยงเบนของความเสี่ยงจากผลการดำเนินงานซึ่งยังคงอยู่ในช่วงความเสี่ยงที่ยอมรับได้

องค์ประกอบที่ 3 ผลการดำเนินงาน (Performance)

เริ่มจากการระบุและประเมินความเสี่ยงที่อาจส่งผลต่อความสามารถในการบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจโดยจัดลาดับความสำคัญของความเสี่ยงตามโอกาสในการเกิดและผลกระทบที่อาจเกิดขึ้น และพิจารณาความเสี่ยงที่องค์กรยอมรับได้ จากนั้นองค์กรจะเลือกตอบสนองต่อความเสี่ยงด้วยวิธีต่างๆ รวมถึงพิจารณาปริมาณความเสี่ยงในภาพรวมเกี่ยวกับปริมาณความเสี่ยงที่องค์กรอาจเผชิญในการบรรลุเป้าหมายกลยุทธ์และวัตถุประสงค์ทางธุรกิจในระดับองค์กรซึ่ง ประกอบด้วยกรอบแนวทางปฏิบัติ 5 หลักการ ดังนี้

หลักการที่ 10 ระบุความเสี่ยง (Identifies Risk)

องค์กรควรระบุความเสี่ยงที่ส่งผลต่อกลยุทธ์และวัตถุประสงค์ทางธุรกิจ เช่น ความเสี่ยงด้านลูกค้า ความเสี่ยงด้านการเงิน ความเสี่ยงด้านการปฏิบัติงาน และความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ ความเสี่ยงทั้งหมดจะถูกเก็บไว้ในโปรไฟล์ความเสี่ยงเพื่อนาไปจัดการความเสี่ยงเหล่านี้ต่อไป

หลักการที่ 11 ประเมินความรุนแรงของความเสี่ยง (Assess Severity of Risk)

องค์กรควรประเมินความรุนแรงของความเสี่ยง โดยประเมินว่าแต่ละปัจจัยเสี่ยงนั้น มีโอกาสที่จะเกิดมากน้อยเพียงใด และหากเกิดขึ้นแล้วจะส่งผลกระทบต่อองค์กรรุนแรงมากน้อยแค่ไหน

หลักการที่ 12 จัดลำดับความสำคัญของความเสี่ยง (Prioritizes Risks)

องค์กรควรคำนวณระดับความเสี่ยง (Risk Exposure) และการจัดลำดับความสำคัญของความเสี่ยง เพื่อเป็นพื้นฐานในการพิจารณาคัดเลือกวิธีตอบสนองต่อความเสี่ยงนั้น การคำนวณระดับความเสี่ยงเท่ากับผลคูณของคะแนนระหว่างโอกาสที่จะเกิดขึ้นกับความเสียหาย เพื่อจัดลำดับความสำคัญและใช้ในการตัดสินใจว่าความเสี่ยงใดควรเร่งจัดการก่อน

หลักการที่ 13 ดำเนินการตอบสนองต่อความเสี่ยง (Implements Risk Responses)

องค์กรควรระบุและคัดเลือกวิธีการตอบสนองต่อความเสี่ยง เช่น การยอมรับความเสี่ยง การลด การโอน หรือการหลีกเลี่ยง โดยศึกษาผลดีผลเสียความเป็นไปได้และค่าใช้จ่ายของแต่ละทางเลือก

หลักการที่ 14 พัฒนากรอบความเสี่ยงในภาพรวม (Develops Portfolio View)

องค์กรควรพัฒนาและประเมินความเสี่ยงในภาพรวมของทั้งองค์กร เครื่องมือที่นิยมใช้แสดงความเสี่ยงมีชื่อเรียกหลายชื่อ ได้แก่ Risk Map หรือ Risk Matrix

องค์ประกอบที่ 4 การทบทวนและปรับปรุงแก้ไข (Review and Revision)

องค์กรควรพิจารณากระบวนการบริหารความเสี่ยงอยู่เป็นระยะ โดยทบทวนความสามารถและแนวทางการบริหารความเสี่ยง ผู้บริหารควรพิจารณาความสามารถและการบริหารความเสี่ยงทั่วทั้งองค์กรว่าเพิ่มคุณค่าให้กับองค์กรมากน้อยเพียงใดและมีสิ่งใดที่ต้องปรับปรุงแก้ไข เพื่อเพิ่มคุณค่าให้กับองค์กรได้ แม้ต้องเผชิญกับความเปลี่ยนแปลงที่สำคัญ ซึ่งประกอบด้วยกรอบแนวทางปฏิบัติ 3 หลักการ ดังนี้

หลักการที่ 15 ประเมินการเปลี่ยนแปลงที่สำคัญ (Assesses Substantial Change)

องค์กรควรระบุและประเมินการเปลี่ยนแปลง ทั้งภายในและภายนอกกิจการที่อาจส่งผลกระทบต่อกลยุทธ์และวัตถุประสงค์ทางธุรกิจที่สำคัญ

หลักการที่ 16 ทบทวนความเสี่ยงและผลการดำเนินงาน (Reviews Risk and Performance)

องค์กรควรทบทวนผลการดำเนินงานขององค์กร รวมถึงพิจารณาทบทวนความเสี่ยงที่เกี่ยวข้อง เช่น องค์กรมีผลการดำเนินงานตามเป้าหมายแล้วหรือไม่

หลักการที่ 17 มุ่งมั่นปรับปรุงการบริหารความเสี่ยงองค์กร (Pursues Improvement in Enterprise Risk Management)

องค์กรควรปรับปรุงการบริหารความเสี่ยงองค์กรอยู่สม่ำเสมอโดยเฉพาะช่วงเวลาการเปลี่ยนแปลงที่สำคัญ เช่น การปรับโครงสร้างองค์กร หลังการประเมินผลการดำเนินงาน หรือการเปลี่ยนแปลงจากสภาพแวดล้อมภายนอกต่างๆ ที่ส่งผลกระทบต่อระบบการบริหารความเสี่ยง

องค์ประกอบที่ 5 สารสนเทศ การสื่อสารและการรายงาน (Information, Communication, and Reporting)

การสื่อสารเป็นกระบวนการต่อเนื่องในการรวบรวมข้อมูลและแบ่งปันข้อมูลที่จาเป็นจากทั่วทั้งองค์กร โดยเป็นข้อมูลที่เกี่ยวข้องทั้งจากแหล่งภายในและแหล่งภายนอก ซึ่งข้อมูลสารสนเทศดังกล่าว จะมาจากทั้งผู้บริหารและพนักงานขององค์กร เพื่อสนับสนุนการบริหารความเสี่ยงทั่วทั้งองค์กร โดยองค์กรจะใช้ประโยชน์จากระบบข้อมูล เพื่อรวบรวม ประมวลผล และจัดการข้อมูลต่างๆ ที่สัมพันธ์กับการบริหารความเสี่ยง จากนั้นองค์กรจึงรายงานข้อมูลความเสี่ยง วัฒนธรรมองค์กร และผลการดำเนินการได้ ซึ่งประกอบด้วยกรอบแนวทางปฏิบัติ 3 หลักการ ดังนี้

หลักการที่ 18 ยกระดับระบบสารสนเทศ (Leverages Information Systems)

องค์กรควรจัดให้มีสารสนเทศอย่างเพียงพอเหมาะสมและทันต่อเวลา องค์กรอาจใช้กระบวนการวิเคราะห์กลุ่มข้อมูลขนาดใหญ่ (Big Data Analytics) เพื่อค้นหารูปแบบความสัมพันธ์ของสิ่งเชื่อมโยงข้อมูลเข้าไว้ด้วยกันนำไปสู่การระบุและจัดการความเสี่ยงได้ดีขึ้น

หลักการที่ 19 สื่อสารข้อมูลความเสี่ยง (Communicates Risk Information)

องค์กรควรสื่อสารข้อมูลการบริหารความเสี่ยงองค์กรผ่านช่องทางการติดต่อต่างๆ ข้อมูลการสื่อสารทั้งระดับบนลงล่าง (Top-down Approach) และระดับล่างขึ้นบน (Bottom-up Approach) การสื่อสารข้อมูลความเสี่ยงควรมีให้เพียงพอทั้งภายในและภายนอกองค์กร

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

องค์กรควรรายงานความเสี่ยง วัฒนธรรมองค์กร และผลการดำเนินงานในทุกระดับให้ครอบคลุมทั่วทั้งองค์กร แม้จะมีการมอบหมายหน้าที่ด้านการรายงานผลให้หน่วยงานหรือบุคคลใดแล้วก็ตาม ผู้บริหารยังต้องมีหน้าที่กำกับดูแลด้วย

ความแตกต่างระหว่าง COSO ERM 2004 กับ COSO ERM 2017

COSO ERM 2004 เป็นหลักการบริหารความเสี่ยงที่เน้นการเชื่อมโยงการบริหารความเสี่ยงกับความเสี่ยงทุกประเภทตามวัตถุประสงค์ทางธุรกิจ (Business Objectives) และสำหรับหน่วยงานทุกระดับ (Enterprise-Wide) ทั่วทั้งองค์กร

COSO ERM 2017 เป็นหลักการบริหารความเสี่ยงที่เน้นการเชื่อมโยงระหว่างการบริหารความเสี่ยงกับการวางแผนกลยุทธ์ เพื่อสร้างมูลค่าเพิ่มให้กับองค์กร

ภาพที่ 28 กรอบการบริหารความเสี่ยง COSO-ERM 2017

ที่มา : ทำความรู้จักกับการประเมินความเสี่ยงด้าน ESG ตามกรอบ COSO ERM 2017. (ชยาภา ชยาวิวัฒนาวงศ์, 2561: 4)

ในปี พ.ศ.2564 กรมบัญชีกลาง กระทรวงการคลัง ได้กำหนดแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่องหลักการบริหารจัดการความเสี่ยงระดับองค์กร ที่ กค 1409.7/ ว 36 (หน้า 148) เพื่อปรับใช้ในการวางระบบการบริหารจัดการความเสี่ยงของหน่วยงานเพื่อให้หน่วยงานได้รับประโยชน์สูงสุดจากการบริหารจัดการความเสี่ยงอย่างแท้จริง โดยหน่วยงานของรัฐแต่ละหน่วยอาจมีศักยภาพแตกต่างกัน ทั้งนี้ขึ้นอยู่กับความพร้อมของหน่วยงาน โดยมีกรอบการบริหารจัดการความเสี่ยงประกอบด้วยหลักการ 8 ประการ ดังนี้

(1) การบริหารจัดการความเสี่ยงต้องดำเนินการแบบบูรณาการทั่วทั้งองค์กร

(2) ความมุ่งมั่นของผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ และผู้บริหารระดับสูง

(3) การสร้างและรักษาบุคลากรและวัฒนธรรมที่ดีขององค์กร

(4) การมอบหมายหน้าที่ความรับผิดชอบด้านการบริหารจัดการความเสี่ยง

(5) การตระหนักถึงผู้มีส่วนได้เสีย

(6) การกำหนดยุทธศาสตร์/กลยุทธ์ วัตถุประสงค์ และการตัดสินใจ

(7) การใช้ข้อมูลสารสนเทศ

(8) การพัฒนาอย่างต่อเนื่อง

(1) การบริหารจัดการความเสี่ยงต้องดำเนินการแบบบูรณาการทั่วทั้งองค์กร

การบริหารจัดการความเสี่ยงต้องดำเนินการแบบบูรณาการทั่วทั้งองค์กรการบริหารจัดการความเสี่ยงแบบบูรณาการควรมีลักษณะ ดังนี้

1. การบริหารจัดการความเสี่ยงต้องมีการบริหารจัดการในภาพรวมมากกว่าแยกเดียวเนื่องจากความเสี่ยงของกิจกรรมหนึ่งอาจมีผลกระทบต่อความเสี่ยงของกิจการอื่นๆ เช่น ความเสี่ยงของความล่าช้าในระบบการขนส่งวัสดุไม่เพียงพอต่อกิจการผลิต อาจมีผลกระทบต่อการขนส่งมอบสินค้า ค่าปรับ ที่อาจจะเกิดคลื่นรวมถึงชื่อเสียงขององค์กร เป็นต้น

2. การบริหารความเสี่ยงกวนผนวกเข้าเป็นส่วนหนึ่งของการดำเนินงานขององค์กรรวมถึงกระบวนการจัดทำแผนกลยุทธ์ และกระบวนการประเมินผล

3. การบริหารจัดการความเสี่ยง ต้องช่วยสนับสนุนกระบวนการตัดสินใจในทุกระดับขององค์กร

(2) ความมุ่งมั่นของผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ และผู้บริหารระดับสูง

ความมุ่งมั่นของผู้กำกับดูแลหัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงการบริหารจัดการความเสี่ยงจะประสบผลสำเร็จขึ้นอยู่กับความมุ่งมั่นของผู้กำกับ ดูแล หัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูง หน่วยงานของรัฐบางแห่งมีผู้กำกับดูแลในรูปแบบของคณะกรรมการซึ่งมีหน้าที่ในการกำกับฝ่ายบริหารให้มีการบริหารจัดการความเสี่ยงตามหลักธรรมาภิบาล ผู้กำกับดูแลซึ่งมีหน้าที่ดังกล่าวจะมีหน้าที่ในการกำกับการบริหารจัดการความเสี่ยงด้วย สำหรับหัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงมีหน้าที่ความรับผิดชอบในการบริหารจัดการความเสี่ยง

การกำกับการบริหารจัดการความเสี่ยงเป็นกระบวนการที่ทำให้ผู้กำกับดูแลเกิดความมั่นใจว่าหัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงได้บริหารจัดการความเสี่ยงอย่างเหมาะสมเพียงพอและมีประสิทธิผล

หัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงมีหน้าที่โดยตรงในการสร้างระบบบริหารจัดการความเสี่ยงที่มีประสิทธิผลประกอบด้วย การสร้างสภาพแวดล้อม วัฒนธรรมองค์กร และระบบการบริหารบุคคลที่เหมาะสม การจัดสรรทรัพยากรที่เพียงพอในการบริหารจัดการความเสี่ยง การดำเนินงานตามกระบวนการบริหารจัดการความเสี่ยง การพัฒนาระบบข้อมูลสารสนเทศ การรายงานและการสื่อสาร เป็นต้น

ผู้กำกับ ดูแล (ถ้ามี) อาจตั้งคณะกรรมการบริหารจัดการความเสี่ยง (หรืออนุกรรมการ หรือคณะที่ปรึกษา) ขึ้น ซึ่งประกอบด้วย ผู้มีทักษะประสบการณ์และผู้เชี่ยวชาญเกี่ยวกับด้านการดำเนินงานของหน่วยงาน เช่น หน่วยงานมีการใช้ระบบเทคโนโลยีสารสนเทศเป็นหลักในการดำเนินงานอาจจำเป็นต้องมีผู้เชี่ยวชาญอิสระในการกำกับหรือให้ความเห็นเกี่ยวกับความเพียงพอและความเหมาะสมของการบริหารจัดการความเสี่ยงในเรื่องความเสี่ยงทางไซเบอร์ของหัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูง เป็นต้น

(3) การสร้างและรักษาบุคลากรและวัฒนธรรมที่ดีขององค์กร

การสร้างและรักษาบุคลากรและวัฒนธรรมที่ดีขององค์กรการขับเคลื่อนหน่วยงานของรัฐต้องอาศัยบุคลากรที่มีศักยภาพการบริหารทรัพยากรบุคคลเริ่มตั้งแต่การสรรหาการพัฒนาบุคลากรให้มีความรู้ความสามารถการส่งเสริมและรักษาไว้ซึ่งบุคลากรที่มีความรู้ความสามารถโดยบุคลากรถือว่าเป็นสินทรัพย์หลักขององค์กรที่ทำให้องค์กรประสบผลสำเร็จ

การสร้างบุคลากรให้มีความรู้และทักษะในการบริหารจัดการความเสี่ยงถือเป็นส่วนหนึ่งของการบริหารจัดการความเสี่ยงบุคลากรควรมีพฤติกรรมการหนักถึงความเสี่ยง (Risk-aware behaviors) รวมถึงวิธีการตัดสินใจโดยใช้ข้อมูลสารสนเทศและข้อมูลการบริหารจัดการความเสี่ยง

การสร้างพฤติกรรมที่ดี (Desired behaviors) ในการส่งเสริมการบริหารจัดการความเสี่ยงผ่านวัฒนธรรมที่ดีขององค์กรเป็นสิ่งสำคัญการสร้างวัฒนธรรมที่สนับสนุนการบริหารจัดการความเสี่ยงประกอบด้วย

1. การสื่อสารและความการตระหนักถึงนโยบายการบริหารจัดการความเสี่ยงของหน่วยงาน
2. การสร้างความตระหนักถึงหน้าที่ของอุปกรณ์ในการแจ้งข้อมูลผิดปกติ
3. การสร้างพฤติกรรมการแบ่งปันข้อมูลภายในอุปกรณ์
4. การสร้างพฤติกรรมการตัดสินใจตามนโยบายการบริหารจัดการความเสี่ยง
5. การสร้างพฤติกรรมการตระหนักถึงความเสี่ยงและโอกาส

(4) การมอบหมายหน้าที่ความรับผิดชอบด้านการบริหารจัดการความเสี่ยง

การมอบหมายหน้าที่ความรับผิดชอบด้านการบริหารจัดการความเสี่ยงหน่วยงานควรมีการกำหนดอำนาจหน้าที่ความรับผิดชอบในเรื่องของการบริหารจัดการความเสี่ยงอย่างชัดเจนและเหมาะสมประกอบด้วยเจ้าของความเสี่ยง (Risk owners) ซึ่งรับผิดชอบในการติดตามรายงานหรือการส่งสัญญาณความเสี่ยงผู้รับผิดชอบในการตัดสินใจในกรณีที่ความเสี่ยงเกิดขึ้นในระดับที่กำหนดไว้และผู้มีหน้าที่ในการควบคุมกำกับติดตามให้มีการบริหารจัดการความเสี่ยงตามแผนการบริหารจัดการความเสี่ยง

(5) การตระหนักถึงผู้มีส่วนได้เสีย

การบริหารจัดการความเสี่ยงการบริหารจัดการความเสี่ยงนอกจากจะคำนึงถึงวัตถุประสงค์ขององค์กรเป็นหลักแล้ว ผู้บริหารต้องคำนึงถึงผู้มีส่วนได้ส่วนเสียในการบริหารจัดการความเสี่ยงด้วย โดยเฉพาะความคาดหวังของผู้รับบริการหรือความคาดหวังของประชาชนที่มีต่อองค์กร รวมถึงผลกระทบที่มีต่อสังคม เศรษฐกิจ และสภาพแวดล้อม

(6) การกำหนดยุทธศาสตร์/กลยุทธ์ วัตถุประสงค์ และการตัดสินใจ

การกำหนดยุทธศาสตร์กลยุทธ์วัตถุประสงค์และการตัดสินใจการบริหารจัดการความเสี่ยงเป็นเครื่องมือช่วยผู้บริหารในการกำหนดยุทธศาสตร์/กลยุทธ์ ขององค์กรเพื่อให้หน่วยงานนั้นมั่นใจว่ายุทธศาสตร์/กลยุทธ์ ขององค์กรสอดคล้องกับพันธกิจตามกฎหมายและหน้าที่ความรับผิดชอบของหน่วยงาน ยุทธศาสตร์/กลยุทธ์ หมายรวมถึงแผนปฏิบัติราชการระยะยาว แผนปฏิบัติราชการระยะปานกลาง หรือแผนปฏิบัติราชการประจำปีของหน่วยงาน

เมื่อหน่วยงานของรัฐกำหนดยุทธศาสตร์/กลยุทธ์โดยสอดคล้องกับความเสี่ยงที่ยอมรับและได้ขนาดองค์กรแล้วการบริหารจัดการความเสี่ยงจะถูกใช้บังคับเป็นเครื่องมือในการกำหนดทางเลือกของงานโครงการ (งานใหญ่ๆ) และการกำหนดวัตถุประสงค์ระดับปฏิบัติงานรวมถึงการมอบหมายความรับผิดชอบในการบริหารจัดการความเสี่ยงทั่วทั้งองค์กรโดยอาจกำหนดเป็นส่วนหนึ่งของตัวชี้วัดผลการปฏิบัติงาน (KPI)

(7) การใช้ข้อมูลสารสนเทศ

การใช้ข้อมูลสารสนเทศในปัจจุบันข้อมูลสารสนเทศเป็นสิ่งสำคัญอย่างยิ่งในการดำเนินงานของหน่วยงานองค์กรที่มีการบริหารจัดการข้อมูลสารสนเทศอย่างมีประสิทธิภาพ ส่งผลโดยตรงต่อการบริหารจัดการความเสี่ยงหน่วยงานควรพิจารณาใช้ข้อมูลสารสนเทศในการบริหารจัดการความเสี่ยง เพื่อให้ผู้บริหารสามารถตัดสินใจโดยใช้ข้อมูลความเสี่ยงเป็นพื้นฐานหน่วยงานควรกำหนดประเภทข้อมูลที่ต้องรวบรวม วิธีการรวบรวม และการวิเคราะห์ข้อมูล และบุคลากรที่ควรได้รับข้อมูล

ข้อมูลความเสี่ยงประกอบด้วย เหตุการณ์ที่เป็นผลกระทบทางลบหรือทางบวกต่อองค์กร สาเหตุความเสี่ยง ตัวผลักดันความเสี่ยงหรือตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk indicators) ข้อมูลสารสนเทศต้องมีความถูกต้อง เชื่อถือได้ เกี่ยวข้องกับการตัดสินใจและทันต่อเวลา ทั้งนี้ หน่วยงานพิจารณาการรวบรวมการประมวลผลหรือการวิเคราะห์ความเสี่ยงแบบอัตโนมัติ เพื่อลดข้อผิดพลาดจากบุคคล (Human error)

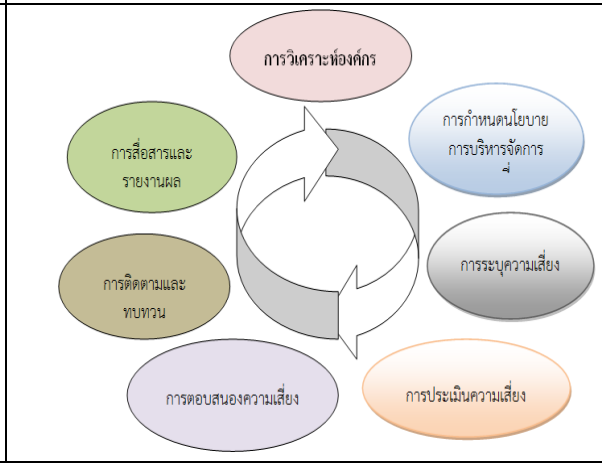
(8) การพัฒนาอย่างต่อเนื่อง

การพัฒนาอย่างต่อเนื่องการบริหารจัดการความเสี่ยง ต้องมีการพัฒนาอย่างต่อเนื่อง ความสมบูรณ์ของระบบการบริหารจัดการความเสี่ยงขึ้นอยู่กับขนาด โครงสร้าง ศักยภาพขององค์กร รวมถึงการใช้ระบบสารสนเทศในการบริหารจัดการความเสี่ยง หน่วยงานอาจพิจารณาทำ Benchmarking เพื่อพัฒนาระบบบริหารจัดการความเสี่ยงขององค์กรอย่างต่อเนื่อง หน่วยงานอาจพัฒนาระบบการบริหารจัดการความเสี่ยงเริ่มต้นจากการบริหารจัดการความเสี่ยงแบบ Silo พัฒนาเป็นการบริหารจัดการความเสี่ยงแบบบูรณาการและพัฒนาต่อเนื่องโดยมีการฝังการบริหารจัดการความเสี่ยงเข้าสู่กระบวนการดำเนินงานโดยปกติของอุปกรณ์และการตัดสินใจบนพื้นฐานข้อมูลด้านความเสี่ยง

กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงเป็นกระบวนการต่อเนื่อง โดยเริ่มต้นด้วยการกำหนดนโยบายหรือวัตถุประสงค์ของการบริหารความเสี่ยงที่ชัดเจนจากฝ่ายบริหาร และดำเนินกระบวนการด้วยกลไกการบริหารความเสี่ยงที่กำหนดขึ้นในองค์กร ร่วมกับกลไกการตรวจสอบหรือการควบคุมภายในจนสามารถประเมินความสำเร็จตามวัตถุประสงค์ได้ และนำไปสู่การปรับปรุงกลไกกระบวนการบริหารความเสี่ยงให้มีประสิทธิภาพสูงขึ้นต่อไป ตามคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง (2555 : 26) ได้มีการระบุไว้ว่า ขั้นตอนดำเนินการตามกระบวนการบริหารความเสี่ยงองค์กรสามารถแบ่งออกเป็น 6 ขั้นตอน แนวทางการบริหารจัดการความเสี่ยงของกรมบัญชีกลาง (ว 36) 7 ขั้นตอน (ตารางที่ 2) (ภาพที่ 28)

ตารางที่ 2 แสดงขั้นตอนดำเนินการตามกระบวนการบริหารความเสี่ยงองค์กร

สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง	**กรมบัญชีกลาง กระทรวงการคลัง (ว 36)**
1. การกำหนดวัตถุประสงค์ (Objective Setting) 2. การระบุความความเสี่ยง (Risk Identification) 3. การประเมินความเสี่ยง (Risk Assessment) 4. การประเมินมาตรการควบคุมภายใน (Risk Control) 5. การจัดการความเสี่ยง (Risk Treatment) 6. การรายงานและติดตามความเสี่ยง (Risk Reporting & Monitoring)	1. การวิเคราะห์องค์กร 2. การกำหนดนโยบายการบริหารจัดการความเสี่ยง 3. การระบุความเสี่ยง 4. การประเมินความเสี่ยง 5. การตอบสนองความเสี่ยง 6. การติดตามและทบทวน 7. การสื่อสารและรายงานผล
	

ภาพที่ 29 กระบวนการบริหารความเสี่ยง

ที่มา : คู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง (2555: 26)

1. การกำหนดวัตถุประสงค์

การกำหนดวัตถุประสงค์ที่ชัดเจนขององค์กรนั้น เป็นขั้นตอนแรกสาหรับกระบวนการบริหารความเสี่ยง ในการกำหนดวัตถุประสงค์ควรจัดทำเป็นลายลักษณ์อักษรอย่างชัดเจน มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์ และความเสี่ยงที่หน่วยงานยอมรับได้ รวมทั้งควรมีการสื่อสารให้แก่ทุกหน่วยงานรับทราบ เพื่อให้มีความเข้าใจที่ตรงกันการกำหนดวัตถุประสงค์ (Objective Setting) เป็นการกำหนดวัตถุประสงค์ของหน่วยงานโดยรวม รวมถึงกระบวนการหลักต่างๆ ให้สอดคล้องกับวัตถุประสงค์ขององค์กร ได้แก่

1) วัตถุประสงค์ด้านกลยุทธ์ (Strategic Objectives) เป็นวัตถุประสงค์ในระดับสูง ซึ่งเชื่อมโยงและสนับสนุนภารกิจขององค์กร โดยหน่วยงานกำหนดวัตถุประสงค์ด้านกลยุทธ์เพื่อแสวงหาทางเลือกหรือวิธีการในการสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้ส่วนเสีย นั่นหมายถึง มีเป้าหมายและแผนงาน

2) วัตถุประสงค์ด้านการปฏิบัติงาน (Operations Objectives) เป็นวัตถุประสงค์ในระดับของการปฏิบัติงานที่มุ่งเน้นการใช้ทรัพยากรอย่างมีประสิทธิภาพ ประสิทธิผลและความคุ้มค่า

3) วัตถุประสงค์ด้านการรายงาน (Reporting Objectives) เป็นวัตถุประสงค์ที่มุ่งเน้นการจัดทำรายงาน ทั้งรายงานทางการเงิน (Financial reporting) และรายงานที่ไม่ใช่ทางการเงิน (Nonfinancial reporting) ซึ่งนำเสนอต่อผู้ใช้ทั้งภายในและภายนอกให้มีความน่าเชื่อถือ โดยมุ่งเน้นถูกต้อง สมบูรณ์ และทันเวลา เพื่อสามารถนำไปใช้ในการตัดสินใจต่างๆ ได้อย่างเหมาะสม

4) วัตถุประสงค์ด้านการปฏิบัติตามกฎระเบียบ (Compliance Objectives) เป็นวัตถุประสงค์ที่มุ่งเน้นความถูกต้องการปฏิบัติตามกฎหมาย หรือกฎระเบียบที่เกี่ยวข้อง

ตาม**คู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน** สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง (2555: 33) ระบุการกำหนดวัตถุประสงค์ที่ดี ควรเป็นไปตามหลักการที่เรียกว่า **“SMART”** ประกอบด้วย

☐ Specific (มีความชัดเจน) วัตถุประสงค์ควรมีความชัดเจนและกำหนดผลตอบแทนหรือผลลัพธ์ที่ต้องการที่ทุกคนสามารถเข้าใจได้อย่างชัดเจน

☐ Measurable (สามารถวัดได้) วัตถุประสงค์ควรสามารถวัดผลได้ ควรมีการระบุหลักเกณฑ์และข้อมูลที่ต้องการใช้ในการวัดผล ในกรณีที่ไม่สามารถวัดผลได้ ผู้บริหารควรเพิ่มความระมัดระวังในการพิจารณากิจกรรมต่างๆ ที่เกี่ยวข้องกับวัตถุประสงค์ด้วย

☐ Achievable (สามารถบรรลุผลได้) มีความเป็นไปได้ที่จะสามารถบรรลุวัตถุประสงค์ได้จริง ภายใต้เงื่อนไขการใช้ทรัพยากรที่มีอยู่ในปัจจุบัน

☐ Relevant (มีความเกี่ยวข้อง) มีความสอดคล้องกับกลยุทธ์และเป้าหมายในการดำเนินงานขององค์การ

☐ Timeliness (มีกำหนดเวลา) ควรมีกำหนดระยะเวลาที่ต้องการบรรลุผลให้ชัดเจน

ดังนั้น สำนักงานตรวจสอบภายใน จึงได้ใช้การกำหนดวัตถุประสงค์แบบ **“SMART”** เพื่อเป็นแนวทางในการกำหนดวัตถุประสงค์ของหน่วยงาน ซึ่งจะทำให้การบริหารงานและการดำเนินงานของสำนักงานตรวจสอบ

ภายในให้มีความสอดคล้องกันทั้งหน่วยงาน ตามแผนปฏิบัติงานประจำปี โดยในการกำหนดวัตถุประสงค์จะทำการแบ่งวัตถุประสงค์ไว้ 2 ระดับ คือ 1. ระดับส่วนงาน และ 2. ระดับกิจกรรม

1. ระดับส่วนงาน

การกำหนดวัตถุประสงค์ระดับส่วน (Division Objectives) เป็นการนำวัตถุประสงค์และเป้าหมายจากแผนปฏิบัติงานประจำปีมาวิเคราะห์ความเสี่ยง อันที่จะทำให้ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนด

2. ระดับกิจกรรม

การกำหนดวัตถุประสงค์ระดับกิจกรรม (Activity-Level Objectives) เป็นการกำหนดวัตถุประสงค์ และเป้าหมายตามพันธกิจของแต่ละกลุ่มภารกิจ เพื่อนาไปสู่การวิเคราะห์ความเสี่ยงที่จะทำให้พันธกิจของกลุ่มภารกิจไม่บรรลุผลตามวัตถุประสงค์ที่วางไว้ ทั้งนี้ การที่องค์กรจะสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ได้ ควรดำเนินงานภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) เพื่อทำให้ผู้บริหารมั่นใจได้ว่าการดำเนินงานขององค์การอยู่ภายในเกณฑ์หรือประเภทของความเสี่ยงที่ยอมรับได้ (Risk Appetite) ความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ประเภท ปัจจัยความเสี่ยง และระดับของความเสี่ยงที่องค์กรจะยอมรับได้ เพื่อช่วยให้องค์กรบรรลุวิสัยทัศน์ และภารกิจขององค์กรความเบี่ยงเบน (Risk Tolerance) หมายถึง ระดับความเบี่ยงเบนจากประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่ยอมรับได้ ตามคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน, กระทรวงการคลัง (2555:35) กำหนดไว้ว่า แผนบริหารความเสี่ยงควรปรากฏในแผนปฏิบัติงานประจำปี และเป้าหมายในแผนบริหารความเสี่ยงควรสอดคล้องกับเป้าหมายที่ระบุในแผนปฏิบัติการประจำปี

2. รัฐวิสาหกิจควรมีแผนการบริหารความเสี่ยงปรากฏในแผนกลยุทธ์ประจำปีของรัฐวิสาหกิจ และเป้าหมายในแผนบริหารความเสี่ยงควรสอดคล้องกับเป้าหมายที่ระบุในแผนปฏิบัติการประจำปีของรัฐวิสาหกิจ

2. การระบุความความเสี่ยง

การระบุความความเสี่ยง หรือ การบ่งชี้ความเสี่ยง (Risk Identification) เป็นขั้นตอนการค้นหาความเสี่ยงและสาเหตุหรือปัจจัยของความเสี่ยง โดยพิจารณาจากปัจจัยต่างๆ ทั้งภายในและภายนอกที่ส่งผลกระทบต่อเป้าหมายผลลัพธ์ขององค์การตามกรอบการบริหารความเสี่ยง ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง แหล่งที่มาของปัจจัยต่าง ๆ ได้แก่

ปัจจัยภายในหน่วยงาน : วัตถุประสงค์ขององค์การนโยบายและกลยุทธ์ การดำเนินงานกระบวนการทำงาน ประสบการณ์การทำงาน โครงสร้างองค์กรและระบบการบริหารงาน การเงินวัฒนธรรมของ องค์การสภาพทางภูมิศาสตร์ เทคโนโลยีสารสนเทศ และกฎหมาย ระเบียบที่เกี่ยวข้องภายในองค์กร เป็นต้น

ปัจจัยภายนอกหน่วยงาน : นโยบายของรัฐบาล นโยบายมหาวิทยาลัย สภาวะเศรษฐกิจ การดำเนินการของหน่วยงานที่เกี่ยวข้อง กฎระเบียบภายนอกองค์กรเหตุการณ์ธรรมชาติ สภาพสังคม และการเมืองเป็นต้น การระบุปัจจัยเสี่ยงจะเริ่มต้นที่เป้าประสงค์ หรือวัตถุประสงค์ขององค์การ โดยการมองปัจจัยเสี่ยงไม่จำเป็นต้องมาก แต่ต้อง

มีเรื่องการบริหารและการควบคุมในการรองรับปัญหาที่ดีพอ ทั้งนี้ การจัดประเภทความเสี่ยงองค์กร จะแบ่งประเภทตามกรอบการบริหารความเสี่ยงองค์การ ได้แก่

1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงอันเกิดจากการที่องค์การไม่สามารถบรรลุวัตถุประสงค์ขององค์กรอันเนื่องมาจากขาดกลยุทธ์ที่เหมาะสมหรือสภาพการแข่งขันที่เปลี่ยนแปลง

2) ความเสี่ยงด้านการปฏิบัติงาน (Operation Risk) ความเสี่ยงอันเกิดจากการดำเนินงานภายในองค์กร ซึ่งเป็นผลมาจากบุคลากร กระบวนการทำงาน โครงสร้างพื้นฐาน รวมถึงการทุจริตภายในองค์การ

3) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงที่ก่อให้เกิดผลกระทบทางด้านการเงินต่อองค์กร

4) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk) ความเสี่ยงอันเกิดจากการไม่ปฏิบัติตามกฎ ระเบียบ ข้อบังคับ โดยครอบคลุมถึงกฎระเบียบของทั้งหน่วยงานภายในและภายนอกที่กากับดูแลองค์การการค้นหาความเสี่ยงสามารถศึกษาได้จากข้อมูลสถิติของความเสี่ยงที่เคยเกิดขึ้น การสำรวจในปัจจุบันหรือคาดว่าอาจจะเกิดขึ้นในอนาคต การรวบรวมข้อมูลเพื่อบ่งชี้เหตุการณ์ที่มีความเสี่ยงจะเป็นการรวบรวมข้อมูลทั้งแบบ Top-down คือ การระดมความคิดเห็นผู้บริหารของหน่วยงานเพื่อระบุความเสี่ยงด้านกลยุทธ์ขององค์การ และแบบ Bottom-up คือ การระดมความคิดเห็นของบุคลากร เพื่อระบุความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านการเงิน และความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ จากนั้นนาข้อมูลที่ได้ทั้งจากผู้บริหารและบุคลากร รวบรวมเป็นรายการความเสี่ยงองค์กร (Risk register) และประเมินความเสี่ยงนั้นๆ ในขั้นตอนต่อไป

ดังนั้น ในการระบุความเสี่ยงผู้ประเมินควรทำความเข้าใจ และทราบถึงวัตถุประสงค์หรือเป้าหมายที่ชัดเจนของงานแต่ละงานและเหตุการณ์ใดหรือกิจกรรมใดของกระบวนการปฏิบัติงาน ที่จะทำให้ไม่บรรลุวัตถุประสงค์ของงานที่วางไว้ รวมถึงการทำความเข้าใจเกี่ยวกับกิจกรรมที่ปฏิบัติอย่างรอบคอบชัดเจนในการระบุความเสี่ยง ให้พิจารณาจากแผนงาน โครงการ/กิจกรรม ตัวชี้วัด เป้าหมาย จากแผนปฏิบัติการประจำปี ผลการดำเนินงานที่ผ่านมาองค์กร ซึ่งในการดำเนินงานอาจเกิดเหตุการณ์ที่ทำให้ไม่สามารถบรรลุเป้าหมาย หรือวัตถุประสงค์ขององค์กรแล้วส่งผลต่อการดำเนินงานโดยรวมขององค์กรการระบุความเสี่ยงให้ระบุโดยพิจารณาตามเหตุแห่งความเสี่ยง (Sources of Risk) ที่อาจส่งผลกระทบต่อวัตถุประสงค์/เป้าหมายของโครงการหรือกิจกรรม หรือสร้างความเสียหายทั้งทางตรงและทางอ้อมอย่างมีนัยสำคัญ ในการวิเคราะห์ความเสี่ยงควรเน้นที่จะระบุปัจจัยเสี่ยงและเหตุการณ์ความเสียหายที่เกี่ยวข้องกับกิจกรรมสำคัญ ทั้งนี้ไม่คำนึงถึงมาตรการควบคุมความเสี่ยงที่มีอยู่ในปัจจุบัน โดยครอบคลุมทั้งความเสี่ยงที่อยู่และไม่อยู่ภายใต้การควบคุม หรือความรับผิดชอบของหน่วยงาน และพิจารณาดูว่าเหตุการณ์นั้นเกิดขึ้นได้อย่างไร ซึ่งจากการพิจารณาความเสี่ยงสามารถแบ่งได้ ดังนี้

1. ความเสี่ยงจากลักษณะธุรกิจ (Inherent Risk) เป็นความเสี่ยงที่มีอยู่โดยธรรมชาติในธุรกิจหรืองานแต่ละอย่าง เมื่อใดก็ตามที่ตัดสินใจที่จะทำธุรกิจหรืองานนั้นๆ ก็ย่อมมีความเสี่ยงเกิดขึ้น

2. ความเสี่ยงที่เหลืออยู่ (Residual Risk) เป็นความเสี่ยงที่เหลืออยู่หลังจากที่ได้ดำเนินการจัดให้มีจุดควบคุมความเสี่ยงนั้นแล้ว

แนวทางที่สามารถใช้ในการระบุความเสี่ยง

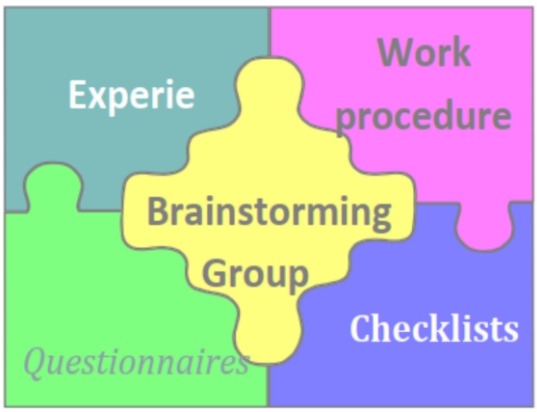
1. การใช้ประสบการณ์ (Experience) ของผู้ประเมินในการระบุเหตุการณ์ที่เคยเกิดขึ้น หรือพิจารณาแล้วว่ามีโอกาสที่จะเกิดขึ้นได้ หรือใช้การเก็บข้อมูลเกี่ยวกับปัญหา/ข้อผิดพลาดในกระบวนการทำงานที่เคยเกิดขึ้นในอดีต และได้มีการบันทึกไว้ หรือเป็นข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์สามารถนามาใช้เป็นแนวทางและเป็นข้อมูลเบื้องต้นได้

2. การใช้คู่มือปฏิบัติงาน (Work procedure Manual) เพื่อลำดับขั้นตอนของกระบวนการทำงานและพิจารณาว่าในแต่ละขั้นตอนอาจจะเกิดเหตุการณ์ต่างๆ ซึ่งอาจจะทำให้กิจกรรมนั้นๆ หยุดชะงักหรือผิดพลาดจนก่อให้เกิดความเสียหายขึ้นได้หรือไม่

3. การระดมความคิด (Brainstorming Group) จากพนักงานที่มีส่วนเกี่ยวข้องกับกิจกรรมดังกล่าวทั้งภายในและภายนอกหน่วยงาน เพื่อร่วมกันพิจารณาว่ามีเหตุการณ์ใดบ้างที่เกิดขึ้นแล้วส่งผลกระทบเสียหายต่องานที่ดูแล

4. การใช้แบบสอบถามความคิดเห็น (Questionnaires) ไปยังผู้รับผิดชอบกิจกรรมต่างๆว่ามีปัญหาข้อผิดพลาด หรือความเสี่ยงในลักษณะใด ก่อให้เกิดความเสียหายมากน้อยแค่ไหน อย่างไรก็ดีควรระลึกว่าการสอบถามควรกระทำกับเจ้าหน้าที่ที่เกี่ยวข้องโดยตรง ซึ่งเป็นผู้ทราบข้อมูลต่างๆ อย่างแท้จริง นอกจากนี้คำตอบที่ได้รับอาจจะไม่ใช่ข้อเท็จจริงทั้งหมด เพราะการตอบคำถามอาจจะรวมข้อคิดเห็น ความรู้สึก และทัศนคติส่วนตัว ดังนั้นผู้ประเมินควรใช้วิธีอื่นควบคู่กันไปด้วย

5. การใช้แบบตรวจสอบรายการ (Checklists) โดยผู้บริหาร และพนักงานในหน่วยงานสามารถตรวจสอบวิธีการทำงาน ขั้นตอนการทำงาน และมาตรฐานการทำงานตาม Checklist ที่จัดทำได้ด้วยตนเอง และควรกำหนดระยะเวลาในการประเมินผลภายในหน่วยงานด้วย Checklist ที่ชัดเจน เช่น ทุก 3 เดือน 6 เดือน หรือ 12 เดือน



ภาพที่ 30 แสดงแนวทางในการระบุความเสี่ยง (Risk Identifications)

ในการเลือกใช้แหล่งข้อมูลหรือวิธีการใดในการระบุความเสี่ยงนั้น อาจแตกต่างกันในแต่ละหน่วยงานและแต่ละมูลเหตุความเสี่ยง โดยขึ้นกับลักษณะงานและวิธีปฏิบัติงานของหน่วยงานความเสี่ยงและเหตุแห่งความเสี่ยงควรครอบคลุมในเรื่องต่อไปนี้

1. ความเสียหายหรือเหตุการณ์ ที่อาจมีผลกระทบในเชิงลบต่อองค์กร

2. ความไม่แน่นอนที่อาจมีผลต่อการบรรลุวัตถุประสงค์และกลยุทธ์ขององค์กร

3. เหตุการณ์ที่อาจทำให้องค์กรสูญเสียโอกาสในการสร้างรายได้หรือสร้างโอกาสทางธุรกิจหรือการได้รับการยอมรับการหน่วยงานภายนอก

นอกจากนี้ในการระบุความเสี่ยงควรพิจารณาให้ครอบคลุมถึง

1. ความเสี่ยงที่อาจเกิดขึ้นทุกด้าน เช่น ความเสี่ยงด้านกลยุทธ์ การเงิน บุคลากรการดำเนินงานชื่อเสียง กฎหมาย ภาษีอากร ระบบงาน และสิ่งแวดล้อม เป็นต้น

2. ความเสี่ยงที่อาจเกิดขึ้นจากสาเหตุทั้งจากปัจจัยภายในและภายนอกองค์กร เพื่อเป็นตัวอย่างในการระบุความเสี่ยงในคู่มือฉบับนี้ ได้เลือกใช้ขั้นตอนวิเคราะห์และออกแบบระบบฐานข้อมูล เพื่อทำการระบุความเสี่ยง โดยใช้เทคนิคการวิเคราะห์ขั้นปฏิบัติการ ซึ่งประกอบด้วย 2 ขั้นตอน คือ

1. การระบุความเสี่ยง ซึ่งเป็นผลของความเสี่ยงที่เกิดขึ้นในแต่ละขั้นตอน

2. การระบุปัจจัยเสี่ยง เป็นต้นเหตุแห่งความเสี่ยงในแต่ละขั้นตอน

ภาพที่ 31 องค์ประกอบที่ทำให้เกิดความเสี่ยง (Risk Driver)

ในการบ่งชี้ความเสี่ยง จะต้องระบุสาเหตุของความเสี่ยงด้วยทุกครั้ง และควรระบุให้ครบทุกสาเหตุที่ทำให้เกิดความเสี่ยงดังกล่าว เพื่อให้ผู้บริหารสามารถกำหนดแผนจัดการความเสี่ยงให้บริหารจัดการความเสี่ยงได้ตรงกับสาเหตุที่ทำให้เกิดความเสี่ยง และสามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล

ตารางที่ 3 แสดงตัวอย่างการระบุปัจจัยเสี่ยง

ขั้นตอน	วัตถุประสงค์ขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง
แผนงานตรวจสอบภายใน			
จัดทำแผนงานด้านงานตรวจสอบภายใน	เพื่อให้มีแผนงานตรวจสอบภายในมีคุณภาพ แล้วเสร็จก่อนภายในปีงบประมาณ และสามารถนำไปปฏิบัติได้จริง	ไม่สามารถจัดทำแผนงานตรวจสอบภายในที่มีคุณภาพแล้วเสร็จได้ตามกำหนด	1. ข้อมูลที่ใช้ในการจัดทำแผนไม่เพียงพอและขาดคุณภาพ 2. บุคลากรขาดความรู้และความชำนาญในด้านการตลาดและการจัดทำแผนงานฯ 3. ขาดการสอบทานคุณภาพของแผนฯ ที่ดีจากผู้บริหาร/หัวหน้างาน
การตรวจสอบภายใน	เพื่อให้การตรวจสอบภายในเป็นไปตามเป้าหมายและมาตรฐานที่กำหนดไว้	การตรวจสอบภายในไม่เป็นไปตามเป้าหมายและมาตรฐานที่กำหนดไว้	1. งบประมาณไม่เพียงพองานตรวจสอบ 2. บุคลากรผู้ปฏิบัติงานขาดความรู้ความเข้าใจในแผนงานตรวจสอบ 3. กระบวนการตรวจสอบคุณภาพ (QC) ไม่มีประสิทธิภาพ

3. การประเมินความเสี่ยง

การประเมินความเสี่ยง (Risk Assessment) เป็นกระบวนการที่ควรดำเนินการหลังจากองค์กรทำการระบุความเสี่ยงแล้วการประเมินความเสี่ยงประกอบด้วย 2 มิติ คือ โอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบของความเสี่ยง (Impact) ดังนั้น ในการประเมินความเสี่ยงผู้ประเมินควรระบุลักษณะของความเสียหายจากความเสี่ยงที่มีโอกาสเกิดขึ้นอย่างชัดเจน เพื่อให้ทราบถึงผลกระทบที่เกิดขึ้นและเป็นข้อมูลในการประเมินระดับความรุนแรงของความเสี่ยง ที่อาจจะส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร ทั้งนี้เพื่อสามารถกำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสมต่อไป ขั้นตอนการประเมินความเสี่ยงนั้น ประกอบด้วยการดำเนินการ 4 ขั้นตอน ได้แก่

1) การกำหนดเกณฑ์ประเมินความเสี่ยง

2) การประเมินโอกาสและผลกระทบของความเสี่ยง

3) การวิเคราะห์ความเสี่ยง

4) การจัดลำดับความเสี่ยง

1) การกำหนดเกณฑ์ประเมินความเสี่ยง

เกณฑ์การประเมินความเสี่ยง เป็นขั้นตอนที่คณะกรรมการบริหารความเสี่ยงและการควบคุมภายในสำนักงานตรวจสอบภายใน กำหนดให้มีการดำเนินการร่วมกันทั่วทั้งหน่วยงาน โดยพิจารณาเงื่อนไขในการกำหนดเกณฑ์การประเมินความเสี่ยง 2 มิติ คือ โอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบของความเสี่ยง (Impact) เพื่อกำหนดระดับความเสี่ยง (Degree of Risks) ของความเสี่ยงแต่ละเหตุการณ์ต่อไป โดยสามารถกำหนดได้ทั้งเกณฑ์ในเชิงปริมาณและเชิงคุณภาพการกำหนดนิยามของแต่ละระดับคะแนน ควรกำหนดให้มีความสอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk appetite) ซึ่งจะมีความสอดคล้องกับสถานการณ์ในแต่ละ

ช่วงเวลา องค์กรจึงควรมีการทบทวนนิยามดังกล่าวในแต่ละปี โดยตัวอย่างนิยามที่ใช้เป็นแนวทางในการพิจารณาประเมินความเสี่ยง (ตารางที่ 4-6)

ตารางที่ 4 แสดงตัวอย่างโอกาสที่จะเกิดความเสี่ยง (Likelihood) เชิงปริมาณ และคุณภาพ

ระดับ	คะแนน	ด้านความเวลา (ระยะเวลาไม่ได้ทบทวนแผน)	โอกาสการเกิดเหตุการณ์
สูงมาก	5	> 5 ปี	- เคยเกิดขึ้นในองค์กรมากกว่า 1 ครั้ง ภายใน 1 ปี หรือ - คาดว่าจะเกิดขึ้นอย่างน้อย 1 ครั้งต่อปี หรือ - มีความเป็นไปได้ค่อนข้างแน่ว่าจะเกิดขึ้น
สูง	4	4 ปี	- เคยเกิดขึ้นในองค์กรมากกว่า 1 ครั้ง หรือ - คาดว่าจะเกิดขึ้นเกินกว่า 1 ครั้งในช่วง 5 ปีข้างหน้า
ปานกลาง	3	3 ปี	- เคยเกิดขึ้นในองค์กร 1 ครั้ง หรือ - คาดว่าจะเกิดขึ้นได้ในช่วง 5 ปีข้างหน้า
น้อย	2	2 ปี	- ไม่เคยเกิดขึ้นในองค์กรมาก่อน หรือ - มีโอกาสเกิดขึ้นน้อย
น้อยมาก	1	≤ 1 ปี	- ไม่เคยเกิดขึ้นในองค์กรมาก่อน หรือ - ไม่มีโอกาสเกิดขึ้นน้อยมาก แต่เป็นไปได้ทางทฤษฎี

ตารางที่ 5 แสดงตัวอย่างผลกระทบของความเสี่ยง (Impact) เชิงคุณภาพ

ระดับ	คะแนน	ด้านกระบวนการปฏิบัติงาน (ผลกระทบต่อกระบวนงาน)
สูงมาก	5	ไม่สามารถบรรลุถึงวัตถุประสงค์ของแผนงาน/โครงการ
สูง	4	มีผลกระทบต่อกระบวนการอย่างรุนแรง/กระทบต่อแผนงาน
ปานกลาง	3	มีผลกระทบต่อกระบวนการปานกลาง
น้อย	2	มีผลกระทบต่อกระบวนการเล็กน้อย
น้อยมาก	1	ไม่มีการชะงักงันของกระบวนการและการดำเนินงานทางธุรกิจ

ตารางที่ 6 แสดงตัวอย่างผลกระทบของความเสี่ยง (Impact) เชิงปริมาณ

ระดับ	คะแนน	ด้านการเงิน (มูลค่าความเสียหาย)	ด้านเวลา (ล่าช้า)
สูงมาก	5	> 500,000 บาท	> 6 เดือน
สูง	4	> 100,000 - 500,000 บาท	> 4 - 6 เดือน
ปานกลาง	3	> 10,000 - 100,000 บาท	> 3 - 4 เดือน
น้อย	2	> 1,000 - 10,000 บาท	> 1 - 3 เดือน
น้อยมาก	1	≤ 1,000 บาท	≤ 1 เดือน

ระดับความเสี่ยง (Degree of Risks) แสดงถึงระดับความสำคัญในการบริหารความเสี่ยง โดยพิจารณาจากผลคูณของระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) กับระดับความรุนแรงของผลกระทบ (Impact) ของความเสี่ยงแต่ละสาเหตุ (โอกาส X ผลกระทบ) ซึ่งระดับความเสี่ยงแบ่งตามความสำคัญเป็น 4 ระดับ (ตารางที่ 7 ภาพที่ 31) ดังนี้

ตารางที่ 7 แสดงตัวอย่างการกำหนดระดับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	ความหมาย
สูงมาก	20-25	ความเสี่ยงที่ต้องกำกับดูแลอย่างใกล้ชิด ซึ่งจะต้องบริหารความเสี่ยงทันที
สูง	10-19	ความเสี่ยงที่ต้องกำกับดูแลอย่างใกล้ชิด ซึ่งจะต้องบริหารความเสี่ยงทันที
ปานกลาง	4-9	ความเสี่ยงที่ต้องเฝ้าระวังซึ่งจะต้องบริหารความเสี่ยงโดยให้ความสนใจเฝ้าระวัง
ต่ำ	1-3	ความเสี่ยงที่ใช้วิธีควบคุมปกติไม่ต้องมีการจัดการเพิ่มเติม

ภาพที่ 32 ตัวอย่างแผนภูมิระดับความเสี่ยง

2) การประเมินโอกาสและผลกระทบของความเสี่ยง

เป็นขั้นตอนการประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Materiality) เพื่อกำหนดระดับความเสี่ยง (Degree of Risks) ของความเสี่ยงแต่ละเหตุการณ์ตามเกณฑ์มาตรฐานที่กำหนด ผู้บริหารควรให้ความสำคัญต่อความเสี่ยงที่มีผลกระทบสูง และมีโอกาสเกิดความเสี่ยงสูง เพื่อจัดการความเสี่ยงดังกล่าวก่อน โดยแสดงระดับความเสี่ยง (Degree of Risks) การคำนวณให้ระดับความเสี่ยงตามผลคูณของระดับคะแนนทั้ง 2 ด้าน ตัวอย่าง (ตารางที่ 8)

ตารางที่ 8 ตัวอย่างการประเมินโอกาสและผลกระทบของความเสี่ยง

ความเสี่ยง	ผลกระทบ	โอกาส	ระดับ
ความเสี่ยง A	1	3	1 x 3 = 3
ความเสี่ยง B	3	3	3 x 3 = 9
ความเสี่ยง C	4	4	4 x 4 = 16
ความเสี่ยง D	5	4	5 x 4 = 20

3) การวิเคราะห์ความเสี่ยง

หลังจากที่มีการประเมินโอกาสและผลกระทบของความเสี่ยงแล้ว ขั้นตอนต่อไปของการดำเนินการคือการวิเคราะห์ความเสี่ยง เพื่อทำให้ทราบว่าความเสี่ยงใดเป็นความเสี่ยงสูงสุดที่ควรเร่งบริหารจัดการความเสี่ยงนั้นก่อนเป็นลำดับแรก โดยทั่วไปในการบริหารความเสี่ยงของหน่วยงานและขององค์กร ควรเลือกงานที่มีความเสี่ยงสูงสุด 3-5 ลำดับแรกมาดำเนินการก่อน แล้วจึงค่อยพิจารณาดำเนินการกับงานที่มีความเสี่ยงในลำดับรองลงไป

ตารางที่ 9 แสดงตัวอย่างการคำนวณให้ระดับความเสี่ยง

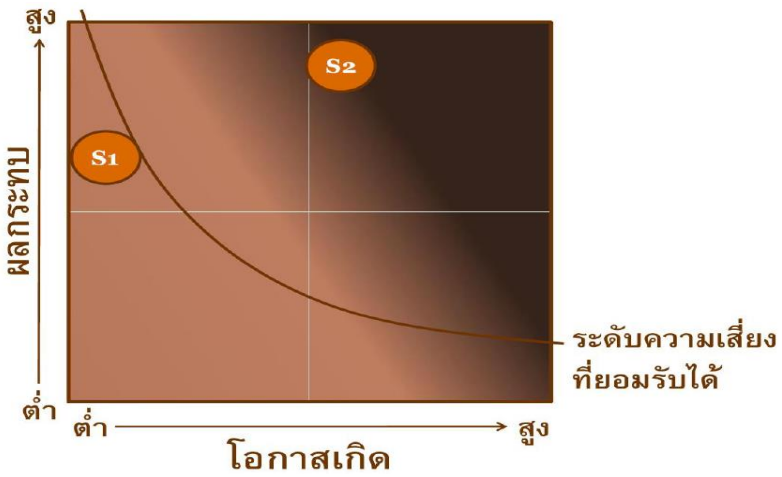
ระดับความเสี่ยง	ระดับคะแนน	ความหมาย
สูงมาก	20-25	ความเสี่ยงที่ต้องกำกับดูแลอย่างใกล้ชิด ซึ่งจะต้องบริหารความเสี่ยงทันที *(ตัวอย่าง ความเสี่ยง D ระดับคะแนนความเสี่ยงเท่ากับ 20)*
สูง	10-19	ความเสี่ยงที่ต้องกำกับดูแลอย่างใกล้ชิด ซึ่งจะต้องบริหารความเสี่ยงทันที *(ตัวอย่าง ความเสี่ยง C ระดับคะแนนความเสี่ยงเท่ากับ 16)*
ปานกลาง	4-9	ความเสี่ยงที่ต้องเฝ้าระวังซึ่งจะต้องบริหารความเสี่ยงโดยให้ความสนใจเฝ้าระวัง *(ตัวอย่าง ความเสี่ยง B ระดับคะแนนความเสี่ยงเท่ากับ 9)*
ต่ำ	1-3	ความเสี่ยงที่ใช้วิธีควบคุมปกติไม่ต้องมีการจัดการเพิ่มเติม *(ตัวอย่าง ความเสี่ยง A ระดับคะแนนความเสี่ยงเท่ากับ 3)*

4) การจัดลาดับความเสี่ยง

ภายหลังจากการวิเคราะห์ความเสี่ยงแล้ว ขั้นตอนไปของการประเมินความเสี่ยงคือ การจัดลำดับความเสี่ยง เพื่อให้หน่วยงานสามารถจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงาน และสามารถนามาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดยพิจารณาจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยง

ตารางที่ 10 แสดงตัวอย่างการจัดลำดับความเสี่ยง

		โอกาสหรือความเป็นไปได้ที่เกิดขึ้น (Likelihood)				
		1 (ต่ำมาก)	2	3	4	5 (สูงมาก)
ผลกระทบของความเสี่ยง (Impact)	5 (สูงมาก)					
	4				ความเสี่ยง C	ความเสี่ยง D
	3	ความเสี่ยง A		ความเสี่ยง B		
	2					
	1 (ต่ำมาก)					

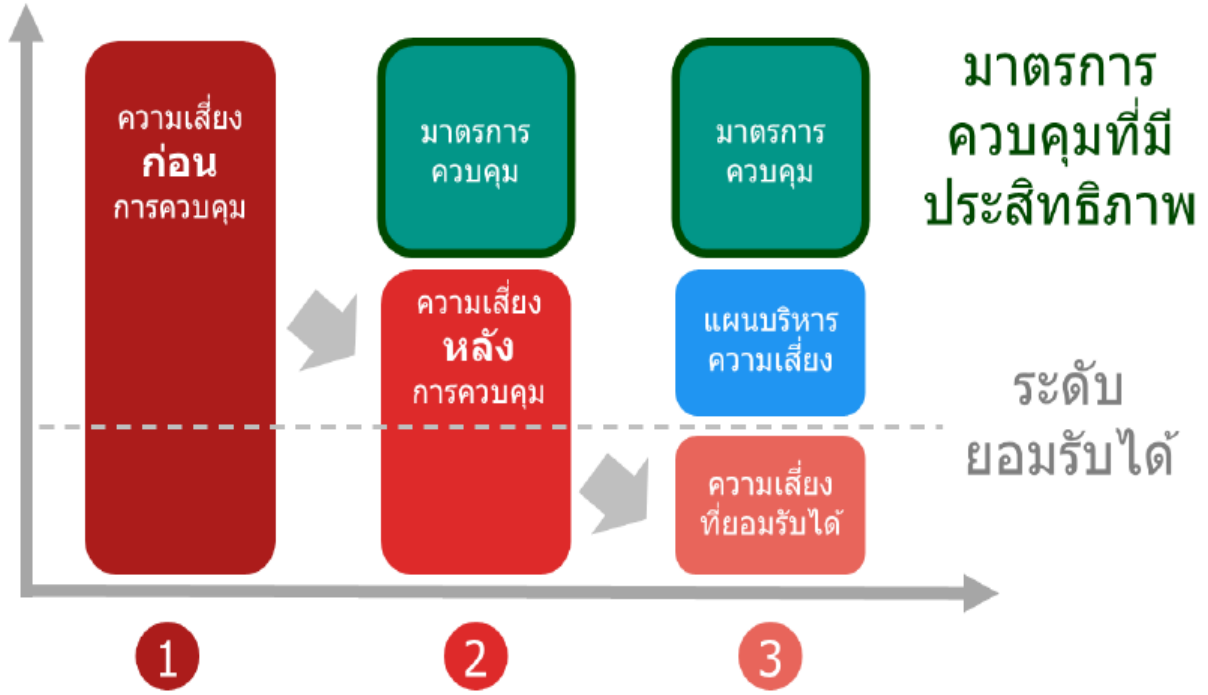


ภาพที่ 33 การจัดลำดับความเสี่ยง

ที่มา : คู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน, กระทรวงการคลัง (2555: 133)

4. การประเมินมาตรการควบคุมภายใน

การประเมินมาตรการควบคุมภายใน (Risk Control) เป็นขั้นตอนในกระบวนการบริหารความเสี่ยง ซึ่งควรดำเนินการหลังจากที่องค์กร หรือหน่วยงานได้มีการประเมินโอกาสและผลกระทบของความเสี่ยง รวมถึงการจัดลำดับความเสี่ยงเรียบร้อยแล้ว ทั้งนี้เพื่อเป็นเครื่องมือในการช่วยควบคุมความเสี่ยงหรือปัจจัยเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กรหรือหน่วยงาน ซึ่งจะทำให้องค์กรหรือหน่วยงานสามารถดำเนินการได้บรรลุวัตถุประสงค์ได้ตามที่วางไว้ การกำหนดมาตรการควบคุมความเสี่ยงของแต่ละองค์กรจะมีมาตรฐานที่แตกต่างกันไปขึ้นกับดุลยพินิจและประสบการณ์ของผู้บริหารงบประมาณด้านการบริหารความเสี่ยง รวมถึงระดับความเสี่ยงที่ยอมรับได้ของแต่ละองค์กรโดยแสดง ระดับความเสี่ยงที่ยอมรับได้ (Acceptable Risk) ตามแผนผังทฤษฎีความเสี่ยง ดังภาพด้านล่างนี้



ภาพที่ 34 แผนผังทฤษฎีความเสี่ยงแสดงระดับความเสี่ยงที่ยอมรับได้

มาตรการควบคุมความเสี่ยง

มาตรการควบคุมความเสี่ยง แบ่งออกเป็น 4 มาตรการ ดังนี้

1. การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นมาตรการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาด เช่น การกำหนดนโยบาย การจัดโครงสร้างองค์กรการแบ่งแยกหน้าที่งานเพื่อป้องกันการทุจริต การควบคุมการเข้าถึงเอกสาร ข้อมูลทรัพย์สิน การกำหนดรหัสผ่าน (Password) ให้กับผู้สิทธิ์เข้าถึงระบบสารสนเทศ เป็นต้น

2. การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นมาตรการควบคุมที่กำหนดขึ้น เพื่อค้นพบข้อผิดพลาดในการทำงาน เช่น การสอบทาน การวิเคราะห์ การยืนยันยอด การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

3. การควบคุมโดยการชี้แนะ (Directive Control) เป็นมาตรการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดผลสำเร็จของงานตามวัตถุประสงค์ที่วางไว้เช่น การสร้างแรงจูงใจในการทำงาน การบริหารงานอย่างเอาใจใส่ของผู้บังคับบัญชา เป็นต้น

4. การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นมาตรการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้น หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำในอนาคต เช่น การสำรองข้อมูลสำคัญขององค์กรในที่ปลอดภัย การซ้อมหนีไฟ กรณีเกิดเพลิงไหม้ในอาคาร การเขียนเงื่อนไขในสัญญาให้มีการชดใช้หากมีการประกันภัยเป็นต้น

ความเสี่ยงคงเหลือ

ความเสี่ยงคงเหลือ (Residual Risk) เป็นจุดเริ่มต้นของการกำหนดความเสี่ยงในระดับที่ยอมรับได้สำหรับองค์กร ในการเผชิญกับความเสี่ยงจากการดำเนินกิจกรรมหรือธุรกิจ (Inherent Risk) ให้ทราบระหว่างระดับความเสี่ยงนั้นสูงกว่าระดับการควบคุม (Control Score) ในสถานการณ์เช่นนี้ บ่งชี้ให้เห็นว่าความเสี่ยงคงเหลือ (Residual Risk) นั้นมีค่าสูงกว่า โดยพิจารณาจากสมการต่อไปนี้

ความเสี่ยงคงเหลือ = ความเสี่ยงจากการดำเนินกิจกรรมหรือธุรกิจ – มาตรการควบคุม

การลดระดับความเสี่ยงคงเหลือ (Residual Risk) สามารถกระทำได้โดยการเพิ่มระดับมาตรการควบคุมที่มีประสิทธิผลมากยิ่งขึ้น หรือการหลีกเลี่ยงการดำเนินกิจกรรมหรือธุรกิจที่ทำให้เกิดความเสี่ยงความเสี่ยงนั้นๆ จากสมการข้างต้น องค์กรสามารถกำหนดระดับความเสี่ยง (Risk Score) และระดับการควบคุม (Control Score) ได้อย่างเหมาะสม

แนวทางประเมินมาตรการควบคุมความเสี่ยง (ตารางที่ 11) ดังนี้

1. นำความเสี่ยงระดับสูงสุดและสูง (จากตารางที่ 9) มากำหนดมาตรการควบคุมความเสี่ยงเพื่อป้องกันหรือลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

2. ประเมินว่าปัจจุบันมีการควบคุมความเสี่ยงเหล่านั้นอยู่หรือไม่

3. กรณีที่มีการควบคุมอยู่แล้ว ให้ประเมินว่าการควบคุมที่มีในปัจจุบันเพียงพอหรือไม่

ตารางที่ 11 แสดงตัวอย่างการประเมินมาตรการควบคุมภายใน

ปัจจัยเสี่ยง (1)	การควบคุมที่ควรจัดทำ (2)	การควบคุมในปัจจุบัน (3)	ผลการประเมินการควบคุมในปัจจุบัน (4)	การควบคุมที่ควรทำเพิ่มเติม (5)
งานนโยบายและแผน				
บุคลากรขาดความรู้และความชำนาญในด้านการตลาดและการจัดทำแผนงานฯ	a) วิเคราะห์และจัดทำ Competency Gap และจัดทำแผนพัฒนาเพื่อปิด Gap	x	x	จัดให้มีการดำเนินการตาม a)
งานตรวจสอบ				
งบประมาณลงทุนไม่เพียงพอต่องานตรวจสอบประจำปี	b) จัดทำแผนสารองกรณีที่ไม่ได้รับอนุมัติงบประมาณตามที่กำหนด	?	?	จัดให้มีการดำเนินการตาม b)
กระบวนการตรวจสอบคุณภาพ (QC) ไม่มีประสิทธิภาพ	C) ทบทวนกระบวนการ QC เพื่อหาจุดอ่อนของการควบคุมและปรับปรุงให้มีประสิทธิภาพอย่างสม่ำเสมอ	√	?	จัดให้มีการดำเนินการตาม C)

หมายเหตุ ความหมายของสัญลักษณ์ในช่อง (3) และ (4)

ช่อง (3) √ : มี x : ไม่มี ? : มีแต่ไม่ได้ปฏิบัติ

ช่อง (4) √ : ได้ผล x : ไม่ได้ผล ? : ได้ผลบ้างแต่ไม่สมบูรณ์

ที่มา : องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย. (2563: 47)

เมื่อมีการประเมินมาตรการควบคุมความเสี่ยงแล้ว หากปัจจัยเสี่ยงที่พิจารณาแล้วว่าสามารถดำเนินการภายใต้การยอมรับของผู้บริหารระดับสูงและภายในงบประมาณที่วางไว้ก็สามารถวางแผนการบริหารจัดการความเสี่ยง เพื่อป้องกันหรือลดความเสี่ยงของงานหรือโครงการต่อไป

การประเมินความเสี่ยง หน่วยงานภาครัฐต้องทำ**การประเมินความเสี่ยงทุจริต** ตามข้อกำหนดหลักเกณฑ์การควบคุมภายในสาหรับหน่วยงานของรัฐ’61 (ว 105) และเกณฑ์การประเมินความโปร่งใสใน การดำเนินงานของหน่วยงานภาครัฐ (ปปช.) ซึ่งได้กล่าวไว้ในหัวข้อการประเมินความเสี่ยงทุจริต (หน้า 65)

5. การจัดการความเสี่ยง

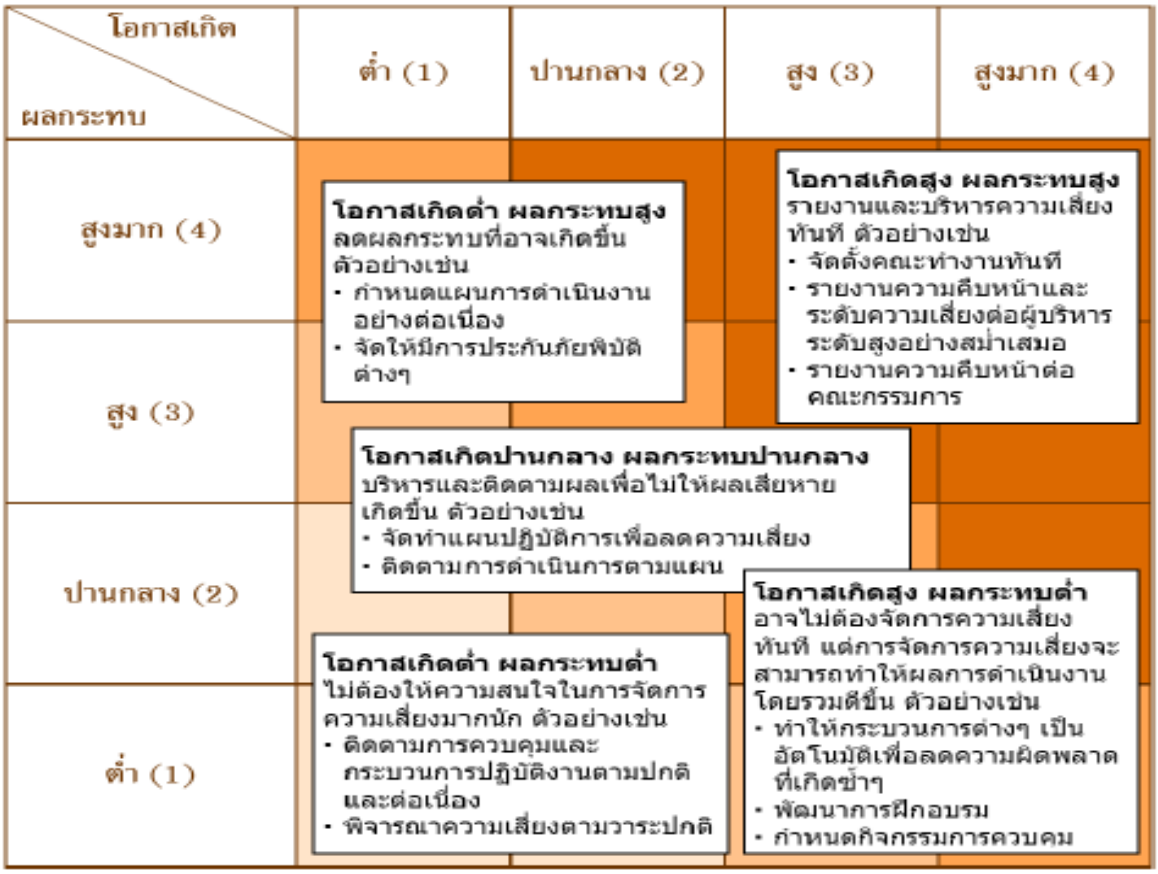
การจัดการความเสี่ยง (Risk Treatment) กลยุทธ์การจัดการความเสี่ยง คือ การดำเนินการเพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้วิธีการจัดการที่สอดคล้องกับระดับความเสี่ยงที่ประเมินไว้และต้นทุนค่าใช้จ่ายที่เกี่ยวข้อง ตามแนวทาง ดังนี้

กลยุทธ์การจัดการความเสี่ยงเพื่อจัดการความเสี่ยง มี 4 กลยุทธ์ ได้แก่ Take Treat Terminate Transfer ซึ่งอาจเรียกว่า **4T’s Strategies**

ภาพที่ 35 กลยุทธ์การจัดการความเสี่ยง 4T's Strategies

ตารางที่ 12 แสดงกลยุทธ์การจัดการความเสี่ยง 4T's Strategies

กลยุทธ์/แนวทาง	ความหมายของกลยุทธ์และการปฏิบัติ
Take risk (การยอมรับความเสี่ยง)	เป็นการยอมรับให้ความเสี่ยงสามารถเกิดขึ้นได้ภายใต้ระดับความเสี่ยงที่สามารถยอมรับได้ โดย*ไม่มีมาตรการหรือกลยุทธ์ใดๆ* ในการควบคุม ซึ่งอาจเนื่องมาจากความเสี่ยงนั้นอยู่ในระดับความเสี่ยงต่ำมาก หรือไม่มีวิธีการใดๆ ในปัจจุบันที่จะควบคุม หรือวิธีการที่จะนำมาใช้มีต้นทุนสูงเมื่อเทียบกับความเสียหายที่อาจเกิดขึ้นจากความเสี่ยงนั้น ไม่คุ้มค่าต่อการดำเนินการ แม้ว่าการยอมรับความเสี่ยงไม่ได้ดำเนินการใดๆ แต่*ต้องติดตาม/เฝ้าระวัง*ความเสี่ยงไม่ให้มีการเพิ่มระดับสูงขึ้น • ตัวอย่าง การตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้ เช่น การติดตามความเสี่ยงและการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ
Treat risk (การควบคุมความเสี่ยง)	เป็นการดำเนินการเพิ่มเติม เพื่อควบคุมโอกาสที่อาจเกิดขึ้นหรือขนาดของผลกระทบจากความเสี่ยงให้อยู่ในระดับที่กำหนด ซึ่งเป็นระดับที่สามารถยอมรับได้ เช่น *การจัดซื้ออุปกรณ์เพื่อป้องกันอันตรายจากการทำงาน* หรือ*การจัดหาอุปกรณ์เพิ่มเติมจากเดิม การปรับปรุงแก้ไขกระบวนงาน การจัดทำแผนฉุกเฉิน* และ*การจัดทำมาตรฐานความปลอดภัย* เป็นต้น • ตัวอย่าง การตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้ เช่น การปรับปรุงและพัฒนานโยบายและกระบวนการ การลงทุนในระบบสารสนเทศ/software/อุปกรณ์ การแก้ไขกระบวนการทางธุรกิจใหม่
Terminate risk (การหลีกเลี่ยง/กำจัดความเสี่ยง)	ใช้ในกรณีที่*ไม่สามารถยอมรับ*ความเสี่ยงได้ อาจใช้วิธีการเปลี่ยนวัตถุประสงค์ *การหยุดดำเนินกิจการ/ระงับ/ยกเลิก* หรือการไม่ดำเนินการกิจกรรมนั้นๆ เลย เช่น การลงทุนในโครงการขนาดใหญ่ มีงบประมาณโครงการสูงอาจมีการประเมิน ความเสี่ยงก่อนเริ่มโครงการ ซึ่งหากมีความเสี่ยงสูงต่อการเกิดปัญหาตามมา ทั้งด้านการเงินและด้านอื่นๆ ก็จะ*ไม่ดำเนินการ* เป็นต้น • ตัวอย่าง การตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้ เช่น การหยุดและเลิกการดำเนินกิจการ การปรับปรุงวัตถุประสงค์เริ่มแรกของธุรกิจ หรือแผนกลยุทธ์
Transfer risk (การถ่ายโอนความเสี่ยง)	เป็นวิธีการร่วมหรือแบ่งความรับผิดชอบให้กับผู้อื่นในการจัดการความเสี่ยง เช่น *การทำประกันภัย* หรือ *การจ้างผู้ความชำนาญดำเนินการแทน (Outsource)* หรือ *การร่วมทุน/หุ้นส่วน* เป็นต้น • ตัวอย่าง การตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้ เช่น การทำประกันภัยโรงงาน การทำ Hedging การร่วมทุนกับบริษัทอื่น



ภาพที่ 36 แนวทางตอบสนอง/จัดการความเสี่ยง

ที่มา : คู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน, กระทรวงการคลัง (2555: 67)

การจัดทำแผนบริหารความเสี่ยงองค์กร

แผนบริหารความเสี่ยงองค์กร เป็นการรวบรวมข้อมูลวิธีการและกิจกรรมการจัดการความเสี่ยงต่างๆ มาพิจารณาในภาพรวม เพื่อให้การบริหารความเสี่ยงองค์การมีประสิทธิภาพสูงขึ้น มีความมั่นใจต่อการบรรลุเป้าหมายตามแผนบริหารความเสี่ยง โดยแผนบริหารความเสี่ยงมีองค์ประกอบในลักษณะเดียวกับแผนปฏิบัติการ (Action plan) คือ มาตรการ/กิจกรรมการจัดการความเสี่ยง กำหนดระยะเวลาดำเนินการของกิจกรรม และผู้รับผิดชอบ

เมื่อดำเนินการจัดทำแผนบริหารความเสี่ยงองค์การเรียบร้อยแล้ว ต้องมีการสื่อสารให้บุคลากรทั้งหมดทราบ เพื่อให้เกิดความเข้าใจที่สอดคล้องกันในหลักการของการบริหารความเสี่ยงองค์การ รวมทั้งสนับสนุนร่วมดำเนินการกิจกรรมต่างๆ ที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ บรรลุผลสำเร็จตามที่ต้องการ

องค์กรมีการดำเนินงานทั้งด้านการบริหารความเสี่ยงและการควบคุมภายใน ซึ่งมีวัตถุประสงค์/เป้าหมายร่วมกันคือ ควบคุมและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยการควบคุมภายในเป็นกระบวนการและมาตรการต่างๆ ที่มีประสิทธิภาพและก่อให้เกิดประสิทธิผลที่องค์การได้กำหนดขึ้น เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลในด้านการดำเนินงาน การรายงานและการปฏิบัติตามกฎระเบียบ ส่วนการบริหารความเสี่ยงเป็นกระบวนการที่ได้รับการออกแบบให้สามารถบ่งชี้เหตุการณ์ที่อาจจะเกิดขึ้นและมีผลกระทบต่อองค์การ เพื่อสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์การยอมรับได้

เมื่อบริหารความเสี่ยงให้ลดลงอยู่ในระดับที่องค์การยอมรับได้แล้วความเสี่ยงนั้นจะถูกส่งต่อไปยังกระบวนการควบคุมภายใน ในทางกลับกันความเสี่ยงที่ไม่สามารถควบคุมได้ด้วยกระบวนการควบคุมภายในความเสี่ยงนั้นจะถูกส่งต่อไปสู่กระบวนการบริหารความเสี่ยง

การระบุทางเลือกในการจัดการความเสี่ยง

การจัดการความเสี่ยงในแต่ละวิธีอาจเหมาะสมกับสถานการณ์บางสถานการณ์เท่านั้น และการจัดการกับความเสี่ยงหนึ่งๆ อาจมีแนวทางได้มากกว่า 1 แนวทาง วิธีจัดการความเสี่ยงสามารถแบ่งออกได้เป็น 2 แนวทางหลัก ได้แก่

1) การลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย (Reduce Likelihood)
2) การลดขนาดผลกระทบความเสี่ยหาย (Reduce Impact)

ก่อนที่จะดำเนินการระบุทางเลือกในการจัดการความเสี่ยง หน่วยงานควรทราบวัตถุประสงค์ว่าต้องการควบคุมความเสี่ยงไปในทิศทางใด/ลักษณะใด โดยดูจากแผนภาพแสดงระดับความรุนแรงของความเสี่ยง (Risk Matrix) ประกอบเช่น ความเสี่ยงที่มีโอกาสที่จะเกิดเหตุการณ์ความเสียหายสูง แต่มีระดับความเสียหายต่ำ (อยู่ด้านล่าง-ด้านขวาของ Matrix) ก็ควรคัดเลือกแนวทางควบคุมที่มุ่งเน้นการลดโอกาสเป็นต้น

1. การลดโอกาสที่จะเกิดความเสียหาย (Reduce Likelihood)

เป็นมาตรการควบคุมความเสี่ยง (Risk Control) ที่จัดการปัจจัยที่ก่อให้เกิดความเสียหาย โดยตรงโดยมุ่งลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย เหมาะกับลักษณะงานที่ต้องปฏิบัติบ่อยครั้งหรือปฏิบัติเป็นประจำ เช่น

- การใช้ระบบงานอัตโนมัติ (Automation) ทดแทนกระบวนการที่ใช้คน (Manual) เป็นผู้กระทำ ซึ่งจะเหมาะสมกับลักษณะงานที่ต้องปฏิบัติซ้ำๆ จำนวนมาก (Routine work)
- การปรับปรุงกระบวนการทำงาน เพื่อลดความซับซ้อน (Complexity) ในการทำงาน
- การมีระบบตรวจจับ (Detection) และป้องกัน (Prevention) การกระทำทุจริต
- การกำหนดให้มี Checklist เพื่อตรวจสอบความถูกต้องครบถ้วนในการทำงาน

2. การลดขนาดของความเสียหาย (Reduce Impact)

เป็นมาตรการจัดการความเสี่ยงโดยมุ่งลดขนาดความเสียหายที่เกิดขึ้นแล้ว เหมาะกับความเสี่ยงที่เกิดจากปัจจัยภายนอกที่ควบคุมได้ยาก หน่วยงานผู้ประเมินอาจจะใช้วิธีการกระจายความเสี่ยงหรือไม่ให้เกิดการกระจุกตัวของความเสี่ยง (Diversification) เช่น การจำกัดขนาดของธุรกรรมหรือปริมาณธุรกรรมโดยรวมไว้ในระดับต่ำ แต่หากความเสี่ยงอยู่นอกเหนือความสามารถที่จะควบคุมหรือไม่สามารถลดการกระจุกตัวได้อาจจะเลือกการจัดการความเสี่ยงโดยการจัดทำแผนดำเนินการ/แผนฉุกเฉิน เพื่อรองรับความเสียหาย และลดผลกระทบจากเหตุการณ์ดังกล่าว เช่น

- จัดทำ Contingency Plan หรือ Business Continuity Plan เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่องในช่วงเกิดเหตุการณ์ความเสียหาย และอยู่ระหว่างการแก้ไขเพื่อให้กลับสู่สภาพการดำเนินงานตามปกติได้เร็วที่สุด

● จัดทำแผนจัดการกับวิกฤตทางธุรกิจ เมื่อเกิดเหตุการณ์ความเสียหาย (Effective Crisis Management Plan) เป็นวิธีการที่เหมาะกับการจัดการปัญหา หรือการหยุดชะงักทางธุรกิจอันเกิดจากเหตุการณ์ที่ไม่ได้คาดคิด ซึ่งส่งผลกระทบต่อชื่อเสียง/ภาพพจน์ขององค์กรอย่างรุนแรงและอาจไม่สามารถควบคุมได้

หากหน่วยงานดำเนินการควบคุมความเสี่ยงตามวิธีการข้างต้นแล้ว พบว่า ความเสี่ยงยังคงเหลืออยู่ อาจพิจารณาจัดการความเสี่ยงดังกล่าว โดยการถ่ายโอนความเสี่ยง (Transfer) บางส่วน/ทั้งหมดให้องค์กรภายนอกที่สามารถจัดการความเสี่ยงข้างต้นได้ดีกว่า หรือหลีกเลี่ยงความเสี่ยง (Terminate/Avoid) หรือยอมรับความเสี่ยง (Take/Accept/Retain) โดยขึ้นอยู่กับว่าความเสี่ยงที่เหลืออยู่นั้นมีระดับโอกาสและระดับความเสียหายเป็นอย่างไร ทั้งนี้การเลือกวิธีจัดการความเสี่ยงให้พิจารณาเปรียบเทียบค่าใช้จ่ายกับผลประโยชน์ที่จะได้รับ (Cost-Benefit Analysis)

3. การถ่ายโอนความเสี่ยง (Risk Transfer)

เป็นการถ่ายโอนความรับผิดชอบหรือภาระของการสูญเสียให้กับบุคคลอื่น เช่น การทำประกันภัยการทำสัญญาป้องกันความเสี่ยง การจ้างบุคคลภายนอกดำเนินการแทนเป็นต้น แต่ในขณะเดียวกันก็ก่อให้เกิดความเสี่ยงจากคู่สัญญาไม่สามารถปฏิบัติตามภาระผูกพัน (Counterparty Risk) ซึ่งเป็นสิ่งที่หน่วยงานควรคำนึงในการคัดเลือกวิธีการจัดการกับความเสี่ยง

4. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)

เป็นการตัดสินใจที่จะไม่เข้าไปเกี่ยวข้องกับสถานการณ์ความเสี่ยงนั้นหรือยุติการดำเนินกิจกรรมที่ก่อให้เกิดความเสี่ยง

5. การยอมรับ/ดำรงความเสี่ยง (Risk Acceptance)

สำหรับกิจกรรมที่ไม่สามารถถ่ายโอนความเสี่ยง หรือยกเลิกกิจกรรมนั้น หน่วยงานจาเป็นต้องยอมรับความเสี่ยงที่อาจเกิดขึ้น แต่ควรพิจารณามาตรการป้องกันความเสี่ยงเพิ่มเติม เช่น การจัดสรรเงินทุนสำรองที่เหมาะสมเพื่อรองรับความเสียหายที่อาจเกิดขึ้นจากความเสี่ยงที่คงเหลืออยู่ภายหลังการจัดการความเสี่ยงตามวิธีดังกล่าวข้างต้นแล้ว เมื่อหน่วยงานทำการประเมินมาตรการควบคุมความเสี่ยง และทราบความเสี่ยงที่ยังเหลืออยู่ รวมถึงทราบกลยุทธ์และทางเลือกในการจัดการความเสี่ยงที่ระบุข้างต้นแล้วนั้น ควรพิจารณาความเป็นไปได้และค่าใช้จ่ายของแต่ละทางเลือกเพื่อการตัดสินใจเลือกมาตรการจัดการความเสี่ยงและดำเนินการอย่างเป็นระบบ ดังนี้

1. พิจารณาว่าจะยอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

2. เปรียบเทียบความคุ้มค่าของต้นทุนในการจัดการความเสี่ยง (Cost) กับผลประโยชน์ (Benefit) ที่จะได้รับจากมาตรการดังกล่าว

3. พิจารณาติดตามผลการบริหารความเสี่ยงในงวดปีก่อนที่ยังไม่ได้ดำเนินการหรืออยู่ระหว่างดำเนินการเพื่อนามาบริหารความเสี่ยงตามกระบวนการดังกล่าวข้างต้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติการควรนามาระบุการควบคุมในแผนบริหารความเสี่ยง

4. กำหนดวิธีการควบคุมความเสี่ยงในแผนบริหารความเสี่ยงอย่างเป็นลายลักษณ์อักษรและควรจัดให้มีการสื่อสารและประชาสัมพันธ์ให้พนักงาน รับทราบและปฏิบัติตามแผนการจัดการความเสี่ยงอย่างทั่วถึงทั้งองค์กร

ตารางที่ 13 แสดงตัวอย่างวิธีการจัดการความเสี่ยง

วิธีการจัดการความเสี่ยง	ตัวอย่างการดำเนินการ
• การลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย (Reduce Likelihood)	เป็นการดำเนินการเพื่อลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย เช่น - จัดให้มีการสอบทานข้อกำหนด และวิธีปฏิบัติ - กำหนดให้มีขั้นตอนการควบคุม และการตรวจสอบ - การจัดตั้งทีมบริหารโครงการ - จัดให้มีแผนกำหนดการบำรุงรักษา - กำหนดมาตรฐานการจัดการ และการรับประกันคุณภาพ - จัดให้มีการพัฒนาและวิจัยด้านเทคโนโลยี - จัดให้มีการฝึกอบรม - การปรับปรุงกระบวนการทำงาน
• การลดผลกระทบ (Reduce Impact)	เป็นการจัดการเพื่อลดผลกระทบหากเกิดเหตุการณ์ความเสี่ยง เช่น - จัดทำ Contingency Plan หรือ Business Continuity Plan - จัดทำแผนจัดการวิกฤต Crisis Management - การกระจายการกระจุกตัว (Diversification)
• การถ่ายโอนความเสี่ยง (Risk Transfer)	เป็นการถ่ายโอนความเสี่ยงให้องค์กรอื่น ได้แก่ การทำสัญญา การทำประกัน การจ้างบุคคลภายนอกดำเนินการแทน เป็นต้น
• การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)	เป็นการหลีกเลี่ยงหรือยุติการดำเนินกิจกรรมที่ก่อให้เกิดความเสี่ยงที่มีระดับความรุนแรงที่ไม่อาจยอมรับได้ (Unacceptable Risk) ซึ่งการดำเนินการดังกล่าวสามารถทำได้ในทางปฏิบัติ
• การยอมรับ/ด้ารงความเสี่ยง (Risk Acceptance)	เป็นแผนดำเนินการจัดสรรเงินทุนที่เหมาะสม เพื่อรองรับความเสียหายที่อาจเกิดขึ้นจากความเสี่ยงที่คงเหลืออยู่ภายหลังการจัดการความเสี่ยงตามวิธีข้างต้นแล้ว หรือเป็นความเสี่ยงที่มีต้นทุนที่ใช้ในการจัดการไม่คุ้มกับผลประโยชน์ที่จะได้รับ หรือเป็นความเสี่ยงที่สำนัก/ส่วนงาน/องค์กรไม่สามารถยุติ/หลีกเลี่ยงความเสี่ยงดังกล่าวได้

ตารางที่ 14 แสดงตัวอย่างการวิเคราะห์ทางเลือกในการจัดการความเสี่ยง

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	การจัดการความเสี่ยง	ต้นทุน	ผลประโยชน์	ทางเลือกเพื่อจัดการความเสี่ยง
งานนโยบายและแผน					
• บุคลากรขาดความรู้และความชำนาญในด้านการตลาดและการจัดทำแผนงานฯ	หลีกเลี่ยง	• ไม่สามารถหลีกเลี่ยงได้เนื่องจากส่งผลกระทบต่อการจัดทำแผนงานฯ อย่างมาก	-	-	วิธีการถ่ายโอน (เนื่องจากบุคลากรไม่มีทักษะและความชำนาญในการจัดทำ Competency Gap ซึ่งถ้าดำเนินการเองมีโอกาสดำเนินการอย่างไม่ถูกต้อง)
	ยอมรับ	• ไม่สามารถหลีกเลี่ยงได้เนื่องจากส่งผลกระทบต่อการจัดทำแผนงานฯ อย่างมาก	-	-	
	ควบคุม	• ปรับกระบวนการดำเนินงานในการกำหนด วิเคราะห์และจัดทำ Competency Gap และจัดทำแผนพัฒนาเพื่อปิด Gap ที่มีความสมบูรณ์	ไม่เสียค่าใช้จ่าย ซึ่งจัดทำเพียงการปรับกระบวนการดำเนินการให้เหมาะสม	ผู้จัดทำแผนงานฯ มีความรู้ความสามารถในการจัดทำแผนงานฯ และได้แผนงานฯ ซึ่งมีเนื้อหาครอบคลุมตามวัตถุประสงค์	
	ถ่ายโอน	• จ้างบริษัท Outsource เป็นผู้ดำเนินการ	เสียค่าใช้จ่ายเพิ่มขึ้นในการจ้างบริษัท Outsource	บริษัทมีความชำนาญในการทำงาน และมีวิธีการที่จะสามารถดำเนินการได้อย่างครบถ้วน	
งานตรวจสอบ					
• งบประมาณลงทุนไม่เพียงพอต่องานตรวจสอบประจำปี	หลีกเลี่ยง	• ไม่สามารถหลีกเลี่ยงได้เนื่องจากส่งผลกระทบต่อการจัดทำแผนงานฯ อย่างมาก	-	-	วิธีการควบคุม
	ยอมรับ	• ไม่สามารถหลีกเลี่ยงได้เนื่องจากส่งผลกระทบต่อการจัดทำแผนงานฯ อย่างมาก	-	-	
	ควบคุม	• จัดทำแผนสำรองกรณีที่ไม่ได้รับอนุมัติงบประมาณตามที่กำหนด	ไม่เสียค่าใช้จ่าย เนื่องจากบุคลากรภายในมีความรู้ความสามารถในการจัดทำแผนสำรองฯ ได้	สามารถจัดทำแผนสำรองฯ เพื่อให้การผลิตผลิตภัณฑ์เป็นไปตามเป้าหมายและมาตรฐานที่กำหนดไว้	
	ถ่ายโอน	• ไม่เลือกเนื่องจากไม่มีงบประมาณในการดำเนินการ			

6. การรายงานและติดตามความเสี่ยง

การรายงานและติดตามความเสี่ยง (Risk Reporting & Monitoring) เมื่อมีการดำเนินงานตามแผนบริหารความเสี่ยงแล้ว จะต้องมีการติดตามผลและการรายงานอย่างต่อเนื่อง เพื่อให้เกิดความมั่นใจว่าได้มีการดำเนินงานไปอย่างถูกต้องและเหมาะสม โดยมีเป้าหมายในการติดตามผล คือ เป็นการประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการดำเนินการไปแล้วว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่ โดยต้องมีการสอบทานดูว่าวิธีการจัดการความเสี่ยงใดที่มีประสิทธิภาพ ควรดำเนินการต่อเนื่อง และวิธีการจัดการความเสี่ยงใดควรปรับเปลี่ยน และนำผลการติดตามดังกล่าว มาจัดทำรายงาน

การรายงานความเสี่ยงเป็นขั้นตอนสำคัญในกระบวนการบริหารความเสี่ยง เพื่อเป็นหลักฐานในการแสดงการวิเคราะห์ ประเมิน และจัดการความเสี่ยงขององค์กร ทั้งนี้เพื่อให้มีการพิจารณาว่ามีความเสี่ยงที่ยังคงเหลืออยู่หรือไม่ และความเสี่ยงดังกล่าวมีระดับความเสี่ยงและมีระดับความรุนแรงที่จะส่งผลต่อการบรรลุวัตถุประสงค์ขององค์กรมากน้อยเพียงใด ในการจัดทำรายงานความเสี่ยงนั้นกำหนดให้มีการนาเสนอต่อผู้บริหารระดับสูงขององค์กรในการพิจารณาอนุมัติดำเนินการ และสั่งการเพื่อจัดการความเสี่ยงนั้น

วัตถุประสงค์การรายงานและติดตามความเสี่ยง

1) เพื่อให้ผู้บริหาร และผู้ที่เกี่ยวข้องได้รับทราบ และตระหนักถึงความเสี่ยงขององค์กร/หน่วยงาน ที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร และพิจารณาแก้ไขได้อย่างทันท่วงที

2) เพื่อให้มั่นใจว่า ความเสี่ยงได้รับการจัดการตามแผนงานที่วางไว้

3) เพื่อประเมินว่าแผนการจัดการความเสี่ยงยังสามารถใช้ดำเนินการในสถานการณ์ปัจจุบัน

การจัดทำรายงานการบริหารความเสี่ยง

การจัดทำรายงานการบริหารความเสี่ยง ควรมีการกาหนดกระบวนการและผู้รับผิดชอบในการจัดทำรายงานการบริหารความเสี่ยง ในแต่ละระดับ ดังนี้

1) ผู้ประสานงานความเสี่ยงประจำฝ่าย/สำนัก

มีบทบาทหน้าที่ในการจัดทำรายงานผลการปฏิบัติงานตามนโยบายบริหารความเสี่ยงในระดับฝ่าย/สำนัก ที่ตนรับผิดชอบเสนอต่อแผนกบริหารความเสี่ยงและควบคุมภายในฝ่ายนโยบายและแผนงาน เป็นประจำทุกไตรมาส

2) แผนกบริหารความเสี่ยงและควบคุมภายใน ฝ่ายนโยบายและแผนงาน

มีบทบาทหน้าที่ความรับผิดชอบหลักในการจัดทำรายงานผลการปฏิบัติงานตามนโยบายบริหารความเสี่ยงเสนอต่อผู้อำนวยการหน่วยงานเป็นประจำทุกไตรมาส

3) ผู้อำนวยการหน่วยงาน

มีบทบาทหน้าที่ความรับผิดชอบหลักในการพิจารณากลั่นกรองรายละเอียดของรายงานผลการปฏิบัติงานตามนโยบายบริหารความเสี่ยงและให้ความเห็นชอบก่อนนำเสนอคณะอนุกรรมการบริหารความเสี่ยง เป็นประจำทุกไตรมาส

4) คณะอนุกรรมการบริหารความเสี่ยง

มีบทบาทหน้าที่ความรับผิดชอบหลักในการควบคุมติดตาม ตรวจสอบ และดูแลให้ทุกหน่วยงานดำเนินการตามนโยบายบริหารความเสี่ยงที่กำหนด โดยพิจารณาผลการปฏิบัติงานตามนโยบายการบริหารความเสี่ยง เพื่อให้มั่นใจได้ว่านโยบายการบริหารความเสี่ยง ได้นำไปปฏิบัติอย่างเหมาะสมนำเสนอผ่านคณะอนุกรรมการบริหารความเสี่ยงหน่วยงาน เป็นประจำทุกไตรมาส

5) คณะกรรมการตรวจสอบ

มีบทบาทหน้าที่ความรับผิดชอบในการรับทราบรายงานผลการปฏิบัติงานตามนโยบายการบริหารความเสี่ยงจากรายงานฯ ของคณะอนุกรรมการบริหารความเสี่ยง เป็นประจำทุกไตรมาส

6) คณะกรรมการ

มีบทบาทหน้าที่ความรับผิดชอบในการรับทราบรายงานผลการปฏิบัติงานตามนโยบายการบริหารความเสี่ยงจากรายงานฯ ของคณะอนุกรรมการบริหารความเสี่ยงเป็นประจำทุกไตรมาส

ในปี พ.ศ.2564 กรมบัญชีกลาง กระทรวงการคลัง ได้กำหนดแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่องหลักการบริหารจัดการความเสี่ยงระดับองค์กร ที่ กค 1409.7/ ว 36 ได้กำหนดกระบวนการบริหารจัดการความเสี่ยงเป็นกระบวนการที่เป็นวงจรต่อเนื่อง ประกอบด้วย *(ที่มา : กรมบัญชีกลากระทรวงการคลัง ที่ กค 1409.7/ ว 36)*

(1) การวิเคราะห์องค์กร
(2) การกำหนดนโยบายการบริหารจัดการความเสี่ยง
(3) การระบุความเสี่ยง
(4) การประเมินความเสี่ยง
(5) การตอบสนองความเสี่ยง
(6) การติดตามและทบทวน
(7) การสื่อสารและรายงานผล

(1) การวิเคราะห์องค์กร (SWOT/PESTLE analysis)

ในการวิเคราะห์องค์กรหน่วยงานต้องเข้าใจเกี่ยวกับพันธะกิจตามกฎหมายอำนาจหน้าที่และความรับผิดชอบของหน่วยงานรวมถึงยุทธศาสตร์ชาติยุทธศาสตร์ระดับกระทรวงรวมถึงนโยบายของรัฐบาลที่เกี่ยวข้องกับหน่วยงานโดยการวิเคราะห์องค์กรต้องลอกทั้งปัจจัยภายในและปัจจัยภายนอกขององค์กรหน่วยงานอาจจะเลือกใช้เครื่องมือการวิเคราะห์องค์กร เช่น

1. SWOT Analysis เป็นการวิเคราะห์จุดแข็งจุดอ่อนโอกาสและอุปสรรค
2. PESTLE Analysis เป็นการวิเคราะห์ด้านการเมือง (Political) ด้านเศรษฐกิจ (Economic) ด้านสังคม (Social) ด้านเทคโนโลยี (Technology) ด้านกฎหมาย (Legal) และด้านสภาพแวดล้อม (Environmental)

(2) การกำหนดนโยบายการบริหารจัดการความเสี่ยง

ผู้บริหารเป็นผู้กำหนดนโยบายบริหารจัดการความเสี่ยง และผู้กำกับดูแลเป็นผู้ให้ความเห็นชอบนโยบายดังกล่าว โดยนโยบายการบริหารจัดการความเสี่ยงอาจจะระบุถึงวัตถุประสงค์ของการบริหารจัดการความเสี่ยงบทบาทหน้าที่ความรับผิดชอบของการบริหารจัดการความเสี่ยง และความเสี่ยงที่ยอมรับได้ในระดับองค์กร

ความเสี่ยงที่ยอมรับได้ในระดับองค์กร (Risk Appetite) หมายถึง ระดับความเสี่ยงในภาพรวมขององค์กรที่หน่วยงานยอมรับเพื่อดำเนินงานให้บรรลุวัตถุประสงค์ขององค์กร การระบุความเสี่ยงที่ยอมรับได้ในระดับองค์กรเป็นการแสดงเจตนารมณ์ของผู้บริหารและผู้กำกับดูแลในการดำเนินงานขององค์กร การกำหนดความเสี่ยงที่ยอมรับได้ควรคำนึงถึงศักยภาพขององค์กรในเรื่องการจัดการความเสี่ยง โดยศักยภาพในการจัดการความเสี่ยงขององค์กร (Risk Capacity) ขึ้นอยู่กับงบประมาณ บุคลากร และความคาดหวังของผู้มีส่วนได้เสีย ทั้งนี้หน่วยงานอาจระบุระดับความเสี่ยงที่ยอมรับได้เป็น 5 ระดับ เช่น ปฏิเสธความเสี่ยง ยอมรับความเสี่ยงได้น้อย ยอมรับความเสี่ยงได้ปานกลาง เต็มใจยอมรับความเสี่ยง และยอมรับความเสี่ยงได้มากที่สุด เป็นต้น

หน่วยงานอาจแสดงนโยบายความเสี่ยงที่ยอมรับได้ในแต่ละประเภทความเสี่ยง เพื่อให้ผู้บริหารระดับรองลงมาสามารถนำไปใช้ในการบริหารจัดการความเสี่ยงในระดับสำนัก กอง ศูนย์ กลุ่ม หรือนำไปสู่การระบุระดับความเสี่ยงที่ยอมรับได้สำหรับประเภทความเสี่ยงย่อย

(3) การระบุความเสี่ยง

การระบุความเสี่ยง คือ การระบุเหตุการณ์ที่อาจเกิดขึ้นที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงานทั้งในด้านบวกและด้านลบ ในการระบุความเสี่ยงหน่วยงานอาจทำรายชื่อความเสี่ยงทั้งหมด (Risk Inventory) โดยรายชื่อความเสี่ยงต้องมีการปรับปรุงอย่างสม่ำเสมอโดยอาศัยข้อมูลที่เป็นปัจจุบัน การระบุความเสี่ยงหน่วยงานควรระบุข้อมูลเกี่ยวกับความเสี่ยง ดังนี้

ก. เหตุการณ์ความเสี่ยง

ข. สาเหตุความเสี่ยงหรือตัวผลักดันความเสี่ยง โดยการวิเคราะห์ถึงสาเหตุที่แท้จริง (Root Cause) ของความเสี่ยง

ค. ผลกระทบทั้งด้านลบและหรือด้านบวก

หน่วยงานอาจจัดความเสี่ยงที่มีลักษณะหรือมีผลกระทบที่เหมือนกันไว้ในประเภทความเสี่ยงเดียวกัน เพื่อให้การพิจารณาและการบริหารจัดการความเสี่ยงประเภทเดียวกันมีมุมมองในภาพรวมที่ชัดเจนมากขึ้น

(4) การประเมินความเสี่ยง

การประเมินความเสี่ยงประกอบด้วย

1. การกำหนดเกณฑ์การประเมินความเสี่ยง หน่วยงานอาจจะให้คะแนนความเสี่ยงตามเกณฑ์การประเมินความเสี่ยงด้านต่างๆ เช่น ด้านโอกาสด้านผลกระทบรวมถึงด้านความสามารถขององค์กรในการจัดการความเสี่ยงและลักษณะของความเสี่ยงโดยช่วงคะแนนอาจกำหนดเป็น 3 ช่วงคะแนนหรือ 5 ช่วงคะแนน

2. การให้คะแนนความเสี่ยงวิธีการให้คะแนนความเสี่ยง เช่น การสัมภาษณ์การทำแบบสำรวจการระบุการประชุมเชิงปฏิบัติการระหว่างหน่วยงานภายในการทำ Benchmarking การวิเคราะห์สถานการณ์

(Scenario Analysis) ทั้งนี้ การให้คะแนนความเสี่ยงของแต่ละกองงาน (Silo Thinking) เพียงวิธีเดียวอาจทำให้การให้คะแนนความเสี่ยงมีความคลาดเคลื่อนได้

3. การพิจารณาความเสี่ยงในภาพรวม เมื่อหน่วยงานประเมินความเสี่ยงในแต่ละความเสี่ยงที่มีต่อวัตถุประสงค์ของกิจกรรมแล้ว หน่วยงานต้องพิจารณาผลกระทบความเสี่ยงที่มีต่อวัตถุประสงค์ในระดับกลุ่ม และผลกระทบที่มีต่อหน่วยงานในภาพรวม เช่น ผลกระทบต่อความเสี่ยงที่มีต่อกิจกรรมอาจจะมีน้อยแต่มีผลกระทบต่อวัตถุประสงค์และระดับกองหรือความเสี่ยง 2 ความเสี่ยงที่ไม่มีผลกระทบต่อกิจการอาจมีผลกระทบต่อหน่วยงานในภาพรวมเป็นต้น

4. การจัดลำดับความเสี่ยง เมื่อหน่วยงานเพียบนานให้คะแนนความเสี่ยงแล้วหน่วยงานต้องลำดับความเสี่ยงเพื่อนำไปสู่การพิจารณาจัดสรรทรัพยากรในการตอบสนองความเสี่ยง หน่วยงานอาจจะใช้คะแนนความเสี่ยง (โอกาส x ผลกระทบ) ในการจัดลำดับความเสี่ยง โดยความเสี่ยงที่เท่ากับอาจพิจารณาปัจจัยอื่นประกอบ เช่น ความสามารถของหน่วยงานในการบริหารจัดการความเสี่ยงด้านนั้นๆ หรือลักษณะของความเสี่ยงที่มีผลกระทบต่อหน่วยงาน เป็นต้น

(5) การตอบสนองความเสี่ยง

การตอบสนองความเสี่ยง คือ กระบวนการตัดสินใจของฝ่ายบริหารในการจัดการความเสี่ยงที่อาจจะเกิดขึ้นโดยผู้บริหารควรพิจารณาประเด็นดังต่อไปนี้ในการตัดสินใจเลือกวิธีการตอบสนองความเสี่ยง เพื่อจัดทำแผนบริหารจัดการความเสี่ยงของหน่วยงาน

1. การจัดการต้นเหตุของความเสี่ยง
2. ทางเลือกวิธีการจัดการความเสี่ยง
3. ทรัพยากรที่ต้องใช้ในการบริหารจัดการความเสี่ยง

หน่วยงานสามารถพิจารณาเลือกวิธีการจัดการความเสี่ยง วิธีที่ ได้วิธีหนึ่งหรือหลายวิธีโดยการพิจารณาวิธีการจัดการความเสี่ยงควรคำนึงถึงต้นทุนกับประโยชน์ ที่ได้รับของวิธีการจัดการความเสี่ยงแต่ละวิธี

ตัวอย่างวิธีการจัดการความเสี่ยงประกอบด้วย

1. ปฏิเสธความเสี่ยงโดยไม่ดำเนินการในกิจกรรมที่มีความเสี่ยง ได้แก่ กิจกรรมที่มีความเสี่ยงสูงและหน่วยงานไม่สามารถยอมรับความเสี่ยงนั้นได้ หน่วยงานอาจพิจารณาไม่ดำเนินงานในกิจกรรมนั้นๆ

2. การลดโอกาสของความเสี่ยง เช่น การลดโอกาสความเสี่ยงการทุจริตด้านการเงินโดยการวางระบบการควบคุมภายใน ได้แก่ การแบ่งแยกหน้าที่ การตรวจสอบ การสอบทาน และการกระทบยอด เป็นต้น

3. การลดผลกระทบความเสี่ยง เช่น การทำประการหรือการใช้เครื่องมือป้องกันความเสี่ยงทางการเงิน (Hedging instruments) เป็นต้น

4. การโอนความเสี่ยง หน่วยงานอาจมีเลือกวิธีการภายในโอนความเสี่ยงของกิจกรรม ที่หน่วยงานเห็นควรดำเนินการเพื่อประโยชน์ของประชาชนแต่หน่วยงานมีข้อจำกัดที่ไม่สามารถดำเนินงานเองได้หรือไม่สามารถบริหารจัดการความเสี่ยง ได้แก่ การให้ภาคเอกชนดำเนินการโดยมีการโอนความเสี่ยงและผลตอบแทนไปด้วย (Public Private Partnership : PPP) เป็นต้น

5. ยอมรับความเสี่ยง โดยไม่ดำเนินการจัดการความเสี่ยงเนื่องจากความเสี่ยงอยู่ในระดับที่หน่วยงานยอมรับได้ หรือต้นทุนการบริหารจัดการความเสี่ยงมีมากกว่าประโยชน์ที่ได้รับ

6. ใช้มาตรการการเฝ้าระวัง หน่วยงานต้องกำหนดข้อมูลที่ต้องมีการเก็บรวบรวม การวิเคราะห์ การแจ้งเตือน และการดำเนินการเมื่อเหตุการณ์เกิดขึ้น เช่น ความเสี่ยงของปริมาณน้ำในเขื่อนมากเนื่องจากปริมาณน้ำฝน

7. ถามแผนฉุกเฉิน การทำแผนฉุกเฉินเป็นการระบุขั้นตอนเมื่อเกิดเหตุการณ์ความเสี่ยงขึ้นโดยต้องระบุบุคคลและวิธีการดำเนินการที่ชัดเจน เช่น ความเสี่ยงกรณีที่เจ้าหน้าที่ไม่สามารถเข้าสถานที่ทำงานได้

8. การส่งเสริมหรือ หรือ ผลักดันเหตุการณ์ที่อาจเกิดขึ้น เมื่อมีเหตุการณ์ที่อาจจะเกิดขึ้นส่งผลกระทบเชิงบวกกับองค์กร รวมถึงกำหนดแผนการดำเนินงานเมื่อเหตุการณ์เกิดขึ้น

แผนการบริหารจัดการความเสี่ยงประกอบด้วย วิธีการจัดการความเสี่ยง บุคคลที่รับผิดชอบในการบริหารจัดการความเสี่ยง ตัวชี้วัดความเสี่ยงที่สำคัญ วิธีการติดตามและการรายงานความเสี่ยง

(6) การติดตามและทบทวน

การติดตามและทบทวน เป็นกระบวนการที่ให้ความเชื่อมั่นว่าการบริหารจัดการความเสี่ยงที่มีอยู่ยังคงมีประสิทธิผล เนื่องจากความเสี่ยงเป็นสิ่งที่เกิดขึ้นและเปลี่ยนแปลงตลอดเวลา ดังนั้น การติดตามและทบทวนเป็นกระบวนการที่เกิดขึ้นสม่ำเสมอ ปัจจัยที่ทำให้หน่วยงานต้องทบทวนการบริหารจัดการความเสี่ยง ได้แก่ การเปลี่ยนแปลงที่สำคัญที่ซึ่งเกิดขึ้นจากปัจจัยภายในและภายนอก หรือผลการดำเนินงานไม่เป็นไปตามเป้าหมายที่กำหนดไว้

การติดตามและทบทวนการบริหารจัดการความเสี่ยงสามารถดำเนินการอย่างต่อเนื่อง หรือเป็นระยะ ซึ่งควรดำเนินการทุกกระบวนการของการบริหารจัดการความเสี่ยง การติดตามและทบทวนอาจจะนำไปสู่การเปลี่ยนแปลงของแผนปฏิบัติงานขององค์กร การเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ รวมถึงการพัฒนาระบบการบริหารจัดการความเสี่ยง

(7) การสื่อสารและการรายงาน

การสื่อสารเป็นการสร้างความตระหนัก ความเข้าใจ และการมีส่วนร่วมของกระบวนการบริหารจัดการความเสี่ยงการสื่อสารเป็นการให้และรับข้อมูล (Two-Way Communication) หน่วยงานควรมีช่องทางสื่อสารทั้งภายในและภายนอกโดยการศึกษาภายในต้องเป็นการศึกษาแบบจากผู้บริหารไปอย่างผู้ใต้บังคับบัญชา (Top Down) จากผู้ใต้บังคับบัญชาไปยังผู้บริหาร (Bottom Up) และระหว่างหน่วยงานย่อยภายใน (Across Divisions)

หน่วยงานควรกำหนดบุคคลที่ควรได้รับข้อมูล ประเภทของข้อมูลที่ควรได้รับความถี่ของการรายงาน รูปแบบและวิธีการรายงาน เพื่อให้ผู้กำกับดูแลผู้บริหารและผู้มีส่วนได้เสียได้รับข้อมูลสารสนเทศที่ถูกต้องครบถ้วน เกี่ยวข้องกับการตัดสินใจและทันต่อเวลา

การสื่อสารและรายงานต่อผู้กำกับ ดูแล เป็นการสื่อสารและการรายงานความเสี่ยงในภาพรวมขององค์กรเพื่อสนับสนุนหน้าที่ผู้กำกับดูแลในการกับการบริหารจัดการความเสี่ยงของฝ่ายบริหาร

หน่วยงานอาจพิจารณากำหนดตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators) เพื่อติดตามข้อมูลความเสี่ยงและการรายงานเมื่อระดับความเสี่ยงถึงจุดตรวจชี้วัดความเสี่ยงที่สำคัญ

การประเมินความเสี่ยงการทุจริต

การประเมินความเสี่ยงการทุจริต มีข้อกำหนดให้หน่วยงานรัฐต้องมีการประเมินทุจริต โดยมีข้อกำหนดอยู่ 2 แห่ง ได้แก่ หลักเกณฑ์การควบคุมภายในสำหรับหน่วยงานของรัฐ'61 (ว 105 ข้อ 8) และเกณฑ์การประเมินความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐ (ปปช.)

ภาพที่ 37 การประเมินทุจริต (1)

ว 105 หลักเกณฑ์การควบคุมภายในสำหรับหน่วยงานของรัฐ'61

๒. การประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ดำเนินการอย่างต่อเนื่องและเป็นประจำ เพื่อระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงานของรัฐ รวมถึงกำหนดวิธีการจัดการความเสี่ยงนั้น ฝ่ายบริหารควรคำนึงถึงการเปลี่ยนแปลงของสภาพแวดล้อมภายนอกและภารกิจภายในทั้งหมดที่มีผลต่อการบรรลุวัตถุประสงค์ของหน่วยงานของรัฐ

การประเมินความเสี่ยงประกอบด้วย ๔ หลักการ ดังนี้

(๖) หน่วยงานของรัฐระบุวัตถุประสงค์การควบคุมภายในของการปฏิบัติงานให้สอดคล้องกับวัตถุประสงค์ขององค์กรไว้อย่างชัดเจนและเพียงพอที่จะสามารถระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับวัตถุประสงค์

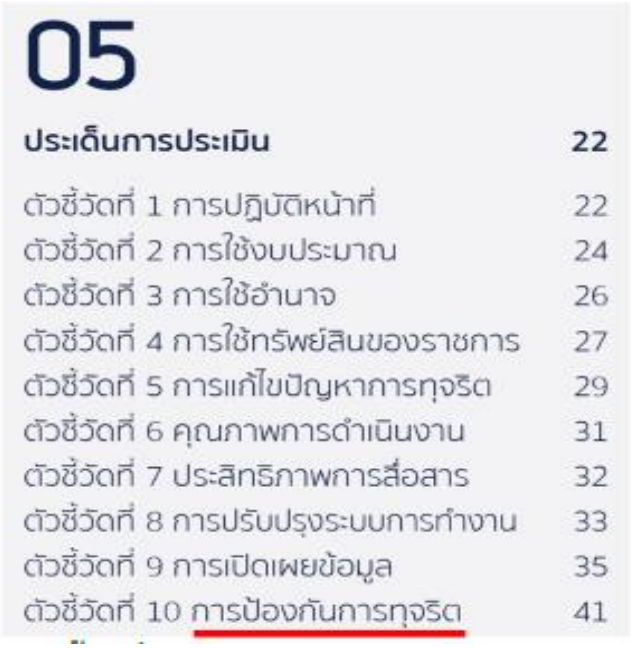
(๗) หน่วยงานของรัฐระบุความเสี่ยงที่มีผลต่อการบรรลุวัตถุประสงค์การควบคุมภายในอย่างครอบคลุมทั้งหน่วยงานของรัฐ และวิเคราะห์ความเสี่ยงเพื่อกำหนดวิธีการจัดการความเสี่ยงนั้น

(๘) หน่วยงานของรัฐพิจารณาโอกาสที่อาจเกิดการทุจริต เพื่อประกอบการประเมินความเสี่ยงที่ส่งผลต่อการบรรลุวัตถุประสงค์

(๙) หน่วยงานของรัฐระบุและประเมินการเปลี่ยนแปลงที่อาจมีผลกระทบอย่างมีนัยสำคัญต่อระบบการควบคุมภายใน

ภาพที่ 38 การประเมินทุจริต (2) - ว 105 ข้อ 8

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ. (2563: 30) ได้จัดทำเอกสาร ITA 2020 Open to Transparency เปิดประตูความโปร่งใส ซึ่งเป็นเอกสารรายละเอียดการประเมินคุณธรรมและความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐ (Integrity and Transparency Assessment: ITA) ประจำปีงบประมาณ พ.ศ. 2563 ได้กำหนดตัวชี้วัดที่ 10 การป้องกันการทุจริต ดังนี้



ภาพที่ 39 การประเมินทุจริต (3) – ITA ตัวชี้วัดที่ 10 การป้องกันการทุจริต

การประเมินความเสี่ยงเพื่อป้องกันการทุจริต

ข้อ	ข้อมูล	องค์ประกอบด้านข้อมูล
o36	การประเมินความเสี่ยงการทุจริตประจำปี	o แสดงผลการประเมินความเสี่ยงของการดำเนินงานหรือการปฏิบัติหน้าที่ที่อาจก่อให้เกิดการทุจริตหรือก่อให้เกิดการขัดกันระหว่างผลประโยชน์ส่วนตนกับผลประโยชน์ส่วนรวมของหน่วยงาน o มีข้อมูลรายละเอียดของผลการประเมิน เช่น เหตุการณ์ความเสี่ยงและระดับของความเสี่ยง มาตรการและการดำเนินการในการบริหารจัดการความเสี่ยง เป็นต้น o เป็นการดำเนินการในปี พ.ศ. 2563
o37	การดำเนินการเพื่อจัดการความเสี่ยงการทุจริต	o แสดงการดำเนินการหรือกิจกรรมที่แสดงถึงการจัดการความเสี่ยงในกรณีที่อาจก่อให้เกิดการทุจริตหรือก่อให้เกิดการขัดกันระหว่างผลประโยชน์ส่วนตนกับผลประโยชน์ส่วนรวมของหน่วยงาน o เป็นกิจกรรมหรือการดำเนินการที่สอดคล้องกับมาตรการหรือการดำเนินการเพื่อบริหารจัดการความเสี่ยงตามข้อ O36 o เป็นการดำเนินการในปี พ.ศ. 2563

ภาพที่ 40 การประเมินทุจริต (4) – เกณฑ์ประเมิน O36 และ O37 (1)

นอกจากนั้น การประเมินทุจริตยังเป็นมาตรฐานการปฏิบัติงานของผู้ตรวจสอบสอบภายใน ซึ่งได้กำหนดไว้ในมาตรฐานการตรวจสอบภายใน ตามหนังสือกรมบัญชีกลางที่ กค 0409.2/ว 123 เรื่องหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 กำหนดไว้ ดังนี้

มาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงาน

มาตรฐานการปฏิบัติงาน

2100 ลักษณะของงานตรวจสอบภายใน

2120 การบริหารความเสี่ยง

2120.A2 : การปฏิบัติงานตรวจสอบภายในต้องประเมินโอกาสของการเกิดทุจริตและวิธีการบริหารความเสี่ยงในเรื่องที่เกี่ยวข้องกับการทุจริต

ภาพที่ 41 การประเมินทุจริต (6) – ตามมาตรฐานการตรวจสอบภายในสำหรับหน่วยงานของรัฐ

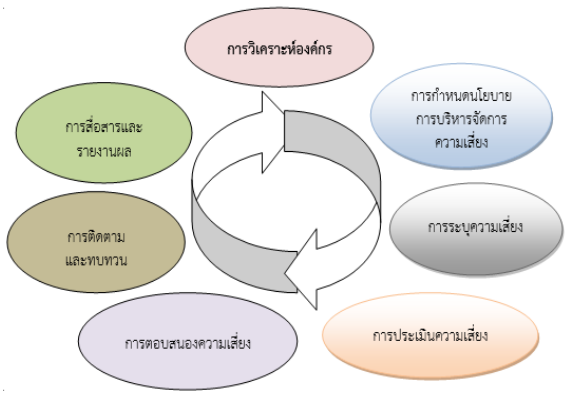
ส่วนที่ 4
แผนบริหารความเสี่ยง

แผนบริหารความเสี่ยง สำนักงานตรวจสอบภายใน รอบปีงบประมาณ 2567 จัดทำขึ้นเพื่อเป็นกรอบแนวทางการปฏิบัติงานในการดำเนินงานการบริหารความเสี่ยงของสำนักงานตรวจสอบภายในให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพและมีประสิทธิผล รวมทั้งเพื่อให้ผู้บริหารและบุคลากร มีความรู้ ความเข้าใจในเรื่องการบริหารความเสี่ยง และสามารถนำไปปฏิบัติในทิศทางเดียวกันได้อย่างมีประสิทธิผลและต่อเนื่อง ซึ่งเป็นไปตามมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ พ.ศ.2562 (ว 23) ข้อ 2.1 ได้กำหนดให้หน่วยงานของรัฐต้องจัดให้มีการบริหารจัดการความเสี่ยง เพื่อให้เกดความเชื่อมั่นอย่างสมเหตุสมผลแก่ผู้มีส่วนได้เสียของหน่วยงานได้ดำเนินการบริหารจัดการความเสี่ยงอย่างเหมาะสม

รวมทั้งหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ซึ่งเป็นส่วนหนึ่งของมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ พ.ศ. 2562 (ว 23) ข้อ 2 ข้อ 6 และข้อ 7 ได้กำหนดเพิ่มเติมให้หน่วยงานของรัฐต้องจัดให้มีการบริหารความเสี่ยง จัดทำแผนบริหารความเสี่ยง และให้หัวหน้าหน่วยงานของรัฐกำกับดูแลบริหารและบุคลากรให้มีการบริหารจัดการความเสี่ยงตามแผนบริหารความเสี่ยงที่กำหนดไว้

กระบวนการบริหารความเสี่ยง

การจัดทำระบบบริหารความเสี่ยงเพื่อให้เกิดประสิทธิภาพและประสิทธิผล สำนักงานตรวจสอบภายใน ได้กำหนดกรอบบริหารความเสี่ยงองค์การประจำปี ซึ่งมีความสอดคล้องและเชื่อมโยงกับวิสัยทัศน์ เป้าประสงค์ และกลยุทธ์ขององค์การ โดยการกำหนดความเสี่ยงระดับองค์กรที่จะต้องมีการวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุเป้าหมายขององค์การ โดยแผนบริหารความเสี่ยงของสำนักงานตรวจสอบภายใน รอบปีงบประมาณ 2567 ได้จัดทำตามขั้นตอนการบริหารจัดการความเสี่ยงตามกระบวนการบริหารจัดการความเสี่ยงตามที่กรมบัญชีกลาง กระทรวงการคลัง กำหนดประกอบด้วย (ภาพที่ 42) *(ที่มา : กรมบัญชีกลาง กระทรวงการคลัง ที่ กค 1409.7/ ว 36)* ดังนี้



ภาพที่ 42 กระบวนการบริหารจัดการความเสี่ยง

1. การวิเคราะห์องค์กร

สำนักงานตรวจสอบภายใน มหาวิทยาลัยราชภัฏเชียงใหม่ ได้มีการประชุมสำนักงานตรวจสอบภายในเพื่อการวิเคราะห์และเพื่อความเข้าใจถึงจุดแข็ง (Strengths) จุดอ่อน(Weaknesses) ภาวะคุกคาม หรืออุปสรรค (Threats) และโอกาส (Opportunities) ในการพัฒนาขององค์กร เพื่อการวางแผนกลยุทธ์ได้ถูกทิศทาง โดยอาศัยข้อมูลการดำเนินงานของสำนักงานตรวจสอบภายในตลอดระยะที่ผ่านมา พบว่า สำนักงานตรวจสอบภายใน ยังมีจุดแข็ง จุดอ่อน และในขณะเดียวกันยังมีโอกาส (Opportunities) และอุปสรรค (Threats) ในการดำเนินงาน ดังนี้

ตารางที่ 15 แสดงการวิเคราะห์องค์กร (SWOT) สำนักงานตรวจสอบภายใน

จุดแข็ง (Strengths)	**จุดอ่อน (Weaknesses)**
1) หน่วยงานมีอิสระในการตรวจสอบและขึ้นตรงต่อคณะกรรมการตรวจสอบ 2) บุคลากรผู้ปฏิบัติงานส่วนใหญ่มีความรู้ ทักษะ และประสบการณ์ในการตรวจสอบ 3) บุคลากรมีความรับผิดชอบต่อภาระงานที่รับมอบหมาย 4) บุคลากรมีคุณธรรม จริยธรรม และซื่อสัตย์ และมีความเป็นกลาง 5) มีวัสดุสำนักงานให้ใช้งานอย่างพอเพียง 6) มีการบริหารจัดการที่มีความกระชับ รวดเร็ว และมีประสิทธิภาพตอบสนองความต้องการได้อย่างเหมาะสม โดยการนำเทคโนโลยีเข้ามาใช้ในการดำเนินงาน	1) การไม่คุ้นชินการใช้เทคโนโลยีในการดำเนินงานบนออนไลน์ 2) ครุภัณฑ์บางอย่างมีอายุการใช้งานเป็นเวลานานประสิทธิภาพการใช้งานลดลง 3) ครุภัณฑ์ภาคสนาม ได้แก่ คอมพิวเตอร์ชนิดพกพาไม่เพียงพอ 4) การใช้โปรแกรมการปฏิบัติงานขั้นสูงในการตรวจสอบ
โอกาส (Opportunities)	**อุปสรรค (Threats)**
1) หน่วยรับตรวจ ให้ความร่วมมือเป็นอย่างดี 2) มหาวิทยาลัยให้หน่วยงานขอรับการสนับสนุนงบประมาณในการดำเนินงานพัฒนาบุคลากรได้อย่างเหมาะสม 3) มหาวิทยาลัยมีนโยบายชัดเจนในด้านความโปร่งใส และการตรวจสอบเป็นเครื่องมือในการบริหารงาน จึงเอื้อต่อการดำเนินงานตรวจสอบ 4) มีเครือข่ายหน่วยตรวจสอบภายในทั้งภายในและภายนอก 5) มีการสนับสนุนด้านเทคโนโลยีสารสนเทศในการปฏิบัติงาน	1) การตรวจสอบต้องใช้ข้อมูลบางส่วนจากหน่วยงานภายนอก 2) การเกิดสถานการณ์ไม่คาดคิด เช่น เกิดโรคอุบัติใหม่ ทำให้ไม่สามารถดำเนินงานปกติได้ ฯลฯ

หมายเหตุ : เลือกใช้เครื่องมือในการวิเคราะห์องค์กร (SWOT analysis) ตาม กค 1409.7/ ว 36 ลว 3 ก.พ.2564

2. การกำหนดนโยบายการบริหารจัดการความเสี่ยง

นโยบาย

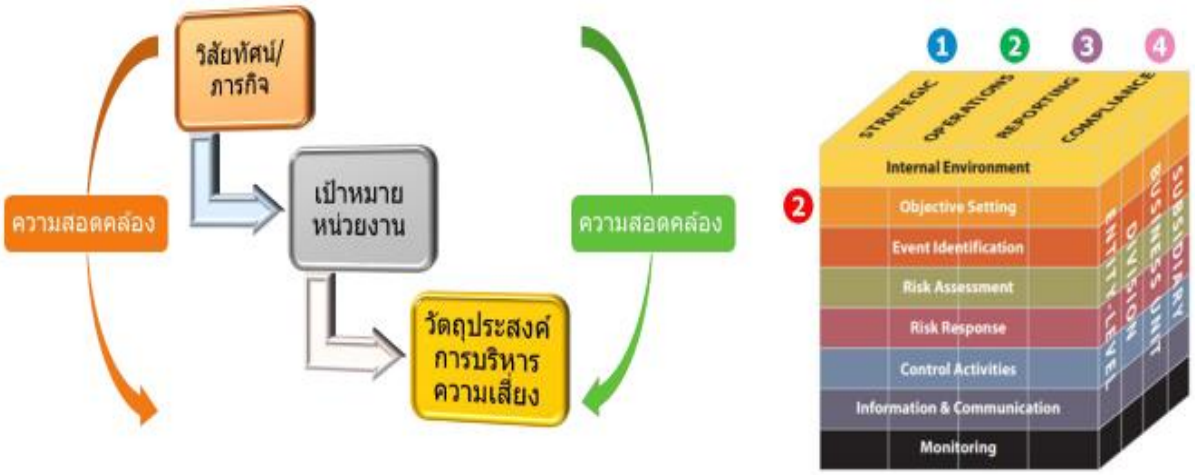
นโยบายการบริหารความเสี่ยง เป็นกรอบการดำเนินงานของสำนักงานตรวจสอบภายในที่ได้ประยุกต์ใช้หลักการบริหารความเสี่ยงองค์กร (Enterprise Risk Management : ERM) เพื่อกำหนดแนวทางในการดำเนินการบริหารจัดการความเสี่ยงและควบคุมภายในองค์กรให้บรรลุเป้าหมายกลยุทธ์ โดยประกาศนโยบายการบริหารความเสี่ยง และสื่อสารผ่านทางการประชุมสำนักงานตรวจสอบภายใน (ภาพที่ 43) คือ

1) ให้มีบริหารความเสี่ยงทั่วทั้งหน่วยงาน (Enterprise Risk Management : ERM) โดยจะยอมรับความเสี่ยงในระดับปานกลางและความเสี่ยงในระดับน้อยในการปฏิบัติงาน
2) ให้ปฏิเสธที่จะยอมรับความสี่ยงที่เกี่ยวข้องกับการทุจริตทุกกรณี (Anti-Corruption) และจะเป็นแบบอย่างที่ดี มุ่งมั่นสร้างระบบการควบคุม ป้องกัน ตรวจสอบ ให้เกิดความเชื่อมั่นในองค์กร
3) ให้ผู้บริหาร/บุคลากรทุกคนมีส่วนร่วมในการบริหารความเสี่ยง (Participation)
4) ให้นำระบบเทคโนโลยีสารสนเทศที่ทันสมัยมาใช้ในกระบวนการบริหารความเสี่ยง และสนับสนุนให้เจ้าหน้าที่ทุกระดับเข้าถึงสารสนเทศการบริหารความเสี่ยง (IT Support)
5) ให้ติดตามทบทวนความเสี่ยงให้สอดคล้องกับสภาวะแวดล้อมที่เปลี่ยนแปลง (Adapt to Change)
6) ส่งเสริม/กระตุ้นให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กร โดยให้เจ้าหน้าที่ทุกคนตระหนักความสำคัญของการบริหารความเสี่ยง (Risk Awareness Culture)
7) ดำเนินการ/สนับสนุนให้การบริหารความเสี่ยง โดยใช้ทรัพยากรที่มีอย่างจำกัด ให้เกิดประสิทธิภาพเพื่อสามารถจัดการความเสี่ยงได้อย่างเหมาะสม (Efficient under limited resource)

ภาพที่ 43 นโยบายการบริหารความเสี่ยง

วัตถุประสงค์

สำนักงานตรวจสอบภายใน กำหนดวัตถุประสงค์ (Objective Setting) ของหน่วยงาน จำนวน 4 ด้าน ได้แก่ ด้านยุทธศาสตร์/กลยุทธ์ ด้านการปฏิบัติงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎระเบียบ โดยยึดหลักการกำหนดวัตถุประสงค์ตามที่สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลังกำหนด หลักการที่เรียกว่า **“SMART”**



ภาพที่ 44 COSO ERM Model - Components – Objective Setting

ตารางที่ 16 แสดงการกำหนดวัตถุประสงค์

วิสัยทัศน์	การกำหนดวัตถุประสงค์
ตรวจสอบอย่างโปร่งใส บริการที่เที่ยงธรรม แนะนำและให้คำปรึกษาที่มีคุณค่า	**1) วัตถุประสงค์ด้านกลยุทธ์ (Strategic Objectives)** • เพื่อดำเนินการทบทวนแผน เป้าหมาย 1 ครั้ง/ปี
	2) วัตถุประสงค์ด้านการปฏิบัติงาน (Operations Objectives) • เพื่อปฏิบัติงานตรวจสอบภายในแก่หน่วยงานที่ได้รับงบประมาณ เป้าหมาย ร้อยละ 100
	3) วัตถุประสงค์ด้านการรายงาน (Reporting Objectives) • เพื่อมีการเบิกจ่ายงบประมาณตามแผนเบิกจ่าย เป้าหมายร้อยละ 96
	4) วัตถุประสงค์ด้านการปฏิบัติตามกฎระเบียบ (Compliance Objectives) • มีการสอบทานกระบวนการปฏิบัติงานตามระเบียบข้อกำหนด เป้าหมาย ร้อยละ 100

3. การระบุความเสี่ยง (Risk Identification)

การกำหนดประเภทความเสี่ยง (Risk Categories)

จากคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน, กระทรวงการคลัง (2555 : 45-46) ได้ระบุว่า กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ และเกณฑ์ประเมินผลการดำเนินงานรัฐวิสาหกิจ ด้านการบริหารจัดการองค์กร กระทรวงการคลัง ได้แบ่งประเภทของความเสี่ยงเป็น 4 ประเภท ดังนี้

3.1 การกำหนดประเภทความเสี่ยง (Risk Categories)

(1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : SR)

(2) ความเสี่ยงด้านการปฏิบัติการ (Operational Risk : OR)

(3) ความเสี่ยงด้านการเงิน (Financial Risk : FR)

(4) ความเสี่ยงด้านกฎระเบียบ/ข้อบังคับ (Compliance Risk : CR)

สำนักงานตรวจสอบภายใน ได้ระบุความเสี่ยงตามคำนิยามของมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ พ.ศ.2562 ตามประเภทความเสี่ยง ดังนี้

ตารางที่ 17 แสดงระบุความเสี่ยงตามประเภทความเสี่ยง

ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความสูญเสียที่อาจเกิดขึ้น/ผลกระทบ
1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : SR)			
SR1	ยุทธศาสตร์/แผนงานไม่สอดคล้องกันระหว่างหน่วยงานกับองค์กร	SR1.1 ระยะเวลาไม่ได้ทบทวนแผน	การดำเนินงานของหน่วยงานไม่สอดคล้องกับยุทธศาสตร์มหาวิทยาลัย
SR2	แผนกลยุทธ์หน่วยงานไม่สามารถนำไปสู่การบรรลุวัตถุประสงค์องค์กร	SR2.1 ระยะเวลาไม่ได้ทบทวนแผน	การดำเนินงานของหน่วยงานไม่สอดคล้องกับยุทธศาสตร์มหาวิทยาลัย
SR3	แผนกลยุทธ์หน่วยงานขาดการพัฒนาจนขาดประสิทธิภาพให้ทันต่อสถานการณ์	SR3.1 ระยะเวลาไม่ได้ทบทวนแผน	การดำเนินงานของหน่วยงานไม่สอดคล้องกับยุทธศาสตร์มหาวิทยาลัย
SR4	การปฏิบัติงานไม่สอดคล้องกับภารกิจ /ยุทธศาสตร์ / นโยบายของหน่วยงาน	SR4.1 ระยะเวลาไม่ได้ทบทวนแผน	การดำเนินงานของหน่วยงานไม่สอดคล้องกับยุทธศาสตร์มหาวิทยาลัย
2) ความเสี่ยงด้านการเงิน (Financial Risk : FR)			
FR1	เบิกจ่ายงบประมาณไม่เป็นไปตามแผน	FR1.1 ไม่ได้กำกับติดตามการเบิกจ่ายงบประมาณ	เป็นปัจจัยทำให้การเบิกจ่ายงบประมาณของมหาวิทยาลัยอาจไม่เป็นไปตามค่าเป้าหมาย
FR2	เบิกจ่ายงบประมาณไม่เป็นไปตามค่าเป้าหมายตามมติคณะรัฐมนตรี (ครม.)	FR2.1 ไม่ได้กำกับติดตามการเบิกจ่ายงบประมาณ FR2.2 ประมาณการของงบประมาณมากไป	เป็นปัจจัยทำให้การเบิกจ่ายงบประมาณของมหาวิทยาลัยอาจไม่เป็นไปตามค่าเป้าหมาย
FR3	เบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา	FR2.2 ประมาณการของงบประมาณมากไป	เป็นปัจจัยทำให้การเบิกจ่ายงบประมาณของมหาวิทยาลัยอาจไม่เป็นไปตามค่าเป้าหมาย
FR4	งบประมาณไม่เพียงพอ	FR4.1 ไม่ได้กำกับติดตามการเบิกจ่ายงบประมาณ	ภารกิจของหน่วยงานไม่บรรลุวัตถุประสงค์
3) ความเสี่ยงด้านการดำเนินงาน (Operation Risk : OR)			
OR1	การปฏิบัติงานไม่เป็นไปตามแผนงาน	OR1.1 สำนักงานตรวจสอบภายในไม่ได้รับข้อมูลตามแผนที่กำหนด OR1.2 เกิดสถานการณ์ไม่คาดคิด ทำให้ไม่สามารถดำเนินงานปกติได้	ภารกิจของหน่วยงานไม่บรรลุวัตถุประสงค์
OR2	ขาดข้อมูลสนับสนุนในการดำเนินงาน	OR2.1 ไม่ได้ประชุมกำกับติดตาม	ภารกิจของหน่วยงานไม่บรรลุวัตถุประสงค์
OR3	บุคลากรขาดทักษะ ความรู้ ความชำนาญ/ ไม่ทันกับสถานการณ์	OR3.1 ชั่วโมงการฝึกอบรมน้อยกว่าเกณฑ์	ภารกิจของหน่วยงานไม่บรรลุวัตถุประสงค์
OR4	บุคลากรไม่สามารถให้คำปรึกษาหรือเป็นวิทยากรได้	OR4.1 จำนวนการเข้าอบรมหลักสูตรที่เกี่ยวข้องมีจำนวนน้อย OR4.2 ข้อมูลนำเสนอมีจำนวนน้อย	ภารกิจของหน่วยงานไม่บรรลุวัตถุประสงค์
OR5	ข้อมูลการตรวจนับพัสดุไม่ตรงกัน	OR5.1 เกิดการคลาดเคลื่อนของข้อมูลพัสดุ OR5.2 การอัพเดตข้อมูลไม่เป็นปัจจุบัน	ภารกิจของหน่วยงานไม่บรรลุวัตถุประสงค์
OR6	การถูกโจมตีทางไซเบอร์ทำให้ข้อมูลสูญหายหรือถูกทำลาย	OR6 ขาดความรู้ ทักษะ การป้องกัน	ภารกิจของหน่วยงานไม่บรรลุวัตถุประสงค์

ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความสูญเสียที่อาจเกิดขึ้น/ ผลกระทบ
4) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk : CR)			
CR1	ปฏิบัติผิดกฎระเบียบ	CR1.1 การไม่รู้กฎระเบียบว่าผิด (ไม่ตั้งใจ)	การดำเนินงานไม่เป็นไปตามมาตรฐานการปฏิบัติงาน
CR2	รู้ไม่ทันกฎหมายใหม่	CR2.1 ผู้ตรวจสอบภายในไม่ได้อบรมความรู้ด้านกฎหมายที่เป็นปัจจุบัน	การดำเนินงานไม่เป็นไปตามมาตรฐานการปฏิบัติงาน
CR3	เกิดความเข้าใจผิด / สับสน / การตีความคลาดเคลื่อน	CR3.1 การไม่รู้ข้อมูลที่ถูกต้อง	การดำเนินงานไม่เป็นไปตามมาตรฐานการปฏิบัติงาน
CR4	การทุจริต *(ว 105 ข้อ 8)*	CR4.1 แรงจูงใจ / โอกาส / ข้ออ้าง (สามเหลี่ยมการทุจริต, ปปช.)	มหาวิทยาลัยเกิดความสูญเสีย/สูญเปล่าทางทรัพยากร /ภาพลักษณ์

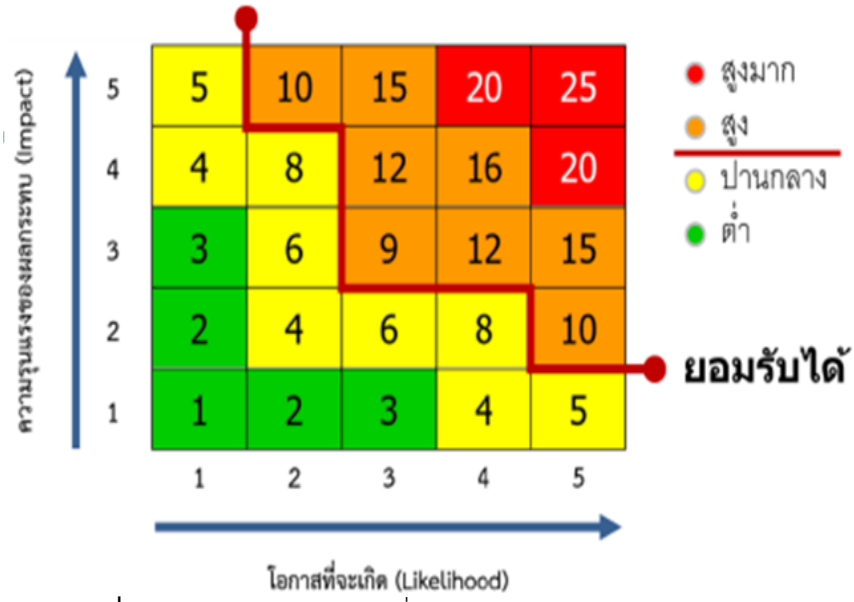
4. การประเมินความเสี่ยง

การประเมินความเสี่ยง (Risk Assessment) สำนักงานตรวจสอบภายใน ดำเนินกระบวนประเมินความเสี่ยง โดยดำเนินการ 4 ขั้นตอน ได้แก่ 1) การกำหนดเกณฑ์ประเมินความเสี่ยง 2) การประเมินโอกาส (Likelihood : L) และผลกระทบ (Impact : I) ของความเสี่ยง 3) การวิเคราะห์ความเสี่ยง และ 4) การจัดลำดับความเสี่ยง 4 ขั้นตอนย่อย คือ

4.1 การกำหนดเกณฑ์ประเมินความเสี่ยง สำนักงานตรวจสอบภายใน ได้กำหนดเกณฑ์การประเมินความเสี่ยง จากระดับคะแนน 1-25 คะแนน เพื่อใช้ประเมินโอกาสและผลกระทบของความเสี่ยง ดังนี้

ตารางที่ 18 แสดงการกำหนดระดับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	การยอมรับ	ความหมาย
สูงมาก	20-25	ยอมรับไม่ได้	ความเสี่ยงที่ต้องกำกับดูแลอย่างใกล้ชิดและต้องบริหารจัดการความเสี่ยง**ทันที**
สูง	9-19	ยอมรับไม่ได้	ความเสี่ยงที่ต้องกำกับดูแลอย่างใกล้ชิดและต้องบริหารจัดการความเสี่ยง**ทันที**
ปานกลาง	4-8	ยอมรับได้	ความเสี่ยงที่ต้องเฝ้าระวังซึ่งจะต้องบริหารความเสี่ยงโดยให้ความสนใจ**เฝ้าระวัง**
ต่ำ	1-3	ยอมรับได้	ความเสี่ยงที่ใช้วิธีควบคุมปกติไม่ต้องมีการจัดการเพิ่มเติม



ภาพที่ 45 แผนภูมิระดับความเสี่ยง

4.2 เกณฑ์ประเมินโอกาส (Likelihood : L) และผลกระทบของความเสี่ยง (Impact : I)

สำนักงานตรวจสอบภายใน ได้กำหนดเกณฑ์ประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood : L) โดยแบ่งไว้เป็น 5 ระดับ (เรียงจากมากไปน้อย) และมีตัวบ่งชี้หรือแนวโน้มตัวชี้วัดโอกาสการเกิดขึ้นของเหตุการณ์ *(ตารางที่ 19)* ได้แก่

ระดับ 5 : สูงมาก

ระดับ 4 : สูง

ระดับ 3 : ปานกลาง

ระดับ 2 : น้อย

ระดับ 1 : น้อยมาก

กำหนดเกณฑ์ประเมินผลกระทบที่จะเกิดความเสี่ยง (Impact : I) โดยแบ่งไว้เป็น 5 ระดับเช่นเดียวกัน (เรียงจากมากไปน้อย) *(ตารางที่ 20)* ได้แก่

ระดับ 5 : สูงมาก

ระดับ 4 : สูง

ระดับ 3 : ปานกลาง

ระดับ 2 : น้อย

ระดับ 1 : น้อยมาก

ตารางที่ 19 แสดงเกณฑ์ประเมินโอกาส (Likelihood : L)

โอกาสที่จะเกิด (Likelihood : L)		L1	L2	L3	L4	L5	L6	L7	L8
ระดับ	โอกาส (Likelihood : L)	ระยะเวลาที่ไม่ได้ทบทวนแผน	เวลาไม่ได้ประชุมกำกับติดตาม	ชั่วโมงฝึกอบรมเฉลี่ย (ตามเกณฑ์)	จำนวนการเข้าอบรมหลักสูตรที่เกี่ยวข้อง	มีข้อมูลนำเสนอ	จำนวนเรื่องที่มิได้อบรม	ประวัติการเกิดขึ้น/โอกาสเกิด	จำนวนงานที่ขาดการสอบทาน
5	**สูงมาก**	*> 5ปี*	*>1 ปี*	*≤15 ชม.*	*≤1 หลักสูตร*	*≤1 เรื่อง*	*>5 เรื่อง*	*≥8 ครั้ง*	*≥6 งาน*
4	**สูง**	*4ปี*	*6 เดือน – 1 ปี*	*15-19 ชม.*	*2-4 หลักสูตร*	*2 เรื่อง*	*>4 เรื่อง*	*6-7 ครั้ง*	*5 งาน*
3	**ปานกลาง**	*3ปี*	*> 3-6 เดือน*	*20-24 ชม.*	*5-6 หลักสูตร*	*3 เรื่อง*	*>3 เรื่อง*	*4-5 ครั้ง*	*3 งาน*
2	**น้อย**	*2ปี*	*>1-3 เดือน*	*25-29 ชม.*	*7-8 หลักสูตร*	*4 เรื่อง*	*>2 เรื่อง*	*2-3 ครั้ง*	*2 งาน*
1	**น้อยมาก**	*≤ 1ปี*	*≤1 เดือน*	*≥30 ชม.*	*≥9 หลักสูตร*	*≥5 เรื่อง*	*≤1 เรื่อง*	*≤1 ครั้ง*	*≤1 งาน*

ตารางที่ 20 แสดงเกณฑ์ประเมินผลกระทบ (Impact : I)

ผลกระทบที่จะเกิด (Impact : I)		I1	I2	I3	I4
ระดับ	**ผลกระทบ**	*ความกว้างของผลกระทบ*	*ความถี่มีเหลว*	*ความล่าช้า*	*มูลค่าความเสียหาย*
5	สูงมาก	*มีผลต่อภายนอกองค์กร*	*≥40 % ตามแผน*	*>6 เดือน*	*>500,000 บาท*
4	สูง	*มีผลในระดับองค์กร*	*31-40 % ตามแผน*	*>4-6 เดือน*	*>100,000-500,000 บาท*
3	ปานกลาง	*มีผลต่อภายในหน่วยงานอื่น*	*21-30 % ตามแผน*	*> 3-4 เดือน*	*> 10,000-100,000 บาท*
2	น้อย	*มีผลเฉพาะภายในหน่วยงาน*	*10-20 % ตามแผน*	*>1-3 เดือน*	*>1,000-10,000 บาท*
1	น้อยมาก	*ไม่มีผลกระทบ*	*≤ 10 % ตามแผน*	*≤1 เดือน*	*≤1,000 บาท*

สำนักงานตรวจสอบภายใน ได้ดำเนินการประเมินความเสี่ยงประกอบด้วย 2 มิติ คือ โอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบของความเสี่ยง (Impact) โดยแสดงเป็นผลคูณของโอกาสและผลกระทบ

คะแนนความเสี่ยง = โอกาส x ผลกระทบ

ตารางที่ 21 แสดงการประเมินโอกาสและผลกระทบของความเสี่ยง

ประเภท		โอกาส (L)	ผลกระทบ (I)	คะแนน
1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : SR)				
SR1	ยุทธศาสตร์/แผนงานไม่สอดคล้องกันระหว่างหน่วยงานกับองค์กร	1	3	**3**
SR2	แผนกลยุทธ์หน่วยงานไม่สามารถนำไปสู่การบรรลุวัตถุประสงค์องค์กร	1	3	**3**
SR3	แผนกลยุทธ์หน่วยงานขาดการพัฒนาจนขาดประสิทธิภาพให้ทันต่อสถานการณ์	1	3	**3**
SR4	การปฏิบัติงานไม่สอดคล้องกับภารกิจ /ยุทธศาสตร์ / นโยบายของหน่วยงาน	1	3	**3**
2) ความเสี่ยงด้านการเงิน (Financial Risk : FR)				
FR1	เบิกจ่ายงบประมาณไม่เป็นไปตามแผน	1	3	**3**
FR2	เบิกจ่ายงบประมาณไม่เป็นไปตามค่าเป้าหมายตามมติคณะรัฐมนตรี (ครม.)	2	3	**6**
FR3	เบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา	1	3	**3**
FR4	งบประมาณไม่เพียงพอ	1	3	**3**
3) ความเสี่ยงด้านการดำเนินงาน (Operation Risk : OR)				
OR1	**การปฏิบัติงานไม่เป็นไปตามแผนงาน**	**3**	**4**	**12**
OR2	ขาดข้อมูลสนับสนุนในการดำเนินงาน	1	4	**4**
OR3	บุคลากรขาดทักษะ ความรู้ ความชำนาญ/ ไม่ทันกับสถานการณ์	1	4	**4**
OR4	บุคลากรไม่สามารถให้คำปรึกษาหรือเป็นวิทยากรได้	2	3	**6**
OR5	ข้อมูลการตรวจนับพัสดุไม่ตรงกัน	1	3	**3**
OR6	การถูกโจมตีทางไซเบอร์ทำให้ข้อมูลสูญหายหรือถูกทำลาย	2	3	6
4) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk : CR)				
CR1	ปฏิบัติผิดกฎระเบียบ	1	2	**2**
CR2	รู้ไม่ทันกฎหมายใหม่	1	3	**3**
CR3	เกิดความเข้าใจผิด / สับสน / การตีความคลาดเคลื่อน	1	2	**2**
CR4	การทุจริต *(ว 105 ข้อ 8)*	1	2	**2**

หมายเหตุ : คะแนนโอกาสของความเสี่ยง (L) มีคะแนนจากผังการประเมินโอกาส (ตารางที่ 22)
คะแนนผลกระทบของความเสี่ยง (I) มีคะแนนจากผังการประเมินผลกระทบ (ตารางที่ 23)
การประเมินทุจริต ดำเนินการตามหลักเกณฑ์การควบคุมภายในสำหรับหน่วยงานของรัฐ'61 (ว 105) ข้อ 8 และเกณฑ์การประเมินความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐ (ปปช.) ซึ่งกล่าวไว้ในหัวข้อการประเมินทุจริต

ตารางที่ 22 แสดงการประเมินโอกาสของความเสี่ยง (Likelihood : L)

Key Risk Indicator (KRI)									
โอกาสที่จะเกิด (Likelihood : L)		**L1**	**L2**	**L3**	**L4**	**L5**	**L6**	**L7**	**L8**
ระดับ	**โอกาส (Likelihood : L)**	**ระยะเวลาไม่ได้ทบทวนแผน**	**เวลาไม่ได้ประชุม/กำกับติดตาม**	**ชั่วโมงฝึกอบรมเฉลี่ย (ตามเกณฑ์)**	**จำนวนการเข้าอบรมหลักสูตรที่เกี่ยวข้อง**	**มีข้อมูลนำเสนอ**	**จำนวนเรื่องที่ไม่ได้อบรม**	**ประวัติการเกิดซ้ำ/โอกาสเกิด**	**จำนวนงานที่ขาดตกบกพร่องตอบทาน**
5	**สูงมาก**	**> 5 ปี**	**> 1 ปี**	≤ 15 ชั่วโมง	≤ 1 หลักสูตร	**≤ 1 เรื่อง**	> 5 เรื่อง	**≥ 8 ครั้ง**	≥ 6 งาน
4	**สูง**	**4 ปี**	> 6 เดือน - 1 ปี	15 – 19 ชั่วโมง	2-4 หลักสูตร	**2 เรื่อง**	> 4 เรื่อง	**6-7 ครั้ง**	**5 งาน**
3	**ปานกลาง**	**3 ปี**	**> 3 - 6 เดือน**	20 – 24 ชั่วโมง	5-6 หลักสูตร	**3 เรื่อง**	> 3 เรื่อง	**4-5 ครั้ง**	**4 งาน**
2	**น้อย**	**2 ปี**	> 1 - 3 เดือน	**25 – 29 ชั่วโมง**	7-8 หลักสูตร	**4 เรื่อง**	> 2 **เรื่อง**	**2-3 ครั้ง**	**3 งาน**
1	**น้อยมาก**	**≤ 1 ปี**	≤ 1 เดือน	≥ 30 ชั่วโมง	≥ 9 หลักสูตร	≥ 5 เรื่อง	≤ 1 เรื่อง	**≤ 1 ครั้ง**	**≤ 1 งาน**
ผลการประเมิน	**คะแนน**								
1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : SR)									
SR1 ยุทธศาสตร์/แผนงานไม่สอดคล้องกันระหว่างหน่วยงานกับองค์กร	1	1							
SR2 แผนกลยุทธ์หน่วยงานไม่สามารถนำไปสู่การบรรลุวัตถุประสงค์องค์กร	1	1							
SR3 แผนกลยุทธ์หน่วยงานขาดการพัฒนาจนขาดประสิทธิภาพให้ทันต่อสถานการณ์	1	1							
SR4 การปฏิบัติงานไม่สอดคล้องกับภารกิจ / ยุทธศาสตร์ / นโยบายของหน่วยงาน	1	1							
2) ความเสี่ยงด้านการเงิน (Financial Risk : FR)									
FR1 เบิกจ่ายงบประมาณไม่เป็นไปตามแผน	1		1					1	
FR2 เบิกจ่ายงบประมาณไม่เป็นไปตามค่า	2		2					2	

Key Risk Indicator (KRI)									
โอกาสที่จะเกิด (Likelihood : L)		L1	L2	L3	L4	L5	L6	L7	L8
ระดับ	โอกาส (Likelihood : L)	ระยะเวลาไม่ได้ทบทวนแผน	เวลาไม่ได้ประชุม/กำกับติดตาม	ชั่วโมงฝึกอบรมเฉลี่ย (ตามเกณฑ์)	จำนวนการเข้าอบรมหลักสูตรที่เกี่ยวข้อง	มีข้อมูลนำเสนอ	จำนวนเรื่องที่ไม่ได้อบรม	ประวัติการเกิดซ้ำ/โอกาสเกิด	จำนวนงานที่ยกเลิกการทบทวน
5	**สูงมาก**	**> 5 ปี**	**> 1 ปี**	≤ 15 ชั่วโมง	≤ 1 หลักสูตร	**≤ 1 เรื่อง**	> 5 เรื่อง	**≥ 8 ครั้ง**	≥ 6 งาน
4	**สูง**	**4 ปี**	> 6 เดือน - 1 ปี	15 – 19 ชั่วโมง	2-4 หลักสูตร	**2 เรื่อง**	> 4 เรื่อง	**6-7 ครั้ง**	**5 งาน**
3	**ปานกลาง**	**3 ปี**	**> 3 - 6 เดือน**	20 – 24 ชั่วโมง	5-6 หลักสูตร	**3 เรื่อง**	> 3 เรื่อง	**4-5 ครั้ง**	**4 งาน**
2	**น้อย**	**2 ปี**	> 1 - 3 เดือน	**25 – 29 ชั่วโมง**	7-8 หลักสูตร	**4 เรื่อง**	> 2 **เรื่อง**	**2-3 ครั้ง**	**3 งาน**
1	**น้อยมาก**	**≤ 1 ปี**	≤ 1 เดือน	≥ 30 ชั่วโมง	≥ 9 หลักสูตร	≥ 5 เรื่อง	≤ 1 เรื่อง	**≤ 1 ครั้ง**	**≤ 1 งาน**
ผลการประเมิน	**คะแนน**								
เป้าหมายตามมติคณะรัฐมนตรี (ครม.)									
FR3 เบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา	1		1					1	
FR4 งบประมาณไม่เพียงพอ	1		1					1	
3) ความเสี่ยงด้านการดำเนินงาน (Operation Risk : OR)									
OR1 การปฏิบัติงานไม่เป็นไปตามแผนงาน	3							3	
OR2 ขาดข้อมูลสนับสนุนในการดำเนินงาน	1		1					1	
OR3 บุคลากรขาดทักษะ ความรู้ ความชำนาญ / ไม่ทันกับสถานการณ์	1			1					
OR4 บุคลากรไม่สามารถให้คำปรึกษาหรือเป็นวิทยากรได้	2				2	2			
OR6 ข้อมูลการตรวจนับพัสดุไม่ตรงกัน	1							1	
OR6 การถูกโจมตีทางไซเบอร์ทำให้ข้อมูลสูญ	2							2	

Key Risk Indicator (KRI)									
โอกาสที่จะเกิด (Likelihood : L)		L1	L2	L3	L4	L5	L6	L7	L8
ระดับ	โอกาส (Likelihood : L)	ระยะเวลาไม่ได้ทบทวนแผน	เวลาไม่ได้ประชุม/กำกับติดตาม	ชั่วโมงฝึกอบรมเฉลี่ย (ตามเกณฑ์)	จำนวนการเข้าอบรมหลักสูตรที่เกี่ยวข้อง	มีข้อมูลน้ำเสนอ	จำนวนเรื่องที่ไม่ได้รายงาน	ประวัติการเกิดซ้ำ/โอกาสเกิด	จำนวนงานที่ยังไม่ได้ทบทวนตอบ
5	**สูงมาก**	**> 5 ปี**	**> 1 ปี**	≤ 15 ชั่วโมง	≤ 1 หลักสูตร	**≤ 1 เรื่อง**	> 5 เรื่อง	**≥ 8 ครั้ง**	≥ 6 งาน
4	**สูง**	**4 ปี**	> 6 เดือน - 1 ปี	15 – 19 ชั่วโมง	2-4 หลักสูตร	**2 เรื่อง**	> 4 เรื่อง	**6-7 ครั้ง**	**5 งาน**
3	**ปานกลาง**	**3 ปี**	**> 3 - 6 เดือน**	20 – 24 ชั่วโมง	5-6 หลักสูตร	**3 เรื่อง**	> 3 เรื่อง	**4-5 ครั้ง**	**4 งาน**
2	**น้อย**	**2 ปี**	> 1 - 3 เดือน	**25 – 29 ชั่วโมง**	7-8 หลักสูตร	**4 เรื่อง**	> 2 **เรื่อง**	**2-3 ครั้ง**	**3 งาน**
1	**น้อยมาก**	**≤ 1 ปี**	≤ 1 เดือน	≥ 30 ชั่วโมง	≥ 9 หลักสูตร	≥ 5 เรื่อง	≤ 1 เรื่อง	**≤ 1 ครั้ง**	**≤ 1 งาน**
ผลการประเมิน	**คะแนน**								
หายหรือถูกทำลาย									
4) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk : CR)									
CR1 ปฏิบัติผิดกฎระเบียบ	1							1	
CR2 รู้ไม่ทันกฎหมายใหม่	1						1		
CR3 เกิดความเข้าใจผิด / สับสน / การตีความคลาดเคลื่อน	1			1				1	
CR4 การทุจริต *(ว 105 ข้อ 8)*	1							1	1

ตารางที่ 23 แสดงการประเมินผลกระทบของความเสี่ยง (Impact : I)

ความรุนแรงผลกระทบที่จะเกิด (Impact : I)		ระดับนัยสำคัญ (Level of Significance)			
		I1	I2	I3	I4
ระดับ	ผลกระทบ	ความกว้างผลกระทบ	ความล้มเหลว	ความล่าช้า	ความเสียหาย
5	สูงมาก	มีผลต่อภายนอกองค์กร	> 40% ตามแผน	> 6 เดือน	> 500,000 บาท
4	สูง	มีผลในระดับองค์กร	31 - 40% ตามแผน	> 4 - 6 เดือน	> 100,000 - 500,000
3	ปานกลาง	มีผลในหน่วยงานอื่นๆ	21 - 30% ตามแผน	> 3 - 4 เดือน	> 10,000 - 100,000
2	น้อย	มีผลเฉพาะภายในหน่วยงาน	10 - 20% ตามแผน	> 1 - 3 เดือน	> 1,000 - 10,000
1	น้อยมาก	ไม่มีผลกระทบ	< 10% ตามแผน	≤ 1 เดือน	≤ 1,000
ผลการประเมิน	**คะแนน**				
1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : SR)					
SR1 ยุทธศาสตร์/แผนงานไม่สอดคล้องกันระหว่างหน่วยงานกับองค์กร	**3**	3			
SR2 แผนกลยุทธ์หน่วยงานไม่สามารถนำไปสู่การบรรลุวัตถุประสงค์องค์กร	**3**	3			
SR3 แผนกลยุทธ์หน่วยงานขาดการพัฒนาจนขาดประสิทธิภาพให้ทันต่อสถานการณ์	**3**	3			
SR4 การปฏิบัติงานไม่สอดคล้องกับภารกิจ / ยุทธศาสตร์ / นโยบายของหน่วยงาน	**3**	3			
2) ความเสี่ยงด้านการเงิน (Financial Risk : FR)					
FR1 เบิกจ่ายงบประมาณไม่เป็นไปตามแผน	**3**	3	3		
FR2 เบิกจ่ายงบประมาณไม่เป็นไปตามค่าเป้าหมายตามมติคณะรัฐมนตรี (ครม.)	**3**	3	3		
FR3 เบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา	**3**	3	3		
FR4 งบประมาณไม่เพียงพอ	**3**	3	3		
3) ความเสี่ยงด้านการดำเนินงาน (Operation Risk : OR)					

ความรุนแรงผลกระทบที่จะเกิด (Impact : I)		ระดับนัยสำคัญ (Level of Significance)			
		I1	I2	I3	I4
ระดับ	ผลกระทบ	ความกว้างผลกระทบ	ความล้มเหลว	ความล่าช้า	ความเสียหาย
5	สูงมาก	มีผลต่อภายนอกองค์กร	> 40% ตามแผน	> 6 เดือน	> 500,000 บาท
4	สูง	มีผลในระดับองค์กร	31 - 40% ตามแผน	> 4 - 6 เดือน	> 100,000 - 500,000
3	ปานกลาง	มีผลในหน่วยงานอื่นๆ	21 - 30% ตามแผน	> 3 - 4 เดือน	> 10,000 - 100,000
2	น้อย	มีผลเฉพาะภายในหน่วยงาน	10 - 20% ตามแผน	> 1 - 3 เดือน	> 1,000 - 10,000
1	น้อยมาก	ไม่มีผลกระทบ	< 10% ตามแผน	≤ 1 เดือน	≤ 1,000
ผลการประเมิน	**คะแนน**				
OR1 การปฏิบัติงานไม่เป็นไปตามแผนงาน	**4**	4	4	4	
OR2 ขาดข้อมูลสนับสนุนในการดำเนินงาน	**3**	3	3	3	
OR3 บุคลากรขาดทักษะ ความรู้ ความชำนาญ / ไม่ทันกับสถานการณ์	**4**	4	4	4	
OR4 บุคลากรไม่สามารถให้คำปรึกษาหรือเป็นวิทยากรได้	**3**	3	3		
OR5 ข้อมูลการตรวจนับพัสดุไม่ตรงกัน	**3**	3			
OR6 การถูกโจมตีทางไซเบอร์ทำให้ข้อมูลสูญหายหรือถูกทำลาย	3	3	3	3	
4) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk : CR)					
CR1 ปฏิบัติผิดกฎระเบียบ	**2**	2			
CR2 รู้ไม่ทันกฎหมายใหม่	**3**	3			
CR3 เกิดความเข้าใจผิด /สับสน /การตีความคลาดเคลื่อน	**2**	2			
CR4 การทุจริต *(ว 105 ข้อ 8)*	**2**	2			2

4.3 การวิเคราะห์ความเสี่ยง

สำนักงานตรวจสอบภายใน ได้วิเคราะห์ความเสี่ยง โดยประเมินความเสี่ยงทั้งสี่ประเภทออกมาเป็นระดับความเสี่ยง 4 ระดับ ได้แก่ 🔴 สูงมาก 🟠 สูง 🟡 ปานกลาง 🟢 ต่ำ ซึ่งเป็นไปตามเกณฑ์การกำหนดระดับความเสี่ยงดังกล่าวข้างต้น

ตารางที่ 24 แสดงการวิเคราะห์ความเสี่ยง

ประเภท		โอกาส (L)	ผลกระทบ (I)	คะแนน	ระดับ
1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : SR)					
SR1	ยุทธศาสตร์/แผนงานไม่สอดคล้องกันระหว่างหน่วยงานกับองค์กร	1	3	**3**	ต่ำ
SR2	แผนกลยุทธ์หน่วยงานไม่สามารถนำไปสู่การบรรลุวัตถุประสงค์องค์กร	1	3	**3**	ต่ำ
SR3	แผนกลยุทธ์หน่วยงานขาดการพัฒนาจนขาดประสิทธิภาพให้ทันต่อสถานการณ์	1	3	**3**	ต่ำ
SR4	การปฏิบัติงานไม่สอดคล้องกับภารกิจ /ยุทธศาสตร์ / นโยบายของหน่วยงาน	1	3	**3**	ต่ำ
2) ความเสี่ยงด้านการเงิน (Financial Risk : FR)					
FR1	เบิกจ่ายงบประมาณไม่เป็นไปตามแผน	1	3	**3**	ต่ำ
FR2	เบิกจ่ายงบประมาณไม่เป็นไปตามค่าเป้าหมายตามมติคณะรัฐมนตรี	2	3	**6**	ปานกลาง
FR3	เบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา	1	3	**3**	ต่ำ
FR4	งบประมาณไม่เพียงพอ	1	3	**3**	ต่ำ
3) ความเสี่ยงด้านการดำเนินงาน (Operation Risk : OR)					
OR1	การปฏิบัติงานไม่เป็นไปตามแผนงาน	3	4	**12**	สูง
OR2	ขาดข้อมูลสนับสนุนในการดำเนินงาน	1	3	**3**	ต่ำ
OR3	บุคลากรขาดทักษะ ความรู้ ความชำนาญ/ ไม่ทันกับสถานการณ์	1	4	**4**	ปานกลาง
OR4	บุคลากรไม่สามารถให้คำปรึกษาหรือเป็นวิทยากรได้	2	3	**6**	ปานกลาง
OR5	ข้อมูลการตรวจนับพัสดุไม่ตรงกัน	1	3	**3**	ต่ำ
OR6	การถูกโจมตีทางไซเบอร์ทำให้ข้อมูลสูญหายหรือถูกทำลาย	2	3	**6**	ปานกลาง
4) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk : CR)					
CR1	ปฏิบัติผิดกฎระเบียบ	1	2	**2**	ต่ำ
CR2	รู้ไม่ทันกฎหมายใหม่	1	3	**3**	ต่ำ
CR3	เกิดความเข้าใจผิด / สับสน / การตีความคลาดเคลื่อน	1	2	**2**	ต่ำ
CR4	การทุจริต *(ว 105 ข้อ 8)*	1	2	**2**	ต่ำ

หมายเหตุ : คะแนนโอกาสของความเสี่ยง (L) มีคะแนนจากผังการประเมินโอกาส (ตารางที่ 22)
คะแนนผลกระทบของความเสี่ยง (I) มีคะแนนจากผังการประเมินผลกระทบ (ตารางที่ 23)

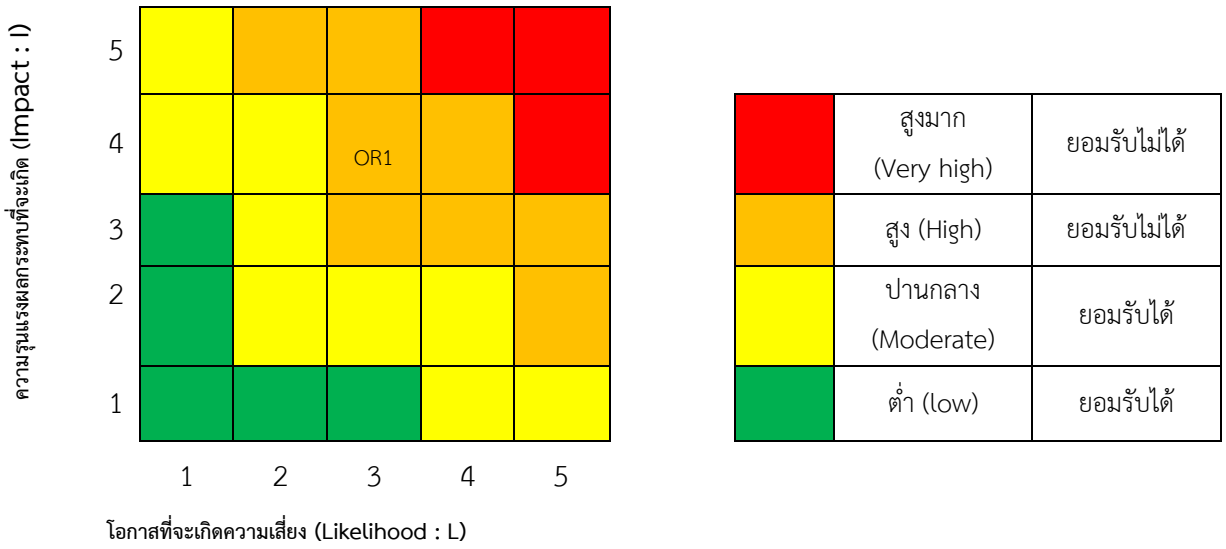
4.4 การจัดลำดับความเสี่ยง

หลังจากการวิเคราะห์ความเสี่ยงแล้ว สำนักงานตรวจสอบภายใน ได้การจัดลำดับความเสี่ยง เพื่อให้หน่วยงานสามารถจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงาน และ

สามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดยพิจารณาจากระดับคะแนนความเสี่ยง ดังตารางข้างล่างนี้

ตารางที่ 25 แสดงการจัดลำดับความเสี่ยง

ประเภท	โอกาส (L)	ผลกระทบ (I)	คะแนน	ระดับ	ลำดับ
3) ความเสี่ยงด้านการดำเนินงาน (Operation Risk : OR)					
OR1 การปฏิบัติงานไม่เป็นไปตามแผนงาน	**3**	**4**	**12**	**สูง**	**1**



ภาพที่ 46 การจัดลำดับความเสี่ยง

5. การตอบสนองความเสี่ยง

5.1 การประเมินมาตรการควบคุมภายใน (Risk Control)

สำนักงานตรวจสอบภายใน ได้ดำเนินการประเมินมาตรการควบคุมภายในตามปัจจัยเสี่ยงแต่ละรายการ เพื่อประเมินประสิทธิภาพการควบคุมภายในที่เป็นอยู่ในปัจจุบันว่าเป็นอย่างไรและกำหนดวิธีการบริหารจัดการควบคุมความเสี่ยงเพิ่มเติม เพื่อเพิ่มประสิทธิภาพประสิทธิผลในการตอบสนองความเสี่ยงยิ่งขึ้น (ตารางที่ 26)

ตารางที่ 26 แสดงการประเมินมาตรการควบคุมภายใน

ปัจจัยเสี่ยง (1)	การควบคุมที่ควรจัดทำ (2)	การควบคุมในปัจจุบัน (3)	ผลการประเมินการควบคุมในปัจจุบัน (4)	การควบคุมที่ควรทำเพิ่มเติม (5)
OR1 การปฏิบัติงานไม่เป็นไปตามแผนงาน				
OR1.1 สำนักงานตรวจสอบภายในไม่ได้รับข้อมูลตามแผนที่กำหนด	1) แผนสำรองข้อมูลจากหน่วยงานที่เกี่ยวข้อง 2) ปรับแผนการดำเนินงาน 3) เร่งรัดประสานอย่างต่อเนื่อง	✓	?	จัดให้มีการดำเนินการตาม (2)
OR1.2 เกิดสถานการณ์ไม่คาดคิด ทำให้ไม่สามารถดำเนินงานปกติได้	นำเทคโนโลยีเข้ามาใช้ในการปฏิบัติงานออนไลน์	✓	?	จัดให้มีการดำเนินการตาม (2)

หมายเหตุ : ความหมายของสัญลักษณ์ในช่อง (3) และ (4)

ช่อง (3) √ : มี x : ไม่มี ? : มีแต่ไม่ได้ปฏิบัติ

ช่อง (4) √ : ได้ผล x : ไม่ได้ผล ? : ได้ผลบ้างแต่ไม่สมบูรณ์

5.2 การจัดการความเสี่ยง

สำนักงานตรวจสอบภายใน ได้ดำเนินการจัดการความเสี่ยง (Risk Treatment) โดยทำ 2 ขั้นตอนย่อย ได้แก่ การประเมินทางเลือกการบริหารความเสี่ยง และแผนบริหารความเสี่ยงสำนักงานตรวจสอบภายใน

ภาพที่ 47 กลยุทธ์การจัดการความเสี่ยง 4T's Strategie

ตารางที่ 27 การประเมินทางเลือกการบริหารความเสี่ยง

ความเสี่ยง/ปัจจัยเสี่ยง	กลยุทธ์	วิธีการจัดการความเสี่ยง	ต้นทุน	ผลประโยชน์	สรุปทางเลือกที่เหมาะสม
(1) OR1 การปฏิบัติงานไม่เป็นไปตามแผนงาน					
OR1.1 สำนักงานตรวจสอบภายในไม่ได้รับข้อมูลตามแผนที่กำหนด	หลีก	• ไม่สามารถหลีกเลี่ยงได้ เนื่องจากส่งผลกระทบต่อการปฏิบัติงานตามแผนงานฯ อย่างมาก	-	-	-
	ยอม	• ไม่สามารถยอมได้ เนื่องจากส่งผลกระทบต่อการปฏิบัติงานตามแผนงานฯ อย่างมาก	-	-	-
	ลด	1) แผนสำรองข้อมูลจากหน่วยงานที่เกี่ยวข้อง 3) ปรับแผนการดำเนินงาน 4) เร่งรัดประสานอย่างต่อเนื่อง	ไม่เสียค่าใช้จ่ายในการดำเนินงาน	เพิ่มการปฏิบัติงานตามแผนงานและบรรลุเป้าหมายอย่างมีประสิทธิภาพ	✅
	ร่วม	• ไม่เลือก เนื่องจากการดำเนินงานตามแผนงานภายในของหน่วยงาน	-	-	-

ความเสี่ยง/ปัจจัยเสี่ยง	กลยุทธ์	วิธีการจัดการความเสี่ยง	ต้นทุน	ผลประโยชน์	สรุปทางเลือกที่เหมาะสม
OR1.2 เกิดสถานการณ์ไม่คาดคิด ทำให้ไม่สามารถดำเนินงานปกติได้	หลีก	• ไม่สามารถหลีกเลี่ยงได้ เนื่องจากส่งผลกระทบต่อการจัดทำแผนงานฯ อย่างมาก	-	-	-
	ยอม	• ไม่สามารถยอมได้ เนื่องจากส่งผลกระทบต่อการจัดทำแผนงานฯ อย่างมาก	-	-	-
	ลด	• นำเทคโนโลยีเข้ามาใช้ในการปฏิบัติงานออนไลน์	อาจมีค่าใช้จ่ายในการดำเนินงานบ้าง	เพิ่มการปฏิบัติงานตามแผนงานและบรรลุเป้าหมายอย่างมีประสิทธิภาพ	✅
	ร่วม	• ไม่เลือก เนื่องจากการดำเนินงานตามแผนงานภายในของหน่วยงาน	-	-	-

ตารางที่ 28 แผนบริหารความเสี่ยงสำนักงานตรวจสอบภายใน ปีงบประมาณ 2567

ลำดับ	ความเสี่ยง	ปัจจัยเสี่ยง	กลยุทธ์จัดการความเสี่ยง				กิจกรรมการจัดการความเสี่ยง	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ
			ยอม	ลด	หลีก	ร่วม			
1.	OR1 การปฏิบัติงานไม่เป็นไปตามแผนงาน	OR1.1 สำนักงานตรวจสอบภายในไม่ได้รับข้อมูลตามแผนที่กำหนด		✓			1) แผนสำรองข้อมูลจากหน่วยงานที่เกี่ยวข้อง 3) ปรับแผนการดำเนินงาน 4) เร่งรัดประสานอย่างต่อเนื่อง	ต.ค.2566 ถึง ก.ย. 2567	คณะกรรมการฯ
		OR1.2 เกิดสถานการณ์ไม่คาดคิดทำให้ไม่สามารถดำเนินงานปกติได้		✓			นำเทคโนโลยีเข้ามาใช้ในการปฏิบัติงานออนไลน์	ต.ค.2566 ถึง ก.ย. 2567	คณะกรรมการฯ

หมายเหตุ : คณะกรรมการฯ หมายถึง คณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน สำนักงานตรวจสอบภายใน

6. การติดตามและทบทวน

สำนักงานตรวจสอบภายใน ได้กำหนดให้มีการติดตามความเสี่ยงเป็นระยะๆ และทบทวนประเด็นความเสี่ยง กระบวนการดำเนินงาน เพื่อให้เกิดความเชื่อมั่นในการบริหารจัดการความเสี่ยงยังคงมีประสิทธิภาพ สามารถกำจัดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ นำไปสู่การบรรลุเป้าหมายตามมาตรฐานหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ข้อ 2.7 หน่วยงานของรัฐต้องมีการติดตามประเมิลการบริหารจัดการความเสี่ยงและทบทวนแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ และหลักเกณฑ์ฯ ข้อ 8 ให้ฝ่ายบริหารและผู้รับผิดชอบต้องจัดให้มีการติดตามประเมินผลการบริหารจัดการความเสี่ยง โดยติดตามประเมินผลอย่างต่อเนื่องในระหว่างปฏิบัติงานหรือติดตามประเมินผลเป็นรายครั้ง หรือใช้ทั้งสองวิธีร่วมกัน กรณีพบข้อพกพร่องที่มีสาระสำคัญให้รายงานทันที โดยมีวัตถุประสงค์และกำหนดให้ดำเนินการติดตามและทบทวนการบริหารจัดการความเสี่ยง (ตารางที่ 29) ดังนี้

วัตถุประสงค์การติดตามและทบทวน

1) เพื่อให้ผู้บริหารและผู้ที่เกี่ยวข้องได้รับทราบ และตระหนักถึงความเสี่ยงขององค์กร/หน่วยงานที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร และพิจารณาแก้ไขได้อย่างทันท่วงที
2) เพื่อให้มั่นใจว่าความเสี่ยงได้รับการจัดการตามแผนงานที่วางไว้
3) เพื่อประเมินว่าแผนการจัดการความเสี่ยงยังสามารถใช้ดำเนินการในสถานการณ์ปัจจุบัน

ตารางที่ 29 แสดงวิธีการดำเนินงานติดตามและทบทวน

ข้อ	วิธีการดำเนินงาน	กำหนดการ
1) การติดตาม	ติดตามผลการดำเนินการโดยนำเข้าที่ประชุมประจำเดือนทุกครั้งที่มีการประชุม	ต.ค.2566 – ก.ย. 2567
2) การทบทวน	กำหนดให้มีการทบทวนแผนการบริหารจัดการความเสี่ยงทุกปีตามโครงการทบทวนแผนยุทธศาสตร์และแผนปฏิบัติการประจำปี	ไตรมาสที่ 2 หรือ 3 (1 ม.ค. - มิ.ย.2567)

7. การสื่อสารและรายงานผล

สำนักงานตรวจสอบภายใน ได้ร่วมกันในนามของคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน ดำเนินการจัดทำแผนการบริหารจัดการความเสี่ยง รอบปีงบประมาณ 2567 และทุกคนได้รับการสื่อสารวัตถุประสงค์ของแผนการดำเนินการที่จะเป็นแนวทางในการบริหารความเสี่ยง ให้เกิดความตระหนัก ความเข้าใจและการมีส่วนร่วมในการบริหารจัดการความเสี่ยงทุกระดับ ให้เป็นไปตามมาตรฐานหลักเกณฑ์การปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ข้อ 2.3 และข้อ 2.6 ในการสื่อสารวัตถุประสงค์และแผนการบริหารความเสี่ยง เป็นไปในทิศทางเดียวกันนำไปสู่การบรรลุเป้าหมายอย่างมีประสิทธิภาพ

ตลอดจนการรายงานผลการบริหารจัดการความเสี่ยง เมื่อสิ้นปีงบประมาณ ให้ผู้บริหารหารหรือคณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายในระดับมหาวิทยาลัยรับทราบผลการดำเนินงาน หรือสั่งการให้มีการดำเนินการอย่างใดอย่างหนึ่ง และเป็นไปตามตามมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานภาครัฐ พ.ศ. 2562 (ว 23) ข้อ 9 ให้ผู้รับผิดชอบของหน่วยงานของรัฐจัดทำรายงานผลการบริหารจัดการความเสี่ยงและเสนอให้หัวหน้าหน่วยงานของรัฐหรือผู้กำกับดูแลแล้วแต่กรณี พิจารณาอย่างน้อยปีละ 1 ครั้ง โดยกำหนดให้มีการรายงาน (ตารางที่ 30) ดังนี้

ตารางที่ 30 แสดงแผนการรายงานผลการบริหารจัดการความเสี่ยง รอบปีงบประมาณ 2567

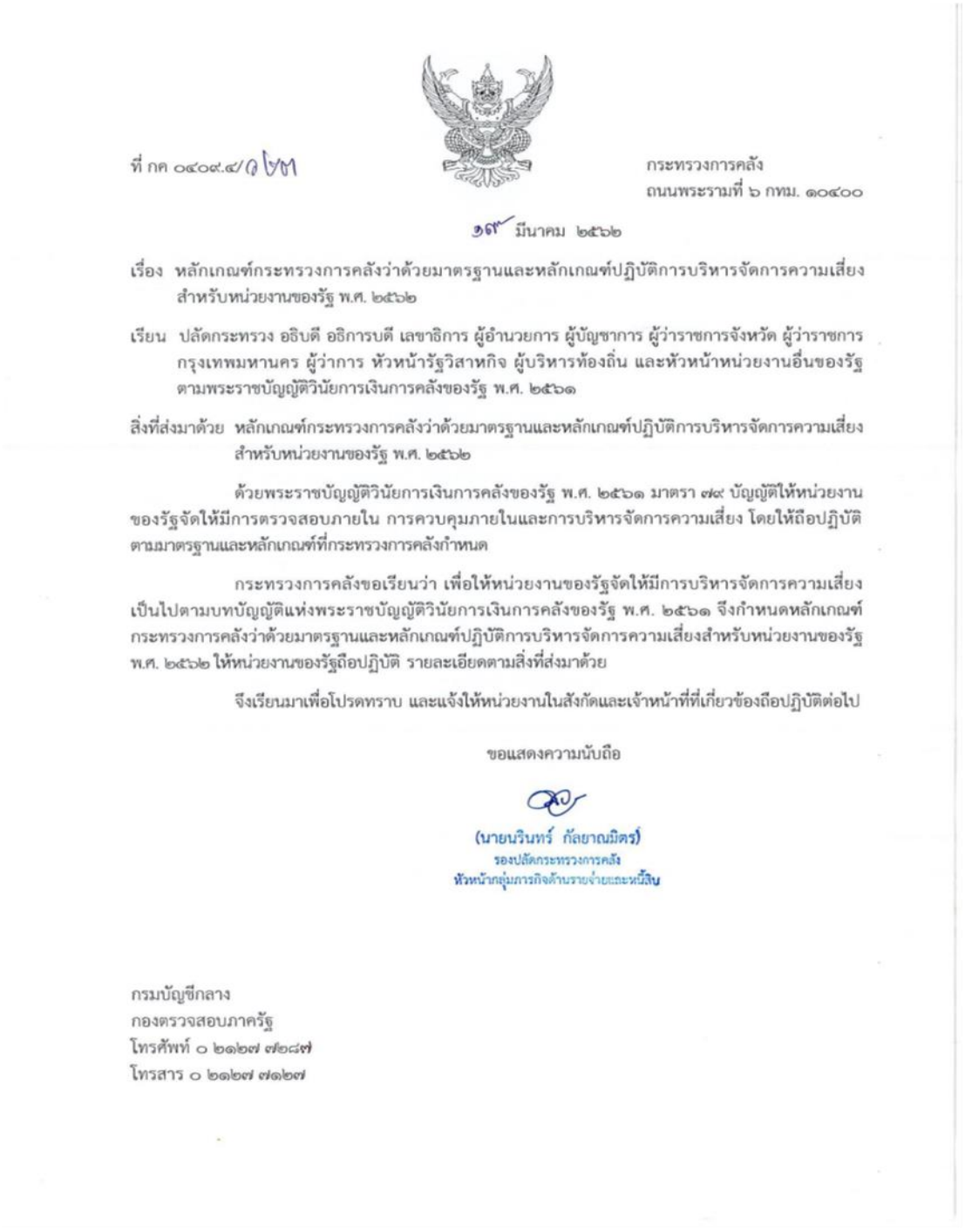
ประเด็น	ข้อปฏิบัติ	กำหนดการ
☞**การรายงาน**	การรายงานปีละ 1 ครั้ง ณ สิ้นปี รอบปีงบประมาณ 2567	ภายใน ต.ค.-ธ.ค.2567
☞**รูปแบบการรายงาน**	รูปแบบการรายงาน รายงานในลักษณะรูปเล่ม เพื่อนำเสนอรายงานต่ออธิการบดี ประธานคณะกรรมการฯ	ภายใน ต.ค.-ธ.ค.2567

ภาคผนวก

ภาคผนวก ก.

หลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562

(ว 23)



ที่ กค ๐๔๐๙.๔/ว ๒๗

กระทรวงการคลัง
ถนนพระรามที่ ๖ กทม. ๑๐๔๐๐

๑๙ มีนาคม ๒๕๖๒

เรื่อง หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒

เรียน ปลัดกระทรวง อธิบดี อธิการบดี เลขาธิการ ผู้อำนวยการ ผู้บัญชาการ ผู้ว่าราชการจังหวัด ผู้ว่าราชการกรุงเทพมหานคร ผู้ว่าการ หัวหน้ารัฐวิสาหกิจ ผู้บริหารท้องถิ่น และหัวหน้าหน่วยงานอื่นของรัฐตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑

สิ่งที่ส่งมาด้วย หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒

ด้วยพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ มาตรา ๗๙ บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

กระทรวงการคลังขอเรียนว่า เพื่อให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการความเสี่ยงเป็นไปตามบทบัญญัติแห่งพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ จึงกำหนดหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒ ให้หน่วยงานของรัฐถือปฏิบัติ รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดทราบ และแจ้งให้หน่วยงานในสังกัดและเจ้าหน้าที่ที่เกี่ยวข้องถือปฏิบัติต่อไป

ขอแสดงความนับถือ

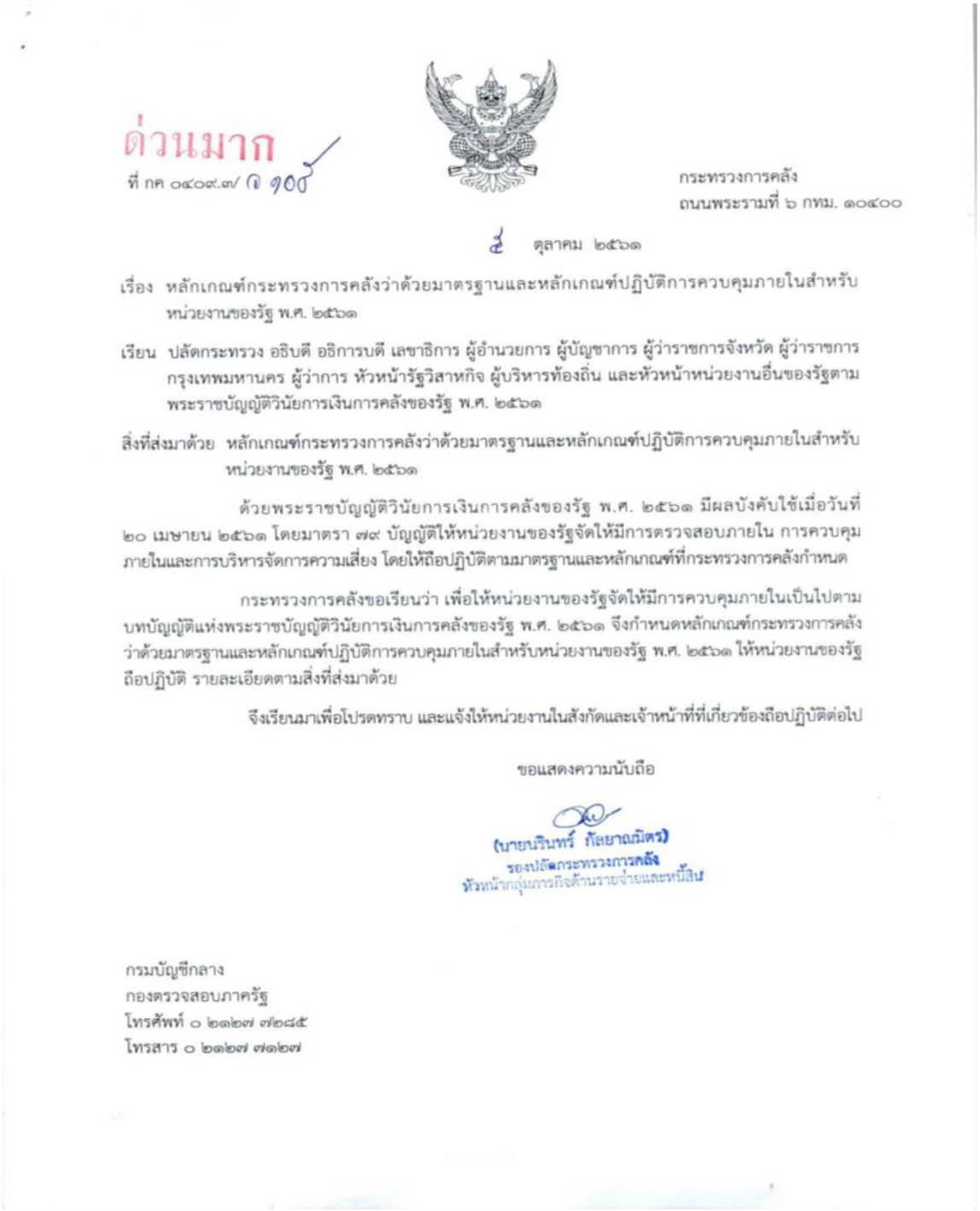
(นายนรินทร์ กัลยาณมิตร)
รองปลัดกระทรวงการคลัง
หัวหน้ากลุ่มภารกิจด้านรายจ่ายและหนี้สิน

กรมบัญชีกลาง
กองตรวจสอบภาครัฐ
โทรศัพท์ ๐ ๒๑๒๗ ๗๒๘๗
โทรสาร ๐ ๒๑๒๗ ๗๑๒๗

อ่านเพิ่มเติมได้ที่ลิงค์ ☞ https://drive.google.com/file/d/1zIRRqmh8MrOHl_eO-iC3-ST4CexDJnyd/view?usp=sharing

ภาคผนวก ข.

หลักเกณฑ์กระทรวงการคลังว่าด้วย มาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายใน สำหรับหน่วยงานของรัฐ พ.ศ. 2561 (ว 105)



ด่วนมาก
ที่ กค ๐๔๐๙.๓/ ว ๑๐๕

กระทรวงการคลัง
ถนนพระรามที่ ๖ กทม. ๑๐๔๐๐

๕ ตุลาคม ๒๕๖๑

เรื่อง หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

เรียน ปลัดกระทรวง อธิบดี อธิการบดี เลขาธิการ ผู้อำนวยการ ผู้บัญชาการ ผู้ว่าราชการจังหวัด ผู้ว่าราชการกรุงเทพมหานคร ผู้ว่าการ หัวหน้ารัฐวิสาหกิจ ผู้บริหารท้องถิ่น และหัวหน้าหน่วยงานอื่นของรัฐตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑

สิ่งที่ส่งมาด้วย หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

ด้วยพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ มีผลบังคับใช้เมื่อวันที่ ๒๐ เมษายน ๒๕๖๑ โดยมาตรา ๗๙ บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

กระทรวงการคลังขอเรียนว่า เพื่อให้หน่วยงานของรัฐจัดให้มีการควบคุมภายในเป็นไปตามบทบัญญัติแห่งพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ จึงกำหนดหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ ให้หน่วยงานของรัฐถือปฏิบัติ รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดทราบ และแจ้งให้หน่วยงานในสังกัดและเจ้าหน้าที่ที่เกี่ยวข้องถือปฏิบัติต่อไป

ขอแสดงความนับถือ

(นายนรินทร์ กัลยาณมิตร)
รองปลัดกระทรวงการคลัง
หัวหน้ากลุ่มภารกิจด้านรายจ่ายและหนี้สิน

กรมบัญชีกลาง
กองตรวจสอบภาครัฐ
โทรศัพท์ ๐ ๒๑๒๗ ๗๒๘๕
โทรสาร ๐ ๒๑๒๗ ๗๑๒๗

อ่านเพิ่มเติมได้ที่ลิงค์ ☞

https://drive.google.com/file/d/15YeecNFyQfvi0zy62uJ7fB_2YB4I0ERl/view?usp=sharing

ภาคผนวก ค.

แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ (ว 36)

ที่ กค ๐๔๐๙.๓/ ว ๓๖ กระทรวงการคลัง
ถนนพระรามที่ ๖ กทม. ๑๐๔๐๐

๓ กุมภาพันธ์ ๒๕๖๔

เรื่อง แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร

เรียน ปลัดกระทรวง อธิบดี อธิการบดี เลขาธิการ ผู้อำนวยการ ผู้บัญชาการ ผู้ว่าราชการจังหวัด ผู้ว่าราชการกรุงเทพมหานคร ผู้ว่าการ ผู้บริหารท้องถิ่น และหัวหน้าหน่วยงานอื่นของรัฐตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑

อ้างถึง หนังสือกระทรวงการคลัง ที่ กค ๐๔๐๙.๔/ว ๒๓ ลงวันที่ ๑๙ มีนาคม ๒๕๖๒

สิ่งที่ส่งมาด้วย แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร จำนวน ๑ เล่ม

ตามหนังสือที่อ้างถึง กระทรวงการคลังได้ประกาศหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒ โดยหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ข้อ ๓ กำหนดให้หน่วยงานของรัฐยกเว้นรัฐวิสาหกิจถือปฏิบัติตามคู่มือหรือแนวทางปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงตามที่กระทรวงการคลังกำหนด นั้น

กระทรวงการคลังขอเรียนว่า หน่วยงานของรัฐมีหน้าที่ในการจัดให้มีการบริหารจัดการความเสี่ยงตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด ตามมาตรา ๗๙ ของพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ เพื่อให้การบริหารจัดการความเสี่ยงของหน่วยงานมีประสิทธิภาพ รวมถึงยกระดับการบริหารจัดการความเสี่ยงของฝ่ายบริหารให้สามารถเป็นเครื่องมือที่สำคัญในการตัดสินใจเชิงกลยุทธ์ (Informed Strategic Decision Making) เพื่อสนับสนุนการบริหารหน่วยงานของรัฐให้บรรลุวัตถุประสงค์ขององค์กรอย่างแท้จริง กระทรวงการคลังจึงได้กำหนดแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กรขึ้น รายละเอียดตามสิ่งที่ส่งมาด้วย โดยหน่วยงานของรัฐสามารถนำหลักการดังกล่าวไปปรับใช้ในการพัฒนาระบบการบริหารจัดการความเสี่ยงให้เหมาะสมกับหน่วยงาน ทั้งนี้ ท่านสามารถดาวน์โหลดแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

เรื่อง....

อ่านเพิ่มเติมได้ที่ลิงค์ ☞

https://drive.google.com/file/d/1waPy_GfxAo4HvkKnCdEABm0xOLvJlJ7l/view?usp=sharing

ภาคผนวก ง.

คำสั่งสำนักงานตรวจสอบภายใน เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน

คำสั่ง สำนักงานตรวจสอบภายใน
ที่ 1/2566
เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน

ด้วยพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 หมวด 4 การบัญชี การรายงานและการตรวจสอบ มาตรา 79 ได้กำหนดให้หน่วยงานของรัฐให้มีการตรวจสอบภายใน และการควบคุมภายในและการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด ซึ่งได้กำหนดหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานภาครัฐ พ.ศ. 2561 และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ.2562 ข้อ 2.4 การบริหารจัดการความเสี่ยงต้องดำเนินการในทุกระดับของหน่วยงานของรัฐ

ดังนั้น เพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าวข้างต้น สำนักงานตรวจสอบภายในจึงดำเนินการบริหารจัดการความเสี่ยงในระดับหน่วยงาน จึงยกเลิกคำสั่งสำนักงานตรวจสอบภายใน ที่ 9/2562 เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน สั่ง ณ วันที่ 1 ตุลาคม 2562 และแต่งตั้งผู้มีรายนามดังต่อไปนี้เป็นคณะกรรมการดำเนินการบริหารความเสี่ยงและควบคุมภายในของสำนักงานตรวจสอบภายใน ดังนี้

1.	นางสาวอรวราวัลย์	สุนิพัฒน์	ประธานกรรมการ
2.	นางสาวจันทนา	พรมแสน	กรรมการ
3.	นางสาวอัมพวา	จินสินจ้อย	กรรมการ
4.	นายประชา	ทองนา	กรรมการ
5.	นายสุวิทย์	วิมุตติโพธิ์	กรรมการและเลขานุการ

โดยให้คณะกรรมการมีหน้าที่ความรับผิดชอบ ดังนี้

1. จัดทำแผนการบริหารจัดการความเสี่ยง
2. ติดตามประเมินผลการบริหารจัดการความเสี่ยง
3. จัดทำรายงานผลตามแผนการบริหารจัดการความเสี่ยง
4. พิจารณาทบทวนแผนการบริหารจัดการความเสี่ยง
5. จัดให้มีระบบการควบคุมภายใน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ 15 มีนาคม พ.ศ. 2566

(นางสาวอรวราวัลย์ สุนิพัฒน์)
ผู้อำนวยการสำนักงานตรวจสอบภายใน

คู่มือการบริหารความเสี่ยง และแผนการบริหารความเสี่ยง

Risk Management Guide & Risk management plan

รอบปีงบประมาณ 2567

ที่ปรึกษา

รองศาสตราจารย์ ดร.ชาตรี มณีโกศล

รักษาการแทนอธิการบดีมหาวิทยาลัยราชภัฏเชียงใหม่

คณะทำงาน

นางสาวอรวรารัศมิ์ สุนิพัฒน์

ผู้อำนวยการสำนักงานตรวจสอบภายใน

นายสุวิทย์ วิมุตติโพธิ์

นางสาวอัมพวา รินสินจ้อย

นางสาวจันทนา พรมเสน

นายประชา ทองนา

จัดทำ เรียบเรียงข้อมูล / รูปเล่ม / ปก

นายสุวิทย์ วิมุตติโพธิ์

สำนักงานตรวจสอบภายใน

อาคารอำนวยการและบริหารกลาง ชั้น ปี 2

มหาวิทยาลัยราชภัฏเชียงใหม่ ศูนย์แม่ริม

มหาวิทยาลัยราชภัฏเชียงใหม่

http://www.internalaudit.cmru.ac.th

คู่มือการบริหารความเสี่ยง และแผนการบริหารความเสี่ยง

Risk Management Guide & Risk management plan

รอบปีงบประมาณ 2567