RISK MANAGEMENT

คู่มือการบริหารความเสี่ยง

กลุ่มตรวจสอบภายใน
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กันยายน 2566

คำนำ

การบริหารความเสี่ยง เป็นกระบวนการปฏิบัติงานที่มีความสำคัญและมีความจำเป็นในการควบคุมและป้องกันความเสี่ยงในด้านต่างๆที่อาจจะเกิดขึ้น จึงจำเป็นที่จะต้องมีบุคลากรที่มีความรู้ความสามารถในการวิเคราะห์ ตรวจสอบ ประเมินความเสี่ยงขององค์กร และสร้างเกราะป้องกันเพื่อสร้างความมั่นใจว่าการดำเนินงานของหน่วยงานจะบรรลุวัตถุประสงค์ ทั้งในด้านความมีประสิทธิภาพ ประสิทธิผลของการดำเนินงาน โดยจะดำเนินงานการบริหารความเสี่ยงตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์การปฏิบัติการควบคุมภายในสำหรับหน่วยงานรัฐ พ.ศ. ๒๕๖๑ และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐาน และหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒ และแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานรัฐในปี พ.ศ. ๒๕๖๔

กลุ่มตรวจสอบภายใน สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ จึงได้จัดทำคู่มือการบริหารความเสี่ยง เพื่อให้หน่วยงานสามารถนำไปใช้เป็นเครื่องมือในการจัดทำระบบการบริหารความเสี่ยงเพื่อให้เกิดความมั่นใจว่าจะสามารถป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และใช้เป็นเครื่องมือผลักดันการดำเนินงานของหน่วยงานให้มีประสิทธิภาพมากยิ่งขึ้น และเกิดผลสัมฤทธิ์ต่อภารกิจภาครัฐ ตลอดจนพัฒนาระบบงานของหน่วยงานให้ดียิ่งขึ้นต่อไป

กลุ่มตรวจสอบภายใน
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
กันยายน ๒๕๖๖

สารบัญ

บทที่ ๑
บทนำ

หลักการและเหตุผล

พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ มาตรา ๗๙ บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายใน และการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด ซึ่งได้แก่ หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒ และแนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานรัฐ ในปี พ.ศ. ๒๕๖๔ เรื่องการบริหารจัดการความเสี่ยงระดับองค์กรขึ้น

แม้ว่าหน่วยงานจะมีการจัดระบบการควบคุมภายในและการบริหารความเสี่ยงไว้ดีอยู่แล้วก็ตาม แต่จากการเปลี่ยนแปลงอย่างรวดเร็วของสภาพเศรษฐกิจ สังคม และเทคโนโลยี ทำให้หน่วยงานของรัฐต้องเผชิญกับความเสี่ยงทั้งปัจจัยภายในและภายนอก และเพื่อให้การดำเนินงานบรรลุวัตถุประสงค์ตามยุทธศาสตร์ หน่วยงานจึงจำเป็นจะต้องมีการดำเนินการเพื่อให้เกิดความมั่นใจว่า ผลการดำเนินงานที่หน่วยงานนั้นได้ปฏิบัติเกิดประโยชน์มากที่สุด การบริหารความเสี่ยงมีความสำคัญและมีความจำเป็นอย่างยิ่งในการป้องกัน และควบคุมความเสี่ยงในด้านต่าง ๆ ที่อาจเกิดขึ้นจากสถานการณ์ที่ไม่แน่นอน ซึ่งจะมีผลกระทบต่อความสำเร็จขององค์กรโดยรวม

วัตถุประสงค์ของคู่มือการบริหารความเสี่ยง

๑. เพื่อเป็นเครื่องมือในการกำหนดแนวทางการบริหารความเสี่ยงและการควบคุมภายใน สำหรับหน่วยงานภาครัฐ

๒. เพื่อเสริมสร้างความรู้ความเข้าใจในองค์ประกอบพื้นฐาน ความสำคัญ และประโยชน์ของการควบคุมภายในและการบริหารจัดการความเสี่ยงที่ดี

๓. เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงและการควบคุมภายในอย่างเป็นระบบและมีความต่อเนื่อง

๔. เพื่อเป็นผลักดันการดำเนินงานของหน่วยงานให้มีประสิทธิภาพมากยิ่งขึ้น และเกิดผลสัมฤทธิ์ต่อภารกิจภาครัฐ

๕. เพื่อให้ระบบการควบคุมภายในและการบริหารจัดการความเสี่ยงของ สดช.เป็นไปตามมาตรฐานที่กระทรวงการคลังกำหนด และสามารถดำเนินภารกิจได้ตามเป้าประสงค์อย่างมีประสิทธิภาพประสิทธิผล

ประโยชน์ที่คาดว่าจะได้รับ

๑. บุคลากรของกลุ่มตรวจสอบภายในมีความรู้ และเข้าใจหลักการและกระบวนการบริหารความเสี่ยง

๒. รักษามาตรฐานคุณภาพงานตรวจสอบภายในภาครัฐของหน่วยงาน

๓. การปฏิบัติงานของหน่วยงานเป็นไปตามกฎระเบียบ หลักเกณฑ์และวิธีปฏิบัติที่เกี่ยวข้อง

ระเบียบและหลักเกณฑ์ที่เกี่ยวข้อง

๑. พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑

๒. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

๓. หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒

๔. แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ในปี พ.ศ. ๒๕๖๔

บทที่ ๒
การบริหารความเสี่ยง

นิยามและคำจำกัดความของการบริหารความเสี่ยง

เพื่อให้การใช้คำที่เกี่ยวกับความเสี่ยงเป็นที่เข้าใจในแนวทางเดียวกัน จึงกำหนดคำนิยามเกี่ยวกับความเสี่ยงไว้ ดังนี้

๑. การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการในการดำเนินการที่สามารถระบุเหตุการณ์ ประเมินความเสี่ยง และวิธีการจัดการตอบสนอง ต่อเหตุการณ์ความไม่แน่นอนที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานรัฐสามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน รวมถึงเพื่อเพิ่มศักยภาพ และขีดความสามารถให้หน่วยงานของรัฐดำเนินงานตามแผนได้ โดยกระบวนการบริหารความเสี่ยงจะมีประสิทธิผลหากแทรกหรือฝังอยู่ในการปฏิบัติงาน

๒. ความเสี่ยง (Risk) หมายถึง กระบวนการในการวิเคราะห์และจัดลำดับความเสี่ยงที่อาจจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลักที่กำหนด ทั้งในด้านยุทธศาสตร์ การเงิน การบริหาร และการปฏิบัติงาน

๓. ปัจจัยเสี่ยง (Risk Factor) หมายถึง สาเหตุหรือต้นเหตุที่มาของความเสี่ยง อาจจะเกิดจากปัจจัยทั้งภายในและภายนอก เช่น เศรษฐกิจ สังคม การเมือง ข้อบังคับภายในองค์กร ประสบการณ์ของเจ้าหน้าที่ ซึ่งปัจจัยเหล่านี้อาจจะเป็นสาเหตุที่ทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ ทั้งนี้สาเหตุของความเสี่ยงที่ระบุต้องเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการจัดการกับความเสี่ยงได้อย่างถูกต้องที่ตรงกับสาเหตุที่แท้จริง (การวิเคราะห์ปัจจัยเสี่ยง อาจใช้ QC Tools) ได้

๔. การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการที่ใช้ในการวิเคราะห์ และจัดลำดับความเสี่ยง ที่อาจจะส่งผลกระทบต่อการบรรลุวัตถุประสงคีขององค์กร ซึ่งการกำหนดระดับความเสี่ยงจำพิจารณาจากการประเมินจากโอกาสที่จะเกิดขึ้นและผลกระทบ

โอกาสที่จะเกิด (Likelihood) หมายถึง การพิจารณามีโอกาสที่จะเกิดความเสี่ยงมากหรือน้อยเพียงใด โดยแบ่งออกเป็น ๕ ระดับ ได้แก่

ระดับ ๕ หมายถึง โอกาสเกิดสูงมาก
ระดับ ๔ หมายถึง โอกาสเกิดสูง
ระดับ ๓ หมายถึง โอกาสเกิดปานกลาง
ระดับ ๒ หมายถึง โอกาสเกิดน้อย
ระดับ ๑ หมายถึง โอกาสเกิดน้อยมาก

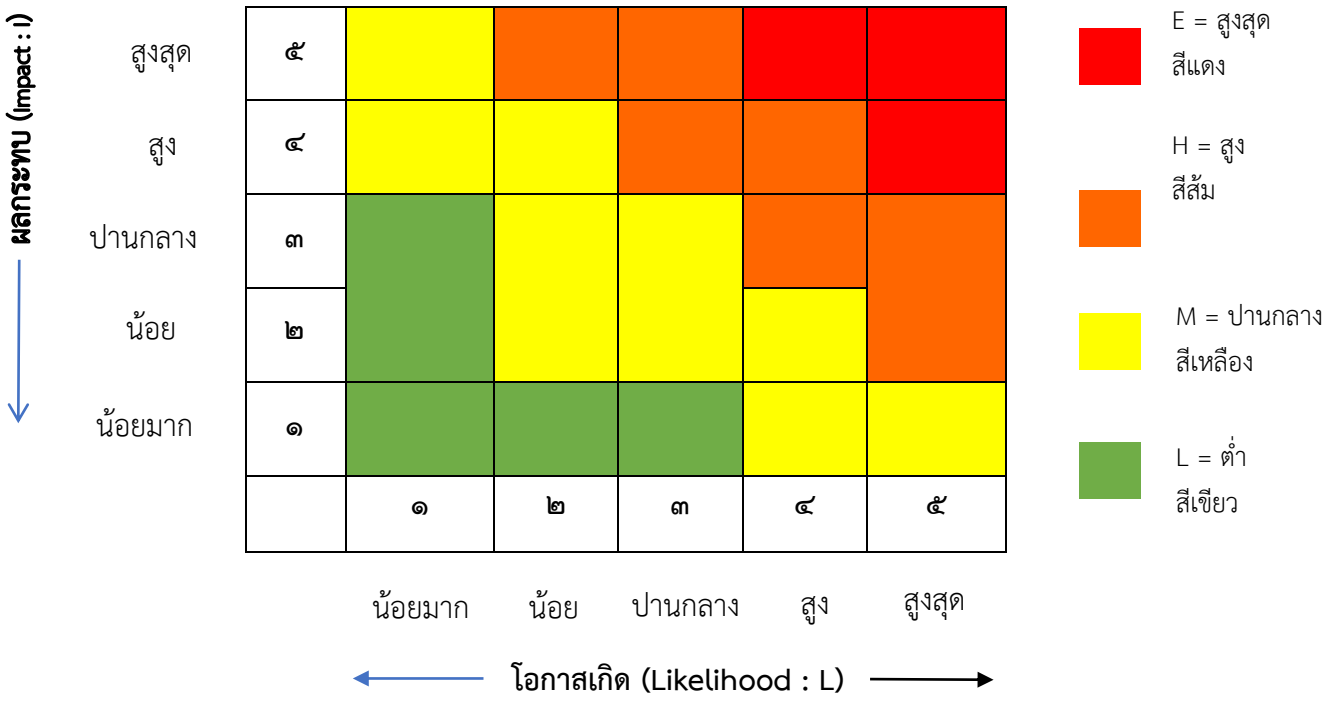
ระดับของผลกระทบ (Impact) หมายถึง การพิจารณาจากระดับความรุนแรง และมูลค่าความเสียหายที่จะเกิดต่อองค์กร ในกรณีที่ความเสี่ยงนั้นเกิดขึ้นสามารถแบ่งระดับของผลกระทบออกเป็น ๕ ระดับ ได้แก่

ระดับ ๕ หมายถึง ผลกระทบสูงมาก
ระดับ ๔ หมายถึง ผลกระทบสูง
ระดับ ๓ หมายถึง ผลกระทบปานกลาง
ระดับ ๒ หมายถึง ผลกระทบน้อย
ระดับ ๑ หมายถึง ผลกระทบน้อยมาก

๕. ความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ประเภทและเกณฑ์ของความเสี่ยงหรือความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้ แต่ต้องสอดคล้องกับเป้าหมายขององค์กรด้วย

๖. ความเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับการเปลี่ยนแปลงจากเกณฑ์หรือประเภทของความเสี่ยงที่ยอมรับได้ ซึ่งค่าเบี่ยงเบนจะเป็นช่วงที่ยอมให้ผลการดำเนินงานเบี่ยงเบนไปจากเป้าหมายที่กำหนด โดยจะต้องมีความสัมพันธ์กับระดับความเสี่ยงที่ยอมรับได้

๗. แผนภูมิความเสี่ยง (Risk Map) หมายถึง แผนผังที่แสดงถึงความเสี่ยงขององค์กร โดยจะต้องสามารถแสดงถึงหรือวิเคราะห์ถึงผลกระทบของแต่ละปัจจัยเสี่ยงที่มีความสัมพันธ์กันทั้งในเชิงปริมาณและเชิงคุณภาพได้อย่างเป็นรูปธรรม



รูปภาพที่ ๑ แผนภูมิความเสี่ยง (Risk Map)

๘. เจ้าของความเสี่ยง (Risk Owner) หมายถึง กอง/กลุ่ม/ศูนย์/บุคคลหรือกลุ่มบุคคลที่มีความรับผิดชอบโดยตรงต่อการบริหารความเสี่ยง โดยเจ้าของความเสี่ยงจะระบุปัจจัย เสี่ยงและจัดทำแผนจัดการความเสี่ยง ซึ่งอาจต้องประสานกับกอง/กลุ่ม/ศูนย์/บุคคลที่เกี่ยวข้องกับปัจจัยเสี่ยงนั้นๆเพื่อลดหรือควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

ประเภทความเสี่ยงขององค์กร

ความเสี่ยงที่อาจเกิดขึ้นในอนาคต และมีผลกระทบต่อการดำเนินงานให้ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กรนั้น จำแนกเป็น ๔ ด้าน ดังนี้

๑. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: S) ความเสี่ยงที่เกี่ยวข้องกับการตัดสินใจด้านกลยุทธ์ที่ครอบคลุมทุกภารกิจของหน่วยงาน เช่น การจัดทำแผนและนโยบายที่ไม่สอดคล้องกับแผนยุทธศาสตร์

๒. ความเสี่ยงด้านการดำเนินงาน (Operational Risk: O) ความเสี่ยงที่เกี่ยวข้องกับระบบขององค์กร ขั้นตอนการปฏิบัติงาน บุคลากร และเทคโนโลยีสารสนเทศ ซึ่งเป็นความเสี่ยงที่ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินงาน เช่น การจัดทำแผนการปฏิบัติงานด้านงบประมาณ ด้านกระบวนการปฏิบัติงาน ด้านผู้รับบริการทั้งภายในและภายนอก และด้านการพัฒนาความรู้ที่อาจจะไม่ครอบคลุมทั้งหมดทำให้เกิดช่องว่างและอาจจะเกิดความเสี่ยงที่เลี่ยงไม่ได้

๓. ความเสี่ยงด้านการเงิน (Financial Risk: F) ความเสี่ยงที่เกี่ยวข้องกับนโยบายและขั้นตอนการปฏิบัติด้านการเงิน และระบบการบริหารการเงิน เช่น การจัดสรรงบประมาณไม่เหมาะสม ตั้งงบประมาณผิดพลาด และใช้งบประมาณเกินความเสี่ยงจากการผันผวนของอัตราดอกเบี้ย ความเสี่ยงจากการขาดสภาพคล่อง เป็นต้น

๔. ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Compliance Risk: C) ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎหมาย หรือกฎระเบียบ ข้อบังคับและข้อกำหนด เช่น บุคลากรที่เกี่ยวข้องละเลยการปฏิบัติตามกฎหมาย ระเบียบหรือข้อบังคับที่กำหนดไว้ ความเสี่ยงจากนโยบายของรัฐบาล เป็นต้น

วัตถุประสงค์ของการบริหารความเสี่ยง

๑. เพื่อให้ผู้บริหารและผู้ปฏิบัติงาน เข้าใจหลักการ และกระบวนการบริหารความเสี่ยงของกลุ่มตรวจสอบภายใน

๒. เพื่อให้ผู้ปฏิบัติงานได้รับทราบขั้นตอน และกระบวนการในการวางแผนบริหารความเสี่ยง

๓. เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๔. เพื่อใช้เป็นเครื่องมือในการบริหารความเสี่ยงของกลุ่มตรวจสอบภายใน

๕. เพื่อลดโอกาสและผลกระทบของความเสี่ยงที่จะเกิดขึ้นกับองค์กร

การบริหารความเสี่ยงตามแนวทางของ COSO ERM

การบริหารความเสี่ยงตามมาตรฐาน COSO ประวัติความเป็นมาของ COSO ที่มาของ COSO เริ่มจากเหตุการณ์วิกฤตทางการเมืองและเศรษฐกิจของสหรัฐอเมริกา ปี ๑๙๗๐ - ๑๙๗๗ สหรัฐอเมริกาได้ประกาศกฎหมายแนวปฏิบัติเกี่ยวกับความไม่สุจริตในการให้สินบนชาวต่างชาติ (the ๑๙๗๗ Foreign Corrupt Practices Act-FCPA) ซึ่งมีการกำหนดเรื่องการควบคุมภายใน ซึ่งเป็นสาระสำคัญในประกาศดังกล่าว

ปี ๑๙๘๕ (ตุลาคม) จัดตั้งองค์กรอิสระ คือ คณะกรรมการเพื่อรายงานการทุจริตแห่งชาติ (National Commission on Fraudulent Financial reporting หรือ Tread way)

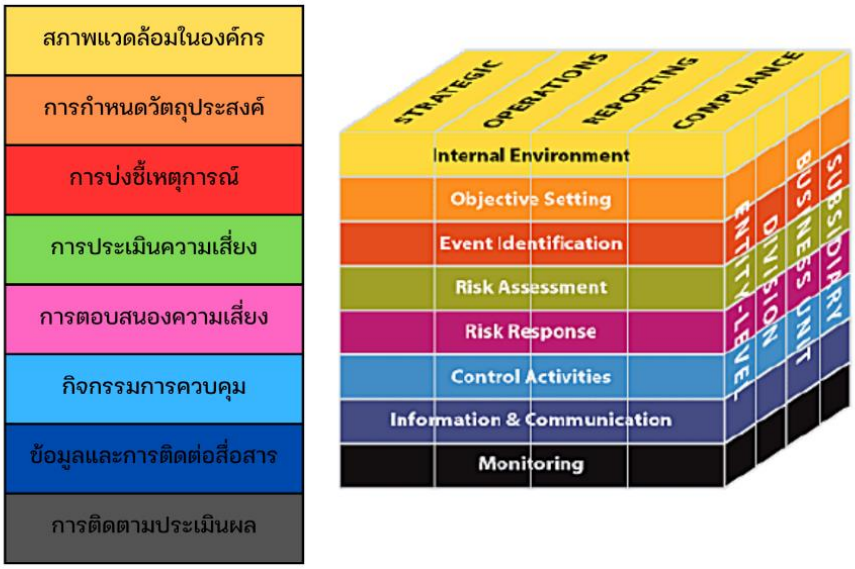
ปี ๑๙๘๗ คณะกรรมการเพื่อการรายงานการทุจริตแห่งชาติได้รับการสนับสนุนจากคณะกรรมการวิชาชีพอิสระอื่นๆ จัดตั้ง The Committee of Sponsoring Organization of the Tread way Commission (COSO)

ปี ๑๙๙๒ COSO เผยแพร่แนวคิดการควบคุมภายใน COSO Internal Control-integrated Framework กำหนดความหมายและกรอบโครงสร้างการควบคุมภายใน

ปี ๒๐๐๔ COSO ได้พัฒนาแนวทางการบริหารความเสี่ยงที่มีมาตรฐานสากลมากขึ้นเพื่อให้องค์กรสามารถใช้เป็นแนวปฏิบัติด้านการบริหารความเสี่ยง

ปี ๒๐๑๓ COSO เริ่มประกาศให้ทราบถึงการปรับปรุง COSO ๑๙๙๒ ตั้งแต่ปลายปี ๒๐๑๐ และประกาศอย่างเป็นทางการในปี ๒๐๑๓ และจะใช้เวอร์ชั่นใหม่เป็นหลักตั้งแต่ ๑๔ ธันวาคม ๒๐๑๔

หลักการสำคัญในการบริหารความเสี่ยงที่ได้รับการยอมรับว่าเป็นแนวทางในการส่งเสริมการบริหารความเสี่ยง และเป็นหลักปฏิบัติที่เป็นสากล คือ กรอบการบริหารความเสี่ยงตามแนวทางของ COSO (The Committee of Sponsoring Organization of the Tread way Commission) ซึ่งเป็นกรอบการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management : ERM) ประกาศใช้ในปี ๒๐๐๔ โดยพัฒนามาจากกรอบการควบคุมภายใน (๑๙๙๔) โดยเพิ่มหลักการและองค์ประกอบสำคัญเพื่อให้ตรงกับความต้องการเกี่ยวกับการบริหารความเสี่ยงในการบริหารงานยุคใหม่ ประกอบด้วยองค์ประกอบ ๘ ประการ ที่มีความสัมพันธ์กัน ดังนี้



รูปภาพที่ ๒ กรอบการบริหารความเสี่ยงตามแนวทางของ COSO

องค์ประกอบของการบริหารความเสี่ยง ERM (Enterprise Risk Management)

ประกอบด้วย องค์ประกอบ ๘ ประการ ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน และการบริหารความเสี่ยง ดังนี้

๑. สภาพแวดล้อมภายในองค์กร (Internal Environment) เป็นองค์ประกอบที่พื้นฐานของการบริหารความเสี่ยงที่ส่งผลต่อวิธีการกำหนดกลยุทธ์และเป้าหมายของการดำเนินงาน

๒. การกำหนดวัตถุประสงค์ (Objective Setting) องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยงให้สอดคล้องกับเป้าหมายเชิงกลยุทธ์ และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม

๓. การระบุความเสี่ยง (Risk Identification) เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งปัจจัยเสี่ยงภายในและภายนอกองค์กร ซึ่งเมื่อเกิดขึ้นแล้วส่งผลให้ไม่บรรลุวัตถุประสงค์หรือเป้าหมาย เช่น นโยบาย การบริหารงานบุคลากร การปฏิบัติงานการเงิน ระบบสารสนเทศ ระเบียบข้อบังคับ เป็นต้น เพื่อให้สามารถพิจารณากำหนดแนวทางและนโยบายจัดการความเสี่ยงที่อาจเกิดขึ้น

๔. การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงจะช่วยให้องค์กรทราบว่าเหตุการณ์ความเสี่ยง/ความไม่แน่นอนที่เกิดขึ้นส่งผลกระทบต่อการบรรลุวัตถุเป้าหมายขององค์กรเป็นอย่างไร โดยวิเคราะห์จากโอกาสที่จะเกิดขึ้น

๕. การตอบสนองความเสี่ยง (Risk Response) เป็นการดำเนินการหลังจากที่องค์กรสามารถระบุความเสี่ยงขององค์กรและประเมินระดับของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการเพื่อลด โอกาสที่จะเกิดความเสี่ยงและลดระดับความรุนแรงของผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้ด้วยวิธีจัดการความเสี่ยงที่เหมาะสมที่สุดและคุ้มค่ากับการลงทุน

๖. กิจกรรมควบคุม (Control Activities) นโยบายการปฏิบัติงาน เพื่อให้มั่นใจว่ามีการจัดการ เนื่องจากแต่ละองค์กรมีการกำหนดวัตถุประสงค์และเทคนิคการนำไปปฏิบัติงานเฉพาะองค์กร จึงทำให้กิจกรรมควบคุมมีความแตกต่างกันไปตามภารกิจขององค์กร

๗. สารสนเทศและการสื่อสาร (Information and Communication) สารสนเทศเป็นสิ่งสำคัญและจำเป็นต่อองค์กรในการบ่งชี้ ประเมิน และจัดการความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องทั้งจากแหล่งภายนอกและภายในควรจะต้องได้รับการบันทึกและสื่อสารอย่างเหมาะสมในด้านรุปแบบและเวลาเพื่อช่วยให้สามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ เช่น การแลกเปลี่ยนข้อมูล

๘. การติดตามประเมินผล (Monitoring) ประเด็นสำคัญในการติดตามและประเมินผลเพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงมีคุณภาพ เหมาะสมนำไปประยุกต์ใช้ในทุกระดับขององค์กร และเพื่อทบทวนแผนการบริหารความเสี่ยงให้มีประสิทธิผล และความเสี่ยงทั้งหมดที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรได้รับการรายงานต่อผู้บริหารที่รับผิดชอบ การติดตามสามารถทำได้ ๒ กรณี คือ การติดตามอย่างต่อเนื่อง และการติดตามเป็นรายครั้ง

บทที่ ๓
กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงของกลุ่มตรวจสอบภายใน

กระบวนการบริหารความเสี่ยงเป็นกระบวนการที่ใช้ระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีผลต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานขององค์กร รวมทั้งการจัดทำแผนบริหารความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกัน หรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งมีกระบวนการบริหารจัดการความเสี่ยงตามมาตรฐานของ COSO ได้สร้างมาตรฐานที่เป็นกรอบแนวคิดของการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management : ERM) เพื่อเป็นแนวทางที่จะช่วยให้องค์กรสามารถแจกแจงปัญหาความเสี่ยงเป็นองค์ประกอบย่อย เพื่อความสะดวกในการวิเคราะห์ และหาแนวทางในการบริหารจัดการ ซึ่งองค์ประกอบของการบริหารความเสี่ยงทั่วทั้งองค์กร (ERM – Enterprise Risk Management) ตามแนวทางการบริหารความเสี่ยงตามหลักการของ COSO ประกอบด้วย ๘ ขั้นตอน ดังนี้

๑. สภาพแวดล้อมภายในองค์กร
๒. การกำหนดวัตถุประสงค์
๓. การระบุความเสี่ยง
๔. การวิเคราะห์ความเสี่ยง
๕. การจัดระดับการความเสี่ยง
๖. การประเมินความเสี่ยงและความควบคุมที่มีอยู่
๗. การจัดการความเสี่ยง (การตอบสนองความเสี่ยง)
๘. การติดตาม ประเมินผล และจัดทำรายงาน

กลุ่มตรวจสอบภายใน มีการจัดทำแผนบริหารความเสี่ยง โดยมีการสำรวจและค้นหาความเสี่ยงที่อาจจะเกิดขึ้นจากการดำเนินงานในปีงบประมาณก่อนมาดำเนินการจัดทำแผนบริหารความเสี่ยงและมีการวิเคราะห์ปัจจัยภายใน/ภายนอก วิเคราะห์โอกาสและผลกระทบ รวมถึงวิเคราะห์ระดับความเสี่ยงของแต่ละความเสี่ยง ตามลำดับขั้นตอน ดังนี้

๑. พิจารณาจากความสำคัญของภารกิจ กิจกรรม นำมาประกอบจัดลำดับความสำคัญ
๒. พิจารณาจากปัจจัยเสี่ยงทั้งภายใน และภายนอกองค์กร

๒.๑) ปัจจัยภายใน หมายถึง ความเสี่ยงที่สามารถควบคุมได้โดยองค์กร เช่น กฎระเบียบ ข้อบังคับของส่วนราชการ วัฒนธรรมองค์กร นโยบายของผู้บริหาร ความรู้ความสามารถ ของบุคลากร กระบวนการในการทำงานข้อมูล/ระบบสารสนเทศ และเครื่องมือ อุปกรณ์ เป็นต้น

๒.๒) ปัจจัยภายนอก หมายถึง ความเสี่ยงที่ไม่สามารถควบคุมการเกิดได้โดยองค์กร เช่น ภาวะเศรษฐกิจ สังคม การเมือง กฎหมาย ผู้รับบริการ เครือข่าย เทคโนโลยี ภัยธรรมชาติและสิ่งแวดล้อม เป็นต้น

๓. พิจารณาจากเหตุการณ์ที่อาจเกิดขึ้นได้ โดยพิจารณาจากปัจจัยเสี่ยงในหลายด้าน ได้แก่

๓.๑) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S) คือ ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ที่ไม่เหมาะสม หรือความเสี่ยงเกิดจากการนำกลยุทธ์ไปใช้ไม่ถูกต้อง

๓.๒) ความเสี่ยงด้านการดำเนินงาน (Operation Risk : O) คือ ความเสี่ยงที่เกิดจากกระบวนการทำงานที่ไม่มีประสิทธิผลหรือไม่มีประสิทธิภาพ

๓.๓) ความเสี่ยงด้านการเงิน (Financial Risk : F) คือ ความเสี่ยงเกี่ยวกับการบริหารจัดการด้านการเงิน เช่น ความเสี่ยงเกี่ยวกับการเบิกจ่ายเงินไม่ถูกต้อง ความเสี่ยงเกี่ยวกับการรับเงินไม่ถูกต้อง ความเสี่ยงในการไม่ปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้องกับการเงินการคลัง รวมถึงความเสี่ยงด้านการทุจริตทางการเงิน เป็นต้น

๓.๔) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk : C) คือ ความเสี่ยงที่หน่วยงานไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หลักเกณฑ์ ประกาศ มติคณะรัฐมนตรี รวมถึงกฎ/นโยบาย/คู่มือ/แนวทางการปฏิบัติงานของหน่วยงาน

ขั้นที่ ๑ กำหนดวัตถุประสงค์ (Objective setting)

หัวหน้าหน่วยงานและผู้ปฏิบัติงานที่เกี่ยวข้างร่วมกันกำหนดวัตถุประสงค์ของการบริหารความเสี่ยงและเชื่อมโยงวัตถุประสงค์เข้ากับการดำเนินงานที่ครอบคลุมการปฏิบัติงานทุกด้าน

การกำหนดวัตถุประสงค์เป็นไปตามหลักค่านิยมของหน่วยงาน “ONDE”

O : Objectivity	เที่ยงธรรม
N : Nature	ความเป็นกันเอง
D : Deftness	เชี่ยวชาญ
E : Ethics	มีจริยธรรม

ขั้นที่ ๒ ระบุความเสี่ยง (Risk identification)

เป็นการหาสาเหตุหรือปัจจัยของความเสี่ยง โดยพิจารณาจากปัจจัยภายในและภายนอกที่ส่งผลกระทบต่อเป้าหมายผลลัพธ์ขององค์กรตามกรอบการบริหารความเสี่ยง ทั้งนี้ การบ่งชี้ความเสี่ยงจะต้องระบุให้ครบทุกสาเหตุที่ทำให้เกิดความเสี่ยง เพื่อให้สามารถกำหนดแผนจัดการความเสี่ยงได้ตรงกับสาเหตุและสามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล โดยวิธีการระบุความเสี่ยงสามารถทำได้หลายแบบตามความถนัดของแต่ละหน่วยงาน เช่น การระดมความคิดจากผู้มีส่วนที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร โดยเฉพาะอย่างยิ่งจากเจ้าของความเสี่ยง (Risk Owner) เพื่อร่วมกันพิจารณาว่ามีเหตุการณ์ใดบ้างที่อาจเกิดขึ้นแล้วส่งผลกระทบเสียหาย การใช้ประสบการณ์ของผู้ประเมินโดยวิเคราะห์โอกาสที่จะเกิดความเสี่ยงจากการเก็บข้อมูลเกี่ยวกับปัญหา/ข้อผิดพลาดที่เคยเกิดขึ้นในอดีตซึ่งมีการบันทึกไว้เพื่อใช้เป็นแนวทางและข้อมูลเบื้องต้น การใช้รายการตรวจสอบ เพื่อตรวจสอบขั้นตอนการทำงาน และการพิจารณาจากคู่มือปฏิบัติงาน เพื่อตรวจสอบขั้นตอนการทำงานที่มีความเสี่ยง ซึ่งอาจจะนำไปสู่ความผิดพลาดจนก่อให้เกิดความเสียหาย

ขั้นที่ ๓ การวิเคราะห์ความเสี่ยง

การวิเคราะห์ความเสี่ยงเพื่อวัดระดับโอกาสหรือความถี่ที่จะเกิดความเสี่ยงและวัดระดับผลกระทบของความเสี่ยงนั้น ๆ โดยนำเหตุการณ์ปัจจัยความเสี่ยงที่มีการค้นพบหรือระบุได้มาทำการวัดประเมินระดับความรุนแรง โอกาสที่จะเป็นไปได้ เพื่อระบุระดับความสำคัญของความเสี่ยง ซึ่งมีองค์ประกอบหลักในการพิจารณาอยู่ ๒ ประการ คือ โอกาสที่จะเกิดและผลกระทบที่เกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง ทั้งนี้จะต้องมีการกำหนดระดับของโอกาสที่จะเกิดและระดับของผลกระทบที่จะเกิด เพื่อให้สามารถกำหนดหรือจัดลำดับความสำคัญของความเสี่ยงได้การติดตามประเมินผลของแผนบริหารความเสี่ยงโดยวิเคราะห์และประเมินผลการบริหารจัดการความเสี่ยงว่ามีประสิทธิผลหรือไม่ หากหน่วยงานได้ดำเนินการตามแผนบริหารความเสี่ยงแล้วยังมีความเสี่ยงที่ไม่อาจยอมรับได้เหลืออยู่ควรพิจารณาต่อไปว่าเป็นความเสี่ยงที่อยู่ในระดับใดและมีวิธีการจัดการความเสี่ยงนั้นอย่างไร เพื่อเสนอต่อผู้บริหารเพื่อทราบและพิจารณาสั่งการรวมถึงการจัดสรรงบประมาณสนับสนุนในลำดับถัดไป ทั้งนี้การบริหารความเสี่ยงจะเกิดผลสำเร็จได้ต้องได้รับการสนับสนุนอย่างจริงจังจากผู้บริหาร ซึ่งหลังจากทราบผลประเมินความเสี่ยงแล้วจะต้องนำความเสี่ยงที่ยังเหลืออยู่มากำหนดวิธีการจัดการความเสี่ยง

๑) พิจารณาโอกาสในการเกิดความเสี่ยง (Likelihood) จากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบันหรือการคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต โดยจัดระดับความเสี่ยงเป็น ๕ ระดับคือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก แทนด้วยตัวเลข ๕ ๔ ๓ ๒ และ ๑ ตามลำดับใช้หลักเกณฑ์ดังต่อไปนี้ **(ตารางที่ ๑)**

ตารางที่ ๑ วิเคราะห์โอกาสและผลกระทบของปัจจัยเสี่ยงหรือสาเหตุของความเสี่ยง

ระดับ (๑)	โอกาสที่จะเกิด (๒)	คำอธิบาย (๓)	
		โอกาสเกิดเชิงคุณภาพ	โอกาสเกิดเชิงปริมาณ
๕	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง	เกิดมากกว่า ๘๐% หรือ < ๑ เดือน/ครั้ง
๔	สูง	มีโอกาสในการเกิดค่อนข้างสูง หรือบ่อย ๆ	เกิดมากกว่า ๗๐% หรือ ๑ – ๖ เดือน/ครั้ง
๓	ปานกลาง	ปานกลาง มีโอกาสเกิดบางครั้ง	เกิดมากกว่า ๕๐% หรือ ๖ – ๑๒ เดือน/ครั้ง
๒	น้อย	น้อย อาจมีโอกาสเกิดแต่นาน ๆ ครั้ง	เกิดมากกว่า ๒๐% หรือ ๑ – ๕ ปี/ครั้ง
๑	น้อยมาก	น้อยมาก มีโอกาสเกิดในกรณียกเว้น	เกิดมากกว่า ๕% หรือ > ๕ ปี/ครั้ง

๒) พิจารณาความรุนแรงของผลกระทบที่เกิดขึ้นจากความเสี่ยง (Impact) หรือมูลค่าความเสียหายจากความเสี่ยงที่คาดหวังว่าได้รับหากเกิดเหตุการณ์ การจัดระดับความรุนแรงของผลกระทบที่เกิด จากความเสี่ยงเป็น ๕ ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก แทนด้วยตัวเลข ๕ ๔ ๓ ๒ และ ๑ ตามลำดับ ซึ่งการกำหนดระดับผลกระทบนั้น จะต้องพิจารณาถึงความเสียหาย หากความเสี่ยงนั้นเกิดขึ้นโดยอาจแบ่งผลกระทบออกเป็นผลกระทบด้านการเงิน หรือทรัพย์สิน การดำเนินงาน ชื่อเสียง หรือภาพลักษณ์บุคลากร เป็นต้น **(ตารางที่ ๒)**

ตารางที่ ๒ ระดับวิเคราะห์ผลกระทบซึ่งกำหนดเกณฑ์ไว้ ๕ ระดับ

ระดับ (๑)	โอกาสที่จะเกิด (๒)	คำอธิบาย (๓)
๕	สูงมาก	ส่งผลกระทบถึงองค์กรอื่นที่ปฏิบัติงานร่วมกัน
๔	สูง	ส่งผลกระทบถึงกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
๓	ปานกลาง	ส่งผลกระทบถึงสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม
๒	น้อย	ส่งผลกระทบเฉพาะกลุ่มตรวจสอบภายใน
๑	น้อยมาก	ส่งผลกระทบต่อภาพลักษณ์ของบุคลากรในกลุ่มตรวจสอบภายใน

ขั้นตอนที่ ๔ การจัดระดับการความเสี่ยง

การนำความเสี่ยงและปัจจัยเสี่ยงที่ได้ทำการประเมินระดับความเสี่ยงในขั้นตอนการวิเคราะห์ความเสี่ยงแล้วมาจัดเรียงลำดับความเสี่ยงตามระดับให้ครบถ้วน โดยเรียงลำดับความเสี่ยงจากระดับความเสี่ยงสูงมาก ถึงน้อยมาก

ขั้นตอนที่ ๕ การประเมินความเสี่ยงและความควบคุมที่มีอยู่

หลังจากระบุระดับความเสี่ยงและจัดลำดับความเสี่ยงได้แล้วได้พิจารณาเลือกปัจจัยเสี่ยงมาประเมินผลการควบคุมที่มีอยู่โดยพิจารณาจากระดับความเสี่ยงที่ยอมรับได้และทรัพยากรที่มีอยู่ของหน่วยงานไม่ว่าจะเป็นบุคลากร งบประมาณ เวลา วัสดุอุปกรณ์ต่าง ๆ ว่าจะสามารถจัดการความเสี่ยงและปัจจัยเสี่ยงได้มากน้อยเพียงไร จากนั้นประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านี้มีการควบคุมอยู่แล้วหรือไม่ ถ้ามี การควบคุมอยู่แล้วให้ประเมินต่อไปว่าการควบคุมนั้นมีประสิทธิผลเพียงพอเหมาะสมหรือไม่ หากผลประเมิน เห็นว่าควรมีการปรับปรุงหรือยังไม่อาจจะยอมรับได้ให้นำปัจจัยเสี่ยงเหล่านั้นไปพิจารณาจัดการความเสี่ยง หรือตอบสนองความเสี่ยงต่อไป

ขั้นตอนที่ ๖ การจัดการความเสี่ยง (การตอบสนองความเสี่ยง)

เมื่อได้มีการประเมินผลการควบคุมและที่ทราบความเสี่ยงที่เหลืออยู่คณะกรรมการบริหารความเสี่ยงฯ จะต้องตัดสินใจหาแนวทางในการจัดการความเสี่ยงหรือตอบสนองความเสี่ยงภายใต้การบริหารทรัพยากรที่มี อยู่ให้เกิดประโยชน์สูงสุดโดยจะต้องคำนึงถึงลักษณะของความเสี่ยงระดับของความเสี่ยงและต้นทุนหรือทรัพยากรที่ต้องใช้ในทางเลือกนั้นเปรียบเทียบกับผลที่คาดว่าจะได้รับโดยรวบรวม และจัดทำเป็นแผนบริหารความเสี่ยงของหน่วยงานต่อไป มีทางเลือกที่จะจัดการความเสี่ยงอยู่ด้วยกัน ๔ วิธี ดังนี้

๑) การยอมรับความเสี่ยง

เป็นความเสี่ยงที่หน่วยงานสามารถยอมรับได้ หรือเป็นความเสี่ยงที่อยู่ในระดับความเสี่ยงต่ำหรือเป็นความเสี่ยงที่มีต้นทุนในการจัดการความเสี่ยงสูงมากจนไม่คุ้มค่ากับผลที่จะได้รับหรือเป็นความเสี่ยงที่อยู่นอกเหนือการควบคุมขององค์กร อาจมีสาเหตุมาจากปัจจัยภายนอกที่ไม่สามารถควบคุมได้ เช่น นโยบายของรัฐบาล เป็นต้น

๒) การกระจายหรือถ่ายโอนความเสี่ยง

เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้หน่วยงานอื่นทั้งภายในและภายนอกองค์กรช่วยแบ่งความรับผิดชอบไป โดยเฉพาะเป็นกรณีที่เห็นว่าเป็นความเสี่ยงที่คาดไม่ถึงหรือป้องกันได้ยาก หรือมีระดับของความรุนแรงสูง เช่น ภัยธรรมชาติ หรือวินาศภัยต่าง ๆ ซึ่งหน่วยงานไม่สามารถแบกรับความเสี่ยงนั้นได้ ก็อาจกระจายหรือถ่ายโอนความเสี่ยงด้วยการทำประกันภัยหรือกรณีความเสี่ยงที่อาจเกิดจากความไม่ชำนาญงานของบุคลากรภายในหน่วยงาน ก็อาจจัดจ้างบุคคลภายนอกมาดำเนินการแทน

๓) การลดหรือควบคุมความเสี่ยง

เป็นการลดหรือควบคุมความเสี่ยง ในกรณีที่หน่วยงานเห็นว่า ความเสี่ยงเหล่านั้นเกิดจากปัจจัยภายใน หรือสาเหตุที่หน่วยงานสามารถลดหรือควบคุมได้ด้วยวิธีการควบคุมภายในหรือปรับปรุงระบบการทำงานโดยออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดความเสียหายหรือผลกระทบให้อยู่ในระดับที่หน่วยงานยอมรับได้ เช่น การจัดอบรมให้กับบุคลากร การจัดทำคู่มือการปฏิบัติงานเพื่อลดความเสี่ยงจากการทำงานผิดพลาด เป็นต้น หรือหากเป็นความเสี่ยงที่เกิดจากปัจจัยภายนอกก็อาจนำกลยุทธ์หรือมาตรการต่าง ๆ มาใช้เพื่อลดผลกระทบหรือความรุนแรงของความเสี่ยงนั้นลงได้ เช่น งาน โครงการ กิจกรรม หรือกระบวนงาน เป็นต้น หากไม่สามารถจัดการด้วยวิธีอย่างหนึ่งอย่างใดข้างต้น ต้องจัดการความเสี่ยงนั้นด้วยการหยุดดำเนินการยกเลิกโครงการลดเนื้องานของโครงการ หรือลดกิจกรรมที่กำหนดไว้ตามโครงการ เป็นต้น

๔) การหลีกเลี่ยงความเสี่ยง

เป็นการปฏิเสธและหลีกเลี่ยงโอกาสที่จะเกิดความเสี่ยง โดยการหยุดยกเลิกหรือเปลี่ยนแปลงกิจกรรมหรือโครงการที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยง

ขั้นตอนที่ ๗ การติดตามและประเมินผล

เป็นกระบวนการประเมินคุณภาพการปฏิบัติงานและประเมินประสิทธิผลที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ เพื่อให้เกิดความมั่นใจในการบริหารความเสี่ยงและควบคุมภายในที่กำหนดไว้มีความเหมาะสมมีการปฏิบัติตามจริงข้อบกพร่องที่พบได้รับการแก้ไขและทันเวลา

เอกสารอ้างอิง

- พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑
- หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑
- หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๒
- แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานรัฐ พ.ศ. ๒๕๖๔ เรื่องการบริหารจัดการความเสี่ยงระดับองค์กร