

1

การบริหารจัดการความเสี่ยง ตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐาน และหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยง สำหรับหน่วยงานของรัฐ พ.ศ. 2562



กองตรวจสอบภาครัฐ
กรมบัญชีกลาง

พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑

การบริหารจัดการความเสี่ยง

หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 หนังสือกระทรวงการคลังที่ กค 0409.4.ว23 ลว. 29 มีนาคม 2562

- มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ
- หลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

การบริหารจัดการความเสี่ยง
ตามหลักเกณฑ์ฯ
ว่าด้วยมาตรฐานและหลักเกณฑ์
การบริหารจัดการความเสี่ยง
สำหรับหน่วยงานของรัฐ พ.ศ. 2561

พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑

มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

คำนิยาม

- หน่วยงานของรัฐ
- ฝ่ายบริหาร
- การบริหารจัดการความเสี่ยง

มาตรฐาน

ประกอบด้วย ๙ ข้อ

คำจำกัดความตามมาตรฐานและหลักเกณฑ์ปฏิบัติ การบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

ความเสี่ยง หมายถึง ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้นและเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ของหน่วยงาน (หลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ของหลักเกณฑ์กระทรวงการคลังฯ)

กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน รวมถึงเพื่อเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ (มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ของหลักเกณฑ์กระทรวงการคลังฯ)

COSO - ERM

กระบวนการที่เกิดขึ้นจากคณะกรรมการขององค์กร ผู้บริหารและบุคลากรอื่นๆ เป็นกระบวนการที่จะถูกนำมาประยุกต์ใช้ในการกำหนดกลยุทธ์ทั่วทั้งองค์กร ได้รับการออกแบบมาเพื่อให้สามารถระบุเหตุการณ์อันอาจเกิดขึ้นและส่งผลกระทบต่อองค์กร และเพื่อจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่องค์กรยอมรับได้ (risk appetite) ซึ่งจะทำให้เกิดความเชื่อมั่นได้อย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร

มาตรฐานการบริหารจัดการความเสี่ยงฯ

- ▶ ต้องจัดให้มีการบริหารจัดการความเสี่ยง
- ▶ ต้องจัดให้มีสภาพแวดล้อมที่เหมาะสมต่อการบริหารจัดการความเสี่ยงภายในองค์กร อย่างน้อยประกอบด้วย การมอบหมายผู้รับผิดชอบเรื่องการบริหารจัดการความเสี่ยงการกำหนดวัฒนธรรมของหน่วยงานของรัฐที่ส่งเสริมการบริหารจัดการความเสี่ยง รวมถึงการบริหารทรัพยากรบุคคล
- ▶ ต้องมีการกำหนดวัตถุประสงค์เพื่อใช้ในการบริหารจัดการความเสี่ยงที่เหมาะสม รวมถึงมีการสื่อสารการบริหารจัดการความเสี่ยงของวัตถุประสงค์ด้านต่างๆ ต่อบุคลากรที่เกี่ยวข้อง
- ▶ ต้องดำเนินการในทุกระดับของหน่วยงานของรัฐ อย่างน้อยต้องประกอบด้วย การระบุความเสี่ยง การประเมินความเสี่ยง และการตอบสนองความเสี่ยง

มาตรฐานการบริหารจัดการความเสี่ยงฯ

- ต้องจัดทำแผนบริหารจัดการความเสี่ยงอย่างน้อยปีละครั้งและต้องมีการสื่อสารแผนบริหารจัดการความเสี่ยงกับผู้ที่เกี่ยวข้องทุกฝ่าย
- ต้องมีการติดตามประเมินผลการบริหารจัดการความเสี่ยงและทบทวนแผนการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ
- ต้องมีการรายงานการบริหารจัดการความเสี่ยงของหน่วยงานต่อผู้ที่เกี่ยวข้อง
- สามารถพิจารณานำเครื่องมือการบริหารความเสี่ยงที่เหมาะสมมาประยุกต์ใช้กับหน่วยงาน เพื่อให้การบริหารจัดการความเสี่ยงของหน่วยงานเกิดประสิทธิภาพสูงสุด

หลักเกณฑ์การบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

คำนิยาม

- หน่วยงานของรัฐ
- หัวหน้าหน่วยงานของรัฐ
- ฝ่ายบริหาร
- ผู้รับผิดชอบ
- การบริหารจัดการความเสี่ยง
- ความเสี่ยง

หลักเกณฑ์

ประกอบด้วย ๑๓ ข้อ

๑ หลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงฯ

➤ จัดให้มีการบริหารจัดการความเสี่ยง โดยใช้มาตรฐานกระทรวงการคลัง

ถือปฏิบัติตามคู่มือหรือแนวทางปฏิบัติที่กระทรวงการคลังกำหนดและสามารถนำคู่มือหรือแนวทางอื่นมาประยุกต์ใช้กับหน่วยงานได้ ถือปฏิบัติตามหลักเกณฑ์

➤ จัดให้มีผู้รับผิดชอบ ซึ่งต้องประกอบด้วยฝ่ายบริหาร และบุคลากรที่มีความรู้

ความเข้าใจเกี่ยวกับการจัดทำยุทธศาสตร์และการบริหารจัดการความเสี่ยง ทั้งนี้ ไม่ควรเป็นผู้ตรวจสอบภายใน

➤ ผู้รับผิดชอบมีหน้าที่ ดังนี้

(๑) จัดทำแผนการบริหารจัดการความเสี่ยง

(๒) ติดตามประเมินผลการบริหารจัดการความเสี่ยง

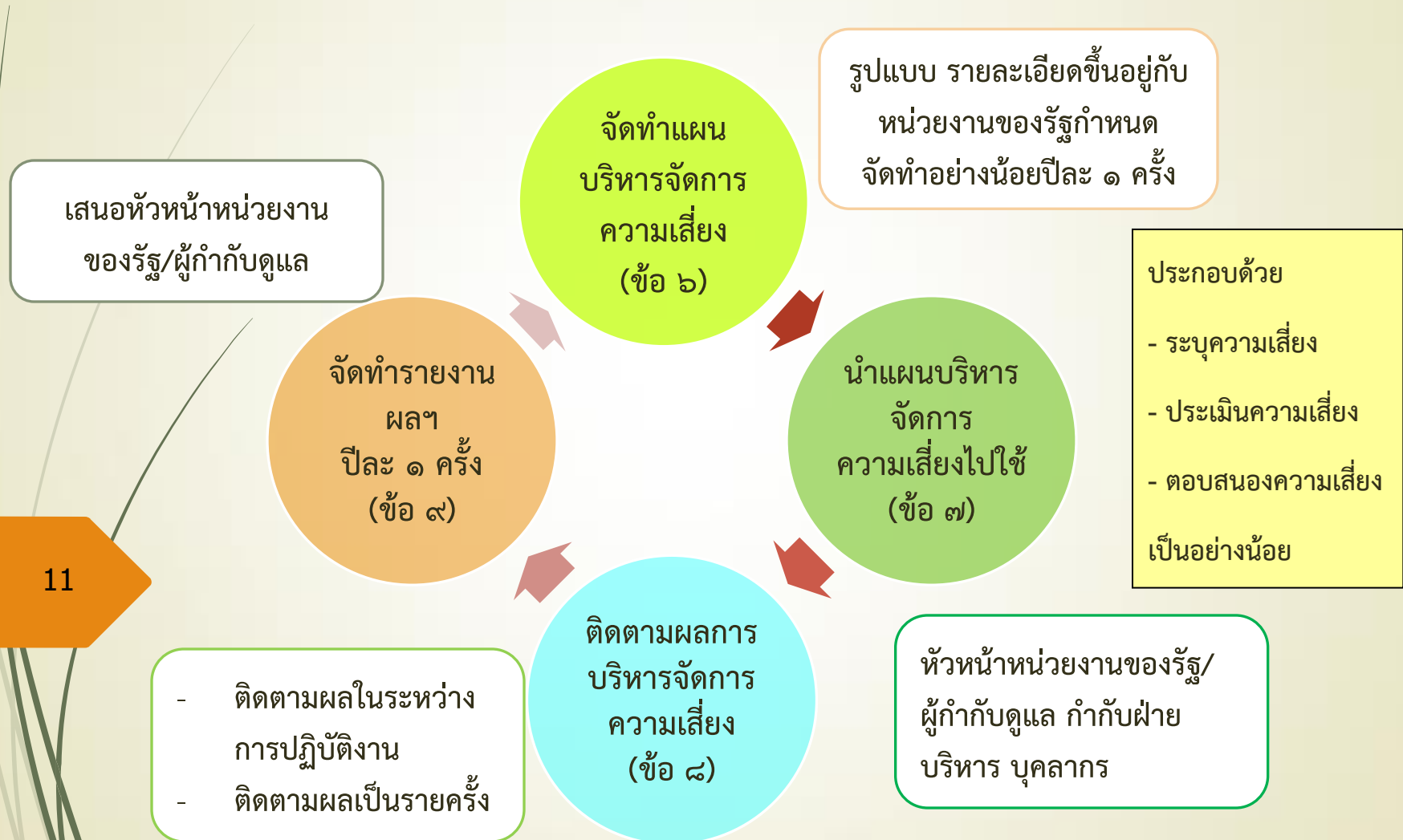
(๓) จัดทำรายงานผลตามแผนการบริหารจัดการความเสี่ยง

(๔) พิจารณาทบทวนแผนการบริหารจัดการความเสี่ยง

หลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงฯ

- ▶ จัดทำแผนบริหารจัดการความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์
- ▶ กำกับดูแลฝ่ายบริหาร ผู้รับผิดชอบ และบุคลากรที่เกี่ยวข้องให้มีการบริหารจัดการความเสี่ยงให้เป็นไปตามแผนการบริหารจัดการความเสี่ยงที่กำหนดไว้
- ▶ ติดตามประเมินผลอย่างต่อเนื่องในระหว่างการปฏิบัติงานหรือติดตามประเมินผลเป็นรายครึ่งหรือใช้ทั้งสองวิธีร่วมกัน กรณีพบข้อบกพร่องที่มีสาระสำคัญให้รายงานทันที
- ▶ จัดทำรายงานเสนอเพื่อพิจารณาอย่างน้อยปีละ ๑ ครั้ง
- ▶ สามารถกำหนดนโยบาย วิธีการ และระยะเวลาการรายงานการบริหารจัดการความเสี่ยง
- ▶ กรมบัญชีกลางขอให้หน่วยงานของรัฐ จัดส่งรายงานและรายงานผลการบริหารจัดการความเสี่ยง หรือ ข้อมูลอื่น ๆ เพิ่มเติมเกี่ยวกับกระบวนการบริหารจัดการความเสี่ยง ให้หน่วยงานของรัฐดังกล่าวดำเนินการตามรูปแบบ วิธีการ และระยะเวลาที่กรมบัญชีกลางกำหนด กรณีไม่สามารถปฏิบัติได้ให้ขอทำความเข้าใจกับกระทรวงการคลัง

มาตรฐานและหลักเกณฑ์การบริหารจัดการความเสี่ยง สำหรับหน่วยงานของรัฐ



กรอบแนวคิดสากลการบริหารจัดการความเสี่ยง

- ▶ Enterprise Risk Management : Integrated framework Version 2004 by COSO
- ▶ Enterprise Risk Management : Integrating with Strategy and Performance Version 2017 by COSO
- ▶ ISO 31000 : 2009 Risk Management
- ▶ ISO 31000 : 2018 Risk Management
- ▶ King report on Corporate Governance

ประเภทความเสี่ยง

➤ ความเสี่ยงด้านกลยุทธ์

ความเสี่ยงที่มีผลกระทบต่อทิศทาง หรือ ภารกิจหลักขององค์กร หรือมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร เนื่องมาจากการเมือง เศรษฐกิจ ความเปลี่ยนแปลงของสถานการณ์ภายนอก ผู้ใช้บริการ ฯลฯ หรือความเสี่ยงที่เกิดจากการกระบวนกรตัดสินใจเชิงกลยุทธ์ผิดพลาด รวมถึงความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงานและนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยภายใน และสภาพแวดล้อมภายนอก อันส่งผลกระทบต่อการบรรลุวิสัยทัศน์ พันธกิจ หรือสถานะขององค์กร

➤ ความเสี่ยงทางด้านการปฏิบัติตามกฎระเบียบ

ความเสี่ยงที่เกิดจากการละเมิดหรือไม่ปฏิบัติตามกฎระเบียบ ข้อบังคับ ข้อสัญญา และข้อกำหนดที่เกี่ยวข้องกับการดำเนินงานขององค์กร เช่น การทุจริต การไม่ปฏิบัติตามเงื่อนไขสัญญา การไม่ปฏิบัติตามกฎหมายเกี่ยวกับผลกระทบสิ่งแวดล้อม

ความเสี่ยง

➤ ความเสี่ยงทางการเงิน

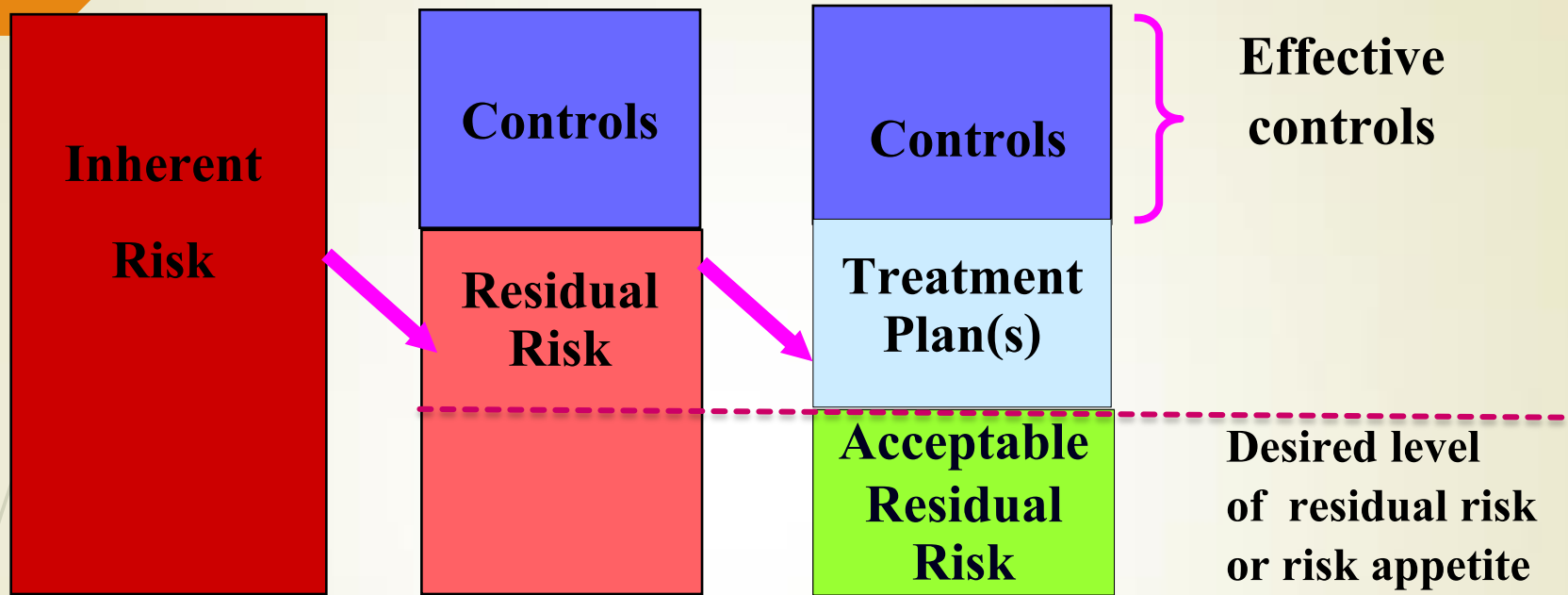
ความเสี่ยงเกี่ยวกับสถานะและการดำเนินงานทางการเงิน เช่น การเบิกจ่ายงบประมาณไม่เป็นไปตามแผน งบประมาณถูกตัด งบประมาณที่ได้รับไม่สอดคล้องกับสถานการณ์ของภารกิจที่เปลี่ยนแปลงไป ทำให้การจัดสรรไม่พอเพียง จนกระทบการดำเนินงานขององค์กรในการบรรลุเป้าหมายตามพันธกิจ เนื่องมาจากการขาดการจัดหาข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงาน เพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้อง เหมาะสม ทำให้ขาดประสิทธิภาพ และไม่ทันต่อสถานการณ์ ซึ่งส่งผลต่อการตัดสินใจทางการเงิน หรือการบริหารงบประมาณที่ผิดพลาด ส่งผลกระทบต่อสถานะการเงินขององค์กร

➤ ความเสี่ยงด้านปฏิบัติการ

ความเสี่ยงเนื่องจากการปฏิบัติงานภายในองค์กร อันเกิดจากกระบวนการ บุคลากร ความเพียงพอของข้อมูล ส่งผลกระทบต่อการดำเนินงานขององค์กร เช่น ขาดการบริหารโครงการที่ดี ขาดบุคลากรที่มีคุณภาพ การใช้งานระบบเทคโนโลยีสารสนเทศไม่เต็มประสิทธิภาพ

แนวคิดของการบริหารความเสี่ยง

15



ความเสี่ยงที่มีอยู่ดั้งเดิม/ก่อนการควบคุม คือ ความเสี่ยงที่เกิดขึ้นจากการดำเนินกิจกรรมต่างๆ ขององค์กร โดยที่ยังไม่ได้ดำเนินการใดๆ เพื่อลดผลกระทบหรือโอกาสเกิดของความเสี่ยงนั้น

ความเสี่ยงที่เหลืออยู่ก่อนการจัดการ/หลังการควบคุม คือ ความเสี่ยงคงเหลือหลังจากพิจารณาถึงการควบคุมต่างๆ ที่มีในปัจจุบัน การประเมินระดับความเสี่ยงหลังการควบคุม ทำให้สามารถพิจารณาได้ว่า การควบคุมที่มีอยู่ในปัจจุบันมีความเพียงพอหรือไม่ หรือมีการควบคุมเกินความจำเป็น หากระดับความเสี่ยงหลังการควบคุมอยู่ในระดับที่สูงเกินกว่าระดับที่องค์กรยอมรับได้ จะต้องกำหนดแผนจัดการความเสี่ยงและดำเนินการตามแผนดังกล่าว

**** พิจารณาค่าความคุ้มครองระหว่างต้นทุน/ดช. กับ ประโยชน์ที่ได้รับ**

องค์ประกอบของ COSO ERM 2004

1. สภาพแวดล้อมภายใน Internal Environment
2. กำหนดวัตถุประสงค์ Objective Setting
3. ระบุความเสี่ยง Event Identification
4. การประเมินความเสี่ยง Risk Assessment
5. การตอบสนองความเสี่ยง Risk Response
6. กิจกรรมการควบคุม Control Activities
7. สารสนเทศและการสื่อสาร Information&Communication
8. การติดตาม Monitoring

องค์ประกอบของ COSO ERM 2004

1. สภาพแวดล้อมภายใน Internal Environment

กำหนดสภาพแวดล้อมภายในองค์กรให้สนับสนุนการบริหารความเสี่ยงทั่วทั้งองค์กร เช่น การกำหนดระดับความเสี่ยงที่ยอมรับได้ วัฒนธรรมองค์กร การเพิ่มขีดความสามารถของบุคลากร โครงสร้างองค์กร เป็นต้น

- คณะกรรมการและผู้บริหารควรกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) และช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance)
- คณะกรรมการและผู้บริหารควรมีหน้าที่กำกับดูแลการบริหารความเสี่ยงองค์กร ให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้

สภาพแวดล้อมภายใน (ต่อ)

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ระดับของความเสี่ยงที่กำหนดขึ้นในภาพรวม ซึ่งองค์กรสามารถยอมรับได้ในการมุ่งไปสู่พันธกิจ (หรือวิสัยทัศน์) ขององค์กรนั้น สามารถระบุได้ในลักษณะเชิงปริมาณ หรือ เชิงคุณภาพ การระบุความเสี่ยงที่ยอมรับได้ อยู่บนพื้นฐานของสถานการณ์ปัจจุบัน และต้องมีการทบทวนอย่างต่อเนื่อง โดยพิจารณาจากปัจจัยภายใน-นอก เช่น ระดับการหลีกเลี่ยงหรือความกลัวความเสี่ยง ความต้องการของผู้มีส่วนได้เสีย ศักยภาพองค์กร เศรษฐกิจ สังคม

ขั้นตอนการกำหนดระดับความเสี่ยงที่ยอมรับได้

1. วิเคราะห์ความคาดหวังของผู้มีส่วนได้ส่วนเสียทั้งจากภายในและภายนอกองค์กรเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้
2. วิเคราะห์เชื่อมโยงกับกลยุทธ์และวัตถุประสงค์การดำเนินงานขององค์กร และข้อมูลความเสี่ยงขององค์กรในแต่ละด้าน
3. กำหนดระดับความเสี่ยงที่ยอมรับได้ขององค์กร โดยพิจารณาจากผลที่ได้จากขั้นตอนที่ 1 – 2

ช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับความเบี่ยงเบนที่ยอมรับได้ที่สัมพันธ์กับการบรรลุวัตถุประสงค์ หรือระดับการเบี่ยงเบนความเสี่ยงที่ยอมรับได้จากตัววัดผลการดำเนินงานที่เกี่ยวข้องกับการบรรลุวัตถุประสงค์ขององค์กร โดยสามารถวัดได้และสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

สภาพแวดล้อมภายใน (ต่อ)

ตัวอย่าง ช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้

องค์กรแห่งหนึ่งมีเป้าหมายในการให้บริการที่ลูกค้าพึงพอใจ ซึ่งในการพิจารณาช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้นั้น ผู้บริหารได้ระบุว่า

- ค่าเป้าหมายของระดับความพึงพอใจของลูกค้า เท่ากับร้อยละ 85 มาเป็นเวลานานหลายปี ซึ่งองค์กรก็สามารถดำเนินงานได้ตามค่าเป้าหมายนี้มาโดยตลอด
- ค่าเฉลี่ยของอุตสาหกรรม เท่ากับร้อยละ 80 และมีแนวโน้มคงที่
- หากความพึงพอใจของลูกค้าลดลงเป็นการชั่วคราว และยังคงอยู่ในระดับที่สูงกว่าค่าเฉลี่ยของอุตสาหกรรม พบว่ามีผลกระทบน้อยมากต่อการตัดสินใจให้บริการของลูกค้า
- หากจะให้ความพึงพอใจของลูกค้าเพิ่มขึ้นสูงกว่าร้อยละ 87 ต้องใช้ทรัพยากรเพิ่มขึ้นอย่างมากและไม่คุ้มกับผลที่ได้รับ
- องค์กรกำลังถูกจับตามองจากสาธารณชนและมีการวิพากษ์วิจารณ์ถึงการที่องค์กรไม่สามารถลดต้นทุนได้

จากข้อมูลดังกล่าว จึงกำหนดว่าควรคงค่าเป้าหมายของระดับความพึงพอใจของลูกค้าที่ร้อยละ 85 และมีช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้อยู่ระหว่างร้อยละ 82-86

สภาพแวดล้อมภายใน (ต่อ)

องค์กรควรจัดให้มี นโยบายการบริหารความเสี่ยง (Risk Management Policy) ที่เป็นลายลักษณ์อักษร โดยให้แสดงถึงความมุ่งมั่นในการให้ความสำคัญกับการบริหารความเสี่ยง กระบวนการปฏิบัติในองค์กร และบทบาทหน้าที่ ความรับผิดชอบในด้านการบริหารความเสี่ยง จัดให้มีโครงสร้างองค์กรที่สนับสนุนให้เกิดการบริหารความเสี่ยงที่มี ประสิทธิภาพ มีการกำหนดสายการรายงาน การมอบอำนาจและความรับผิดชอบ สามารถแก้ไขปัญหาต่างๆ ได้อย่าง เหมาะสม รวมทั้งให้มีการกำหนดเจ้าของความเสี่ยง (Risk Owner) ที่จะต้องดำเนินการรับผิดชอบในการจัดการบริหารความเสี่ยงนั้นๆ นอกจากนี้ ควรมีการกำหนดผู้รับผิดชอบหลัก ในการพัฒนา วางระบบ และติดตามการบริหารความเสี่ยงขององค์กร

ในการจัดทำนโยบายการบริหารความเสี่ยง ควรมีหัวข้อ

1. วัตถุประสงค์ของนโยบาย
2. คำจำกัดความของความเสี่ยง
3. บทบาทและความรับผิดชอบ
4. การทบทวนนโยบายการบริหารความเสี่ยง
5. การติดตามและการรายงานผล

สภาพแวดล้อมภายใน (ต่อ)

ตัวอย่างนโยบายการบริหารความเสี่ยง

บทบทและความรับผิดชอบ

1. คณะกรรมการ(หรือหัวหน้าหน่วยงานของรัฐ)เป็นผู้กำกับดูแลและสนับสนุนการนำนโยบายการบริหารความเสี่ยงนี้ไปปฏิบัติใน...ชื่อหน่วยงานของรัฐ...ผ่านทางคณะกรรมการบริหารความเสี่ยง(และหัวหน้าหน่วยงานของรัฐ)ของ...ชื่อหน่วยงานของรัฐ...
2. คณะกรรมการบริหารความเสี่ยง เป็นผู้กำกับดูแลการนำนโยบายและกรอบการบริหารความเสี่ยงไปปฏิบัติภายในองค์กร ติดตามกระบวนการบริหารความเสี่ยง ความเพียงพอของการจัดการความเสี่ยงที่สำคัญ และรายงานให้คณะกรรมการ(หรือหัวหน้าหน่วยงานของรัฐ)ทราบเป็นระยะ
3. ผู้บริหารเป็นผู้รับผิดชอบในการนำนโยบายการบริหารความเสี่ยงไปปฏิบัติ และติดตามการนำไปใช้อย่างต่อเนื่อง โดยได้รับการสนับสนุนจากคณะกรรมการบริหารความเสี่ยง
4. บุคลากรทุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและคู่มือการบริหารความเสี่ยง

สภาพแวดล้อมภายใน (ต่อ)

ตัวอย่างนโยบายการบริหารความเสี่ยง

การทบทวนนโยบายการบริหารความเสี่ยง

1. ในกรณีที่ผู้บริหารพบว่านโยบายการบริหารความเสี่ยงไม่เหมาะสมกับสภาพการดำเนินงาน ต้องนำเสนอต่อคณะกรรมการ(หรือหัวหน้าหน่วยงานของรัฐ) ผ่านคณะกรรมการบริหารความเสี่ยง เพื่อขออนุมัติในการปรับปรุงนโยบายการบริหารความเสี่ยง
2. คณะกรรมการบริหารความเสี่ยงจะทบทวนนโยบายการบริหารความเสี่ยงทุกปี และนำเสนอต่อคณะกรรมการ(หรือหัวหน้าหน่วยงานของรัฐ) เพื่อให้มั่นใจว่านโยบายดังกล่าวยังเหมาะสมกับสภาพแวดล้อมการดำเนินงานขององค์กร

ทั้งนี้ นโยบายนี้มีผลบังคับใช้กับกรรมการ ผู้บริหาร และบุคลากรทุกคน นับแต่นี้เป็นต้นไป
อนุมัติโดย

(.....)

ประธานกรรมการ(หัวหน้าหน่วยงานของรัฐ)

วันที่

ตัวอย่างบทบาท อำนาจหน้าที่ความรับผิดชอบ

คณะกรรมการ

เห็นชอบนโยบายและควบคุมดูแลการบริหารความเสี่ยง และการควบคุมภายในขององค์กรให้เพียงพอเหมาะสม
คณะกรรมการตรวจสอบ

1. กำกับดูแลให้มีระบบการตรวจสอบที่เหมาะสม เพียงพอ
2. กำกับดูแลให้มีระบบข้อมูล ระบบบัญชี และรายงานทางการเงิน รายงานทางการบริหารที่ถูกต้อง เพียงพอและเชื่อถือได้
3. กำกับดูแลให้มีการปฏิบัติตามกฎ ระเบียบ ข้อบังคับ มติคณะรัฐมนตรี และนโยบายที่คณะกรรมการกำหนด
4. กำกับดูแลให้มีการดำเนินงานเป็นไปอย่างมีประสิทธิภาพ และประหยัด

คณะกรรมการบริหารความเสี่ยง (RMC) มีหน้าที่ดังนี้

1. พิจารณา อนุมัติ นโยบายการบริหารความเสี่ยง และคู่มือการบริหารความเสี่ยง
2. พิจารณาอนุมัติความเสี่ยงระดับองค์กร แผนบริหารความเสี่ยง และเกณฑ์ประเมินความเสี่ยง
3. ติดตามผลการบริหารความเสี่ยงระดับองค์กรอย่างสม่ำเสมอ ส่งเสริมสนับสนุนให้คำแนะนำในการทบทวน ปรับปรุงมาตรการต่างๆ ที่กำหนดในแผนบริหารความเสี่ยง และแก้ไขปัญหาที่เกี่ยวกับการบริหารความเสี่ยง
4. รายงานผลการบริหารความเสี่ยง ต่อคณะกรรมการ และคณะกรรมการตรวจสอบ

ตัวอย่างบทบาท อำนาจหน้าที่ความรับผิดชอบ

คณะกรรมการบริหารความเสี่ยง (RMS) มีหน้าที่ดังนี้

1. กำกับดูแลการดำเนินการตามแผนงานเกี่ยวกับการบริหารความเสี่ยง
2. จัดทำนโยบายการบริหารความเสี่ยง คู่มือการบริหารความเสี่ยง ความเสี่ยงระดับองค์กร แผนบริหารความเสี่ยง เกณฑ์ประเมินความเสี่ยง
3. ติดตามประเมินผลการดำเนินงานเรื่องการบริหารความเสี่ยงให้เป็นไปตามเป้าหมาย
4. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยง
5. ส่งเสริมให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการปฏิบัติงานปกติและเป็นวัฒนธรรม
6. เสนอแนะแนวทางปรับปรุงแก้ไขปัญหาอุปสรรค จัดทำแผนบริหารความเสี่ยงในภาพรวมองค์กร

ผู้อำนวยการองค์การคลังสินค้า มีหน้าที่ดังนี้

1. ติดตามและให้ข้อสังเกตในการบริหารความเสี่ยง
2. สนับสนุน ส่งเสริมการบริหารความเสี่ยง ให้เป็นกระบวนการที่ต่อเนื่อง และเป็นวัฒนธรรมขององค์กร
รอง/ผู้ช่วยผู้อำนวยการ

1. วางแนวทางและติดตามผลการบริหารความเสี่ยงขององค์กร พร้อมกับมอบหมายผู้รับผิดชอบดำเนินการ
2. สนับสนุน ส่งเสริมการดำเนินการตามแผนการบริหารความเสี่ยงขององค์กรให้มีความเชื่อมโยงและบูรณาการทั่วทั้งองค์กร

ตัวอย่างบทบาท อำนาจหน้าที่ความรับผิดชอบ

ผู้อำนวยการสำนัก/กอง/ศูนย์

1. ระบุ ประเมินความเสี่ยง รวมทั้งจัดทำแผนบริหารความเสี่ยงตามแนวทางและนโยบายที่ผู้บริหารระดับสูงมอบหมาย
2. ประเมิน ติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยง ตามกำหนดเวลา
3. สนับสนุน ส่งเสริมการดำเนินการตามแผนบริหารความเสี่ยง ของบุคลากรในหน่วยงาน ให้มีประสิทธิภาพ

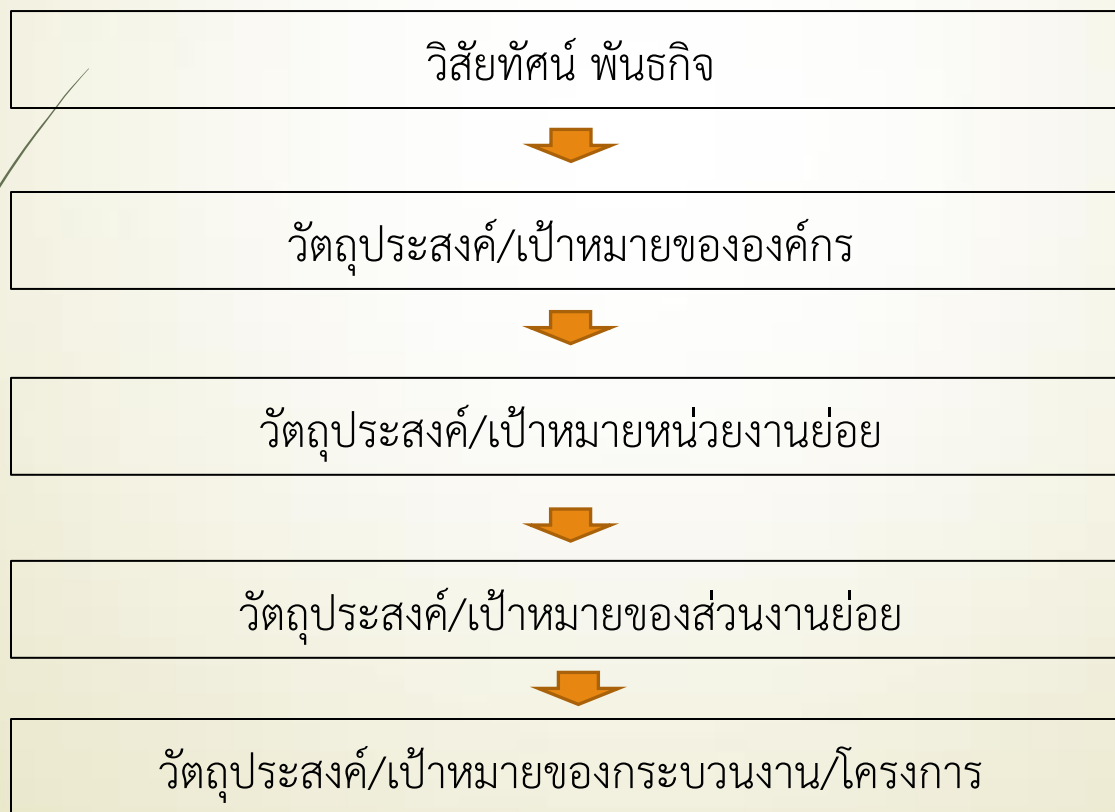
หน้าส่วนงาน /ผู้ปฏิบัติงาน

1. ระบุ ประเมินความเสี่ยง กำหนดมาตรการ/แผนงานในแผนบริหารความเสี่ยง และรับผิดชอบการนำแผนงานไปปฏิบัติตามแนวทางที่กำหนดได้อย่างเหมาะสมและมีประสิทธิภาพ
2. ปฏิบัติงาน ดูแลและติดตามงานต่าง ๆ ตามกรอบและกระบวนการบริหารความเสี่ยงรวมถึงรายงาน ความเสี่ยงของการปฏิบัติงานรายวันให้ผู้บริหารหน่วยงานทราบอย่างสม่ำเสมอ
3. ส่งเสริม สนับสนุน ให้ความร่วมมือ และปฏิบัติตามกรอบการบริหารความเสี่ยงของหน่วยงานที่ปฏิบัติงานอยู่ในขณะนั้น เพื่อให้การบริหารความเสี่ยงเป็นวัฒนธรรมในการปฏิบัติงานประจำตามปกติ

องค์ประกอบของ COSO ERM 2004

2. กำหนดวัตถุประสงค์ Objective Setting

กำหนดวัตถุประสงค์ที่ชัดเจน และสอดคล้องกัน ทั้งวัตถุประสงค์ด้านกลยุทธ์ และวัตถุประสงค์ด้านการดำเนินงานขององค์กร และจะต้องเป็นไปในแนวทางเดียวกันกับระดับความเสี่ยงที่ยอมรับได้ขององค์กร



กำหนดวัตถุประสงค์ (ต่อ)

ตัวอย่างวัตถุประสงค์

- เพิ่มระดับการบริการของศูนย์บริการลูกค้า (Call Center) ให้ลูกค้ามีความพึงพอใจที่มากกว่าปีที่ผ่านมาอย่างน้อย 5% ภายในธันวาคม 2563
- ขยายการดำเนินงานด้านสินเชื่รถยนต์ให้ครอบคลุมทุกจังหวัดในภาคตะวันออกเฉียงเหนือ โดยให้วงเงินเพิ่มขึ้นเป็นสองเท่าของปีที่ผ่านมา ภายใน 3 ปีข้างหน้า
- พัฒนาบุคลากรในหน่วยงานตรวจสอบภายใน ให้ได้เป็นผู้ตรวจสอบภายในวิชาชีพอย่างน้อย 5 คน ภายในธันวาคม 2563

องค์ประกอบของ COSO ERM 2004

3. ระบุความเสี่ยง Event Identification

ระบุเหตุการณ์ที่อาจจะเกิดขึ้นและส่งผลกระทบต่อองค์กรและจะต้องมีความเข้าใจถึงปัจจัยต่างๆ ทั้งภายในและภายนอกองค์กร ทั้งเหตุการณ์ที่เคยเกิดขึ้นมาแล้วในอดีต และการคาดการณ์ในอนาคต ขั้นตอนการระบุเหตุการณ์

1. ศึกษา และพิจารณาถึงเหตุการณ์ที่จะทำให้ไม่บรรลุวัตถุประสงค์ต่างๆ โดยพิจารณาทั้งปัจจัยทั้งภายในและภายนอก เหตุการณ์ที่เกิดขึ้นแล้ว หรือคาดว่าจะเกิดขึ้นในอนาคต
2. สรุปประเด็นเหตุการณ์ที่อาจเกิดขึ้นซึ่งมีผลกระทบต่อการบรรลุวัตถุประสงค์ และสาเหตุของเหตุการณ์ หรือความเสี่ยงดังกล่าว ให้เป็นลายลักษณ์อักษร เพื่อหารือร่วมกัน หากเหตุการณ์ที่มีผลกระทบในเชิงลบถือเป็นความเสี่ยงที่ต้องประเมินและจัดการความเสี่ยงนั้น สำหรับเหตุการณ์ที่มีผลกระทบในเชิงบวกเป็นโอกาส ซึ่งควรนำไปพิจารณาอีกครั้งในกระบวนการกำหนดวัตถุประสงค์ และกลยุทธ์ในการดำเนินงานต่อไป
 - ต้องระบุสาเหตุของความเสี่ยงด้วยทุกครั้ง
 - ระบุให้ครบทุกสาเหตุที่ทำให้เกิดความเสี่ยงดังกล่าว

เพื่อให้สามารถกำหนดแผนจัดการความเสี่ยงให้ได้ตรงกับสาเหตุที่ทำให้เกิดความเสี่ยง และสามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล

ระบุความเสี่ยง (ต่อ)

เลขที่ ความเสี่ยง	ความเสี่ยง	เลขที่ สาเหตุ	สาเหตุความเสี่ยง
R1	การจำหน่ายสินค้าและ/หรือ การให้บริการ มีปริมาณลดลง	C1	เหตุการณ์วิกฤตน้ำท่วม เนื่องจากน้ำท่วมส่งผลกระทบต่อสภาพเศรษฐกิจของ ประเทศ และความสามารถในการใช้จ่ายของประชาชน ส่งผลกระทบให้อุปสงค์ ลดลง
R2	การขาดความต่อเนื่อง ในการดำเนินงาน	C1	เจ้าหน้าที่มีการสับเปลี่ยนหมุนเวียนกันบ่อย
		C2	การเกิดเหตุการณ์ความไม่สงบทางการเมือง
		C3	การเกิดความเสียหายด้านระบบเทคโนโลยีสารสนเทศในการบริหารจัดการธุรกิจ
R3	คุณภาพสินค้าลดต่ำลง	C1	การตรวจสอบคุณภาพสินค้าไม่ทั่วถึง

องค์ประกอบของ COSO ERM 2004

4. การประเมินความเสี่ยง Risk Assessment

ประเมินความเสี่ยงที่ชัดเจนและเป็นระบบ โดยการประเมินความเสี่ยงจะมีการพิจารณาทั้งด้านโอกาสที่ความเสี่ยงจะเกิดขึ้น และผลกระทบหากความเสี่ยงเกิดขึ้นจริง การประเมินความเสี่ยงสามารถทำได้ทั้งในเชิงคุณภาพ และในเชิงปริมาณ และสามารถทำการประเมินได้ตั้งแต่ระดับองค์กรไปจนถึงระดับหน่วยงาน

- วิเคราะห์โอกาสที่ความเสี่ยงดังกล่าวจะเกิดขึ้น และผลกระทบหากความเสี่ยงเกิดขึ้นจริง โดยการประเมินความเสี่ยงจะต้องประเมินทั้งความเสี่ยงที่มีอยู่ตามธรรมชาติ (Inherent Risk) และความเสี่ยงที่เหลืออยู่หลังการตอบสนองต่อความเสี่ยง (Residual Risk)

- อาจประเมินเป็นด้านต่างๆ เช่น ความเสี่ยงด้านกลยุทธ์ Strategic Risk ด้านปฏิบัติการ Operational Risk การเงิน Financial Risk และการปฏิบัติตามกฎระเบียบ Compliance Risk (S-O-F-C)

ความเสี่ยง คืออะไร ???



- โอกาสที่จะเกิดความผิดพลาดความเสียหาย
- การรื้อไหล ความสูญเสียเปล่า หรือ
- เหตุการณ์ซึ่งไม่พึงประสงค์ ที่ทำให้งานไม่ประสบ
ความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด

การประเมินความเสี่ยง (ต่อ)

การวิเคราะห์ความเสี่ยง

ระดับหรือความรุนแรงของความเสี่ยง พิจารณาจากผลกระทบ (Impact) และโอกาสที่จะเกิดขึ้น (Likelihood) หรือ $I \times L$

ตัวอย่างผังจัดระดับความเสี่ยง

ความรุนแรงของผลกระทบ	โอกาสที่จะเกิดขึ้น				
	1 - น้อยมาก	2 - น้อย	3 - ปานกลาง	4 - สูง	5 - สูงมาก
5 - สูงมาก	ต่ำ	กลาง	สูง	สูงมาก	สูงมาก
4 - สูง	ต่ำ	ต่ำ	กลาง	สูง	สูงมาก
3 - ปานกลาง	ต่ำมาก	ต่ำ	ต่ำ	กลาง	สูง
2 - น้อย	ต่ำมาก	ต่ำ	ต่ำ	ต่ำ	กลาง
1 - น้อยมาก	ต่ำมาก	ต่ำมาก	ต่ำมาก	ต่ำ	ต่ำ

ตัวอย่างเกณฑ์ประเมินโอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง

โอกาสที่จะเกิดความเสี่ยง	เปอร์เซ็นต์โอกาสที่จะเกิดขึ้น	ระดับคะแนน
สูงมาก	มากกว่า 80 %	5
สูง	70-79 %	4
ปานกลาง	60-69 %	3
น้อย	50-59 %	2
น้อยมาก	น้อยกว่า 50 %	1

โอกาสที่จะเกิดความเสี่ยง	ความถี่ที่เกิดขึ้น (เฉลี่ย)	ระดับคะแนน
สูงมาก	มากกว่า 1 ครั้งต่อเดือน	5
สูง	ระหว่าง 1-6 เดือนต่อครั้ง	4
ปานกลาง	ระหว่าง 6-12 เดือนต่อครั้ง	3
น้อย	มากกว่า 1 ปีต่อครั้ง	2
น้อยมาก	มากกว่า 5 ปีต่อครั้ง	1

ตัวอย่างเกณฑ์ประเมินผลกระทบต่อการเงิน

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	มากกว่า 10 ล้านบาท	5
สูง	มากกว่า 5 แสนบาท - 10 ล้านบาท	4
ปานกลาง	มากกว่า 1 แสนบาท - 5 แสนบาท	3
น้อย	1 หมื่นบาท - 1 แสนบาท	2
น้อยมาก	น้อยกว่า 1 หมื่นบาท	1

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	เสียค่าใช้จ่ายเกิน ๑,๐๐๐,๐๐๐ บาท	๕
สูง	เสียค่าใช้จ่าย ๒๕๐,๐๐๑ - ๑,๐๐๐,๐๐๐ บาท	๔
ปานกลาง	เสียค่าใช้จ่าย ๕๐,๐๐๑ - ๒๕๐,๐๐๐ บาท	๓
น้อย	เสียค่าใช้จ่าย ๑๐,๐๐๑ - ๕๐,๐๐๐ บาท	๒
น้อยมาก	เสียค่าใช้จ่ายไม่เกิน ๑๐,๐๐๐ บาท	๑

ตัวอย่างเกณฑ์ประเมินผลกระทบต่อด้านชื่อเสียง

35

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	มีการเผยแพร่ข่าวเกิน 1 เดือน /ทางสื่อมวลชนทั้งในประเทศ+ ตปท.	๕
สูง	มีการเผยแพร่ข่าวไม่เกิน 1 เดือน /ทางสื่อมวลชนในประเทศ	๔
ปานกลาง	มีการเผยแพร่ข่าวไม่เกิน 1 สัปดาห์/ทางหนังสือพิมพ์ไม่เกิน 2 ฉบับ	๓
น้อย	มีการเผยแพร่ข่าวไม่เกิน 1 วัน/ทางหนังสือพิมพ์ไม่เกิน 1 ฉบับ	๒
น้อยมาก	ไม่มีการเผยแพร่ข่าว	๑

ตัวอย่างเกณฑ์ประเมินผลกระทบต่อด้านผู้ใช้บริการ

ผลกระทบ ต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	ผู้ใช้บริการลดลงมากกว่า 50 คน ต่อเดือน	5
สูง	ผู้ใช้บริการลดลงตั้งแต่ 40-50 คน ต่อเดือน	4
ปานกลาง	ผู้ใช้บริการลดลงตั้งแต่ 30-39 คน ต่อเดือน	3
น้อย	ผู้ใช้บริการลดลงตั้งแต่ 20-29 คน ต่อเดือน	2
น้อยมาก	ผู้ใช้บริการลดลงไม่เกิน 19 คน ต่อเดือน	1

องค์ประกอบของ COSO ERM 2004

5. การตอบสนองความเสี่ยง Risk Response

กำหนดการตอบสนองต่อความเสี่ยงให้สอดคล้องกับระดับความรุนแรงของความเสี่ยง และช่วงความเปี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ แนวทางในการตอบสนองต่อความเสี่ยงที่สามารถพิจารณาปฏิบัติมี 4 ทาง คือ การหลีกเลี่ยงความเสี่ยง การลดความเสี่ยง การถ่ายโอนความเสี่ยง และการยอมรับความเสี่ยง

ความเสี่ยง	กลยุทธ์จัดการความเสี่ยง	คำอธิบายวิธีการจัดการความเสี่ยง	ต้นทุน	ประโยชน์
	หลีกเลี่ยง			
	ลด			
	ถ่ายโอน			
	ยอมรับ			
สรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง				

องค์ประกอบของ COSO ERM 2004

6. กิจกรรมการควบคุม Control Activities

กำหนดกิจกรรมการควบคุม เพื่อให้มั่นใจว่าองค์กรได้มีการดำเนินการตามแนวทางการตอบสนองต่อความเสี่ยงที่ได้กำหนดไว้ กิจกรรมการควบคุมสามารถจัดประเภทได้ตามลักษณะของความสัมพันธ์กับวัตถุประสงค์ขององค์กร ซึ่งได้แก่ กลยุทธ์ การปฏิบัติการ การรายงาน และการปฏิบัติตามกฎระเบียบ สะท้อนผ่านทางนโยบาย และขั้นตอนการปฏิบัติ อย่างเหมาะสมและทันกาล ผู้บริหารองค์กรสามารถพิจารณาเลือกประเภทของกิจกรรมควบคุมที่มีอยู่หลากหลาย เช่น การควบคุมเชิงป้องกัน การควบคุมเชิงค้นหา การควบคุมด้านการบริหาร การควบคุมระบบสารสนเทศ

ตัวอย่างกิจกรรมการควบคุม

1. การกำหนดระเบียบ ข้อบังคับ วิธีปฏิบัติ
2. การแบ่งแยกหน้าที่ความรับผิดชอบ
3. การกำหนดขอบเขต อำนาจหน้าที่ความรับผิดชอบ
4. การจัดทำบัญชี ทะเบียน รายงาน การกระทบยอด
5. การควบคุมทางกายภาพ
6. การสับเปลี่ยนหมุนเวียนงาน
7. การควบคุมการประมวลผลข้อมูล
8. การกำหนดดัชนีวัดผลการดำเนินงาน

ฯลฯ



องค์ประกอบของ COSO ERM 2004

7. สารสนเทศและการสื่อสาร Information&Communication

กำหนดให้มีสารสนเทศและการสื่อสารที่สนับสนุนการบริหารความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในองค์กรและภายนอกองค์กรควรได้รับการบันทึกและสื่อสารอย่างเหมาะสมและทันกาล โดยเฉพาะข้อมูลสนับสนุนที่มีความสำคัญเกี่ยวกับการบ่งชี้ ประเมิน และการตอบสนองต่อความเสี่ยง เพื่อให้องค์กรสามารถตอบสนองต่อความเสี่ยงได้อย่างรวดเร็วและมีประสิทธิภาพ รัฐวิสาหกิจควรมีการสื่อสารให้บุคลากรมีความตระหนักและเข้าใจการบริหารความเสี่ยง

องค์ประกอบของ COSO ERM 2004

8. การติดตาม Monitoring

กำหนดให้การติดตามการบริหารความเสี่ยงเป็นไปอย่างสม่ำเสมอและต่อเนื่อง โดยผสมผสานให้เข้ากับกระบวนการดำเนินการต่างๆ ตามปกติของธุรกิจ และหรือติดตามแยกต่างหาก/อย่างเป็นอิสระ ควรมีการติดตามดูแลกิจกรรมต่างๆ ที่เกี่ยวข้องกับการบริหารความเสี่ยง เพื่อให้สามารถปรับเปลี่ยนการบริหารความเสี่ยงหรือประยุกต์ใช้ให้เหมาะสมกับการเปลี่ยนแปลงต่างๆ ได้อย่างทันกาล

- มอบหมายให้หน่วยงานบริหารความเสี่ยงเป็นผู้รับผิดชอบหลักในการติดตามการบริหารความเสี่ยง โดยหน่วยงานบริหารความเสี่ยงสามารถกำหนดให้เจ้าของความเสี่ยงเป็นผู้ติดตามและรวบรวมข้อมูลเพื่อรายงานความคืบหน้าของแผนจัดการความเสี่ยงต่อหน่วยงานบริหารความเสี่ยงเป็นระยะ

- หน่วยงานบริหารความเสี่ยงควรคัดกรองและวิเคราะห์ข้อมูลอย่างสม่ำเสมอตามความเหมาะสมของระดับความรุนแรงและข้อมูล เช่น อาจมีการรวบรวมและวิเคราะห์คัดกรองเป็นรายเดือน หรือรายไตรมาส เพื่อนำเสนอต่อคณะกรรมการบริหารความเสี่ยง

การบริหารจัดการความเสี่ยงสากล

2. ISO 31000

ISO 31000 เป็นอีกมาตรฐานหนึ่งที่ได้รับความนิยม และเพิ่มขึ้นอย่างรวดเร็ว และปัจจุบันมีหลายองค์กรของไทยโดยเฉพาะภาคเอกชนและรัฐวิสาหกิจบางแห่งมีการนำมาใช้ทดแทนแนวของ COSO หรือ นำมาแก้ไขจุดอ่อนของ COSO เพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพขึ้น ประกอบด้วย 5 ขั้นตอนดังนี้

1. การสื่อสารและการให้คำแนะนำ (communicate and consult)
2. การกำหนดสภาพแวดล้อม (establish the context)
3. การประเมินความเสี่ยง (risk assessment)
4. การจัดการความเสี่ยง (treat the risks)
5. การเฝ้าระวังติดตาม และการทบทวนความเสี่ยง (monitor and review)

การบริหารจัดการความเสี่ยงสากล

2. ISO 31000

ขั้นตอนที่ 1: การสื่อสารและการให้คำแนะนำ

เป็นการบอกกล่าวให้แก่ผู้ที่มีส่วนเกี่ยวข้องทั้งภายในและภายนอกองค์กร รวมถึงการให้คำแนะนำเกี่ยวกับขั้นตอนและกระบวนการบริหาร ความเสี่ยง เพื่อให้เกิดความเข้าใจในการตัดสินใจดำเนินการบริหารความเสี่ยง ทราบถึงความจำเป็นและขอบเขต โดยสื่อสารกับผู้ที่เกี่ยวข้องเพื่อให้เกิดความเข้าใจในแนวคิด หลักการและวิธีปฏิบัติที่ตรงกัน ตลอดจนสามารถ วิเคราะห์ และจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

การบริหารจัดการความเสี่ยงสากล

2. ISO 31000

ขั้นตอนที่ 2: การกำหนดสภาพแวดล้อม เป็นการระบุสภาพแวดล้อมทั้งภายนอกและภายในขององค์กรที่มีความสัมพันธ์และเกี่ยวข้องกับองค์กร ทำให้เกิดผลกระทบต่อองค์กร จึงต้องนำไปสู่กระบวนการ บริหารความเสี่ยง

2.1 การกำหนดสภาพแวดล้อมภายนอก องค์กรประกอบต่าง ๆ ที่อยู่ภายนอกองค์กรที่มีอิทธิพลต่อความสำเร็จในวัตถุประสงค์ขององค์กร เช่น เศรษฐกิจ การเมือง วัฒนธรรม กฎหมาย ข้อบังคับ การเงิน สภาพแวดล้อมในการแข่งขันทั้งภายในประเทศและต่างประเทศ รวมถึงการยอมรับของผู้มีส่วนได้ส่วนเสียภายนอก เป็นต้น

2.2 การกำหนดสภาพแวดล้อมภายใน สิ่งที่อยู่ภายในองค์กร ซึ่งมีอิทธิพลต่อความสำเร็จของวัตถุประสงค์ขององค์กร โดยกระบวนการบริหารความเสี่ยง จะต้อง สอดคล้องในทิศทางเดียวกันกับวัฒนธรรมกระบวนการ และโครงสร้างขององค์กร เช่น นโยบาย วัตถุประสงค์ วิสัยทัศน์พันธกิจ และกลยุทธ์ที่จะต้องประสบ ความสำเร็จ ชัดความสามารถขององค์กร ในรูปของทรัพยากร และความรู้ ระบบสารสนเทศ ผู้มีส่วนได้ส่วนเสียภายในองค์กร การรับรู้ คุณค่า และวัฒนธรรมองค์กร โครงสร้าง เช่น ระบบการจัดการ บทบาทหน้าที่ และความรับผิดชอบ เป็นต้น

การบริหารจัดการความเสี่ยงสากล

2. ISO 31000

ขั้นตอนที่ 3 : การประเมินความเสี่ยง ประกอบด้วยกระบวนการหลัก 3 กระบวนการ ดังนี้

3.1 การระบุความเสี่ยง

3.2 การวิเคราะห์ความเสี่ยง

3.3 การประเมินความเสี่ยง

การบริหารจัดการความเสี่ยงสากล

2. ISO 31000

ขั้นตอนที่ 4: การจัดการความเสี่ยง ประกอบด้วย

- 4.1 การหลีกเลี่ยงความเสี่ยง
- 4.2 การลดความเสี่ยง
- 4.3 การแบ่งปันความเสี่ยงให้กับหน่วยงานอื่น ๆ
- 4.4 การยอมรับหรือเก็บรักษาความเสี่ยงไว้

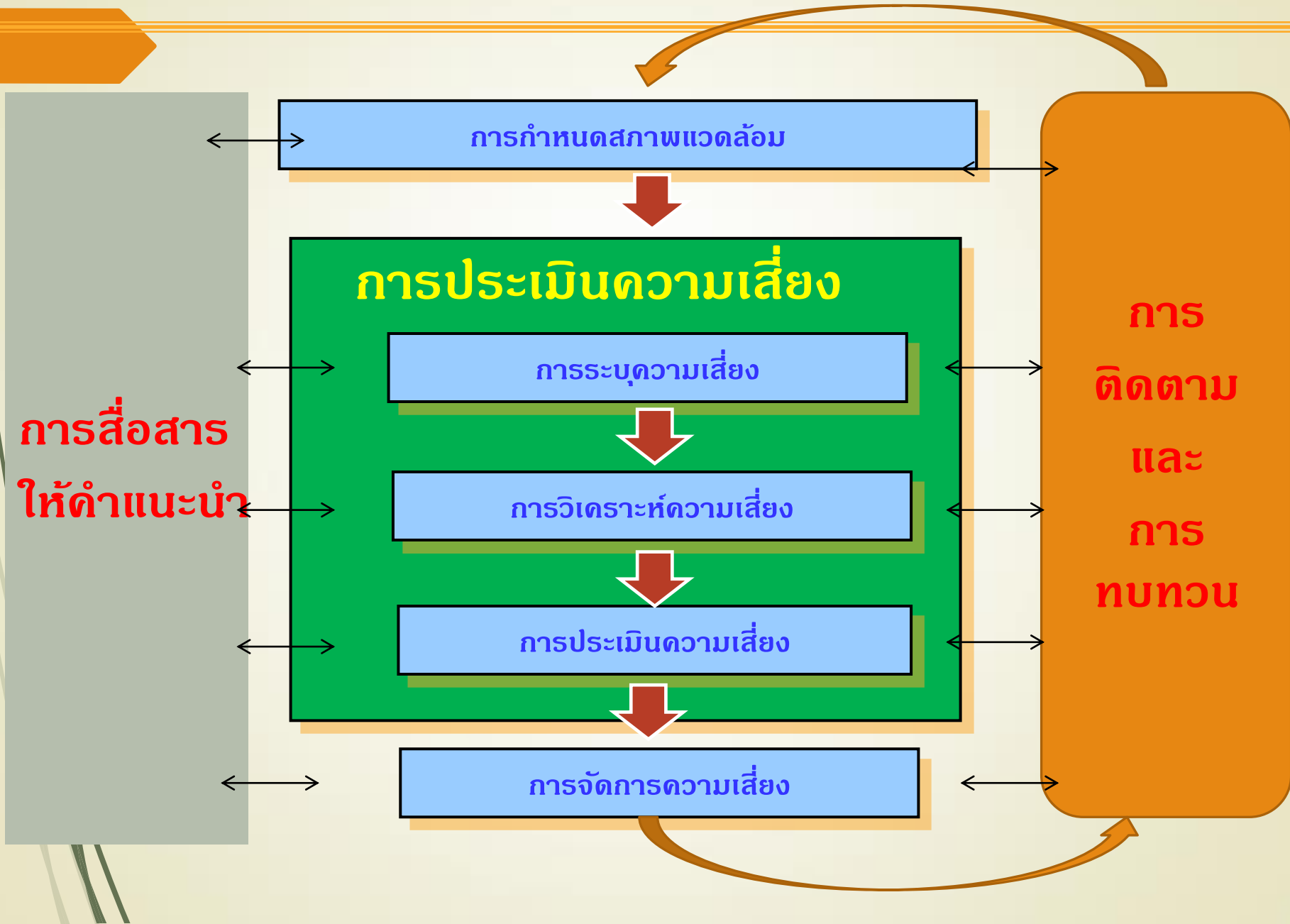
การบริหารจัดการความเสี่ยงสากล

2. ISO 31000

ขั้นตอนที่ 5: การเฝ้าติดตาม และการทบทวนความเสี่ยง

องค์กรจะต้องจัดให้มีการเฝ้าติดตามและทบทวนไว้เป็นหนึ่งในกระบวนการบริหารความเสี่ยง โดย จะต้องมีการกำหนดผู้รับผิดชอบและกรอบเวลาในการดำเนินการไว้อย่างชัดเจน ทั้งนี้การเฝ้าติดตามและ ทบทวน จะต้องครอบคลุมในทุก ๆ ส่วนของกระบวนการบริหารความเสี่ยง

ISO 31000



การบริหารจัดการความเสี่ยงสากล

องค์ประกอบของ COSO-ERM	องค์ประกอบของ ISO 31000
1. สภาพแวดล้อมภายใน	2. การกำหนดสภาพแวดล้อม
2. การกำหนดวัตถุประสงค์	
3. การบ่งชี้เหตุการณ์	3. การประเมินความเสี่ยง
4. การประเมินความเสี่ยง	
5. การตอบสนองความเสี่ยง	4. การจัดการความเสี่ยง
6. กิจกรรมการควบคุม	
7. สารสนเทศและการสื่อสาร	1. การสื่อสารและการให้คำแนะนำ
8. การติดตามและประเมินผล	5. การเฝ้าระวังติดตาม และ การทบทวนความเสี่ยง

ความสัมพันธ์ของการบริหารความเสี่ยง

การกำกับดูแลกิจการที่ดี
(Corporate Governance)

การบริหารความเสี่ยง
(Risk Management)

การควบคุมภายใน
(Internal Control)

การตรวจสอบภายใน
(Internal Audit)

การ
ตรวจสอบ
ภายนอก
(External
Audit)

หน่วยงาน AA

50

กระบวนการบริหารจัดการความเสี่ยง

1 คณะกรรมการหรือคณะทำงาน

* ตั้งผู้รับผิดชอบ โดยมีผู้บริหารระดับสูง และตัวแทนที่รับผิดชอบพันธกิจหลักและยุทธศาสตร์ของหน่วยงาน

2 การวิเคราะห์และระบุความเสี่ยง

* วิเคราะห์และระบุความเสี่ยง และปัจจัยที่ก่อให้เกิดความเสี่ยงอย่างน้อย 4 ด้าน ประกอบด้วย ด้านกลยุทธ์ ด้านการดำเนินงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎ/ระเบียบ/ข้อบังคับ

3 การประเมินความเสี่ยง

* ประเมินโอกาสและผลกระทบของความเสี่ยงและจัดลำดับความเสี่ยงที่ได้จากการวิเคราะห์ความเสี่ยง (หลักเกณฑ์โอกาสและผลกระทบที่ชัดเจน)

4 จัดทำแผนบริหาร
ความเสี่ยงและดำเนินการ
ตอบสนองความเสี่ยง

* จัดทำแผนบริหารความเสี่ยงที่มีระดับความเสี่ยงสูง และดำเนินการตามแผน (สร้างความรู้ / มาตรการควบคุมความเสี่ยง 4 วิธี)

5 ติดตามและประเมินผล

* ติดตามและประเมินผลการดำเนินงานตามแผน และรายงานปีละ 1 ครั้ง (การดำเนินงาน ผลสำเร็จ ปัญหาอุปสรรค แนวทางแก้ไข ข้อเสนอแนะ)

6 ทบทวน/ปรับปรุงแผน
บริหารความเสี่ยง

* นำผลการประเมินและข้อเสนอแนะไปใช้ในการปรับแผนหรือวิเคราะห์ความเสี่ยงในรอบปีถัดไป

การบริหารความเสี่ยง-แผน

ประเด็นยุทธศาสตร์	1. หลักสูตรที่พัฒนาความเชี่ยวชาญ บุคลากร และสร้างความสามารถในการลงมือปฏิบัติ
เป้าประสงค์	1. หลักสูตร.....
ตัวชี้วัด	1. จำนวนหลักสูตรที่ 2. ระดับความสำเร็จของ
กลยุทธ์	1. 2.
โครงการ/งาน	1. โครงการ..... 2. โครงการ..... 3. โครงการเสริมสร้างความรู้ให้กับนักศึกษาโดยผู้มีประสบการณ์ทางวิชาการ/วิชาชีพ จากหน่วยงานหรือชุมชนภายนอก(ทุกหลักสูตร) 4. โครงการพัฒนาระบบสารสนเทศสำหรับการเรียนการสอน
ผู้รับผิดชอบ	คณะครุศาสตร์ คณะเทคโนโลยีอุตสาหกรรม คณะมนุษยศาสตร์และสังคมศาสตร์ คณะวิทยาการจัดการ คณะวิทยาศาสตร์และเทคโนโลยี บัณฑิตวิทยาลัย สำนักงานอธิการบดี ฯลฯ

ปัจจัยเสี่ยง	การวิเคราะห์ความเสี่ยง		ระดับความเสี่ยง	วิธีการบริหารความเสี่ยง				แนวทาง การปรับปรุง
	โอกาส	ผลกระทบ		ยอมรับ	หลีกเลี่ยง	ถ่ายโอน	ควบคุม	

การบริหารความเสี่ยง-แผน

ประเด็นยุทธศาสตร์	1. หลักสูตรที่พัฒนาความเชี่ยวชาญ บุคลากร และสร้างความสามารถในการลงมือปฏิบัติ
เป้าประสงค์	1. หลักสูตร.....
ตัวชี้วัด	1. จำนวนหลักสูตรที่..... 2. ระดับความสำเร็จของ
กลยุทธ์	1. เร่งรัดการพัฒนาหลักสูตร..... 2. พัฒนาระบบการจัดการเรียนการสอนให้บัณฑิตมีคุณภาพพึงประสงค์ มีความรู้ คู่คุณธรรม เชี่ยวชาญในศาสตร์ที่ศึกษา
โครงการ/งาน	1. โครงการจัดทำและพัฒนาหลักสูตร..... 2. โครงการพัฒนาระบบการเรียนการสอนและเสริมสร้างศักยภาพการเรียนรู้ที่เน้นผู้เรียนเป็นสำคัญ 3. โครงการเสริมสร้างความรู้ให้กับนักศึกษาโดยผู้มีประสบการณ์ทางวิชาการ/วิชาชีพ จากหน่วยงานหรือชุมชนภายนอก(ทุกหลักสูตร) 4. โครงการพัฒนาระบบสารสนเทศสำหรับการเรียนการสอน
ผู้รับผิดชอบ	คณะครุศาสตร์ คณะเทคโนโลยีอุตสาหกรรม คณะมนุษยศาสตร์และสังคมศาสตร์ คณะวิทยาการจัดการ คณะวิทยาศาสตร์และเทคโนโลยี บัณฑิตวิทยาลัย สำนักงานอธิการบดี ฯลฯ

ปัจจัยเสี่ยง	ระดับความเสี่ยง ที่มีอยู่	แนวทางการปรับปรุง	ผลการดำเนินการ ปรับปรุง	ระดับความเสี่ยง คงเหลือ	แนวทางแก้ไข (เพิ่มเติม)
ข้อมูลจากแผนการบริหารความเสี่ยง			ข้อมูลจากการติดตามผลการดำเนินงานจริง		



ขอบคุณ

กองตรวจสอบภาครัฐ

กรมบัญชีกลาง

โทร. 0 2127 7000 ต่อ 4374

E-mail address : IASTD@cgd.go.th