**ใบความรู้ที่3**

**ระบบคุณภาพในองค์กร**

**ความเสี่ยง (Risk) คือ การวัดความสามารถ ที่จะดำเนินการให้วัตถุประสงค์ของงานประสบความสำเร็จ ภายใต้การตัดสินใจ งบประมาณ กำหนดเวลา และข้อจำกัดด้านเทคนิคที่เผชิญอยู่ อย่างเช่น การจัดทำโครงการเป็นชุดของกิจกรรม ที่จะดำเนินการเรื่องใดเรื่องหนึ่งในอนาคต โดยใช้ทรัพยากรที่มีอยู่อย่างจำกัด มาดำเนินการให้ประสบความสำเร็จ ภายใต้กรอบเวลาอันจำกัด ซึ่งเป็นกำหนดการปฏิบัติการในอนาคต ความเสี่ยงจึงอาจเกิดขึ้นได้ตลอดเวลา อันเนื่องมาจากความไม่แน่นอน และความจำกัดของทรัพยากรโครงการ ผู้บริหารโครงการจึงต้องจัดการความเสี่ยงของโครงการ เพื่อให้ปัญหาของโครงการลดน้อยลง และสามารถดำเนินการให้ประสบความสำเร็จ ตามเป้าหมายที่ตั้งไว้อย่างมีประสิทธิผลและประสิทธิภาพ**

**การจัดการความเสี่ยงหรือ การบริหารความเสี่ยง (Risk managment)คือ การจัดการความเสี่ยง ทั้งในกระบวนการในการระบุ วิเคราะห์(Risk analysis) ประเมิน (Risk assessment) ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับ กิจกรรม หน้าที่และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง หรือเรียกว่า อุบัติภัย (Accident)**

**นิยามของความเสี่ยง**

ความเสี่ยงมีความหมายในหลากหลายแง่มุม เช่น ความเสี่ยงคือ

* โอกาสที่เกิดขึ้นแล้วธุรกิจจะเกิดความเสียหาย (Chance of Loss)
* ความเป็นไปได้ที่จะเกิดความเสียหายต่อธุรกิจ (Possibility of Loss)
* ความไม่แน่นอนของเหตุการณ์ที่จะเกิดขึ้น (Uncertainty of Event)
* การคลาดเคลื่อนของการคาดการณ์ (Dispersion of Actual Result)

**ศัพท์ทางเทคนิค**

* ภัย (Peril) คือ สาเหตุของความเสียหาย ซึ่งภัยสามารถเกิดขึ้นได้จากภัยธรรมชาติ เช่น เกิดพายุ สึนามิ น้ำท่วม แผ่นดินไหว เป็นต้น ภัยนอกจากจะเกิดขึ้นได้จากภัยธรรมชาติแล้ว ภัยนั้นยังเกิดขึ้นจากการกระทำของมนุษย์ เช่น อัคคีภัย จลาจล ฆาตกรรม เป็นต้น สำหรับสาเหตุสุดท้ายที่จะเกิดภัยได้นั้นคือภัยที่เกิดขึ้นจากภาวะเศรษฐกิจ เพราะภัยที่เกิดจากภาวะเศรษฐกิจ เป็นอีกสาเหตุที่สำคัญ เพราะเมื่อเกิดขึ้นแล้วคนทั้งประเทศ หรือทั้งภูมิภาคจะได้รับผลกระทบอย่างกว้างขวาง
* ความเสี่ยง (Risk) คือ ความไม่แน่นอนของเหตุการณ์ ซึ่งไม่สามารถคาดเดาได้ว่าจะเกิดขึ้นเมื่อใด แต่ความเสี่ยงนั้น ๆ จะมีแนวโน้มที่เกิดขึ้นไม่มากก็น้อยในบริษัท
* สภาวะที่จะทำให้เกิดความเสียหาย (Hazard) คือ สภาพเงื่อนไขที่เป็นสาเหตุที่ทำให้ความเสียหายเพิ่มสูงขึ้น โดยสภาวะต่าง ๆ นี้สามารถแบ่งออกได้เป็น สภาวะทางด้านกายภาพ (Physical) คือ สภาวะของโอกาสที่จะเกิดความเสียหาย เช่น ชนิดและทำเลที่ตั้งของสิ่งปลูกสร้าง อาจเอื้อต่อการเกิดเพลิงไหม้ สภาวะทางด้านศีลธรรม (Moral) คือ สภาวะของโอกาสที่จะเกิดขึ้นจากความไม่ซื่อสัตย์ต่อหน้าที่การงาน เช่น การฉ้อโกงของพนักงาน และสภาวะด้านจิตสำนึกในการป้องกันความเสี่ยง (Morale) คือ สภาวะที่ไม่ประมาทและเลินเล่อ หรือการไม่เอาใจใส่ในการป้องกันความเสี่ยง เช่น การที่พนักงานปล่อยให้เครื่องจักรทำงานโดยไม่ควบคุม

**องค์ประกอบของการบริหารความเสี่ยง**

1. การระบุชี้ว่าองค์กรกำลังมีภัย
เป็นการระบุชี้ว่าองค์กรมีภัยอะไรบ้างที่มาเผชิญอยู่ และอยู่ในลักษณะใดหรือขอบเขตเป็นอย่างไร นับเป็นขั้นตอนแรกของการบริหารความเสี่ยง
2. การประเมินผลกระทบของภัย
เป็นการประเมินผลกระทบของภัยที่จะมีต่อองค์กรซึ่งอาจเรียกอีกอย่างหนึ่งว่า การประเมินความเสี่ยงที่องค์กรต้องเตรียมตัวเพื่อรับมือกับภัยแต่ละชนิดได้อย่างเหมาะสมมากที่สุด
3. การจัดทำมาตรการตอบโต้ตอบความเสี่ยงจากภัย
การจัดทำมาตรการตอบโต้ตอบความเสี่ยงเป็นมาตรการที่จัดเรียงลำดับความสำคัญแล้วในการประเมินผลกระทบของภัย มาตรการตอบโต้ที่นิยมใช้เพื่อการรับมือกับภัยแต่ละชนิด อาจจำแนกดังนี้
* มาตรการขจัดหรือลดความรุนแรงของความอันตรายของภัยที่ต้องประสบ
* มาตรการที่ป้องกันผู้รับภัยมิให้ต้องประสบภัยโดยตรง เช่นมาตรการลดความรุนแรงของสถานการณ์ฉุกเฉิน เช่น กรณีเกิดเพลิงไหม้ในอาคาร ได้มีการขจัดและลดความรุนแรง โดยออกแบบตัวอาคารให้มีผนังกันไฟ กันเพลิงไหม้รุนลาม
	+ ภัยจากการที่ต้องปีนไปในที่สูงก็มีมาตรการป้องกันโดยต้องติดเข็มขัดนิรภัย กันการพลาดพลั้งตกลงมา
	+ ภัยจากไอระเหยหรือสารพิษก็ป้องกันโดยออกมาตรการให้สวมหน้ากากป้องกันไอพิษ เป็นต้น
* ไปยังบริเวณใกล้เคียง และมีการติดตั้งระบบสปริงเกอร์ ก็จะช่วยลดหรือหยุดความรุนแรงของอุบัติภัยลงได้
* มาตรการกู้ภัยก็เป็นการลดความสูญเสียโดยตรง ลงได้มาก
* มาตรการกลับคืนสภาพ ก็เป็นอีกมาตรการในการลดความเสียหายต่อเนื่องจากภัยหรืออุบัติภัยแต่ละครั้งลงได้

ประเภทความเสี่ยง

การจำแนกประเภทความเสี่ยงตามหลักเกณฑ์ของกระทรวงการคลัง สามารถแบ่งความเสี่ยงออกเป็น 5 ประเภท ดังนี้

1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S) เป็นความเสี่ยงที่เกี่ยวข้องในระดับยุทธศาสตร์ เช่น การเมือง เศรษฐกิจ สังคม สถานการณ์โลก ภาวะผู้นำ กลไกตลาด เป็นต้น

2) ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk : O) เป็นความเสี่ยงที่เกี่ยวข้องในระดับการปฏิบัติงาน เช่น ระบบงานขององค์กร กระบวนการทำงาน เทคโนโลยี บุคลากร ข้อมูลข่าวสาร เป็นต้น

3) ความเสี่ยงด้านการเงิน (Financial Risk : F) เป็นความเสี่ยงที่เกี่ยวข้องกับทางด้านการเงิน เช่น อัตราการแลกเปลี่ยนเงินตรา อัตราดอกเบี้ย งบประมาณ สภาพคล่อง ความสามารถในการชำระหนี้ ความน่าเชื่อถือทางการเงิน เป็นต้น

4) ความเสี่ยงด้านการปฏิบัติตามระเบียบและกฎหมาย (Compliance Risk : C) เป็นความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามระเบียบและกฎหมาย เช่น ระเบียบ กฎหมาย พระราชกฤษฎีกา ระเบียบข้อบังคับ ข้อกำหนดของทางการ นโยบายของรัฐ เป็นต้น

5) ความเสี่ยงด้านความปลอดภัย (Hazardous Risk : H) เป็นความเสี่ยงที่เกี่ยวข้องกับการจัดการด้านความปลอดภัย เช่น ข้อกำหนดด้านความปลอดภัยภายในองค์กร อาคาร หรือสถานที่ ที่จะต้องเป็นไปตามมาตรฐานกำหนด

**ระบบ ERM**

Enterprise Risk Management Thailand เป็น Blog ที่จัดทำขึ้น เพื่อเผยแพร่ความรู้เกี่ยวกับการบริหารจัดการความเสี่ยงขององค์กร ตามมาตรฐานของ COSO หรือ Committee of Sponsoring Organizations of The Treadway Commission
นอกจากบทความต่างๆที่เกี่ยวกับการบริหารจัดการความเสี่ยง Blog นี้ยังได้เป็นการแสดงตัวอย่างเครื่องมือในการวิเคราะห์ บริหารจัดการและควบคุมความเสี่ยงภายในองค์กร ที่น่าจะเหมาะสมกับองค์กรที่มีขนาดไม่ใหญ่มาก  โดยเครื่องมือนี้เป็นการพ้ฒนาในรูปแบบของเว็ปแอพพลิเคชั่น ที่สะดวกต่อการเข้าใช้งาน และอีกทั้งยังสามารถทำให้ผู้ใช้งานได้รับข้อมูลที่ทันสมัย  ผู้ที่สนใจสามารถติดต่อเพื่อขอชื่อผู้ใช้งาน และรหัสเข้าใช้งานได้จากทางเจ้าหน้าที่ หรืออีเมล์ไปที่ผู้ดูแลระบบ
**การทำงานของระบบ ERM**
เนื่องจากระบบนี้ได้ถูกออกแบบตามมาตรฐานการบริหารความเสี่ยง COSO  การทำงานของระบบจึงได้มีขั้นตอนคล้ายกับ 8 ขั้นตอนของ COSO คือ การกำหนดหรือวิเคราะห์สภาพแวดล้อมภายในองค์กร, การกำหนดวัตถุประสงค์, การบ่งชี้เหตุการณ์, การประเมินความเสี่ยง, การตอบสนองความเสี่ยง, การกำหนดกิจกรรมควบคุม, การเผยแพร่รายงาน สารสนเทศและการสื่อสาร และการติดตามประเมินผล  ซึ่งในทุกขั้นตอนนี้ระบบจะกำหนดให้ผู้ใช้งานปฏิบัติตามขั้นตอน  ในแต่ละขั้นจะเป็นการรับข้อมูลจากผู้ปฏิบัติงานในแต่ละหน่วยงาน ให้ระบบนำเข้ามาวิเคราะห์หาผลสรุปเป็นภาพรวมในระดับขององค์กร แล้วใช้เป็นฐานข้อมูลในการสร้างรายงานมาตรฐานให้กับองค์กรนั้นๆ



***ขั้นตอนที่ 1***: การกำหนดหรือวิเคราะห์สภาพแวดล้อมภายในองค์กร
เป็นการระบุสภาพแวดล้อมภายในองค์กร ซึ่งในขั้นตอนนี้ระบบจะรับข้อมูลจากการที่ผู้ใช้งานตอบแบบสอบถาม แล้วระบบจะนำมาวิเคราะห์เพื่อแสดงออกเป็นรายงาน
**ขั้นตอนที่ 2**: การกำหนดวัตถุประสงค์
เป็นขั้นตอนที่ผู้ใช้งานจะต้องบันทึกแผนงาน หรือโครงการของหน่วยงาน และระบุวัตถุประสงค์ของแผนงานหรือโครงการ, ตัวชี้วัดระดับองค์กรที่สอดคล้องกับแผนงานหรือโครงการ, ระบุประเด็นยุทธ์ศาสตร์ที่แผนงานหรือโครงการนั้นๆสนับสนุน, กิจกรรมต่างๆ (เฉพาะกิจกรรมหลัก) ที่มีอยู่ภายใต้แต่ละแผนงานหรือโครงการ และวัตถุประสงค์ของการควบคุม ของแต่ละกิจกรรมหลักนั้นๆ
***ขั้นตอนที่ 3***: การบ่งชี้เหตุการณ์
เป็นการวิเคราะห์ความเสี่ยงสำหรับแต่ละกิจกรรมหลักที่ได้บันทึกไว้ เพื่อระบุปัจจัยเสี่ยง (Risk Factor), ผลกระทบที่มีนัยสำคัญ, ประเภทของความเสี่ยง และลักษณะความเสี่ยง
***ขั้นตอนที่ 4***: การประเมินความเสี่ยง
เป็นการระบุการควบคุมที่มีอยู่ แล้วประเมินว่าเพียงพอหรือไม่ เพื่อระบุปัจจัยเสี่ยงที่ยังคงมีอยู่ให้ทำการจัดการ โดยกำหนดค่าระดับของผลกระทบและโอกาสของความเสี่ยงนั้นๆ เพื่อให้ระบบคำนวณระดับความเสี่ยงตามค่ามาตรฐาน (อ้างอิงค่าจาก Risk Profile Matrix 5×5 โดยค่าที่ได้จะเป็นค่าตั้งแต่ 1 ถึง 25 โดยที่เลข 25 จะเป็นระดับความเสี่ยงที่สูงที่สุด)
เมื่อผ่านขั้นตอนที่ 4 นี้ ระบบจะทำการคัดกรองเอาเฉพาะกิจกรรมหลักที่มีระดับความเสี่ยงสูงกว่า “ต่ำ” (ตัวเลขตั้งแต่ 6 ขึ้นไป)  เพื่อนำไปวิเคราะห์ในขั้นตอนต่อๆไป สำหรับความเสี่ยงที่มีระดับความเสี่ยง “ต่ำ” ระบบจะเก็บไว้ แล้วจะแสดงในรายงานสรุปให้กับผู้ใช้งานทราบอีกครั้งหนึ่ง
***ขั้นตอนที่ 5***: การตอบสนองความเสี่ยง
เป็นขั้นตอนในการระบุวิธีการจัดการความเสี่ยง ซึ่งอ้างถึงมาตรฐานทางเลือกที่มีอยู่ คือ การหลีกเลี่ยง, การควบคุม, การยอมรับ และการถ่ายโอน แล้วทำการเลือกว่าการจัดการความเสี่ยงแบบใดเหมาะสมที่สุด เพื่อกำหนดแผนและผู้รับผิดชอบในการจัดการความเสี่ยง สำหรับกิจกรรมหลักนั้นๆ
***ขั้นตอนที่ 6***: การบันทึกกิจกรรมควบคุม
เป็นบันทึกรายละเอียดกิจกรรมในการควบคุม ตามหัวข้อที่เป็นมาตรฐานตามแนวทางของคู่มือการควบคุมความเสี่ยงของ สตง. โดยจะประกอบไปด้วย 7 หัวข้อ ดังนี้

* การกำหนดนโยบายและระเบียบวิธีปฏิบัติงาน
* การสอบทานโดยผู้บริหาร
* การควบคุมการประมวลผลข้อมูล
* การอนุมัติ
* การดูแลป้องกันทรัพย์สิน
* การแบ่งแยกหน้าที่
* การจัดทำเอกสารหลักฐาน
***ขั้นตอนที่ 7***: การเผยแพร่รายงานผ่านระบบสารสนเทศและการสื่อสาร
เป็นการแสดงรายงานการบริหารจัดการความเสี่ยงของทั้งระดับหน่วยงาน และระดับองค์กร จากข้อมูลที่ระบบได้รับตั้งแต่ขั้นตอนที่ 1 ถึง 6 ซึ่งรายงานจะแบ่งออกได้เป็น 2 ส่วนหลัก คือ
1. รายงานการควบคุมภายใน ที่ประกอบไปด้วยรายงานแบบปย.1 และ แบบ ปย.2 ตามมาตรฐานของสำนักงานตรวจเงินแผ่นดิน (สตง.) *(แบบ ปย. 1:  รายงานผลการประเมินองค์ประกอบของการควบคุมภายใน และ แบบ ปย. 2:  รายงานการประเมินผลและการปรับปรุงการควบคุมภายใน)*
2. รายงานการจัดการความเสี่ยง สรุปความเสี่ยงและการจัดการในระดับของหน่วยงาน *(รายงานแผนบริหารความเสี่ยงของหน่วยงานย่อย)*
***ขั้นตอนที่ 8***: การติดตามประเมินผล
เป็นการบันทึกติดตามผล การทำกิจกรรมควบคุมความเสี่ยงที่ได้ทำแผนไว้ในขั้นตอนที่ 5 เพื่อเปรียบเทียบกับตัวชี้วัด โดยใส่รายละเอียดของการติดตามผล แล้วประเมินระดับความเสี่ยงที่คงเหลืออยู่ภายหลังจากที่ได้มีกิจกรรมควบคุม ว่าระดับความเสี่ยงคงเหลืออยู่ในระดับใด  ซึ่งผลที่ได้นี้ สามารถนำไปใช้เป็นข้อมูลพื้นฐานในการวิเคราะห์ในรอบต่อๆไปได้
**ประโยชน์ของระบบ ERM**
ระบบ ERM (Enterprise Risk Management) เป็นระบบที่ได้ถูกออกแบบตามหลักการ 8 ขั้นตอน ของการจัดการบริหารความเสี่ยงของ COSO  เพื่อให้องค์กรที่นำไปใช้งานได้ประโยชน์ดังนี้
3. ระบบนี้สามารถเป็นเครื่องมือ เพื่อช่วยผู้บริหารในการประเมินความเพียงพอเหมาะสมของการควบคุม และทำให้มีการแก้ไขปัญหา ปรับปรุงการทำงานให้ดีขึ้น ซึ่งจะส่งผลให้งานของทั้งส่วนงานย่อย ฝ่ายงาน และสายการบังคับบัญชา บรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น
4. ข้อมูลที่ได้รับจากระบบ เป็นข้อมูลรวมจากระดับปฏิบัติการที่มีอยู่ของหน่วยงานย่อยในองค์กร ซึ่งจะช่วยให้ค้นพบปัญหาที่เกิดขึ้นหรือมีแนวโน้มที่จะเกิดขึ้น ก่อนที่จะเกิดความเสียหาย ทำให้หน่วยงานสามารถวางแผนเพื่อจัดการแก้ไขได้
5. การใช้งานระบบนี้ เป็นการเปิดโอกาสให้ผู้ปฏิบัติงานในทุกระดับ แสดงความเห็น ข้อเสนอแนะ และร่วมกันกำจัดอุปสรรค และข้อขัดข้องต่างๆ
6. ขั้นตอนการทำงานของระบบ เป็นการนำเสนอแนวทางปฏิบัติตามกรอบของนโยบายองค์กร ทำให้พนักงานเข้าใจเป้าหมายขององค์กรที่ตนได้มีส่วนร่วม อีกทั้งช่วยสร้างบรรยากาศที่ดีของการทำงาน และการรับผิดชอบร่วมกันต่อผลสำเร็จขององค์กร
7. ระบบมีแบบแผนขั้นตอนการดำเนินการที่ชัดเจน ในการกำหนดเป้าหมายขององค์กร, ตัวชี้วัดความสำเร็จ, การวิเคราะห์งานเพื่อระบุความเสี่ยง, ประเมินความเสี่ยง, การควบคุมความเสี่ยง และการติดตามความเสี่ยง โดยสามารถนำรายละเอียดดังกล่าวมาสร้างเป็นรายงานต่างๆได้
8. จากการให้พนักงานมีส่วนร่วมในการให้ข้อมูล จะทำให้เกิดความเข้าใจ และการยอมรับจากผู้ปฏิบัติงานได้ดี มากกว่าการควบคุมสั่งการโดยผู้บริหารแต่ฝ่ายเดียว