

กรอบการบริหารความเสี่ยง (ERM Framework)		
เรื่อง : การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)	ออกครั้งที่ : 1	แก้ไขครั้งที่ : -
วันที่บังคับใช้ : 17 มกราคม 2561	หน้าที่ 1 ของ 7	

1. บทนำ

ในการดำเนินธุรกิจ บริษัทจะต้องเผชิญกับเหตุการณ์ที่ไม่แน่นอนซึ่งอาจเกิดจากปัจจัยภายในและภายนอก อาทิเช่น ภาวะเศรษฐกิจที่ชะลอตัว ความผันผวนของอัตราแลกเปลี่ยนเงินตรา ความบกพร่องในกระบวนการทำงาน การเปลี่ยนแปลงด้านบุคลากร เป็นต้น ความไม่แน่นอนเหล่านี้ คือความเสี่ยงที่บริษัทต้องเผชิญ โดยแต่ละเหตุการณ์อาจมีความเสี่ยงที่ไม่เท่ากันขึ้นอยู่กับโอกาส และผลกระทบ ส่งผลให้การดำเนินงานไม่เป็นไปตามวัตถุประสงค์ ดังนั้น เพื่อให้มั่นใจว่าบริษัทมีการบริหารจัดการความเสี่ยงในระดับองค์กรที่เพียงพอและเหมาะสม คณะกรรมการจึงกำหนดให้มีกรอบการบริหารความเสี่ยงอ้างอิงตามหลักสากล COSO ERM (Enterprise Risk Management – Integrated Frame Work, the Committee of Sponsoring Organizations of the Treadway Commission)

2. วัตถุประสงค์

- 1) กรอบการบริหารความเสี่ยงกำหนดขึ้นเพื่อเป็นแนวทางให้บริษัทมีระบบการบริหารความเสี่ยงที่มีประสิทธิภาพ เชื่อมโยงกับวัตถุประสงค์และเป้าหมายของบริษัทตามที่กำหนดไว้ในแผนงานประจำปี
- 2) เพื่อให้มีกระบวนการวิเคราะห์ปัจจัยเสี่ยงที่อาจมีผลกระทบต่อผลสำเร็จของการดำเนินงาน ตลอดจนสามารถวางแผนบริหารจัดการความเสี่ยงโดยลดโอกาสและผลกระทบที่อาจเกิดขึ้นให้อยู่ในระดับที่ยอมรับได้
- 3) เพื่อให้บริษัทมีระบบการบริหารความเสี่ยงและได้รับการปฏิบัติอย่างต่อเนื่องทั่วทั้งองค์กร

3. นิยาม

อ้างอิงตามกรอบการบริหารความเสี่ยงของตลาดหลักทรัพย์แห่งประเทศไทย (ฉบับเผยแพร่ทางเว็บไซต์, 2558 : 1)

- 1) ความเสี่ยง (Risk) หมายถึง โอกาสหรือเหตุการณ์ที่มีความไม่แน่นอน หรือสิ่งที่ทำให้แผนงานหรือการดำเนินการอยู่ ณ ปัจจุบันไม่บรรลุวัตถุประสงค์หรือเป้าหมายตามที่กำหนดไว้ และก่อให้เกิดผลกระทบหรือความเสียหายต่อองค์กรในที่สุด ทั้งในแง่ของผลกระทบที่เป็นตัวเงินหรือผลกระทบที่มีต่อภาพลักษณ์และชื่อเสียงองค์กร
- 2) การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management) หมายถึง กระบวนการที่คณะกรรมการและบุคลากรในองค์กร ปฏิบัติร่วมกันเพื่อช่วยในการกำหนดกลยุทธ์และการดำเนินงานผ่านกระบวนการบริหารความเสี่ยงที่ได้รับการออกแบบเพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้

กรอบการบริหารความเสี่ยง (ERM Framework)		
เรื่อง : การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)	ออกครั้งที่ : 1	แก้ไขครั้งที่ : -
วันที่บังคับใช้ : 17 มกราคม 2561	หน้าที่ 2 ของ 7	

4. นโยบายการบริหารความเสี่ยง

คณะกรรมการตระหนักถึงความสำคัญของการบริหารความเสี่ยงจึงได้กำหนดให้มีกรอบการบริหารความเสี่ยงเพื่อเป็นแนวทางปฏิบัติให้กับบุคลากรในองค์กร ทั้งนี้ คณะกรรมการได้แต่งตั้งคณะกรรมการตรวจสอบให้เป็นผู้กำกับดูแลการบริหารความเสี่ยงของบริษัท โดยจะทำหน้าที่ทบทวนนโยบาย และกรอบการดำเนินงาน เพื่อให้มั่นใจว่าบริษัทมีระบบการบริหารจัดการความเสี่ยงที่เพียงพอและเหมาะสม

5. โครงสร้างและหน้าที่ความรับผิดชอบในการบริหารความเสี่ยง

- 1) คณะกรรมการบริษัท มีหน้าที่ความรับผิดชอบในการกำหนดนโยบายและกรอบการบริหารความเสี่ยง
- 2) คณะกรรมการตรวจสอบ มีหน้าที่ความรับผิดชอบในการทบทวนกรอบการบริหารความเสี่ยงให้มีความเหมาะสม พร้อมทั้งพิจารณาและให้ความเห็นชอบในการกำหนดเกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria) และระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)
- 3) กรรมการผู้จัดการ มีหน้าที่สนับสนุนให้มีการประเมินและทบทวนความเสี่ยงของบริษัทอย่างต่อเนื่องทั่วทั้งองค์กร พร้อมทั้งติดตามความเสี่ยงที่สำคัญเพื่อให้มั่นใจว่าบริษัทมีแผนการจัดการที่เพียงพอและเหมาะสม โดยความเสี่ยงที่สำคัญจะต้องรายงานต่อคณะกรรมการบริษัทให้ทราบ
- 4) คณะกรรมการบริหาร มีหน้าที่ประเมินและจัดการความเสี่ยงที่มีผลกระทบต่อกลยุทธ์และเป้าหมายของบริษัท พร้อมทั้งกำกับดูแลให้แต่ละสายงานปฏิบัติตามกรอบการบริหารความเสี่ยง
- 5) หน่วยงานบริหารความเสี่ยงองค์กร มีหน้าที่ความรับผิดชอบดังต่อไปนี้
 - 5.1 สนับสนุนคณะกรรมการตรวจสอบในการทบทวนกรอบการบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria) และระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ให้มีความเหมาะสม
 - 5.2 สนับสนุนคณะกรรมการบริหารในการประเมินและติดตามความเสี่ยงที่อาจมีผลกระทบต่อเป้าหมายของบริษัท
 - 5.3 สื่อสารกรอบการบริหารความเสี่ยง รวมทั้งจัดให้มีการอบรม สร้างความเข้าใจให้พนักงานตระหนักถึงความสำคัญในการบริหารความเสี่ยง
 - 5.4 จัดทำแผนงานบริหารความเสี่ยงโดยแบ่งกลุ่มการทำงานเป็นระดับองค์กรและระดับปฏิบัติการ พร้อมทั้งประสานงานกับผู้รับผิดชอบในแต่ละกลุ่มเพื่อให้มั่นใจว่าบริษัทมีการบริหารจัดการความเสี่ยงอย่างต่อเนื่อง
 - 5.5 รายงานผลการประเมินและการจัดการความเสี่ยงต่อคณะกรรมการบริหารเป็นรายไตรมาส

กรอบการบริหารความเสี่ยง (ERM Framework)		
เรื่อง : การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)	ออกครั้งที่ : 1	แก้ไขครั้งที่ : -
วันที่บังคับใช้ : 17 มกราคม 2561	หน้าที่ 3 ของ 7	

6. ขอบเขตการบริหารความเสี่ยง

ขอบเขตการบริหารความเสี่ยงครอบคลุมประเภทความเสี่ยงที่อาจส่งผลกระทบต่อกลยุทธ์ เป้าหมายในการดำเนินงาน การปฏิบัติตามกฎหมาย รวมทั้งคุณภาพ ความปลอดภัย อาชีวอนามัยและสิ่งแวดล้อม โดยจัดประเภทความเสี่ยงเป็น 4 ประเภทดังนี้

- 1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)
- 2) ความเสี่ยงด้านการดำเนินงาน (Operational Risk)
- 3) ความเสี่ยงด้านการเงิน (Financial Risk)
- 4) ความเสี่ยงด้านกฎหมายและการปฏิบัติตามกฎระเบียบ (Legal and Compliance Risk)

7. กระบวนการบริหารความเสี่ยงประกอบด้วย 7 ขั้นตอนดังต่อไปนี้

1) การกำหนดสภาพแวดล้อมในองค์กร (Internal Environment)

บริษัทสนับสนุนให้พนักงานเกิดการตระหนักเรื่องความเสี่ยงและการควบคุมความเสี่ยง โดยจัดให้มีการอบรมพัฒนาความรู้เรื่องการบริหารความเสี่ยง และกำหนดให้มีหน่วยงานที่รับผิดชอบโดยตรง

2) การกำหนดวัตถุประสงค์ (Objective)

บริษัทมีการกำหนดเป้าหมาย และกลยุทธ์ทางธุรกิจที่ชัดเจนสอดคล้องตามวิสัยทัศน์ของบริษัท โดยจะแบ่งเป็น 2 ระดับคือ 1) ระดับองค์กร 2) ระดับปฏิบัติการ

3) การระบุความเสี่ยง (Risk Identification)

การระบุเหตุการณ์ความเสี่ยงจัดทำโดยการวิเคราะห์ความสัมพันธ์ระหว่างเหตุการณ์ในอดีต ปัจจุบัน เพื่อให้ทราบถึงสาเหตุที่แท้จริงของความเสี่ยง จากนั้นจึงระบุผลกระทบที่อาจเกิดขึ้นในอนาคตโดยวิเคราะห์จากปัจจัยภายในและภายนอก รวมถึงกิจกรรมควบคุมที่มีอยู่

4) การประเมินความเสี่ยง (Risk Assessment)

บริษัทมีการจัดทำเกณฑ์การประเมินความเสี่ยงโดยกำหนดระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) ดังต่อไปนี้

- **โอกาสที่จะเกิดความเสี่ยง (Likelihood)**

กรอบการบริหารความเสี่ยง (ERM Framework)		
เรื่อง : การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)	ออกครั้งที่ : 1	แก้ไขครั้งที่ : -
วันที่บังคับใช้ : 17 มกราคม 2561	หน้าที่ 4 ของ 7	

โอกาสที่จะเกิดความเสี่ยง	คำอธิบาย
สูงมาก	มีเหตุการณ์เกิดขึ้นมากกว่า 5 ครั้ง ใน 1 ปี
สูง	มีเหตุการณ์เกิดขึ้น 4-5 ครั้ง ใน 1 ปี
ปานกลาง	มีเหตุการณ์เกิดขึ้น 2-3 ครั้ง ใน 1 ปี หรือเคยเกิดขึ้นมากกว่า 3 ครั้งใน 5 ปีที่ผ่านมา
ต่ำ	มีเหตุการณ์เกิดขึ้น 1 ครั้ง ใน 1 ปี หรือเคยเกิดขึ้น 2-3 ครั้งใน 5 ปีที่ผ่านมา
ต่ำมาก	ไม่เคยมีเหตุการณ์เกิดขึ้นในอดีต หรือเกิดขึ้นเพียง 1 ครั้งใน 5 ปีที่ผ่านมา

หมายเหตุ : ในกรณีที่เหตุการณ์ใดเข้าเกณฑ์การพิจารณาทั้งสองเหตุการณ์ให้ใช้แบบที่มีโอกาสเกิดมากที่สุดมาพิจารณา

- **ระดับความรุนแรงของผลกระทบ (Impact) ที่เป็นตัวเงิน (Financial Impact)**

ระดับคะแนน	ผลกระทบ	ผลกระทบที่เป็นตัวเงิน (เปรียบเทียบกับงบประมาณ)		
		กำไร (ล้านบาท)	รายได้ (ล้านบาท)	DE Ratio (เท่า)
5	สูงมาก	≥ 40	≥ 200	≥ 2.0
4	สูง	≤ 30	≤ 150	≥ 1.5
3	ปานกลาง	≤ 20	≤ 100	≥ 1.25
2	ต่ำ	≤ 10	≤ 50	≥ 1.1
1	ต่ำมาก	≤ 5	≤ 10	< 1.1

กรอบการบริหารความเสี่ยง (ERM Framework)		
เรื่อง : การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)	ออกครั้งที่ : 1	แก้ไขครั้งที่ : -
วันที่บังคับใช้ : 17 มกราคม 2561	หน้าที่ 5 ของ 7	

● **ระดับความรุนแรงของผลกระทบ (Impact) ที่ไม่เป็นตัวเงิน (Non-Financial Impact)**

ระดับ คะแนน	ผลกระทบ	ผลกระทบที่ไม่เป็นตัวเงิน				
		ด้านการปฏิบัติงาน	กฎหมาย/กฎระเบียบ	ความปลอดภัย	ภาพลักษณ์ ความน่าเชื่อถือ	ส่วนแบ่งตลาด
5	สูงมาก	ทุกหน่วยงานไม่สามารถปฏิบัติงานได้	บริษัทถูกฟ้องร้อง กรรมการผู้บริหารได้รับโทษทางแพ่ง / อาญา	พนักงานเสียชีวิตระหว่างปฏิบัติงาน	มีผลกระทบต่อภาพลักษณ์ในระยะเวลายาวนานมากกว่า 1 ปี	มีโอกาสที่จะไม่สามารถรักษาไว้ได้ภายในระยะเวลา มากกว่า 24 เดือน
4	สูง	3 หน่วยงานหยุดชะงัก ไม่สามารถปฏิบัติงานได้	บริษัทถูกหน่วยงานกำกับดูแลเปรียบเทียบปรับ	พนักงานได้รับบาดเจ็บระหว่างปฏิบัติงานและหยุดงานเกิน 5 วัน	มีผลกระทบต่อภาพลักษณ์ในระยะเวลาระหว่าง 6 - 12 เดือน	สามารถแข่งขันส่วนแบ่งตลาดกลับมาได้ภายในระยะเวลา 12-24 เดือน
3	ปานกลาง	2 หน่วยงานหยุดชะงัก ไม่สามารถปฏิบัติงานได้	บริษัทถูกหน่วยงานกำกับดูแลเข้าตรวจสอบ	พนักงานได้รับบาดเจ็บระหว่างปฏิบัติงานและหยุดงาน 3-5 วัน	มีผลกระทบต่อภาพลักษณ์ในระยะเวลาระหว่าง 1 – 6 เดือน	สามารถแข่งขันส่วนแบ่งตลาดกลับมาได้ภายในระยะเวลา 6-12 เดือน
2	ต่ำ	1 หน่วยงานหยุดชะงัก ไม่สามารถปฏิบัติงานได้	บริษัทถูกหน่วยงานกำกับดูแลแจ้งเตือนเป็นลายลักษณ์อักษร	พนักงานได้รับบาดเจ็บระหว่างปฏิบัติงานและหยุดงาน 1-2 วัน	มีผลกระทบต่อภาพลักษณ์ในระยะเวลาระหว่าง 1 สัปดาห์ – 1 เดือน	สามารถแข่งขันส่วนแบ่งตลาดกลับมาได้ในระยะ 3-6 เดือน
1	ต่ำมาก	การปฏิบัติงานหยุดชะงักบางส่วนและถูกจำกัดเพียง 1 หน่วยงาน	บริษัทถูกหน่วยงานกำกับดูแลแจ้งเตือนโดยวาจา	พนักงานได้รับบาดเจ็บเล็กน้อยระหว่างปฏิบัติงานและไม่หยุดงาน	มีผลกระทบต่อภาพลักษณ์ในระยะเวลาน้อยกว่า 1 สัปดาห์	สามารถแข่งขันส่วนแบ่งตลาดกลับมาได้ในระยะเวลาน้อยกว่า 3 เดือน

กรอบการบริหารความเสี่ยง (ERM Framework)		
เรื่อง : การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)	ออกครั้งที่ : 1	แก้ไขครั้งที่ : -
วันที่บังคับใช้ : 17 มกราคม 2561	หน้าที่ 6 ของ 7	

● การกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ (Risk Appetite)

Risk Assessment Matrix		โอกาส				
		ต่ำมาก 1	ต่ำ 2	ปานกลาง 3	สูง 4	สูงมาก 5
ผลกระทบ	สูงมาก 5			ระดับความเสี่ยงสูงไม่สามารถยอมรับได้ มีความจำเป็นที่จะต้องบริหารความเสี่ยง เพื่อให้อยู่ในระดับที่สามารถยอมรับได้		
	สูง 4					
	ปานกลาง 3					
	ต่ำ 2	ระดับความเสี่ยงที่ยอมรับได้				
	ต่ำมาก 1					

← Risk Boundary

	ความหมาย
สูงมาก	ระดับความเสี่ยงสูงมาก ยอมรับไม่ได้ จำเป็นเร่งด่วนที่จะต้องบริหารความเสี่ยง มิฉะนั้นองค์กรอาจประสบปัญหารุนแรง
สูง	ระดับความเสี่ยงสูงไม่สามารถยอมรับได้ มีความจำเป็นที่จะต้องบริหารความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้
ปานกลาง	เริ่มที่จะไม่สามารถยอมรับความเสี่ยงได้ และต้องมีการลดและ/หรือควบคุมความเสี่ยงเพิ่มเติม เพื่อให้ไม่ให้ความเสี่ยงเพิ่มมากขึ้นไปอยู่ในระดับที่ยอมรับไม่ได้
ต่ำ	พอที่จะยอมรับความเสี่ยงได้ แต่ควรมีการควบคุมความเสี่ยงเพื่อไม่ให้ความเสี่ยงเกินกว่า Risk Appetites
ต่ำมาก	ยอมรับความเสี่ยงได้โดยไม่ต้องมีการจัดการความเสี่ยงเพิ่มเติม

กรอบการบริหารความเสี่ยง (ERM Framework)		
เรื่อง : การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)	ออกครั้งที่ : 1	แก้ไขครั้งที่ : -
วันที่บังคับใช้ : 17 มกราคม 2561	หน้าที่ 7 ของ 7	

5) **การตอบสนองความเสี่ยง (Risk Respond)**

ในการกำหนดแผนเพื่อตอบสนองความเสี่ยงจะต้องคำนึงถึงความเสี่ยงที่บริษัทยอมรับได้ (Risk Appetite) ต้นทุนที่อาจเกิดขึ้น และประโยชน์ที่จะได้รับ รวมถึงข้อกำหนดกฎหมายอื่นๆ ที่เกี่ยวข้อง โดยแนวทางในการตอบสนองต่อความเสี่ยงมีดังต่อไปนี้

- **การหลีกเลี่ยงความเสี่ยง (Avoid)** มักใช้ในกรณีที่ความเสี่ยงมีความสำคัญสูง ไม่สามารถหาวิธีจัดการให้อยู่ในระดับที่ยอมรับได้
- **การโอนความเสี่ยง (Transfer)** เป็นการโอนความเสี่ยงบางส่วน หรือทั้งหมดไปยังบุคคลภายนอกหรือหน่วยงานภายนอก เช่น การซื้อกรมธรรม์ประกันภัย
- **การลด (Reduce)** เป็นการหามาตรการเพื่อลดโอกาส ผลกระทบ จากเหตุการณ์ความเสี่ยงที่เกิดขึ้น เช่น การเตรียมแผนฉุกเฉิน
- **การยอมรับ (Accept)** เป็นการยอมรับความเสี่ยงที่อยู่ในระดับที่ยอมรับได้ โดยไม่ดำเนินการใดๆ เพื่อลดโอกาสหรือผลกระทบ

6) **กิจกรรมควบคุม (Control Activities)** เป็นกระบวนการปฏิบัติงานเพื่อให้มั่นใจว่าบริษัทได้มีการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อป้องกันไม่ให้เกิดผลกระทบต่อวัตถุประสงค์ของบริษัท โดยกิจกรรมควบคุมสามารถแบ่งออกเป็น 4 ประเภทดังนี้

- 1) การควบคุมเพื่อการป้องกัน (Preventive Control)
- 2) การควบคุมโดยการตรวจสอบ (Detective Control)
- 3) การควบคุมโดยการกำหนดให้จัดทำ (Directive Control)
- 4) การควบคุมโดยการแก้ไข (Corrective Control)

7) **การสื่อสาร การรายงาน และติดตามผล (Communication, Reporting and Monitoring)** เป็นกระบวนการสำคัญที่ส่งผลให้การบริหารจัดการความเสี่ยงดำเนินไปอย่างต่อเนื่องและมีประสิทธิภาพ โดยหน่วยงานบริหารความเสี่ยงจะประสานงานกับผู้รับผิดชอบ รายงานสถานะความเสี่ยง รวมถึงแผนการปฏิบัติงานเพื่อลดความเสี่ยงไตรมาสละ 1 ครั้ง และรายงานต่อคณะกรรมการบริหาร

กรอบการบริหารความเสี่ยงฉบับนี้มีผลบังคับใช้ ตั้งแต่วันที่ 17 มกราคม 2561