ACE
ABSOLUTE CLEAN ENERGY
PUBLIC COMPANY LIMITED

Corporate Risk **Management**

www.ace-energy.co.th

แนวทางการจัดการความเสี่ยงองค์กร (Risk Management Approach)

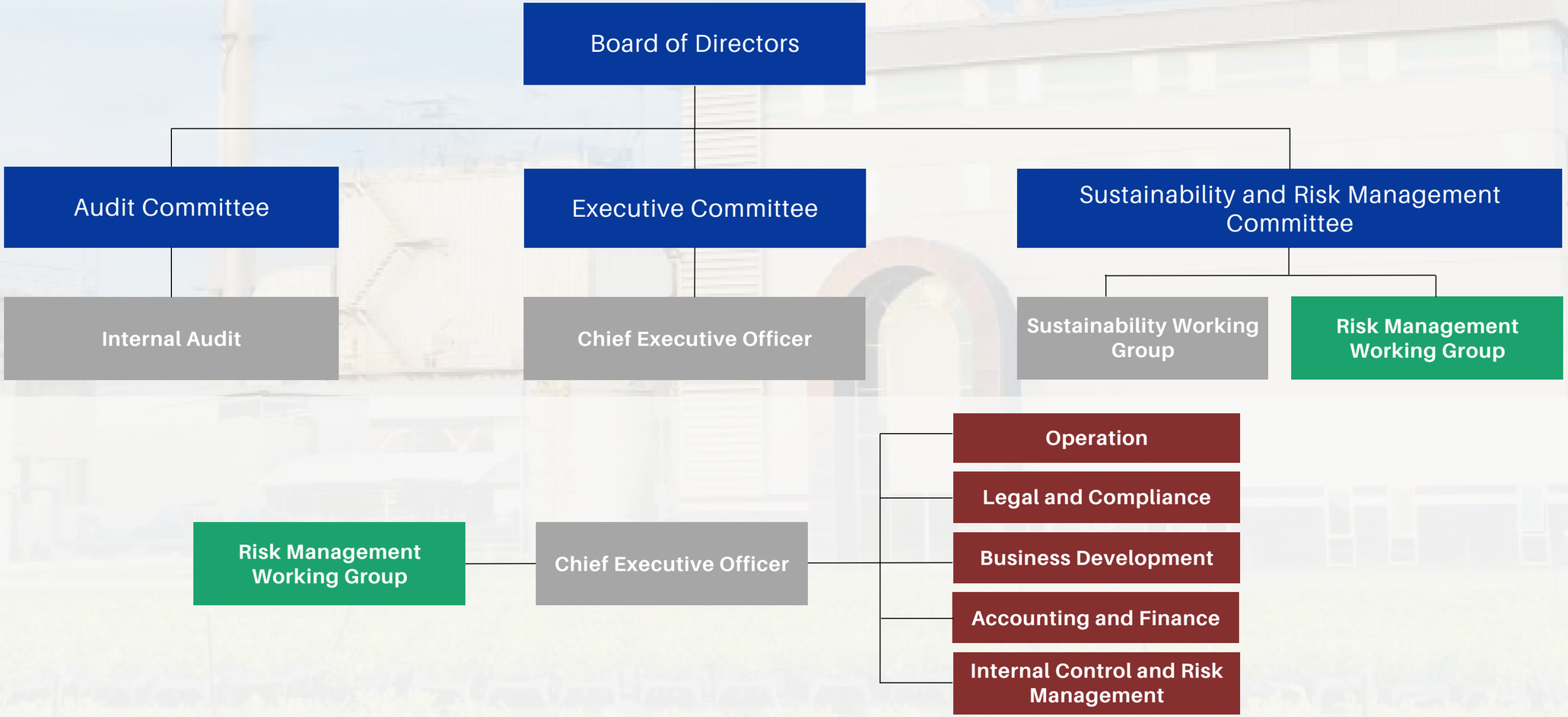
กลุ่มบริษัทตระหนักถึงความสำคัญของการบริหารจัดการองค์กรที่ดี เพื่อขับเคลื่อนองค์กรให้มีการเติบโตและขยายธุรกิจอย่างมีเสถียรภาพ พร้อมทั้งรักษาฐานะการเงินที่มั่นคง และสร้างผลตอบแทนให้แก่ผู้ถือหุ้น ตลอดจนเพื่อเป็นการดำเนินตามหลักการกำกับดูแลกิจการที่ดี จึงได้กำหนด **“นโยบายบริหารความเสี่ยง (Risk Management Policy)”** พร้อมทั้งจัดตั้ง **“คณะกรรมการความยั่งยืนและบริหารความเสี่ยง (Sustainability and Risk Management Committee)”** เพื่อกำกับดูแลและส่งเสริมประสิทธิภาพในการบริหารจัดการความเสี่ยงขององค์กร

โดยในการดำเนินการบริหารจัดการความเสี่ยงทั่วทั้งองค์กร **(Enterprise Risk Management: ERM)** ได้ยึดถือตามมาตรฐานสากล COSO-ERM ซึ่งเป็นกรอบที่จะช่วยให้องค์กรสามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยมีความเสี่ยงครอบคลุมอย่างน้อย 4 ด้าน ได้แก่ ด้านกลยุทธ์ (Strategic Risk) ด้านการเงิน (Financial Risk) การดำเนินงาน (Operational Risk) และด้านกฎหมายและกฎระเบียบ (Compliance Risk) นอกจากนี้ บริษัทฯ ยังได้มีผนวก ESG Risk เข้ากับความเสี่ยงดังกล่าว รวมถึงการพิจารณาความเสี่ยงเกิดใหม่ (Emerging Risks) อาทิ ความเสี่ยงจากการคุมคามทางไซเบอร์และความเป็นส่วนตัว ร่วมด้วย

ทั้งนี้ การบริหารจัดการความเสี่ยงถือเป็นหน้าที่ของผู้บริหารและพนักงานทุกระดับ เพื่อให้มั่นใจว่าการดำเนินธุรกิจของบริษัทฯ จะมีการจัดการที่เป็นระบบและมีประสิทธิภาพในภาพรวม

โครงสร้างการบริหารความเสี่ยงองค์กร (Risk Management Structure)

เพื่อให้การบริหารความเสี่ยงองค์กรดำเนินไปอย่างมีประสิทธิภาพและประสิทธิผล รวมถึงมีการตอบสนองและติดตามผล บริษัทได้มีการกำหนดโครงสร้างการบริหารความเสี่ยง โดยคณะกรรมการบริษัทได้มีการแต่งตั้งคณะกรรมการความยั่งยืนและบริหารความเสี่ยง เพื่อทำหน้าที่สำคัญเกี่ยวกับการบริหารความเสี่ยงของบริษัท ทั้งในด้านนโยบายและแผนการบริหารความเสี่ยงองค์กร การให้คำแนะนำ และการดูแลการบริหารความเสี่ยงให้มีประสิทธิภาพ



*** *Note: Roles and responsibilities of each level are outlined in the Risk Management Policy.*

กรอบการบริหารความเสี่ยงองค์กร (Enterprise Risk Management Framework)

COSO Enterprise Risk Management

INTERNAL ENVIRONMENT

หมายถึง สภาพแวดล้อมภายในองค์กร ซึ่งจะกำหนดทิศทางและโทนขององค์กร รวมถึงกำหนดวัฒนธรรมในการตระหนักและรับมือกับความเสี่ยงของบุคลากรภายในองค์กร ประกอบด้วยคติแนวคิดการบริหารความเสี่ยง (Risk Management Philosophy) เพดานความเสี่ยงที่ยอมรับได้ (Risk Appetite) จรรยาบรรณกับศีลธรรมในการทำงาน และสภาพแวดล้อมการทำงาน

OBJECTIVE SETTING

หมายถึง การกำหนดวัตถุประสงค์ หากคณะผู้บริหารไม่ได้ทำการกำหนดวัตถุประสงค์ในการดำเนินธุรกิจ คณะผู้บริหารจะไม่สามารถระบุเหตุการณ์หรือห่วงโซ่เหตุการณ์ที่สามารถก่อให้เกิดผลกระทบกับการบรรลุเป้าหมายได้ การบริหารความเสี่ยงจะให้ความเชื่อมั่นต่อคณะผู้บริหารว่าการกำหนดวัตถุประสงค์ได้ผ่านกระบวนการและขั้นตอนที่สามารถบ่งบอกถึงความสอดคล้องกับพันธกิจ (Mission) และเพดานความเสี่ยงที่ยอมรับได้ขององค์กร

EVENT IDENTIFICATION

หมายถึง การระบุเหตุการณ์ ทั้งที่อาจเกิดจากภายในและภายนอก ซึ่งสามารถส่งผลกระทบต่อการบรรลุเป้าหมายขององค์กรได้ โดยแยกออกเป็นความเสี่ยงและโอกาส เหตุการณ์โอกาสที่ถูกระบุจะสะท้อนกลับไปในการกำหนดกลยุทธ์และวัตถุประสงค์ของคณะผู้บริหาร

RISK ASSESSMENT

หมายถึง การประเมินความเสี่ยง โดยวิเคราะห์และพิจารณาจากโอกาสที่จะเกิดขึ้น (Likelihood) และความรุนแรงของผลกระทบ (Impact) เพื่อให้เป็นพื้นฐานในการกำหนดวิธีการจัดการความเสี่ยง ความเสี่ยงจะถูกประเมินในรูปแบบโดยแท้ (Inherent) และคงเหลือ (Residual)

กรอบการบริหารความเสี่ยงองค์กร (Enterprise Risk Management Framework)

COSO Enterprise Risk Management & COSO Internal Control

RISK RESPONSE

หมายถึง การตอบสนองความเสี่ยงที่คณะผู้บริหารเลือกจากหลีกเลี่ยงความเสี่ยง (Risk Avoidance), ยอมรับความเสี่ยง (Risk Acceptance), ลดความเสี่ยง (Risk Mitigation) และถ่ายโอนความเสี่ยง (Risk Transfer) เพื่อกำหนดแนวปฏิบัติต่อความเสี่ยงที่สอดคล้องกับเพดานความเสี่ยง และระดับความเบี่ยงเบนของความเสี่ยงที่สามารถลดและยอมรับได้ (Risk Tolerance)

CONTROL ACTIVITIES

หมายถึง กิจกรรมการควบคุม เช่น นโยบายและระเบียบปฏิบัติงานที่กำหนดขึ้นเพื่อช่วยให้การตอบสนองความเสี่ยงดำเนินการไปอย่างมีประสิทธิผล

INFORMATION AND COMMUNICATION

หมายถึง สารสนเทศที่เกี่ยวข้อง ซึ่งได้ถูกระบุ สรุปใจความสำคัญ และสื่อสารอย่างมีรูปแบบและกรอบเวลา เพื่อให้บุคลากรที่เป็นฝ่ายรับข้อมูลนำไปใช้งานและปฏิบัติหน้าที่ตามความรับผิดชอบได้ นอกจากนี้ การสื่อสารอย่างมีประสิทธิผลยังเกิดขึ้นในระดับสูง กลาง และระหว่างองค์กร

MONITORING

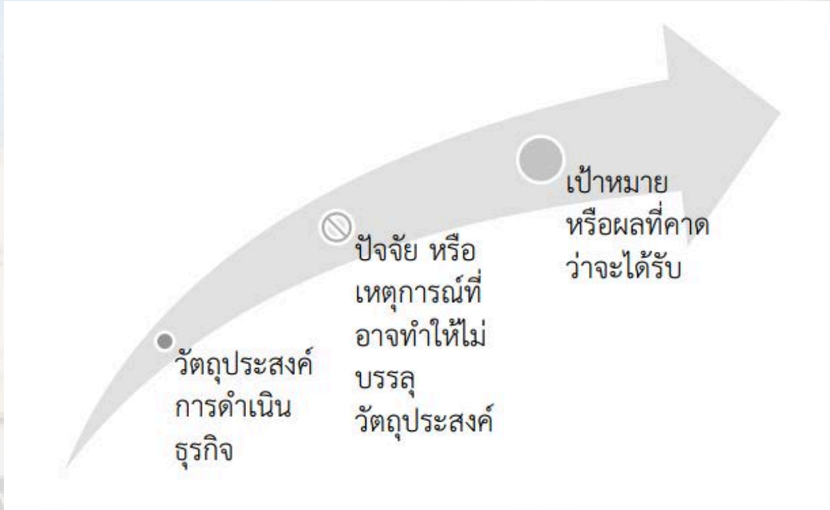
หมายถึง การติดตามสถานะ โดยองค์รวมของการบริหารความเสี่ยง องค์กรจะได้รับการติดตามสถานะและปรับเปลี่ยนแนวทางได้ตามความสำคัญ การติดตามสถานะจะทำผ่านการดำเนินงานของคณะผู้บริหาร การประเมินผล หรือทั้งสองอย่างควบคู่กันไป

กระบวนการบริหารความเสี่ยง (Risk Management Process)

แนวทางที่บริษัทฯ ได้มีการนำมาประยุกต์ใช้ในการประเมินความเสี่ยงองค์กรนี้ มาจากวิธีการประเมินความเสี่ยง (Risk Assessment) ที่เป็นไปตามมาตรฐานการบริหารความเสี่ยงองค์กรตามกรอบแนวคิด COSO (COSO Enterprise Risk Management Framework) ตามลำดับ ดังนี้

กระบวนการบริหารความเสี่ยง (Risk Management Process)

การกำหนดวัตถุประสงค์ (Objective Setting)



หากองค์กรไม่มีกำหนดวัตถุประสงค์การดำเนินธุรกิจเป็นอันดับแรก อาจทำให้ผู้บริหารและกลุ่มผู้ปฏิบัติงานไม่ทราบถึงเป้าหมายหรือผลที่คาดว่าจะได้รับจากการดำเนินธุรกิจ และดำเนินงานในส่วนงานของตนเองได้ ดังนั้น ในการกำหนดวัตถุประสงค์ บริษัทจะมองควบคู่ไปกับเป้าหมายหรือผลที่คาดว่าจะได้รับ ซึ่งช่วยในการมองเห็นและคาดการณ์ถึงปัจจัยหรือเหตุการณ์ที่อาจทำให้องค์กรไม่บรรลุวัตถุประสงค์และเป้าหมายดังกล่าว

กระบวนการบริหารความเสี่ยง (Risk Management Process)

การระบุเหตุการณ์ความเสี่ยง (Risk Identification)

บริษัทฯ ได้สำรวจประเด็นความเสี่ยงที่เกิดขึ้นจริงและอาจเกิดขึ้น มาใช้เพื่อระบุเหตุการณ์ความเสี่ยงขององค์กร โดยการประเมินความเสี่ยงองค์กรครอบคลุมกิจกรรมทางธุรกิจหลักทั้งหมดของบริษัทและบริษัทย่อย รวมถึงครอบคลุมพื้นที่ร้อยละ 100 ของพื้นที่ปฏิบัติการทั้งหมดของบริษัท และบริษัทย่อย ซึ่งความเสี่ยงที่เกิดขึ้นจริงและอาจเกิดขึ้นนั้น เกิดขึ้นจากการนำวิธีการและเทคนิคมาประยุกต์ใช้ในขั้นตอนการระบุความเสี่ยงประกอบด้วย

- การระดมสมองระหว่างส่วนงานที่เกี่ยวข้องกัน (Brainstorm)
- การวิเคราะห์ต้นตอของสาเหตุ (Root Cause Analysis)
- การวิเคราะห์ SWOT (SWOT Analysis)
- การค้นคว้าข้อมูล (Research) จากอุตสาหกรรมเดียวกันเพื่อนำมาเปรียบเทียบ (Peer Comparison)
- การสัมภาษณ์ (Interview) คณะผู้บริหาร และบุคลากรระดับบริหารจัดการในสายงาน

กระบวนการบริหารความเสี่ยง (Risk Management Process)

การระบุประเภทความเสี่ยง

ภายหลังจากการระบุเหตุการณ์ความเสี่ยงขององค์กร บริษัทฯ ได้ระบุประเภทของความเสี่ยงให้สอดคล้องกับนโยบายบริหารความเสี่ยงของบริษัท ซึ่งระบุความเสี่ยงไว้ 4 ประเภทใหญ่ ได้แก่

01

Strategic Risk

หมายถึง ความเสี่ยงทางกลยุทธ์ ที่อาจก่อให้เกิดผลกระทบกับเป้าหมายระดับสูง หรือการเติบโตขององค์กร เหตุการณ์ประเภทนี้จะมีความเกี่ยวเนื่องกับพันธกิจและวัตถุประสงค์การดำเนินธุรกิจขององค์กรในระยะยาว

02

Financial Risk

หมายถึง ความเสี่ยงทางการเงิน ที่อาจก่อให้เกิดผลกระทบโดยตรงกับการบริหารทางการเงินขององค์กร และผลกระทบโดยอ้อมกับการใช้ข้อมูลทางการเงินประกอบการตัดสินใจของคณะผู้บริหาร รวมไปถึงการรายงานทางการเงิน

03

Operational Risk

หมายถึง ความเสี่ยงทางปฏิบัติการ เหตุการณ์ดังกล่าวอาจก่อให้เกิดผลกระทบต่อการใช้ทรัพยากรขององค์กรในการปฏิบัติงาน ในแง่ของประสิทธิภาพ และประสิทธิผลของกระบวนการปฏิบัติการที่เกิดขึ้นทุกๆ วัน และเป็นกิจกรรมหลักในการดำเนินธุรกิจขององค์กร

04

Compliance Risk

หมายถึง ความเสี่ยงทางการปฏิบัติตามระเบียบข้อบังคับ ที่ได้ถูกกำหนดขึ้นโดยพรบ.ต่างๆ กฎหมาย และกฎระเบียบของ ก.ล.ต. ซึ่งเป็นหน่วยงานกำกับดูแลกลุ่มบริษัทมหาชน และจดทะเบียนในตลาดหลักทรัพย์ โดยอาจก่อให้เกิดผลกระทบต่อสถานะการซื้อขายหลักทรัพย์ หรือกระทั่งการดำรงสถานะเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์

*** บริษัทได้มีการผนวก ESG Risk เข้าไปอยู่ในความเสี่ยงในแต่ละประเภทข้างต้น

กระบวนการบริหารความเสี่ยง (Risk Management Process)

การประเมินความเสี่ยง (Risk Assessment)

เป็นการประเมิน 2 มิติ โดยการใช้เมทริกซ์ 4x4 เพื่อพิจารณาผลกระทบ (Impact) ที่องค์กรจะได้รับหากความเสี่ยงนั้นเกิดขึ้นจริง และโอกาสที่ความเสี่ยงนั้นจะเกิดขึ้น (Likelihood) แล้วนำผลการประเมินจากทั้ง 2 มิติมาคำนวณเป็นคะแนน (Risk Score) เพื่อใช้บ่งบอกความรุนแรงของความเสี่ยงนั้น ซึ่งสามารถประเมินความเสี่ยงขององค์กรโดยรวมออกมาได้ทั้งหมด 4 ระดับดังนี้

แผนผังความเสี่ยง (Risk Profile)

Likelihood	Impact 1	2	3	4
4	Medium	High	Very High	Very High
3	Medium	High	High	Very High
2	Low	Medium	High	High
1	Low	Low	Medium	Medium

Low มีโอกาสในการเกิด และมีผลกระทบปานกลาง
Medium มีโอกาสในการเกิด และมีผลกระทบอย่างมีนัยสำคัญ
High มีโอกาสในการเกิด และมีผลกระทบสูง
Very High มีโอกาสในการเกิดสูง และมีผลกระทบรุนแรง

Criteria for Risk Assessment

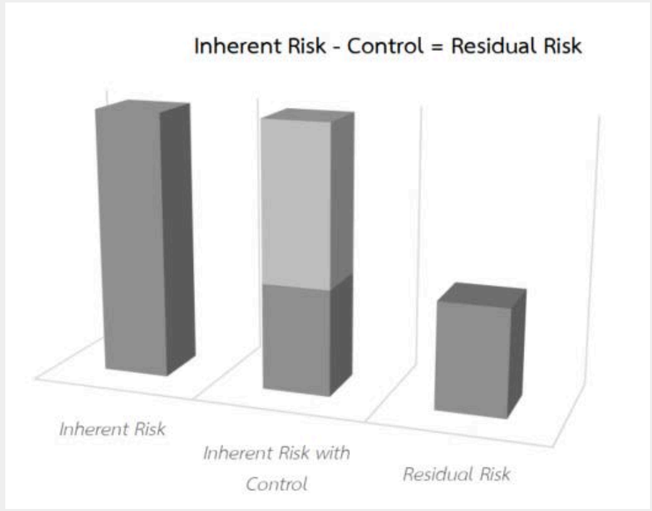
เกณฑ์โอกาสเกิด (Likelihood)	1	2	3	4
ความเป็นไปได้ของเหตุการณ์	เหตุการณ์ที่อาจเกิดขึ้นน้อยมากในการดำเนินธุรกิจ	เหตุการณ์ที่น่าจะเป็นไปได้ หรืออาจเกิดขึ้นได้บางครั้งในการดำเนินธุรกิจ	เหตุการณ์ที่เป็นไปได้สูง หรือเกิดขึ้นเป็นปกติในการดำเนินธุรกิจส่วนใหญ่	เหตุการณ์ที่มีความแน่นอน หรือเกิดขึ้นเป็นปกติในทุกๆ การดำเนินธุรกิจ
ความน่าจะเป็นของการเกิดเหตุการณ์ต่อไตรมาส (%)	<40%	40-59.99%	69-75%	>75%

เกณฑ์ผลกระทบ (Impact)	1	2	3	4
รายได้รวมต่อไตรมาสลดลง (%)	ต่ำ	ปานกลาง	สูง	สูงมาก
กำไรสุทธิต่อไตรมาสลดลง (%)	ต่ำ	ปานกลาง	สูง	สูงมาก
โครงการเกิด Cost Overrun จากที่กำหนดไว้ใน Feasibility Study ที่สถาบันการเงินอนุมัติ (%)	ต่ำ	ปานกลาง	สูง	สูงมาก

กระบวนการบริหารความเสี่ยง

การประเมินความเสี่ยง (Risk Assessment)

บริษัทฯ ดำเนินการประเมินความเสี่ยงทั้งหมด 2 ครั้ง ลงในทะเบียนคุมความเสี่ยง ได้แก่ ประเมินความเสี่ยงตั้งต้น (Inherent Risk) และความเสี่ยงคงเหลือ (Residual Risk) โดยจะประเมินความเสี่ยงตั้งต้นก่อน แล้วจึงค่อยประเมินความเสี่ยงคงเหลือ



INHERENT RISK

เมื่อบริษัทฯ เริ่มประเมิน Inherent Risk ได้จำลองสถานการณ์ว่าหากบริษัทไม่มีวิธีการควบคุม หรือมาตรการตอบสนองใดๆ อยู่เลย (ซึ่งปัจจุบันบริษัทอาจมีอยู่แล้ว) ความเสี่ยงนั้นจะมีโอกาสมากน้อยเพียงใดที่จะเกิดขึ้น รวมถึงจะก่อให้เกิดผลกระทบรุนแรงเพียงใดเมื่อเกิดขึ้น ผลที่ได้จากการประเมินในครั้งนี้ คือ Inherent Risk

RESIDUAL RISK

เมื่อบริษัททำการประเมิน Residual Risk ในรอบนี้ จะไม่ต้องจำลองสถานการณ์เหมือนครั้งก่อน แต่มีการพิจารณาว่าด้วยวิธีการควบคุมหรือมาตรการตอบสนองที่บริษัทมีและใช้อยู่ในปัจจุบัน ทำให้โอกาสเกิดและผลกระทบลดลงมาเหลือที่ระดับใด ผลที่ได้จากการประเมินในครั้งนี้ คือ Residual Risk

*** Residual Risk จะมี Risk Score ต่ำกว่าของ Inherent Risk เนื่องจากบริษัทมีและใช้วิธีการควบคุม หรือมาตรการตอบสนองปัจจุบัน เพื่อลดโอกาสเกิดและผลกระทบลงมาได้ในระดับหนึ่ง

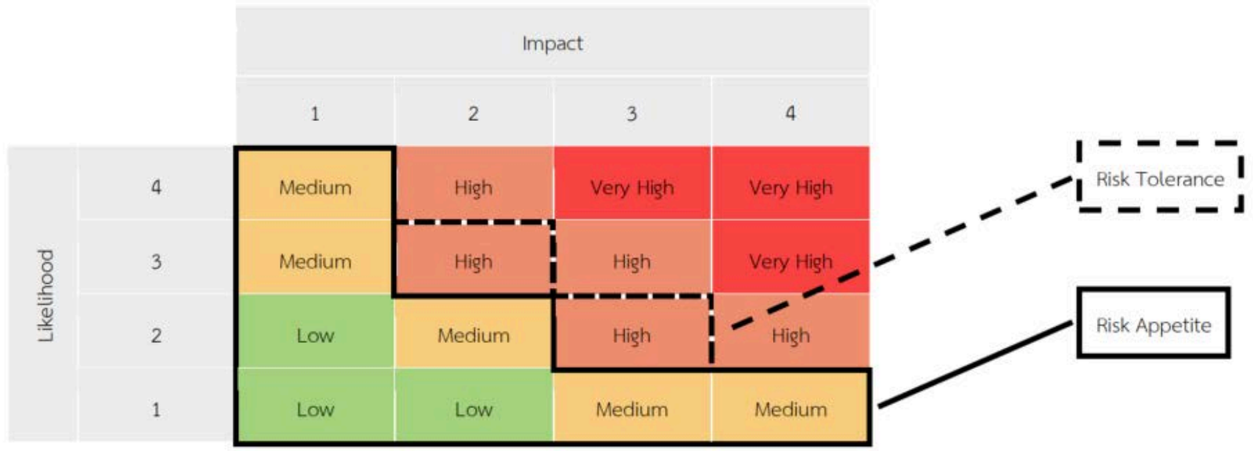
ทะเบียนคุมความเสี่ยง (Risk Register)

No.	Risk Event	Description and Impact	Cause	Category	Assessment of Inherent Risk				Mitigation Strategy	Assessment of Residual Risk				L (Target)	I (Target)	Mitigation Strategy (Additional)	Target Date	Risk Owner	Impact Group
					L	I	Score	Rating		L	I	Score	Rating						
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)

กระบวนการบริหารความเสี่ยง (Risk Management Process)

การจัดลำดับความสำคัญ (Risk Prioritization)

ภายหลังจากที่องค์กรได้ประเมินความเสี่ยงครบทุกเหตุการณ์ และครบทั้ง 2 ครั้งแล้วใน Inherent Risk และ Residual Risk จะนำความเสี่ยงที่ได้ประเมินมาใส่ลงแผนผังความเสี่ยง (Risk Profile) เพื่อให้ทราบว่าความเสี่ยงทั้งหมดขององค์กรกระจายอยู่ในโซนใดบ้าง และมีจำนวนมากน้อยเพียงใด ดังนั้น หาก Risk Profile ขององค์กรมีความเสี่ยงอยู่ในระดับสูงมาก หมายความว่าองค์กรต้องให้ความสำคัญกับความเสี่ยงนั้นเป็นลำดับแรกก่อนอย่างอื่น แล้วจึงค่อยให้ความสำคัญกับความเสี่ยงระดับรองลงมา



ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และค่าความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance)

เป็นความเสี่ยงระดับต่ำ
เป็นความเสี่ยงระดับปานกลาง
เป็นความเสี่ยงระดับสูง
เป็นความเสี่ยงระดับสูงมาก

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ระดับความเสี่ยงที่องค์กรจะไม่กำหนดวิธีการควบคุมหรือมาตรการตอบสนองเพิ่มเติม คือเลือกที่จะยอมรับความเสี่ยงที่ระดับนี้ ดังนั้น Risk Appetite จึงเปรียบเสมือนเป้าหมาย ที่บริษัทต้องลดความเสี่ยงที่ยังมีระดับสูงกว่าจนลงมาถึงระดับที่ปลอดภัย

ค่าความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance) คือระดับความเสี่ยงที่มากกว่าระดับ Risk Appetite แต่ยังสามารถยอมรับได้ ดังนั้น Risk Tolerance จึงเปรียบเสมือนโซนพิเศษ ที่องค์กรยอมรับให้ความเสี่ยงบางเหตุการณ์ไปอยู่ในระดับดังกล่าว ซึ่งเป็นระดับที่ยอมรับได้มากที่สุดแล้ว แต่จะไม่มากเกินไปกว่านี้

กระบวนการบริหารความเสี่ยง (Risk Management Process)

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือระดับความเสี่ยงสูงสุดที่ยอมรับได้ในระดับองค์กร ซึ่งอาจกำหนดขึ้นโดยคณะกรรมการบริษัท หรือโดยกลุ่มบุคคลหรือบุคคลที่คณะกรรมการบริษัทมอบหมาย เช่น คณะกรรมการตรวจสอบ คณะกรรมการบริหาร คณะทำงานบริหารความเสี่ยง หรือประธานเจ้าหน้าที่บริหาร (CEO) และให้ใช้ประกอบการประเมินและบริหารความเสี่ยง โดยความเสี่ยงใดก็ตามที่ได้รับการวิเคราะห์และประเมินแล้วพบว่าอาจส่งผลกระทบต่อบริษัทและบริษัทย่อยเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ให้หน่วยงานเจ้าของความเสี่ยงนั้นๆ จัดทำและทบทวนแผนปฏิบัติการบริหารความเสี่ยง และรายงานต่อคณะทำงานบริหารความเสี่ยง โดยแบ่งระดับความเสี่ยงที่ยอมรับได้ออกเป็น 3 ด้านดังนี้

1

ระดับความเสี่ยงที่ยอมรับได้ด้านการเงิน

บริษัทและบริษัทย่อยยอมรับให้มีการสูญเสียเงิน หรือการลดลงของรายได้ในระดับหนึ่ง แต่ไม่เกินกว่าระดับที่ส่งผลกระทบอย่างเป็นสำคัญต่อสภาพคล่องหรือฐานะทางการเงินของบริษัทและบริษัทย่อย

2

ระดับความเสี่ยงที่ยอมรับได้ด้านความต่อเนื่องในการดำเนินธุรกิจ

บริษัทและบริษัทย่อยยอมรับให้มีการหยุดชะงักหรือความล่าช้าในความต่อเนื่องในการดำเนินธุรกิจได้ในระดับหนึ่ง แต่ไม่ยอมรับให้เกิดการหยุดชะงักหรือความล่าช้าที่เป็นเวลานานจนก่อให้เกิดความเสียหายที่เป็นผลกระทบต่อเนื่องในการปฏิบัติงาน ซึ่งส่งผลต่อระดับความเชื่อมั่นคุณภาพของผลิตภัณฑ์และการให้บริการ และระดับความพึงพอใจของลูกค้าอย่างเป็นสำคัญ

3

ระดับความเสี่ยงที่ยอมรับได้ด้านความพึงพอใจของลูกค้า

บริษัทและบริษัทย่อยไม่ยอมรับให้ผลการประเมินความพึงพอใจของลูกค้าโดยการสุ่มสำรวจของบริษัทและบริษัทย่อยไม่เป็นไปตามระดับมาตรฐานที่ยอมรับได้ของบริษัทและบริษัทย่อย ซึ่งจะส่งผลกระทบต่อผลการดำเนินงานและชื่อเสียงของบริษัทและบริษัทย่อยในอนาคต

กระบวนการบริหารความเสี่ยง (Risk Management Process)

การตอบสนองความเสี่ยง (Risk Response)

Risk Acceptance

การยอมรับความเสี่ยง
เป็นการที่องค์กรเลือกที่จะยอมรับผลกระทบที่องค์กรจะได้รับทั้งหมด หากความเสี่ยงนั้นเกิดขึ้นจริง ในอีกนัยหนึ่ง นั่นคือ องค์กรพิจารณาแล้วว่ามาตรการอื่นๆ อาจไม่คุ้มค่ากับประโยชน์ที่คาดว่าจะได้รับ"

Risk Transfer

การถ่ายโอนความเสี่ยง
เป็นการที่องค์กรเลือกที่จะถ่ายโอนความเสี่ยงที่อาจเกิดขึ้นกับองค์กร ไปให้องค์กรหรือกิจการอื่นที่ไม่ได้อยู่ภายใต้การกำกับดูแลขององค์กรเป็นผู้รับผิดชอบด้วยส่วนหนึ่งหรือทั้งหมด ดังนั้น โอกาสที่ความเสี่ยงนั้นจะเกิดขึ้นกับองค์กร หรือผลกระทบจะน้อยลง เช่น หากอาคารสำนักงานเกิดอัคคีภัย แล้วองค์กรทำประกันอัคคีภัยไว้ บริษัทประกันภัยจะเป็นผู้ชดเชยค่าความเสียหายให้แทน องค์กรจึงได้รับผลกระทบในเรื่องค่าใช้จ่ายน้อยลง

Risk Mitigation

การลดความเสี่ยง
เป็นการที่องค์กรกำหนดวิธีควบคุมขึ้นมาเพื่อลดโอกาสในการเกิดความรุนแรงของผลกระทบ หรือทั้งสองอย่างควบคู่กัน เช่น มาตรการควบคุม มาตรการทางเลือกเสริม มาตรการสำรอง เป็นต้น อย่างไรก็ตาม อาจไม่สามารถลดโอกาสเกิดและผลกระทบได้ทั้งหมด ขึ้นอยู่กับว่าวิธีควบคุมได้ผลจริงมากน้อยเพียงใด

Risk Avoidance

การหลีกเลี่ยงความเสี่ยง
เป็นการที่องค์กรเลือกที่จะไม่ดำเนินกิจกรรมที่อาจทำให้เกิดความเสี่ยงนั้น โดยองค์กรอาจเลือกที่จะระงับกิจกรรมดังกล่าว หรือเปลี่ยนไปดำเนินกิจกรรมอื่นแทนที่ไม่ได้รับผลกระทบจากความเสี่ยงดังกล่าว หรือมีโอกาสที่จะทำให้เกิดความเสี่ยงน้อยลง หากองค์กรเปลี่ยนไปดำเนินกิจกรรมอื่นแทน กิจกรรมนั้นต้องสามารถทำให้องค์กรบรรลุเป้าหมายทางธุรกิจได้ด้วย

ตัวอย่างปัจจัยเสี่ยงองค์กร (Examples of Organizational Risk Factors)

ความเสี่ยงเกิดใหม่ : การคุมคามทางไซเบอร์และความเป็นส่วนตัว	
รายละเอียด / สาเหตุความเสี่ยง	จากความก้าวหน้าทางเทคโนโลยีและการติดต่อสื่อสารด้วยระบบออนไลน์ที่เข้ามามีบทบาทต่อรูปแบบการทำงานมากขึ้น ทำให้กลุ่มบริษัทฯ มีโอกาสที่ต้องเผชิญกับความเสี่ยงจากภัยคุกคามไซเบอร์และความเป็นส่วนตัวของข้อมูล ซึ่งอาจส่งผลกระทบต่อการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล หรือการโจรกรรมข้อมูล
มาตรการจัดการความเสี่ยง	เพื่อเป็นการป้องกันผลกระทบดังกล่าว กลุ่มบริษัทฯ จึงได้กำหนดแนวทางบริหารจัดการเพื่อลดผลกระทบจากความเสี่ยงดังกล่าวที่อาจมีต่อการดำเนินธุรกิจ โดยการวางแผนการดำเนินธุรกิจให้มีความคล่องตัวและยืดหยุ่น สามารถรองรับการเปลี่ยนแปลงของเทคโนโลยี พร้อมทั้งวางแผนกระบวนการทำงานให้สามารถตอบสนองต่อการเปลี่ยนแปลงของเทคโนโลยีที่อาจเกิดขึ้นในอนาคต นอกจากนี้ยังได้กำหนดให้ฝ่ายเทคโนโลยีสารสนเทศของกลุ่มบริษัทฯ มีกการติดตามวิวัฒนาการและรูปแบบการโจมตีทางด้านไซเบอร์ รวมถึงประเมินประสิทธิภาพระบบการรักษาความปลอดภัย (Cyber Security) อย่างสม่ำเสมอ พร้อมทั้งเพิ่มเติมระบบการกู้คืนข้อมูลเมื่อถูกโจมตี เพื่อรองรับความต่อเนื่องในการดำเนินธุรกิจ และส่งเสริมสนับสนุนให้บุคลากรได้รับการอบรมเพื่อเพิ่มพูนความรู้ด้านเทคโนโลยี และเสริมสร้างการตระหนักถึงความปลอดภัยด้านเทคโนโลยีแก่บุคลากรในองค์กรทุกระดับ
ประเภทความเสี่ยง	Compliance Risk / ESG Risk : Governance

ตัวอย่างปัจจัยเสี่ยงองค์กร (Examples of Organizational Risk Factors)

ความเสี่ยงจากการพึ่งพาแหล่งเงินทุนจากสถาบันการเงินหลักแห่งเดียว	
รายละเอียด / สาเหตุความเสี่ยง	เงินกู้ยืมของกลุ่มบริษัทมากกว่าร้อยละ 90 มาจากสถาบันการเงินแห่งเดียว
มาตรการจัดการความเสี่ยง	• สร้างความสัมพันธ์ที่ดีกับสถาบันการเงิน : การสร้างความสัมพันธ์ที่ดีกับสถาบันการเงินจะช่วยให้กลุ่มบริษัทสามารถเข้าถึงแหล่งเงินทุนได้ง่ายขึ้น อีกทั้งยังสามารถได้รับอัตราดอกเบี้ยที่ดีและเงื่อนไขที่เหมาะสม รวมทั้งสร้างความมั่นใจให้กับสถาบันการเงินในความสามารถในการชำระหนี้และการบริหารความเสี่ยงทางการเงินของบริษัท • กระจายการกู้ยืมเงินในสถาบันการเงินหลายราย ซึ่งช่วยลดความเสี่ยงที่อาจเกิดจากการพึ่งพาสถาบันการเงินเดียวเกินไป เช่น ความเสี่ยงจากการปรับเปลี่ยนอัตราดอกเบี้ยหรือการจำกัดวงเงินกู้จากสถาบันการเงินแห่งเดียว โดยการมีหลายแหล่งเงินทุนจะช่วยให้มีความยืดหยุ่นมากขึ้นในการบริหารจัดการหนี้สิน
ประเภทความเสี่ยง	Financial Risk / ESG Risk : Governance

ตัวอย่างปัจจัยเสี่ยงองค์กร (Examples of Organizational Risk Factors)

ความเสี่ยงจากการหยุดชะงักของเครื่องจักรที่อยู่นอกเหนือแผนงาน	
รายละเอียด / สาเหตุความเสี่ยง	ผลการดำเนินงานของกลุ่มบริษัทฯ ขึ้นอยู่กับจำนวนชั่วโมงการเดินเครื่องจักรเป็นสำคัญ ซึ่งในอดีตที่ผ่านมา มีเหตุการณ์ที่ต้องหยุดเดินเครื่องจักรที่อยู่นอกเหนือแผนที่กำหนดไว้ (Unplanned Shutdown) ซึ่งเกิดจากเหตุขัดข้องของเครื่องจักร และส่งผลกระทบโดยตรงต่อการดำเนินงาน
มาตรการจัดการความเสี่ยง	• พัฒนาเครื่องจักรให้มีประสิทธิภาพสูงขึ้น และมีการซ่อมบำรุงให้สามารถเดินเครื่องจักรต่อเนื่องได้ในระยะเวลาที่นานขึ้น รวมทั้งให้เครื่องจักรมีอายุการใช้งานที่ยาวนานขึ้น ซึ่งจะส่งผลให้อัตราการหยุดเดินเครื่องของเครื่องจักรนอกเหนือแผนที่กำหนดไว้มีอัตราที่ลดลง • กำหนดขั้นตอนการคัดเลือกผู้จัดหาและติดตั้งเครื่องจักร โดยผู้ที่จะได้รับคัดเลือกจะต้องเป็นผู้ที่มีความเชี่ยวชาญและมีประสบการณ์โดยตรง มีผลงานในอดีตที่น่าเชื่อถือ อีกทั้งต้องมีการรับประกันผลงานในระยะเวลาที่เหมาะสม รวมทั้งกำหนดแผนการซ่อมบำรุงโรงไฟฟ้า ประกอบด้วยการซ่อมบำรุงประจำปี เพื่อตรวจเช็คสภาพของเครื่องจักรปีละ 2 ครั้ง รวมวันหยุดทั้งสิ้น 12 วัน โดยมีเป้าหมายในการหยุดซ่อมประจำปี ปีละ 1 ครั้ง ครั้งละไม่เกิน 10 วัน และแผนการซ่อมบำรุงใหญ่ ทุก 4 ปี รวมวันหยุดครั้งละ 15 วัน โดยจะกำหนดแผนการตรวจสอบเครื่องจักรแต่ละส่วน เพื่อให้มั่นใจได้ว่าเครื่องจักรทุกเครื่องมีสภาพพร้อมใช้งานและสามารถเดินเครื่องผลิตไฟฟ้าได้ตามปกติ • จัดเตรียมแผนการรับมือในกรณีเกิดเหตุสุดวิสัยและทำให้เกิดการหยุดชะงักขึ้น โดยทีมช่างหรือวิศวกรประจำโรงไฟฟ้า จะเข้าไปตรวจสอบและแก้ไขในเบื้องต้น หากกรณีที่ไม่สามารถแก้ไขได้ จะติดต่อทีมงานผู้เชี่ยวชาญเข้าไปตรวจสอบเพื่อแก้ไขปัญหาดังกล่าวต่อไปโดยเร็ว • ความเสียหายอื่นๆ ที่อาจเกิดจากเหตุการณ์ที่ไม่สามารถควบคุมได้ เช่น ไฟไหม้ ภัยลมพายุ ภัยน้ำท่วม ภัยจากการประท้วง ภัยจากการลุกไหม้ หรือการระเบิดตามธรรมชาติ ซึ่งอาจส่งผลให้โรงไฟฟ้าไม่สามารถเดินเครื่องผลิตไฟฟ้าและการดำเนินธุรกิจหยุดชะงัก ดังนั้น ให้จัดทำประกันความเสี่ยงภัยทรัพย์สินโครงการโรงไฟฟ้าในรูปแบบของประกันความเสี่ยงภัยทรัพย์สิน (Property All Risks) เพื่อลดความเสียหายที่อาจเกิดขึ้นโดยคุ้มครองความสูญเสียหรือความเสียหายต่อทรัพย์สินที่เอาประกันภัย รวมถึงความคุ้มครองประเภทการประกันธุรกิจหยุดชะงัก ซึ่งคุ้มครองความสูญเสียหรือความเสียหายทรัพย์สินที่เอาประกันภัย โดยมีเหตุการณ์ที่ระบุไว้ภายใต้กรมธรรม์ประกันภัยนั้นเพิ่มเติมด้วย
ประเภทความเสี่ยง	Operational Risk / ESG Risk : Governance, Environment

ตัวอย่างปัจจัยเสี่ยงองค์กร (Examples of Organizational Risk Factors)

ความเสี่ยงด้านการทุจริตและคอร์รัปชัน : กระบวนการเบิกจ่ายเงิน	
รายละเอียด / สาเหตุความเสี่ยง	การขาดความรู้ความเข้าใจ และการมีแนวทางปฏิบัติที่ไม่ชัดเจน รวมถึงระบบที่ไม่รองรับ อาจทำให้เกิดการเบิกจ่ายที่ผิดพลาดหรือไม่เหมาะสม ซึ่งอาจถูกเบิกจ่ายให้กับบุคคลหรือองค์กรที่ไม่เกี่ยวข้อง ส่งผลให้เกิดความเสียหายต่อองค์กรในหลายด้าน อาทิ ภาพลักษณ์ ความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย ค่าปรับ การขัดขวางการพัฒนาองค์กรในระยะยาว เป็นต้น
มาตรการจัดการความเสี่ยง	• กำหนดนโยบายด้านการบัญชีและการเงิน แนวทางการเบิกจ่ายและการปฏิบัติที่เกี่ยวข้อง ตลอดจนอำนาจอนุมัติและดำเนินการที่ชัดเจน และดำเนินการทบทวนเพื่อให้สอดคล้องกับปัจจุบันหรือการเปลี่ยนแปลงที่เกิดขึ้น • อบรมและสื่อสารแนวทางการปฏิบัติ และสร้างความตระหนักเกี่ยวกับความเสี่ยงด้านการทุจริตและคอร์รัปชันแก่บุคลากร • หัวหน้างานกำกับดูแลให้พนักงาน/ผู้ใต้บังคับบัญชาปฏิบัติตามระเบียบการเบิกจ่ายเงินอย่างเคร่งครัด • หน่วยงานบัญชี/การเงินตรวจสอบรายการการเบิกจ่ายและเอกสารประกอบ พร้อมทั้งการขออนุมัติจากผู้มีอำนาจในรายการนั้นๆ ก่อนทำรายการและจัดเก็บเอกสารตามแนวทางที่กำหนด • สร้างระบบการบันทึกและติดตามการเบิกจ่ายเงินที่โปร่งใสและสามารถตรวจสอบได้ • ให้มีการตรวจสอบบัญชีจากหน่วยงานภายนอก และมีการหมุนเวียนผู้สอบบัญชี (Auditor Rotation) ตามแนวทางของหน่วยงานกำกับ อาทิ กลต. โดยดำเนินการคัดเลือกผู้สอบบัญชีใหม่เป็นระยะ เพื่อความโปร่งใสขององค์กร
ประเภทความเสี่ยง	Strategy & Financial Risk / ESG Risk : Governance

THANK YOU