นโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยงขององค์กร

(Enterprise Risk Management Policy and Guidelines)

บริษัท ไมโครไฟเบอร์อุตสาหกรรม จำกัด

ทบทวนและปรับปรุงวันที่ 28 สิงหาคม 2568

ประวัติการแก้ไข

ฉบับที่	รายละเอียด	วันที่แก้ไข	วันที่มีผลบังคับใช้
00	**นโยบายการบริหารความเสี่ยง**		16 ส.ค. 2565
01	**1. การจัดประเภทความเสี่ยง เพิ่มเติม:** **ความเสี่ยงด้านการเงิน** (Financial Risk : F) หมายถึง ความเสี่ยงเกี่ยวกับสภาพคล่องทางการเงิน การบริหารทางการเงินและงบการเงิน เช่น ความเสี่ยงจากการจัดสรรงบประมาณไม่เหมาะสม ตั้งงบประมาณผิดพลาดและใช้งบประมาณเกิน รวมทั้งความเสี่ยงจากความผันผวนของปัจจัยทางการตลาด (Market Risk) และ ความเสี่ยงจากการที่คู่สัญญาไม่ปฏิบัติตามภาระผูกพัน (Credit Risk) **ความเสี่ยงที่จะเกิดใหม่** (Emerging Risk: E) ความเสี่ยงที่จะเกิดใหม่เป็นความสูญเสียที่เกิดขึ้นจากความเสี่ยงที่ยังไม่ได้ปรากฏขึ้นในปัจจุบันแต่อาจจะเกิดขึ้นได้ในอนาคตเนื่องจากสภาวะแวดล้อมที่เปลี่ยนไป ความเสี่ยงประเภทนี้เป็นความเสี่ยงที่เกิดขึ้นอย่างช้า ๆ ยากที่จะระบุได้ มีความถี่ของการเกิดต่ำ เมื่อเกิดขึ้นแล้วจะส่งผลกระทบอย่างรุนแรง ความเสี่ยงที่จะเกิดใหม่นี้มักจะถูกระบุขึ้นมาจากการคาดการณ์บนพื้นฐานของการศึกษาจากหลักฐานที่มีปรากฏอยู่ ความเสี่ยงที่จะเกิดใหม่นี้มักจะเป็นผลมาจากการเปลี่ยนแปลงทางการเมือง กฎหมาย สังคม เทคโนโลยี สภาพแวดล้อมทางกายภาพ หรือการเปลี่ยนแปลงตามธรรมชาติ **ความเสี่ยงที่จะเกิดการทุจริต**(Fraud Risk: Fr) เป็นความเสี่ยงที่เกิดจากจากการดำเนินงานที่อาจก่อให้เกิดการทุจริต การขัดกันระหว่างผลประโยชน์ส่วนตนกับผลประโยชน์ส่วนรวม หรือการรับสินบนความเสี่ยงประเภทนี้อาจกระทบต่อชื่อเสียงภาพลักษณ์ของกิจการและอื่นๆ เป็นต้น **ความเสี่ยงในการดำเนินงานอย่างยั่งยืน**(Environmental, Social and Governance : ESG) เป็นความเสี่ยงที่เกี่ยวข้องกับประเด็นด้านสิ่งแวดล้อม สังคมและบรรษัทภิบาลความเสี่ยงประเภทนี้อาจกระทบต่อชื่อเสียงภาพลักษณ์ของกิจการและอื่นๆเป็นต้น **ความเสี่ยงด้านข้อมูลส่วนบุคคล** (Privacy : P) เป็นความเสี่ยงที่มุ่งเรื่องการปฏิบัติการในการประมวลผลข้อมูล เริ่มตั้งแต่กระบวนการเก็บ การเก็บรักษา การใช้ การส่งต่อหรือเปิดเผยและการลบและทำลายที่อาจทำให้สูญหาย รั่วไหลหรือละเมิดข้อมูลส่วนบุคคลซึ่งกระทบต่อสิทธิและเสรีภาพของส่วนบุคคล	**แก้ไขครั้งที่ 1** ว20 ธ.ค. 2565	24 ม.ค. 2566
	2. แก้ไข: 3 ระดับ ดังนี้		

ฉบับที่	รายละเอียด	วันที่แก้ไข	วันที่มีผลบังคับใช้
	ระดับ 1. **H: High Risk** ความเสี่ยงสูงระดับที่มีนัยสำคัญ โดยผู้บริหารจำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ทันที (ระดับคะแนน 15-25 คะแนน) ระดับ 2. **M: Moderate Risk** ความเสี่ยงระดับปานกลาง โดยต้องมีการจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป หรือการติดตามอย่างเหมาะสม เพื่อป้องกันไม่ให้ความเสี่ยงดังกล่าวเกิดขึ้น (ระดับ 5-12 คะแนน) ระดับ 3. **L: Low Risk** ความเสี่ยงระดับต่ำ โดยต้องมีการควบคุมเพื่อป้องกัน หรือการติดตามอย่างเหมาะสม เพื่อไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ (ระดับคะแนน 1-4 คะแนน)		
	3. แก้ไข: 4.1 วิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น โดยมีแนวทางในการจัดการ / บริหารความเสี่ยงได้ 4 วิธี ดังนี้ 4.1.1 การควบคุม/ลด (Reduce) คือ การควบคุมความเสี่ยงหรือหาวิธีการบริหารความเสี่ยง เช่น ใช้เทคนิควิชาการทางวิศวกรรมหรือการจัดทำแผนฉุกเฉิน หรือการปรับปรุงแก้ไขกระบวนการดำเนินงาน เป็นต้น 4.1.2 การโอนย้าย (Transfer) คือ การถ่ายโอนความเสี่ยงหรือโอนย้ายความเสี่ยงให้ผู้อื่นรับผิดชอบ เช่นการทำประกันภัยหรือจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน เป็นต้น 4.1.3 การหลีกเลี่ยง (Avoid) คือ การกำจัดความเสี่ยงหรือหลีกเลี่ยงไม่ยอมรับความเสี่ยงนั้นเลย เช่น การเปลี่ยนวัตถุประสงค์หรือหยุดทำกิจกรรม เป็นต้น 4.1.4 การยอมรับ (Accept) ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใด ๆ เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก มักใช้กับความเสี่ยงที่ต้นทุนของมาตรการจัดการสูงไม่คุ้มกับประโยชน์ที่ได้รับ		
	4. เพิ่มเติม: บริษัทกำหนดให้ทั่วทั้งองค์กรทั้งระดับองค์กรและฝ่ายร่วมมือในการจัดการประเมินความเสี่ยง พร้อมทั้งรายงานการประเมินความเสี่ยงและกำหนดกระบวนการติดตามและประเมินผลการ		
	ดำเนินงานตาม แผนการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อรายงานต่อคณะกรรมการตรวจสอบ/คณะกรรมการบริษัท		

ฉบับที่	รายละเอียด	วันที่แก้ไข	วันที่มีผลบังคับใช้
	5. เพิ่มเติม: บริษัทจะกำหนดให้มีการสอบทานและทบทวนนโยบายการบริหารความเสี่ยงเป็นประจำอย่างน้อยปีละ 1 ครั้งเพื่อให้สอดคล้องกับการปฏิบัติงานปัจจุบัน		
02	**แก้ไขเพิ่ม ดังนี้** 1. แก้ไขเพิ่มเติมชื่อนโยบาย เป็น นโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยงขององค์กร PL-MI-05	**แก้ไขครั้งที่ 2** **28 ส.ค. 2568**	**28 ส.ค. 2568**
	1. ข้อ 1. คำจำกัดความของความเสี่ยงและการบริหารความเสี่ยงองค์กร		
	2. ข้อ 2. ขอบเขตการบริหารความเสี่ยง		
	3. กรอบการบริหารความเสี่ยงตามแนวทางของ COSO ERM 2017		
	4. การบริหารความเสี่ยงตามแนวทางของ COSO ERM 2017 ของกลุ่มบริษัท องค์ประกอบที่ 1 การกำกับดูแลวัฒนธรรมองค์กร (Governance & Culture) องค์ประกอบที่ 2 การกำหนดวัตถุประสงค์และกลยุทธองค์กร (Strategy & Objective Setting) องค์ประกอบที่ 3 ผลการปฏิบัติงาน (Performance) องค์ประกอบที่ 4 การสอบทานและการแก้ไขปรับปรุง (Review & Revision) องค์ประกอบที่ 5 สารสนเทศการสื่อสารและรายงาน (Information, Communication & Reporting)		
	5. ขั้นตอนการปฏิบัติงานบริหารความเสี่ยงเพื่อป้องกันการเข้าสู่ภาวะวิกฤต (กระบวนการหลัก)		
	6. ขอบเขตอำนาจดำเนินการที่เกี่ยวข้องกับกระบวนการบริหารความเสี่ยง		

นโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยงขององค์กร
(Enterprise Risk Management Policy and Guidelines)

1. คำจำกัดความของความเสี่ยงและการบริหารความเสี่ยงองค์กร

ความเสี่ยง (Risk) หมายถึง โอกาส/เหตุการณ์ที่มีความไม่แน่นอน หรือสิ่งที่ทำให้แผนงานหรือการดำเนินงานอยู่ ณ ปัจจุบัน ไม่บรรลุวัตถุประสงค์/เป้าหมาย ที่กำหนดไว้ โดยก่อให้เกิดผลกระทบหรือความเสียหายต่อองค์กรในที่สุด ทั้งในแง่ของผลกระทบที่เป็นตัวเงินหรือผลกระทบที่มีต่อภาพลักษณ์และชื่อเสียงองค์กร

การระบุความเสี่ยง (Risk Identification) หมายถึง การระบุ โอกาส/เหตุการณ์ ในเชิงลบ ที่มีความไม่แน่นอนซึ่งมีผลกระทบทำให้บริษัทฯไม่บรรลุวัตถุประสงค์/เป้าหมายที่กำหนดไว้ทั้งในระดับองค์กร ระดับฝ่าย ระดับหน่วยงาน ซึ่งอาจมาจากทั้งปัจจัยภายใน และปัจจัยภายนอกองค์กร

การควบคุม (Control) หมายถึง นโยบายและกระบวนการปฏิบัติงาน ที่ถูกออกแบบไว้เป็นอย่างดี เพื่อให้มั่นใจว่าเมื่อได้ปฏิบัติตามแล้ว สามารถควบคุมหรือการจัดการความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้ ซึ่งเพียงพอต่อการบรรลุเป้าหมายของบริษัทฯ

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการวิเคราะห์และจัดลำดับความเสี่ยงที่อาจจะเกิดขึ้น โดยพิจารณาจากการประเมินถึงโอกาสที่จะเกิดความเสี่ยง และความรุนแรงของผลกระทบจากความเสี่ยงที่เคยเกิดขึ้น หรืออาจจะเกิดขึ้น ซึ่งมีผลกระทบต่อการบรรลุวัตถุประสงค์ของ บริษัทฯ

ความเสี่ยงโดยธรรมชาติ (Inherent Risk: ความเสี่ยงก่อนการควบคุม) หมายถึง ความเสี่ยงที่เกี่ยวข้องกับวัตถุประสงค์ของบริษัทที่เกิดขึ้น ก่อนการพิจารณาการควบคุมที่มีอยู่ของบริษัท

การควบคุมที่มีอยู่ (Existing Control) หมายถึง การควบคุมที่บริษัทกำหนดขึ้นเพื่อป้องกันหรือควบคุมความเสี่ยงโดยธรรมชาติ (Inherent Risk)

ความเสี่ยงคงเหลือ (Residual Risk) หมายถึง ความเสี่ยงคงเหลือ ภายหลังจากที่มีการพิจารณาวิธีการจัดการมาตรการควบคุมภายในที่มีอยู่ (Inherent Risk – Existing Control = Residual Risk)

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ระดับความเสี่ยงที่บริษัทฯ สามารถยอมรับได้ อยู่ในระดับที่เหมาะสมเพียงพอต่อการบรรลุเป้าหมาย โดยในที่นี้หมายถึงระดับความเสี่ยงที่เป็น Residual Risk มีค่าตั้งแต่ระดับปานกลาง (Medium) ระดับต่ำ (Low) และระดับต่ำมาก (Very Low) (Residual Risk มีค่าเท่ากับ Medium, Low, Ver Low)

แผนงานบริหารความเสี่ยง (Risk management Plan) มาตรการการควบคุมที่กำหนดขึ้น เพื่อควบคุมความเสี่ยงคงเหลือ (Residual Risk) ภายหลังจากการพิจารณาการควบคุมที่มีอยู่ เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite)

การบริหารความเสี่ยงองค์กร (Enterprise Risk Management) หมายถึง กระบวนการที่กำหนดขึ้นและนำไปใช้โดยคณะกรรมการ ฝ่ายบริหาร และบุคลากรอื่นๆขององค์กร เพื่อกำหนดกลยุทธ์และใช้กับหน่วยงานทั้งหมดในองค์กร โดยได้รับการออกแบบมาเพื่อระบุเหตุการณ์ที่อาจเกิดขึ้นซึ่งอาจมีผลกระทบต่อองค์กร รวมทั้งการบริหารความเสี่ยงให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ (risk appetite) ทั้งนี้ เพื่อให้ความมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์ที่ตั้งไว้

ตัวชี้วัดความเสี่ยง (KRI : Key Risk Indicator) หมายถึง เครื่องมือที่หน่วยงานเจ้าของความเสี่ยง (Risk Owner) ใช้ติดตามสถานะความเสี่ยงโดยพิจารณาจากข้อมูลที่มีการกำหนดไว้สำหรับใช้เป็นสัญญานเตือน หรือแนวโน้ม ที่อาจจะทำให้เกิดวิกฤต หรือ ความเสี่ยงเป็นการล่วงหน้า รวมถึงกำหนดมาตรการควบคุมเพื่อป้องกันไม่ให้เกิดเป็นวิกฤต

2. ขอบเขตการบริหารความเสี่ยง

บริษัทฯ มีการกำหนดขอบเขตการบริหารความเสี่ยงให้สอดคล้องกับกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยงของบริษัทฯ และให้ครอบคลุมประเภทความเสี่ยงที่อาจส่งผลกระทบต่อรายได้ เงินทุน ชื่อเสียง หรือการดำรงอยู่ของบริษัทฯ ดังต่อไปนี้

1) **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)** ความเสี่ยงที่เกิดจากการกำหนดนโยบาย แผนกลยุทธ์ แผนการดำเนินงาน และการนำไปปฏิบัติอย่างไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอกซึ่งรวมถึงการเปลี่ยนแปลงทางสังคม เทคโนโลยี และความคาดหวังของสาธารณชน
2) **ความเสี่ยงด้านการบริหารจัดการทางการเงิน (Financial Risk)** ความเสี่ยงที่เกิดจากการที่บริษัทฯ ไม่สามารถชำระหนี้สินและภาระผูกพันเมื่อถึงกำหนด เนื่องจากไม่สามารถเปลี่ยนสินทรัพย์เป็นเงินสดได้ หรือไม่สามารถจัดหาเงินทุนได้อย่างเพียงพอ หรือสามารถจัดหาเงินมาชำระได้ด้วยต้นทุนที่สูงเกินกว่าที่จะยอมรับได้
3) **ความเสี่ยงด้านปฏิบัติการ (Operational Risk)** ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดี ขาดธรรมาภิบาลในองค์กร หรือขาดการควบคุมที่ดีที่เกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน บุคลากร ระบบงาน ระบบเทคโนโลยีสารสนเทศ ความปลอดภัยของข้อมูล หรือเหตุการณ์ภายนอก
4) **ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Compliance Risk)** ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบข้อบังคับของหน่วยงานกำกับดูแล เช่น กรมโรงงานอุตสาหกรรม กรมแรงงาน คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เป็นต้น
5) **ความเสี่ยงด้านชื่อเสียง (Reputation Risk)** หมายความรวมถึง ความเสี่ยงที่เกิดจากความเสียหายต่อบริษัทฯ จากการเสื่อมเสียชื่อเสียงหรือจุดยืนเนื่องจาก ลูกค้า คู่ค้า ผู้ถือหุ้นและ/หรือหน่วยงานกำกับดูแลที่มีมุมมองภาพลักษณ์ต่อบริษัทฯ ในแง่ลบ
6) **ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)** หมายความรวมถึง ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งจะผลกระทบต่อระบบหรือการปฏิบัติงานของบริษัทฯ รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (Cyber threat)
7) **ความเสี่ยงด้านการทุจริต (Fraud Risk)** หมายถึง ความเสี่ยงที่อาจทำให้เกิดความเสียหายใด ๆ กับบริษัท ซึ่งประกอบไปด้วยเจตนาในการกระทำการอย่างใดอย่างหนึ่ง โดยผู้กระทำได้รับประโยชน์หรือเอื้อประโยชน์ให้ผู้อื่นได้รับในสิ่งที่มิควรได้ ดังนี้ การยักยอกทรัพย์สิน (Asset Misappropriation) การคอร์รัปชัน (Corruption) โดยใช้อำนาจหน้าที่การงานของตนเพื่อแสวงหาผลประโยชน์อันมิควรได้ และรวมไปถึง การรายงานอันเป็นเท็จ (Fraudulent Statement) ที่เกี่ยวข้องกับตัวเลขทางการเงินหรือด้านการปฏิบัติงาน ซึ่งทำให้บริษัทเสียหายทั้งด้านการเงินและภาพลักษณ์ของบริษัท
8) **ความเสี่ยงด้านความยั่งยืน (ESG Risk)** ความเสี่ยงด้านความยั่งยืน เป็นความเสี่ยงที่เกี่ยวข้องกับประเด็นด้าน “ESG” ได้แก่ สิ่งแวดล้อม (Environmental) สังคม (Social) และบรรษัทภิบาล (Governance) โดยรวมที่เกิดจากการดำเนินกิจกรรมทางธุรกิจของบริษัทฯ และรวมไปถึงเหตุปัจจัยภายนอกที่เกี่ยวข้องกับประเด็นดังกล่าวข้างต้น ซึ่งมีผลกระทบต่อการดำเนินธุรกิจของบริษัทฯ

3. กรอบการบริหารความเสี่ยงตามแนวทางของ COSO ERM 2017

บริษัทฯ ได้กำหนดถือแนวปฏิบัติสำหรับการบริหารความเสี่ยง ตามกรอบการบริหารความเสี่ยง COSO-ERM 2017 ซึ่งถือเป็นหลักปฏิบัติสากลที่ได้รับการยอมรับ โดยเป็นการบูรณาการร่วมการกำหนดเป้าหมายทางธุรกิจ (พันธกิจ วิสัยทัศน์ และ

กลยุทธ์) การพัฒนากลยุทธ์ การกำหนดวัตถุประสงค์ทางธุรกิจ รวมไปถึงการนำไปปฏิบัติ และมีการวัดผลอย่างเป็นระบบ เพื่อสร้างมูลค่าเพิ่มให้กับองค์กร โดยพิจารณาปัจจัยเสี่ยงที่สำคัญเพื่อให้ผู้มีส่วนได้เสียมั่นใจว่าองค์กรจะบรรลุวัตถุประสงค์บนพื้นฐานของการบริหารความเสี่ยงที่มีประสิทธิภาพและประสิทธิผล

ที่มา : ตลาดหลักทรัพย์แห่งประเทศไทย

บริษัทฯ ให้ความสำคัญกับการสร้างวัฒนธรรมการบริหารความเสี่ยงภายในองค์กร และดำเนินการเพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการทำงานของพนักงานทุกคน โดยผู้บริหารระดับสูงมีการกำหนดทิศทาง นโยบาย และแนวปฏิบัติในการบริหารความเสี่ยง สื่อสารวัตถุประสงค์และประโยชน์ที่จะได้รับจากการบริหารความเสี่ยงไปยังพนักงานทุกคนเพื่อให้เกิดความตระหนักและเห็นคุณค่าของการบริหารความเสี่ยง บูรณาการการบริหารความเสี่ยงเข้ากับการตัดสินใจทางธุรกิจ การกำกับดูแลกิจการ และการควบคุมภายในบริษัทฯ

นอกจากนี้ บริษัทฯ ยังกำหนดให้มีการอบรมพัฒนาบุคลากรของบริษัทฯ ให้มีความรู้ความเข้าใจความระมัดระวัง และตระหนักถึงความเสี่ยงที่อาจจะเกิดขึ้นและมีผลกระทบต่อฝ่ายงาน ต่อองค์กร และต่อผู้เกี่ยวข้อง รวมทั้งส่งเสริมให้มีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆ ภายในองค์กร เพื่อให้การบริหารความเสี่ยงเกิดประสิทธิผลสูงสุด

4. การบริหารความเสี่ยงตามแนวทาง COSO ERM 2017

การบริหารความเสี่ยงของกลุ่มบริษัท – การบูรณาการร่วมกันกับกลยุทธ์และผลการปฏิบัติงาน เป็นกรอบการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017 เพื่อสร้างความชัดเจนเกี่ยวกับความสำคัญของการบริหารความเสี่ยงของกลุ่มบริษัทฯ ในการวางแผนกลยุทธ์ และความสำคัญในการนำการบริหารความเสี่ยงของกลุ่มบริษัท ไปใช้ร่วมกับการดำเนินงานตามปกติทั่วทั้งกลุ่มบริษัท (ทั้งนี้ เนื่องจากความเสี่ยงมีอิทธิพลต่อทุกแผนกและหน้าที่งาน อีกทั้งความเสี่ยงทำให้กลยุทธ์ต้องสอดคล้องกับผลการปฏิบัติงานในทุกแผนกและหน้าที่งาน) กรอบโครงสร้างนี้เป็นชุดของหลักการองค์ประกอบและหลักการ ที่สัมพันธ์กัน มีสาระสำคัญโดยกลุ่มบริษัทได้ดำเนินการปรับใช้ตามหลักการข้างต้นดังนี้

องค์ประกอบที่ 1 : การกำกับดูแลและวัฒนธรรม (Governance & Culture)

การกำกับดูแลกำหนดท่าทีขององค์กร เสริมสร้างความสำคัญ รวมทั้งกำหนดความรับผิดชอบในการควบคุมดูแล สำหรับการบริหารความเสี่ยงขององค์กร วัฒนธรรมที่เกี่ยวข้องกับคุณค่าทางจริยธรรม พฤติกรรมที่พึงประสงค์ และความเข้าใจในความเสี่ยงขององค์กร ประกอบด้วย 4 หลักการ คือ

หลักการที่ 1 : **คณะกรรมการบริษัทกำกับดูแลความเสี่ยง (Execute Board Risk Oversight)**คณะกรรมการบริษัททำหน้าที่ในการควบคุมดูแลกลยุทธ์และการกำกับดูแลเพื่อสนับสนุนผู้บริหารในการ ดำเนินการเพื่อบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยบริษัทมีการกำหนดเป้าหมายทางธุรกิจทั้งระยะสั้นและระยะยาว โดยผ่านการพิจารณาอนุมัติโดยคณะกรรมการของบริษัท ตลอดจน คณะกรรมการมีหน้าที่กำกับดูแลให้มีการบริหารความเสี่ยงที่เหมาะสม

หลักการที่ 2 : **การจัดโครงสร้างสายการบังคับบัญชา (Establishes Operating Structures)** องค์กรจัดตั้งโครงสร้าง ดำเนินงาน เพื่อให้บรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ ในส่วนของกิจกรรมการกำกับดูแลและการบริหารความเสี่ยงบริษัทได้กำหนด โครงสร้างการบริหารความเสี่ยง เพื่อให้มีการดำเนินงานอย่างมีประสิทธิภาพและประสิทธิผล ดังนี้

คณะกรรมการบริหาร (Executive Committee) มีหน้าที่รับผิดชอบ ดังนี้

1. พิจารณาให้ความเห็นต่อนโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยงขององค์กร กลยุทธ์การบริหารความเสี่ยง และกรอบการบริหาร ความเสี่ยงองค์กร ที่สอดคล้องกับวัตถุประสงค์ เป้าหมายหลัก แผนธุรกิจของบริษัท และความเสี่ยงที่ยอมรับได้ของกิจการ ในเรื่องของการบริหารความเสี่ยงโดยรวม และครอบคลุมถึงความเสี่ยงหลัก เช่น ความเสี่ยงด้านธุรกิจ ความเสี่ยงด้านการตลาด ความเสี่ยงด้านสภาพคล่อง ความเสี่ยงด้านปฏิบัติการ และความเสี่ยงที่มีผลกระทบต่อชื่อเสียงของกิจการ เป็นต้น ก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ
2. วางกลยุทธ์ให้สอดคล้องกับนโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยงขององค์กร โดยสามารถประเมินติดตาม และดูแลระดับความเสี่ยงขององค์กรให้อยู่ในระดับที่เหมาะสม สอดคล้องกับกลยุทธ์และเป้าหมายทางธุรกิจ รวมถึงสถานการณ์ที่เปลี่ยนแปลงไป รวมถึงการพิจารณากำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk

Appetite) และความเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ของบริษัทฯ (Risk Tolerance) ก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ

3. ประเมินผลกระทบและโอกาสที่เกิดขึ้นของความเสี่ยงที่ได้ระบุไว้เพื่อจัดลำดับความเสี่ยง และมีวิธีจัดการความเสี่ยงที่เหมาะสม ก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ
4. ดูแลและสนับสนุนให้มีการสอบทาน ทบทวนนโยบายและกรอบการบริหารความเสี่ยง ของบริษัทฯ เป็นประจำอย่างน้อยปีละ 1 ครั้งเพื่อให้แน่ใจว่า นโยบายและกรอบการบริหารความเสี่ยงดังกล่าว ยังคงสอดคล้องและเหมาะสมกับสภาพการดำเนินธุรกิจในภาพรวม และกิจกรรมการบริหารความเสี่ยงของบริษัทฯ
5. มีอำนาจในการเรียกบุคคลที่เกี่ยวข้องมาชี้แจง หรือแต่งตั้งและกำหนดบทบาทที่ให้ผู้ปฏิบัติงานทุกระดับมีหน้าที่บริหารความเสี่ยงตามความเหมาะสม และให้รายงานต่อคณะกรรมการบริหารเพื่อให้การบริหารความเสี่ยงบรรลุวัตถุประสงค์
6. รายงานความเสี่ยงที่สำคัญของบริษัทฯ รวมถึงสถานะของความเสี่ยง แนวทางในการจัดการความเสี่ยง ความคืบหน้า และผลของการบริหารความเสี่ยงให้แก่คณะกรรมการบริษัทเพื่อรับทราบเป็นประจำ และในกรณีที่มีปัจจัยหรือเหตุการณ์สำคัญ ซึ่งอาจมีผลกระทบต่อบริษัทอย่างมีนัยสำคัญ ต้องรายงานต่อคณะกรรมการบริษัทเพื่อทราบและพิจารณาโดยเร็วที่สุด
7. มีอำนาจในการแต่งตั้งคณะทำงานบริหารความเสี่ยงตามความจำเป็น โดยสนับสนุนคณะทำงานบริหารความเสี่ยงในด้านบุคลากร งบประมาณ และทรัพยากรอื่นที่จำเป็น ให้สอดคล้องกับขอบเขตความรับผิดชอบ
8. ให้คำแนะนำ และการสนับสนุนแก่คณะกรรมการบริษัท และคณะทำงานบริหารความเสี่ยง ในเรื่องการบริหารความเสี่ยงระดับองค์กร รวมถึงส่งเสริมและสนับสนุนให้มีการปรับปรุง และพัฒนาระบบการบริหารความเสี่ยงภายในบริษัทอย่างต่อเนื่องและสม่ำเสมอ
9. ขอความเห็นทางวิชาชีพจากบุคคลหรือองค์กรภายนอก เพื่อให้คำปรึกษาหรือคำแนะนำที่เป็นอิสระเกี่ยวกับการบริหารจัดการความเสี่ยงให้แก่คณะกรรมการบริหารและผู้เกี่ยวข้อง รวมทั้งการว่าจ้างบุคคลภายนอกเฉพาะคราว เพื่อช่วยให้การปฏิบัติงานของคณะทำงานบริหารความเสี่ยง เพื่อให้สามารถปฏิบัติหน้าที่ให้บรรลุวัตถุประสงค์ภายในระยะเวลาที่กำหนด
10. ระบุความเสี่ยง โดยพิจารณาจากปัจจัยทั้งภายนอกและภายในบริษัทที่อาจส่งผลให้บริษัทไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ ก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ
11. สื่อสารแลกเปลี่ยนข้อมูล และประสานงานเกี่ยวกับความเสี่ยง และการควบคุมภายในกับคณะกรรมการตรวจสอบ อย่างน้อยปีละ 1 ครั้ง
12. ประเมินผลกระทบ และโอกาสที่เกิดขึ้นของความเสี่ยงที่ได้ระบุไว้เพื่อจัดลำดับความเสี่ยง และมีวิธีจัดการความเสี่ยงที่เหมาะสมก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ
13. ทบทวนความเพียงพอของนโยบาย และระบบการบริหารความเสี่ยง โดยรวมถึงความมีประสิทธิผลของระบบและการปฏิบัติตามนโยบายที่กำหนด
14. พิจารณารายงานผลการประเมินโอกาสที่จะเกิดการทุจริตขึ้น รวมถึงผลกระทบโดยครอบคลุมการทุจริตแบบต่าง ๆ เช่น การจัดทำรายงานทางการเงินเท็จ การทำให้สูญเสียทรัพย์สิน การคอร์รัปชั่น การที่ผู้บริหารสามารถฝ่าฝืนระบบควบคุมภายใน (management override of internal controls) การเปลี่ยนแปลงข้อมูลในรายงานที่สำคัญ การได้มาหรือใช้ไปซึ่งทรัพย์สินโดยไม่ถูกต้อง เป็นต้น
15. ปฏิบัติหน้าที่อื่นใดตามที่คณะกรรมการบริษัทมอบหมาย

คณะทำงานบริหารความเสี่ยง

คณะทำงานบริหารความเสี่ยง ได้แก่ ผู้จัดการฝ่ายและพนักงานในบริษัทฯ ทุกคนจะเป็นผู้รับแนวทางการจัดการความเสี่ยงไปจัดทำแผนรองรับความเสี่ยงที่เกี่ยวข้อง ดำเนินการและรายงานผลการดำเนินการตามแผนให้เลขานุการคณะกรรมการบริหารตามกำหนดเวลา ภายใต้การกำกับดูแลของคณะกรรมการบริหาร ซึ่งแต่ละฝ่ายจะต้องดำเนินการดังต่อไปนี้ระบุความเสี่ยงด้านต่าง ๆ พร้อมทั้งวิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้น รวมทั้งแนวโน้มผลกระทบต่อบริษัทฯ

1. จัดทำแผนการบริหารความเสี่ยงในสายงานที่รับผิดชอบ เพื่อให้มีการนำระบบการบริหารความเสี่ยงมาเป็นส่วนหนึ่งของกระบวนการทำงาน รวมทั้งสื่อสารและถ่ายทอดให้ผู้ปฏิบัติงานในสายงานรับทราบ และถือปฏิบัติโดยถูกต้องเพื่อให้มั่นใจว่าการปฏิบัติมีการประเมิน จัดการ และรายงานความเสี่ยงอย่างเพียงพอ
2. ศึกษา ทบทวน และประเมินความเสี่ยงที่อาจเกิดขึ้น รวมถึงแนวโน้มของผลกระทบที่อาจมีต่อองค์กร ทั้งความเสี่ยงจากภายนอกและภายในองค์กร
3. กำหนดนโยบายบริหารความเสี่ยง แนวทาง และกระบวนการบริหารความเสี่ยงเสนอต่อคณะกรรมการบริหารเพื่อพิจารณาในเรื่องการบริหารความเสี่ยงโดยรวม
4. กำหนดกลยุทธ์ และทรัพยากรที่ใช้ในการบริหารความเสี่ยงของบริษัทฯ ให้สอดคล้องกับนโยบายการบริหารความเสี่ยงตลอดจนกลยุทธ์และทิศทางธุรกิจของบริษัทฯ
5. รายงานผลการดำเนินการในการบริหารความเสี่ยง และจัดการความเสี่ยง รวมถึงสถานะความเสี่ยงในแต่ละหัวข้อที่กำหนดไว้ต่อคณะกรรมการบริหาร เพื่อพิจารณาทุกไตรมาส
6. ปฏิบัติงานอื่น ๆ ตามที่คณะกรรมการบริหารมอบหมาย

คณะกรรมการตรวจสอบ (Audit Committee)

คณะกรรมการตรวจสอบ มีบทบาทหน้าที่การพิจารณาความเสี่ยงที่สำคัญของบริษัทฯ พร้อมเสนอแนะวิธีป้องกันหรือแจ้งให้คณะกรรมการบริษัททราบ เพื่อหามาตรการป้องกันเพื่อลดความเสี่ยงนั้น

รวมถึงสอบทานความเพียงพอและความมีประสิทธิภาพในการบริหารความเสี่ยงของบริษัทฯ

ผู้ตรวจสอบภายใน

1. สอบทานและประเมินประสิทธิผลของกระบวนการบริหารความเสี่ยง
2. สื่อสารทำความเข้าใจกับผู้บริหารและผู้รับการตรวจสอบเกี่ยวกับความเสี่ยง เพื่อวางแผนการตรวจสอบที่เน้นตามความเสี่ยง (Risk Based Auditing)
3. ให้ความมั่นใจว่า บริษัทมีการควบคุมภายในที่เพียงพอและเหมาะสมต่อการจัดการความเสี่ยง และการควบคุมนั้นได้มีการปฏิบัติตามอย่างมีประสิทธิผล

หลักการที่ 3 : **กำหนดวัฒนธรรมที่พึงประสงค์ (Defines Desired Culture)** องค์กรกำหนดพฤติกรรมที่พึงประสงค์ซึ่งแสดงให้เห็นถึงลักษณะของวัฒนธรรมที่กิจการพึงประสงค์ ผ่านนโยบายและแนวปฏิบัติต่างๆ ขององค์กร ตลอดจนผู้บริหารของบริษัทได้ปฏิบัติให้เป็นตัวอย่างแก่พนักงาน เพื่อให้พนักงานเกิดความตระหนักรู้

หลักการที่ 4 : **จูงใจ พัฒนาและรักษาบุคลากรที่มีความสามารถ (Attracts, Develops, and Retains Capable Individuals)** องค์กรยึดมั่นที่จะสร้างทรัพยากรบุคคล เพื่อให้สอดคล้องกับกลยุทธ์และ วัตถุประสงค์ทางธุรกิจ โดยกลุ่มบริษัทฯ กำหนดให้มีระเบียบสวัสดิการสำหรับพนักงาน รวมถึงผลตอบแทนให้กับพนักงานที่อยู่ในเกณฑ์ที่เหมาะสมสอดคล้องกับกลุ่มธุรกิจอุตสาหกรรมเดียวกัน

องค์ประกอบที่ 2: การกำหนดวัตถุประสงค์และกลยุทธองค์กร (Strategy & Objective Setting) กระบวนการวางแผนกลยุทธ์เป็นการทำงานร่วมกันของการบริหารความเสี่ยงขององค์กร กลยุทธ์และการกำหนดวัตถุประสงค์

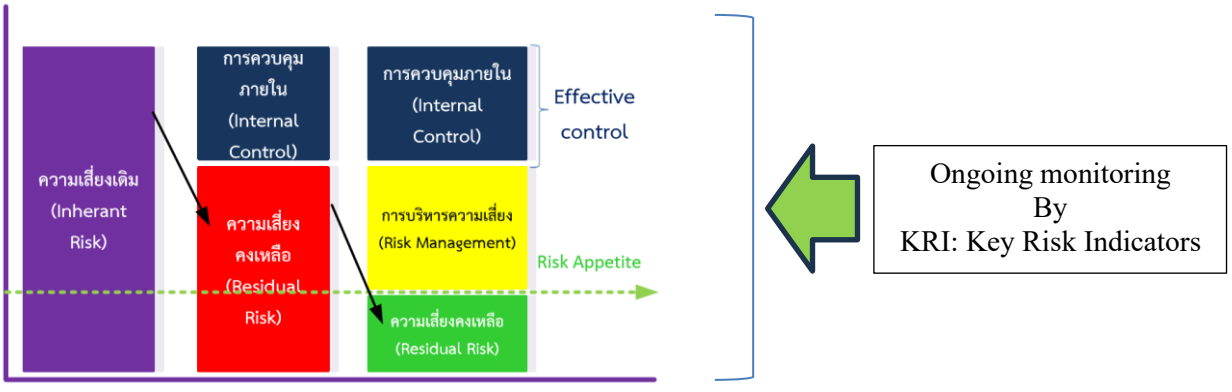
องค์กรกำหนดระดับความเสี่ยงที่ยอมรับได้ให้สอดคล้องกับกลยุทธ์ วัตถุประสงค์ทางธุรกิจทำให้เกิดการ ดำเนินการตามกลยุทธ์ ในขณะเดียวกันก็ใช้เป็นเกณฑ์ในการระบุ ประเมิน และตอบสนองความเสี่ยง ประกอบด้วย 4 หลักการ ได้แก่

หลักการที่ 1 : วิเคราะห์บริบททางธุรกิจ (Analyzes Business Context) – องค์กรพิจารณาผลกระทบที่อาจเป็นไปได้ของบริบททางธุรกิจต่อภาพความเสี่ยง โดยใช้เครื่องมือ SWOT Analysis เพื่อวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค์ ของกลุ่มบริษัท เพื่อให้เกิดความชัดเจนกิจกรรมธุรกิจของกลุ่มบริษัท ตลอดจนนำมากำหนดวัตถุประสงค์ กลยุทธ และแผนธุรกิจขององค์กร

หลักการที่ 2 : กำหนดระดับความเสี่ยงที่ยอมรับได้ (Defines Risk Appetite) - องค์กรกำหนดระดับความเสี่ยงที่ยอมรับได้ในบริบทของการสร้างคุณค่า การรักษาคุณค่า และการทำให้คุณค่าเกิดขึ้นจริง สำหรับการประเมินความเสี่ยงนั้น บริษัทจะพิจารณาจากความเสี่ยงที่คงเหลือจากการควบคุม (Residual Risk) ว่าอยู่ในระดับที่ยอมรับได้หรือไม่ โดยหากพบว่าระดับความเสี่ยงอยู่ในระดับที่ต้องดำเนินการจัดการ (สูง : High และ สูงมาก : Critical) บริษัทจะกำหนดมาตรการการตอบสนองความเสี่ยง หรือกิจกรรมการควบคุมเพิ่มเติม เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (ต่ำมาก Very Low ถึง ปานกลาง (Medium) ต่อไป

หลักการที่ 3 : ประเมินกลยุทธ์ทางเลือก (Evaluates Alternative Strategies) – องค์กรประเมินกลยุทธ์ที่เป็นทางเลือกและผลกระทบที่อาจเกิดขึ้นต่อภาพความเสี่ยงโดยมีกลยุทธในการตอบสนองความเสี่ยง **(Risk Response)** ดังนี้

เมื่อบริษัทฯ ได้ประเมินความเสี่ยงแล้ว พบว่า ความเสี่ยงคงเหลือ (Residual Risk) ยังอยู่ในระดับสูง (High) หรือสูงมาก (Critical) บริษัทฯ จะพิจารณาทางเลือก วิธีการตอบสนองต่อความเสี่ยง ที่เหมาะสม โดยคำนึงถึงต้นทุนที่เกิดขึ้นเปรียบเทียบกับประโยชน์ที่จะได้รับ รวมถึงข้อกฎหมายและข้อกำหนดอื่นๆ ที่เกี่ยวข้อง เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite) หรือกำหนดตัวชี้วัดความเสี่ยง (KRI : Key Risk Indicator) เพื่อกำหนดจุด Early Warning สำหรับติดตามสถานะความเสี่ยง และกำหนดมาตรการป้องกันเพื่อไม่ให้ไปสู่เหตุการณ์วิกฤต



แนวทางในการจัดการความเสี่ยง

- **การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)** คือ การดำเนินการเพื่อหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง มักใช้ในกรณีที่ความเสี่ยงมีความรุนแรงสูง ไม่สามารถหาวิธีลด/จัดการให้อยู่ในระดับที่ยอมรับได้
- **การลดความเสี่ยง (Risk Reduction)** คือ การหามาตรการจัดการ เพื่อลดโอกาสการเกิดเหตุการณ์ความเสี่ยง หรือลดผลกระทบที่อาจเกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้
- **การกระจายความเสี่ยงหรือการโอนความเสี่ยง (Risk Transfer)** คือ การร่วมหรือถ่ายโอนความเสี่ยงทั้งหมดหรือบางส่วนไปยังบุคคล/หน่วยงานภายนอกองค์กร ให้ช่วยแบกรับภาระความเสี่ยงแทน
- **การยอมรับความเสี่ยง (Risk Acceptance)** คือ ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใดๆ เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก มักใช้กับความเสี่ยงที่ต้นทุนของมาตรการจัดการสูงไม่คุ้มกับประโยชน์ที่ได้รับ
- **การติดตามความเสี่ยง (Pursue)** คือ การยอมรับความเสี่ยงเพื่อสร้างโอกาส โดยที่พิจารณาแล้วว่าหากบริษัทฯ ยอมรับความเสี่ยงนั้นจะเกิดประโยชน์ และสร้างมูลค่าเพิ่มหรือการเติบโตให้กับบริษัทฯ

หลักการที่ 4 : กำหนดวัตถุประสงค์ทางธุรกิจ (Formulates Business Objectives) องค์กรพิจารณาความเสี่ยงในขณะที่กำหนดวัตถุประสงค์ทางธุรกิจในระดับต่างๆ ที่สอดคล้องและสนับสนุนกับกลยุทธ์

บริษัทฯ มีการกำหนดวัตถุประสงค์ทางธุรกิจที่ชัดเจน รวมถึงมีการกำหนดตัวชี้วัดอย่างเหมาะสม ผ่านการพิจารณาจากคณะกรรมการบริษัทฯ การบริหารความเสี่ยงขององค์กรจะทำให้เกิดความมั่นใจว่าวัตถุประสงค์ที่กำหนดนั้นจะสนับสนุนและสอดคล้องกับเป้าหมายเชิงกลยุทธ์ขององค์กรและความเสี่ยงที่องค์กรยอมรับได้ โดยบริษัทได้กำหนดวัตถุประสงค์ของกลุ่มบริษัท ดังนี้

วิสัยทัศ (Vision)

“ก้าวเป็นผู้นำอันดับ 1 ใน ASEAN สำหรับนวัตกรรมฉนวนกันความร้อน กันไฟ ป้องกันและดูดซับเสียง ภายในปี 2570”

พันธกิจ (Mission)

“ผลักดันให้ทุกภาคส่วนในอุตสาหกรรมก่อสร้างให้ความสำคัญของการอนุรักษณ์พลังงาน ความปลอดภัย และความเป็นมิตรต่อสิ่งแวดล้อมเป็นอันดับแรก”

กลยุทธ์ (Strategy)

1. นำเสนอผลิตภัณฑ์ฉนวนกันความร้อนแบบครบวงจร โดยการนำความชำนาญในใยแก้วของเราผนวกกับนวัตกรรมใหม่ๆพัฒนาต่อยอดเพื่อเพิ่มการใช้งานใหม่ๆ (new application) และ/หรือใน segment ใหม่ๆ รวมถึงเพิ่มสินค้าในส่วน non-glass wool เพื่อตอบสนองความต้องการลูกค้าอย่างครบวงจร
2. ขยายตลาดไปยังประเทศใน ASEAN โดยผ่านตัวแทนจำหน่ายของเราในต่างประเทศรวมถึงการตั้งสำนักงานสาขาและ/หรือการเข้าซื้อกิจการ
3. จัดเตรียมโครงสร้างธุรกิจเพื่อการพัฒนา ไมโครไฟเบอร์ให้เป็นองค์กรแห่งการเรียนรู้และแบ่งปันอย่างยั่งยืน โดยการสร้างทีมและพัฒนาทักษะในทุกภาคส่วนรวมถึงการนำระบบสารสนเทศ มาใช้ในการวิเคราะห์เพื่อยกระดับองค์กรไปสู่ระดับภูมิภาค (regional level) รวมทั้งยึดมั่นผลประโยชน์

ของผู้มีส่วนได้ส่วนเสียเป็นศูนย์กลาง ยึดถือความเป็นธรรม และรับผิดชอบต่อสิ่งแวดล้อมและสังคมโดยรวม

องค์ประกอบที่ 3 : ผลการปฏิบัติงาน (Performance)

ความเสี่ยงที่อาจมีผลกระทบต่อความสำเร็จของกลยุทธ์และวัตถุประสงค์ทางธุรกิจ จำเป็นต้องถูกระบุและประเมิน ความเสี่ยงจะต้องถูกจัดลำดับความสำคัญตามความรุนแรงในบริบทของระดับความเสี่ยงที่ยอมรับได้ ต่อจากนั้นองค์กร จึงคัดเลือกวิธีการตอบสนองความเสี่ยงและพิจารณาภาพรวมของค่าความเสี่ยงที่องค์กรรับไว้ ผลของกระบวนการข้างต้นนี้จะรายงานต่อผู้มีส่วนได้เสียสำคัญของความเสี่ยง โดยการวัดผลการปฏิบัติงานของกิจกรรมการบริหารความเสี่ยงจะถูกดำเนินการตามหลักการณ์สำคัญดังนี้

หลักการที่ 1 : การระบุความเสี่ยง (Identifies Risk) องค์กรระบุความเสี่ยงที่อาจส่งผลกระทบต่อผลการปฏิบัติงานตามกลยุทธ์และวัตถุประสงค์ทางธุรกิจ

การระบุเหตุการณ์ บริษัทฯ พิจารณาความเสี่ยงทุกด้านที่อาจเกิดขึ้น พิจารณาแหล่งความเสี่ยงทั้งจากสภาพแวดล้อมภายในและภายนอกองค์กร และ*ส่งผลกระทบต่อการบรรลุเป้าหมายของบริษัทฯ เป็นสำคัญ* รวมถึงการจำแนกระหว่างเหตุการณ์ที่เป็นความเสี่ยง โอกาส หรือเป็นทั้งความเสี่ยงและโอกาส ซึ่งการระบุเหตุการณ์อาจดำเนินการโดยการสัมภาษณ์ผู้บริหารระดับสูง หรือฝ่ายจัดการที่รับผิดชอบในแผนงานหรือการดำเนินการนั้น และรวบรวมประเด็นความเสี่ยงสำคัญที่ได้รับความสนใจ หรือเป็นประเด็นที่กังวล เพื่อนำมาจัดทำภาพรวมความขององค์กร (Risk Profile)

สภาพแวดล้อมภายนอกองค์กร บริษัทฯ พิจารณาจากปัจจัยที่เกี่ยวข้อง เช่น

- วัฒนธรรม การเมือง กฎหมาย ความขัดแย้งทางภูมิรัฐศาสตร์ ข้อบังคับ การเงิน เทคโนโลยี เศรษฐกิจ สภาพแวดล้อมในการแข่งขันทั้งภายในประเทศและต่างประเทศ
- ตัวขับเคลื่อนหลักและแนวโน้มที่ส่งผลกระทบต่อวัตถุประสงค์ขององค์กร
- การยอมรับและคุณค่าของผู้มีส่วนได้เสีย
- ความคาดหวังของผู้มีส่วนได้เสียภายนอกองค์กร (สังคม ชุมชน หน่วยงานภาครัฐ ฯลฯ)

สภาพแวดล้อมภายในองค์กร

- ขีดความสามารถขององค์กร ในแง่ของทรัพยากรและความรู้ เช่น เงินทุน เวลา บุคลากร กระบวนการระบบและเทคโนโลยี
- ระบบสารสนเทศ การ Flow ของข้อมูล และกระบวนการตัดสินใจทั้งที่เป็นทางการและไม่เป็นทางการ
- ผู้มีส่วนได้เสียภายในองค์กร
- นโยบาย วัตถุประสงค์ และกลยุทธ์ของบริษัทฯ
- การรับรู้ คุณค่าและวัฒนธรรมองค์กร
- มาตรฐานและแบบจำลองที่พัฒนาโดยบริษัทฯ
- โครงสร้าง เช่น ระบบการจัดการ บทบาทหน้าที่และความรับผิดชอบ

หลักการที่ 2 : ประเมินความรุนแรงของความเสี่ยง (Assesses Severity of Risk) กลุ่มบริษัท มีการประเมินระดับความรุ่นแรงของความเสี่ยงได้แก่

- การประเมินความเสี่ยงที่เกิดขึ้นโดยธรรมชาติ (Inherent Risk) ซึ่งเมื่อกลุ่มบริษัทมีการดำเนินกิจกรรมทางธุรกิจ จึงหลีกเลี่ยงไม่ได้ที่จะเกิดความเสี่ยงต่อการดำเนินกิจกรรมฯ ซึ่งจะทำให้เห็นปัจจัยเสี่ยงที่สำคัญ (Key Risk) ที่มีผลกระทบต่อวัตถุประสงค์ของกลุ่มบริษัท

- การประเมินความเสี่ยงคงเหลือ (Residual Risk) ภายหลังจากการระบุกิจกรรมการควบคุมที่มีอยู่ (Existing control) เพื่อพิจารณาประสิทธิภาพและประสิทธิผลของการควบคุมภายในที่บริษัทได้ออกแบบไว้ ว่าสามารถควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้หรือไม่ เพื่อกำหนดมาตรการจัดการกับความเสี่ยง ตามหลักการที่ 6 รวมถึงกำหนดแผนงาน และตัวชี้วัดความเสี่ยงที่สำคัญ (KRI : Key Risk Indicator) เพื่อเฝ้าระวัง

สำหรับการประเมินความเสี่ยงเป็นขั้นตอนที่จะต้องดำเนินการต่อจากการระบุความเสี่ยง โดยการประเมินความเสี่ยงประกอบด้วย 2 กระบวนการหลัก ได้แก่

1) การวิเคราะห์ความเสี่ยง

การพิจารณาสาเหตุและแหล่งที่มาของความเสี่ยง ผลกระทบที่ตามมาทั้งในทางบวกและทางลบ รวมทั้งโอกาสที่อาจเกิดขึ้นของผลกระทบที่อาจตามมา โดยจะต้องมีการระบุถึงปัจจัยที่มีผลกระทบและโอกาสที่จะเกิดขึ้น ทั้งนี้ เหตุการณ์หรือสถานการณ์หนึ่งๆ อาจจะเกิดผลที่ตามมาและกระทบต่อวัตถุประสงค์หรือเป้าหมายหลายด้าน นอกจากนั้น ในการวิเคราะห์ ควรพิจารณาถึงมาตรการจัดการความเสี่ยงที่ดำเนินการอยู่ ณ ปัจจุบัน รวมถึงประสิทธิผลของมาตรการดังกล่าวด้วย

2) การประเมินความเสี่ยง

การประเมินความเสี่ยงจะเปรียบเทียบระหว่างระดับของความเสี่ยงที่ได้จากการวิเคราะห์ความเสี่ยง เทียบกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ในกรณีที่ระดับของความเสี่ยงไม่อยู่ในระดับที่ยอมรับได้ของเกณฑ์การยอมรับความเสี่ยง ความเสี่ยงดังกล่าวจะได้รับการจัดการทันที

<u>ปัจจัยที่นำมาพิจารณาเพื่อประกอบการกำหนดเกณฑ์ความเสี่ยง</u>

- ลักษณะและประเภทของผลกระทบที่สามารถเกิดขึ้นและแนวทางในการประเมินผลกระทบ
- แนวทางในการระบุโอกาสในการเกิดขึ้น
- กรอบเวลาของโอกาสและผลกระทบที่เกิดขึ้น
- แนวทางในการกำหนดระดับความเสี่ยง
- ระดับของความเสี่ยงที่ยอมรับได้
- ระดับของความเสี่ยงที่จะต้องจัดการ

บริษัทฯ ได้กำหนดหลักเกณฑ์การประเมินระดับโอกาสและผลกระทบไว้ 5 ระดับ ซึ่งในการประเมินความเสี่ยงนั้นๆ คณะกรรมการตรวจสอบจะเป็นผู้พิจารณากำหนดเกณฑ์ประเมินระดับโอกาสและผลกระทบสำหรับความเสี่ยงนั้นๆ ซึ่งเสนอโดยคณะทำงานบริหารความเสี่ยง โดยเฉพาะต่อไป

โอกาสที่จะเกิดเหตุการณ์ความเสี่ยง (Likelihood)

ระดับของโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงและระดับของความเสียหาย แบ่งเป็น 5 ระดับ โดยกำหนดนิยามในแต่ละระดับ เพื่อเป็นหลักเกณฑ์ประเมินความเสี่ยงทั้งด้านผลกระทบ (Impact) และโอกาสที่จะเกิดความเสี่ยง (Probability) ดังนี้

1. <u>เกณฑ์การประเมินความเสี่ยงด้านผลกระทบ (Impact)</u> บริษัทฯ ได้กำหนดให้มีการประเมินผลกระทบต่อวัตถุประสงค์ 4 ด้านดังนี้
   - ผลกระทบด้านประสิทธิผลการปฏิบัติการ
   - ผลกระทบด้านมูลค่าความเสียหายทางการเงิน
   - ผลกระทบด้านการปฏิบัติตามกฎเกณฑ์ทางการ (ภาครัฐ)
   - ผลกระทบด้านกลยุทธ์ของบริษัทฯ

โดยแบ่งระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นดังนี้

Risk Criteria : Impact

Impact			ด้านประสิทธิผลปฏิบัติการ	ด้านมูลค่าความเสียหายทางการเงิน	ด้านการปฏิบัติการกฎเกณฑ์ทางการ	ด้านกลยุทธ์
ระดับ	คำอธิบาย	ระดับความรุนแรง	การดำเนินงานไม่เป็นไปตามเป้าหมาย	มูลค่าความเสียหายทางการเงิน (บาท) : หนึ่งรายการที่เกิดขึ้น	ผลกระทบ	การดำเนินงานไม่เป็นไปตามเป้าหมาย
5	วิกฤต	สูงมาก	ไม่เป็นไปตามเป้าหมายมากกว่า 40%	> 800,000	• คดีขึ้นสู่ศาล หรือ กระทบต่อใบอนุญาต หรือ เสียสิทธิทางการค้าละเมิดสัญญา	ไม่สามารถบรรลุเป้าหมายตามกลยุทธ์ทุกข้อที่กำหนดไว้
4	มีนัยสำคัญ	สูง	ไม่เป็นไปตามเป้าหมายมากกว่า 30-40%	600,001 - 800,000	• ถูกปรับเนื่องจากมิได้ปฏิบัติตามกฎเกณฑ์ • หนังสือเตือนจากภาครัฐเพื่อให้แก้ไข	ไม่สามารถบรรลุเป้าหมายหลักเพียงบางข้อ โดยจำเป็นต้องปรับแผนหลักเพื่อให้บรรลุ
3	ปานกลาง	ปานกลาง	ไม่เป็นไปตามเป้าหมายมากกว่า20-30%	400,001 - 600,000	• ไม่มีการถูกดำเนินคดี หรือ ฟ้องร้อง สามารถเจรจาประนีประนอมได้ • กระทบการปฏิบัติงานภายในบริษัท และสามารถปรับปรุงแก้ไขแต่ต้องใช้ระยะเวลานาน (Long term)	สามารถบรรลุเป้าหมายหลักเพียงบางข้อ แต่ควรปรับแผนสนับสนุนเพื่อให้บรรลุเป้าหมายหลัก
2	น้อย	น้อย	ไม่เป็นไปตามเป้าหมายมากกว่า 10-20%	200,001-400,000	• สามารถตรวจพบได้โดยกระบวนการภายในและดำเนินการแก้ไขภายในได้ทันที มีให้ระดับความรุนแรงเพิ่มขึ้น • กระทบการปฏิบัติงานภายในบริษัท และสามารถปรับปรุงแก้ไขในระยะเวลาที่กำหนด (short term)	สามารถบรรลุเป้าหมายหลักได้ทุกข้อ แต่ควรปรับแผนสนับสนุนเพื่อให้บรรลุเป้าหมายในระยะเวลาที่กำหนดได้
1	ไม่เป็นนัยสำคัญ	น้อยมาก	ไม่เป็นไปตามเป้าหมายน้อยกว่าหรือเท่ากับ 10%	< 200,000	• กระทบการปฏิบัติงานเฉพาะแค่หน่วยงานนั้นๆ และสามารถปรับปรุงแก้ไขได้ทันที	สามารถบรรลุเป้าหมายหลักได้ทุกข้อ และอาจพิจารณาปรับแผนสนับสนุนเพื่อให้บรรลุเป้าหมาย

2. เกณฑ์การประเมินความเสี่ยงด้านโอกาสที่จะเกิดความเสี่ยง (Probability) บริษัทฯ ได้กำหนดเกณฑ์การประเมินโอกาสที่จะเกิดโดยมีรายละเอียดดังนี้

ระดับ	คำอธิบาย	โอกาสในการเกิด		Approx.
5	ค่อนข้างแน่นอน	สูงมาก	มากกว่า 20 ครั้ง / ปี	ดำเนินกิจกรรมนั้นในทุกวัน
4	น่าจะเกิด	สูง	16-20 ครั้ง/ปี	ดำเนินกิจกรรมนั้นในทุกสัปดาห์
3	เป็นไปได้ที่จะเกิด	ปานกลาง	11-15 ครั้ง /ปี	ดำเนินกิจกรรมนั้นใน 3 ครั้งเดือน
2	ไม่น่าจะเกิด	น้อย	5-10 ครั้ง / ปี	ดำเนินกิจกรรมนั้นใน 1-2 ครั้ง/ เดือน
1	ยากที่จะเกิด	น้อยมาก	น้อยกว่า 5 ครั้ง / 1 ปี	ดำเนินกิจกรรมนั้นทุกปี หรือทุกสามเดือน

แผนภาพความเสี่ยง (Risk Map)

แผนภาพความเสี่ยงเป็นเครื่องมือที่ใช้สำหรับการรายงานระดับความเสี่ยงที่ได้รับการประเมิน โดยแสดงถึงความสัมพันธ์ระหว่างโอกาสที่จะเกิดเหตุการณ์และผลกระทบของความเสี่ยง โดยประกอบด้วย 2 แกน คือ

- แกนผลกระทบของความเสี่ยง (Impact)
- แกนโอกาสที่จะเกิดความเสี่ยง (Probability)

ระดับความเสี่ยง คือ ตัวชี้วัดที่ใช้ในการกำหนดความสำคัญของความเสี่ยง โดยค่าระดับความเสี่ยงได้จากการนำโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงมาพิจารณาร่วมกัน ดังนี้

ระดับความเสี่ยง = ระดับโอกาสที่จะเกิดความเสี่ยง x ระดับผลกระทบที่เกิดขึ้น

ระดับความเสี่ยงที่ได้จากการคำนวณตามสูตรข้างต้น บริษัทฯจะกำหนดความหมายของแต่ละระดับดังนี้

Risk Matrix

ระดับ		ไม่มีนัยสำคัญ	น้อย	ปานกลาง	มาก	ร้ายแรงมาก
ความน่าจะเกิด		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
บ่อยครั้ง	5					
บ่อย	4					
ปานกลาง	3					
ไม่บ่อย	2					
นาน ๆ ครั้ง	1					

คำอธิบายไม่ตรงกับด้านบน เช่น นานๆครั้ง - ยากที่จะเกิด

หลักการที่ 3 : จัดลำดับความสำคัญของความเสี่ยง (Prioritizes Risks)

องค์กรจัดลำดับความสำคัญของ ความเสี่ยง (เพื่อใช้เป็นเกณฑ์ในการเลือกวิธีการตอบสนองความเสี่ยง) ตลอดจนพิจารณาถึงความเร่งด่วนของการปรับปรุงมาตรการควบคุมความเสี่ยง ซึ่งพิจารณาถึงความคุ้มค่าของงบประมาณ ระยะเวลาในการดำเนินการ กลุ่มบริษัทฯ ได้กำหนดระดับความสำคัญของความเสี่ยงไว้ดังนี้

ระดับความเสี่ยง	คำอธิบาย
ต่ำมาก (Very Low)	ระดับความเสี่ยงที่ยอมรับได้ ภายใต้วิธีการจัดการความเสี่ยงที่มีอยู่เดิมไม่ต้องมีการจัดการเพิ่มเติม (โซนสีเขียวอ่อน)
ต่ำ (Low)	ระดับความเสี่ยงที่ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ไม่สามารถยอมรับได้ (โซนสีเขียวเข้ม)
ปานกลาง (Medium)	ระดับความเสี่ยงที่ยอมรับได้ แต่หน่วยงานเจ้าของความเสี่ยงอาจกำหนดให้มีการควบคุมเพื่อป้องกัน หรือการติดตามสถานะความเสี่ยงไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ไม่สามารถยอมรับได้ (โซนสีเหลือง)
สูง (High)	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้หรือมีการกำหนดตัวชี้วัดความเสี่ยงที่มีการติดตามอย่างใกล้ชิด (รายสัปดาห์/รายเดือน) (โซนสีส้ม)
สูงมาก (Critical)	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้โดยเร็วที่สุด และกำหนดตัวชี้วัดความเสี่ยงอย่างเข้มข้น รวมถึงมีการติดตามอย่างใกล้ชิด (Real time/ รายวัน/ รายสัปดาห์) (โซนสีแดง)

สำหรับการประเมินความเสี่ยงนั้น บริษัทจะพิจารณาจากความเสี่ยงที่คงเหลือจากการควบคุม (Residual Risk) ว่าอยู่ในระดับที่ยอมรับได้หรือไม่ โดยหากพบว่าระดับความเสี่ยงอยู่ในระดับที่ต้องดำเนินการจัดการ (สูง : High และ สูงมาก : Critical) บริษัทจะกำหนดมาตรการการตอบสนองความเสี่ยง หรือกิจกรรมการควบคุมเพิ่มเติม เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ต่ำมาก (Very Low) ถึง ปานกลาง (Medium) ต่อไป

หลักการที่ 4 : ดำเนินการตอบสนองต่อความเสี่ยง (Implements Risk Responses)

องค์กรระบุและเลือกวิธีการตอบสนองความเสี่ยง ผ่านการกำหนด กิจกรรมการควบคุม (Control Activities) ซึ่งประกอบไปด้วย แผนงาน (กำหนดวิธีการควบคุม) งบประมาณบริหารความเสี่ยง ระยะเวลาดำเนินการ

กิจกรรมการควบคุม คือ นโยบายและกระบวนการปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้ เพื่อป้องกัน (Mitigation Plan) ไม่ให้เกิดผลกระทบต่อเป้าหมายขององค์กร บริษัทฯ จึงกำหนดกิจกรรมการควบคุม ดังนี้

1) การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก
2) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อให้ค้นพบข้อผิดพลาดที่ได้เกิดขึ้นแล้ว
3) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ
4) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้น และป้องกันไม่ให้เกิดซ้ำอีกในอนาคต

ทั้งนี้ ในการดำเนินกิจกรรมการควบคุมควรต้องคำนึงถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุนกับผลประโยชน์ที่คาดว่าจะได้รับ รวมถึง การควบคุมนั้นต้องถูกกำหนดให้มีขึ้นอย่างชัดเจนเป็นลายลักษณ์อักษร (Present) และนำไปปฏิบัติจริง (Function) โดยกิจกรรมการควบคุมควรมีองค์ประกอบดังนี้

- กำหนดวิธีการดำเนินงาน (ขั้นตอนและกระบวนการ) ที่สอดคล้องกับนโยบายหลักของกลุ่มบริษัทฯ
- การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น ซึ่งควรมีความรับผิดชอบดังนี้

(1) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

(2) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

- การติดตามผลเพื่อให้เกิดการพัฒนาระบบการควบคุมภายในอย่างต่อเนื่อง

หลักการที่ 5 : พัฒนาภาพรวมความเสี่ยง (Develops Portfolio View)

องค์กรพัฒนาและประเมินภาพรวม ของความเสี่ยง ภาพรวมของความเสี่ยงช่วยให้คณะกรรมการ ผู้บริหาร พิจารณาเห็นถึงประเภทความรุนแรง และความสัมพันธ์ระหว่างความเสี่ยงต่างๆ รวมถึงผลกระทบในการปฏิบัติงาน ทั้งเชิงปริมาณและคุณภาพ เพื่อช่วยให้มีการตัดสินใจในการจัดการความเสี่ยงและเฝ้าระวังไม่ให้ความเสี่ยงกลายเป็นวิกฤต

องค์ประกอบที่ 4 : การสอบทานและแก้ไขปรับปรุง (Review & Revision)

ทำได้โดยสอบทานผลการปฏิบัติงานขององค์กร ทำให้สามารถพิจารณาได้ว่าองค์ประกอบของการบริหารความเสี่ยงขององค์กรทำหน้าที่ได้ดีเพียงใดในช่วงที่ผ่านมา และเมื่อเกิดการเปลี่ยนแปลงที่สำคัญ รวมทั้งมีสิ่งใดที่จำเป็นต้องมีการแก้ไขปรับปรุง

หลักการที่ 1 : ประเมินการเปลี่ยนแปลงที่มีสารสำคัญ (Assess Substantial Change)

องค์กรระบุและประเมินการเปลี่ยนแปลงที่อาจส่งผลกระทบอย่างมากต่อกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยพิจารณาจาก<u>สภาพแวดล้อมภายใน</u> เช่น โครงสร้าง กระบวนการที่สำคัญ ระบบสารสนเทศ นวัตกรรม ผู้นำและทรพัยากรบุคคล <u>สภาพแวดล้อมภายนอก</u> เช่น กฎหมาย ข้อกำหนดหน่วยงานราชการ เศรษฐกิจ การเมือง สังคม พฤติกรรมผู้บริโภค ภัยธรรมชาติ สงครามความขัดแย้งทางภูมิรัฐศาสตร์ สิ่งแวดล้อม กระแสวัฒนธรรม เป็นต้น

หลักการที่ 2 : สอบทานความเสี่ยงและผลการปฏิบัติงาน (Reviews Risk and Performance)

คณะกรรมการบริษัทพิจารณาติดตามและสอบทานผลการดำเนินการของบริษัท ร่วมกับความเสี่ยงของกลุ่มบริษัท อาจมีผลต่อการบรรลุวัตถุประสงค์ โดยผ่านการกำกับดูแลของคณะกรรมการตรวจสอบ คณะทำงานบริหารความเสี่ยง ตลอดจนหน่วยงานเจ้าของความเสี่ยงที่มีการวัดผลการปฏิบัติงานประจำวัน รายเดือน หรือรายไตรมาส โดยพิจารณาความเสี่ยงที่อาจเกิดขึ้นในขณะที่มีการปฏิบัติงาน โดยกำหนดให้มีการรายงานความเสี่ยงอุบัติใหม่ผ่านกระบวนการรายงาน Incidence Report

หลักการที่ 3 : กำหนดแนวทางการปรับปรุงการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง (Pursues Improvement in Enterprise Risk Management)

กลุ่มบริษัทฯ พยายามปรับปรุงการบริหารความเสี่ยงขององค์กร อย่างต่อเนื่อง โดยกลุ่มบริษัทฯ กำหนดให้มีการทบทวนนโยบาย หลักเกณฑ์ ที่สำคัญที่เกี่ยวข้องกับกระบวนการบริหารความเสี่ยงเพื่อให้ทันต่อสถานการที่มีการเปลี่ยนแปลงอย่างรวดเร็ว รวมถึง พัฒนาความรู้ของบุคคลากรของกลุ่มบริษัทฯ ผ่านแผนการฝึกอบรมของกลุ่มบริษัทฯ ซึ่งได้กำหนดไว้ในแผนการพัฒนาบุคลากรของกลุ่มบริษัท

องค์ประกอบที่ 5 : สารสนเทศ การสื่อสารและการรายงาน (Information, Communication, & Reporting)

การบริหารความเสี่ยงขององค์กรจำเป็นต้องมีกระบวนการที่ต่อเนื่องเพื่อการได้มาและการใช้สารสนเทศที่จำเป็นร่วมกัน ทั้งสารสนเทศจากแหล่งภายในและภายนอกซึ่งไหลเวียนอยู่ทั่วทั้งองค์กร ประกอบด้วย 3 หลักการ ได้แก่

หลักการที่ 1 : ผลักดันการใช้เทคโนโลยีสารสนเทศ (Leverages Information and Technology)

กลุ่มบริษัทฯ ใช้ประโยชน์จากระบบสารสนเทศและเทคโนโลยีของกิจการเพื่อสนับสนุนการบริหารความ เสี่ยงขององค์กร โดยมีการพิจารณาใช้ฐานข้อมูลที่บริษัทมี ในการกำหนดตัวชีวัดความเสี่ยงที่สำคัญ (KRI : Key Risk Indicator) ที่มีผลต่อการบรรลุวัตถุประสงค์ของกลุ่มบริษัทฯ

บริษัทฯ จัดให้มีระบบสารสนเทศที่เชื่อถือได้ มีรูปแบบที่เหมาะสมและสอดคล้องกับขนาด ลักษณะ และความซับซ้อนของธุรกิจ โดยระบบสารสนเทศดังกล่าวจะสามารถสนับสนุน ติดตามดูแล และควบคุมการบริหารความเสี่ยง รวมถึงการนำข้อมูลไปใช้อย่างถูกต้องและมีประสิทธิภาพ การจัดให้มีระบบการจัดเก็บข้อมูลที่ปลอดภัย มีการกำหนดสิทธิในการเข้าถึงข้อมูลของบุคลากรเฉพาะที่เกี่ยวข้อง และจัดให้มีระบบสำรองข้อมูลรวมทั้งกระบวนการกู้คืนข้อมูลในกรณีที่เกิดเหตุฉุกเฉินขึ้น ตามแผนบริหารความต่อเนื่องของฝ่ายเทคโนโลยีสารสนเทศ บริษัทฯ กำหนดให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นความเสี่ยงสำคัญขององค์กรที่จะต้องได้รับการเฝ้าระวัง ติดตาม และประเมินผลอย่างต่อเนื่อง และให้ความสำคัญในการจัดสรรทรัพยากรให้เพียงพอต่อการบรรลุวัตถุประสงค์ของบริษัทฯ รวมถึงมีการกำหนดตั้วชี้วัดความเสี่ยงที่สำคัญอย่างครอบคลุม

หลักการที่ 2 : การสื่อสารสารสนเทศด้านความเสี่ยง (Communication Risk Information)

องค์กรใช้ช่องทางการ สื่อสารต่างๆ เพื่อสนับสนุนการบริหารความเสี่ยงขององค์กร สารสนเทศเป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ ประเมิน และจัดการความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กร ควรได้รับการบันทึกและสื่อสารไปยังบุคลากรในองค์กรอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อให้สามารถปฏิบัติงานตามหน้าที่และความรับผิดชอบได้ รวมถึงเป็นการรายงานการบริหารจัดการความเสี่ยง เพื่อให้ทุกคนในองค์กรได้รับทราบถึงความเสี่ยงที่เกิดขึ้นและผลของการบริหารจัดการความเสี่ยงเหล่านั้น การสื่อสารที่มีประสิทธิภาพยังครอบคลุมถึงการสื่อสารจากระดับบนลงล่าง ระดับล่างไปสู่บน และการสื่อสารระหว่างหน่วยงาน การบริหารความเสี่ยง ควรใช้ทั้งข้อมูลในอดีตและปัจจุบัน ข้อมูลในอดีตจะแสดงแนวโน้มของเหตุการณ์และช่วยคาดการณ์การปฏิบัติงานในอนาคต ส่วนข้อมูลปัจจุบันมีประโยชน์ต่อผู้บริหารในการพิจารณาความเสี่ยงที่เกิดขึ้นในกระบวนการ สายงาน หรือหน่วยงานซึ่งช่วยให้องค์กรสามารถปรับเปลี่ยนกิจกรรมการควบคุมตามความจำเป็นเพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

หลักการที่ 3 : รายงานความเสี่ยง วัฒนธรรมและผลการปฏิบัติงาน (Reports on Risk, Culture, and Performance) –

องค์กรรายงานความเสี่ยง วัฒนธรรม และผลการปฏิบัติงานในระดับต่างๆ ครอบคลุมทั้งองค์กร บริษัทฯ มีความจำเป็นต้องได้รับการสื่อสารถึงการประเมินความเสี่ยงและการควบคุมความคืบหน้าในการบริหารความเสี่ยง การดูแลติดตามแนวโน้มของความเสี่ยงหลัก รวมถึงการเกิดเหตุการณ์ผิดปกติอย่างต่อเนื่อง เพื่อให้มั่นใจว่า

- เจ้าของความเสี่ยง (Risk Owner) มีการติดตาม ประเมินสถานการณ์ วิเคราะห์ และบริหารความเสี่ยงที่อยู่ภายใต้ความรับผิดชอบของตนอย่างสม่ำเสมอ และเหมาะสม
- ความเสี่ยงที่มีผลกระทบสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กร ได้รับการรายงานถึงความคืบหน้าในการบริหารความเสี่ยง และแนวโน้มของความเสี่ยงต่อผู้บริหารที่รับผิดชอบและคณะกรรมการตรวจสอบ
- มีระบบการควบคุมภายที่เพียงพอ เหมาะสม และมีประสิทธิภาพ โดยมีการนำมาปฏิบัติใช้จริงเพื่อป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้น รวมทั้งมีการปรับปรุงแก้ไขการควบคุมภายในอยู่เสมอเพื่อให้สอดคล้องกับสถานการณ์หรือความเสี่ยงที่เปลี่ยนไป

บริษัทฯ จัดให้มีระบบการรายงานข้อมูลการบริหารความเสี่ยงและสถานะความเสี่ยงตามประเภทของความเสี่ยง โดยคำนึงถึงความเสี่ยงภาพรวมของบริษัทฯ โดยจัดให้มีการทำรายงานดังต่อไปนี้

- สรุปรายงานสถานะความเสี่ยง และสรุปรายงานการปฏิบัติตามมาตรการบริหารความเสี่ยงที่ผ่านการกลั่นกรองจากคณะทำงานบริหารความเสี่ยง และคณะกรรมการตรวจสอบ ก่อนเสนอต่อคณะกรรมการบริษัทฯ เพื่อพิจารณาอย่างน้อยไตรมาสละ 1 ครั้ง
- รายงานผลการบริหารความเสี่ยงต่อคณะกรรมการบริษัท อย่างน้อยไตรมาสละ 1 ครั้ง เพื่อประกอบการพิจารณาทบทวนความเพียงพอของกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยง
- รายงานเหตุการณ์สำคัญอันอาจส่งผลกระทบต่อความมั่นคงและความยั่งยืนของบริษัทฯอย่างมีนัยสำคัญ

5. ขั้นตอนการปฏิบัติงานบริหารความเสี่ยงเพื่อป้องกันการเข้าสู่ภาวะวิกฤต (กระบวนการหลัก)

บริษัทฯ กำหนดให้มีการจัดทำนโยบาย คู่มือการบริหารความเสี่ยง โดยมีการพิจารณาทบทวนอย่างน้อยปีละ 1 ครั้งเพื่อให้มีการปรับปรุงกระบวนการบริหารความเสี่ยงให้ทันสมัยและมีประสิทธิภาพ ประสิทธิผลอย่างต่อเนื่อง โดยภาพรวมของ

ระบบการบริหารจัดการความเสี่ยงของบริษัท สามารถแสดงเป็นแผนภาพดังนี้

6. ขอบเขตอำนาจดำเนินการที่เกี่ยวข้องกับกระบวนการบริหารความเสี่ยง

ลำดับ	เรื่อง	MGR	DIR/GM	RWG[1]	Ex-com	RMC	BOD	หมายเหตุ
11.1	**การดำเนินการบริหารความเสี่ยง**							
	1. ผลการประเมินความเสี่ยง	V	V	C	C	A	K	
	2. การตอบสนองความเสี่ยง	V	V	C	C	A	K	
	3. ตัวชี้วัดความเสี่ยง (Key Risk Indicator: KRI)	V	V	C	C	A	K	
	4. แผนงานและงบประมาณบริหารความเสี่ยง	V	V	C	C	A	K	
	5. การปรับลดระดับความเสี่ยงที่ดำเนินการตามแผนงานแล้ว	V	C	A	K	K		
	6. การจัดการความเสี่ยงหรือเหตุการณ์ฉุกเฉิน (Incident)		V	V	A	K	K	
11.2	**ระเบียบอำนาจดำเนินการ**							
	1. กฎบัตรคณะทำงานการบริหารความเสี่ยง			V	C	A		
	2. ระเบียบอำนาจดำเนินการบริหารความเสี่ยง			V	C	A		
	3. กระบวนการบริหารความเสี่ยง			V	A	K		ประธานคณะทำงานลงนาม
	4. ทบทวนกฎบัตร ระเบียบอำนาจดำเนินการ กระบวนการบริหารความเสี่ยง			V	C	A	K	
11.3	**การรายงานกิจกรรมการบริหารความเสี่ยง**							
	1. รายงาน Incident	V	V	A	K	K	K	
	2. รายงานสถานะความเสี่ยง		V	A	K	K	K	
	3. รายงานความคืบหน้าแผนงานบริหารความเสี่ยง		V	A	K	K	K	

[1] RWG = Risk Management Working Group

แนวทางปฏิบัติ				
K	=	Acknowledge	=	รับทราบ
A	=	Approve	=	อนุมัติ
Co-A	=	Co-Approve	=	อนุมัติร่วม
Co-V	=	Co-Verify	=	ตรวจสอบร่วม
C	=	Consent	=	เห็นชอบก่อนนำเสนออนุมัติในลำดับถัดไป
V	=	Verify	=	ตรวจสอบ