ต้นฉบับ

S.A.F. SPECIAL STEEL PUBLIC COMPANY LIMITED

บริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน)

S.A.F. SPECIAL STEEL PUBLIC COMPANY LIMITED

นโยบาย

(Policy)

เรื่อง การบริหารความเสี่ยง

(เลขที่ PC-MG-04)

แก้ไขครั้งที่ 03 ประกาศใช้วันที่ 17 ธันวาคม 2568

จัดทำโดย		อนุมัติโดย
คณะทำงานบริหารความเสี่ยง	คณะกรรมการตรวจสอบ	คณะกรรมการบริษัท

ประวัติการจัดทำ และทบทวนเอกสาร

ครั้งที่	วันที่แก้ไข	รายละเอียด
00	10 ก.ย. 64	เผยแพร่เพื่อใช้งานครั้งที่ 1
01	1 เม.ย. 65	แก้ไขชื่อนิติบุคคลและตราบริษัทหลังแปรสภาพเป็น บมจ.
02	9 พ.ค. 67	เพิ่มเติม Financial Risk
03	17 ธ.ค. 68	ทบทวนประจำปี 2568 และปรับปรุงเนื้อหาให้เหมาะสม / เพิ่ม ESG Risk

1. **วัตถุประสงค์**

เพื่อให้กรรมการ ผู้บริหาร และพนักงานทุกคนตระหนักถึงความสำคัญของการบริหารความเสี่ยงในทุกด้านของการดำเนินธุรกิจของบริษัท (Key List) และ การบริหารความเสี่ยงในด้านสิ่งแวดล้อม (Environment) ด้านสังคม (Social) และด้านบรรษัทภิบาล (Governance) หรือ ESG Risk และเพื่อจัดการปัญหาอุปสรรคในการทำงาน ป้องกันหรือลดโอกาสที่จะเกิดเหตุการณ์ไม่พึงประสงค์และผลกระทบที่อาจเกิดขึ้น ซึ่งจะทำให้การดำเนินงานไม่บรรลุวัตถุประสงค์ แผนกลยุทธ์ แผนงานและการดำเนินงาน และเป้าหมายขององค์กร นอกจากนี้ยังเป็นการส่งเสริมให้มีการกำกับดูแลกิจการที่ดี

2. **ขอบเขต**

ครอบคลุมหลักเกณฑ์การพิจารณา ประเมิน ควบคุม และตรวจสอบการบริหารความเสี่ยง โดยกำหนดให้คณะกรรมการบริษัท ผู้บริหาร และพนักงานทุกระดับทุกคน นำแนวทางการบริหารความเสี่ยงไปประยุกต์ใช้อย่างเหมาะสม

3. **นิยาม**

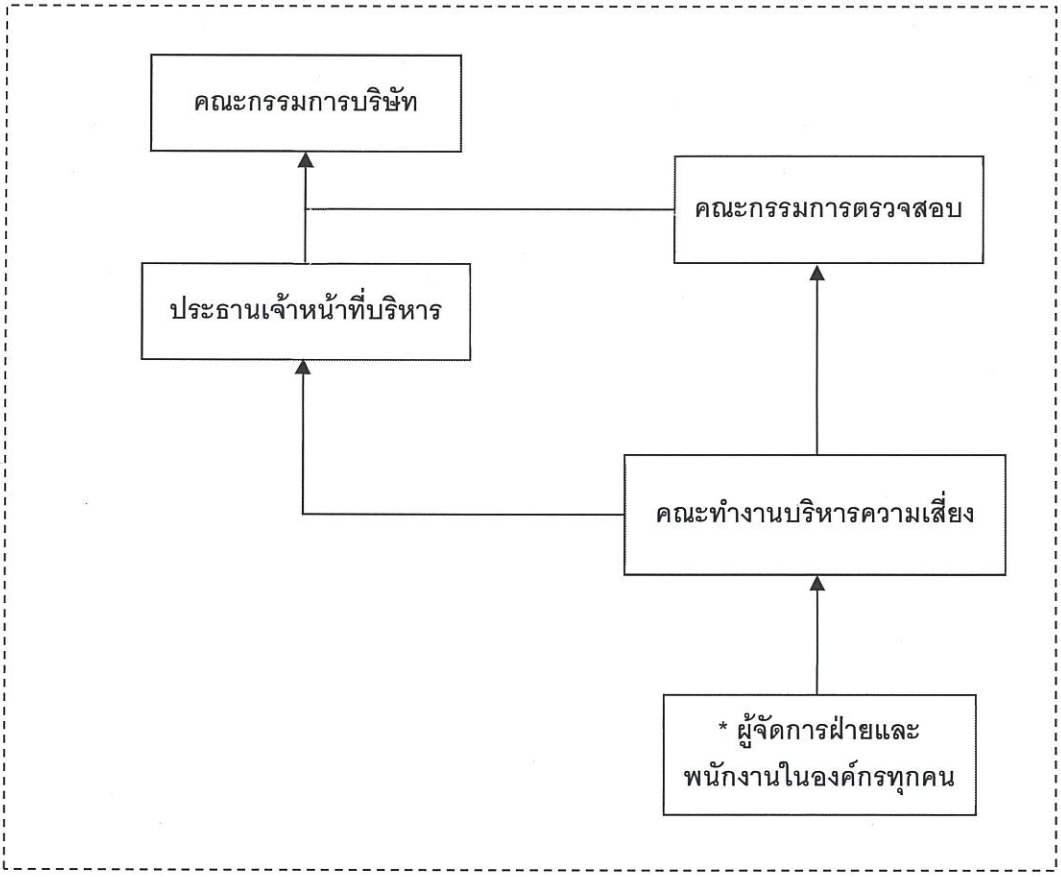
ความเสี่ยง คือ เหตุการณ์การกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และอาจจะส่งผลกระทบหรือสร้างความเสียหาย หรือความล้มเหลว หรือเหตุการณ์ที่ไม่พึงประสงค์ที่เป็นอุปสรรคต่อการทำงาน หรือลดโอกาสที่จะบรรลุความสำเร็จของเป้าหมายและวัตถุประสงค์ของบริษัท ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้ ทั้งความเสี่ยงด้าน ESG และ ความเสี่ยงด้านการดำเนินธุรกิจ อาทิ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านการเงิน และความเสี่ยงด้านการปฏิบัติตามกฎระเบียบข้อบังคับ

การบริหารความเสี่ยง คือ กระบวนการดำเนินการเกี่ยวกับความเสี่ยงในการดำเนินงานของบริษัทตามเป้าหมายที่ได้วางไว้ โดยจัดให้มีระบบและแบบแผนในการปฏิบัติงานด้านความเสี่ยง เพื่อการจัดการความเสี่ยงที่ส่งผลกระทบต่อบริษัทให้ระดับและขนาดของผลกระทบที่จะเกิดขึ้นอยู่ในระดับที่สามารถยอมรับได้ รวมทั้ง มีการประเมินควบคุมและการตรวจสอบได้อย่างมีระบบโดยคำนึงถึงการบรรลุเป้าหมายของบริษัทเป็นสำคัญ

4. <u>นโยบาย</u>

ทุกหน่วยงานต้องจัดให้มีการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง ภายใต้กระบวนการบริหารความเสี่ยงที่เป็นมาตรฐานเดียวกัน โดยการนำเทคโนโลยีสารสนเทศมาใช้ เพื่อให้เกิดความรวดเร็วในการสื่อสารและประมวลผล ตลอดจนต้องมีการติดตามและประเมินผลพร้อมปรับแผนการบริหารความเสี่ยงเป็นระยะๆอย่างสม่ำเสมอ เพื่อให้การดำเนินการบรรลุวัตถุประสงค์

โครงสร้างการบริหารความเสี่ยง



หมายเหตุ

* ผู้จัดการฝ่ายและพนักงานในองค์กรทุกคนขอเรียกว่า ผู้ปฏิบัติงานบริหารความเสี่ยงของฝ่าย หรือคณะผู้ปฏิบัติงาน

โครงสร้างการบริหารความเสี่ยงประกอบด้วย คณะทำงานบริหารความเสี่ยงและคณะผู้ปฏิบัติงาน

- **ระดับองค์กร** ได้แก่ คณะกรรมทำงานบริหารความเสี่ยง ภายใต้นโยบายและการกำกับดูแลของคณะกรรมการตรวจสอบ โดยมีประธานเจ้าหน้าที่บริหารรับผิดชอบให้เป็นไปตามแนวทางปฏิบัติของบริษัท
- **ระดับฝ่าย** ได้แก่ ผู้จัดการฝ่าย และพนักงานภายในองค์กรทุกคน (เรียกว่า คณะผู้ปฏิบัติงาน) ภายใต้การกำกับดูแลของคณะทำงานบริหารความเสี่ยง

หน้าที่และความรับผิดชอบในการบริหารความเสี่ยง

<u>หน้าที่ความรับผิดชอบของคณะทำงานบริหารความเสี่ยงในการดำเนินกิจการ</u>

คณะทำงานบริหารความเสี่ยง มีหน้าที่และความรับผิดชอบดังนี้

1) กำหนดนโยบายและโครงสร้างการบริหารความเสี่ยง เพื่อเสนอต่อคณะกรรมการตรวจสอบ โดยใช้แนวทางการบริหารความเสี่ยงของตลาดหลักทรัพย์แห่งประเทศไทย และสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย
2) วางกลยุทธ์ให้สอดคล้องกับนโยบายการบริหารความเสี่ยง เพื่อให้สามารถประเมิน ติดตาม และควบคุมความเสี่ยงแต่ละประเภทให้อยู่ในระดับที่ยอมรับได้ โดยให้หน่วยงานต่างๆมีส่วนร่วมในการบริหารและควบคุมความเสี่ยง
3) ประเมินความเสี่ยงในระดับองค์กร และกำหนดวิธีการบริหารความเสี่ยงนั้นให้อยู่ในระดับที่ยอมรับได้ รวมทั้งควบคุมดูแลให้มีการบริหารความเสี่ยงตามวิธีการที่กำหนดไว้
4) ทบทวนนโยบายการบริหารความเสี่ยงและปรับปรุงให้มีประสิทธิภาพและประสิทธิผลอย่างเพียงพอที่จะควบคุมความเสี่ยง
5) มีอำนาจในการเรียกบุคคลที่เกี่ยวข้องมาชี้แจงหรือแต่งตั้งและกำหนดบทบาทที่ให้ผู้ปฏิบัติงานทุกระดับ มีหน้าที่บริหารความเสี่ยงตามความเหมาะสม และให้รายงานต่อคณะทำงานบริหารความเสี่ยงเพื่อให้การบริหารความเสี่ยงบรรลุวัตถุประสงค์
6) รายงานผลของการบริหารความเสี่ยงต่อคณะกรรมการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการบริษัทเป็นประจำทุกไตรมาส

นอกจากนี้คณะทำงานบริหารความเสี่ยง ยังมีหน้าที่ที่ต้องดำเนินการดังต่อไปนี้

1) จัดทำคู่มือการบริหารความเสี่ยง
2) ระบุความเสี่ยงด้านต่างๆ พร้อมทั้งวิเคราะห์และประเมินความเสี่ยงที่อาจเกิดขึ้น รวมทั้งแนวโน้มซึ่งมีผลกระทบบริษัท
3) จัดทำแผนงานเพื่อป้องกันหรือลดความเสี่ยง

4) ประเมินผลและจัดทำรายงานการบริหารความเสี่ยง
5) จัดวางระบบบริหารความเสี่ยงแบบบูรณาการโดยเชื่อมโยงระบบสารสนเทศ
6) ปฏิบัติงานอื่นๆตามที่คณะกรรมการตรวจสอบเห็นสมควร

หน้าที่ความรับผิดชอบของคณะผู้ปฏิบัติงาน

คณะผู้ปฏิบัติงาน ซึ่งได้แก่ ผู้จัดการฝ่ายและพนักงานในองค์กรทุกคน จะเป็นผู้รับแนวทางการจัดการความเสี่ยงไปจัดทำแผนรองรับความเสี่ยงที่เกี่ยวข้อง ดำเนินการและรายงานผลการดำเนินการตามแผนให้แก่เลขานุการคณะทำงานบริหารความเสี่ยงตามกำหนดเวลา ภายใต้การกำกับดูแลของคณะทำงานบริหารความเสี่ยง ซึ่งแต่ละฝ่ายจะต้องดำเนินการดังต่อไปนี้

1) ระบุความเสี่ยงด้านต่างๆ พร้อมทั้งวิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้น รวมทั้งแนวโน้มซึ่งมีผลกระทบต่อบริษัท
2) จัดทำแผนเพื่อป้องกัน หรือ ลดความเสี่ยง
3) ประเมินผลและจัดทำรายงานการบริหารความเสี่ยงของแผนก
4) จัดวางระบบบริหารความเสี่ยงเชื่อมโยงกับระบบสารสนเทศ
5) ปฏิบัติงานอื่นๆตามที่คณะทำงานบริหารความเสี่ยงมอบหมาย

หน้าที่ความรับผิดชอบของคณะกรรมการตรวจสอบ (Audit Committee)

คณะกรรมการตรวจสอบ (Audit Committee) สอบทานให้บริษัทมีระบบบริหารความเสี่ยงที่เหมาะสมและมีประสิทธิผล กำกับดูแลและติดตามการบริหารความเสี่ยงอย่างเป็นอิสระ ตลอดจนสื่อสารกับคณะทำงานบริหารความเสี่ยง เพื่อให้เข้าใจความเสี่ยงที่สำคัญและเชื่อมโยงกับการควบคุมภายใน รายงานต่อคณะกรรมการบริษัทเกี่ยวกับความเสี่ยงและการจัดการความเสี่ยง

หน้าที่ความรับผิดชอบของฝ่ายตรวจสอบภายใน

ฝ่ายตรวจสอบภายใน สอบทานและประเมินประสิทธิผลของกระบวนการบริหารความเสี่ยง และใช้เป็นข้อมูลในการวางแผนการตรวจสอบของฝ่ายตรวจสอบภายใน

องค์ประกอบการบริหารความเสี่ยง

บริษัทได้นำองค์ประกอบระบบการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management Integrated Framework) ของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) มาใช้เป็นแนวทางในการบริหารความเสี่ยง ซึ่งมีองค์ประกอบการบริหารความเสี่ยง ดังนี้

1) กำหนดวัตถุประสงค์ (Objective Setting)
2) การระบุความเสี่ยง (Risk Identification)
3) การประเมินความเสี่ยง (Risk Assessment)
4) การจัดทำแผนจัดการความเสี่ยง (Risk Response)
5) กิจกรรมการควบคุม (Control Activities)
6) ติดตามและประเมินผล (Monitoring & Evaluation)

จากองค์ประกอบกระบวนการบริหารความเสี่ยงตามแนวทางของ COSO ข้างต้น มีกระบวนการที่ทุกหน่วยงานต้องดำเนินการอย่างต่อเนื่อง 6 ขั้นตอน เรียกว่า "กระบวนการการบริหารความเสี่ยง"

นอกจากนี้อีก 2 ข้อ คือ สภาพแวดล้อมภายในองค์กร และ สารสนเทศและการสื่อสาร เป็นองค์ประกอบที่เสริมให้กระบวนการบริหารความเสี่ยงทั้ง 6 ขั้นตอน มีประสิทธิภาพ และเพิ่มโอกาสให้การบริหารความเสี่ยงบรรลุวัตถุประสงค์

<u>สภาพแวดล้อมภายในองค์กร (Internal Environment)</u>

บริษัทจะจัดให้มีสภาพแวดล้อมและบรรยากาศที่เอื้ออำนวย ซึ่งเป็นพื้นฐานสำหรับขั้นตอนอื่นๆในการบริหารความเสี่ยงในองค์กร หากไม่มีสภาพแวดล้อมภายในองค์กรที่ดี จะมีผลต่อการการกำหนดกลยุทธ์และเป้าหมายของบริษัท การกำหนดกิจกรรมการบ่งชี้การประเมินและการจัดการกับความเสี่ยง องค์ประกอบที่สำคัญต่อสภาพแวดล้อม ประกอบด้วย

1) ปรัชญา ความเชื่อ วัฒนธรรมในการบริหารความเสี่ยง เพื่อสร้างมูลค่าให้กับบริษัทในระยะยาว
2) บทบาทของคณะกรรมการตรวจสอบเป็นปัจจัยสำคัญในการกำกับดูแลการบริหารความเสี่ยง

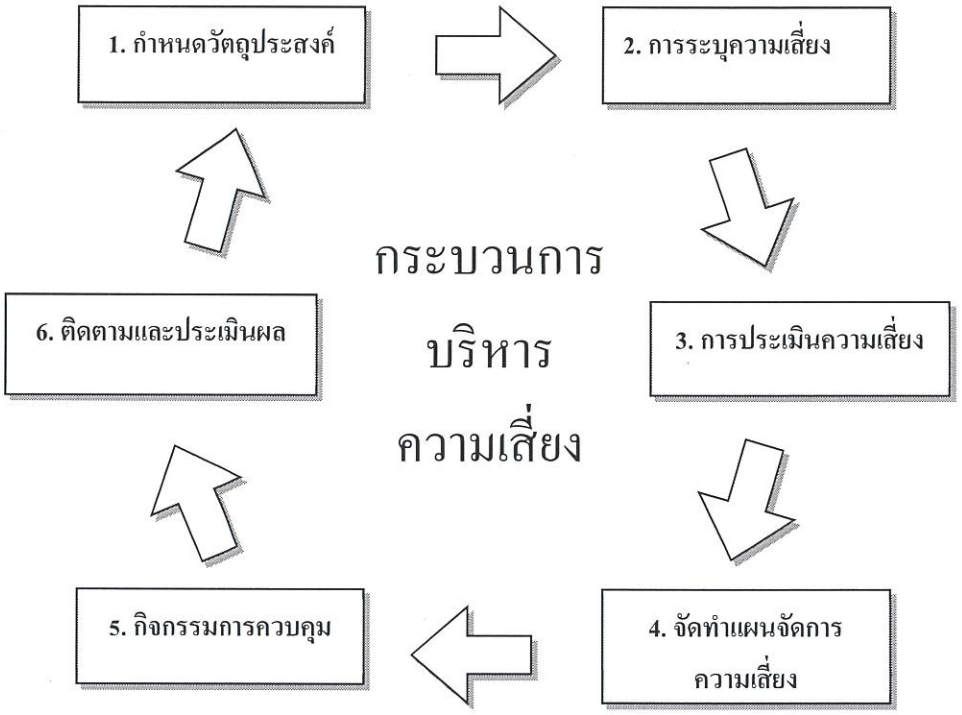
3) คัดเลือกบุคลากรที่มีความรู้ความสามารถ ความซื่อสัตย์ และพัฒนาให้เหมาะสมกับงานที่รับผิดชอบ
4) จัดให้มีโครงสร้างองค์กรที่เหมาะสม
5) การกำหนดอำนาจหน้าที่ที่เหมาะสมให้พนักงานสามารถปฏิบัติหน้าที่ให้บรรลุวัตถุประสงค์ของบริษัท

สารสนเทศและการสื่อสาร (Information & Communication)

1) ต้องมีการสื่อสารที่ชัดเจนจากคณะกรรมการบริษัทและผู้บริหารระดับสูงเกี่ยวกับนโยบายการบริหารความเสี่ยง และให้พนักงานทุกคนได้เข้าใจบทบาทหน้าที่ของตนในการบริหารความเสี่ยง เพื่อปรับเปลี่ยนพฤติกรรมและกิจกรรมที่ต้องดำเนินการ โดยคาดหวังให้ความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้
2) ต้องมีการระบุแหล่งที่มาและรวบรวมสารสนเทศทั้งจากภายในและภายนอกองค์กร จัดเก็บและสื่อสารในรูปแบบที่กำหนดและภายในระยะเวลาที่กำหนด เพื่อให้ผู้บริหารและพนักงานสามารถรับรู้ทันต่อเหตุการณ์ ปฏิบัติหน้าที่และติดต่อสื่อสารทางด้านการบริหารความเสี่ยงอย่างสม่ำเสมอและมีประสิทธิภาพ

<u>แนวทางการบริหารความเสี่ยง</u> :

ตามแนวทางของ COSO <u>กระบวนการบริหารความเสี่ยง</u>ของบริษัท ประกอบด้วย 6 ขั้นตอน ดังนี้



ขั้นตอนที่ 1. การกำหนดวัตถุประสงค์ (Objective Setting)

ขั้นตอนที่ 2. การระบุความเสี่ยง (Risk Identification)

ขั้นตอนที่ 3. การประเมินความเสี่ยง (Risk Assessment)

ขั้นตอนที่ 4. การจัดทำแผนการจัดการความเสี่ยง (Risk Response)

ขั้นตอนที่ 5. กิจกรรมการควบคุม (Control Activities)

ขั้นตอนที่ 6. การติดตามและประเมินผล (Monitoring & Evaluation)

ขั้นตอนที่ 1 การกำหนดวัตถุประสงค์ (Objective Setting)

เพื่อให้ทราบขอบเขตการดำเนินงานในแต่ระดับ และสามารถวิเคราะห์ความเสี่ยงที่คาดว่าจะเกิดขึ้นได้อย่างครบถ้วน ดังนั้น การกำหนดวัตถุประสงค์ในการบริหารความเสี่ยงที่ดีของระดับหน่วยงาน และเพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าหมาย มีดังนี้

1. จะต้องมีความชัดเจน สามารถวัดได้ สามารถปฏิบัติได้ มีเหตุผล และมีกรอบระยะเวลาที่จะดำเนินการได้แล้วเสร็จ ซึ่งเป็นไปตามหลักการ “SMART” ซึ่งย่อมาจาก

   - Specific: เฉพาะเจาะจง / ชัดเจน
   - Measurable: สามารถวัดได้
   - Achievable: สามารถบรรลุผลได้ / ปฏิบัติได้
   - Reasonable: เป็นจริงได้ / สมเหตุสมผล
   - Time constrained: มีกำหนดเวลา / กรอบเวลา

2. จะต้องมีการเชื่อมโยงกับเป้าหมายและสอดคล้องกับวัตถุประสงค์ของบริษัท หรือตัวชี้วัดของหน่วยงาน และสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับของความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance)

Risk Appetite หมายถึง ประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่บริษัทยอมรับได้ เพื่อช่วยให้บริษัทบรรลุวิสัยทัศน์และภารกิจของบริษัท

Risk Tolerance หมายถึง ระดับความเบี่ยงเบนจากประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่ยอมรับได้

ขั้นตอนที่ 2 การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยง เป็นการค้นหาว่ามีความเสี่ยงใดที่มีโอกาสเกิดขึ้นและทำให้หน่วยงานและองค์กรไม่บรรลุวัตถุประสงค์ซึ่งการระบุความเสี่ยงมีขั้นตอน ดังนี้

1. พิจารณาจาก กิจกรรม โครงการ กระบวนการทำงานที่เกี่ยวข้อง ตามแผนงานต่างๆของบริษัท เช่น แผนปฏิบัติการประจำปีและแผนธุรกิจประจำปีและอื่นๆเป็นต้น ที่ทำให้ไม่สามารถบรรลุวัตถุประสงค์และเป้ามาย

2. ระบุความเสี่ยงหรือค้นหาความเสี่ยงและสาเหตุ โดยพิจารณาแหล่งที่มาของความเสี่ยงทั้งปัจจัยภายในและปัจจัยภายนอกที่มีผลทำให้การดำเนินงานของแต่ละกิจกรรม โครงการ กระบวนการทำงาน ไม่บรรลุวัตถุประสงค์และเป้าหมาย

<u>วิธีการระบุความเสี่ยงที่สำคัญ</u> มีดังนี้

1. วิเคราะห์ทางเดินของงานและเอกสาร หรือวิเคราะห์กระบวนการ
2. การระดมสมอง
3. จัดประชุมเชิงปฏิบัติการ
4. การเก็บข้อมูลประวัติเหตุการณ์ความเสียหายที่เกิดขึ้น

<u>แหล่งที่มาของความเสี่ยงจากปัจจัยภายใน</u> อาจมาจากปัจจัยต่างๆ ดังนี้

1. วัตถุประสงค์ของบริษัท
2. นโยบายและกลยุทธ์
3. การดำเนินงาน กระบวนการทำงาน
4. โครงสร้างองค์กรและระบบการบริหารงาน
5. การเงิน

<u>แหล่งที่มาของความเสี่ยงจากปัจจัยภายนอก</u> อาจมาจากปัจจัยต่างๆ ดังนี้

1. นโยบายของรัฐบาล
2. สภาวะเศรษฐกิจ
3. การแข่งขัน (คู่แข่งขันทางการดำเนินธุรกิจ)
4. กฎระเบียบ

5. เหตุการณ์ธรรมชาติ
6. อื่นๆ

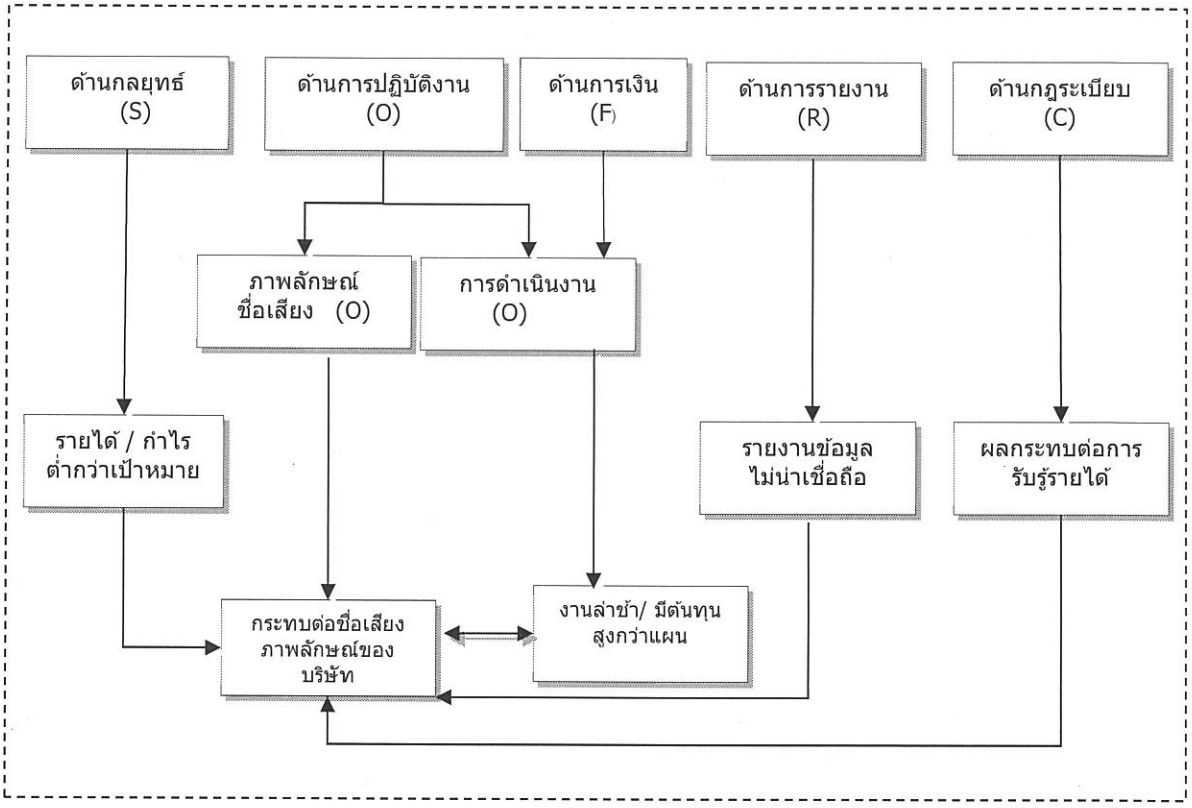
3. การจัดประเภทความเสี่ยง ดังต่อไปนี้

3.1 <u>ความเสี่ยงในการดำเนินธุรกิจของบริษัท</u>สามารถแบ่งเป็น 5 ประเภท ดังนี้

1) **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: S)** หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมาย กลยุทธ์ โครงสร้างองค์กร ภาวะการณ์แข่งขัน
2) **ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk: O)** หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงานทุกๆขั้นตอน โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ อุปกรณ์เทคโนโลยี และบุคลากรในการปฏิบัติงาน
3) **ความเสี่ยงด้านการเงิน (Financial Risk: F)** หมายถึง ความเสี่ยงที่เกิดจากการจัดการด้านงบประมาณ ซึ่งส่งผลกระทบต่อสถานะทางการเงินขององค์กร
4) **ความเสี่ยงด้านการรายงาน (Report Risk: R)** หมายถึง ความเสี่ยงเกี่ยวกับการเก็บรักษา การใช้ และการรายงานข้อมูลต่างๆ ให้มีความถูกต้องชัดเจน สร้างความน่าเชื่อถือ รวมถึงความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล (Cyber & Data Security) และการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance) ตัวอย่างความเสี่ยง เช่น การรายงานผลประกอบการของบริษัท เป็นต้น
5) **ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบต่างๆ (Compliance Risk: C)** หมายถึง ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบกฎหมายที่เกี่ยวข้องได้ หรือกฎระเบียบกฎหมายที่มีอยู่ไม่เหมาะสม หรือเป็นอุปสรรคในการปฏิบัติงาน

การจัดประเภทความเสี่ยงให้เป็นหมวดหมู่ จะแสดงให้เห็นความสัมพันธ์ของความเสี่ยงแต่ละประเภทแต่ละเรื่องได้อย่างชัดเจน เพื่อให้สามารถบริหารจัดการความเสี่ยงที่เป็นต้นเหตุของความเสียหายอย่างแท้จริง โดยสามารถแสดงให้เห็นได้จากการจัดทำแผนที่ความเสี่ยง (Risk Map)

การจัดทำแผนที่ความเสี่ยงในการดำเนินธุรกิจ (Key Risk Map) ตามประเภทของความเสี่ยง



3.2 <u>ความเสี่ยงด้านความยั่งยืน (ESG Risk)</u> มุ่งเน้น 3 ด้านดังนี้

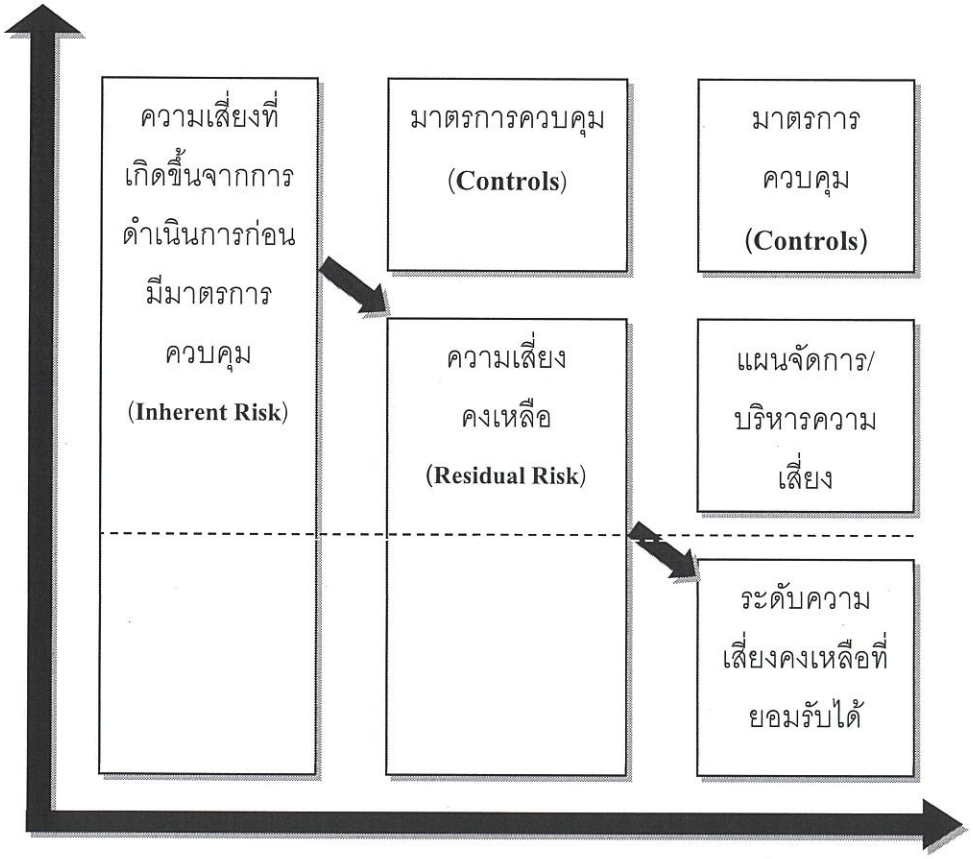
1) **ด้านสิ่งแวดล้อม (Environment) :** ประเด็นด้านสิ่งแวดล้อมที่บริษัทให้ความสำคัญได้แก่ การปล่อยก๊าซเรือนกระจก การจัดการพลังงาน การจัดการของเสียและวัตถุอันตราย และความเสี่ยงด้านสภาพภูมิอากาศ

2) ด้านสังคม (Social): ประเด็นด้านสังคมที่บริษัทให้ความสำคัญได้แก่ สิทธิมนุษยชน และการดูแลด้านอาชีวอนามัยและความปลอดภัย

3) ด้านบรรษัทภิบาล (Governance): ประเด็นด้านบรรษัทภิบาลที่บริษัทให้ความสำคัญได้แก่ ความยึดมั่นในคุณธรรม (Integrity) ความโปร่งใส ตรวจสอบได้ (Transparency) การป้องกันการทุจริตคอร์รัปชัน (Anti-Corruption) ความรับผิดชอบต่อผู้มีส่วนได้ส่วนเสีย และร่วมรับผิดชอบ (Responsibility & Accountability)

การระบุความเสี่ยง ESG โดยใช้เครื่องมือการบริหารความเสี่ยงขององค์กร อาทิ การตอบแบบสอบถาม การจัดประชุม การสัมภาษณ์ผู้บริหารเพื่อทำความเข้าใจกับความเสี่ยงที่อาจมีอยู่เดิม และความเสี่ยงที่คาดว่าจะเกิดขึ้นใหม่ (Emerging Risk) และกำหนดความหมายและของเขตความเสี่ยงให้ชัดเจน

ขั้นตอนที่ 3 การประเมินความเสี่ยง (Risk Assessment)



การประเมินความเสี่ยง หมายถึง การวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยงที่ได้จากขั้นตอนที่ 2 (การระบุความเสี่ยง) มาประเมินความเสี่ยงโดยมีขั้นตอน ดังนี้

1. พิจารณาความเสี่ยงที่เกิดขึ้นจากการดำเนินการก่อนมีมาตรการการควบคุมความเสี่ยงที่ได้จากการระบุความเสี่ยงในขั้นตอนที่ 2 โดยพิจารณาระดับความรุนแรงของความเสี่ยง และ โอกาสที่อาจจะเกิดขึ้นก่อนมีมาตรการควบคุม (Inherent Risk)

2. ระบุมาตรการควบคุมที่มีอยู่ (Controls) เพื่อควบคุม/ลดความเสี่ยงของแต่ละสาเหตุความเสี่ยง

3. ประเมินความเสี่ยงที่เหลืออยู่หลังจากมีมาตรการควบคุม (Residual Risk) โดยวิเคราะห์หาโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) ตามเกณฑ์ในการพิจารณาหาระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) ซึ่งสามารถพิจารณาได้ทั้งเชิงคุณภาพและเชิงปริมาณ โดยบริษัทกำหนดเกณฑ์ในการประเมินไว้ 5 ระดับ

   “ระดับความเสี่ยง” เท่ากับ ผลคูณของ โอกาสที่จะเกิดความเสี่ยง (Likelihood) กับ ระดับความรุนแรงของผลกระทบ (Impact)

4. นำ “ระดับความเสี่ยง “ที่ได้ประเมินแล้วตามข้อ 3. มาจัดลำดับโดยระดับความสำคัญของความเสี่ยงมีทั้งหมด 4 ระดับ ดังนี้

   - ระดับ 1. **E: Extremely Risk** ความเสี่ยงสูงมาก ซึ่งต้องบริหารความเสี่ยงทันที ผู้บริหารต้องติดตามอย่างใกล้ชิด (ระดับ 16-25 คะแนน)
   - ระดับ 2. **H: High Risk** ความเสี่ยงสูงระดับที่มีนัยสำคัญ ซึ่งต้องบริหารความเสี่ยงโดยผู้บริหารต้องให้ความสนใจเฝ้าระวัง (ระดับ 10-15 คะแนน)
   - ระดับ 3. **M: Moderate Risk** ความเสี่ยงระดับปานกลาง ซึ่งต้องกำหนดความรับผิดชอบในการบริหารความเสี่ยง (ระดับ 4-9 คะแนน)
   - ระดับ 4. **L: Low Risk** ความเสี่ยงระดับต่ำ ซึ่งบริหารความเสี่ยงด้วยวิธีปกติ (ระดับ 1-3 คะแนน)

การประเมินความเสี่ยงต้องดำเนินการทั้งก่อนการจัดทำแผนจัดการ/บริหารความเสี่ยง และหลังจากที่ได้ดำเนินการตามแผนจัดการ/บริหารความเสี่ยงแล้ว ซึ่งจะทำให้ทราบว่าแผนจัดการ/บริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผลเพียงใด ควรทบทวนหรือปรับปรุงแผนจัดการ/บริหารความเสี่ยงหรือไม่

ตารางจัดลำดับความเสี่ยง (Risk Matrix) และระดับความเสี่ยงที่ยอมรับได้

"คณะทำงานบริหารความเสี่ยง กำหนดระดับความเสี่ยงที่ยอมรับได้ไว้ที่ระดับความเสี่ยง**ไม่เกิน 9 คะแนน**"

ระดับความเสี่ยงและผลกระทบ

ระดับ		ไม่มีนัยสำคัญ	น้อย	ปานกลาง	มาก	ร้ายแรงมาก
		Insignificant	Minor	Moderate	Major	Catastrophic
ความน่าจะเกิด		1	2	3	4	5
บ่อยครั้ง	5	5	10	15	20	25
บ่อย	4	4	8	12	16	20
ปานกลาง	3	3	6	9	12	15
นานๆครั้ง	2	2	4	6	8	10
ต่ำมาก	1	1	2	3	4	5

ขั้นตอนที่ 4 การจัดทำแผนการจัดการความเสี่ยง (Risk Response)

การจัดทำแผนการจัดการความเสี่ยง หมายถึง การกำหนดแนวทางการดำเนินงาน เพื่อลดโอกาสที่จะเกิดความสูญเสีย โดยนำผลจากการประเมินความเสี่ยงที่ได้จากขั้นตอนที่ 3 มาจัดทำแผนจัดการ/บริหารความเสี่ยงตามลำดับความสำคัญของความเสี่ยง โดยหน่วยงานเจ้าของความเสี่ยง ซึ่งเข้าใจความเสี่ยงที่เกี่ยวข้องกับหน่วยงานตนเองมากที่สุดเป็นผู้จัดทำแผนจัดการ/บริหารความเสี่ยง โดยวิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น วิธีการใดวิธีการหนึ่งหรือหลายวิธีรวมกันเพื่อลดโอกาสที่จะเกิดขึ้น และ/หรือลดความรุนแรงของผลกระทบให้อยู่ในระดับที่หน่วยงานยอมรับได้ และจัดทำเป็นแผนจัดการ/บริหารความเสี่ยงของหน่วยงานตนเอง

วิธีการจัดการความเสี่ยง

1. วิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น โดยมีแนวทางในการจัดการ/ บริหารความเสี่ยงได้ 4 วิธี (4 T) ดังนี้
   1) **การควบคุม/ลด (Treat)** คือ การควบคุมความเสี่ยงหรือหาวิธีการบริหารความเสี่ยง เช่น ใช้เทคนิควิชาการทางวิศวกรรมหรือการจัดทำแผนฉุกเฉิน หรือการปรับปรุงแก้ไขกระบวนการดำเนินงาน เป็นต้น
   2) **การโอนย้าย (Transfer)** คือ การถ่ายโอนความเสี่ยงหรือโอนย้ายความเสี่ยงให้ผู้อื่นรับผิดชอบ เช่น การทำประกันภัยหรือจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน เป็นต้น
   3) **การหลีกเลี่ยง/กำจัด (Terminate)** คือ การกำจัดความเสี่ยงหรือหลีกเลี่ยงไม่ยอมรับความเสี่ยงนั้นเลย เช่น การเปลี่ยนวัตถุประสงค์หรือหยุดทำกิจกรรม เป็นต้น
   4) **การยอมรับ (Take)** เนื่องจากองค์กรอาจมีระบบควบคุมที่มีประสิทธิภาพหรือมีเงินทุนเพียงพอที่จะรองรับผลกระทบที่อาจเกิดขึ้นหรือระดับความเสี่ยงเหลืออยู่ในระดับที่ยอมรับได้ หรือการยอมรับให้มีความเสี่ยงเนื่องจากค่าใช้จ่ายในการบริหารความเสี่ยง โดยการสร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้ แต่ควรมีมาตรการติดตามและควบคุมดูแล

   ทั้งนี้การเลือกวิธีการจัดการความเสี่ยง ต้องพิจารณาเปรียบเทียบต้นทุนในการจัดการ/บริหารความเสี่ยงและความเสียหายที่เกิดขึ้นด้วย
2. จัดทำแผนจัดการ/บริหารความเสี่ยงเพิ่มเติมโดยมีขั้นตอน ดังนี้
   1) ระบุวิธีการ มาตรการที่เป็นทางเลือกจากวิธีการจัดการความเสี่ยง (4 T) เพื่อให้ความเสี่ยงคงเหลืออยู่ในระดับที่ยอมรับได้ และสอดคล้องกับวัตถุประสงค์ที่กำหนดไว้
   2) ศึกษาเปรียบเทียบความเป็นไปได้และค่าใช้จ่ายของแต่ละทางเลือกตามข้อ 1) โดยคำนึงถึงความคุ้มค่าในการลงทุนทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน โดยต้นทุนในการดำเนินการต้องไม่สูงกว่าความเสียหายที่คาดว่าจะเกิดขึ้น
   3) เลือกวิธีการที่ดีที่สุด โดยกำหนด ผู้รับผิดชอบ / ระยะเวลา / งบประมาณ พร้อมกำหนดแผนปฏิบัติการ

4) พิจารณาความสอดคล้องกับมาตรฐานที่เกี่ยวข้องในอุตสาหกรรม ความคาดหวังของผู้มีส่วนได้เสีย รวมถึงพันธกิจ วิสัยทัศน์ และค่านิยมองค์กร

ขั้นตอนที่ 5 กิจกรรมการควบคุม (Control Activities)

กิจกรรมการควบคุม หมายถึง นโยบายและแนวทางการปฏิบัติงานในการควบคุมที่ฝ่ายบริหารกำหนดขึ้น เพื่อให้มั่นใจว่าแผนจัดการ/บริหารความเสี่ยงที่กำหนดขึ้นอย่างมีประสิทธิภาพมีการกำหนดผู้รับผิดชอบและระยะเวลาในการดำเนินงานไว้อย่างชัดเจน และกิจกรรมการควบคุมนั้นก็เป็นวิธีการหนึ่งในการจัดการ/บริหารความเสี่ยง

ตัวอย่าง กิจกรรมการควบคุม

1. การควบคุมโดยการจัดทำนโยบายและวิธีปฏิบัติงาน
2. การสอบทานและการกำกับดูแลการปฏิบัติงาน
3. ระบบงานคอมพิวเตอร์และการควบคุมด้านคอมพิวเตอร์
4. การควบคุมทางกายภาพ
5. ดัชนีตัวชี้วัดผลการดำเนินงาน
6. การแบ่งแยกหน้าที่ความรับผิดชอบงาน

กิจกรรมการควบคุมที่จะเกิดประโยชน์มากที่สุดควรจะแทรกอยู่ในกระบวนการ สามารถป้องกันและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยต้นทุนในการดำเนินงานการต้องไม่สูงกว่าความเสียหายที่คาดว่าจะเกิดขึ้น

การกำหนดกิจกรรมการควบคุมอย่างชัดเจนจะทำให้แผนการจัดการบริหารความเสี่ยงที่ได้จัดทำไว้บรรลุวัตถุประสงค์ โดยจัดทำนโยบายและวิธีปฏิบัติเพิ่มเติม กำหนดผู้รับผิดชอบและระยะเวลาแล้วเสร็จอย่างชัดเจน ในบางกรณีอาจจัดทำกระบวนการควบคุมภายในเพิ่มเติม เช่น การสอบทาน การกำกับดูแล การแบ่งแยกหน้าที่งานเพิ่ม เป็นต้น

กิจกรรมการควบคุม เป็นองค์ประกอบหนึ่งของระบบการควบคุมภายใน ในลักษณะการเสนอแนะ (Suggestive Control) เพื่อปรับปรุงและพัฒนาระบบการดำเนินงานและระบบการควบคุมภายในให้เหมาะสม

กับสถานการณ์ที่หน่วยงานต้องจัดทำให้มีขึ้น เพื่อลดความเสี่ยงและทำให้เกิดความคุ้มค่า ตลอดจนให้ฝ่ายบริหารเกิดความมั่นใจในประสิทธิผลของระบบการควบคุมภายในที่มีอยู่

ขั้นตอนที่ 6 การติดตามและประเมินผล (Monitoring & Evaluation)

การติดตามและประเมินผล หมายถึง กระบวนการควบคุมคุณภาพการปฏิบัติงานและประเมินผลแผนการจัดการ/บริหารความเสี่ยงเพิ่มเติม หรือกิจกรรมการควบคุมที่วางไว้อย่างต่อเนื่องและสม่ำเสมอ โดยการติดตามในระหว่างการปฏิบัติงานและการประเมินผลเป็นครั้งคราวตามระยะเวลา เพื่อให้มั่นใจว่าการจัดการ/การบริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผล จึงต้องมีรายงานความก้าวหน้า ปัญหา อุปสรรคของการจัดการ/บริหารความเสี่ยง เพื่อใช้เป็นแนวทางในการทบทวนหรือปรับปรุงแผนการจัดการ/บริหารความเสี่ยงต่อไป

รายงานที่ต้องจัดทำและขั้นตอนการรายงาน มีดังนี้

+ แผนบริหารความเสี่ยง ซึ่งประกอบด้วย
    1) รายงานปัจจัยความเสี่ยง ระดับความเสี่ยง
    2) การควบคุมที่มีอยู่ การจัดการความเสี่ยงที่เหลือ
    3) หน่วยงาน/ผู้รับผิดชอบ ความเสี่ยงหลังการควบคุม
+ รายงานต่อผู้บริหารระดับสูงหรือคณะกรรมการบริษัท ซึ่งประกอบด้วย
    1) ความเสี่ยงที่คลาดเคลื่อนเกินกว่าที่ยอมรับได้
    2) ความเสี่ยงสูงสุด 5 ระดับ
    3) เหตุการณ์ที่แม้จะมีโอกาสต่ำ แต่จะมีผลต่อ
        - ความปลอดภัยต่อพนักงานหรือบุคคลอื่น
        - การกระทำผิดกฎหมาย
        - ผลเสียหายสำคัญต่อทรัพย์สิน การด้อยค่าของทรัพย์สิน
        - ชื่อเสียงของหน่วยงาน
        - การจัดทำงบและรายงานทางการเงินไม่เหมาะสม

<u>แนวทางการตอบสนองต่อประเด็นความเสี่ยงด้าน ESG ของบริษัท เพื่อป้องกันและลดความเสี่ยงของ ESG Risk ที่จะเกิดขึ้น</u> บริษัทมีแนวทางการตอบสนองความเสี่ยงด้าน ESG ดังต่อไปนี้

1. <u>การบริหารจัดการคู่ค้า (Upstream)</u>

• แผนกจัดหาจะดำเนินการจัดทำ Supplier CoC (Certificate of Conformity) และ ESG Assessment Questionnaire เพื่อสร้างความโปร่งใสในการดำเนินงานของคู่ค้าในห่วงโซ่อุปทาน

2. <u>การดำเนินงานของบริษัท (Own Operation)</u>

• บริษัทมุ่งเน้นการลดการปล่อยก๊าซเรือนกระจก การจัดการของเสีย การใช้พลังงานทดแทน และการใช้ทรัพยากรอย่างมีประสิทธิภาพ

• บริษัทจัดให้มีนโยบายด้านสิทธิมนุษยชน (Human Rights Policy) ซึ่งยึดมั่นในความรับผิดชอบต่อสังคมและผู้มีส่วนได้เสียทุกกลุ่ม

• แผนกทรัพยากรบุคคลมีนโยบายที่เกี่ยวข้องกับการบริหารจัดการบุคลากรและการปฏิบัติตามกฎหมายแรงงานอย่างเคร่งครัด

• บริษัทจัดให้มีมาตรการป้องกันการทุจริตภายในองค์กร

• บริษัทจัดให้มีกรอบการกำกับดูแลกิจการที่ดี ซึ่งได้รับการอนุมัติจากคณะกรรมการบริษัท และกำหนดบทบาทหน้าที่ ความรับผิดชอบของคณะกรรมการบริษัทและผู้บริหารอย่างชัดเจน รวมถึงมีการแต่งตั้งคณะกรรมการชุดย่อยต่างๆ เพื่อช่วยกำกับดูแลและกลั่นกรองเรื่องสำคัญต่างๆ

• บริษัทกำหนดหลักจริยธรรมในการดำเนินธุรกิจ และกำหนดให้ผู้บริหารและพนักงานต้องปฏิบัติตามอย่างเคร่งครัดเพื่อให้การดำเนินธุรกิจเป็นไปอย่างโปร่งใส รวมถึงมีการเปิดเผยข้อมูลข่าวสารและผลการดำเนินงานของบริษัทให้ลูกค้าและคู่ค้าสามารถเข้าถึงได้อย่างสะดวก

บริษัทจะจัดให้มีการทบทวนนโยบายการบริหารความเสี่ยงให้สอดคล้องกับสภาวการณ์และธุรกิจของบริษัทอย่างสม่ำเสมอเป็นประจำทุกปี