การบริหารความเสี่ยง

คณะกรรมการบริษัทฯ สนับสนุนส่งเสริมให้มีระบบการบริหารความเสี่ยงภายในองค์กรซึ่ง เป็นกลไกหนึ่งที่สำคัญต่อการบรรลุวัตถุประสงค์และการเพิ่มพูนมูลค่าให้กับผู้มีส่วนได้เสีย โดยคณะกรรมการบริษัทฯ กำหนดให้ผู้บริหารและพนักงานในหน่วยงานต่างๆเป็นเจ้าของความเสี่ยง มี บทบาท หน้าที่ ความรับผิดชอบที่จะประเมินและจัดการความเสี่ยงที่รับผิดชอบให้อยู่ในระดับความเสี่ยงที่ บริษัทฯ ยอมรับได้ พร้อมทั้งส่งเสริมและกระตุ้นให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กร โดยให้ทุก คนตระหนักถึงความสำคัญของการบริหารความเสี่ยง โดยจัดให้มีกระบวนการบริหารความเสี่ยงที่มี ประสิทธิภาพในทุกขั้นตอน โดยปฏิบัติตามกรอบโครงสร้างการบริหารความเสี่ยงอ้างอิงตาม มาตรฐานสากลของ The Committee of Sponsoring Organization of the Treadway Commission (COSO) ซึ่งประกอบด้วย กรอบแนวทางระบบการควบคุมภายใน (COSO) และกรอบแนวทางการบริหาร ความเสี่ยง (Enterprise Risk Management, ERM) ตามหลักการของการกำกับดูแลกิจการที่ดี เพื่อช่วยเพิ่มโอกาสแห่งความสำเร็จโดยการใช้ทรัพยากรที่มีจำกัดอย่างมีประสิทธิภาพ และลดความ ไม่แน่นอนในผลการดำเนินงาน โดยมีกระบวนการบริหารความเสี่ยงของบริษัทฯ ประกอบด้วย 8 องค์ประกอบ ดังนี้

1. สภาพแวดล้อมภายในองค์กร (Internal Environment)

เป็นการพิจารณาขั้นตอนการวางแผนกลยุทธ์ เพื่อทำความเข้าใจหลักการ และเหตุผลในการกำหนดกลยุทธ์ของบริษัทฯ เพื่อให้การกำหนดปัจจัยเสี่ยงครอบคลุมทุกกิจกรรมที่สำคัญภายในองค์กร ซึ่งทางบริษัทฯ กำหนดกลยุทธ์โดยเริ่มจากผู้บริหารระดับสูงพิจารณากำหนดพันธกิจประจำปี ให้สอดคล้องกับวิสัยทัศน์ขององค์กร โดยการนำกลยุทธ์ไปสู่ภาคปฏิบัติ ผ่าน BSC (Balanced Scorecard) นับเป็นหน้าที่ของผู้บริหารแต่ละหน่วยงานต้องกำหนดแผนงานประจำปี และงบประมาณโดยพิจารณาจากกิจกรรมต่างๆ รวมทั้งกำหนด KPIs เพื่อใช้วัดผลความสำเร็จของทุกกิจกรรม

2. การกำหนดวัตถุประสงค์ (Objective Setting)

การกำหนดวัตถุประสงค์จะต้องมีความสอดคล้อง และเป็นไปในทิศทางเดียวกัน กล่าวคือ วัตถุประสงค์ของบริษัทฯ จะต้องสอดคล้องกับวิสัยทัศน์ พันธกิจ และทิศทางการดำเนินงานของบริษัทฯ และจะต้องมีความสอดคล้องกันตั้งแต่ระดับบริษัทฯ หน่วยงาน กิจกรรม จนถึงระดับบุคคลเพื่อให้ วัตถุประสงค์ในภาพรวมบรรลุเป้าประสงค์ ทราบขอบเขตการดำเนินงานในแต่ละระดับ และสามารถวิเคราะห์ ความเสี่ยงที่จะเกิดขึ้นได้ครบถ้วน ดังนั้นวัตถุประสงค์จะต้องแสดงให้เห็นถึงผลลัพธ์ที่บริษัทฯต้องการ จะบรรลุไม่ใช่การกล่าวถึงกระบวนการในการปฏิบัติ

3. การชี้บ่งเหตุการณ์ (Event Identification)

จัดประชุมเชิงปฏิบัติการ (Work Shop) กับบุคคลที่เกี่ยวข้องเพื่อระบุเหตุการณ์ความเสี่ยง โดยพิจารณาแจกแจงกระบวนการปฏิบัติงานที่มีผลต่อการบรรลุวัตถุประสงค์ของหน่วยงานและบริษัทฯ เพื่อระบุเหตุการณ์หรือความไม่แน่นอนที่ทำให้เกิดความผิดพลาด ล้มเหลว เสียหายหรือเสียโอกาส ซึ่งจะส่งผลต่อการบรรลุวัตถุประสงค์ของหน่วยงาน และบริษัทฯ โดยไม่ต้องพิจารณาการควบคุมที่มีอยู่ปัจจุบัน และความเป็นไปได้ของเหตุการณ์หรือความไม่แน่นอน เพื่อให้มั่นใจว่าการระบุเหตุการณ์ความเสี่ยงมีความครอบคลุมทุกกิจกรรม นำเหตุการณ์ความเสี่ยงมาพิจารณาหาความสัมพันธ์และวิเคราะห์หาต้นเหตุของความสัมพันธ์ โดยวิเคราะห์หาความสัมพันธ์ของเหตุการณ์ความเสี่ยง และพิจารณาต้นเหตุของความสัมพันธ์ เพื่อกำหนดเป็นปัจจัยเสี่ยง พร้อมทั้งระบุประเภทของความเสี่ยง (Risk Categories) ซึ่งคณะกรรมการบริหารและจัดการความเสี่ยงได้จำแนกประเภทของความเสี่ยงออกเป็น 3 ลักษณะ คือ

- Strategic Risk คือ ความเสี่ยงที่เกี่ยวข้องในระดับยุทธศาสตร์
- Operation and Compliance Risk คือ ความเสี่ยงที่เกี่ยวข้องในระดับปฏิบัติการ และ การปฏิบัติไม่ถูกต้องตามกฎหมาย
- Financial Risk คือ ความเสี่ยงที่เกี่ยวข้องกับด้านการเงิน

4. การประเมินความเสี่ยง (Risk Assessment)

หลังจากหน่วยงานค้นหาและระบุความเสี่ยงได้แล้ว ต่อไปจะเป็นการวัดระดับความเสี่ยงว่า อยู่ในระดับใด เมื่อเทียบกับความเสี่ยงที่ยอมรับได้ของบริษัทฯ ซึ่งจะทำการวัดระดับความเสี่ยง โดยธรรมชาติของปัจจัยเสี่ยงที่ไม่มีการดำเนินการใดๆ (Inherent Risk) และทำการวัดระดับความเสี่ยงอีก ครั้งภายหลังพิจารณาการควบคุมที่มีประสิทธิผลของปัจจัยเสี่ยงนั้นๆ (Residual Risk) โดยมีแนวทาง ปฏิบัติตามรายละเอียด ดังนี้

4.1 การประเมินระดับความเสี่ยง โดยนำเหตุการณ์และปัจจัยเสี่ยงที่มีการค้นพบหรือระบุในขั้นตอน ก่อนหน้านี้ มาทำการวัดหรือประเมินระดับความรุนแรง กับความถี่หรือโอกาสที่จะเป็นไปได้ เพื่อระบุ ระดับความสำคัญของความเสี่ยง

4.2 การจัดระดับความเสี่ยง เป็นการพิจารณาปัจจัยเสี่ยงที่มีหลายตัว นำมาจัดระดับความเสี่ยง เพื่อให้เกิดความชัดเจนในการพิจารณาเลือกปัจจัยเสี่ยงนำไปกำหนดแผนการจัดการความเสี่ยง เพื่อลดระดับความเสี่ยง และอยู่ในระดับความเสี่ยงที่ยอมรับได้ขององค์กร

5. กิจกรรมการควบคุม (Control Activities)

เป็นการพิจารณาประสิทธิภาพ ประสิทธิผลของจุดควบคุมภายในที่มีการกำหนดไว้เพื่อลดระดับ ความเสี่ยงให้อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ โดยจะมีการพิจารณาจุดควบคุมภายใน ภายหลังการประเมิน Inherent Risk และ ภายหลังมีการกำหนดแผนจัดการความเสี่ยง (Risk Response) ประสิทธิภาพ ประสิทธิผล ของจุดควบคุมภายใน พิจารณาจากการเลือกใช้ทรัพยากรที่มีอยู่ของหน่วยงาน ไม่ว่าจะเป็นบุคลากร งบประมาณเวลา วัสดุ อุปกรณ์ต่างๆ ที่มีอยู่ เพื่อลด ป้องกันโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง หรือลดผลกระทบหากเกิดเหตุการณ์ความเสี่ยง ซึ่งจะต้องมีต้นทุนดำเนินการคุ้มค่า หรือน้อยกว่าผลกระทบที่เกิดขึ้นหากเกิดเหตุการณ์ตามปัจจัยความเสี่ยงที่มีการระบุไว

6. การจัดการความเสี่ยง (Risk Response)

หลังจากประเมินระดับความเสี่ยง และจัดระดับความเสี่ยงซึ่งทำให้ทราบความเสี่ยงที่คงเหลืออยู่ และความเสี่ยงที่อยู่ในระดับที่สูงกว่าความเสี่ยงที่ยอมรับได้ ซึ่งผู้รับผิดชอบความเสี่ยง (Risk Owner) จะต้องพิจารณาแผนการดำเนินการ เพื่อลดโอกาสที่จะเกิด และผลกระทบที่อาจเกิดขึ้น หากเกิดเหตุการณ์ ความเสี่ยง โดยคำนึงถึงการบริหารทรัพยากรที่มีอยู่ให้เกิดประโยชน์สูงสุด โดยจะต้องคำนึงถึงลักษณะของความเสี่ยง ระดับของความเสี่ยงและต้นทุนหรือทรัพยากรที่ต้องใช้ในทางเลือกนั้นๆ เปรียบเทียบกับผลที่คาดว่าจะได้รับ ซึ่งคณะกรรมการบริหารและจัดการความเสี่ยงได้มีการก าหนดให้เจ้าของความเสี่ยง (Risk Owner) ของแต่ละหน่วยงานระบุ KRI (Key Risk Indicator) และ KPI (Key Performance Indicator) เพื่อวัดผลสำเร็จของแผนบริหารความเสี่ยง (Action Plan) โดยมีทางเลือกที่จะจัดการกับความเสี่ยงอยู่ด้วยกัน 4 วิธี ดังนี้

6.1 การหลีกเลี่ยง (Avoid) เป็นการหลีกเลี่ยงความเสี่ยงที่อยู่ในระดับสูงมากหรือหน่วยงาน ไม่อาจยอมรับความเสี่ยงได้ ซึ่งมีผลกระทบกับองค์กร งานโครงการ กิจกรรม หรือกระบวนการอย่างสูง แต่ไม่สามารถจัดการด้วยวิธีอย่างหนึ่งอย่างใดได้ จึงต้องจัดการความเสี่ยงนั้นด้วยการหยุดดำเนินการยกเลิกโครงการลดเนื้องานของโครงการ หรือลดกิจกรรมที่กำหนดไว้ตามโครงการ เป็นต้น

6.2 การร่วมจัดการ (Share) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้หน่วยงานอื่น ทั้งภายในและภายนอกองค์กร โดยเฉพาะเป็นกรณีที่เห็นว่าเป็นความเสี่ยงที่คาดไม่ถึงหรือป้องกันได้ยาก หรือมีระดับความรุนแรงสูง เช่น ภัยธรรมชาติ หรือวินาศภัยต่างๆ ซึ่งหน่วยงานไม่สามารถแบกรับความเสี่ยงนั้นได้ ก็อาจจะกระจายหรือถ่ายโอนความเสี่ยงด้วยการทำประกันภัย หรือกรณีความเสี่ยงที่อาจเกิดขึ้นจากความไม่ชำนาญงานของบุคลากรภายในหน่วยงาน ก็อาจจัดจ้างที่ปรึกษา เป็นต้น

6.3 การลด (Reduce) เป็นการลดหรือควบคุมความเสี่ยงในกรณีที่หน่วยงานเห็นว่าความเสี่ยงเหล่านั้น เกิดจากปัจจัยภายในหรือสาเหตุที่หน่วยงานสามารถลดหรือควบคุมได้ด้วยวิธีการควบคุมภายในหรือปรับปรุงระบบการทำงาน โดยออกแบบวิธีการทำงานใหม่เพื่อลดโอกาสที่จะเกิดความเสียหายหรือผลกระทบให้อยู่ในระดับที่หน่วยงานยอมรับได้ เช่น การจัดอบรมให้บุคลากร การจัดหาคู่มือ การปฏิบัติงาน เพื่อลดความเสี่ยงจากการทำงานผิดพลาดหรือหากเป็นความเสี่ยงที่เกิดจาก ปัจจัยภายนอก ก็อาจนำกลยุทธ์หรือมาตรการต่างๆ มาใช้เพื่อลดผลกระทบหรือความรุนแรง ของความเสี่ยง

6.4 การยอมรับ (Accept) เป็นความเสี่ยงที่หน่วยงานยอมรับได้ หรือเป็นความเสี่ยงที่อยู่ในระดับความเสี่ยงต่ำ หรือเป็นความเสี่ยงที่มีต้นทุนในการจัดการความเสี่ยงสูงมากจนไม่คุ้มค่ากับผลที่จะได้รับ หรือเป็นความเสี่ยงที่อยู่นอกเหนือการควบคุมขององค์กร หรืออาจมีสาเหตุจากปัจจัยภายนอกที่ไม่สามารถควบคุมได้ แต่บริษัทฯ มีความจำเป็นต้องดำเนินการเพื่อให้บรรลุเป้าหมาย เช่น นโยบายของรัฐบาล กฎหมาย เป็นต้น

7. การติดตามผล (Monitoring)

เป็นการติดตามประเมินผลแผนการจัดการความเสี่ยง ตามที่ผู้รับผิดชอบความเสี่ยง มีการกำหนดไว้ โดยวิเคราะห์และประเมินผลการบริหารจัดการความเสี่ยงว่ามีประสิทธิผลหรือไม่ หากหน่วยงานได้ดำเนินการตามแผนบริหารความเสี่ยงแล้วยังมีความเสี่ยงที่ไม่อาจยอมรับได้เหลืออยู่ ควรพิจารณาต่อไปว่าเป็นความเสี่ยงที่อยู่ในระดับใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไร จากนั้นจึงเสนอต่อคณะกรรมการบริหารและจัดการความเสี่ยงพิจารณาให้ความเห็นรวมถึงการจัดสรรงบประมาณสนับสนุน

8. สารสนเทศและการสื่อสาร (Information & Communication)

การบริหารความเสี่ยงเชิงบูรณาการจะเกิดขึ้นได้และมีการถือปฏิบัติอย่างต่อเนื่อง จะต้องได้รับ การสนับสนุนจากผู้บริหารสูงสุดของบริษัทฯ และได้รับความร่วมมือจากบุคลากรทุกคนภายในองค์กร ดังนั้นการให้ทุกคนภายในองค์กรมีความเข้าใจและรับทราบบทบาทของตนเอง ต่อระบบบริหารความเสี่ยงเชิงบูรณาการของบริษัทฯ ได้อย่างครบถ้วน จะต้องมีการวางระบบสารสนเทศ และการสื่อสารที่มีประสิทธิผล ทั้งในส่วนการประชาสัมพันธ์ การฝึกอบรมความรู้ รวมทั้งการติดตามให้มีการดำเนินการอย่างต่อเนื่อง ซึ่งปัจจุบันบริษัทฯ มีการสื่อสารผ่านการประชุมคณะกรรมการบริหารและจัดการความเสี่ยง โดยเชิญผู้รับผิดชอบความเสี่ยง (Risk Owner) รายงานสถานการณ์ที่เกิดขึ้นจริง หลังจากมีการจัดทำกำหนดแผนการบริหารความเสี่ยงของหน่วยงานที่ตนรับผิดชอบ

Risk Management

The Board of Directors promotes and supports the implementation of an internal risk management system, which is a critical mechanism for achieving organizational objectives and enhancing value for all stakeholders. The Board of Directors requires executives and employees across all departments to act as "Risk Owners," with the roles, duties, and responsibilities to assess and manage risks within their respective areas to stay within the company's risk appetite. Furthermore, the Board fosters and encourages risk management as part of the corporate culture, ensuring that everyone recognizes its importance. The company establishes an efficient risk management process at every stage, adhering to the international risk management framework of The Committee of Sponsoring Organizations of the Treadway Commission (COSO). This includes the COSO Internal Control Framework and the Enterprise Risk Management (ERM) framework, based on good corporate governance principles. These frameworks aim to increase the likelihood of success through the efficient use of limited resources and to reduce uncertainty in operational performance. The Company's risk management process consists of the following 8 components:

1. Internal Environment

This process is designed to ensure a thorough understanding of the principles and rationales behind the Company's strategy formulation. It ensures that the identification of risk factors covers all critical activities across the organization. The Company's strategic formulation begins with Senior Management establishing the Annual Mission, aligning it with the corporate Vision. To translate strategy into practice, the Balanced Scorecard (BSC) framework is utilized. It is the responsibility of the management in each department to develop Annual Work Plans and budgets based on their respective activities. This includes defining Key Performance Indicators (KPIs) to measure the success and effectiveness of all operational activities.

2. Objective Setting

Objective Setting must be consistent and aligned throughout the organization. In other words, the Company's objectives must align with its Vision, Mission, and overall Strategic Direction. This alignment must flow from the corporate level down to departments, specific activities, and individual levels. This ensures that the overall goals are achieved, the operational scope at each level is clearly defined, and potential risks can be comprehensively analyzed. Furthermore, objectives must clearly demonstrate the desired outcomes the Company intends to achieve, rather than merely describing the operational processes or procedures.

3. Event Identification

Risk Identification Workshops are conducted with relevant stakeholders to identify potential risk events. This involves a detailed breakdown of operational processes that impact the achievement of both departmental and corporate objectives. The goal is to identify events or uncertainties that could lead to errors, failures, damages, or missed opportunities, all of which could hinder the company's success. At this stage, risks are identified without considering existing internal controls or the current likelihood of occurrence, ensuring that the identification process comprehensively covers all activities. These risk events are then analyzed to determine their interrelationships and to identify the root causes behind them. This analysis allows for the formal definition of "Risk Factors" and the categorization of risks into specific Risk Categories. The Risk Management Committee has classified these risks into three distinct characteristics:

- Strategic Risk: Risks related to the strategic level.
- Operation and Compliance Risk: Risks related to the operational level and legal non-compliance.
- Financial Risk: Risks related to the financial aspect.

4. Risk Assessment

Once the department has identified the risks, the next step is to measure the risk level against the Company's risk appetite. This involves measuring the Inherent Risk (the natural state of risk factors without any intervention) and re-measuring the Residual Risk (the remaining risk level after considering the effectiveness of existing controls). The guidelines are as follows:

4.1 Risk Assessment: The events and risk factors identified in the previous step are measured or assessed based on their Impact (severity) and Likelihood (frequency) to determine the risk significance level.

4.2 Risk Ranking: This involves prioritizing multiple risk factors to provide clarity in selecting which risks should be addressed through a risk management plan. This ensures risk levels are reduced and maintained within the organization's risk appetite.

5. Control Activities

This is a consideration of the efficiency and effectiveness of the internal control points established to reduce risk to the organization's risk appetite level. Internal control points are evaluated after the Inherent Risk assessment and after the Risk Response plan has been defined. The efficiency and effectiveness of these internal control points are determined by the utilization of the department's existing resources-including personnel, budget, time, materials, and equipment—to reduce or prevent the likelihood of risk events or to mitigate their impact. The cost of implementation must be cost-effective or less than the potential impact of the identified risk factors.

6. Risk Response

After assessing and ranking risks to identify Residual Risk and any risks exceeding the Risk Appetite, the Risk Owner must develop an action plan to reduce the likelihood and potential impact of such events. This planning must optimize existing resources, considering the nature of the risk, the risk level, and the cost or resources required for each option compared to the expected benefits. The Risk Management Committee requires each Risk Owner to define Key Risk Indicators (KRI) and Key Performance Indicators (KPI) to measure the success of the Action Plan. There are 4 options for managing risk:

6.1 **Avoid:** Avoiding risks that are at a very high level or are unacceptable to the department, significantly impacting the organization, projects, or processes. When such risks cannot be managed by other means, they must be addressed by ceasing operations, canceling projects, or reducing the scope of work or activities.

6.2 **Share:** Distributing or transferring risk to other internal or external parties. This applies to unforeseen, difficult-to-prevent, or high-severity risks, such as natural disasters or accidents. Methods include taking out insurance or hiring consultants in cases where risks arise from a lack of internal expertise.

6.3 **Reduce:** Reducing or controlling risks identified as stemming from internal factors or causes that the department can influence through internal controls or process improvements. New workflows are designed to minimize the likelihood of damage or impact to an acceptable level, such as providing staff training or operating manuals to reduce errors. For risks from external factors, specific strategies or measures may be applied to mitigate the severity.

6.4 **Accept:** Accepting risks that are within the acceptable level, are at a low level, or where the cost of management far outweighs the benefits. This also applies to risks beyond the organization's control or caused by uncontrollable external factors, yet the company must proceed to achieve its goals, such as compliance with government policies or laws.

7. Monitoring

This involves monitoring and evaluating the risk management plans as defined by the Risk Owners. The process analyzes and assesses whether the risk management actions have been effective. If, after implementing the risk management plan, unacceptable risks still remain, further consideration must be given to the risk level and the appropriate management methods. Subsequently, these findings are proposed to the Risk Management Committee for their review and opinion, including the allocation of supporting budgets.

8. Information & Communication

Integrated risk management can only be achieved and sustained through the support of the Company's top management and the cooperation of all personnel within the organization. Therefore, to ensure that everyone thoroughly understands and recognizes their roles in the Company's integrated risk management system, effective information and communication systems must be established. This includes public relations, knowledge training, and consistent follow-up on implementation.