1.4 Risk and Crisis Management

Risk Management

To ensure effective organizational risk management, EGAT has established a risk management and internal control policy, along with implementation guidelines on good governance, risk management, and compliance (GRC). The risk management structure includes the EGAT Board of Directors, the Risk Management and Internal Control Committee, the EGAT Executive Committee, risk management committees at operational line level, the Audit Committee under the Office of Internal Audit, and all EGAT personnel. The Risk Management and Internal Control Department, under the Strategic Planning Division, supports enterprise-wide risk management by formulating policies, setting acceptable risk levels, developing risk management guidelines, and preparing an annual risk management manual and review.

Under EGAT's Governance, Risk Management, and Compliance (GRC) framework, risk management responsibilities are structured according to the Three Lines of Defense model. The **1st Line of Defense ("Owner")**, comprising business and functional units, is responsible for identifying, owning, assessing, and managing risks within their respective operations. The **2nd Line of Defense ("Oversee")** consists of dedicated oversight functions and committees at the management level that establish risk management and internal control standards, provide guidance, monitor compliance, and oversee the effectiveness of risk management practices across the organization. The **3rd Line of Defense ("Independent Assurer")**, represented by the internal audit function, provides independent assurance regarding the adequacy and effectiveness of risk management, internal control, and compliance processes.

In addition, EGAT integrates risk considerations into the development of power plant projects, which are the organization's core business activities. As part of the project development

process, stakeholder engagement activities and public consultation forums are conducted to gather perspectives, concerns, and recommendations from relevant stakeholders. Feedback received through these engagement processes is incorporated into the project risk assessment process and is used to support the identification, evaluation, and management of project-related risks. This approach helps ensure that risk management measures are comprehensive, appropriate, and responsive to stakeholder expectations throughout the project development lifecycle.

To strengthen risk governance capabilities across the organization, EGAT regularly promotes risk management knowledge and competency development among directors and executives. In 2024, the Board of Directors received training on **ESG Risk Management and Energy Transition**, while executives participated in training programs on **Governance, Risk Management and Compliance (GRC)** and **Enterprise Risk Management: Sustainability and Growth**, enhancing their understanding of emerging risks, sustainability-related challenges, and enterprise risk management practices.

Furthermore, EGAT's risk management process is subject to external assessment under the **State Enterprise Assessment Model (SE-AM)** conducted annually by the **State Enterprise Policy Office (SEPO)**. The assessment is used to evaluate the appropriateness and effectiveness of EGAT's enterprise risk management framework. The SE-AM framework is developed based on internationally recognized standards and best practices relating to governance, risk management, and internal control, including **COSO 2017, COBIT, ISO 31000:2018, and COSO 2013**, supporting EGAT's alignment with good corporate governance principles and internationally accepted risk management practices. Additionally, EGAT's risk management process is internally audited by the Audit Committee and the Internal Audit Office who are responsible for conducting independent reviews on an annual basis to ensure that the organization's risk management system is adequate, effective, and efficient.

EGAT also reviews its risk exposure and risk management performance on a regular basis to ensure that risk management measures remain effective and aligned with changing circumstances. Risk management performance is monitored and reported on a **quarterly basis** to support management oversight and decision-making. The review process facilitates the continuous improvement of risk management practices, taking into account changes in the operating environment, emerging risks, and significant organizational developments. Where risk management outcomes do not achieve the established objectives, corrective actions and improvement measures are defined and implemented to strengthen the effectiveness of risk management across the organization.

Related Documents

- Risk Management and Internal Control Policy
  https://www.egat.co.th/home/policy-risk-internal-control/
- Guidelines on Good Governance, Risk Management, and Compliance (GRC)
  https://www.egat.co.th/home/policy-risk-internal-control/

Remark: The detailed GRC Structure, including the roles and responsibilities of the 1st Line of Defense ("Owner"), 2nd Line of Defense ("Oversee"), and 3rd Line of Defense ("Independent Assurer"), is provided in the Guidelines on Good Governance, Risk Management, and Compliance (GRC). The source document is available in Thai language. Please refer to the supporting note and translation provided in the additional comments section.

As organizations transition into the digital era, EGAT has adopted digital technologies to enhance operational efficiency. However, this shift also introduces cybersecurity risks, such as server attacks, network intrusions, and other forms of cyber threats. To address these challenges, EGAT conducts annual assessments of cybersecurity and information risk.

EGAT continued its enterprise-level cybersecurity risk management efforts from 2023, implementing both existing controls and mitigation plans to reduce risk severity to an acceptable level (Risk Appetite). Key measures included strengthening access control for critical systems, regularly reviewing and updating access rights to sensitive systems and data, and conducting phishing email simulations to raise cybersecurity awareness among employees. These simulations featured diverse email content and were accompanied by targeted communications before and after testing to reinforce learning.

As a result of implementing access control measures, EGAT reviewed system access rights and notified system administrators to restrict access in accordance with ISO/IEC 27001 standards. The enhanced phishing email content led to a reduction in the number of employees who fell for simulated attacks, meeting the organization's targets. Consequently, EGAT's cybersecurity risk management in 2024 achieved its objectives, with no severe cyber incidents impacting the organization.

Emerging Risks:

EGAT recognizes that emerging risks may arise from changes in the business, regulatory, environmental, technological, and social landscape. The organization continuously assesses potential impacts and implements proactive measures to strengthen resilience and support sustainable operations. Examples of key emerging risks and corresponding management approaches are presented below:

AI-Driven Threats to Intelligent Power Systems

Description

Rapid advancements in artificial intelligence are creating new forms of cyber threats that have not previously been encountered in the power sector. AI-enabled malware and autonomous attack tools may significantly increase the speed, scale, adaptability, and sophistication of cyberattacks against critical energy infrastructure. As EGAT continues to expand the use of digital technologies, automation, and intelligent power systems, the emergence of AI-driven cyber threats introduces unprecedented risks for which industry experience and established response practices remain limited.

Impact

Over the long term, AI-driven cyber threats could affect the security and resilience of critical systems supporting electricity generation, transmission, and grid operations. The increasing convergence of operational technology (OT) and information technology (IT) may create new vulnerabilities requiring substantial investment in cybersecurity capabilities, system architecture, and workforce competencies. If threat actor's leverage advanced AI to bypass conventional controls, EGAT may need to adapt its digital transformation strategy, cybersecurity governance framework, and technology deployment approach to maintain operational reliability, energy security, and stakeholder trust.

Mitigation

EGAT continuously strengthens its cybersecurity governance and resilience capabilities through advanced threat monitoring, cyber risk assessments, incident response planning, and protection of critical OT and IT systems. The organization is enhancing preparedness for emerging AI-driven threats by integrating cyber risk considerations into digital transformation initiatives, strengthening cyber defense capabilities for intelligent power systems, conducting cybersecurity exercises, and monitoring technological developments to ensure that cybersecurity strategies remain effective against increasingly sophisticated AI-enabled attack methods.