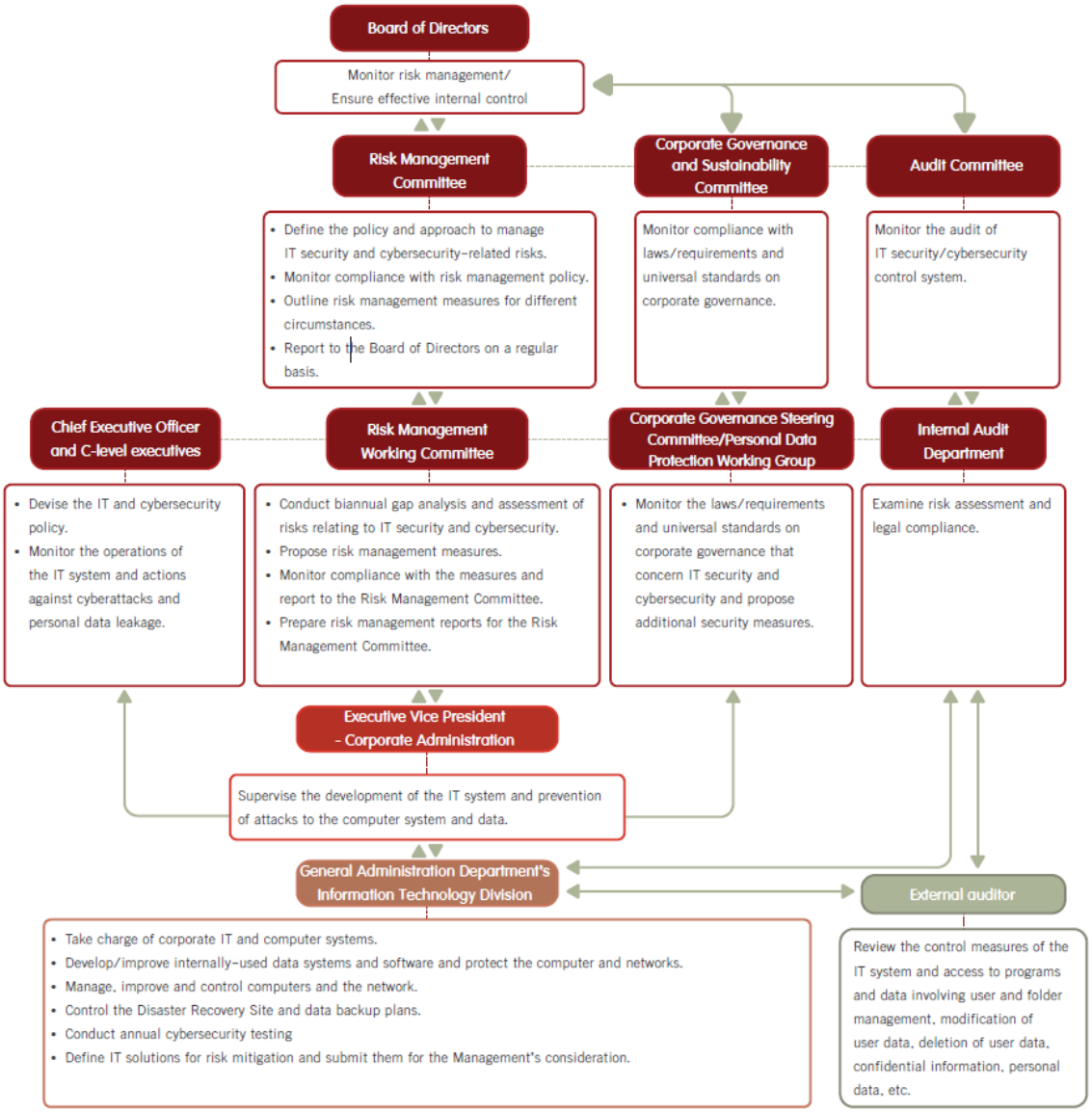
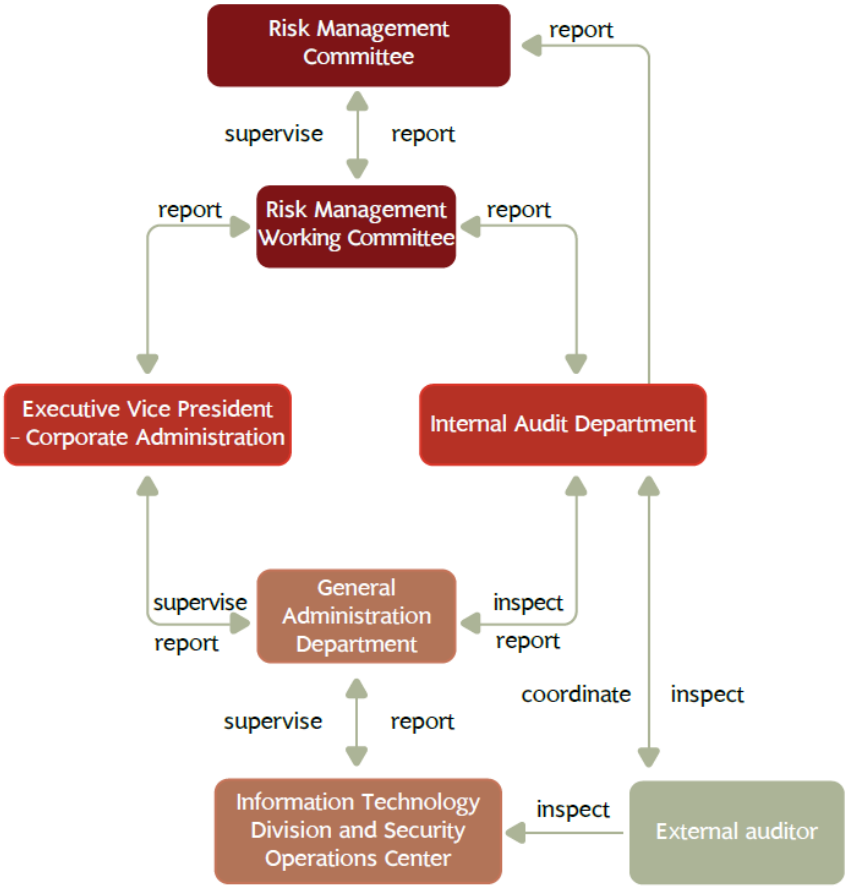
## IT Security and Cybersecurity

Cyberattacks are a significant global risk, according to World Economic Forum's Global Risks Report 2024. RATCH, considering cyberattack a risk due to possible impacts on the operations, has given importance to cybersecurity and the security of information technology to ensure business continuity and proper protection of confidential information. In this regard, the Information Technology Division under the Corporate Administration Function is the primary unit responsible for the information technology system as well as IT security and cybersecurity. The division performs its duties under the Company's IT and cybersecurity policy and operational guidelines, to preserve competitiveness and retain stakeholders' trust.

**Structure of IT security and cybersecurity supervision**



IT security monitoring




## Responsibilities

| | |
|---|---|
| **Risk Management Working Committee** | Follow up on IT security and cybersecurity measures twice a year |
| **Internal Audit Department** | 1. Review compliance with following policies/standard practices;<br>• Information Technology Security Policy<br>• Efficiency and adequacy of risk mitigation and security systems<br>• Emergency response plan in light of disasters<br>• Exercise of emergency plan under the Business Continuity Plan<br>• Security measures for computer equipment<br>• Assessment of security risks of the IT system<br>2. Report the cyberthreat watch on an annual basis |
| **Information Technology Division and SecurityOperations Center** | Monitor, track, screen, prevent and respond to cyberattacks, originated internally or externally; and monitor IT systems such as Intrusion Prevention System, Firewall and Cybersecurity Protection System. |
| **External Auditor** | Review the IT system control and access to programs and data relating to folder management, user access modification and user revocation, etc. The annual review is included in the annual audit of the Company's financial statements. |

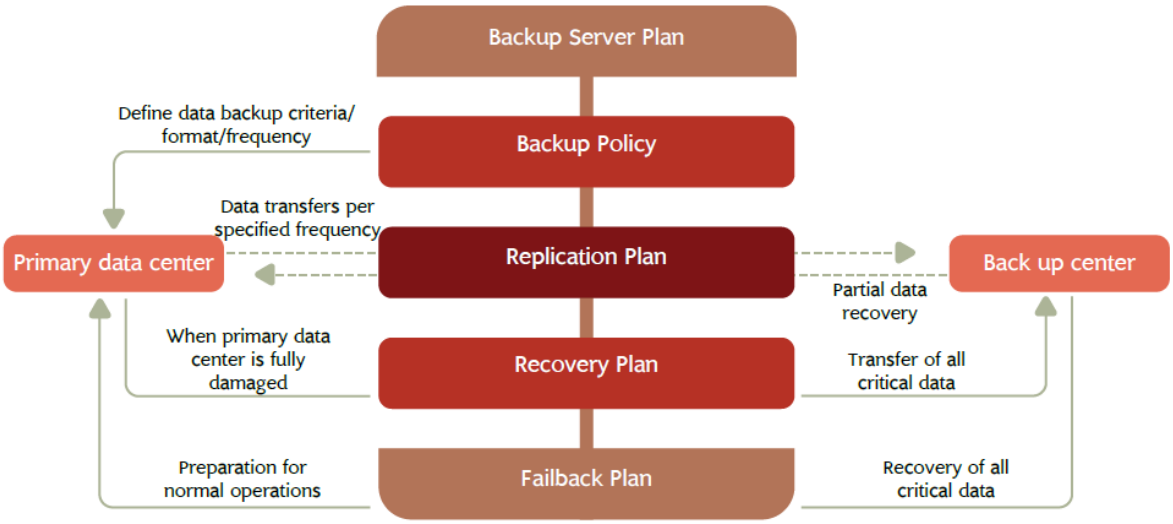
**IT and cybersecurity risks**

The Company conducted IT and Cyber risks and clearly identified control and mitigation measures as following:

| **Risk factor:** Physical and environmental risk | **Level of residual risk:** Low |
|---|---|
| **Nature of risk:** Internal and external user's access, usage and system check of Data Center Room where servers are located | |
| **Control measures:**<br>• Install the system to block unauthorized access and the finger scan system that limits access only to authorized persons; control the Data Center Room's entry and exit of the outsourced party; and examine the entry and exit log on a monthly basis.<br>• Prepare inspection by the Internal Audit Department and the external auditor. | |
| **Risk factor:** Usage of application software on the Company's computers | **Level of residual risk:** Low |
| **Nature of risk:** Installation of unsafe or malicious software, intentionally or unintentionally | |
| **Control measures:**<br>• Impose the computer and network usage regulations.<br>• Install Firewall as well as Endpoint Protection and Data Inventory software for malware prevention; and inspect the effectiveness.<br>• Raise employee awareness against the installation of unprovided programs on a regular basis and identify penalties for breach. | |
| **Risk factor:** Usage of corporate network | **Level of residual risk:** Low |
| **Nature of risk:** Outsiders' access or attacks | |
| **Control measures:**<br>• Establish cyberthreat protection to block access/attacks on servers and in-use computers.<br>• Establish the 24-hour Security Operation Center (SOC), powered by AI or manpower, to watch out for and prevent external attacks to the Company's system/equipment. | |
| **Risk factor:** Personal risks from inappropriate authorization | **Level of residual risk:** Low |
| **Nature of risk:** Data access and modification by unauthorized persons | |
| **Control measure:** Set control on computer system access and usage and install the intrusion prevention system. | |
| **Risk factor:** Disasters and emergency incidents | **Level of residual risk:** Low |
| **Nature of risk:** Man-made and natural disasters, interrupted power supply, and protests that may disrupt production/business operations | |
| **Control measure:** Prepare the IT-related Disaster Response Plan and Business Continuity Plan; and schedule an annual review and exercise. | |
| **Risk factor:** Incompatibility in management | **Level of residual risk:** Medium |
| **Nature of risk:** Incompatibility of policy and guidelines for possible risks/incidents | |
| **Control measures:**<br>• Assess risks, likelihood, impacts, directions and trends encompassing risks associated with the production, job operators or emergency situations.<br>• Schedule an annual review on the policy, guidelines and response plan to emergency situations.<br>• Organize training to raise awareness in the cyberthreat policy, guidelines and protection.<br>• Run a test on data backups and SAP by internal and external parties.<br>• Seek an external audit on IT system control/protection. | |

| Risk factor: AI management | Level of residual risk: Medium |
|---|---|
| **Nature of risk:** Inappropriate and uncontrolled application of AI technology that causes harm or data leakage | |
| **Control measures:**<br>• Educate employees on appropriate and safe application of AI technology.<br>• Establish AI policy/usage guidelines.<br>• Develop the AI usage system that is systematic, safe and verifiable. | |

RATCH has established the backup center and recovery plans for disasters and emergency incidents relating to IT security and cybersecurity, in preparation for emergencies that may affect the IT system's capabilities and effectiveness. The response process is as follows:




**Escalation process for employees to report incidents**