Governance：

Compliance

Our Concept of Compliance

The Mitsubishi Electric Group regards "ethics and compliance" as the foundation of corporate management, and issues the message to all officers and employees as part of its efforts to establish even stronger relationships of trust with customers, stakeholders and society.

Compliance Motto – "Always Act with Integrity"

Always Act with Integrity
いかなるときも「誠実さ」を貫く

The Mitsubishi Electric Group established a compliance motto "Always Act with Integrity" for all Mitsubishi Electric Company's officers and employees on June 1, 2021."Integrity" means the strong will and attitude to persist in doing the right thing and having character traits such as "being fair," "being honest," "being sincere," "taking responsibility for one's behavior" and "respecting others."

At the same time of the establishment of the compliance motto, we established "Questions to test for Integrity" as a hint for officers of employees to ask themselves whether their action or decision is right if they are at a loss as to whether their action or decision is right.

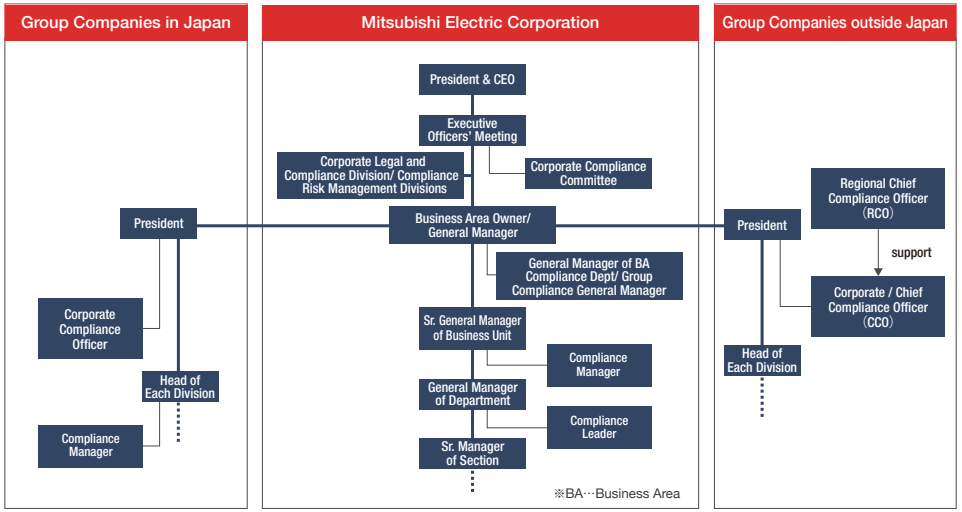
Questions to test for Integrity

1	Is your action or decision in line with laws and regulations, internal rules, contractual terms or this Code of Conduct?
2	Can you tell your family and friends about your action or decision without feeling ashamed?
3	Will you be proud of your action or decision if it is reported in the mass media or social media?
4	Does your action or decision give priority to compliance over other considerations, e.g., profit, efficiency, etc.?
5	Can you rationally and honestly defend your action or decision without having to give excuses such as, "It is just a small thing, there will be no problem"; "It will not be found out "; "I need to do this for the company"; "It has been done this way for a long time"; "My senior colleague also did that" or "I was instructed by my superior"?
6	Do you first assess if your superior's instructions are right in light of this Code of Conduct before acting upon the instructions?

Mitsubishi Electric Group Compliance Promotion Structure

The Mitsubishi Electric Group's compliance promotion structure is based on the recognition that the promotion of compliance is inseparably linked with business promotion. Based on this structure, the President and CEO of Mitsubishi Electric Corporation is the chief compliance promotion officer, and each Mitsubishi Electric business division as well as each affiliate in Japan and overseas proactively promotes compliance.

The Corporate Compliance Committee has been established as a company-wide organization in order to formulate overall compliance policies for the Mitsubishi Electric Group, to develop measures to maintain and strengthen the systems necessary to promote compliance, and to share information.



■Mitsubishi Electric Group compliance promotion structure

Meeting of compliance managers in the Europe region

Meeting of compliance managers in the Korea region

Governance：

Risk Management

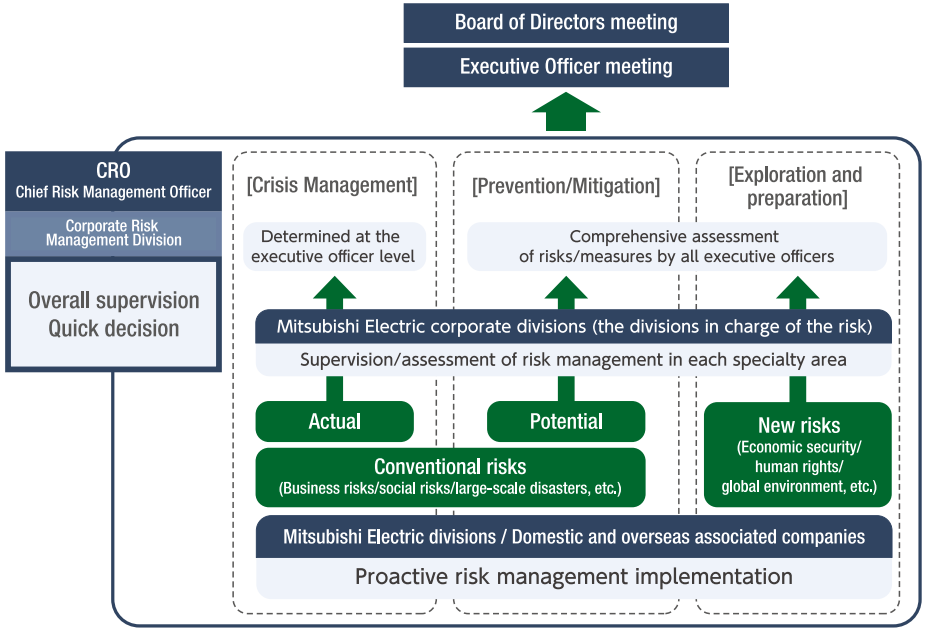
Basic Policy

With overseas revenue accounting for over 50%, the Mitsubishi Electric Group aims to transform into a “Circular Digital-Engineering Company” in a wide range of business areas. We also take the various compliance incidents that came to light seriously and have been working to improve our internal control system and others. To fulfil its responsibility to all stakeholders beginning with society, customers, shareholders, and employees, and to realize sustainability, the Group appropriately manages risks associated with the conduct of its business while strengthening its internal control system with an emphasis on prevention. Specifically, the framework incorporates risk management into business activities whereby risks are managed according to the size and characteristics of each business. Significant risks common to the entire Group are managed and prioritized according to their impact on the management of the Group as a whole. For new risks, such as human rights, demand for decarbonization, geopolitical risks, and game-changing trends in the future, we will respond in an effective manner through cross organizational and flexible team behavior.

Risk Management Framework

Risk management is implemented independently by each division and by domestic and overseas associated companies. In addition, the Group has built a framework to enable appropriate and quick decision making where Mitsubishi Electric's each corporate division (division in charge of risk management) supervises and assesses each division and domestic and overseas associated companies in their respective specialized areas, and a CRO (Chief Risk Management Officer) and a Corporate Risk Management Division supervise the entire Group.

We will focus on a wide variety of risks according to their degree of impact on the management of the entire Group, and will not only respond to conventional risks such as large-scale disasters and social risks, but also flexibly and strategically investigate and prepare for new risks in areas such as economic security, human rights, and the global environment. In particular, important matters related to management supervision and execution are deliberated upon and decided at the Board of Directors meetings and the Executive Officer meetings.



■Risk management framework (Mitsubishi Electric Group)

Economic Security

Against the backdrop of the recent competition for dominance in technology between the U.S. and China, more countries are introducing their unique systems that are beyond the traditional export controls based on international agreements within investment, procurement, development, human resources, network, data management, and so on. As tensions rise in the international community due to the global economic turmoil caused by the COVID-19 pandemic, Russia's invasion of Ukraine, and other events, risk management should go beyond the status quo of individual compliance in order to decipher the background and intent of policies and regulations from a bird's-eye view and the necessary control measures should be implemented accordingly.

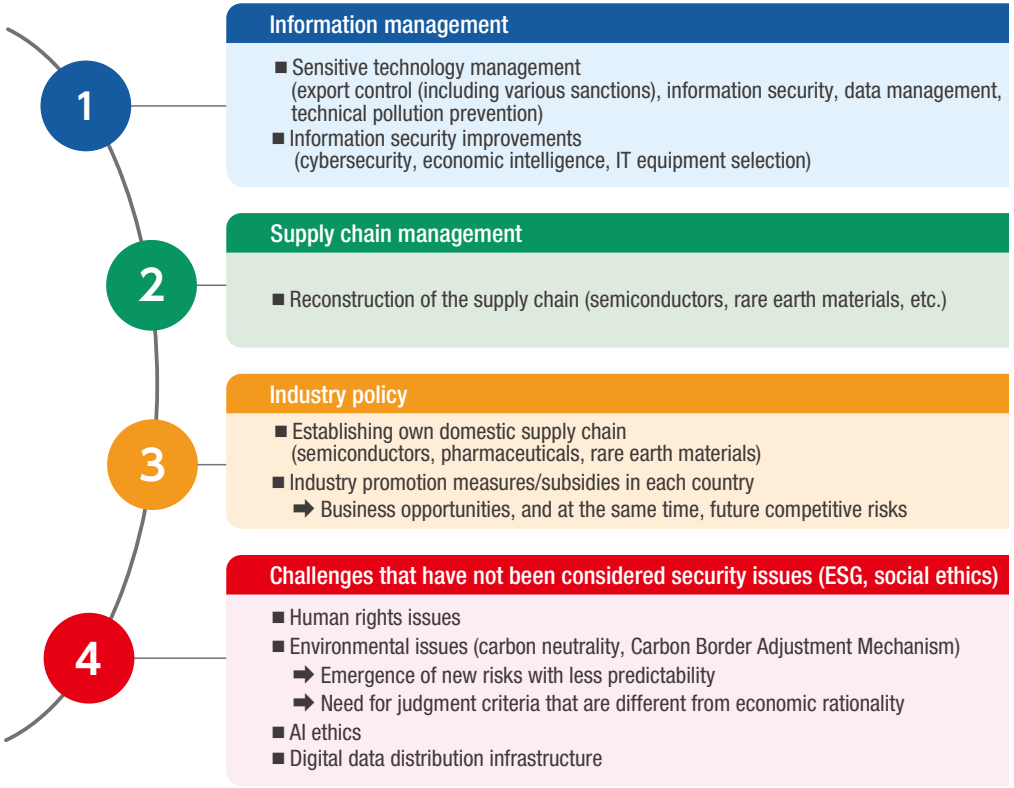
Meanwhile, there is growing concern about forced labor and environmental issues in supply chains. With respect to the former in particular, the U.S. has enacted the Uyghur Forced Labor Prevention Act, and Japan has issued "Guidelines for Respecting Human Rights in Responsible Supply Chains, etc." In these areas, there is a steady shift from soft law norms created by NGOs and NPOs to hard law, and the EU is also preparing the EU Corporate Sustainability Due Diligence Directive (CSDDD). It is important for risk management to properly identify trends and respond to them at as early a stage as possible, including by participating in rulemaking.

In addition, the geopolitical risks that have arisen as a result of Russia's invasion of Ukraine are directly related to supply chain disruptions and the risk of supply disruptions for critical commodities. To ensure business continuity, it is essential to identify vulnerable items and commercial distribution channels as well as to strengthen supply chains through appropriate risk control.

In addition to compliance with individual regulations as we have been thus far, in order to keep up with the dynamic changes in the economic security environment, we have set up the Corporate Economic Security Division directly under the president. This division investigates and analyzes technologies, policy trends and legal systems related to security as well as implements integrated management from a perspective of comprehensive economic security as it relates to company-wide information management, supply chains, industry policies, ESG, and social ethics.

We have also created a groupwide economic security system by setting up the Economic Security Secretariat in each department, the Economic Security Office in affiliated companies in Japan, and the Economic Security Administrator in affiliated companies overseas.

The four aspects of economic security considered by Mitsubishi Electric



Governance：

Information Security

Basic Policy

In order to prevent the recurrence of a data leak incident caused by unauthorized system access, the Mitsubishi Electric Group will continue to strengthen its information management and utilization systems and other functions, and it will strengthen its security measures for cyberattacks. As a specific target, we will aim to achieve level 2 or higher in the Cybersecurity Maturity Model Certification (CMMC ver. 2).*

Mitsubishi Electric manages information entrusted to the company by its customers and stakeholders and confidential corporate information relating to sales, engineering, intellectual property, and other areas. This management is carried out based on the Declaration of Confidential Corporate Information Security Management established in February 2005. In light of past events, we will once again work to increase awareness of this declaration further within the Mitsubishi Electric Group and strive to protect and manage information even more carefully.

* Framework for Cybersecurity Maturity Model Certification set forth by the U.S. Department of Defense. Level 2 or higher means that excellent security measures and management systems are put in place.

web Declaration of Confidential Corporate Information Security Management

Framework and Guidelines

A new "Corporate Information Security Division" was established under the direct control of the president, to oversee all the Group's information security management. Since April 2020, it has integrated three functions that were previously separate: management of confidential corporate information and personal data protection, information system security, and product security. Since April 2021, we have enhanced the structure and add members of Corporate Information Security Division. In addition, we will invest more than ¥50 billion to implement cybersecurity measures and establish sustainable information security management system so that we can achieve Level 2 or higher of the Cybersecurity Maturity Model.

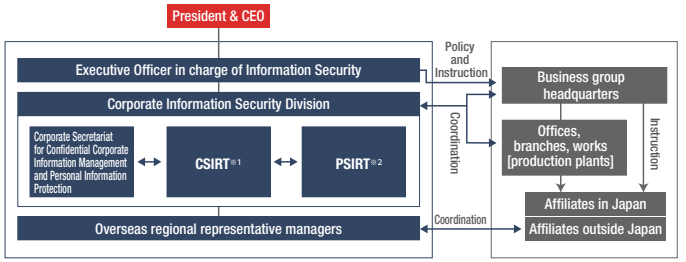
The Executive Officer in charge of Information Security is responsible for the Group's overall information security management. Under this officer's direction, the Corporate Information Security Division is in charge of planning and implementing the Group's information security management structure and rules as well as activities to ensure the security of information systems. The Division is striving to ensure information security by working closely with the Computer Security Incident Response Team (CSIRT) established in each business group and office that utilizes and manages the data and systems.

As other companies suffered cyberattacks that affected their factory productivity, Mitsubishi Electric also formed a section to ensure factory security, thereby bolstering preparedness.

In addition, as part of PSIRT activities*1 to promote product security measures, we were accredited as a CNA*2 in November 2020 and we now assign CVE IDs*3 to vulnerabilities that affect Mitsubishi Electric products and publish them by ourselves. This has strengthened a framework to practice efficient vulnerability handling with external stakeholders. Identified vulnerabilities are reported, instructions are given in keeping with this framework, and appropriate response is taken to prevent secondary damage.

Business groups and offices (offices, branches, works [production plants]) issue instructions and guidance on information security to affiliates in and outside Japan. Paying special attention to the circumstances and special characteristics of overseas affiliates, the Corporate Information Security Division will build close cooperative relations with overseas regional representative managers at sites in the Americas, Europe, and Asian countries to ensure information security.

*1 PSIRT is an abbreviation for Product Security Incident Response Team, which works on the security quality of products and services.
*2 CVE Numbering Authority. CVE is an abbreviation for Common Vulnerabilities and Exposures.
*3 Internationally used vulnerability identifiers



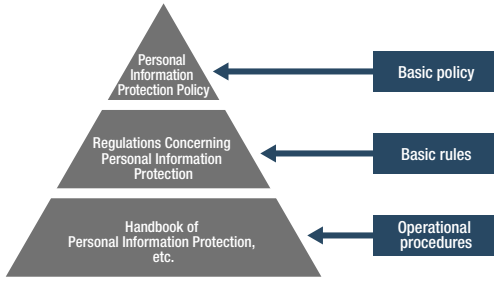
■Information security organization structure (Mitsubishi Electric Group)

Personal Information Protection

In efforts to protect personal information, Mitsubishi Electric first created company rules on personal information protection in October 2001, and since then it has required all employees and affiliated persons to obey those rules strictly. Mitsubishi Electric issued a personal information protection policy in 2004, complying with the requirements of JIS Q 15001:2006 Personal Information Protection Management Systems. In January 2008, we were granted the right to use the "PrivacyMark," which certifies the establishment of management systems that ensure proper measures for personal information protection. We have maintained our "PrivacyMark" certification until the present.

We have also conducted a review of our internal regulations to ensure a proper response to Japan's amended Act on the Protection of Personal Information, which went into force in April 2022.

web Privacy Policy



■System of rules for personal information protection

Cyber-Attack Countermeasures

Cyber-attacks have become a major threat for businesses as they are growing increasingly sophisticated and diverse year-by-year. The Mitsubishi Electric Group is centrally managing the network, devices, and servers (cloud) and working to implement a multilayered defense which is based on the concept of zero-trust security* as countermeasures for cyber-attacks that are growing increasingly sophisticated and diverse, along with the wider use of cloud services and the wider adoption of teleworking. A multilayered defense lets us protect ourselves from cyber-attacks, detect suspicious signs and intrusions, and put in place a system to respond immediately should an incident occur, to prevent or minimize damage.

In addition, we have implemented multi-factor authentication that supports operations being conducted through access from offices, teleworking sites, and business trip destinations, and we manage authentication in a centralized manner. Internet websites are constantly exposed to many external threats, and so we only launch websites that are approved by Mitsubishi Electric in order to maintain a high security level.

* Concept of not giving trust to anything either inside or outside of the company, and testing and authorizing all communication attempts.